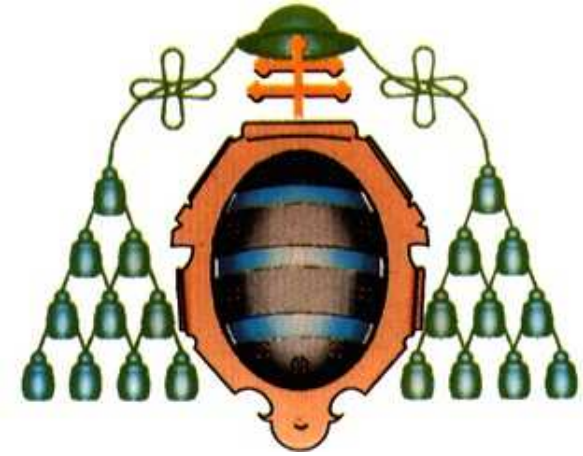


UNIVERSIDAD DE OVIEDO

DEPARTAMENTO DE MATEMÁTICAS

ON ASYMPTOTICALLY GOOD STRONGLY MULTIPLICATIVE LINEAR SECRET SHARING

TESIS DOCTORAL DE

Ignacio Cascudo Pueyo

UNIVERSIDAD DE OVIEDO

DEPARTAMENTO DE MATEMÁTICAS

Ignacio Cascudo Pueyo

ON ASYMPTOTICALLY GOOD STRONGLY MULTIPLICATIVE LINEAR SECRET SHARING

Tesis doctoral dirigida por:

Consuelo Martínez López (Universidad de Oviedo)

Ronald Cramer (Leiden University/ CWI Amsterdam)

Junio 2010

Agradecimientos/ Acknowledgements

Quiero expresar en primer lugar mi agradecimiento a mi directora de tesis, Consuelo Martínez, por el trabajo, ayuda y tiempo que he recibido de ella durante todos estos años, en especial, por supuesto, a la hora de su finalización. También quiero agradecer, por su apoyo y consejos, a todos los compañeros en el grupo de Álgebra, Codificación y Criptografía de la Universidad de Oviedo: Conchita López, Elena Couselo, Ignacio Fernández Rua, Alejandro Piñera, Pelayo Puche, Hugo Villafañe, Cristina García Pillado y Adriana Suárez Corona, así como a Maribel González Vasco (actualmente en la Universidad Rey Juan Carlos, pero que perteneció a este grupo antes de que yo me incorporara) y a Santos González por la creación de este grupo de investigación y su especial entusiasmo en todo lo que rodea a este tema, así como en que yo me incorporara al grupo. Querría hacer especial mención a Ignacio, quien también ha contribuido con comentarios muy valiosos a la redacción del texto final, así como a Cristina y Adriana, por su gran apoyo en los últimos meses de redacción del trabajo y sin las cuales todo se habría hecho mucho más difícil. Espero poder devolverles algún día toda esta ayuda.

Durante todos estos años han sido muchas las personas con las que he trabajado, comentado ideas y problemas y de quienes en definitiva he aprendido mucho. No quiero hacer una lista detallada, puesto que estoy seguro de que me olvidaría de alguien, pero querría mencionar en especial a Carles Padró y a Oriol Farrás de la Universidad Politécnica de Catalunya, con los que he trabajado, discutido ideas y compartido buenos momentos y espero seguir haciéndolo en años venideros.

Este trabajo fue posible gracias a la financiación de la beca-contrato de Formación de Profesorado Universitario (AP2005-0836) actualmente gestionada por el Ministerio de Educación de España, cofinanciada por el Fondo

Social Europeo. También recibí ayudas de los proyectos MTM2007-67884-C04-01 del Ministerio de Ciencia e Innovación e IB-08-147 del FICYT.

I would like to thank my other advisor, Ronald Cramer, in first place for inviting me to the CWI of Amsterdam where I had the opportunity to meet and work with some of the best experts in the world in the topic of cryptography. Collaboration with Ronald has been very fruitful over these years and I am glad I have had the opportunity to participate in the development of a new research topic on which I have enjoyed a lot working. Of course I would also like to thank all members of the group of cryptology of the CWI from whom I have learnt a lot. But I have to highlight former member Robbert de Haan, coauthor of one of my works and with whom I really enjoyed working. Alp Bassa and Otto Johnston also helped me by reading some parts of this dissertation and providing valuable comments.

I also want to thank the rest of my coauthors, Hao Chen and Chaoping Xing, who contributed a lot to the quality of my research with their ideas. I also performed two short but very successful stays in the Nanyang Technical University in Singapore invited by Chaoping in which I had a great time. Some other people have also suggested ideas which have led to some nice results, especially Alp Bassa, Peter Beelen and Bas Edixhoven, which contributed to the results of Chapter 10. Berry Schoenmakers also provided many useful comments about the text. Surely many other people have also indirectly contributed to this thesis and I want to thank all these people for that.

He querido dejar para el final a mi familia, que son las personas que más me han apoyado durante estos años y que han tenido que sufrir en mis malos momentos durante este tiempo con mis problemas y dificultades que gracias a su apoyo incondicional he conseguido superar.

Y en general, a todos aquellos que me habéis ayudado de una u otra manera a finalizar este trabajo con éxito.

Contents

Resumen

Contexto

Los esquemas de compartición de secretos fueron introducidos en 1979 de forma independiente por Shamir [72] y Blakley [12]. Un esquema de compartición de secretos es una herramienta combinatoria que permite dividir el conocimiento acerca de cierto secreto s en varios fragmentos de información $a_1, a_2, \ldots, a_n$, de tal manera que cualquier conjunto lo suficientemente grande de estos fragmentos determina completamente el secreto, mientras que cualquier conjunto pequeño de fragmentos es independiente de él. Los esquemas de compartición de secretos tienen numerosas aplicaciones en criptografía. Aunque originalmente fueron propuestos como un medio de almacenar claves criptográficas, posteriormente fue utilizado en otras áreas dentro de la criptografía como la *threshold cryptography* ("criptografía umbral", cuyo estudio fue iniciado en [35]) o la computación multiparte, de la que volveremos a hablar más adelante. Algunas de estas aplicaciones requieren esquemas de compartición de secretos con algunas propiedades algebraicas adicionales. En esta tesis, consideraremos esquemas de compartición de secretos lineales (ECSL) ideales *con t-multiplicación fuerte*.

La linealidad es una propiedad que garantiza que tanto el secreto como los fragmentos son elementos de espacios vectoriales sobre cierto cuerpo finito $\mathbb{F}_q$ y que si dos secretos s y s' tienen como "vectores de fragmentos" $(a_1, a_2, \ldots, a_n)$ y $(a'_1, a'_2, \ldots, a'_n)$ respectivamente, entonces para cualquier elemento $\lambda \in \mathbb{F}_q$, $(a_1 + \lambda a'_1, a_2 + \lambda a'_2, \ldots, a_n + \lambda a'_n)$ es un vector de fragmentos del secreto $s + \lambda s'$. Los esquemas lineales *ideales* son aquellos en los que el secreto y todos los fragmentos son elementos del propio cuerpo $\mathbb{F}_q$.

Cramer, Damgård y Maurer [32] introdujeron las propiedades de multiplicación y t-multiplicación fuerte de un esquema de compartición de secretos lineal ideal. Un esquema de este tipo tiene multiplicación si el conjunto de los productos de fragmentos $(a_1a'_1, a_2a'_2, \ldots, a_na'_n)$ determina el producto de los secretos ss'. Y tiene t-multiplicación fuerte si satisface dos requerimientos: por una parte tiene t-privacidad, es decir, cualquier conjunto de t fragmentos (o menos) es independiente del secreto; por otro lado si quitamos cualquier conjunto de t fragmentos, el esquema tiene multiplicación para el conjunto de $n - t$ fragmentos restantes.

Las aplicaciones originales de los esquemas de compartición de secretos lineales ideales con t-multiplicación fuerte pertenecían al dominio de la computación multiparte (MPC). Se ha realizado una investigación muy prolífica en este área de la criptografía en los últimos 20 años. Se pueden consultar

algunos resúmenes de la investigación en este área en [27] o la tesis doctoral de Robbert de Haan [42].

A grandes rasgos, la computación multiparte estudia el siguiente problema: un conjunto de participantes $P_1, \ldots, P_n$, cada uno de los cuales posee un cierto dato privado $x_1, \ldots, x_n$ quiere computar de forma conjunta una función pública de estos datos $f(x_1, \ldots, x_n)$ sin revelar más información de la necesaria acerca de ellos, y esto debería seguir siendo así incluso si algunos de los participantes hacen trampas de forma coordinada. De forma un poco más precisa, se persiguen tres objetivos: ningún subconjunto de participantes $S = \{P_{i_1}, \ldots, P_{i_t}\}$ que puedan coordinarse para hacer trampas debería obtener más información acerca del dato privado x_j de un participante $P_j \notin S$ que la que se puede obtener a partir de sus datos iniciales $\{x_{i_1}, \ldots, x_{i_t}\}$ y la evaluación de la función $f(x_1, \ldots, x_n)$ que obtienen (*privacidad*); además la posible intervención de un conjunto de participantes tramposos no puede evitar que la computación de la función finalice (*robustez*) y que el resultado obtenido por el resto de participantes sea el valor correcto $f(x_1, \ldots, x_n)$ (*correctitud*). Otro modo de entender los objetivos de la computación multiparte es considerar que los participantes deberían *emular*, por medio de un protocolo, un escenario ideal donde existe una tercera parte de confianza que es incorruptible, recibe los datos $x_1, \ldots, x_n$ de los participantes, calcula $f(x_1, \ldots, x_n)$ y les comunica este valor. En el protocolo real, los participantes no tienen acceso a esta tercera parte de confianza ideal, sólo pueden enviarse mensajes unos a otros (supondremos que cada par de participantes se puede comunicar por medio de un canal privado, de forma que el contenido de los mensajes enviados entre ellos permanece inescrutable para los demás participantes). Sin embargo la información obtenida acerca del resultado de la computación y de los datos de los demás participantes debería ser la misma que en la situación ideal.

Que un protocolo de computación multiparte cumpla los objetivos anteriores depende de qué conjuntos de participantes pueden cooperar para hacer trampas. Normalmente se supone que los participantes tramposos han sido corrompidos por cierto adversario externo, que obtiene toda la información recibida por ellos durante el protocolo y controla totalmente las acciones que estos ejecutan, por lo que les puede hacer desviarse del protocolo de forma coordinada. Para los participantes honestos no es posible, al menos al principio del protocolo, determinar qué participantes son corruptos y por tanto se considera que el adversario puede corromper cualquier conjunto en cierta familia de subconjuntos de $\{P_1, \ldots, P_n\}$. El ejemplo más frecuente es

que el adversario puede corromper cualquier subconjunto de como mucho t participantes, para cierto entero t.

En 1988, Ben-Or, Goldwasser y Wigderson [10] e (independientemente) Chaum, Crépeau y Damgård [21] demostraron el teorema fundamental de la computación multiparte *incondicionalmente* segura. Este resultado afirma que cualquier función puede ser calculada por un conjunto de n participantes intercambiando una cantidad total de información polinomial en el número de participantes n y en el tamaño de cierta descripción de la función y además el protocolo es incondicionalmente seguro si el adversario corrompe como mucho $t < n/3$ participantes. Aquí, la palabra incondicional quiere decir que el protocolo es seguro independientemente del poder computacional del adversario. Por tanto, la seguridad del protocolo no depende del hecho de que cierto problema matemático no pueda ser resuelto eficientemente por el aadversario, como es el caso en otras áreas de la criptografía, por ejemplo el cifrado de clave pública. Por supuesto, existen muchos resultados interesantes relativos a la computación multiparte con seguridad *computacional*, comenzando con el trabajo de Goldreich, Micali y Wigderson [40], pero no nos ocuparemos de ellos aquí.

Los protocolos de computación multiparte de [10] y [21] utilizan los esquemas de compartición de secretos de Shamir, que se propusieron ya en [72]. Estos esquemas de compartición de secretos lineales ideales se pueden definir para cualquier cuerpo finito $\mathbb{F}_q$ y cualquier número n de fragmentos siempre que $n < q$. Además tienen t-multiplicación fuerte para cualquier entero t tal que $3t < n$.

Los protocolos se basan en el hecho de que toda función se puede escribir como un circuito aritmético sobre algún cuerpo finito $\mathbb{F}_q$ (es decir tanto los datos iniciales como el resultado de la evaluación son elementos del cuerpo $\mathbb{F}_q$ y el resultado de la función se puede calcular por medio de un circuito en el que las puertas son sumas o multiplicaciones de dos variables o de una variable por un elemento fijo del cuerpo $\mathbb{F}_q$). Usan el esquema de compartición de secretos de Shamir como una suerte de *sistema de cifrado dedicado* con el que todos los participantes pueden "cifrar" cierta información pero sólo un conjunto suficientemente grande de participantes puede descifrarla (reuniendo los fragmentos que cada uno tiene). La linealidad y t-multiplicación fuerte implican que este mecanismo de cifrado tiene propiedades homomórficas en el sentido de que conociendo los cifrados de dos elementos a y b del cuerpo $\mathbb{F}_q$, los participantes pueden calcular, mediante un proceso interactivo si es necesario, un cifrado de cualquier función lineal de a y b o del producto

ab, *sin revelar información alguna acerca de a y b* al adversario. Además, el adversario no puede impedir que estas computaciones se completen con éxito. Por tanto en cada puerta del circuito, los participantes del protocolo pueden computar de forma segura un cifrado de la salida de la puerta a partir de cifrados de las entradas. Los participantes solo descifran (de forma conjunta) el resultado de la función, y no los valores cuyos cifrados han sido computados en los pasos intermedios. El adversario no puede interrumpir este descifrado abandonando el protocolo, ya que los demás participantes conocen suficientes fragmentos del resultado para poder recuperarlo. La correctitud de este paso de descifrado se basa en parte en técnicas de corrección de errores, que permiten el descifrado eficiente del resultado en presencia de fragmentos incorrectos, desbaratando por tanto cualquier intento del adversario de evitar el éxito del protocolo comunicando información falsa a los participantes honestos en este último paso.

Aunque estos protocolos usan implicitamente las propiedades del esquema de Shamir que hemos mencionado antes, la propiedad de t-multiplicación fuerte no fue definida explícitamente en estos artículos. Cramer, Damgård y Maurer [32] no sólo introdujeron la noción de esquema de compartición de secretos lineal con t-multiplicación fuerte, sino que de hecho generalizaron los resultados anteriores, demostrando que a partir de cualquier esquema con n fragmentos que satisfaga estas propiedades (y no sólo de los esquemas de Shamir) podemos construir un protocolo eficiente de computación multiparte para n participantes para computar un circuito aritmético sobre $\mathbb{F}_q$ y que es incondicionalmente seguro contra cualquier adversario que corrompa t participantes. Por tanto, para obtener las mejores construcciones en términos de seguridad, necesitamos utilizar esquemas de compartición de secretos lineales ideales con la mayor tolerancia de corrupción posible, la que se define como el cociente $\frac{3t}{n-1}$. Otra propiedad muy interesante de cualquier esquema de compartición de secretos lineal con t-multiplicación fuerte es que, como fue demostrado en [28], existe un algoritmo que permite la reconstrucción eficiente de un secreto a partir del conjunto de todos los fragmentos incluso si algún subconjunto de t de estos fragmentos son erróneos.

Algunos esquemas de Shamir tienen la mejor tolerancia de corrupción para esquemas de compartición de secretos lineales ideales, así que cuando los utilizamos en la construcción de Cramer, Damgård y Maurer obtenemos los mejores protocolos de computación multiparte en términos de seguridad, y en este sentido podemos decir que los protocolos de [10], [21] son casos particulares "óptimos". El inconveniente es que, como hemos dicho, los es-

quemas de Shamir sólo están definidos si $n < q$ y por lo tanto no se pueden utilizar para construir un protocolo de computación multiparte para computar un circuito aritmético sobre $\mathbb{F}_q$ para n participantes si $n \geq q$, al menos no utilizando la construcción de [32]. Una posible solución sería llevar a cabo los cálculos en $\mathbb{F}_{q^k}$, una extensión de $\mathbb{F}_q$ tal que $q^k > n$, pero esto haría crecer la complejidad de comunicación del protocolo, ya que cualquier elemento comunicado durante un paso en el que se comparte un secreto pertenecería a $\mathbb{F}_{q^k}$ y por tanto la cantidad de información enviada sería k veces mayor.

Una alternativa es buscar esquemas de compartición de secretos lineales ideales sin la restricción $n < q$ del esquema de Shamir pero con *tolerancia de corrupción grande*. En 2006, Chen y Cramer iniciaron el estudio del comportamiento asintótico de los esquemas lineales con t-multiplicación fuerte. Para ello, introdujeron los esquemas de compartición de secretos algebraico-geométricos, que se construyen a partir de *códigos lineales* algebraico-geométricos. Estos esquemas son generalizaciones de los esquemas de Shamir pero no requieren la condición $n < q$. De hecho para un q fijo se pueden construir esquemas algebraico-geométricos sobre $\mathbb{F}_q$ para un número arbitrario de participantes. Además Chen y Cramer demostraron algunos resultados acerca de la multiplicación fuerte de sus esquemas. Probaron que para *algunos* cuerpos finitos, se puede construir una familia infinita de esquemas de compartición de secretos con un número creciente de participantes tales que estos esquemas tienen t-multiplicación fuerte para $t = \Omega(n)$, es decir, que su tolerancia de corrupción está acotada inferiormente por alguna constante.

Debemos mencionar también que los esquemas de compartición lineales ideales que no tienen necesariamente t-multiplicación fuerte pero sí tienen t-privacidad para un t grande y al mismo tiempo multiplicación, se pueden utilizar como base para construir protocolos de computación multiparte, como se demostró en [32]. Sin embargo, estos protocolos no obtienen seguridad perfecta, ya que tienen cierta probabilidad de error. En [19], se demostró que este tipo de esquemas de compartición de secretos se pueden obtener a partir de códigos autoduales, que están bien estudiados (ver por ejemplo [67]). Sin embargo, la propiedad de t-multiplicación fuerte parece ser mucho más complicada de obtener.

Recientemente el trabajo de Chen y Cramer se ha aplicado sorprendentemente en algunos problemas criptográficos, algunos de ellos fuera del dominio de la computación multiparte. Ishai, Kushilevitz, Ostrovsky y Sahai mostraron una notable aplicación en el contexto de las pruebas de conocimiento cero [46]. Construyeron un protocolo de conocimiento cero para

el problema de la satisfacibilidad de un circuito, que es un problema NP-completo, que requiere la comunicación de $O(1)$ bits por puerta del circuito. En [48] Ishai, Prabkharan y Sahai demostraron como transformar un protocolo de computación multiparte que sea seguro sólo si la mayoría de los participantes son honestos en un protocolo seguro sin esta condición suponiendo que exista una implementación ideal de un protocolo de transferencia inconsciente (oblivious transfer). En [47], Ishai, Kushilevitz, Ostrovsky y Sahai aplicaron de nuevo los resultados de [20] en el contexto de la *"criptografía resistente a fugas de información" (leakage resilient cryptography)*. El trabajo de [47] introduce extractores de correlaciones, una herramienta que permite proteger los protocolos de computación biparte contra fugas de información. Para esta aplicación se necesitan también familias de esquemas de compartición de secretos con t-multiplicación fuerte para $t = \Omega(n)$, pero además se requiere una propiedad de independencia de fragmentos: todo fragmento debe ser independiente de todo subconjunto de t fragmentos distintos de él. Pero la construcción de [20] también disfruta de esta propiedad.

Contribuciones

El principal objetivo de esta tesis es el estudio del comportamiento asintótico de las familias de esquemas de compartición de secretos que son adecuadas para la computación multiparte; es decir esquemas de secretos lineales ideales con t-multiplicación fuerte. Para hacer esto, definiremos para cada cuerpo finito $\mathbb{F}_q$ una clase de códigos lineales sobre $\mathbb{F}_q$, que llamaremos $\mathcal{C}^\dagger(\mathbb{F}_q)$, a partir de cuyos elementos podemos construir esquemas de compartición de secretos lineales ideales con multiplicación. Introduciremos también el concepto de tolerancia de corrupción $\widehat{\tau}(C)$ de un código $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$, que es una medida de la tolerancia de corrupción de los correspondientes esquemas de compartición de secretos, y finalmente la tolerancia de corrupción asintótica óptima $\widehat{\tau}(q)$ de un cuerpo finito $\mathbb{F}_q$, definida como $\widehat{\tau}(q) = \limsup_{n\to\infty} T_q(n)$, donde para todo entero $n > 1$, $T_q(n)$ denota el valor máximo que puede alcanzar $\widehat{\tau}(C)$ cuando consideramos todos los códigos $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ de longitud $n+1$. Es decir, $\widehat{\tau}(q)$ representa la mejor tolerancia de corrupción que podemos obtener *asintóticamente* para familias infinitas de esquemas de compartición de secretos lineales ideales tal que el número de fragmentos tiende a infinito.

El estudio del parámetro $\widehat{\tau}(q)$ es el objetivo más importante de esta tesis. Demostraremos que para cualquier cuerpo finito $\mathbb{F}_q$, $0 < \widehat{\tau}(q) < 1$, y daremos

cotas inferiores y superiores explícitas para estos valores.

Bastantes resultados de esta tesis han sido publicados (ver [15], [16], [17] y [18]).

El texto está estructurado en tres partes.

En la parte I se introducen las nociones y resultados preliminares necesarios acerca de códigos lineales, cuerpos de funciones algebraicas y esquemas de compartición de secretos.

La parte II se dedicará al estudio asintótico de los esquemas de compartición de secretos lineales ideales con multiplicación fuerte. Esta parte tiene cuatro capítulos. En el capítulo 4 definimos para todo cuerpo finito $\mathbb{F}_q$, una clase de códigos lineales sobre $\mathbb{F}_q$, denotada por $\mathcal{C}^\dagger(\mathbb{F}_q)$. Todo código $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ da lugar al menos a un esquema de compartición de secretos li-neal $\Sigma(C,i)$ con multiplicación, donde i es una coordenada prefijada del código. Introduciremos la tolerancia de corrupción $\widehat{\tau}(C)$ del código C. Para ello consideraremos todos los esquemas de compartición de secretos lineales $\Sigma(C,i)$ que se pueden construir a partir de C y tienen t_i-multiplicación fuerte para algún $t_i > 0$ y definiremos $\widehat{\tau}(C)$ como el máximo del cociente $\frac{3t_i}{n-1}$, donde $n+1$ denota la longitud de C. Como veremos, $0 \leq \widehat{\tau}(C) \leq 1$, donde $\widehat{\tau}(C) = 1$ sólo puede ocurrir para códigos MDS. En el capítulo 5 definimos, para todo cuerpo finito $\mathbb{F}_q$ y todo entero $n > 1$, el valor $T_q(n)$ como la máxima tolerancia de corrupción $\widehat{\tau}(C)$ cuando consideramos todos los códigos $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ de longitud $n+1$ e introducimos el parámetro $\widehat{\tau}(q) = \limsup_{n\to\infty} T_q(n)$. El estudio de este parámetro es el objetivo principal de esta tesis. También recordaremos los resultados de [20], que implican que $\widehat{\tau}(q) > 0$ para algunos cuerpos finitos $\mathbb{F}_q$ (en realidad para un número infinito de cuerpos finitos). En el capítulo 6, demostraremos que, en realidad, se tiene $\widehat{\tau}(q) > 0$ para *todo* cuerpo finito $\mathbb{F}_q$ y daremos algunas cotas inferiores explícitas para $\widehat{\tau}(q)$. Finalmente, en el Capítulo 7, demostraremos que también se tiene $\widehat{\tau}(q) < 1$ para todo cuerpo finito $\mathbb{F}_q$ y daremos de forma explícita cotas superiores para $\widehat{\tau}(q)$.

Finalmente, en la parte III introduciremos los sistemas de ecuaciones de Riemann-Roch y demostraremos que las soluciones a ciertos sistemas de este tipo dan lugar a códigos lineales con ciertas propiedades combinatorias. Como aplicaciones obtendremos cotas inferiores mejoradas para $\widehat{\tau}(q)$ para algunos cuerpos finitos $\mathbb{F}_q$ y estudiaremos un problema asintótico concerniente a la complejidad de las multiplicaciones en extensiones de cuerpos finitos. Esta parte tiene cinco capítulos. Primero, en el capítulo 8 definimos los sistemas de ecuaciones de Riemann-Roch. Las ecuaciones de estos sistemas

son igualdades de dimensiones de Riemann-Roch asociadas a divisores de un cuerpo de funciones algebraicas y la indeterminada es un divisor. Demostraremos que las soluciones de ciertos sistemas de ecuaciones permiten construir códigos algebraico-geométricos con ciertas propiedades combinatorias. Obtendremos también condiciones sobre los parámetros del sistema y el cuerpo de funciones algebraicas sobre el que está definido que son suficientes para asegurar que existen soluciones. Estas condiciones involucran dos tipos de parámetros: el número A_r de divisores positivos de un cierto grado fijo r del cuerpo de funciones algebraicas y el tamaño del subgrupo de m-torsión $\mathrm{Cl}_0(\mathbb{F})[m]$ del grupo de clases de divisores de grado cero $\mathrm{Cl}_0(\mathbb{F})$ del cuerpo de funciones algebraicas. En el capítulo 9, daremos cotas superiores para el número de divisores positivos de cierto grado de un cuerpo de funciones algebraicas. En el capítulo 10, obtendremos varias cotas superiores *asintóticas* para los parámetros $|\mathrm{Cl}_0(\mathbb{F})[m]|$, usando resultados conocidos de geometría algebraica, como los resultados clásicos de Weil acerca de la torsión de variedades abelianas, resultados acerca de los pares de Weil y el teorema de Deuring-Shafarevich.

En el capítulo 11, planteamos en primer lugar sistemas de ecuaciones de Riemann-Roch cuyas soluciones dan lugar a códigos algebraico-geométricos con cierta tolerancia de corrupción. Aplicamos los resultados del capítulo 8 y las cotas del capítulo 9 para obtener condiciones suficientes para la resolubilidad de este tipo particular de sistemas de Riemann-Roch. Finalmente aplicando las cotas del capítulo 10 obtenemos cotas inferiores para $\widehat{\tau}(q)$ que en algunos casos son mejores que las obtenidas en la parte II. Por último, en el capítulo 12 mostramos una aplicación interesante de las técnicas desarrolladas en esta parte a un problema que no está (directamente) ligado a la criptografía. Analizaremos la complejidad asintótica de la multiplicación en extensiones de cuerpos finitos. Dada una extensión $\mathbb{F}_{q^k}$ de un cuerpo finito $\mathbb{F}_q$, consideramos la mínima complejidad $m(q,k)$ de cierto tipo de algoritmos que computan el producto de dos elementos en $\mathbb{F}_{q^k}$. El valor $m(q,k)$ representa el mínimo número de productos en $\mathbb{F}_q$ que necesitamos para calcular este producto mediante uno de estos algoritmos. D. V. Chudnovski y G. V. Chudnovski [23] fueron los primeros en proponer el uso de códigos algebraico-geométricos para obtener cotas superiores para $m(q,k)$. Más tarde, Shparlinski, Tsfasman y Vladut [73] analizaron el comportamiento asintótico de este parámetro (cuando q está fijo y k crece). Sin embargo, hay un paso de una de sus demostraciones que no está completamente justificado. Esto tiene consecuencias en su demostración de las cotas superiores

para el parámetro asintótico $\mu(q) = \liminf_{k\in\mathbb{N}} m(q,k)/k$ y también afecta a algunos trabajos posteriores de otros autores sobre este tema. En el capítulo 12 nos ocuparemos de este problema y veremos como se puede resolver, utilizando la maquinaria introducida en esta parte de la tesis, para obtener cotas superiores para $\mu(q)$.

Introduction

Context

Secret sharing schemes were introduced in 1979, independently by Blakley [12] and Shamir [72]. A secret sharing scheme is a combinatorial object which allows for the split of the knowledge of certain secret s into several pieces of information $a_1, a_2, \ldots, a_n$ (*the shares*), in such a way that any large enough subset of these shares determines the secret, while any small subset of shares is information-theoretically independent of it. Secret sharing has found many important applications in cryptography. It was first proposed as a means of storing cryptographic keys. However, secret sharing has also been applied in other cryptographic areas like threshold cryptography (starting with [35]) and multiparty computation, of which more will be explained afterwards. Some of these applications require special secret sharing schemes with some extra algebraic properties. This thesis will be mostly concerned with *ideal linear* secret sharing schemes (LSSS) *with t-strong multiplication.*

Linearity is a property that guarantees that the secret and shares are elements of vector spaces over some finite field $\mathbb{F}_q$ and if two secrets s and s' have as share vectors $(a_1, a_2, \ldots, a_n)$ and $(a'_1, a'_2, \ldots, a'_n)$ then for any $\lambda \in \mathbb{F}_q$, $(a_1 + \lambda a'_1, a_2 + \lambda a'_2, \ldots, a_n + \lambda a'_n)$ is a vector of shares for the secret $s + \lambda s'$. Ideal linear schemes are those where the secret and all the shares are elements of the field $\mathbb{F}_q$.

The properties of multiplication and t-strong multiplication of an ideal linear secret sharing scheme were first defined by Cramer, Damgård and Maurer [32]. A linear secret sharing scheme has multiplication if the set of product of shares $(a_1 a'_1, a_2 a'_2, \ldots, a_n a'_n)$ determines the product of the secrets ss'. And a scheme has t-strong multiplication if it satisfies two requirements: on the one hand, it has t-privacy, that is, any set of t (or less) shares is independent of the secret; on the other hand, if we remove any subset of t shares, the scheme has multiplication for the remaining set of $n - t$ shares.

Original applications of ideal linear secret sharing schemes with t-strong multiplication belonged to the domain of multiparty computation (MPC). Research in this fundamental area of cryptography has been very prolific within the last 20 years. For overviews in this subject, see [27] or Robbert de Haan's Ph.D. thesis [42].

At a high level, multiparty computation studies the following problem: a set of players $P_1, \ldots, P_n$, each holding a certain private input $x_1, \ldots, x_n$, want to jointly compute some public function of these data $f(x_1, \ldots, x_n)$ without revealing more information than necessary about their inputs, and

this should hold even if some of the players cheat, possibly in a coordinated way. More precisely, three goals are pursued: no set of possibly colluding players $S = \{P_{i_1}, \ldots, P_{i_t}\}$ should obtain more information about the input x_j of a player $P_j \notin S$ other than what is implied by their inputs $\{x_{i_1}, \ldots, x_{i_t}\}$ and the evaluation $f(x_1, \ldots, x_n)$ (*privacy*) and despite the possible presence of cheaters, the computation of the function succeeds and the players obtain an output(*robustness*) which is the actual value $f(x_1, \ldots, x_n)$(*correctness*). Another way to look at this problem is by saying that the players $P_1, \ldots, P_n$ should *emulate*, by means of a protocol, an ideal scenario where a trustworthy, incorruptible third party receives the inputs from the players, computes the function and returns the output of the function to them. In the actual protocol, the players do not have access to such a idealized trustworthy third party; instead, each player can send messages to every other player (we assume the existence of untappable private channels between each pair of players). Yet the information obtained by the players about the output and the inputs of other players should be the same as in this ideal situation.

That a specific MPC protocol achieves the goals above depends on which players collude and cheat. It is usually assumed that all the cheating players are corrupted by some external adversary, who obtains all the information received by them and takes full control of the actions of these players, possibly making them deviate from the protocol. For the honest players it is not possible, at least at the beginning of the protocol, to determine which players are corrupt and therefore it is considered that the adversary could corrupt any set in a certain family of subsets of $\{P_1, \ldots, P_n\}$. The most usual example is that the adversary can corrupt any set of up to t players, for some integer t.

In 1988, Ben-Or, Goldwasser and Wigderson [10] and (independently) Chaum, Crépeau and Damgård [21] proved the fundamental theorem of *unconditionally* secure multiparty computation. This result states that every function can be computed by a set of n players exchanging a total amount of information which is polynomial in n and in the size of certain description of the function and this protocol is unconditionally secure if the adversary corrupts up to $t < n/3$ players. Here the word unconditional means that the protocol executed by the players is secure regardless of the computational power of the adversary. Therefore, the security of the protocol does not depend on the fact that a certain mathematical problem cannot be efficiently solved by the adversary, as it is the case in other areas of cryptography, like public key encryption. Of course, there are also many interesting results

concerning *computationally* secure multiparty computation protocols, starting with the work of Goldreich, Micali and Wigderson [40], but these will not be addressed here.

The MPC protocols in [10] and [21] use Shamir's secret sharing schemes, which were already proposed in the seminal paper [72]. These ideal linear secret sharing schemes can be defined for any field $\mathbb{F}_q$ and any number n of shares whenever $n < q$. Moreover they have t-strong multiplication for any integer t with $3t < n$.

The protocols are based on the fact that every function can be written as an arithmetic circuit over some finite field $\mathbb{F}_q$ (that is, the inputs and outputs are elements of the field $\mathbb{F}_q$ and the output can be computed from the inputs by a circuit whose gates consist on sums, multiplications of two inputs or multiplications of an input with a fixed constant of the field $\mathbb{F}_q$). They use Shamir's secret sharing scheme as *a dedicated encryption system* with which every player can "encrypt" some information but only a large enough subset of the players can decrypt it (by pooling together their shares). Linearity and t-strong multiplication imply that this encryption mechanism has homomorphic properties in the sense that knowing the encryptions of two elements a and b of the field $\mathbb{F}_q$, the players can compute, possibly by an interactive process, an encryption of any linear function of a and b or of the product ab, *without leaking any information about* a *and* b to the adversary. Furthermore, the success of these computations cannot be disrupted by the possibly faulty behaviour of the adversary. Hence, the players can securely compute an encryption of the output of every gate of the circuit given the encryptions of the inputs. The players only decrypt (jointly) the output of the function, and not the values computed at the intermediate steps. The adversary cannot stop this decryption by leaving the protocol, since the other players still know enough shares of the output to be able to recover it. The correctness of this decryption step is partially based on *error correcting* techniques, which allow for the efficient decryption of the output in the presence of incorrect shares, thus thwarting any attempt of the adversary to disrupt the protocol by communicating false information in this step.

Even though these protocols implicitly use the algebraic properties of Shamir's scheme that we have mentioned earlier, the t-strong multiplication property was not explicitly defined in these papers. Cramer, Damgård and Maurer [32] not only defined the notion of linear secret sharing scheme with t-strong multiplication, but in fact also generalized the previous results, proving that from any ideal scheme with n shares satisfying these properties (and

not only from Shamir's schemes) we can construct an efficient multiparty computation protocol for n players to compute an arithmetic circuit over $\mathbb{F}_q$ and that is unconditionally secure against any active adversary corrupting t parties. Therefore, in order to obtain the best constructions in terms of security, we need to use ideal linear secret sharing schemes with the largest possible *corruption tolerance*, which is defined as the ratio $\frac{3t}{n-1}$. Another very interesting property of any LSSS with t-strong multiplication is that, as it was proved in [28], there is an algorithm that allows for the efficient reconstruction of a secret from the set of all shares even if some subset of up to t of these shares are false.

Some Shamir's schemes achieve the best possible corruption tolerance for ideal linear secret sharing schemes, so when plugged into the construction by Cramer, Damgård and Maurer they yield the best MPC protocols in terms of security, and in that sense we can say the protocols of [10], [21] are "optimal" particular cases. The drawback is that, as we have said, Shamir's scheme can only be used if $n < q$ and hence cannot be used in order to construct an MPC protocol to compute an arithmetic circuit over $\mathbb{F}_q$ for n players if $n \geq q$, at least not using the paradigm in [32]. A possible solution is to carry out the computations in $\mathbb{F}_{q^k}$, an extension field of $\mathbb{F}_q$ such that $q^k > n$, but this blows up the communication complexity of the protocol, as every element communicated during a secret sharing step belongs to $\mathbb{F}_{q^k}$ and hence the amount of information to be sent is k times bigger.

An alternative is to search for ideal linear secret sharing schemes without the restriction $n < q$ of Shamir's scheme and still have *large corruption tolerance*. In 2006, Chen and Cramer [20] initiated the study of the asymptotic behaviour of linear secret sharing schemes with t-strong multiplication. They introduced algebraic geometric secret sharing schemes, which are constructed from algebraic geometric *linear codes*. These schemes are generalizations of Shamir's schemes but they do not require that $n < q$. In fact, for a fixed q one can construct algebraic geometric schemes for an arbitrary number of players. At the same time, Chen and Cramer proved some results concerning strong multiplication of their schemes. They showed that for *some* finite fields, one can construct an infinite family of secret sharing schemes with unbounded number of players such that they have t-strong multiplication for $t = \Omega(n)$, that is, their corruption tolerances were lower bounded by some constant.

We should also mention that ideal linear secret schemes which do not necessarily have t-strong multiplication, but do have t-privacy for large t and

at the same time multiplication for the set of all players, can also be used as a basis to construct MPC protocols, as was also proved in [32]. However, these protocols do not achieve *perfect* security, since they have some probability to fail. In [19], it was proved that this kind of secret sharing schemes can be obtained from self-dual codes, which are well studied (see for example [67]). However, the property of t-strong multiplication seems to be much more elusive.

There have been some surprising applications of the work by Chen and Cramer in cryptographic problems, some of them outside the domain of multiparty computation. Ishai, Kushilevitz, Ostrovsky and Sahai showed a remarkable application in the context of zero knowledge proofs [46]. They constructed a zero knowledge protocol for the problem of circuit satisfiability, which is an NP-complete problem, requiring only the communication of $O(1)$ bits per gate in the circuit. In [48] Ishai, Prabkharan and Sahai showed how to transform an MPC protocol which is secure only if the majority of the players are honest into an MPC protocol which is secure without this assumption in the oblivious transfer-hybrid model, that is, assuming we had an ideal implementation of an oblivious transfer protocol. In [47], Ishai, Kushilevitz, Ostrovsky and Sahai applied again the results of [20] in the context of *leakage resilient cryptography*. The work of [47] introduces correlation extractors, a tool that allows for the protection of two-party computation protocols against information leakage. Families of secret sharing schemes with t-strong multiplication for $t = \Omega(n)$ are needed, but in addition they requiere a property of independence of shares: any share should be independent from every subset of t shares. But the construction from [20] also enjoys this property.

Contributions

The main goal of this thesis is the study of the asymptotical behaviour of families of "MPC-friendly" secret sharing schemes; that is, ideal linear secret sharing schemes with t-strong multiplication. In order to do this, we introduce for every finite field $\mathbb{F}_q$ a class of $\mathbb{F}_q$-linear codes $\mathcal{C}^\dagger(\mathbb{F}_q)$ whose elements give rise to ideal linear secret sharing schemes with multiplication. We also introduce the corruption tolerance $\widehat{\tau}(C)$ of a code $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$, as the measure of the corruption tolerance of the corresponding linear secret sharing schemes, and finally the asymptotical optimal corruption tolerance $\widehat{\tau}(q)$ of a finite field $\mathbb{F}_q$, defined as $\widehat{\tau}(q) = \limsup_{n\to\infty} T_q(n)$, where for any integer

$n > 1$, $T_q(n)$ denotes the maximal corruption tolerance $\widehat{\tau}(C)$ among all codes $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ of length $n+1$. So $\widehat{\tau}(q)$ represents the best possible corruption tolerance that we can achieve asymptotically for infinite families of linear secret sharing schemes with unbounded number of players.

The study of the parameter $\widehat{\tau}(q)$ is the most important concern of this thesis. We will prove that for every finite field $\mathbb{F}_q$, $0 < \widehat{\tau}(q) < 1$, giving explicit lower and upper bounds for these values.

Many of the results of the thesis have been published in the papers [15], [16], [17] and [18].

The text is structured in three parts.

In Part I the necessary preliminary notions and results about linear codes, algebraic function fields and codes and secret sharing schemes are introduced.

Part II is devoted to the study of asymptotics of ideal linear secret sharing schemes with strong multiplication. This part has four chapters. In Chapter 4, we define, for every finite field $\mathbb{F}_q$, a class of $\mathbb{F}_q-$linear codes $\mathcal{C}^{\dagger}(\mathbb{F}_q)$. Every code $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ gives rise to at least one ideal linear secret sharing scheme $\Sigma(C,i)$ with multiplication, where i is a special coordinate of the code. We introduce the corruption tolerance $\widehat{\tau}(C)$ of the code C. For this we consider all linear secret sharing schemes $\Sigma(C,i)$ that can be constructed from C having t_i-strong multiplication for some $t_i > 0$ and define $\widehat{\tau}(C)$ as the maximum of the ratio $\frac{3t_i}{n-1}$, where $n+1$ is the length of C. As we will show, we have that $0 \leq \widehat{\tau}(C) \leq 1$, where $\widehat{\tau}(C) = 1$ may only happen for MDS codes. In Chapter 5 we define for every finite field $\mathbb{F}_q$ and every integer $n > 1$, $T_q(n)$ as the maximal corruption tolerance $\widehat{\tau}(C)$ among all codes $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ of length $n+1$ and we introduce the parameter $\widehat{\tau}(q) = \limsup_{n\to\infty} T_q(n)$. The study of this parameter is the main goal of this thesis. We also revisit the results of [20], which imply that $\widehat{\tau}(q) > 0$ for some finite fields $\mathbb{F}_q$ (in fact for an infinite number of finite fields).

In Chapter 6, we prove that $\widehat{\tau}(q) > 0$ actually holds for *all* finite fields $\mathbb{F}_q$ and give some explicit lower bounds for $\widehat{\tau}(q)$. Finally, in Chapter 7, we prove that $\widehat{\tau}(q) < 1$ also holds for all finite fields $\mathbb{F}_q$ and give explicit upper bounds for $\widehat{\tau}(q)$.

Finally, in Part III we introduce Riemann-Roch systems of equations and show that solutions of certain Riemann-Roch systems yield algebraic geometric codes with certain combinatorial properties. As applications we obtain improved lower bounds for $\widehat{\tau}(q)$ for some finite fields $\mathbb{F}_q$ and we study an asymptotical problem about the complexity of multiplications in extensions of finite fields. This part has five chapters. First, in Chapter 8 we define

the Riemann-Roch systems of equations. The equations in these systems are equalities of the Riemann-Roch dimensions of divisors of a function field and the indeterminate is a divisor. We prove that a solution of a certain Riemann-Roch system yields an algebraic geometric code with certain combinatorial properties. We also give general conditions on the parameters of the system and the function fields which are sufficient to ensure the existence of solutions. These conditions involve two special kinds of parameters: the number A_r of positive divisors of a given degree r and the size of the m-torsion subgroup $\mathrm{Cl}_0(\mathbb{F})[m]$ of the degree zero divisor class group $\mathrm{Cl}_0(\mathbb{F})$ of the functsion field. In Chapter 9, we give upper bounds for the number of positive divisors of a certain degree of a function field. In Chapter 10, we deduce several *asymptotically* upper bounds for the parameters $|\mathrm{Cl}_0(\mathbb{F})[m]|$, using known algebraic geometric results, such as Weil's classical results on torsion of abelian varieties, Weil Pairing and Deuring-Shafarevich theorem. In Chapter 11, we first pose Riemann-Roch systems of equation whose solutions yield algebraic geometric codes with a certain corruption tolerance. We apply the results of Chapter 8 and the bound in Chapter 9 to give sufficient conditions for the solvability of these particular Riemann-Roch systems. Applying the bounds in Chapter 10 we obtain bounds for $\widehat{\tau}(q)$ which in some cases are better than the lower bounds obtained in Part II. Finally, in Chapter 12 we show an interesting application of the techniques developed in this part to a different problem which is not (directly) related with cryptography. We analyze the asymptotical complexity of multiplication over extensions of finite fields. Given an extension field $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$, we consider the minimal complexity $m(q,k)$ of certain kind of algorithms that compute the product of two elements in $\mathbb{F}_{q^k}$. The value $m(q,k)$ represents the minimal number of products in $\mathbb{F}_q$ that we need to compute the product. D. V. Chudnovski and G. V. Chudnovski [23] first proposed the use of algebraic geometric codes to obtain upper bounds for $m(q,k)$. Later, Shparlinski, Tsfasman and Vladut [73] analyzed the asymptotical behaviour of this parameter (when q is fixed and k grows). However, there is an unjustified step in one of their proofs. This gap has consequences in the proof of their upper bounds for the asymptotical parameter $\mu(q) = \liminf_{k\in\mathbb{N}} m(q,k)/k$ and also affects subsequent work about this topic by other authors. In Chapter 12 we identify and repair this gap, using the machinery introduced in this part of the thesis.

Part I

Background

Chapter 1

Linear codes

This chapter is an overview of some basic notions and results about linear codes over finite fields, which will be used throughout the text. Most of these notions can be found in the books by Huffman and Pless [44] and MacWilliams and Sloane [53].

1.1 Definitions

We state now the basic definitions about linear codes over finite fields.

DEFINITION 1.1 *A* linear code C *over* $\mathbb{F}_q$ *of length* $\mathfrak{k}(C)$ *is a* $\mathbb{F}_q$*-vector subspace of* $\mathbb{F}_q^{\mathfrak{k}(C)}$. *The elements* $\mathbf{c} \in C$ *are the* words *of the code.*

DEFINITION 1.2 *Let* C *be a linear code over* $\mathbb{F}_q$. *If* $\mathbf{c} \in C$, *its coordinate vector is denoted as* $(\pi_0(\mathbf{c}), \pi_1(\mathbf{c}), \ldots, \pi_{\mathfrak{k}(C)-1}(\mathbf{c})) \in \mathbb{F}_q^{\mathfrak{k}(C)}$ *and the set* $\mathcal{I}(C) := \{0, 1, \ldots, \mathfrak{k}(C) - 1\}$ *is used to index the coordinates. For a subset* $A \subseteq \mathcal{I}(C)$, π_A *denotes the projection* $\pi_A : C \to \mathbb{F}_q^{|A|}$ *given by* $\mathbf{c} \mapsto (\pi_i(\mathbf{c}))_{i \in A}$.

Two important parameters are the dimension and the minimum distance of a linear code over $\mathbb{F}_q$.

DEFINITION 1.3 *The* dimension $\dim C$ *of a linear code* C *over* $\mathbb{F}_q$ *is its dimension as an* $\mathbb{F}_q$*-linear subspace of* $\mathbb{F}_q^{\mathfrak{k}(C)}$. *The number of words in* C *is* $q^{\dim C}$.

DEFINITION 1.4 *Let $r \geq 1$ be an integer. Let $\mathbf{x} = (\pi_0(\mathbf{x}), \pi_1(\mathbf{x}), \ldots, \pi_{r-1}(\mathbf{x}))$ and $\mathbf{y} = (\pi_0(\mathbf{y}), \pi_1(\mathbf{y}), \ldots, \pi_{r-1}(\mathbf{y})) \in \mathbb{F}_q^r$. The distance between $\mathbf{x}$ and $\mathbf{y}$ is*

$$d(\mathbf{x}, \mathbf{y}) := |\{i \in \{0, 1, \ldots, r-1\} : \pi_i(\mathbf{x}) \neq \pi_i(\mathbf{y})\}|.$$

The minimum distance *$d(C)$ of a linear code over $\mathbb{F}_q$, is*

$$d(C) := \min\{d(\mathbf{w_1}, \mathbf{w_2}) : \mathbf{w_1}, \mathbf{w_2} \in C, \mathbf{w_1} \neq \mathbf{w_2}\}$$

if $C \neq \{\mathbf{0}\}$ and $d(C) = \mathfrak{k}(C) + 1$ if $C = \{0\}$.

The minimum distance $d(C)$ can be characterized using the notion of Hamming weights, which will also be useful for us.

DEFINITION 1.5 *Given $\mathbf{x} = (\pi_0(\mathbf{x}), \pi_1(\mathbf{x}), \ldots, \pi_{r-1}(\mathbf{x})) \in \mathbb{F}_q^r$, its* Hamming weight *is*

$$w_{Ham}(\mathbf{x}) := |\{i \in \{0, 1, \ldots, r-1\} : \pi_i(\mathbf{x}) \neq \mathbf{0}\}| = d(\mathbf{x}, \mathbf{0}).$$

LEMMA 1.6 *If $\{\mathbf{0}\} \neq C$ is a linear code over $\mathbb{F}_q$, then*

$$d(C) = \min_{\mathbf{c} \in C, \mathbf{c} \neq \mathbf{0}} w_{Ham}(\mathbf{c}).$$

The concept of dual code will also be especially useful in this text.

DEFINITION 1.7 *Let C be a linear code over $\mathbb{F}_q$. Its* dual code *is the following linear code over $\mathbb{F}_q$*

$$C^\perp := \{\mathbf{c}^* \in \mathbb{F}_q^{\mathfrak{k}(C)} :< \mathbf{c}^*, \mathbf{c} >= 0 \ \forall \mathbf{c} \in C\}$$

where $< \cdot, \cdot >$ denotes the inner product in $\mathbb{F}_q^{\mathfrak{k}(C)}$.

One can easily check:

LEMMA 1.8 *We have the following properties:*

- *$C^\perp$ is a linear code over $\mathbb{F}_q$, with $\mathfrak{k}(C^\perp) = \mathfrak{k}(C)$.*
- *$(C^\perp)^\perp = C$.*
- *$\dim C = \mathfrak{k}(C) - \dim C^\perp$.*

DEFINITION 1.9 *A linear code C over $\mathbb{F}_q$ is* self-dual *if $C = C^\perp$ and* self-orthogonal *if $C \subseteq C^\perp$*

There are more ways in which a linear code over $\mathbb{F}_q$ can be obtained from a given one. Next we explain the concept of shortened codes, which we will use later on.

DEFINITION 1.10 (SHORTENED CODE) *Let C be a linear code over $\mathbb{F}_q$ and $\emptyset \neq A \subseteq \mathcal{I}(C)$. Let $C_{A,\mathbf{0}} := \{\mathbf{c} \in C : \pi_A(\mathbf{c}) = \mathbf{0}\}$. The linear code D over $\mathbb{F}_q$* obtained by shortening C at A *is*

$$D := \{\pi_B(\mathbf{c}) : \mathbf{c} \in C_{A,\mathbf{0}}\} \subseteq \mathbb{F}_q^{|B|}$$

where $B = \mathcal{I}(C) \setminus A$.

1.2 Bounds on the parameters

We will need some upper bounds for the dimension $\dim C$ of a linear code C over $\mathbb{F}_q$, in terms of $d(C)$ and $\mathfrak{k}(C)$.

THEOREM 1.11 (SINGLETON BOUND) *For any linear code C over $\mathbb{F}_q$, we have*

$$\dim C + d(C) \leq \mathfrak{k}(C) + 1.$$

DEFINITION 1.12 *A linear code C over $\mathbb{F}_q$ is a* maximum distance separable (MDS) code *if it attains the Singleton bound, i.e., if* $\dim C + d(C) = \mathfrak{k}(C) + 1$.

The following is a well known result (see for example [53]).

THEOREM 1.13 *If C is an MDS code then $C^\perp$ is also an MDS code.*

"Trivial" examples of MDS codes over a finite field $\mathbb{F}_q$ with arbitrary length and dimensions in a certain range exist over any finite field.

LEMMA 1.14 *Let $\mathbb{F}_q$ be a finite field, $\ell > 0$ an integer. For any integer $k \in \{0, 1, \ell - 1, \ell\}$, there exists an MDS code C over $\mathbb{F}_q$ with $\mathfrak{k}(C) = \ell$ and $\dim C = k$.*

Indeed, for every finite field $\mathbb{F}_q$ and integer ℓ, consider the linear codes over $\mathbb{F}_q$ of length ℓ defined as $C_1 = \{\mathbf{0}\}$, $C_2 = \{(\lambda, \lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_q\}$, $C_3 = C_2^{\perp}$, $C_4 = C_1^{\perp} = \mathbb{F}_q^{\ell}$. These have dimensions $0, 1, \ell - 1, \ell$, respectively.

As we will recall later on, there exist MDS codes C whose dimensions do not belong to the set $\{0, 1, \mathfrak{k}(C) - 1, \mathfrak{k}(C)\}$, but this does not happen for arbitrary finite fields and arbitrary values of $\mathfrak{k}(C)$. Hence, it is usual to make the following distinction.

DEFINITION 1.15 *A MDS code C is* trivial *if* $\dim C \in \{0, 1, \mathfrak{k}(C) - 1, \mathfrak{k}(C)\}$ *and* nontrivial *otherwise.*

In the sequel, we need the following notation.

DEFINITION 1.16 *Let $t \geq 0$ be an integer. $\mathbb{F}_q[X]_{\leq t}$ denotes the subset of all polynomials f in $\mathbb{F}_q[X]$ with* $\deg f \leq t$.

Now we describe a family of linear codes over $\mathbb{F}_q$, Reed-Solomon codes. They are MDS codes and, in some cases, nontrivial.

DEFINITION 1.17 (REED-SOLOMON CODE) *Let $\mathbb{F}_q$ be a finite field and let $t, n \in \mathbb{Z}$ such that $0 \leq t \leq n < q$ and $n \geq 1$. A Reed-Solomon code C of length $\mathfrak{k}(C) = n + 1$ and dimension* $\dim C = t + 1$ *(denoted by $RS_q[n, t]$-code) is a linear code over $\mathbb{F}_q$ of the form*

$$C = \{(f(x_0), f(x_1), \ldots, f(x_n)) : f \in \mathbb{F}_q[X]_{\leq t}\}$$

where $x_0, x_1, \ldots, x_n$ are distinct elements in $\mathbb{F}_q$. [1]

PROPOSITION 1.18 *For every $RS_q[n, t]$-code C, $d(C) = n - t + 1$. Hence, C is an MDS code. If in addition $1 \leq t \leq n - 2$, C is a nontrivial MDS code.*

By definition, for every $RS_q[n, t]$-code C, $\mathfrak{k}(C) \leq q$. But in fact, there exist a priori upper bounds on the length of any *nontrivial* MDS code.

[1] This definition is a bit more general than the usual one, since the standard definition of Reed-Solomon code also requires $\mathfrak{k}(C) = q - 1$ and $x_i \neq 0$ for all i. In fact, the definition here is a particular case of the notion of *generalized Reed-Solomon code* (see [44]).

THEOREM 1.19 *([53], ch.11.3 cor.7) Let C be an MDS code over $\mathbb{F}_q$ with $2 \leq \dim C \leq \mathfrak{k}(C) - 2$. Then*

$$q \geq \max\{\dim C + 1, \mathfrak{k}(C) - \dim C + 1\}.$$

Consequently,

$$\mathfrak{k}(C) \leq 2q - 2$$

for any nontrivial MDS code C over $\mathbb{F}_q$.

It has been conjectured (see [53]) that

REMARK 1.20 (MAIN CONJECTURE ON MDS CODES) *Let C be a non trivial MDS code over $\mathbb{F}_q$. If q is even and either $\dim C = 3$ or $\dim C = q - 1$, then $\mathfrak{k}(C) \leq q + 2$. Otherwise $\mathfrak{k}(C) \leq q + 1$.*

For completeness we state now, for a linear code C over $\mathbb{F}_q$, more upper bounds for $\dim C$ in terms of $d(C)$, $\mathfrak{k}(C)$ and q. In order to do this it is useful to consider the following numbers.

DEFINITION 1.21 *For every finite field $\mathbb{F}_q$ and $d, \ell \in \mathbb{Z}$ with $0 < d \leq \ell + 1$, let*

$$A_q(\ell, d) := \max\{|C| : C \text{ linear code over } \mathbb{F}_q \text{ with } \mathfrak{k}(C) = \ell, d(C) = d\}.$$

Note $A_q(\mathfrak{k}(C), \mathfrak{k}(C) + 1) = 1$.

LEMMA 1.22 *For any linear code C over $\mathbb{F}_q$, $q^{\dim C} \leq A_q(\mathfrak{k}(C), d(C))$.*

DEFINITION 1.23 *Let $\mathbb{F}_q$ be a finite field, $r, n \geq 0$ be integers and let $\mathbf{x} \in \mathbb{F}_q^n$. The* Hamming ball of radius r centered at $\mathbf{x}$ *is*

$$B_r(\mathbf{x}) := \{\mathbf{y} \in \mathbb{F}_q^n, d(\mathbf{x}, \mathbf{y}) \leq r\}.$$

We denote the cardinality of any $B_r(\mathbf{x})$ *as*

$$M_q(n, r) := |B_r(\mathbf{x})| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

(note the definition is indeed independent on the selection of $\mathbf{x} \in \mathbb{F}_q^n$).

Finally we state the upper bounds.

THEOREM 1.24 (HAMMING (OR SPHERE PACKING) UPPER BOUND) *For any finite field* $\mathbb{F}_q$ *and any* $d, \ell \in \mathbb{Z}$ *with* $1 \leq d \leq \ell + 1$,

$$A_q(\ell, d) \leq \frac{q^\ell}{M_q(\ell, \lfloor \frac{d-1}{2} \rfloor)}.$$

THEOREM 1.25 (PLOTKIN UPPER BOUND) *For any finite field* $\mathbb{F}_q$ *and any* $d, \ell \in \mathbb{Z}$ *with* $1 \leq d \leq \ell + 1$,

$$A_q(\ell, d) \leq \lfloor \frac{d}{d - \theta_q \ell} \rfloor$$

where $\theta_q = 1 - \frac{1}{q}$.

Now we will state the "*asymptotical* versions" of these bounds. We first need the following definitions and result.

DEFINITION 1.26 *Define the* relative dimension *of a linear code* C *over* $\mathbb{F}_q$ *as* $R(C) := \frac{\dim C}{\mathfrak{k}(C)}$ *and its* relative minimum distance *as* $\delta(C) := \frac{d(C)}{\mathfrak{k}(C)}$.

DEFINITION 1.27 *Define*

$$V_q = \{(\delta(C), R(C)), \{0\} \neq C \text{ linear code over } \mathbb{F}_q\} \subseteq [0,1] \times [0,1]$$

and U_q *the set of accumulation points of* V_q.

THEOREM 1.28 *(Manin [55]) There is a continuous decreasing function* $\alpha_q : [0,1] \to [0,1]$ *such that*

$$U_q = \{(\delta, R) | \delta \in [0,1] \text{ and } R \in [0, \alpha_q(\delta)]\}.$$

Moreover $\alpha_q(0) = 1$ *and* $\alpha_q(\delta) = 0$ *for* $\delta \in [1 - \frac{1}{q}, 1]$.

The exact value of $\alpha_q(\delta)$ is not known, except in the cases $\delta = 0$ and $\delta \in [1 - \frac{1}{q}, 1]$ listed above. The upper bounds for $\dim C$ for any linear code over $\mathbb{F}_q$ stated before imply upper bounds for α_q. In order to state them, we need the following definition, that will turn out to be useful throughout the text.

DEFINITION 1.29 (q-ARY ENTROPY FUNCTION) *The q-ary entropy function is the continuous function defined as*

$$H_q : [0, 1 - \frac{1}{q}] \to \mathbb{R}$$

$$x \mapsto \begin{cases} x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x) & \text{if } 0 < x \leq 1 - \frac{1}{q}. \\ 0 & \text{if } x = 0. \end{cases}$$

THEOREM 1.30 (UPPER BOUNDS FOR α_q) *Let $\theta_q = 1 - \frac{1}{q}$.*

- *$\alpha_q(\delta) \leq 1 - \frac{\delta}{\theta_q}$ for $\delta \in [0, \theta_q]$ (asymptotical Plotkin upper bound).*
- *$\alpha_q(\delta) \leq 1 - H_q(\delta/2)$ for $\delta \in [0, 1]$ (asymptotical Hamming upper bound).*

Next we state a well known *lower* bound for the quantities $A_q(\ell, d)$.

THEOREM 1.31 (GILBERT-VARSHAMOV LOWER BOUND) *For any finite field $\mathbb{F}_q$ and any $d, \ell \in \mathbb{Z}$ such that $1 \leq d \leq \ell$,*

$$A_q(\ell, d) \geq \frac{q^\ell}{M_q(\ell, d-1)}.$$

Consequently, there exists a linear code C over $\mathbb{F}_q$ with $d(C) = d$, $\mathfrak{k}(C) = \ell$ and such that

$$\dim C \geq \mathfrak{k}(C) - \log_q M_q(\mathfrak{k}(C), d(C) - 1).$$

The asymptotical version of this theorem is as follows:

THEOREM 1.32 (ASYMPTOTICAL GILBERT-VARSHAMOV LOWER BOUND) *For $\delta \in [0, 1 - \frac{1}{q}]$, we have*

$$\alpha_q(\delta) \geq 1 - H_q(\delta).$$

Gilbert-Varshamov bound says that for any $\delta \in [0, 1 - \frac{1}{q}]$ there exists a family of linear codes $\mathfrak{C} = \{C^{(m)}\}_{m \in \mathbb{N}}$ over $\mathbb{F}_q$ such that $\lim_{m \to \infty} \mathfrak{k}(C^{(m)}) = \infty$,

$$\lim_{m \to \infty} \delta(C^{(m)}) = \delta$$

and

$$\lim_{m \to \infty} R(C^{(m)}) = 1 - H_q(\delta).$$

Until the early 80's, it was believed that Gilbert-Varshamov lower bound was sharp. However, Tsfasman, Vlăduţ and Zink showed in [78] that this bound could be exceeded.

THEOREM 1.33 (TSFASMAN-VLĂDUŢ-ZINK BOUND FOR q SQUARE) *Let $\mathbb{F}_q$ be a finite field with q square. Then for $\delta \in [0, 1 - \frac{1}{\sqrt{q}-1}]$, we have*

$$\alpha_q(\delta) \geq (1 - \frac{1}{\sqrt{q}-1}) - \delta.$$

For $q \geq 49$, there exist $0 < \delta_1(q) < \delta_2(q) < 1 - \frac{1}{\sqrt{q}-1}$ such that this bound is better than the Gilbert-Varshamov bound in the interval $(\delta_1(q), \delta_2(q))$.

1.3 Generalized linear codes

In the sequel we will need a generalization of the notion of linear code over $\mathbb{F}_q$, where the coordinates of the words are not restricted to be in $\mathbb{F}_q$.

DEFINITION 1.34 *Let $\mathbb{F}_q$ be a finite field. Fix an algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. A* generalized $\mathbb{F}_q$-linear code *C of length $\mathfrak{t}(C)$ is an $\mathbb{F}_q$-linear subspace $C \subset \overline{\mathbb{F}}_q^{\mathfrak{t}(C)}$ with $\dim_{\mathbb{F}_q} C < \infty$.*

Note that for any generalized $\mathbb{F}_q$-linear code, there exist $k_0, k_1, \ldots, k_n \geq 1$ such that

$$C \subseteq \mathbb{F}_{q^{k_0}} \times \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_n}}.$$

DEFINITION 1.35 *A* space of definition *of C is any generalized $\mathbb{F}_q$-linear code V of the form*

$$V = \mathbb{F}_{q^{k_0}} \times \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_n}}$$

for integers $k_0, \ldots, k_n \geq 1$ such that $C \subseteq V$.

Chapter 2

Algebraic function fields and codes

In this chapter, we give some basic definitions and results about algebraic function fields and algebraic geometric codes, which will be necessary afterwards. The terminology and results explained in this chapter are taken from Stichtenoth [75] except when indicated. The proofs of most results can also be found in [75].

2.1 Algebraic function fields

We give basic definitions and properties about algebraic function fields.

DEFINITION 2.1 *Let K be a field. An* algebraic function field $\mathbb{F}/K$ in one variable over K *(function field for short) is an extension field $\mathbb{F} \supseteq K$ such that $\mathbb{F}$ is a finite extension of $K(x)$, where $x \in \mathbb{F}$ is trascendental over K.*

Obviously in the definition above $\mathbb{F}$ is an algebraic extension of $K(x)$ because it is a finite extension, but $\mathbb{F}$ is a trascendental extension of K because it contains x. *In this text we will only consider function fields $\mathbb{F}/K$ with K a* perfect *field.*

DEFINITION 2.2 *The set $\widetilde{K}$ of all elements in $\mathbb{F}$ that are algebraic over K is called the* field of constants *of $\mathbb{F}/K$*

Note that if $\widetilde{K}$ is the field of constants of $\mathbb{F}/K$ then $\mathbb{F}/\widetilde{K}$ is also a function field. *In the sequel we only consider function fields $\mathbb{F}/K$ where $\widetilde{K} = K$.*

THEOREM 2.3 *If $\mathbb{F}/K$ is a function field over K we can write*

$$\mathbb{F} = K(x, y)/(\phi(y))$$

where $\phi(T) \in K(x)[T]$ is an irreducible polynomial.

DEFINITION 2.4 *A* valuation ring $\mathcal{O}$ of $\mathbb{F}/K$ *is a subring $\mathcal{O}$ of $\mathbb{F}$ satisfying*

- $K \subsetneq \mathcal{O} \subsetneq \mathbb{F}$.
- *For any $f \in \mathbb{F}$, at least one of the elements f, f^{-1} belongs to $\mathcal{O}$.*

PROPOSITION 2.5 *A valuation ring $\mathcal{O}$ of $\mathbb{F}/K$ is a local ring, i.e., its only maximal ideal is $P = \mathcal{O} \setminus \mathcal{O}^*$, where $\mathcal{O}^*$ denotes the group of units of $\mathcal{O}$.*

2.2 Places

DEFINITION 2.6 *A* place P *of $\mathbb{F}/K$ is the maximal ideal of some valuation ring $\mathcal{O}$ of $\mathbb{F}/K$. $\mathbb{P}(\mathbb{F})$ denotes the set of all places of $\mathbb{F}$.*

THEOREM 2.7 *For any function field $\mathbb{F}/K$, $|\mathbb{P}(\mathbb{F})|$ is infinite.*

PROPOSITION 2.8 *Given $P \in \mathbb{P}(\mathbb{F})$, there is a unique valuation ring $\mathcal{O}_P$ such that P is its maximal ideal. This valuation ring is precisely*

$$\mathcal{O}_P = \{f \in \mathbb{F} : f^{-1} \notin P\}.$$

PROPOSITION 2.9 *Any valuation ring $\mathcal{O}$ in $\mathbb{F}/K$ is also a principal ideal domain. Therefore, any place P of $\mathbb{F}/K$ is a principal ideal and can be written in the form $P = t_P\mathcal{O}_P$ for some $t_P \in P$.*

REMARK 2.10 *Valuation rings which are also principal ideal domains are called* discrete valuation rings.

DEFINITION 2.11 *Let $P \in \mathbb{P}(\mathbb{F})$. An* uniformizing parameter for P *is any element $t_P \in P$ such that $P = t_P\mathcal{O}_P$.*

PROPOSITION 2.12 *Given $P \in \mathbb{P}(\mathbb{F})$ and a uniforming parameter t_P for P, every element $f \neq 0$ in $\mathcal{O}_P$ can be written in a unique way as $f = t_P^n u$, for $n \in \mathbb{Z}$, $n \geq 0$, and $u \in \mathcal{O}_P^*$. Furthermore, for any $f \neq 0$ in $\mathcal{O}_P$ and any two uniformizing parameters t_P, t'_P of P, if $f = t_P^n u = (t'_P)^{n'} u'$ are the corresponding representations then $n = n'$.*

DEFINITION 2.13 *Let $P \in \mathbb{P}(\mathbb{F})$ and t_P be a uniformizing parameter for P. Let the function*

$$v_P : \mathbb{F} \to \mathbb{Z} \cup \{\infty\}$$

be defined as follows:

$$v_P(f) := \begin{cases} n & \text{if } 0 \neq f \in \mathcal{O}_P, \text{and } f = t_P^n u, u \in \mathcal{O}_P^* \\ -n & \text{if } f \in \mathbb{F} \setminus \mathcal{O}_P, \text{and } f^{-1} = t_P^n u, u \in \mathcal{O}_P^* \\ \infty & \text{if } f = 0 \end{cases}$$

The value $v_P(f)$ is the valuation of f at P.

The fact that $\mathcal{O}_P$ is a valuation ring ($f \in \mathbb{F} \setminus \mathcal{O}_P$ implies $f^{-1} \in \mathcal{O}_P$) and Proposition 2.12 ensure that this is well defined. Note that for any $f \in \mathbb{F} \setminus \{0\}$, we have $v_P(f) = -v_P(f^{-1})$.

PROPOSITION 2.14 *The valuation at $P \in \mathbb{P}(\mathbb{F})$ satisfies the following properties:*

- $v_P(f) = \infty \iff f = 0$.
- $v_P(f+g) \geq \min\{v_P(f), v_P(g)\}$ *for any $f, g \in \mathbb{F}$. If $v_P(f) \neq v_P(g)$ then equality holds.*
- $v_P(fg) = v_P(f) + v_P(g)$ *for any $f, g \in \mathbb{F}$.*
- *There exists $f \in \mathbb{F}$ such that $v_P(f) = 1$.*
- $v_P(f) = 0$ *for any $f \in K \setminus \{0\}$.*

Any function whose domain is a field, whose image is contained in $\mathbb{Z} \cup \{\infty\}$ and satisfies these properties is a *discrete valuation*. Any discrete valuation v of $\mathbb{F}$, satisfies $v = v_P$ for some place P of $\mathbb{F}$.

We now describe how to evaluate a function $f \in \mathbb{F}$ in a place $P \in \mathbb{P}(\mathbb{F})$.

DEFINITION 2.15 *Given $P \in \mathbb{P}(\mathbb{F})$, $F_P = \mathcal{O}_P/P$ is the* residue class field *of P. The* evaluation *of an element $f \in \mathcal{O}_P$ in P is its residue class in F_P and is denoted $f(P)$. For $f \notin \mathcal{O}_P$, its* evaluation at P *is defined as $f(P) = \infty$.*

DEFINITION 2.16 *Let $m > 0$ be an integer. We say that $P \in \mathbb{P}(\mathbb{F})$ is a* zero of $f \in F$ of order m *if $f \in P$ (i.e. $f(P) = 0$) and $v_P(f) = m$. We say that P is a* pole of f of order m *if $f \notin \mathcal{O}_P$ (i.e. $f(P) = \infty$) and $v_P(f) = -m$.*

PROPOSITION 2.17 *Let $P \in \mathbb{P}(\mathbb{F})$. Then $K \subseteq \mathcal{O}_P$ and $K \cap P = \{0\}$. Hence there is a canonical embedding of K into F_P, so K can be considered as a subfield of F_P. Furthermore the degree $|F_P : K|$ of the field extension satisfies $|F_P : K| \leq |\mathbb{F} : K(x)| < \infty$, for any $0 \neq x \in P$.*

DEFINITION 2.18 *For every $P \in \mathbb{P}(\mathbb{F})$, the* degree of P *is the positive integer* $\deg P = |F_P : K|$.

DEFINITION 2.19 *For any integer $k \geq 1$, let*

$$\mathbb{P}^{(k)}(\mathbb{F}) := \{P \in \mathbb{P}(\mathbb{F}) : \deg P = k\}.$$

REMARK 2.20 *If $\mathbb{F}/K$ is a function field with K an algebraically closed field, then $\mathbb{P}(\mathbb{F}) = \mathbb{P}^{(1)}(\mathbb{F})$.*

2.3 Divisors

DEFINITION 2.21 *A* divisor *D of the function field $\mathbb{F}/K$ is a formal sum $D = \sum_{P \in \mathbb{P}(\mathbb{F})} m_P P$ with $m_P \in \mathbb{Z}$ such that $m_P = 0$ except for a finite number of places $P \in \mathbb{P}(\mathbb{F})$.*
The set of places P such that $m_P \neq 0$ is called the support *of D and denoted* $\operatorname{supp} D$. *The set of divisors of $\mathbb{F}/K$ is denoted* $\operatorname{Div}(\mathbb{F})$.

Given a place $P \in \mathbb{P}(\mathbb{F})$, by abuse of notation, P also denotes the divisor $P := 1 \cdot P \in \operatorname{Div}(\mathbb{F})$.

DEFINITION 2.22 *Given $D = \sum_{P \in \mathbb{P}(\mathbb{F})} m_P P \in \operatorname{Div}(\mathbb{F})$, its* degree *is the integer* $\deg D := \sum_{P \in \mathbb{P}(\mathbb{F})} m_P \deg P$.

DEFINITION 2.23 *Given $D = \sum_{P \in \mathbb{P}(\mathbb{F})} m_P P, D' = \sum_{P \in \mathbb{P}(\mathbb{F})} n_P P \in \operatorname{Div}(\mathbb{F})$, their sum is $D + D' := \sum_{P \in \mathbb{P}(\mathbb{F})} (m_P + n_P) P$.*

LEMMA 2.24 *$(\operatorname{Div}(\mathbb{F}), +)$ is an abelian group. Its zero element is*

$$0 := \sum_{P \in \mathbb{P}(\mathbb{F})} 0 \cdot P \in \operatorname{Div}(\mathbb{F}).$$

DEFINITION 2.25 *For any $r \in \mathbb{Z}$, let*

$$\operatorname{Div}_r(\mathbb{F}) := \{D \in \operatorname{Div}(\mathbb{F}) : \deg D = r\} \subseteq \operatorname{Div}(\mathbb{F}).$$

LEMMA 2.26 $\mathrm{Div}_0(\mathbb{F})$ *is a subgroup of* $\mathrm{Div}(\mathbb{F})$. *For any integer* $r \in \mathbb{Z}$ *such that* $\mathrm{Div}_r(\mathbb{F}) \neq \emptyset$, $\mathrm{Div}_r(\mathbb{F})$ *is a coset of* $\mathrm{Div}_0(\mathbb{F})$ *inside* $\mathrm{Div}(\mathbb{F})$, *i.e., given* $D \in \mathrm{Div}_r(\mathbb{F})$, *we have* $\mathrm{Div}_r(\mathbb{F}) = D + \mathrm{Div}_0(\mathbb{F})$.

THEOREM 2.27 (SCHMIDT) *Let* $\mathbb{F}/\mathbb{F}_q$ *be a function field over a* finite field $\mathbb{F}_q$. *Then* $\mathrm{Div}_1(\mathbb{F}) \neq \emptyset$ *and consequently* $\mathrm{Div}_r(\mathbb{F}) \neq \emptyset$ *for all* $r \in \mathbb{Z}$.

REMARK 2.28 *If* K *is an algebraically closed field, then the result above also holds, and in fact in that case it is trivial since for every* $P \in \mathbb{P}(\mathbb{F})$, $\deg P = 1$ *and* the divisor $P \in \mathrm{Div}(\mathbb{F})$ *belongs to* $\mathrm{Div}_1(\mathbb{F})$.

Next we define a partial order in the set $\mathrm{Div}(\mathbb{F})$.

DEFINITION 2.29 *Given* $D = \sum_{P \in \mathbb{P}(\mathbb{F})} m_P P, D' = \sum_{P \in \mathbb{P}(\mathbb{F})} n_P P \in \mathrm{Div}(\mathbb{F})$, *we say that* $D \leq D'$ *if* $m_P \leq n_P$ *for every* $P \in \mathbb{P}(\mathbb{F})$.

DEFINITION 2.30 *A divisor* D *is called* effective *(or* positive*) if* $D \geq 0$.

LEMMA 2.31 *If* $D, D' \in \mathrm{Div}(\mathbb{F})$ *are such that* $D \leq D'$ *then* $\deg D \leq \deg D'$. *Hence any effective divisor* $D \in \mathrm{Div}(\mathbb{F})$ *satisfies* $\deg D \geq 0$ *and the only effective divisor in* $\mathrm{Div}_0(\mathbb{F})$ *is* 0.

A divisor can be associated to every $f \in \mathbb{F} \setminus \{0\}$. In order to define these divisors, we first need to state the following result.

THEOREM 2.32 *Every* $f \in \mathbb{F} \setminus \{0\}$ *has finitely many zeros and poles. In other words,* $v_P(f) = 0$ *except for finitely many* $P \in \mathbb{P}(\mathbb{F})$.

Later we will state a stronger result. But this is enough to define principal divisors:

DEFINITION 2.33 *Given* $f \in \mathbb{F} \setminus \{0\}$, *the divisor*

$$(f) := \sum_{P \in \mathbb{P}(\mathbb{F})} v_P(f) P \in \mathrm{Div}(\mathbb{F})$$

is the principal divisor associated to f.
$\mathrm{Pr}(\mathbb{F}) := \{D \in \mathrm{Div}(\mathbb{F}) : \exists f \in \mathbb{F} \setminus \{0\}$ *with* $D = (f)\}$ *is the set of principal divisors.*

DEFINITION 2.34 *Let $f \in \mathbb{F} \setminus \{0\}$ and denote by Z (respectively N) the set of zeros (resp. poles) of $f \in \mathbb{P}(\mathbb{F})$. We define*

$$(f)_0 := \sum_{P \in Z} v_P(f)P \in \mathrm{Div}(\mathbb{F})$$

and

$$(f)_\infty := \sum_{P \in N} (-v_P(f))P \in \mathrm{Div}(\mathbb{F})$$

Note that for any $f \in \mathbb{F} \setminus \{0\}$, $(f)_0, (f)_\infty \geq 0$, $(f) = (f)_0 - (f)_\infty$ and $(f) = 0 \Leftrightarrow f \in K \setminus \{0\}$ (remember we are assuming $K = \widetilde{K}$, the last statement is not true otherwise).

The next important result states that any function $f \in \mathbb{F} \setminus K$ has at least a zero and a pole and in fact, it has the same number of poles and zeros counting multiplicities.

THEOREM 2.35 *Let $\mathbb{F}/K$ be a function field. For any $f \in \mathbb{F} \setminus K$,*

$$deg(f)_0 = deg(f)_\infty = |\mathbb{F} : K(f)|.$$

COROLLARY 2.36 *For any $f \in \mathbb{F} \setminus \{0\}$, we have* $\deg(f) = 0$. *Consequently* $\mathrm{Pr}(\mathbb{F}) \subseteq \mathrm{Div}_0(\mathbb{F})$.

The following property is a consequence of the properties of the discrete valuations (see Proposition 2.14).

PROPOSITION 2.37 *For any $f, g \in \mathbb{F} \setminus \{0\}$, $(fg) = (f) + (g)$.*

COROLLARY 2.38 $\mathrm{Pr}(\mathbb{F})$ *is a subgroup of* $\mathrm{Div}_0(\mathbb{F})$.

2.4 Class groups

Since $\mathrm{Pr}(\mathbb{F})$ is a subgroup of $\mathrm{Div}(\mathbb{F})$, we can consider the following quotient group.

DEFINITION 2.39 *The* divisor class group of $\mathbb{F}/K$ *is the quotient*

$$\mathrm{Cl}(\mathbb{F}) := \mathrm{Div}(\mathbb{F})/\mathrm{Pr}(\mathbb{F}).$$

For $D \in \mathrm{Div}(\mathbb{F})$*, the class of* D *in* $\mathrm{Cl}(\mathbb{F})$ *is denoted by* $[D]$*. The* degree zero divisor class group of $\mathbb{F}/K$ *is*

$$\mathrm{Cl}_0(\mathbb{F}) := \mathrm{Div}_0(\mathbb{F})/\mathrm{Pr}(\mathbb{F}).$$

Note that $\mathrm{Cl}_0(\mathbb{F})$ *is a subgroup of* $\mathrm{Cl}(\mathbb{F})$*.*

DEFINITION 2.40 *We say that* D*,* $D' \in \mathrm{Div}(\mathbb{F})$ *are* equivalent *(denoted as* $D \sim D'$*) if* $D - D' \in \mathrm{Pr}(\mathbb{F})$*, i.e., if they lie in the same class in* $\mathrm{Cl}(\mathbb{F})$*.*

Corollary 2.36 implies

LEMMA 2.41 *Let* $D, D' \in \mathrm{Div}(\mathbb{F})$ *such that* $D \sim D'$*. Then* $\deg D = \deg D'$*.*

This guarantees the correctness of the following definition.

DEFINITION 2.42 *For any* $D \in \mathrm{Div}(\mathbb{F})$*, the degree of the class* $[D] \in \mathrm{Cl}(\mathbb{F})$ *is* $\deg[D] := \deg D$*.*

DEFINITION 2.43 *Let* $\mathbb{F}/K$ *be a function field. For any integer* $r \in \mathbb{Z}$*, we define the set*

$$\mathrm{Cl}_r(\mathbb{F}) := \{[D] \in \mathrm{Cl}(\mathbb{F}) : \deg[D] = r\}.$$

This definition is consistent with that of the group $\mathrm{Cl}_0(\mathbb{F})$*. Furthermore any* $\mathrm{Cl}_r(\mathbb{F})$ *for* $r \neq 0$ *is a coset of* $\mathrm{Cl}_0(\mathbb{F})$ *contained in* $\mathrm{Cl}(\mathbb{F})$*.*

The number of classes of equivalence in $\mathrm{Cl}_r(\mathbb{F})$ is the same for any $r \in \mathbb{Z}$ and is given by the class number, which is defined next.

DEFINITION 2.44 *The* class number *of a function field* $\mathbb{F}/K$ *is the integer* $h(\mathbb{F}) := |\mathrm{Cl}_0(\mathbb{F})|$*. Note that* $h(\mathbb{F}) = |\mathrm{Cl}_r(\mathbb{F})|$ *for all* $r \in \mathbb{Z}$*. When* $\mathbb{F}$ *is clear by the context we will write* h*.*

THEOREM 2.45 *For any function field* $\mathbb{F}/K$*,* h *is finite.*

We will need the following well-known "interpolation" lemma.

THEOREM 2.46 (WEAK APPROXIMATION THEOREM) *Let $\mathbb{F}/K$ be a function field, a* finite *number of places $P_1, \ldots, P_n \in \mathbb{P}(\mathbb{F})$, with $P_i \neq P_j$, possibly equal elements $x_1, \ldots, x_n \in \mathbb{F}$ and $r_1, \ldots, r_n \in \mathbb{Z}$. Then, there exists $x \in \mathbb{F}$ such that $v_{P_i}(x - x_i) = r_i$ for all $i = 1, \ldots, n$.*

Whenever we use the Approximation Theorem, we will refer to the following consequence.

COROLLARY 2.47 *Given a divisor $D \in Div(\mathbb{F})$ and a* finite *number of places $P_1, \ldots, P_n \in \mathbb{P}(\mathbb{F})$ there exists $D' \in Div(\mathbb{F})$ such that $D' \sim D$ and*

$$supp(D') \cap \{P_1, \ldots, P_n\} = \emptyset.$$

PROOF. Let $r_i = -v_P(D)$, $i = 1, \ldots, n$. By the Weak Approximation Theorem there exists $x \in \mathbb{F}$ such that $v_{P_i}(x) = r_i$. Then $D' = (x) + D$ satisfies $D' \sim D$ and $v_{P_i}(D') = 0$ for $i = 1, \ldots, n$. △

2.5 Riemann-Roch spaces and genus

To every divisor of a function field $\mathbb{F}/K$ one can associate a vector space over K in the following way.

DEFINITION 2.48 *Let $D \in \mathrm{Div}(\mathbb{F})$. The* Riemann-Roch space associated to *D is*

$$\mathcal{L}(D) := \{f \in \mathbb{F}, (f) + D \geq 0\} \cup \{0\}$$

If a divisor D is written as $D = \sum_{P \in \mathcal{P}} m_P P - \sum_{Q \in \mathcal{Q}} n_Q Q$, for some $\mathcal{P}, \mathcal{Q} \subseteq \mathbb{P}(\mathbb{F})$ with $\mathcal{P} \cap \mathcal{Q} = \emptyset$ and $m_P \geq 0$ for all $P \in \mathcal{P}$, $n_Q \geq 0$ for all $Q \in \mathcal{Q}$, then $\mathcal{L}(D)$ collects all functions $f \in \mathbb{F}$ such that f *has* a zero of order *at least* n_Q in Q, for all $Q \in \mathcal{Q}$ and *can have* a pole of order *at most* m_P in P, for all $P \in \mathcal{P}$.

PROPOSITION 2.49 *Let $\mathbb{F}/K$ be a function field and $D \in \mathrm{Div}(\mathbb{F})$. Then $\mathcal{L}(D)$ is a K-vector space of finite dimension.*

DEFINITION 2.50 *Let $\mathbb{F}/K$ be a function field and $D \in \mathrm{Div}(\mathbb{F})$. $\ell(D)$ denotes the dimension of $\mathcal{L}(D)$ as a vector space over K.*

LEMMA 2.51 *We have the following properties:*

- *For any* $D \in \mathrm{Div}(\mathbb{F})$, $\ell(D) \leq \deg D + 1$. *Therefore, if* $\deg D < 0$, $\ell(D) = 0$.
- *Let* $D, D' \in \mathrm{Div}(\mathbb{F})$, $D \sim D'$. *Then* $\mathcal{L}(D) \cong \mathcal{L}(D')$. *Consequently* $\ell(D) = \ell(D')$.
- $\mathcal{L}(0) = K$ *and therefore* $\mathcal{L}(D) \cong K$ *for any* $D \in \mathrm{Pr}(\mathbb{F})$. *Consequently* $\ell(0) = 1$ *and* $\ell(D) = 1$ *for any* $D \in \mathrm{Pr}(\mathbb{F})$.
- *For all* $D \in \mathrm{Div}_0(\mathbb{F}) \setminus \mathrm{Pr}(\mathbb{F})$, $\ell(D) = 0$.

The second of these properties allows for the definition of the Riemann-Roch dimension of a *class* of divisors.

DEFINITION 2.52 *For any* $D \in \mathrm{Div}(\mathbb{F})$, *the* Riemann-Roch dimension of the class $[D] \in \mathrm{Cl}(\mathbb{F})$ *is* $\ell([D]) := \ell(D)$.

The notion of genus of a function field will be introduced next.

THEOREM 2.53 *(Riemann's Theorem) There exists* $M \in \mathbb{Z}$ *such that for all divisors* $D \in \mathrm{Div}(\mathbb{F})$,

$$\ell(D) \geq M + \deg D.$$

DEFINITION 2.54 *The* genus *of* $\mathbb{F}/K$ *is the following non-negative integer*

$$g(\mathbb{F}) := \max_{D \in \mathrm{Div}(\mathbb{F})} \deg D - \ell(D) + 1.$$

When $\mathbb{F}$ *is clear by the context we write* g.

This number exists and is not negative because of Theorem 2.53.

In particular, function fields of genus 0 can be characterized in some cases as follows.

DEFINITION 2.55 *A function field* $\mathbb{F}/K$ *is* rational *if* $\mathbb{F} = K(x)$ *for some* $x \in \mathbb{F}$.

THEOREM 2.56 *Let* $\mathbb{F}/K$ *be a function field.* $\mathbb{F}/K$ *is a rational function field if and only if* $\mathrm{Div}_1(\mathbb{F}) \neq \emptyset$ *and* $g(\mathbb{F}) = 0$.
If, in addition, K *is a finite field or an algebraically closed field, then* $\mathbb{F}/K$ *is a rational function field if and only if* $g(\mathbb{F}) = 0$.

2.6 Canonical divisors

Canonical divisors are a special class of divisors. We introduce them now and prove some properties.[1]

DEFINITION 2.57 *Let $\mathbb{F}/K$ be a function field. The space of differential forms of $\mathbb{F}$, $\Omega(\mathbb{F})$, is the $\mathbb{F}$-vector space generated by the symbols df, $f \in \mathbb{F}$, subject to the relations:*

- $d(f+g) = df + dg$, *for all* $f, g \in \mathbb{F}$
- $d(fg) = f \cdot dg + g \cdot df$ *for all* $f, g \in \mathbb{F}$
- $df = 0$ *for all* $f \in K$

PROPOSITION 2.58 *$\Omega(\mathbb{F})$ is a 1-dimensional $\mathbb{F}$-vector space. Moreover, df is a basis of $\Omega(\mathbb{F})$ over $\mathbb{F}$ if and only if $\mathbb{F}/K(f)$ is a finite separable extension.*

PROPOSITION 2.59 *Let $t_P \in \mathbb{F}$ be a uniformizing parameter for $P \in \mathbb{P}(\mathbb{F})$. Then, for every $w \in \Omega(\mathbb{F})$ there exists $f \in \mathbb{F}$ with $w = f \cdot dt_P$. Such f is denoted by $\frac{w}{dt_P}$.*

PROPOSITION 2.60 *The valuation $v_P(\frac{w}{dt_P})$ is independent of the uniformizing parameter t_P, i.e., $v_P(\frac{w}{dt_P}) = v_P(\frac{w}{dt'_P})$ for any two uniformizing parameters t_P, t'_P.*

Therefore the following notion is well defined.

DEFINITION 2.61 *For any $w \in \Omega(\mathbb{F})$ and any place $P \in \mathbb{P}(\mathbb{F})$ we define $v_P(w) := v_P(\frac{w}{dt_P})$ for a uniformizing parameter t_P in P*

PROPOSITION 2.62 *Let $w \in \Omega(\mathbb{F}) \setminus \{0\}$. Then $v_P(w) = 0$ for all but a finite number of places $P \in \mathbb{P}(\mathbb{F})$*

This allows us to associate a divisor to every nonzero differential form. These divisors will be called canonical.

[1] In [75], Stichtenoth introduces, more generally, canonical divisors for function fields $\mathbb{F}/K$ with K non necessarily a perfect field and in order to do that, he uses the notion of Weil differentials. However in the case of perfect fields, his definition is equivalent to the one presented in this section, as follows from Remark 4.3.7 of [75].

DEFINITION 2.63 (CANONICAL DIVISOR) *Let $w \in \Omega(\mathbb{F}) \setminus \{0\}$. The* canonical divisor *associated to w is*

$$(w) := \sum_{P \in \mathbb{P}(\mathbb{F})} v_P(w) \cdot P \in \mathrm{Div}(\mathbb{F})$$

Finally, we state several important facts about canonical divisors.

PROPOSITION 2.64 *For all $w_1, w_2 \in \Omega(\mathbb{F}) \setminus \{0\}$, $(w_1) \sim (w_2)$. Furthermore, given any $w \in \Omega(\mathbb{F}) \setminus \{0\}$, if $D \sim (w)$ then D is also a canonical divisor $D = (w')$ for some $w' \in \Omega(\mathbb{F}) \setminus \{0\}$. In other words, the set of canonical divisors is a class in* $\mathrm{Cl}(\mathbb{F})$.

THEOREM 2.65 *For any canonical divisor $W \in \mathrm{Div}(\mathbb{F})$, we have*

$$\deg W = 2g - 2 \text{ and } \ell(W) = g.$$

2.7 The Riemann-Roch theorem

Riemann-Roch theorem characterizes the dimension of a Riemann-Roch space.

THEOREM 2.66 (RIEMANN-ROCH THEOREM) *Let $\mathbb{F}/K$ be a function field and $D \in \mathrm{Div}(\mathbb{F})$. For any canonical divisor $W \in \mathrm{Div}(\mathbb{F})$, we have*

$$\ell(D) = \ell(W - D) + \deg D - g + 1.$$

COROLLARY 2.67 *Let $\mathbb{F}/K$ be a function field and $D \in \mathrm{Div}(\mathbb{F})$.*
If $\deg D \geq 2g - 1$ then $\ell(D) = \deg D - g + 1$.

PROOF. For any canonical divisor W, $\deg W = 2g - 2$. Hence we have $\deg(W - D) < 0$ and therefore $\ell(W - D) = 0$ by Lemma 2.51. △

2.8 The zeta function of a function field

The zeta function of a function field collects information about the number of effective divisors of degree r for every $r \in \mathbb{Z}$. In this section we define zeta functions and state results about the number of effective divisors of a given degree.

The results of this section and the rest of this chapter are valid for function fields over *finite fields*.

DEFINITION 2.68 *Let $\mathbb{F}/\mathbb{F}_q$ be a function field and $r \in \mathbb{Z}$. Let*

$$\mathcal{A}_r(\mathbb{F}) := \{D \in \mathrm{Div}_r(\mathbb{F}) : D \geq 0\}$$

and denote $A_r(\mathbb{F})$ its cardinality. When $\mathbb{F}$ is clear by the context we write $\mathcal{A}_r$ and A_r.

LEMMA 2.69 *Let $\mathbb{F}/\mathbb{F}_q$ be a function field. For every $r \in \mathbb{Z}$, A_r is finite.*

Note that for every function field $\mathbb{F}/\mathbb{F}_q$, $A_r = 0$ for $r < 0$, $A_0 = 1$, and $A_1 = |\mathbb{P}^{(1)}(\mathbb{F})|$. In general, we can state the following results.

PROPOSITION 2.70 *Let $r \in \mathbb{Z}$, $\mathbb{F}/\mathbb{F}_q$ a function field. Let $[D] \in \mathrm{Cl}_r(\mathbb{F})$. Then*

$$|\mathcal{A}_r \cap [D]| = \frac{q^{\ell(D)} - 1}{q - 1}$$

PROPOSITION 2.71 *Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}/\mathbb{F}_q$ a function field. For $r > 2g - 2$,*

$$A_r = \frac{h}{q-1}(q^{r+1-g} - 1)$$

The zeta function of $\mathbb{F}$ collects the information about the numbers $A_r(\mathbb{F})$ for all $r > 0$.

DEFINITION 2.72 (ZETA FUNCTION OF $\mathbb{F}$) *Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}/\mathbb{F}_q$ a function field. The formal power series*

$$Z(T) := \sum_{i=0}^{\infty} A_i T^i \in \mathbb{C}[[T]]$$

is the zeta function of $\mathbb{F}/\mathbb{F}_q$.

For the rest of the chapter, let $Z(T)$ be the zeta function of $\mathbb{F}/\mathbb{F}_q$.

PROPOSITION 2.73 *$Z(T)$ is convergent for every $T \in \mathbb{C}$ with $|T| < 1/q$.*

THEOREM 2.74 (FUNCTIONAL EQUATION OF $Z(T)$) *$Z(T)$ satisfies the following functional equation:*

$$Z(T) = q^{g-1}T^{2g-2}Z(\frac{1}{qT}).$$

THEOREM 2.75 $(1-T)(1-qT)Z(T) \in \mathbb{Z}[T]$.

DEFINITION 2.76 (L-POLYNOMIAL OF $\mathbb{F}$) *The L-polynomial of $\mathbb{F}/\mathbb{F}_q$ is the polynomial*

$$L(T) := (1-T)(1-qT)Z(T)$$

PROPOSITION 2.77 (PROPERTIES OF THE L-POLYNOMIAL) *We have:*

- $\deg(L(T)) = 2g$.
- *$L(T)$ satisfies the functional equation $L(T) = q^g T^{2g} L(\frac{1}{qT})$.*
- $L(1) = h$.
- *If we write $L(T) = a_0 + a_1 T + \cdots + a_{2g} T^{2g}$, then $a_0 = 1$, $a_{2g} = q^g$ and $a_{2g-i} = q^{g-i} a_i$ for all $0 \leq i \leq g$. Moreover $a_1 = |\mathbb{P}^{(1)}(\mathbb{F})| - (q+1)$.*

THEOREM 2.78 *There exist $\alpha_1, \alpha_2, \ldots, \alpha_{2g} \in \mathbb{C}$ such that $L(T)$ can be decomposed as $L(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$ and $\alpha_i \alpha_{g+i} = q$ holds for all $1 \leq i \leq g$.*

COROLLARY 2.79 *Let $L(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$ be the L-polynomial of $\mathbb{F}/\mathbb{F}_q$. Then*

$$|\mathbb{P}^{(1)}(\mathbb{F})| = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Finally we state an important result, known as the Hasse-Weil Theorem. This can be regarded as an analogue, for function fields, of the Riemann Hypothesis. Details can be checked in [68] and [75].

THEOREM 2.80 (HASSE-WEIL THEOREM) *Let $L(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$ be the L-polynomial of $\mathbb{F}/\mathbb{F}_q$. Then $|\alpha_i| = \sqrt{q}$ for every $i = 1, \ldots, 2g$.*

2.9 Hasse-Weil and Drinfeld-Vlăduţ bounds and Ihara's constant $A(q)$

Let $\mathbb{F}/\mathbb{F}_q$ be a function field. The results given in the previous section imply upper bounds on $|\mathbb{P}^{(1)}(\mathbb{F})|$. We describe some of these bounds in this section.

THEOREM 2.81 (HASSE-WEIL BOUND) *Write* $N = |\mathbb{P}^{(1)}(\mathbb{F})|$. *Then*

$$|N - (q+1)| \leq 2g\sqrt{q}.$$

DEFINITION 2.82 *A function field* $\mathbb{F}/\mathbb{F}_q$ *is called maximal if it achieves*

$$|\mathbb{P}^{(1)}(\mathbb{F})| = (q+1) + 2g\sqrt{q}.$$

We now consider *asymptotical* bounds for $|\mathbb{P}^{(1)}(\mathbb{F})|$ with respect to $g(\mathbb{F})$.

DEFINITION 2.83 *For every finite field* $\mathbb{F}_q$, *and any integer* $g \geq 0$, *let*

$$N_q(g) := \max_{\mathbb{F}/\mathbb{F}_q : g(\mathbb{F})=g} |\mathbb{P}^{(1)}(\mathbb{F})|.$$

DEFINITION 2.84 (IHARA'S CONSTANT) Ihara's constant *is defined for every finite field* $\mathbb{F}_q$ *as*

$$A(q) := \limsup_{g\to\infty} N_q(g)/g.$$

Ihara's constant has been studied extensively, yet its value is not known for all q. The Hasse-Weil bound gives the upper bound $A(q) \leq 2\sqrt{q}$. However this bound is too optimistic. In fact, the following is known:

THEOREM 2.85 (DRINFELD-VLĂDUŢ BOUND) *For every finite field* $\mathbb{F}_q$,

$$A(q) \leq \sqrt{q} - 1.$$

It turns out that when q is a square, the Drinfeld-Vlăduţ bound *is attained.*

THEOREM 2.86 *Let* $\mathbb{F}_q$ *be a finite field with* q *square. Then* $A(q) = \sqrt{q} - 1$.

The result was proved independently by Ihara [45] and Tsfasman,Vlăduţ and Zink [78].

For other fields $\mathbb{F}_q$, the exact value of $A(q)$ is not known, but there exist lower bounds. Serre [70] proved the following result.

THEOREM 2.87 *There exists an absolute constant* $c \in \mathbb{R}$, $c > 0$, *such that* $A(q) > c \log q > 0$ *for all finite field* $\mathbb{F}_q$.

REMARK 2.88 *The previous result is known to be true for* $c = \frac{1}{96}$ *(see [63]).*

But better lower bounds are known for specific finite fields. For example, the currently tightest lower bound for $A(2)$ is due to from Xing and Yeo [84]:

PROPOSITION 2.89 $A(2) \geq \frac{97}{376} = 0.2579\ldots$

This is still far away from the upper bound by Drinfeld and Vlăduţ which is $A(2) \leq 0.4142\ldots$

For cubic fields, there exist better lower bounds for $A(q)$. Zink [86] proved:

THEOREM 2.90 *Let p be a prime. Then*

$$A(p^3) \geq 2\frac{p^2-1}{p+2}.$$

Bezerra, Garcia and Stichtenoth [11] extended this result and proved:

THEOREM 2.91 *Let $\mathbb{F}_q$ be a finite field, with q a cube and let $\ell = \sqrt[3]{q}$. Then*

$$A(q) \geq 2\frac{\ell^2-1}{\ell+2}.$$

Niederreiter and Xing [62] proved the following bounds for Ihara's constant on other fields of non-prime cardinality.

THEOREM 2.92 *We have*

- *Let $\mathbb{F}_q$ be a finite field with q an odd number and $m \geq 3$ an integer, then:*
$$A(q^m) \geq \frac{2q}{\lfloor 2\sqrt{2q+1}\rfloor + 1}.$$
- *Let $\mathbb{F}_q$ be a finite field with q an even number, $q \geq 4$ and $m \geq 3$ an odd integer, then:*
$$A(q^m) \geq \frac{q+1}{\lfloor 2\sqrt{2q+2}\rfloor + 2}.$$

It will be helpful for us to introduce the notion of Ihara's limit of an infinite family of function fields with unbounded genus.

DEFINITION 2.93 *Let $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m\in\mathbb{N}}$ be an infinite family of function fields over $\mathbb{F}_q$ such that*

$$\lim_{m\to\infty} g(\mathbb{F}^{(m)}) = \infty.$$

We define Ihara's limit of a family of function fields as

$$A(\mathcal{F}) := \limsup_{m\to\infty} \frac{|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})|}{g(\mathbb{F}^{(m)})}.$$

We say $\mathcal{F}$ is an asymptotically good family *if $A(\mathcal{F}) > 0$ and an* asymptotically optimal family *if in addition it attains the optimal value $A(\mathcal{F}) = A(q)$.*

2.10 Towers of function fields

Most of the proofs of the results on lower bounds for $A(q)$ of the previous section rely on deep methods from number theory and algebraic geometry. A "more elementary" approach to this problem consists in the recursive construction of *towers of function fields*, where each function field of the family is explicitly written as a simple algebraic extension of the previous one. This approach was first proposed by Garcia and Stichtenoth in [37]. An advantage of these constructions is that some properties of these families can be analyzed more easily, and this will be important in Chapter 10.

DEFINITION 2.94 (ALGEBRAIC EXTENSIONS OF FUNCTION FIELDS) *A function field $\mathbb{F}'/K'$ is an* algebraic extension *of $\mathbb{F}/K$ if $K \subseteq K'$, $\mathbb{F} \subseteq \mathbb{F}'$ and $\mathbb{F}'$ is an algebraic field extension of $\mathbb{F}$. The extension $\mathbb{F}'|K'$ is called a* constant field extension *if $\mathbb{F}' = \mathbb{F}K'$ is the compositum of $\mathbb{F}$ and K'.*

DEFINITION 2.95 (TOWERS OF FUNCTION FIELDS) *A tower of function fields over $\mathbb{F}_q$ is an infinite family of function fields over $\mathbb{F}_q$, $\mathbb{F}^{(0)} \subsetneqq \mathbb{F}^{(1)} \subsetneqq \dots$, where $\lim_{i\to\infty} g(\mathbb{F}^{(i)}) = \infty$ and for every $i > 0$, $\mathbb{F}^{(i+1)}/\mathbb{F}_q$ is an algebraic extension of $\mathbb{F}^{(i)}/\mathbb{F}_q$ such that the field extension $\mathbb{F}^{(i+1)}|\mathbb{F}^{(i)}$ is finite and separable.*

Note that since the extensions $\mathbb{F}^{(i+1)}|\mathbb{F}^{(i)}$ are finite then they are also algebraic. Furthermore, the fact that they are also separable implies, by the primitive element theorem, that they are simple. Hence, $\mathbb{F}^{(i+1)} = \mathbb{F}^{(i)}(x_i)$ for some $x_i \in \mathbb{F}^{(i+1)}$, algebraic over $\mathbb{F}^{(i)}$.

Garcia and Stichtenoth constructed in [37], [38] (see also [75]), towers of function fields attaining the Drinfeld-Vlăduţ bound. Their constructions

are defined over all finite fields of *square cardinality* q. We will recall the definitions of the tower in [37], which we will henceforth refer to as the First Garcia-Stichtenoth tower.

DEFINITION 2.96 (FIRST GARCIA-STICHTENOTH TOWER) *Let $\mathbb{F}_q$ be a finite field with q square. The First Garcia-Stichtenoth tower of function fields over $\mathbb{F}_q$ is the tower $\mathcal{F} = \{\mathbb{F}^{(n)}\}_{n\geq 0}$, where $\mathbb{F}^{(0)} = \mathbb{F}_q(x_0)$ where $x_0 \in \mathbb{F}^{(0)}$ is trascendental over $\mathbb{F}_q$ and, for $n \geq 0$, $\mathbb{F}^{(n+1)}$ is recursively defined as $\mathbb{F}^{(n+1)} = \mathbb{F}^{(n)}(x_{n+1})$, where $x_n^{\sqrt{q}-1}x_{n+1}^{\sqrt{q}} + x_{n+1} = x_n^{\sqrt{q}}$.*

Not only did Garcia and Stichtenoth prove that the tower achieves Drinfeld-Vlăduţ bound but they also show that the genus of all the function fields in the tower can be explicitly computed.

THEOREM 2.97 *Let $\mathcal{F} = \{\mathbb{F}^{(n)}\}_{n\geq 0}$ be the First Garcia-Stichtenoth tower of function fields over $\mathbb{F}_q$. Then*

1. *The genus $g(\mathbb{F}^{(n)})$ of the function field $\mathbb{F}^{(n)}/\mathbb{F}_q$ is given by*

$$g(\mathbb{F}^{(n)}) = \begin{cases} \sqrt{q}^{n+1} + \sqrt{q}^{n} - \sqrt{q}^{n/2+1} - 2\sqrt{q}^{n/2} + 1 & \text{if } n \text{ even} \\ \sqrt{q}^{n+1} + \sqrt{q}^{n} - \frac{1}{2}\sqrt{q}^{(n+3)/2} - \frac{3}{2}\sqrt{q}^{(n+1)/2} - & \\ -\sqrt{q}^{(n-1)/2} + 1 & \text{if } n \text{ odd.} \end{cases}$$

   In particular, $g(\mathbb{F}^{(n)}) \to \infty$ when $n \to \infty$.

2. *The tower $\mathcal{F}$ attains the Drinfeld-Vlăduţ bound, i.e., its Ihara's limit $A(\mathcal{F})$ is given by*

$$A(\mathcal{F}) = \sqrt{q} - 1.$$

Another example of a tower $\mathcal{F}$ of function fields over any finite field $\mathbb{F}_q$ with q square, such that $A(\mathcal{F}) = \sqrt{q}-1$ was given by Garcia and Stichtenoth in [38].

2.11 Algebraic geometric codes

Algebraic geometric codes were introduced by V. Goppa [41] in 1981 and are described next, together with some of their properties. More details can be found in [75] or [77].

THEOREM 2.98 *Let $\mathbb{F}/\mathbb{F}_q$ be a function field. Let $P_0, P_1, \ldots, P_n \in \mathbb{P}^{(1)}(\mathbb{F})$ with $P_i \neq P_j$ for $i \neq j$. Define $D = \sum_{i=0}^{n} P_i \in \mathrm{Div}(\mathbb{F})$. Let $G \in \mathrm{Div}(\mathbb{F})$ such that* $\mathrm{supp}\ G \cap \mathrm{supp}\ D = \emptyset$. *The set*

$$C_L(D, G) := \{(f(P_0), f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$$

is a linear code over $\mathbb{F}_q$.

Note that, for all $i = 0, \ldots, n$, f cannot have a pole in P_i because of the condition $\mathrm{supp}\ G \cap \mathrm{supp}\ D = \emptyset$ and the evaluations $f(P_i)$ indeed belong to $\mathbb{F}_q$ by the fact that $\deg P_i = 1$ and Definition 2.15, Proposition 2.17 and Definition 2.18.

DEFINITION 2.99 *$C_L(D, G)$ is an* algebraic geometric (AG) evaluation code *or* Goppa function code[2].

REMARK 2.100 *AG evaluation codes are in fact a generalization of Reed-Solomon codes (Definition 1.17). Any $RS_q[n, t]$-code can be written as an AG evaluation code $C_L(D, G)$ over the* rational function field $\mathbb{F}_q(x)/\mathbb{F}_q$, *where $G = tP_\infty$ for a certain place $P_\infty \in \mathbb{P}^{(1)}(\mathbb{F}_q(x))$ and $P_0, P_1, \ldots, P_n$ are distinct (and different from P_∞) places in $\mathbb{P}^{(1)}(\mathbb{F}_q(x))$. It can be seen that $|\mathbb{P}^{(1)}(\mathbb{F}_q(x))| = q + 1$ so we can indeed define this linear code for any integers t, n with $0 \leq t \leq n < q$.*

The parameters of an AG evaluation code can be related to the Riemann-Roch spaces of some divisors.

PROPOSITION 2.101 *Let $C_L(D, G)$ be an algebraic geometric evaluation code. Then*

- *$C_L(D, G) \simeq \mathcal{L}(G)/\mathcal{L}(G - D)$ and hence*

$$\dim C_L(D, G) = \ell(G) - \ell(G - D).$$

  If $\deg G < \deg D$, then $\dim C_L(D, G) = \ell(G)$.

- *$d(C_L(D, G)) \geq n + 1 - \deg G$.*

[2]Given a function field $\mathbb{F}/\mathbb{F}_q$ and D, G as in Theorem 2.98 one can also define another linear code $C_\Omega(D, G)$ over $\mathbb{F}_q$ known as Goppa *residue* code (see again [75] or [77]) but we will not need these codes here.

The dual code of an AG evaluation code $C_L(D,G)$ can also be written as an algebraic geometric evaluation code.

PROPOSITION 2.102 *Let $C_L(D,G)$ be an algebraic geometric evaluation code. There exists a canonical divisor $W \in \mathrm{Div}(\mathbb{F})$ such that*

$$\mathrm{supp}\ (W - G + D) \cap \mathrm{supp}\ D = \emptyset$$

and

$$C_L(D,G)^{\perp} = C_L(D, W - G + D).$$

Hence we can also give a bounds for $d(C_L(D,G)^{\perp})$ in terms of $\deg G$ and g.

PROPOSITION 2.103 $d(C_L(D,G)^{\perp}) \geq \deg G - 2g + 2$.

The proof of the lower bound for $\alpha_q(\delta)$ in Theorem 1.33 uses families of algebraic-geometric codes defined on an asymptotically optimal family of function fields over $\mathbb{F}_q$. Theorem 1.33 was stated for every finite field $\mathbb{F}_q$ with q square. Next we state the general version of the theorem and also include for completion the proof, which can also be read in [75].

THEOREM 2.104 *Let $\mathbb{F}_q$ be a finite field. Then for $\delta \in [0, 1 - \frac{1}{A(q)}]$, we have*

$$\alpha_q(\delta) \geq (1 - \frac{1}{A(q)}) - \delta.$$

PROOF. Let $\mathcal{F} = \{\mathbb{F}^{(i)}\}_{i>0}$ be a family of function fields with

$$\lim_{i\to\infty} g(\mathbb{F}^{(i)}) = \infty$$

and

$$\lim_{i\to\infty} \frac{|\mathbb{P}^{(1)}(\mathbb{F}^{(i)})|}{g(\mathbb{F}^{(i)})} = A(q).$$

For all $i > 0$, write $n_i = |\mathbb{P}^{(1)}(\mathbb{F}^{(i)})|$, $g_i = g(\mathbb{F}^{(i)})$ and select $r_i \in \mathbb{Z}$ with $r_i < n_i$ and such that

$$\lim_{i\to\infty} \frac{r_i}{n_i} = 1 - \delta.$$

Let $D_i = \sum_{P \in \mathbb{P}^{(1)}(\mathbb{F}^{(i)})} P$ and select any $G_i \in \mathrm{Div}_{r_i}(\mathbb{F}^{(i)})$. Consider the linear code $C_i = C_L(D_i, G_i)$ over $\mathbb{F}_q$ with $\mathfrak{k}(C_i) = n_i$. By Proposition 2.101, we have $d(C_i) \geq n_i + 1 - r_i$. Since

$$\frac{d(C_i)}{\mathfrak{k}(C_i)} \geq 1 - \frac{r_i}{n_i},$$

there exists $\widetilde{\delta} \geq \delta$ such that

$$\limsup_{i \to \infty} \frac{d(C_i)}{\mathfrak{k}(C_i)} = \tilde{\delta}$$

and without loss of generality we can assume

$$\lim_{i \to \infty} \frac{d(C_i)}{\mathfrak{k}(C_i)} = \tilde{\delta}.$$

Again, by Proposition 2.101 and the definition of genus,

$$\dim C_i = \ell(G_i) \geq r_i - g_i + 1,$$

so

$$\limsup_{i \to \infty} \frac{\dim C_i}{\mathfrak{k}(C_i)} \geq \limsup_{i \to \infty} \frac{r_i - g_i + 1}{n_i} = 1 - \delta - \frac{1}{A(q)}.$$

Then $\alpha_q(\tilde{\delta}) \geq 1 - \delta - \frac{1}{A(q)}$ and, since α_q is decreasing and $\tilde{\delta} \geq \delta$, we also have $\alpha_q(\delta) \geq 1 - \delta - \frac{1}{A(q)}$. △

Finally, we show how to extend the construction of AG evaluation codes in order to obtain generalized linear codes (see section 1.3). Note that, according to Definition 2.15, Proposition 2.17 and Definition 2.18, the evaluation of a function f of some function field $\mathbb{F}/\mathbb{F}_q$ in a place $P \in \mathbb{P}^{(k)}(\mathbb{F})$ (provided f does not have a pole in P) is an element of a certain extension of $\mathbb{F}_q$ of degree k, that we can identify with $\mathbb{F}_{q^k}$. Therefore we have the following.

THEOREM 2.105 *Let $\mathbb{F}/\mathbb{F}_q$ be a function field. Let $P_0, P_1, \ldots, P_n \in \mathbb{P}(\mathbb{F})$ with $P_i \neq P_j$ for $i \neq j$. Let $k_i := \deg P_i$. Define $D = \sum_{i=0}^{n} P_i \in \mathrm{Div}(\mathbb{F})$. Let $G \in \mathrm{Div}(\mathbb{F})$ such that* $\mathrm{supp}\ G \cap \mathrm{supp}\ D = \emptyset$. *The set*

$$C_L(D, G) := \{(f(P_0), f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$$

is a generalized linear code over $\mathbb{F}_q$ with space of definition

$$\mathbb{F}_{q^{k_0}} \times \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_n}}.$$

DEFINITION 2.106 $C_L(D, G)$ *is a* generalized AG evaluation code.

THEOREM 2.107 *For any generalized AG evaluation code* $C_L(D, G)$*, we have* $\dim_{\mathbb{F}_q} C_L(D, G) = \ell(G) - \ell(G - D)$.

Chapter 3

Secret sharing

In this chapter we give formal definitions of the notion of secret sharing and some related concepts and properties, including the properties of linearity and t-strong multiplication.

3.1 Basic definitions

Secret sharing schemes will be defined in terms of random variables. We first need to recall some notions and properties about entropies of random variables. We will use the following terminology.

DEFINITION 3.1 *Let (R, Ω, Pr) be a probability space, (E, μ) be a measurable space and $X : (R, \Omega, Pr) \to (E, \mu)$ a random variable. Then we say that X is a random variable over the probability space R and with alphabet E. The notation "$X = x$" is, as usual in information theory, a shorthand for the set $\{r \in R : X(r) = x\}$. The support of X is*

$$\text{supp } X = \{x \in E : Pr(X = x) > 0\}.$$

The entropy of a random variable X measures how many bits of information are necessary *on average* to describe the values taken by X (see [24] for more information about this aspect). *Throughout this thesis we abbreviate* $\log_2 x$ *by* $\log x$.

DEFINITION 3.2 *Let X be a random variable with finite alphabet E. $H(X)$ is the (Shannon) entropy of X, given by*

$$H(X) := -\sum_{x \in E} Pr(X = x) \log Pr(X = x).$$

We have the following properties.

PROPOSITION 3.3 *Let X be a random variable with finite alphabet E.*

- $0 \leq H(X) \leq \log |E|$.
- $H(X) = 0$ *if and only if there exists* $x \in E$ *such that* $Pr(X = x) = 1$.
- $H(X) = \log |E|$ *is attained if and only if X has the uniform distribution over E.*

The conditional entropy measures the amount of information that a random variable gives about another random variable defined over the same probability space.

DEFINITION 3.4 *Let X, Y be two random variables over the same probability space (R, Ω, Pr) and with alphabets E, F respectively. The conditional entropy of Y with respect to X is $H(Y|X) := \sum_{x \in E} Pr(X = x) H(Y|X = x)$ where the variable $Y|X = x$ has the probability distribution of Y conditioned to the event $X = x$.*

PROPOSITION 3.5 *Let X, Y be random variables over the same probability space (R, Ω, Pr) and with alphabets E, F respectively. Then*

- $0 \leq H(Y|X) \leq H(Y)$.
- *If $H(Y|X) = 0$, then for every value $x \in E$, there exists $y \in F$ such that $Pr(Y = y|X = x) = 1$ ("the value of Y is fully determined by the value of X").*
- $H(Y|X) = H(Y)$ *if and only if X and Y are independent (Y gives no information about X).*
- $H(Y|X) = H(X \times Y) - H(X)$.

We will also need the following notation.

DEFINITION 3.6 *Let $S_1, \ldots, S_n$ be random variables over the same probability space (R, Ω, Pr) and with alphabets $E_1, \ldots, E_n$ respectively. For any subset $A = \{i_1, i_2, \ldots, i_t\} \subseteq \{1, \ldots, n\}$, S_A is the random variable $\prod_{i \in A} S_i$, i.e., the variable with alphabet $\prod_{i \in A} E_i$ such that for all $(a_{i_1}, \ldots, a_{i_t}) \in \prod_{i \in A} E_i$,*

$$Pr(S_A = (a_{i_1}, \ldots, a_{i_t})) := Pr(S_{i_1} = a_{i_1}, \ldots, S_{i_t} = a_{i_t}).$$

We can finally give the general definition of secret sharing scheme.

DEFINITION 3.7 (SECRET SHARING SCHEME) *A* secret sharing scheme *is a tuple* $\Sigma = (n, E_0, E_1, \ldots, E_n, S_0, S_1, \ldots, S_n)$ *where* $n \geq 2$ *is a positive integer and* $S_0, S_1, \ldots, S_n$ *are random variables over the same probability space* (R, Ω, Pr) *and with finite alphabets* $E_0, E_1, \ldots, E_n$ *and the following properties are satisfied:*

- $H(S_0) \neq 0$
- $H(S_0|S_{\{1,\ldots,n\}}) = 0$

S_0 *is called the* secret *and* $S_1, \ldots, S_n$ *are called the* shares.

Two families of subsets of $\{1, \ldots, n\}$, the access and adversary structures, are associated to a secret sharing scheme.

DEFINITION 3.8 (ACCESS STRUCTURE) *Let* Σ *be a secret sharing scheme. We define its* access structure $\Gamma(\Sigma) \subset 2^{\{1,\ldots,n\}}$ *(where* $2^{\{1,\ldots,n\}}$ *denotes the power set of* $\{1, \ldots, n\}$*) as the following family of sets:*

$$\Gamma(\Sigma) := \{A \subseteq \{1, \ldots, n\} \text{ such that } H(S_0|S_A) = 0\}.$$

A qualified set *is a set* $A \in \Gamma(\Sigma)$.

Therefore $\Gamma(\Sigma)$ contains all subsets $A \subseteq \{1, \ldots, n\}$ such that S_A fully determines S_0. Note that $\{1, \ldots, n\} \in \Gamma(\Sigma)$ by definition.

PROPOSITION 3.9 (MONOTONY OF THE ACCESS STRUCTURE) *If* $A \in \Gamma(\Sigma)$ *and* $A \subseteq B \subseteq \{1, \ldots, n\}$*, then* $B \in \Gamma(\Sigma)$.

DEFINITION 3.10 (ADVERSARY STRUCTURE) *Let* Σ *be a secret sharing scheme. We define its* adversary structure $\mathcal{A}(\Sigma) \subset 2^{\{1,\ldots,n\}}$ *as the following family sets:*

$$\mathcal{A}(\Sigma) := \{A \subseteq \{1, \ldots, n\} \text{ such that } H(S_0|S_A) = H(S_0)\} \cup \{\emptyset\}.$$

An unqualified set *is a set* $A \in \mathcal{A}(\Sigma)$.

Consequently, the adversary structure collects (in addition to the empty set) all subsets $A \subseteq \{1, \ldots, n\}$ such that S_A and S_0 are independent random variables, i.e., S_A does not give any information about S_0. Clearly the following is satisfied.

PROPOSITION 3.11 (ANTIMONOTONY OF THE ADVERSARY STRUCTURE) *If* $A \in \mathcal{A}(\Sigma)$ *and* $B \subseteq A \subseteq \{1, \ldots, n\}$, *then* $B \in \mathcal{A}(\Sigma)$.

PROPOSITION 3.12 *For any secret sharing scheme* Σ, *we have*

$$\Gamma(\Sigma) \cap \mathcal{A}(\Sigma) = \emptyset.$$

We now define the reconstruction and privacy thresholds of a secret sharing scheme.

DEFINITION 3.13 *The* reconstruction threshold $r(\Sigma)$ *of* Σ *is defined as the smallest integer* r *such that every* $A \subset \{1, \ldots, n\}$ *with* $|A| = r$ *is qualified, i.e.* $A \in \Gamma(\Sigma)$. *For any* $r' \geq r(\Sigma)$ *we say that* Σ *has* r'*-reconstruction.*

DEFINITION 3.14 *The* privacy threshold $t(\Sigma)$ *of* Σ *is defined as the smallest integer* t *such that every* $A \subset \{1, \ldots, n\}$ *with* $|A| = t$ *is unqualified, i.e.* $A \in \mathcal{A}(\Sigma)$. *For any* $t' \leq t(\Sigma)$ *we say that* Σ *has* t'*-privacy.*

Given an arbitrary secret sharing scheme Σ there may exist, in principle, three different kinds of subsets of $\{1, \ldots, n\}$. Apart from the qualified and unqualified sets, there can also be subsets $A \subseteq \{1, \ldots, n\}$ such that $0 < H(S_0|S_A) < H(S_0)$. However, there are examples of secret sharing schemes where this does not happen.

DEFINITION 3.15 *A secret sharing scheme* Σ *is* perfect *if*

$$\Gamma(\Sigma) \cup \mathcal{A}(\Sigma) = 2^{\{1,\ldots,n\}}.$$

An even stronger property is the following one.

DEFINITION 3.16 *A secret sharing scheme* Σ *is a* threshold *scheme if* $t(\Sigma) = t$ *and* $r(\Sigma) = t + 1$ *for some* $1 \leq t < n$.

There is an important limitation for perfect schemes, that we explain next.

DEFINITION 3.17 *Let* Σ *be a perfect scheme. We say that an index* $i \in \{1, \ldots, n\}$ *is* dummy *if* i *does not belong to any minimal qualified set, that is, if there does not exist a set* $A \subseteq \{1, \ldots, n\} \setminus \{i\}$ *such that* $A \notin \Gamma(\Sigma)$ *and* $A \cup \{i\} \in \Gamma(\Sigma)$.

THEOREM 3.18 *Let Σ be a perfect secret sharing scheme. If i is not a dummy index then $H(S_i) \geq H(S_0)$.*

It is a usually desirable for the applications that the share variables of a secret sharing scheme have as small entropy as possible compared to the secret. This is because the smaller the entropy is, the smaller the average amount of information which is needed to encode the values taken by S_i according to its probability distribution. Typically one wants to store (or send) the smallest possible amount of information for a secret of certain size.

DEFINITION 3.19 *Let Σ be a perfect secret sharing scheme. We say Σ is* pseudoideal *if $H(S_i) = H(S_0)$ for some $i \in \{1, \ldots, n\}$ and, whenever $H(S_j) \neq H(S_0)$ for some $j \in \{1, \ldots, n\}$, then j is dummy. If, in addition, there are no dummy players, then Σ is* ideal.

3.2 Linear secret sharing schemes

An important class of secret sharing schemes are linear secret sharing schemes.

DEFINITION 3.20 *Let $\mathbb{F}_q$ be a finite field. Let*

$$\Sigma = (n, E_0, E_1, \ldots, E_n, S_0, S_1, \ldots, S_n)$$

be a secret sharing scheme and denote $S := S_{\{0,1,\ldots,n\}}$. Then Σ is a linear secret sharing scheme(LSSS) over $\mathbb{F}_q$ *if E_i is a finite dimensional vector space over $\mathbb{F}_q$ for $i = 0, 1, \ldots, n$,* supp $S \subseteq \bigoplus_{i=0}^{n} E_i$ *is also a vector space over $\mathbb{F}_q$ and the probability distribution of S is uniform on* supp S.

PROPOSITION 3.21 *If Σ is a LSSS over $\mathbb{F}_q$, then for every $A \subseteq \{0, \ldots, n\}$ the support of every random variable S_A is also a $\mathbb{F}_q$-linear space and the probability distribution of S_A is uniform on* supp S_A. *In particular, this happens for $S_0, S_1, \ldots, S_n$.*

We can consider, without loss of generality, $E_i :=$ supp S_i. More generally,

DEFINITION 3.22 *For every $A \subseteq \{0, \ldots, n\}$, let $E_A :=$ supp S_A and $d_A := \dim E_A$. For every $i \in \{0, \ldots, n\}$, let $E_i := E_{\{i\}}$ $d_i := d_{\{i\}}$. Finally, let $E :=$ supp S.*

One can now restate the properties of general secret sharing schemes given before in the particular case that these are linear. Note first:

LEMMA 3.23 *For every $A \subseteq \{0, \ldots, n\}$, we have $H(S_A) = \log |E_A| = d_A \log q$.*

Using the fact that for any two random variables X, Y, it holds that $H(Y|X) = H(X \times Y) - H(X)$, one gets

LEMMA 3.24 *For every $A, B \subseteq \{0, \ldots, n\}$, we have*

$$H(S_B|S_A) = H(S_{A\cup B}) - H(S_A) = (d_{A\cup B} - d_A) \log q$$

and in particular for every $A \subseteq \{1, \ldots, n\}$,

$$H(S_0|S_A) = H(S_{A\cup\{0\}}) - H(S_A) = (d_{A\cup\{0\}} - d_A) \log q.$$

Now we obtain the following characterization of the access and adversary structures of Σ (see Definitions 3.8 and 3.10).

PROPOSITION 3.25 *Let $A \subseteq \{1, \ldots, n\}$. Then*

$$A \in \Gamma(\Sigma) \iff d_{A\cup\{0\}} = d_A$$

and

$$A \in \mathcal{A}(\Sigma) \iff d_{A\cup\{0\}} = d_0 + d_A \text{ or } A = \emptyset.$$

In other words, we have

$$\Gamma(\Sigma) = \{A \subseteq \{1, \ldots, n\} : E_{A\cup\{0\}} \simeq E_A\}$$

(where $\simeq$ denotes an isomorphism of $\mathbb{F}_q$-vector spaces) and

$$\mathcal{A}(\Sigma) = \{A \subseteq \{1, \ldots, n\} : E_{A\cup\{0\}} = E_0 \times E_A\} \cup \{\emptyset\}.$$

Finally, we note that an ideal linear scheme is characterized by the following:

PROPOSITION 3.26 *A perfect LSSS Σ is ideal if there are no dummy indices and $d_i = d_0$ for all $i = 1, \ldots, n$.*

3.3 Multiplication and strong multiplication

We introduce now the properties of multiplication of a linear secret sharing scheme. These have found important applications in a number of works. The main motivation for this property is the problem of multiparty computation. The property was introduced by Cramer, Damgård and Maurer in [32].

In order to introduce these properties, we need to define some product in the supports $E_0, E_1, \ldots, E_n$ of the secret and share variables. We will consider that these supports are $E_i = \mathbb{F}_q^{r_i}$, for possibly diferent integers $r_i > 0$, and the products that we consider are Schur products, which are introduced next.

DEFINITION 3.27 *The* Schur product *(also known as Hadamard product or coordinatewise product) of two vectors* $\mathbf{x} = (x_0, x_1, \ldots, x_{r-1}) \in \mathbb{F}_q^r$ *and* $\mathbf{y} = (y_0, y_1, \ldots, y_{r-1}) \in \mathbb{F}_q^r$*, is defined as the vector*

$$\mathbf{x} * \mathbf{y} := (x_0 y_0, x_1 y_1, \ldots, x_{r-1} y_{r-1}) \in \mathbb{F}_q^r.$$

Now we can define the t-multiplication property as follows:

DEFINITION 3.28 (t-MULTIPLICATION) *Let* $r_0, r_1, \ldots, r_n > 0$ *be integers and*

$$\Sigma = (n, \mathbb{F}_q^{r_0}, \mathbb{F}_q^{r_1}, \ldots, \mathbb{F}_q^{r_n}, S_0, S_1, \ldots, S_n)$$

be a linear secret sharing scheme. Let t *be an integer with* $1 \leq t \leq n$*. We say* Σ *has* t*-multiplication if the following holds:*

- $t(\Sigma) \geq t$.
- *There exists a linear function* $\Psi : \bigoplus_{i=1}^n \mathbb{F}_q^{r_i} \to \mathbb{F}_q^{r_0}$ *such that for all* $x, y \in E$*,*

  $$\pi_0(x) * \pi_0(y) = \Psi\left(\pi_1(x) * \pi_1(y), \ldots, \pi_n(x) * \pi_n(y)\right)$$

  where for $x \in E \subseteq \bigoplus_{i=0}^n \mathbb{F}_q^{r_i}$*, if we write* $x = (x_0, x_1, \ldots, x_n)$ *with* $x_i \in \mathbb{F}_q^{r_i}$ *for all* $i \in \{0, \ldots, n\}$*, then* $\pi_i(x) := x_i$.

REMARK 3.29 *In this thesis, we will be only interested in the case where* $r_i = 1$ *for all* $i \in \{0, 1, \ldots, n\}$*. Hence the product* $*$ *is simply the ordinary product in* $\mathbb{F}_q$.

Note also that the multiplication property can be defined with respect to other types of products. For example, if the vector spaces E_i *are seen as extension fields* $\mathbb{F}_{q^{r_i}}$ *of* $\mathbb{F}_q$ *and we consider the field product in* $\mathbb{F}_{q^{r_i}}$.

The following fact can be found in [32].

THEOREM 3.30 *If Σ has t-multiplication for an integer $t \geq 1$, then $2t < n$.*

Now one can generalize this notion and consider the case where it suffices to have some of the products $\pi_i(x) * \pi_i(y)$ in order to determine $\pi_0(x) * \pi_0(y)$.

DEFINITION 3.31 *Let Σ be a LSSS with $t(\Sigma) \geq 1$. Let $\widehat{\Gamma}$ be a non-empty family of subsets of $\{1, \ldots, n\}$. We say that Σ has the $\widehat{\Gamma}$-product reconstruction property if for any $A \in \widehat{\Gamma}$, there exists a linear function $\Psi_A : \prod_{i \in A} E_i \to E_0$ such that for all $x, y \in E$,*

$$\pi_0(x) * \pi_0(y) = \Psi_A((\pi_i(x) * \pi_i(y))_{i \in A})$$

DEFINITION 3.32 *Let Σ be a LSSS with $t(\Sigma) \geq 1$. Let us define $\widehat{\Gamma}(\Sigma)$ as the maximal family $\widehat{\Gamma}$ for which Σ has the $\widehat{\Gamma}$-product reconstruction property (or $\widehat{\Gamma}(\Sigma) := \emptyset$ if there is no $\widehat{\Gamma}$ for which Σ has the $\widehat{\Gamma}$-product reconstruction property).*

Note that $\widehat{\Gamma}(\Sigma)$ is a monotone structure, that is if $A \subseteq B$ and $A \in \widehat{\Gamma}(\Sigma)$, then $B \in \widehat{\Gamma}(\Sigma)$. Consequently if $\widehat{\Gamma}(\Sigma) \neq \emptyset$, clearly $\{1, \ldots, n\} \in \widehat{\Gamma}(\Sigma)$. Now note that it is straightforward that

LEMMA 3.33 *If $t(\Sigma) \geq t$ and Σ has the $\widehat{\Gamma}$-product reconstruction property for $\widehat{\Gamma} = \{\{1, \ldots, n\}\}$ then Σ has the t-multiplication property. In other words Σ has the t-multiplication property if and only if $t(\Sigma) \geq t$ and $\widehat{\Gamma}(\Sigma) \neq \emptyset$.*

The fundamental property for applications to multiparty computation is the property of strong multiplication, which is defined next.

DEFINITION 3.34 *We say that a LSSS Σ has the* strong multiplication *property with respect to $\widetilde{\mathcal{A}}$ if:*

- *$\widetilde{\mathcal{A}} \subseteq \mathcal{A}(\Sigma)$, that is every set in $\widetilde{\mathcal{A}}$ is in the adversary structure of Σ.*
- *For every set $A \in \widetilde{\mathcal{A}}$, we have $A^c \in \widehat{\Gamma}(\Sigma)$, where $A^c := \{1, \ldots, n\} \setminus A$.*

As a particular case of great interest in this text, the concept of t-strong multiplication is defined next.

DEFINITION 3.35 (t-STRONG MULTIPLICATION) *Let $t \in \mathbb{Z}$ with $t \geq 1$. We say that a LSSS Σ has* t-strong multiplication *if it has the* strong multiplication *property with respect to $\widetilde{\mathcal{A}}$, where $\widetilde{\mathcal{A}}$ contains all sets $A \subseteq \{1, \ldots, n\}$ of size t.*

So a LSSS Σ has t-strong multiplication if and only if $t(\Sigma) \geq t$ and Σ has "$(n-t)$-product reconstruction", i.e., any set $B \subseteq \{1, \ldots, n\}$ of size $n-t$ is in $\widehat{\Gamma}(\Sigma)$. Note that:

LEMMA 3.36 *If Σ has t-strong multiplication, then for any integer t' with $1 \leq t' \leq t$, Σ has t'-strong multiplication.*

Moreover the following facts are known:

THEOREM 3.37 *Let Σ be a LSSS with t-strong multiplication. Then we have $r(\Sigma) \leq (n - 2t)$. Consequently $3t < n$. In addition, if $3t = n - 1$ then $t(\Sigma) = t$ and $r(\Sigma) = t + 1$.*

3.4 Specific examples

In this section, two examples of families of linear secret sharing schemes will be presented.

3.4.1 Shamir's schemes

The following family of secret sharing schemes was proposed in the seminal paper about secret sharing [72] and has been widely used in cryptography.

DEFINITION 3.38 (SHAMIR'S SECRET SHARING SCHEME) *Let $\mathbb{F}_q$ be a finite field. Let t,n be integers such that $1 \leq t < n < q$. Let $x_1, x_2, \ldots, x_n$ be distinct nonzero elements in $\mathbb{F}_q$. Shamir's scheme $\Sigma_{Sh}(\mathbb{F}_q, t, n, x_1, \ldots, x_n)$ is the vector of $n+1$ random variables $(S_0, S_1, \ldots, S_n)$ which take values in $\mathbb{F}_q$ (that is, $E_0 = E_1 = \cdots = E_n = \mathbb{F}_q$) according to the following probability distribution: $S_0 = f(0)$ and $S_i = f(x_i)$ for $i = 1, \ldots, n$ where f is sampled uniformly at random from the set $\mathbb{F}_q[X]_{\leq t}$.*

The well known Lagrange interpolation Theorem, which we recall now, can be used to show some properties about Shamir's scheme.

THEOREM 3.39 (LAGRANGE INTERPOLATION) *Let $x_1, \ldots, x_{t+1}, y_1, \ldots, y_{t+1}$ be arbitrary elements in $\mathbb{F}_q$, where $x_i \neq x_j$ for any $i \neq j$. Then there exists a unique polynomial $f \in \mathbb{F}_q[X]_{\leq t}$ such that $f(x_i) = y_i$ for any $i \in 1, \ldots, t+1$. This polynomial is*

$$f(X) = \sum_{i=1}^{t+1} y_i \cdot \frac{\prod_{j=1, j\neq i}^{t+1}(X - x_j)}{\prod_{j=1, j\neq i}^{t+1}(x_i - x_j)}.$$

THEOREM 3.40 *$\Sigma = \Sigma_{Sh}(\mathbb{F}_q, t, n, x_1, \ldots, x_n)$ is an ideal threshold linear secret sharing scheme satisfying $t(\Sigma) = t$, $r(\Sigma) = t + 1$.*

Note that indeed, Σ is linear. In fact, the support of the product random variable S is a $RS_q[n, t]$-code. For every $i \in \{1, \ldots, n\}$, S_i has the uniform distribution on $\mathbb{F}_q$, and so does S_0, and therefore $H(S_i) = H(S_0)$. Lagrange's theorem can be used to prove that Σ is threshold: for any $A \subset \{1, \ldots, n\}$ with $|A| = t + 1$, the values of the variables $S_i, i \in A$ are the evaluations of a polynomial $f \in \mathbb{F}_q[X]_{\leq t}$ in the $t + 1$ points x_i with $i \in A$. By Lagrange's Theorem, f is uniquely determined by these values, and hence so is $f(0)$ and consequently the value of S_0. Therefore $r(\Sigma) \leq t + 1$. On the other hand for any set B with $|B| = t$, any values $(y_i)_{i\in B} \in \mathbb{F}_q^{|B|}$ and any $s \in \mathbb{F}_q$ there exists exactly one polynomial of degree at most t such that $f(x_i) = y_i$ for all $i \in B$ and $f(0) = s$, again by the interpolation Lemma. So $S_0|S_B = (f(x_i))_{i\in B}$ has the uniform distribution and $t(\Sigma) = t$ (so in addition $r(\Sigma) = t + 1$). Therefore Σ is threshold and consequently perfect.

THEOREM 3.41 *$\Sigma_{Sh}(\mathbb{F}_q, t, n, x_1, \ldots, x_n)$ has t-multiplication if and only if $2t < n$. Moreover $\Sigma_{Sh}(\mathbb{F}_q, t, n, x_1, \ldots, x_n)$ has t-strong multiplication if and only if $3t < n$.*

This is due to the fact that for any $f, g \in \mathbb{F}_q[X]_{\leq t}$ and $i \in \{0, \ldots, n\}$, we have $f(x_i)g(x_i) = (fg)(x_i)$ and $fg \in \mathbb{F}_q[X]_{\leq 2t}$. By Lagrange interpolation Theorem, if $2t < n$, the value $fg(x_0)$ is determined by the values $fg(x_i)$, $i = 1, \ldots, n$. In fact it is determined by any subset $fg(x_i)$, $i \in B$, $B \subseteq \{1, \ldots, n\}, |B| = 2t + 1$. If in addition $3t < n$, then $2t + 1 \leq n - t$ and the interpolation Theorem proves that Σ has t-strong multiplication. Theorems 3.30 and 3.37 state that these two facts cannot happen for larger t.

Shamir's schemes can only be defined in the case $n < q$. But in fact, one can slightly modify the definition of Shamir's scheme to cope with the case

$n = q$. In this case, the shares are the evaluations of a polynomial randomly chosen in $\mathbb{F}_q[X]_{\leq t}$ in *all* q points of $\mathbb{F}_q$. The secret is now the coefficient of X^t of this polynomial (in the case that the chosen polynomial has degree less than t, the secret is then 0). Theorems 3.40 and 3.41 are still valid for these modified schemes.

3.4.2 Algebraic geometric secret sharing schemes

In [20], Cramer and Chen introduced algebraic geometric schemes, which have strong multiplication but are not restricted by the condition $n \leq q$. These schemes are ideal LSSS based on algebraic geometric codes. Just as algebraic geometric codes are a generalization of Reed-Solomon codes, so it happens that algebraic geometric schemes are a generalization of Shamir's scheme.

DEFINITION 3.42 (ALGEBRAIC GEOMETRIC SCHEME) *Let $n \geq 2$ be an integer and $\mathbb{F}/\mathbb{F}_q$ be a function field with $|\mathbb{P}^{(1)}(\mathbb{F})| \geq n+1$.*
Let $P_0, P_1, \ldots, P_n \in \mathbb{P}^{(1)}(\mathbb{F})$, with $P_i \neq P_j$ for $i \neq j$ and define $D = \sum_{i=0}^{n} P_i$.
Let $G \in \mathrm{Div}(\mathbb{F})$ such that supp $G \cap$ supp$D = \emptyset$, *$\ell(G) > \ell(G - P_0)$ and $\ell(G - \sum_{i=1}^{n} P_i) = \ell(G - \sum_{i=0}^{n} P_i)$.*
The algebraic geometric linear secret sharing scheme *$\Sigma_{AG}(\mathbb{F}, G, P_0, P_1, \ldots, P_n)$ is the vector of random variables $(S_0, S_1, \ldots, S_n)$ which take the values $S_i = f(P_i), i = 0, \ldots, n$, where f is selected uniformly at random in $\mathcal{L}(G)$.*
In addition we write, for every set $A \subseteq \{1, \ldots, n\}$, $P_A := \sum_{i \in A} P_i \in \mathrm{Div}(\mathbb{F})$.

Note that the sets $E_1, \ldots, E_n$ are either the trivial space $\{0\}$ or $\mathbb{F}_q$. $E_0 = \mathbb{F}_q$ since $\ell(G) > \ell(G - P_0)$ and

$$\text{supp } S_{\{0,1,\ldots,n\}} = C_L(D, G).$$

The following results were proved in [20].

PROPOSITION 3.43 *Let $\Sigma = \Sigma_{AG}(\mathbb{F}, G, P_0, P_1, \ldots, P_n)$. Then for every set $A \subseteq \{1, \ldots, n\}$,*

$$A \in \Gamma(\Sigma) \Leftrightarrow \ell(G - P_A - P_0) = \ell(G - P_A).$$

Moreover

$$\ell(2G - P_A - P_0) = \ell(2G - P_A) \Rightarrow A \in \widehat{\Gamma}(\Sigma)$$

One can argue by simply considering the degrees of the divisors involved and applying Lemma 2.51 and Corollary 2.67

THEOREM 3.44 *Let* $\Sigma = \Sigma_{AG}(\mathbb{F}, G, P_0, P_1, \ldots, P_n)$. *Then* $t(\Sigma) \geq \deg G - 2g$ *and* $r(\Sigma) \leq \deg G + 1$. *Moreover, assume that* $\deg G = 2g + t$. *Then* Σ *has* t*-multiplication if* $2t < n - 4g$ *and* t*-strong multiplication if* $3t < n - 4g$.

Part II

Asymptotics of strongly multiplicative secret sharing

Chapter 4

A coding theoretic framework for strongly multiplicative secret sharing

In this chapter we explore the connection between ideal linear secret sharing schemes and linear codes and introduce a coding theoretic framework for the study of linear secret sharing schemes with t-strong multiplication. In order to do this, we define the notion of *corruption tolerance* of a linear code. This framework has been published in [15], although some of the notions are defined in a slightly different language in this text.

In addition to this, we will establish some limitations of linear threshold schemes by showing the connection to MDS codes and using the upper bounds for the length of these codes stated in Chapter 1. This will motivate the asymptotical study in next chapters.

4.1 Basic notions and properties

We first introduce the following notation.

DEFINITION 4.1 *Let C be a linear code over $\mathbb{F}_q$ of length $\mathfrak{k}(C)$. We define $n(C) := \mathfrak{k}(C) - 1$.*

For the rest of the chapter, C will denote a linear code over $\mathbb{F}_q$ with $n(C) \geq 2$.

DEFINITION 4.2 *Let n be an integer with $n \geq 2$ and let $\mathbb{F}_q$ be a finite field. For a non-empty set $B \subset \{0, 1, \ldots, n\}$, the $\mathbb{F}_q$-linear projection map $\pi_B^{q,n+1}$ is defined as*

$$\pi_B^{q,n+1} : C \longrightarrow \mathbb{F}_q^{|B|},$$
$$(c_0, c_1, \ldots, c_n) \mapsto (c_i)_{i \in B}.$$

When q and n are clear from the context, we write π_B instead. Also, if $B = \{i\}$ for some index i, we write π_i instead of $\pi_{\{i\}}$.

DEFINITION 4.3 *Let C be a linear code over $\mathbb{F}_q$. For all $x \in \mathbb{F}_q$, $i \in \mathcal{I}(C)$, we define the set*

$$C_{i,x} := \{\mathbf{c} \in C : \pi_i(\mathbf{c}) = x\} \subseteq C.$$

In particular $C_{i,0}$ is a linear subcode of C. Moreover, for $\emptyset \neq A \subseteq \mathcal{I}(C)$, and $\mathbf{x} \in \mathbb{F}_q^{|A|}$ we define

$$C_{A,\mathbf{x}} := \{\mathbf{c} \in C : \pi_A(\mathbf{c}) = \mathbf{x}\}.$$

The notion of minimal weight at an index, which will be introduced next, will be fundamental throughout this text.

DEFINITION 4.4 (MINIMAL WEIGHT AT AN INDEX) *Let C be a linear code over $\mathbb{F}_q$ and $i \in \mathcal{I}(C)$. The* minimal weight of C at the index i *is defined as*

$$w_i(C) := \begin{cases} \min_{\mathbf{c} \in C_{i,1}} w_{Ham}(\mathbf{c}) & \text{if } C_{i,1} \neq \emptyset. \\ 0 & \text{if } C_{i,1} = \emptyset. \end{cases}$$

In addition, let $w_i^{\perp}(C) := w_i(C^{\perp})$ be the minimal weight of $C^{\perp}$ at the index i.

REMARK 4.5 *Let C be a linear code over $\mathbb{F}_q$ and $i \in \mathcal{I}(C)$. For all $x \neq 0$, $C_{i,x} \neq \emptyset \iff w_i^{\perp}(C) \neq 1$. Moreover, if $C_{i,x} \neq \emptyset$ then $C_{i,x} = \mathbf{c} + C_{i,0}$ for some $\mathbf{c} \in C_{i,x}$.*

In fact, for all $x \in \mathbb{F}_q \setminus \{0\}$, there exists a bijection between $C_{i,1}$ and $C_{i,x}$ (that is the scalar multiplication by x) that preserves the weight of every word, so the combinatorial properties of both sets (regarding the distribution of zeros in the words) are the same and the definition of $w_i(C)$ would not differ if we substitute the value 1 by any $x \in \mathbb{F}_q \setminus \{0\}$.

The primal and dual distances of C can of course be related to the minimal weights $w_i(C)$ as follows.

LEMMA 4.6 *Let C be a linear code over $\mathbb{F}_q$. If $C \neq \{\mathbf{0}\}$ then*

$$d(C) = \min\{w_i(C) : i \in \mathcal{I}(C), w_i(C) > 0\}.$$

If $C \neq \mathbb{F}_q^{\ell(C)}$ then

$$d(C^\perp) = \min\{w_i^\perp(C) : i \in \mathcal{I}(C), w_i^\perp(C) > 0\}.$$

LEMMA 4.7 *Let C be a linear code over $\mathbb{F}_q$, $i \in \mathcal{I}(C)$. We have*

- *$w_i(C) = 0 \iff C = C_{i,0} \iff \mathbf{u}_i \in C^\perp \iff w_i^\perp(C) = 1$ where $\mathbf{u}_i \in \mathbb{F}_q^{n(C)+1}$ denotes the i-th unit vector, i.e., the vector given by $\pi_i(\mathbf{u}_i) = 1$ and $\pi_j(\mathbf{u}_i) = 0$ for all $j \in \mathcal{I}(C) \setminus \{i\}$.*
- *By dualization $w_i(C) = 1 \iff w_i^\perp(C) = 0$.*
- *As a consequence of both facts $w_i(C) \geq 2 \iff w_i^\perp(C) \geq 2$.*

In the following sections, we will consider linear codes over $\mathbb{F}_q$ in certain class, which we will introduce next.

DEFINITION 4.8 *Let C be a linear code over $\mathbb{F}_q$. An index $i \in \mathcal{I}(C)$ is called* good *if $w_i(C) > 1$. The set of all good indices of C is written $I(C)$.*

On account of Lemma 4.7, if we replace the condition $w_i(C) > 1$ by $w_i^\perp(C) > 1$ we get an equivalent definition. Moreover, $I(C) = I(C^\perp)$. Now, we define the class of codes which have at least one good index.

DEFINITION 4.9 *$\mathcal{C}(\mathbb{F}_q)$ is the set of all linear codes over $\mathbb{F}_q$ with $I(C) \neq \emptyset$.*

In the next section we will describe how to construct a LSSS from a pair (C, i) with $C \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(C)$. First we give definitions of some notions associated to these pairs (C, i). These are combinatorial definitions that do not contain any reference to secret sharing. However, they will later be associated to known concepts related to the corresponding LSSS, which we introduced in Chapter 3.

DEFINITION 4.10 *For $C \in \mathcal{C}(\mathbb{F}_q)$, $i \in I(C)$, we denote $\mathcal{P}(C, i) := \mathcal{I}(C) \setminus \{i\}$. For any $A \subseteq \mathcal{P}(C, i)$, let A^c denote the complement of A within $\mathcal{P}(C, i)$, that is $A^c := \mathcal{P}(C, i) \setminus A$.*

DEFINITION 4.11 *Let $C \in \mathcal{C}(\mathbb{F}_q), i \in I(C)$.*
The access structure of the pair (C,i) *is defined as*

$$\Gamma(C,i) := \{A \subseteq \mathcal{P}(C,i) : \exists \mathbf{c} \in C^{\perp} \text{ with } \pi_i(\mathbf{c}) = 1, \pi_{A^c}(\mathbf{c}) = \mathbf{0}\} \cup \{\mathcal{P}(C,i)\}.$$

The adversary structure of the pair (C,i) *is*

$$\mathcal{A}(C,i) := \{A \subseteq \mathcal{P}(C,i) : \exists \mathbf{c} \in C \text{ with } \pi_i(\mathbf{c}) = 1, \pi_A(\mathbf{c}) = \mathbf{0}\} \cup \{\emptyset\}.$$

Since for any $i \in I(C)$, we know that both $w_i(C), w_i^{\perp}(C) > 1$, it is not difficult to check that:

LEMMA 4.12 *For any $C \in \mathcal{C}(\mathbb{F}_q)$ and any $i \in I(C)$, we have $\emptyset \notin \Gamma(C,i)$, $\mathcal{P}(C,i) \in \Gamma(C,i)$, $\emptyset \in \mathcal{A}(C,i)$ and $\mathcal{P}(C,i) \notin \mathcal{A}(C,i)$.*

Note that $\mathcal{P}(C,i) \in \Gamma(C,i)$, $\emptyset \in \mathcal{A}(C,i)$ are only stated here for completion, since both hold by definition.

The following properties follow directly from the definitions of the access and adversary structures.

LEMMA 4.13 *For any $C \in \mathcal{C}(\mathbb{F}_q)$ and any $i \in I(C)$,*

- *$\Gamma(C,i)$ is monotone, i.e., for any $A \subseteq B \subseteq \mathcal{P}(C,i)$, if $A \in \Gamma(C,i)$ then $B \in \Gamma(C,i)$.*
- *$\mathcal{A}(C,i)$ is antimonotone, i.e., for any $A \subseteq B \subseteq \mathcal{P}(C,i)$, if $B \in \mathcal{A}(C,i)$ then $A \in \mathcal{A}(C,i)$.*

We now prove some useful results involving these notions.

THEOREM 4.14 *Let $C \in \mathcal{C}(\mathbb{F}_q)$, $i \in I(C)$. We have the following properties:*

1. *$\Gamma(C,i) \amalg \mathcal{A}(C,i) = 2^{\mathcal{P}(C,i)}$ (where $\amalg$ denotes the disjoint union).*
2. *$A \in \Gamma(C,i) \iff A^c \notin \Gamma(C^{\perp},i)$.*

PROOF. 1) We prove first $\mathcal{A}(C,i) \cap \Gamma(C,i) = \emptyset$. Suppose there exists $A \in \mathcal{A}(C,i) \cap \Gamma(C,i)$. Clearly $A \neq \emptyset$ and $A \neq \mathcal{P}(C,i)$ because of Lemma 4.12. Then $A \in \mathcal{A}(C,i)$ implies that there exists a word $\mathbf{c} \in C_{i,1}$ with $\pi_A(\mathbf{c}) = \mathbf{0}$.

On the other hand, $A \in \Gamma(C,i)$ implies that there exists $\mathbf{w} \in (C^\perp)_{i,1}$ with $\pi_{A^c}(\mathbf{w}) = \mathbf{0}$. Then, since $\mathcal{I}(C) = \{i\} \cup A \cup A^c$,

$$0 =< \mathbf{c}, \mathbf{w} >= \pi_i(\mathbf{c})\pi_i(\mathbf{w}) + < \pi_A(\mathbf{c}), \pi_A(\mathbf{w}) > + < \pi_{A^c}(\mathbf{c}), \pi_{A^c}(\mathbf{w}) >=$$

$$= 1 \cdot 1 + 0 + 0$$

which is a contradiction.

Now we prove $\mathcal{A}(C,i) \cup \Gamma(C,i) = 2^{\mathcal{P}(C,i)}$. Assume $A \notin \Gamma(C,i)$. If $A = \emptyset$, then $A \in \mathcal{A}(C,i)$ by definition. Otherwise apply the following reasoning. $A \notin \Gamma(C,i)$ implies $A \neq \mathcal{P}(C,i)$ and $A^c \neq \emptyset$ and that the vector $\mathbf{y} \in \mathbb{F}_q^{1+|A^c|}$ defined by $\pi_i(\mathbf{y}) = 1$, $\pi_{A^c}(\mathbf{y}) = \mathbf{0}$ is not in $\pi_{\{i\}\cup A^c}(C^\perp)$. Hence $\pi_{\{i\}\cup A^c}(C^\perp) \neq \mathbb{F}_q^{1+|A^c|}$. Therefore, the space $(\pi_{\{i\}\cup A^c}(C^\perp))^\perp$ must contain a vector $\mathbf{x} \neq \mathbf{0}$, such that $< \mathbf{x}, \mathbf{y} >\neq 0$. Consequently $\pi_i(\mathbf{x}) \neq 0$. We may assume without of loss of generality, $\pi_i(\mathbf{x}) = 1$. Define now the element $\mathbf{c} \in \mathbb{F}_q^{n(C)+1}$ given by $\pi_A(\mathbf{c}) = \mathbf{0}$ and $\pi_{\{i\}\cup A^c}(\mathbf{c}) = \mathbf{x}$. This element $\mathbf{c}$ is clearly in $(C^\perp)^\perp = C$ and $\pi_i(\mathbf{c}) = 1$, $\pi_A(\mathbf{c}) = \mathbf{0}$. So by definition, $A \in \mathcal{A}(C,i)$.

2) First, note that if $A = \mathcal{P}(C,i)$ then $A \in \Gamma(C,i)$ and $A^c = \emptyset \notin \Gamma(C^\perp, i)$ (Lemma 4.12). Now, for all $A \neq \mathcal{P}(C,i)$, we have that $A \in \Gamma(C,i)$ holds if and only if there exists $\mathbf{c} \in (C^\perp)_{i,1}$ with supp $\mathbf{c} \subseteq A \cup \{i\}$ (by definition). But this happens if and only if there exists $\mathbf{c} \in (C^\perp)_{i,1}$ with $\pi_{A^c}(\mathbf{c}) = \mathbf{0}$ which is equivalent by definition to $A^c \in \mathcal{A}(C^\perp, i)$. Finally, by the first part of the theorem this is equivalent to $A^c \notin \Gamma(C^\perp, i)$. △

DEFINITION 4.15 *Let* $C \in \mathcal{C}(\mathbb{F}_q), i \in I(C)$. *The* reconstruction threshold $r(C,i)$ *is*

$$r(C,i) := \min\{r \in \{0,\ldots,n(C)\} : A \in \Gamma(C,i)\ \forall A \subseteq \mathcal{P}(C,i)\ \textit{with}\ |A| = r\}.$$

The privacy threshold $t(C,i)$ *is*

$$t(C,i) := \max\{t \in \{0,\ldots,n(C)\} : B \in \mathcal{A}(C,i)\ \forall B \subseteq \mathcal{P}(C,i)\ \textit{with}\ |B| = t\}.$$

Note that, on account of Lemma 4.12, these thresholds are well defined and $1 \leq r(C,i) \leq n(C)$ and $0 \leq t(C,i) \leq n(C) - 1$ for all $C \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(C)$. Also, due to Lemma 4.13, $\forall r' \in \mathbb{Z}$ with $r(C,i) \leq r' \leq n(C)$ and any $A' \subseteq \mathcal{P}(C,i)$ with $|A'| = r'$, we have $A' \in \Gamma(C,i)$; and $\forall t' \in \mathbb{Z}$ with $0 \leq t' \leq t(C,i)$ and any $B' \subseteq \mathcal{P}(C,i)$ with $|B'| = t'$, we have $B' \in \mathcal{A}(C,i)$.

As a consequence of Theorem 4.14 we can state

PROPOSITION 4.16 *Let $C \in \mathcal{C}(\mathbb{F}_q)$, $i \in I(C)$. Then $r(C,i) > t(C,i)$ and $t(C^\perp, i) = n(C) - r(C,i)$.*

We can characterize $r(C,i)$ and $t(C,i)$ in terms of $w_i(C)$ and $w_i^\perp(C)$:

PROPOSITION 4.17 *Let $C \in \mathcal{C}(\mathbb{F}_q)$, $i \in I(C)$. Then*

$$r(C,i) = n(C) - w_i(C) + 2.$$

PROOF. By definition of the weight $w_i(C)$, every word $\mathbf{w} \in C_{i,1}$ has at most $n(C) - w_i(C) + 1$ zeros and there exists $\mathbf{w}' \in C_{i,1}$ with exactly that number of zeros. These two facts imply that $n(C) - w_i(C) + 2$ is the smallest integer r for which every $\mathbf{w} \in C_{i,1}$ has strictly fewer than r zeros. Therefore $n(C) - w_i(C) + 2$ is the smallest integer r such that for all $A \subseteq \mathcal{P}(C,i)$ with $|A| = r$, we have that $A \notin \mathcal{A}(C,i)$, and consequently (by Theorem 4.14) $A \in \Gamma(C,i)$. △

PROPOSITION 4.18 *Let $C \in \mathcal{C}(\mathbb{F}_q)$, $i \in I(C)$. Then $t(C,i) = w_i(C^\perp) - 2$.*

PROOF. By Proposition 4.16, $t(C,i) = n(C) - r(C^\perp, i)$. Applying Proposition 4.17 to $C^\perp$, $t(C,i) = w_i(C^\perp) - 2$. △

We state now some consequences of these two propositions. First, using Proposition 4.18, we can bound the dimension of the code.

PROPOSITION 4.19 *Let $C \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(C)$. We have*

$$\dim C \geq w_i^\perp(C) - 1 = t(C,i) + 1 \text{ and } d(C) \leq w_i(C).$$

PROOF. By definition of $t(C,i)$, there is a set $A \subseteq \mathcal{P}(C,i)$ of size $|A| = t(C,i) + 1$ such that $A \notin \mathcal{A}(C,i)$. However for any index $j \in A$, we have $|A \setminus \{j\}| = t(C,i)$, so $A \setminus \{j\} \in \mathcal{A}(C,i)$. By definition of $\mathcal{A}(C,i)$ there exists $\mathbf{c}_j \in C_{i,1}$ with $\pi_{A\setminus\{j\}}(\mathbf{c}_j) = \mathbf{0}$ but there does *not* exist any word $\mathbf{w} \in C_{i,1}$ with $\pi_A(\mathbf{w}) = \mathbf{0}$. Therefore $\pi_j(\mathbf{c}_j) \neq 0$. Then the set $\{\mathbf{c}_j : j \in A\}$ is clearly a set of linearly independent words in C and contains $t(C,i) + 1$ words, so $\dim C \geq t(C,i) + 1$. The second claim is trivial, since $w_i(C) > 0$. △

The following result states that given any linear code C over $\mathbb{F}_q$ an any index $i \in \mathcal{I}(C)$, $w_i(C)$ and $w_i^\perp(C)$ cannot be very large simultaneously.

PROPOSITION 4.20 *Let C be a linear code over $\mathbb{F}_q$, $i \in \mathcal{I}(C)$. Then*

$$w_i(C) + w_i^{\perp}(C) \leq n(C) + 3$$

PROOF. If $w_i^{\perp}(C) = 0$ or $w_i^{\perp}(C) = 1$, then

$$w_i(C) + w_i^{\perp}(C) = 1 \leq n(C) + 3.$$

So suppose $w_i(C) \geq 2$, i.e., $C \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(C)$. Then Propositions 4.16, 4.17 and 4.18 imply that

$$w_i^{\perp}(C) - 2 = t(C,i) < r(C,i) = n(C) - w_i(C) + 2.$$

Hence $w_i(C) + w_i^{\perp}(C) < n(C) + 4$. △

In Chapter 7, new limitations to $w_i(C)$ and $w_i^{\perp}(C)$ will be obtained not only in terms of $\mathfrak{k}(C)$ but also of the cardinality of the field $\mathbb{F}_q$ over which C is defined. This is analogous to what happens for the upper bounds on the distance and dimension of a linear code. The Singleton bound gives an upper bound for the sum of these two parameters that depends on the length of the code, while more elaborated bounds like Hamming and Plotkin bounds also take into account the size of the underlying field.

4.2 A coding view on ideal linear secret sharing

The possibility to obtain secret sharing schemes from linear codes was first proposed by J. Massey in [56]. We recall this construction next.

DEFINITION 4.21 *Let $C \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(C)$. The secret sharing scheme $\Sigma(C,i)$, defined on the set of players $\mathcal{P}(C,i)$, consists of the random variables S_i, the secret, and $(S_j)_{j \in \mathcal{P}(C,i)}$, the vector of shares, where each variable S_k, $k \in \mathcal{I}(C)$ takes the value $\pi_k(\mathbf{c})$ where $\mathbf{c}$ is selected uniformly at random in C.*

We use the notations introduced in Chapter 3. For $A \subseteq \mathcal{I}(C)$, S_A denotes the random variable $S_A = \prod_{i \in A} S_i$. S denotes the variable $S_{\mathcal{I}(C)}$.

We now prove that $\Sigma(C,i)$ is indeed a linear secret sharing scheme and state some properties of the scheme.

THEOREM 4.22 *Let $C \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(C)$. We have:*

1. *$\Sigma(C,i)$ is a linear secret sharing scheme.*
2. *$\Gamma(\Sigma(C,i)) = \Gamma(C,i)$ and $\mathcal{A}(\Sigma(C,i)) = \mathcal{A}(C,i)$.*
3. *$\Sigma(C,i)$ is perfect, and pseudoideal. Moreover, if $I(C) = \mathcal{I}(C)$ it is ideal.*
4. $$r(\Sigma(C,i)) = n(C) - w_i(C) + 2 \leq n(C) - d(C) + 2$$
   and
   $$t(\Sigma(C,i)) = w_i^{\perp}(C) - 2 \geq d(C^{\perp}) - 2.$$

PROOF.

1) We first need to verify the two properties required in the definition of secret sharing scheme (Definition 3.7): First, $H(S_i) \neq 0$ because $w_i(C) > 0$ implies that $\pi_i(C) = \mathbb{F}_q$. On the other hand $H(S_i|S_{\mathcal{P}(C,i)}) = 0$ is proved as follows. Since $w_i(C^{\perp}) > 1$, there exists a word $\mathbf{c}^* \in C^{\perp}$ with $\pi_i(\mathbf{c}^*) = 1$. Fix one such word $\mathbf{c}^*$. Then for any $\mathbf{c} \in C$,

$$0 =< \mathbf{c}, \mathbf{c}^* >= \pi_i(\mathbf{c})\pi_i(\mathbf{c}^*) + < \pi_{\mathcal{P}(C,i)}(\mathbf{c}), \pi_{\mathcal{P}(C,i)}(\mathbf{c}^*) > .$$

This implies $\pi_i(\mathbf{c}) = - < \pi_{\mathcal{P}(C,i)}(\mathbf{c}), \pi_{\mathcal{P}(C,i)}(\mathbf{c}^*) >$. So the value $\pi_i(\mathbf{c})$ is determined by $\pi_{\mathcal{P}(C,i)}(\mathbf{c})$.
The linearity is obvious since for all $j \in \mathcal{I}(C)$, we have supp $S_j = \pi_j(C)$ and either $\pi_j(C) = \mathbb{F}_q$ (if $w_j(C) > 0$) or $\pi_j(C) = 0$ (if $w_j(C) = 0$). Furthermore supp $S = C$ (which is a vector space over $\mathbb{F}_q$) and the distribution of S is the uniform on C.

2) Assume $A \in \Gamma(C,i)$. Then there exists a word $\mathbf{c} \in (C^{\perp})_{i,1}$ with supp $\mathbf{c} \subseteq A \cup \{i\}$. Hence for any word $\mathbf{w} \in C$, we have

$$0 =< \mathbf{c}, \mathbf{w} >= \pi_i(\mathbf{c})\pi_i(\mathbf{w}) + < \pi_A(\mathbf{c}), \pi_A(\mathbf{w}) >$$

and since $\pi_i(\mathbf{c}) = 1$, it holds that $\pi_i(\mathbf{w}) = - < \pi_A(\mathbf{c}), \pi_A(\mathbf{w}) >$. Hence the function

$$\rho_A : \mathbb{F}_q^{|A|} \to \mathbb{F}_q$$
$$\mathbf{x} \mapsto - < \pi_A(\mathbf{c}), \mathbf{x} >$$

satisfies $\pi_i(\mathbf{w}) = \rho_A(\pi_A(\mathbf{w}))$ for every word $\mathbf{w} \in C$. Therefore the value of $\pi_i(\mathbf{w})$ is uniquely determined by $\pi_A(\mathbf{w})$ for all $\mathbf{w} \in C$. Consequently

the value of S_i is determined by the value of S_A. So $A \in \Gamma(\Sigma(C,i))$ and $\Gamma(C,i) \subseteq \Gamma(\Sigma(C,i))$.

On the other hand if $A \in \mathcal{A}(C,i)$, either $A = \emptyset \in \mathcal{A}(\Sigma(C,i))$ (see Definition 3.10) or $A \neq \emptyset$. In the latter case there exists a word $\mathbf{c} \in C_{i,1}$ with $\pi_A(\mathbf{c}) = \mathbf{0}$. Then for any $\mathbf{y} \in \pi_A(C)$, and any two elements $x, x' \in \mathbb{F}_q$, we have that $|C_{i,x} \cap C_{A,\mathbf{y}}| = |C_{i,x'} \cap C_{A,\mathbf{y}}|$ since the map

$$\phi : C_{i,x} \cap C_{A,\mathbf{y}} \to C_{i,x'} \cap C_{A,\mathbf{y}}$$

$$\mathbf{w} \mapsto \mathbf{w} + (x' - x)\mathbf{c}$$

is a bijection. This means that

$$P(S_i = x | S_A = \mathbf{y}) = P(S_i = x' | S_A = \mathbf{y}) = |C_{i,x'} \cap C_{A,\mathbf{y}}|/|C_{A,\mathbf{y}}|.$$

Therefore the variable $S_i|S_A = \mathbf{y}$ has the uniform distribution over $\mathbb{F}_q$ for any $\mathbf{y} \in \pi_A(C)$. Since S_i also has the uniform distribution over $\mathbb{F}_q$, we conclude that $H(S_i|S_A) = H(S_i)$ and therefore $A \in \mathcal{A}(\Sigma(C,i))$. Hence $\mathcal{A}(C,i) \subseteq \mathcal{A}(\Sigma(C,i))$.
Recall that $\Gamma(C,i) \amalg \mathcal{A}(C,i) = 2^{\mathcal{P}(C,i)}$ (Theorem 4.14). Since we have proved that $\Gamma(C,i) \subseteq \Gamma(\Sigma(C,i))$ and $\mathcal{A}(C,i) \subseteq \mathcal{A}(\Sigma(C,i))$ and we know $\Gamma(\Sigma(C,i)) \cap \mathcal{A}(\Sigma(C,i)) = \emptyset$ by Proposition 3.12, the only possibility is that $\Gamma(\Sigma(C,i)) = \Gamma(C,i)$ and $\mathcal{A}(\Sigma(C,i)) = \mathcal{A}(C,i)$.
We can now combine 2) with the results proved for $\Gamma(C,i)$ and $\mathcal{A}(C,i)$ in the previous section in order to prove the remaining claims.

3) By Theorem 4.14, we have $2^{\mathcal{P}(C,i)} = \Gamma(\Sigma(C,i)) \amalg \mathcal{A}(\Sigma(C,i))$, and therefore $\Sigma(C,i)$ is perfect. Once we have established that, we can prove it is pseudoideal. Note that S_i has the uniform distribution in $\mathbb{F}_q$ and for $j \in \mathcal{P}(C,i)$, S_j has the uniform distribution in $\mathbb{F}_q$ if $w_j(C) > 0$ and is identically zero if $w_j(C) = 0$. In the first case $H(S_i) = H(S_j) = \log q$ and in the second case j is clearly a dummy index. But this second case cannot happen when $\mathcal{I}(C) = I(C)$.

4) From the Definitions 3.13, 3.14 and 4.15, and again property 2), we deduce $r(\Sigma(C,i)) = r(C,i)$ and $t(\Sigma(C,i)) = t(C,i)$. We can then apply Propositions 4.17, 4.18 and 4.19 to obtain

$$r(\Sigma(C,i)) = n(C) - w_i(C) + 2 \leq n(C) - d(C) + 2$$

and

$$t(\Sigma(C,i)) = w_i^{\perp}(C) - 2 \geq d(C^{\perp}) - 2.$$

△

4.3 Capturing strong multiplication

Our goal now is to study t-strong multiplication of ideal linear secret sharing schemes using the coding theoretic framework explained in this chapter.

4.3.1 Schur-product transforms of codes

We introduce the notion of Schur-product transforms of a linear code C. Recall that $\mathbf{x} * \mathbf{y}$ denotes the Schur product of two vectors $\mathbf{x}$ and $\mathbf{y}$ (Definition 3.27).

DEFINITION 4.23 *Given a generalized $\mathbb{F}_q$-linear code C, the* k-th order Schur-product transform *of C is the generalized $\mathbb{F}_q$-linear code*

$$C^{\circledast k} := \mathbb{F}_q < \{\mathbf{x}_1 * \cdots * \mathbf{x}_k : \mathbf{x}_1, \ldots, \mathbf{x}_k \in C\} >$$

where for a set $S \subseteq \mathbb{F}_q^r$, for some integer $r > 0$, $\mathbb{F}_q < S >$ denotes the $\mathbb{F}_q$-vector space spanned by the elements of the set S. We write $\widehat{C} := C^{\circledast 2}$ and call this code Schur square *of C.*

In this thesis, we will be mostly concerned about the Schur squares of given codes. We can state some basic properties about $\widehat{C}$ for codes $C \in \mathcal{C}(\mathbb{F}_q)$.

PROPOSITION 4.24 *Let $C \in \mathcal{C}(\mathbb{F}_q)$. Then:*

1. $n(C) = n(\widehat{C})$.
2. $\forall i \in \mathcal{I}(C)$, $w_i(\widehat{C}) \leq w_i(C)$ *(and consequently $d(\widehat{C}) \leq d(C)$).*
3. $\forall i \in \mathcal{I}(C)$, $w_i(C) > 0 \Leftrightarrow w_i(\widehat{C}) > 0$.
4. $I(\widehat{C}) \subseteq I(C)$. *In fact, it may happen that $I(\widehat{C}) = \emptyset$.*

PROOF. Claim 1 is obvious. For Claim 2, assume first that $w_i(C) > 0$. Note that for all $\mathbf{c} \in C_{i,1}$, $\mathbf{c} * \mathbf{c} \in (\widehat{C})_{i,1}$. Then the claim is a consequence of $w_{Ham}(\mathbf{c}) = w_{Ham}(\mathbf{c} * \mathbf{c})$. If $w_i(C) = 0$, every word in C is in $C_{i,0}$ and therefore every word in $\widehat{C}$ is in $(\widehat{C})_{i,0}$ so $w_i(\widehat{C}) = 0$. This completes the proof of Claim 2 and proves one implication in Claim 3. The other implication is again a consequence of the fact that for all $\mathbf{c} \in C_{i,1}$, we have $\mathbf{c} * \mathbf{c} \in (\widehat{C})_{i,1}$. The claim $I(\widehat{C}) \subseteq I(C)$ is then a consequence of the previous ones. An example of a code $C \in \mathcal{C}(\mathbb{F}_2)$ where $I(\widehat{C}) = \emptyset$ is the following: Take

$$C = \mathbb{F}_2 < (1,1,0,0), (1,0,1,0), (0,1,0,1) > .$$

It is easy to check that $C \in \mathcal{C}(\mathbb{F}_2)$, in fact $I(C) = \mathcal{I}(C)$. However $\widehat{C} = \mathbb{F}_2^4$, so $w_i(\widehat{C}) = 1$ for all $i \in \mathcal{I}(\widehat{C})$ and $I(\widehat{C}) = \emptyset$. △

4.3.2 The class $\mathcal{C}^\dagger(\mathbb{F}_q)$

We define now the following class of linear codes over $\mathbb{F}_q$.

DEFINITION 4.25 *$\mathcal{C}^\dagger(\mathbb{F}_q)$ denotes the set of all linear codes C over $\mathbb{F}_q$ such that $I(\widehat{C}) \neq \emptyset$.*

REMARK 4.26 *$\mathcal{C}^\dagger(\mathbb{F}_q) \subseteq \mathcal{C}(\mathbb{F}_q)$ because $I(\widehat{C}) \subseteq I(C)$ for any $C \in \mathcal{C}(\mathbb{F}_q)$.*

We might wonder at this point if codes in $\mathcal{C}^\dagger(\mathbb{F}_q)$ are rare. In the proof of Proposition 4.24 we gave an example of a code in $\mathcal{C}(\mathbb{F}_2) \setminus \mathcal{C}^\dagger(\mathbb{F}_2)$. However, a large class of codes studied in the literature, self-orthogonal codes, can be seen to be in $\mathcal{C}^\dagger(\mathbb{F}_q)$.

PROPOSITION 4.27 *Let $\{\mathbf{0}\} \neq C$ be a self-orthogonal linear code over $\mathbb{F}_q$. Then $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$.*

PROOF. Let $\mathbf{0} \neq \mathbf{c} \in C$. Take any $i \in \text{supp } \mathbf{c}$. Without loss of generality, we may assume $\pi_i(\mathbf{c}) = 1$. Then $i \in I(\widehat{C})$ is proved as follows. First, $w_i(\widehat{C}) > 0$ because $\mathbf{c} * \mathbf{c} \in \widehat{C}$ and $\pi_i(\mathbf{c} * \mathbf{c}) = 1$. On the other hand, for all $\mathbf{w}, \mathbf{w}' \in C$, $< \mathbf{w}, \mathbf{w}' >= 0$ because C is self-orthogonal. This is equivalent to $< (1,1,\ldots,1), \mathbf{w} * \mathbf{w}' >= 0$ for all $\mathbf{w}, \mathbf{w}' \in C$ and, by linearity, $(1,1,\ldots,1) \in (\widehat{C})^\perp$ so $w_i^\perp(\widehat{C}) \neq 0$ and this implies $w_i(\widehat{C}) \neq 1$. In fact, it has been proved that if C is self-orthogonal, $w_i(C) > 0$ implies $i \in I(\widehat{C})$. △

4.3.3 Corruption tolerance of a code

We define now, for every code in $\mathcal{C}^\dagger(\mathbb{F}_q)$, two parameters that, as we will later prove, give information about strong multiplication of a LSSS defined from C.

DEFINITION 4.28 *For $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$, we define:*

$$\widehat{t}(C) := \max_{i \in I(\widehat{C})} \min\{w_i^\perp(C) - 2, w_i(\widehat{C}) - 2\}.$$

The LSSS $\Sigma(C)$ is by definition $\Sigma(C, i)$ where i is chosen as the smallest index where this maximum is attained. This index is denoted i_s.

We introduce now the notion of corruption tolerance of a code, which is a relative measure of $\widehat{t}(C)$ against $n(C)$.

DEFINITION 4.29 (CORRUPTION TOLERANCE) *Let $\mathbb{F}_q$ be a finite field. The* corruption tolerance *of $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$, is the real number*

$$\widehat{\tau}(C) := \frac{3\widehat{t}(C)}{n(C) - 1}.$$

4.3.4 Strong multiplication as a code property

Recall that $\widehat{\Gamma}(\Sigma(C, i))$ denotes the family of subsets of $\mathcal{I}(C)\backslash\{i\}$ with product reconstruction (Definition 3.32). We have:

THEOREM 4.30 *Let $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ and $i \in I(\widehat{C})$, such that $w_i^\perp(C) \geq 3$. Then* $\Gamma(\widehat{C}, i) \subseteq \widehat{\Gamma}(\Sigma(C, i))$

PROOF. First note that $w_i^\perp(C) \geq 3$ implies $t(\Sigma(C, i)) \geq 1$. Therefore $\widehat{\Gamma}(\Sigma(C, i))$ is well defined.

Let $A \in \Gamma(\widehat{C}, i)$. We need to prove that there exists a function $\Psi_A : \mathbb{F}_q^{|A|} \to \mathbb{F}_q$ such that for any two words $\mathbf{c}, \mathbf{c}' \in C$,

$$\pi_i(\mathbf{c})\pi_i(\mathbf{c}') = \Psi_A((\pi_j(\mathbf{c})\pi_j(\mathbf{c}'))_{j \in A}).$$

But note that if $A \in \Gamma(\widehat{C}, i) = \Gamma(\Sigma(\widehat{C}, i))$, there exists a function $\rho_A : \mathbb{F}_q^{|A|} \to \mathbb{F}_q$ with

$$\pi_i(\mathbf{w}) = \rho_A(\pi_A(\mathbf{w}))$$

for all $\mathbf{w} \in \widehat{C}$ and in particular any word of the form $\mathbf{w} = \mathbf{c} * \mathbf{c}'$ for $\mathbf{c}, \mathbf{c}' \in C$. For all $j \in \mathcal{I}(C)$, $\pi_j(\mathbf{c} * \mathbf{c}') = \pi_j(\mathbf{c})\pi_j(\mathbf{c}')$ so we can take $\Psi_A = \rho_A$ and the theorem is proved. △

As a consequence of this proposition, the codes in $\mathcal{C}^\dagger(\mathbb{F}_q)$ give rise to linear secret sharing schemes with multiplication, if these schemes have at least 1-privacy.

COROLLARY 4.31 *Let $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$. Assume there exists $i \in I(\widehat{C})$ such that $w_i^\perp(C) \geq 3$ and let t be an integer such that $1 \leq t \leq w_i^\perp(C) - 2$. Then $\Sigma(C, i)$ has t-multiplication (i.e. $t(\Sigma(C, i)) \geq t$ and $\mathcal{P}(C, i) \in \widehat{\Gamma}(\Sigma(C, i))$.*

PROOF. First, we have $t(\Sigma(C, i)) = w_i^\perp(C) - 2 \geq t \geq 1$ by Proposition 4.18 and Theorem 4.22. Now note that $\mathcal{P}(C, i) = \mathcal{P}(\widehat{C}, i)$. Since $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ we have that $\widehat{C} \in \mathcal{C}(\mathbb{F}_q)$ and by Lemma 4.12, $\mathcal{P}(\widehat{C}, i) \in \Gamma(\widehat{C}, i)$. Finally Theorem 4.30 implies the result. △

Now we state the main result of this section: we show the relationship between the parameter $\widehat{t}(C)$ and the *strong* multiplication of the LSSS $\Sigma(C)$ (see Definition 4.28).

THEOREM 4.32 *Let $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$. Assume $\widehat{t}(C) \geq 1$ and let t be an integer with $1 \leq t \leq \widehat{t}(C)$. Then $\Sigma(C)$ has t-strong multiplication.*

PROOF. It has been proved (Proposition 4.18 and Theorem 4.22) that

$$t(\Sigma(C)) = t(C, i_s) = w_{i_s}^\perp(C) - 2 \geq t.$$

On the other hand, since $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ and $i_s \in I(\widehat{C})$, applying Proposition 4.17 we have that $r(\widehat{C}, i_s) = n(C) - w_{i_s}(\widehat{C}) + 2 \leq n(C) - t$ so any $A \subseteq \mathcal{P}(C, i_s)$ with $|A| = n(C) - t$ belongs to $\Gamma(\widehat{C}, i_s)$. Moreover, by Theorem 4.30, any such set A belongs to $\widehat{\Gamma}(\Sigma(C, i_s))$. This proves the property. △

In particular $\widehat{t}(C)$ is a lower bound for $t(\Sigma(C))$. But, interestingly, we can also obtain an upper bound for $r(\Sigma(C))$ in terms of $\widehat{t}(C)$.

PROPOSITION 4.33 *Let $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ and assume $\widehat{t}(C) \geq 1$. Then*

$$r(C, i_s) \leq n(C) - 2\widehat{t}(C)$$

(and consequently $r(\Sigma(C)) \leq n(C) - 2\widehat{t}(C)$).

PROOF. Write $\widehat{t}(C) = t$. Assume $r(C, i_s) \geq n(C) - 2t + 1$. Then, by definition of $r(C, i_s)$ (see Definition 4.15) there exists a set $A \subseteq \mathcal{P}(C, i_s)$ with $|A| = n(C) - 2t$ such that $A \notin \Gamma(C, i_s)$ and consequently (by Theorem 4.14) $A \in \mathcal{A}(C, i_s)$. By definition there is a word $\mathbf{c}_A \in C_{i_s,1}$ with $\pi_A(\mathbf{c}_A) = \mathbf{0}$.
Now take any set $B \subseteq \mathcal{I}(C) \setminus \{i_s\}$ with $|B| = t$, $A \cap B = \emptyset$. Then $t \leq \widehat{t}(C)$ implies $w_{i_s}^{\perp}(C) \geq t + 2$ and by Proposition 4.18 $B \in \mathcal{A}(C, i_s)$. Then there exists a word $\mathbf{c}_B \in C_{i_s,1}$ with $\pi_B(\mathbf{c}_B) = \mathbf{0}$.
The Schur product $\mathbf{c} = \mathbf{c}_A * \mathbf{c}_B \in \widehat{C}_{i_s,1}$ satisfies $\pi_{A \cup B}(\mathbf{c}) = \mathbf{0}$. But, since $|A \cup B| = n(C) - t$, we know $w_{Ham}(\mathbf{c}) \leq t + 1$. Therefore $w_{i_s}(\widehat{C}) \leq t + 1$ and consequently by Definition 4.28, $\widehat{t}(C) \leq t - 1$, which is a contradiction. △

This implies the following bound for $\widehat{t}(C)$.

COROLLARY 4.34 *Let $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$. Then $3\widehat{t}(C) \leq n(C) - r(C, i_s) + t(C, i_s)$ and in fact $3\widehat{t}(C) \leq n(C) - 1$.*

PROOF. We have proved that $t(C, i_s) \geq \widehat{t}(C)$ and $r(C, i_s) \leq n(C) - 2\widehat{t}(C)$. This implies that $3\widehat{t}(C) \leq n(C) - r(C, i_s) + t(C, i_s)$. But $r(C, i_s) \geq t(C, i_s) + 1$ (Proposition 4.16) and this leads to the result. △

We can now give bounds on the corruption tolerance of any code.

PROPOSITION 4.35 *For all $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$, $0 \leq \widehat{\tau}(C) \leq 1$. If $\widehat{\tau}(C) = 1$, then $\Sigma(C)$ is a threshold LSSS and $t(\Sigma(C)) = \widehat{t}(C)$.*

PROOF. Since $\widehat{t}(C) \geq 0$, $\widehat{\tau}(C) \geq 0$. From $3\widehat{t}(C) \leq n(C) - 1$ (Corollary 4.34) it is straightforward that $\widehat{\tau}(C) \leq 1$.

Assume now $\widehat{\tau}(C) = 1$. Then $3\widehat{t}(C) = n(C) - 1$. But in fact Corollary 4.34 also states $3\widehat{t}(C) \leq n(C) - r(C, i_s) + t(C, i_s)$ so $3\widehat{t}(C) = n(C) - 1$ only happens in the case $r(C, i_s) = t(C, i_s) + 1$. This means that $\Sigma(C)$ is a threshold LSSS.

In addition, by Proposition 4.33, $r(C, i_s) \leq n(C) - 2\widehat{t}(C)$, so

$$t(C, i_s) \leq n(C) - 2\widehat{t}(C) - 1 = \frac{n(C) - 1}{3}.$$

On the other hand, by Proposition 4.18,

$$t(C, i_s) = w_{i_s}^{\perp}(C) - 2 \geq \widehat{t}(C) = \frac{n(C) - 1}{3}.$$

Consequently

$$t(\Sigma(C)) = t(C, i_s) = \frac{n(C) - 1}{3} = \widehat{t}(C).$$

△

The last part of the theorem motivates the analysis of threshold LSSS, that we will carry on in the next section.

As an aside, we remark an interesting *error correcting* property of linear secret sharing schemes with t-strong multiplication.

Let $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ be such that $\widehat{t}(C) \geq t \geq 1$ and assume without loss of generality that $i_s = 0$. Write $n = n(C)$. Note first that

PROPOSITION 4.36 *Let* $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$. *Assume there exist*

$$\mathbf{c} = (s, c_1, c_2, \ldots, c_n) \text{ and } \mathbf{c}' = (s', c_1', c_2', \ldots, c_n') \in C$$

with

$$d((c_1, c_2, \ldots, c_n), \mathbf{x}) \leq t \text{ and } d((c_1', c_2', \ldots, c_n'), \mathbf{x}) \leq t.$$

Then $s = s'$.

PROOF. Note that $w_{Ham}(\mathbf{c} - \mathbf{c}') \leq 2t + 1$. But since we have proved in Proposition 4.33 that $r(C, 0) \leq n - 2\widehat{t}(C)$, then $w_0(C) \geq 2t + 2$, so $\mathbf{c} - \mathbf{c}'$ belongs to $C_{i,0}$ and therefore $s = s'$.

Note however that $\mathbf{c}$ and $\mathbf{c}'$ can be different, as long as their 0-th coordinate is the same. △

Therefore, the LSSS $\Sigma(C, 0)$ has the property that if a secret s is shared using this scheme, the full vector of n shares determines the secret even if t of these shares are corrupted.

Furthermore, Cramer et al. showed in [28] that under the conditions above, the secret s can be efficiently reconstructed.

THEOREM 4.37 *There exists an efficient algorithm that takes as input a vector* $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ *such that there is a word* $\mathbf{c} = (s, c_1, c_2, \ldots, c_n) \in C$ *with* $d((c_1, c_2, \ldots, c_n), (x_1, x_2, \ldots, x_n)) \leq t$ *and outputs the only* s *satisfying this property.*

The recovery algorithm can be seen as a generalization of the well known Berlekamp-Welch error-correcting algorithm for Reed-Solomon codes and also bears some similarity with the error correcting algorithm proposed by Pellikaan in [64].

4.4 Limitations of threshold schemes

It is a known fact, already proved in [50] (see also [13]), that MDS codes and threshold LSSS are equivalent. We now give an alternative proof of this fact and at the same time characterize the dimension and distance of these codes in terms of the minimal weights at the indices of the codes.

PROPOSITION 4.38 *Let C be a linear code over $\mathbb{F}_q$. The following are equivalent*

1. $w_i(C) + w_i^\perp(C) = n(C) + 3$ *for* some $i \in \mathcal{I}(C)$.
2. *C is an MDS code with $C \neq \{\mathbf{0}\}, \mathbb{F}_q^{\ell(C)}$.*
3. $w_i(C) + w_i^\perp(C) = n(C) + 3$ *for* all $i \in \mathcal{I}(C)$.
4. *For* some $i \in I(C)$, $\Sigma(C,i)$ *is a threshold LSSS.*
5. $\mathcal{I}(C) = I(C)$ *and for* all $i \in I(C)$, $\Sigma(C,i)$ *is a threshold LSSS.*

If these conditions hold, then for all $i \in \mathcal{I}(C)$, we have $\dim C = w_i^\perp(C) - 1$, $d(C) = w_i(C)$ *and* $d(C^\perp) = w_i^\perp(C)$.

PROOF. We will show the implications 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1), 1) $\iff$ 4) and 3) $\iff$ 5).

1) $\Rightarrow$ 2): Take an index $i \in \mathcal{I}(C)$ satisfying

$$w_i(C) + w_i^\perp(C) = n(C) + 3.$$

Note that $w_i(C) > 1$ and $w_i^\perp(C) > 1$ since otherwise $w_i(C) + w_i^\perp(C) = 1$ (by Lemma 4.7). Let $t = t(C,i)$ and $r = r(C,i)$. Now $w_i(C) + w_i^\perp(C) = n(C) + 3$ implies $r - t = 1$ by Propositions 4.17 and 4.18. By definition of t, for all $A \subseteq \mathcal{P}(C,i)$ with $|A| = t$, there exists $\mathbf{c}_A \in C_{i,1}$ with $\pi_A(\mathbf{c}_A) = \mathbf{0}$. But since $r = t + 1$ this word cannot have $t + 1$ zeros, that is $\pi_j(\mathbf{c}_A) \neq 0$ for $j \notin A$. Hence all the $\mathbf{c}_A$, $|A| = t$ are different.

Then $d(C) = w_i(C)$ because of the following: By Proposition 4.19, $d(C) \leq w_i(C)$. Now suppose $d(C) < w_i(C)$. There exists $\mathbf{0} \neq \mathbf{w} \in C$ such that its weight is $w_{Ham}(\mathbf{w}) = d(C)$. Note that $\pi_i(\mathbf{w}) = 0$ (otherwise we have $w_i(C) = d(C)$). Applying Proposition 4.18 we have

$$d(C) + t < w_i(C) + w_i(C^\perp) - 2 = n(C) + 1$$

and therefore we can select a set $B \subseteq \mathcal{P}(C,i)$ with $B \cap \operatorname{supp} \mathbf{w} = \emptyset$ and $|B| = t$. We take the word $\mathbf{c}_B \in C_{i,1}$ as defined above, which has zeros exactly in B. Note that $\operatorname{supp} \mathbf{w} \subseteq \operatorname{supp} \mathbf{c}_B$. Now the existence of $\mathbf{w}$ and $\mathbf{c}_B$ implies that there is a word $\mathbf{c}' \in C_{i,1}$ of weight smaller than $w_i(C)$, which is constructed as follows: Take an index $j \in \operatorname{supp} \mathbf{w} \subseteq \operatorname{supp} \mathbf{c}_B$. Take

$$\lambda = -\frac{\pi_j(\mathbf{c}_B)}{\pi_j(\mathbf{w})},$$

(clearly $\lambda \neq 0$) and let $\mathbf{c}' = \mathbf{c}_B + \lambda \mathbf{w}$. This word is in $C_{i,1}$ and, since $\pi_j(\mathbf{c}') = 0$, $\operatorname{supp} \mathbf{c}' \subseteq \operatorname{supp} \mathbf{c}_{B'} \setminus \{j\}$, so

$$w_H(\mathbf{c}') \leq w_i(C) - 1$$

which is a contradiction. Therefore $d(C) = w_i(C)$.

Hence by the previous and Proposition 4.19,

$$d(C) + \dim C \geq w_i(C) + (w_i^{\perp}(C) - 1) = \mathfrak{k}(C) + 1.$$

By Singleton's bound, $d(C) + \dim C = \mathfrak{k}(C) + 1$, so C is an MDS code and $\dim C = w_i^{\perp}(C) - 1$ in this case. The condition $w_i(C) > 0$ guarantees that $C \neq \{\mathbf{0}\}$ and $w_i^{\perp}(C) > 0$ ensures $C \neq \mathbb{F}_q^{\mathfrak{k}(C)}$.

2) $\Rightarrow$ 3): If C is an MDS code, $C^{\perp}$ is an MDS code. Therefore we have $d(C) + \dim C = \mathfrak{k}(C) + 1$ and $d(C^{\perp}) + \dim C^{\perp} = \mathfrak{k}(C) + 1$. In addition to this, $\dim C = \mathfrak{k}(C) - \dim C^{\perp}$. These three equations imply

$$d(C) + d(C^{\perp}) = \mathfrak{k}(C) + 2.$$

Take any index $i \in \mathcal{I}(C)$. If $w_i(C) = 0$, then $d(C^{\perp}) = 1$. Note that this would imply $\dim C^{\perp} = \mathfrak{k}(C)$ and $\dim C = 0$ by the fact that $C^{\perp}$ is MDS. Similarly, if $w_i^{\perp}(C) = 0$, $\dim C = \mathfrak{k}(C)$ so $C = \mathbb{F}_q^{\mathfrak{k}(C)}$.

Hence $w_i(C), w_i^{\perp}(C) \neq 0$ and therefore, $w_i(C) \geq d(C)$, $w_i^{\perp}(C) \geq d(C^{\perp})$ by Lemma 4.6. Therefore

$$w_i(C) + w_i^{\perp}(C) \geq d(C) + d(C^{\perp}) = \mathfrak{k}(C) + 2 = n(C) + 3$$

so $w_i(C) + w_i^{\perp}(C) = n(C) + 3$ by Proposition 4.20.

3) $\Rightarrow$ 1): Obvious.

1) $\iff$ 4): Note first that $w_i(C)+w_i^\perp(C) = n(C)+3$ for some $i \in \mathcal{I}(C)$ implies $i \in I(C)$. So assume $i \in I(C)$. Then, since $r(C,i) = n(C)-w_i(C)+2$ and $t(C,i) = w_i^\perp(C) - 2$ we have

$$\Sigma(C,i) \text{ is threshold } \iff r(C,i) = t(C,i)+1 \iff w_i(C)+w_i^\perp(C) = n(C)+3$$

3) $\iff$ 5): This is proved repeating the arguments of the proof of 1) $\iff$ 4) for all indices $i \in \mathcal{I}(C)$.

Note that in the proof of the implication 1) $\Rightarrow$ 2), it has been shown that if C satisfies the equivalent conditions of the statement, then for any index $i \in \mathcal{I}(C)$ we have $d(C) = w_i(C)$ and $\dim C = w_i^\perp(C) - 1$.

$\triangle$

Even though in the case of MDS codes we have $w_i(C) = d(C)$ and $w_i^\perp(C) = \dim C + 1$ for all $i \in \mathcal{I}(C)$, in general for an arbitrary code there may exist indices for which the bounds in Proposition 4.19 are far from sharp. An important example of the fact that a weight $w_i(C)$ may be far from the minimal distance $d(C)$ of the code will be given in Chapter 6. Note now that in the conditions above if $\dim C = 1$, then $w_i^\perp(C) = 2$ (and consequently $t(C,i) = 0$) and if $\dim C = \mathfrak{k}(C) - 1$, then $w_i(C) = 2$ and consequently $r(C,i) = n(C)$. Hence we have a very convenient characterization of *non-trivial* MDS codes (see Definition 1.15).

COROLLARY 4.39 *Let C be a linear code over $\mathbb{F}_q$. The following are equivalent*

1. *For some $i \in \mathcal{I}(C)$, $w_i(C) + w_i^\perp(C) = n(C) + 3$, and $w_i(C) \geq 3$, $w_i^\perp(C) \geq 3$.*
2. *C is a* non-trivial *MDS code.*
3. *For all $i \in \mathcal{I}(C)$, $w_i(C) + w_i^\perp(C) = n(C) + 3$, and $w_i(C) \geq 3$, $w_i^\perp(C) \geq 3$.*
4. *For some $i \in I(C)$, $\Sigma(C,i)$ is a threshold LSSS with $t(\Sigma(C,i)) \geq 1$, $r(\Sigma(C,i)) \leq n(C) - 1$.*
5. *$\mathcal{I}(C) = I(C)$ and for* all *$i \in I(C)$, $\Sigma(C,i)$ is a threshold LSSS with $t(\Sigma(C,i)) \geq 1$, $r(\Sigma(C,i)) \leq n(C) - 1$.*

The upper bound on the length of nontrivial MDS codes has important consequences to the existence of threshold LSSS. Indeed combining Theorem 1.19 and Corollary 4.39:

COROLLARY 4.40 *If $C \in \mathcal{C}(\mathbb{F}_q), i \in I(C)$ are such that $\Sigma(C,i)$ is a threshold LSSS with $t(\Sigma(C,i)) = t \geq 1$, $r(\Sigma(C,i)) = t+1 \leq n(C)-1$, then*

$$q \geq \max\{t+2, n(C)-t+1\}.$$

In particular $n(C) \leq 2q-3$.

However, note that for every finite field $\mathbb{F}_q$ and every integer $n > 1$, there exists $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $n(C) = n$ such that $\Sigma(C,i)$ is a threshold linear secret sharing scheme with $t(C,i) = 0$ for some $i \in \mathcal{I}(C)$. Indeed, take the code $C = \mathbb{F}_q < (1,1,\ldots,1) >\subseteq \mathbb{F}_q^{n+1}$. On the other hand, there also exists $C' \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $n(C') = n$ and such that $\Sigma(C',i)$ is threshold with $r(C',i) = n$ (and hence $t(C',i) = n-1$). For example, we can take the code $C' = \mathbb{F}_q < (1,1,\ldots,-1,\ldots,1) >^{\perp}$ (where the -1 is in the i-th position).

In Theorem 4.35, we proved that $\widehat{\tau}(C) = 1$ may only happen for codes $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ such that $\Sigma(C)$ is threshold. We can now use the results of this section to find new restrictions for the codes such that $\widehat{\tau}(C) = 1$.

THEOREM 4.41 *Let $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ and assume $\widehat{\tau}(C) = 1$. Then C is a nontrivial MDS code with $\dim C = \frac{n(C)-1}{3} + 1$.*

PROOF. By Proposition 4.35, $\widehat{\tau}(C) = 1$ implies $\Sigma(C)$ is a threshold scheme with $t(C,i_s) = t(\Sigma(C)) = \widehat{t}(C)$. But Proposition 4.38 ensures C is an MDS code and $\dim C = w_{i_s}^{\perp}(C) - 1$.

Since in addition $t(C,i_s) = w_{i_s}^{\perp}(C) - 2$ (by Proposition 4.18), we have

$$\dim C = w_{i_s}^{\perp}(C) - 1 = t(C,i_s) + 1 = \widehat{t}(C) + 1.$$

Now if $\widehat{\tau}(C) = 1$, we have $\widehat{t}(C) = \frac{n(C)-1}{3}$ and therefore $\dim C = \frac{n(C)-1}{3} + 1$. It is easy to check that C is then a nontrivial MDS code. $\triangle$

Therefore we know that $\widehat{\tau}(C) = 1$ can not happen for $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ of arbitrary length, due to the upper bounds for the length of nontrivial MDS codes over $\mathbb{F}_q$ (Theorem 1.19). More precisely,

COROLLARY 4.42 *Let $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $\widehat{\tau}(C) = 1$. Then $n(C) \leq \frac{3q-4}{2}$.*

PROOF. Theorem 1.19 states $q \geq \max\{\dim C + 1, \ell(C) - \dim C + 1\}$. Since $\dim C = \frac{n(C)-1}{3} + 1$, it is easy to check that $q \geq \frac{2n(C)+4}{3}$ and this in turn implies $n(C) \leq \frac{3q-4}{2}$. △

It is not true however that if C is a nontrivial MDS code then $\widehat{\tau}(C) = 1$. Note that in fact this cannot happen unless $\dim C = \frac{n(C)-1}{3} + 1$. Even if that is the case in principle we cannot ensure that $\widehat{\tau}(C) = 1$. However, for some finite fields, $\widehat{\tau}(C) = 1$ is achievable. In order to prove this, we first determine the corruption tolerance of Reed-Solomon codes.

THEOREM 4.43 *Let $\mathbb{F}_q$ be a finite field with $q > 2$, $t, n \in \mathbb{Z}$ with $n > 1$ and $0 \leq t \leq n < q$. Let C be an $RS_q[n, t]$-code. If $2t \leq n - 1$ then $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ and*

$$\widehat{t}(C) = \min\{t, n - 2t - 1\}.$$

PROOF. We know (Proposition 1.18) C is an MDS code with $n(C) = n$, $\dim C = t + 1$ and $d(C) = n - t + 1$. We can use Theorem 4.38 to determine that $w_i^\perp(C) = \dim C + 1 = t + 2$ for all $i \in \mathcal{I}(C)$.

Note that

$$C = \{(f(x_0), f(x_1), \ldots, f(x_n)), f \in \mathbb{F}_q[X]_{\leq t}\},$$

for distinct $x_0, x_1, \ldots, x_n \in \mathbb{F}_q$. Then

$$\widehat{C} = \{(h(x_0), h(x_1), \ldots, h(x_n)), h \in \mathbb{F}_q[X]_{\leq 2t}\}$$

since $\mathbb{F}_q[X]_{\leq 2t} = \mathbb{F}_q < \{fg : f, g \in \mathbb{F}_q[X]_{\leq t}\} >$.

If $2t \leq n - 1$, then $\widehat{C}$ is also an $RS_q[n, 2t]$-code. Note $d(\widehat{C}) = n - 2t + 1$. Again applying Theorem 4.38, we deduce $w_i(\widehat{C}) = n - 2t + 1 \geq 2$ for all $i \in \mathcal{I}(C)$ so $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ and by definition $\widehat{t}(C) = \min\{t, n - 2t - 1\}$. This implies the result. △

Hence we have:

PROPOSITION 4.44 *Let $\mathbb{F}_q$ be a finite field, and $1 < n < q$ an integer such that $n = 1 \pmod 3$. If C is a $RS_q[n, \frac{n-1}{3}]$-code, then $\widehat{\tau}(C) = 1$.*

We can recast the results for Shamir's threshold scheme, given in Chapter 3, in the framework introduced in this chapter. Let $\mathbb{F}_q$ be a finite field

and $t, n \in \mathbb{Z}$ with $1 \leq t < n < q$ and select $x_1, \ldots, x_n \in \mathbb{F}_q \setminus \{0\}$ with $x_i \neq x_j$ for $i \neq j$. Consider the $RS_q[n,t]$-code

$$C = \{(f(x_0), f(x_1), \ldots, f(x_n)) : f \in \mathbb{F}_q[X]_{\leq t}\}.$$

Then $\Sigma(C,0)$ is Shamir's scheme $\Sigma_{Sh}(\mathbb{F}_q, t, n, x_1, \ldots, x_n)$ (see Definition 3.38). We can now prove the known result about strong multiplication of Shamir's scheme (Theorem 3.41). Assume $3t < n$. Then also $2t < n$ and we can apply Theorem 4.43. We obtain $\widehat{t}(C) = \min\{t, n-2t-1\}$, but since $3t < n$, we have $t \leq n - 2t - 1$ so $\widehat{t}(C) = t$. Therefore the LSSS $\Sigma(C)$ (see Definition 4.28), has t-strong multiplication by Theorem 4.32. But in fact it is easy to see that $\Sigma(C) = \Sigma(C,0)$ since $C^\perp$ and $\widehat{C}$ are MDS codes and therefore $w_0^\perp(C) = w_i^\perp(C)$ and $w_0(\widehat{C}) = w_i(\widehat{C})$ for all $i \in \mathcal{I}(C)$.

Summary of the chapter: For every linear code C over $\mathbb{F}_q$ we have defined the set of good indices $I(C)$. We have introduced the class $\mathcal{C}(\mathbb{F}_q)$ of all codes with $I(C) \neq \emptyset$. For every code $C \in \mathcal{C}(\mathbb{F}_q)$ and every $i \in I(C)$, we have constructed an ideal linear secret sharing scheme $\Sigma(C,i)$ for $n(C)$ players, where $n(C) = \mathfrak{k}(C) - 1$. We have introduced the minimal weight $w_i(C)$ of C at an index i and related $w_i(C)$ and $w_i(C^\perp)$ to the privacy and reconstruction thresholds of $\Sigma(C,i)$. For every linear code C we have defined its Schur product square $\widehat{C}$. We have defined the class $\mathcal{C}^\dagger(\mathbb{F}_q)$ of all codes with $I(\widehat{C}) \neq \emptyset$. For any code $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ we have introduced the parameter $\widehat{t}(C)$ as the largest integer t for which some scheme $\Sigma(C,i)$ has t-strong multiplication and the corruption tolerance $\widehat{\tau}(C) = \frac{3\widehat{t}(C)}{n(C)-1}$. We have shown that $0 \leq \widehat{\tau}(C) \leq 1$ for every $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ and that $\widehat{\tau}(C) = 1$ can only hold if $\Sigma(C,i)$ is a threshold scheme for some $i \in I(C)$. We have shown that $\Sigma(C,i)$ is threshold if and only if C is an MDS code. Using the known bounds for the length of a MDS code, we have found limitations on the length of the codes $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ with $\widehat{\tau}(C) = 1$.

Chapter 5

The asymptotical optimal corruption tolerance $\widehat{\tau}(q)$

In this chapter we define the asymptotical corruption tolerance $\widehat{\tau}(q)$ of a finite field $\mathbb{F}_q$. This is a measure of how large the corruption tolerance of linear codes over $\mathbb{F}_q$ can be *asymptotically*, that is, when we consider infinite families of such codes. In this chapter we will define this parameter and recast the results of Chen and Cramer [20], which implied non-trivial lower bounds for $\widehat{\tau}(q)$ for infinitely many finite fields, in our framework.

5.1 Definition and motivation

We will define now the asymptotical optimal corruption tolerance of a finite field.

DEFINITION 5.1 *Let $\mathbb{F}_q$ be a finite field. For all integer $n > 1$, define*

$$T_q(n) := \max_{\substack{C \in \mathcal{C}^\dagger(\mathbb{F}_q) \\ n(C)=n}} \widehat{\tau}(C)$$

Note that $T_q(n)$ is well defined because for any fixed integer $n > 1$ there are only a finite number of codes $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ with $n(C) = n$.

DEFINITION 5.2 (ASYMPTOTICAL OPTIMAL CORRUPTION TOLERANCE) *Let $\mathbb{F}_q$ be a finite field. The* asymptotical optimal corruption tolerance *of $\mathbb{F}_q$ is*

$$\widehat{\tau}(q) := \limsup_{n \to \infty} T_q(n).$$

This parameter will be central in this thesis.

From Proposition 4.35 we can immediately derive the following result:

LEMMA 5.3 $0 \leq \widehat{\tau}(q) \leq 1$ *for any finite field* $\mathbb{F}_q$.

QUESTION 5.4 *Is* $\widehat{\tau}(q) > 0$ *possible for some* q*?. And if so, is* $\widehat{\tau}(q) = 1$ *possible?*

In Chapter 4 we studied the corruption tolerance of Reed-Solomon codes. We showed that some of these codes even achieve the optimal corruption tolerance $\widehat{\tau}(C) = 1$. However, the length of a Reed-Solomon code is bounded by the size of the field. Consequently, we do not have an infinite family of Reed-Solomon codes over a fixed finite field. Therefore, we cannot use Proposition 4.44 to show $\widehat{\tau}(q) > 0$, at least in a straightforward manner.

Moreover, we proved that if $\widehat{\tau}(C) = 1$ then C is an MDS code (Proposition 4.35) and in fact $n(C) \leq \frac{3q-4}{2}$ (Corollary 4.42). Consequently, for a fixed finite field $\mathbb{F}_q$, $T_q(n) < 1$ for all $n > \frac{3q-4}{2}$. Still, this a priori does not rule the possibility that $\widehat{\tau}(q) = 1$ for some finite field $\mathbb{F}_q$, because there could exist an infinite family of codes whose corruption tolerance *converges* to 1.

A possible alternative could be to combine Reed-Solomon codes over a tower of extension fields over the base field $\mathbb{F}_q$ with a concatenation method which would allow us to map these codes into codes over the base field, in a way that the corruption tolerances "do not degrade too much". In Section 6.5 of next chapter we give a construction of this type. However it does not enable us to prove $\widehat{\tau}(q) > 0$.

We will completely resolve the open question in the following two chapters. But first, we note that the algebraic geometric results in [20] already offered partial answers: these results implied that $\widehat{\tau}(q) > 0$ for *infinitely many* finite fields and provided some lower bounds for this parameter. In the next section we recast the results of [20] in our code-theoretic framework.

5.2 Known bounds for $\widehat{\tau}(q)$

The linear secret sharing schemes introduced in [20] (see Chapter 3) can be reinterpreted in our notation as the LSSS $\Sigma(C, i)$ associated to some algebraic geometric evaluation code C whose parameters satisfy certain conditions.

The properties of the schemes are summarized in the following propositions. First, the bounds on the distance of algebraic geometric codes (Propositions 2.101 and 2.103) imply the following.

PROPOSITION 5.5 *Let $t \geq 1$ be an integer and let $\mathbb{F}/\mathbb{F}_q$ be a function field of genus g with at least $n+1$ different places $P_0, P_1, \ldots, P_n$ of degree 1. Define $D = \sum_{i=0}^{n} P_i$. Let $G \in \mathrm{Div}_{2g+t}(\mathbb{F})$, such that* supp $D \cap$ supp $G = \emptyset$. *Let $C = C_L(D, G)$.*
Then $n(C) = n$, $d(C^\perp) \geq t+2$ and $d(C) \geq n - 2g - t + 1$.

Note that $d(C^\perp) \geq 2$ automatically implies that $I(C) \neq \emptyset$ and therefore $C \in \mathcal{C}(\mathbb{F}_q)$. Therefore:

COROLLARY 5.6 *Under the conditions above, $C \in \mathcal{C}(\mathbb{F}_q)$. Moreover, for all $i \in I(C)$, we have $w_i^\perp(C) \geq t+2$, $w_i(C) \geq n - 2g - t + 1$ and consequently $t(C,i) \geq t$, $r(C,i) \leq 2g + t + 1$.*

The multiplication properties are analyzed in the following proposition.

PROPOSITION 5.7 (CHEN AND CRAMER, [20]) *Under the conditions above, $\widehat{C} \subseteq C_L(D, 2G)$. Furthermore, assume that $n > 4g + 3t$. Then $d(\widehat{C}) \geq t+2$, $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ and $\widehat{t}(C) \geq t$.*

PROOF. If we take two (possibly equal) words $\mathbf{c}, \mathbf{c}' \in C$, then

$$\mathbf{c} = (f(P_0), f(P_1), \ldots, f(P_n)),$$

$$\mathbf{c}' = (g(P_0), g(P_1), \ldots, g(P_n))$$

for some $f, g \in \mathcal{L}(G)$. Then

$$\mathbf{c} * \mathbf{c}' = (fg(P_0), fg(P_1), \ldots, fg(P_n)).$$

Note that $fg \in \mathcal{L}(2G)$. Hence $\widehat{C} \subseteq C_L(D, 2G)$[1].

Again by the known bounds on the distance of AG codes,

$$d(\widehat{C}) \geq \mathfrak{k}(C) - \deg 2G = n + 1 - 4g - 2t > t + 1$$

so $d(\widehat{C}) \geq t+2$ and by Proposition 5.5 $d(C^\perp) \geq t+2$.

Now, $d(\widehat{C}) \geq 2$ implies $I(\widehat{C}) \neq \emptyset$, so $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$. For any $i \in I(\widehat{C})$, Proposition 4.19 implies

$$w_i(\widehat{C}) \geq d(\widehat{C}) \geq t+2,$$

[1] In this general case (unlike the particular case of Reed-Solomon codes, which are also AG codes) we cannot prove the equality: there can be elements in $\mathcal{L}(2G)$ which cannot be expressed as a linear combination of products of pairs of functions in $\mathcal{L}(G)$

and since $i \in I(C)$ (because $I(\widehat{C}) \subseteq I(C)$, see Proposition 4.24), it also implies that

$$w_i^{\perp}(C) \geq d(C^{\perp}) \geq t+2.$$

Therefore $\widehat{t}(C) \geq t$. △

This means that:

THEOREM 5.8 (CHEN AND CRAMER, [20]) *Let $t \geq 1$ be an integer. Suppose there exists a function field $\mathbb{F}/\mathbb{F}_q$ with genus g and such that $|\mathbb{P}^{(1)}(\mathbb{F})| \geq 4g+3t+2$.*
Then there exists a code $C \in C^{\dagger}(\mathbb{F}_q)$ with $n(C) = 4g+3t+1$ and $\widehat{t}(C) \geq t$ and consequently

$$\widehat{\tau}(C) \geq \frac{3t}{4g+3t}.$$

The asymptotical consequence is the following:

THEOREM 5.9 (CHEN AND CRAMER, [20]) *Let $\mathbb{F}_q$ be a finite field. If $A(q) > 4$, then*

$$\widehat{\tau}(q) \geq 1 - \frac{4}{A(q)} > 0.$$

PROOF. By definition of $A(q)$ (Definition 2.84) there exists an infinite family of natural numbers $\{g_m\}_{m\in\mathbb{N}}$ with $g_i < g_j$ for $i < j$ such that for any $\epsilon > 0$, there exists M with $N_q(g_m) > (A(q)-\epsilon)g_m$ for all $m > M$. This means (see Definition 2.83) that for every $m > M$ there exists a function field $\mathbb{F}^{(m)}$ over $\mathbb{F}_q$ with $g(\mathbb{F}^{(m)}) = g_m$ and $|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| > (A(q)-\epsilon)g_m$. Set

$$t_m = \lfloor \frac{(A(q)-4-\epsilon)g_m - 2}{3} \rfloor.$$

We have that

$$|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| \geq 4g(\mathbb{F}^{(m)}) + 3t_m + 2.$$

By Theorem 5.8, there exists $C^{(m)} \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $n(C^{(m)}) = 4g_m + 3t_m + 1$ and

$$\widehat{\tau}(C^{(m)}) \geq \frac{3t_m}{4g_m+3t_m}.$$

Since

$$(A(q)-4-\epsilon)g_m - 3 \leq 3t_m \leq (A(q)-4-\epsilon)g_m - 2$$

we have

$$\widehat{\tau}(C^{(m)}) \geq \frac{(A(q)-4-\epsilon)g_m - 3}{(A(q)-\epsilon)g_m - 2} = 1 - \frac{4g_m}{(A(q)-\epsilon)g_m - 2}$$

Finally

$$\limsup_{m>M} \widehat{\tau}(C^{(m)}) \geq 1 - \frac{4}{A(q)-\epsilon}.$$

Then

$$\widehat{\tau}(q) \geq 1 - \frac{4}{A(q)-\epsilon}$$

and since this is valid for any $\epsilon > 0$,

$$\widehat{\tau}(q) \geq 1 - \frac{4}{A(q)}$$

△

Now one can plug in the known results for $A(q)$. Theorem 2.86 implies:

THEOREM 5.10 *Let q be a* square *prime power, with $q \geq 49$. Then*

$$\widehat{\tau}(q) \geq 1 - \frac{4}{\sqrt{q}-1} > 0.$$

On the other hand Serre's theorem (Theorem 2.87) implies:

THEOREM 5.11 *There exists $Q \in \mathbb{Z}_+$, such that for all $q > Q$, $\widehat{\tau}(q) > 0$.*

Remark 2.88 implies this is true for $Q = 2^{4 \cdot 96} = 2^{384}$.

These two results imply that the asymptotical optimal corruption tolerance of certain finite fields is strictly positive. However this still does not prove that $\widehat{\tau}(q) > 0$ for *all* q. There are fields for which it is not known whether $A(q) \leq 4$ or $A(q) > 4$. And in fact, Drinfeld-Vladut bound (Theorem 2.85) states that $A(q) \leq \sqrt{q} - 1$ and consequently $A(q) \leq 4$ for all $q \leq 25$. In particular, the case $q = 2$ is not covered by these results.

Chapter 6

$\widehat{\tau}(q) > 0$ for all q

In this chapter, we prove that $\widehat{\tau}(q) > 0$ for all finite fields $\mathbb{F}_q$.

The proof of this result relies on the combination of the results in section 5.2 and a dedicated *field descent technique*. This is a tool which allows us to map a code $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^k})$, where k is an integer with $k \geq 2$, into another code $D \in \mathcal{C}^\dagger(\mathbb{F}_q)$ in such a way that $\widehat{t}(D) \geq \widehat{t}(C)$, at the cost of increasing $n(C)$ by some factor. This factor only depends, however, on q and k, but *not* on $n(C)$. The technique consists in the application of a special map, which we will call multiplication-friendly embedding, to every coordinate of a word in C, except the one in the special index allocating the secret.

Many of the definitions and results of this chapter were published in [15].

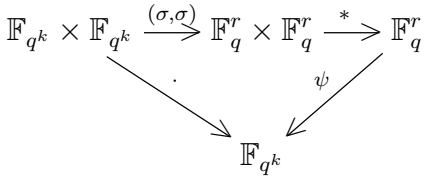
6.1 Multiplication-friendly embeddings

The field descent technique consists in the application of certain maps, which were named multiplication-friendly embeddings in [15]. As it will be remarked afterwards, the notion was however not new.

A multiplication-friendly embedding is a representation of elements in $\mathbb{F}_{q^k}$ as elements of $(\mathbb{F}_q)^r$ for some integer r, which "behaves sufficiently nicely with respect to multiplication". More precisely,

DEFINITION 6.1 *A* multiplication-friendly embedding of the extension field $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ *is a triple* (r, σ, ψ) *where* r *is a positive integer and where* $\sigma : \mathbb{F}_{q^k} \to \mathbb{F}_q^r$ *and* $\psi : \mathbb{F}_q^r \to \mathbb{F}_{q^k}$ *are* $\mathbb{F}_q$*-linear maps such that the follow-*

ing diagram commutes:



(where $(\sigma,\sigma)(x,y) := (\sigma(x),\sigma(y))$ for $x,y \in \mathbb{F}_{q^k}$, $*$ is the Schur product in $\mathbb{F}_q^r$ and $\cdot$ is the usual product in the field $\mathbb{F}_{q^k}$)

Or in other words, $xy = \psi(\sigma(x) * \sigma(y))$ for all x, y in $\mathbb{F}_{q^k}$. The integer r is called the expansion.

The following lemma (which justifies the use of the name embedding) will be helpful in the sequel.

LEMMA 6.2 *Let (r, σ, ψ) be a multiplication-friendly embedding. Then σ is injective.*

PROOF. σ is a linear map so we only need to prove that $\operatorname{Ker}\sigma = \{0\}$. But $x = 1 \cdot x = \psi(\sigma(1) * \sigma(x))$, by definition of multiplication-friendly embedding, so if $\sigma(x) = \mathbf{0}$, then $x = \psi(\sigma(1) * \mathbf{0}) = \psi(\mathbf{0}) = 0$ by linearity of ψ. △

In the sequel we will be interested in multiplication-friendly codes with expansion as small as possible. We define the following notion:

DEFINITION 6.3 *Let $\mathbb{F}_q$ be a finite field, $k \geq 2$ an integer. For every integer $r \geq 1$, let $\mathfrak{M}(q,k,r)$ denote the class of multiplication-friendly embeddings of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ with expansion r (if there is no such multiplication-friendly embedding, then let $\mathfrak{M}(q,k,r) = \emptyset$). We define*

$$m(q,k) := \min\{r \geq 1 : \mathfrak{M}(q,k,r) \neq \emptyset\}.$$

It will be helpful to define a certain class of generalized $\mathbb{F}_q$-linear codes, from which we can construct multiplication-friendly embeddings.

DEFINITION 6.4 *Let $r, k > 1$ be integers. An* (r,k)-multiplication-friendly code C over $\mathbb{F}_q$ *is a generalized $\mathbb{F}_q$-linear code $C \subseteq \mathbb{F}_{q^k} \times (\mathbb{F}_q)^r$ such that $\pi_0(C) = \mathbb{F}_{q^k}$, and $(x, \mathbf{0}) \notin \widehat{C}$ for all $x \in \mathbb{F}_{q^k} \setminus \{0\}$ where $\pi_0 : \mathbb{F}_{q^k} \times (\mathbb{F}_q)^r \to \mathbb{F}_{q^k}$ is the projection onto the 0-th coordinate.*

There is a correspondence between multiplication-friendly codes satisfying a certain property and multiplication-friendly embeddings.

PROPOSITION 6.5 *There is a one-to-one correspondence between $\mathfrak{M}(q,k,r)$ and the set of (r,k)-multiplication-friendly codes C over $\mathbb{F}_q$ with $|C| = q^k$.*

PROOF.

Let C be a (r,k)-multiplication-friendly code with $|C| = q^k$. Then $\pi_0(C) = \mathbb{F}_{q^k}$ implies that for any $x \in \mathbb{F}_{q^k}$, there exists a unique word $\mathbf{c}(x)$ in C such that $\pi_0(\mathbf{c}(x)) = x$. Therefore we can define the $\mathbb{F}_q$-linear mapping

$$\sigma : \mathbb{F}_{q^k} \to (\mathbb{F}_q)^r$$

$$x \mapsto \pi_{\mathcal{I}^*}(\mathbf{c}(x))$$

where $\mathcal{I}^* := \{1, \ldots, r\}$. Next we note the following fact: given two words $\mathbf{c}, \mathbf{c}' \in \widehat{C}$ such that $\pi_{\mathcal{I}^*}(\mathbf{c}) = \pi_{\mathcal{I}^*}(\mathbf{c}')$, it holds that $\pi_{\mathcal{I}^*}(\mathbf{c} - \mathbf{c}') = 0$. Since $\mathbf{c} - \mathbf{c}' \in \widehat{C}$ and C is a multiplication-friendly code, by Definition 6.1, we have $\pi_0(\mathbf{c} - \mathbf{c}') = 0$, so $\pi_0(\mathbf{c}) = \pi_0(\mathbf{c}')$. This guarantees that the following map is well defined: let

$$\psi : \pi_{\mathcal{I}^*}(\widehat{C}) \subseteq (\mathbb{F}_q)^r \to \mathbb{F}_{q^k}$$

$$\mathbf{v} \mapsto x$$

where $x \in \mathbb{F}_{q^k}$ is the only element such that $(x, \mathbf{v}) \in \widehat{C}$.

Moreover, this map is clearly $\mathbb{F}_q$-linear. One can linearly extend this map to a map $\psi : (\mathbb{F}_q)^r \to \mathbb{F}_{q^k}$. Finally we need to verify $xy = \psi(\sigma(x) * \sigma(y))$ for all x, y in $\mathbb{F}_{q^k}$. Now $\sigma(x) = \pi_{\mathcal{I}^*}(\mathbf{c}(x))$ and $\sigma(y) = \pi_{\mathcal{I}^*}(\mathbf{c}(y))$ imply

$$\sigma(x) * \sigma(y) = \pi_{\mathcal{I}^*}(\mathbf{c}(x) * \mathbf{c}(y)).$$

Note that $\mathbf{c}(x) * \mathbf{c}(y) \in \widehat{C}$ so the vector $\mathbf{v} = \pi_{\mathcal{I}^*}(\mathbf{c}(x) * \mathbf{c}(y))$ is in $\pi_{\mathcal{I}^*}(\widehat{C})$. Then $\psi(\sigma(x) * \sigma(y)) = \pi_0(\mathbf{c}(x) * \mathbf{c}(y)) = xy$ by construction. Consequently $(r, \sigma, \psi) \in \mathfrak{M}(q,k,r)$.

On the other hand suppose $(r, \sigma, \psi) \in \mathfrak{M}(q,k,r)$. Then consider the generalized $\mathbb{F}_q$-linear code $C = \{(x, \sigma(x)), x \in \mathbb{F}_{q^k}\}$. Note that $|C| = q^k$ and $\pi_0(C) = \mathbb{F}_{q^k}$. Suppose $(x, \mathbf{0}) \in \widehat{C}$ for some $x \in \mathbb{F}_{q^k}$. Then

$$(x, \mathbf{0}) = \sum_{\ell=1}^{m} \lambda_\ell \mathbf{c}_\ell * \mathbf{c}'_\ell$$

for some words $\mathbf{c}_\ell = (x_\ell, \sigma(x_\ell))$, $\mathbf{c}'_\ell = (y_\ell, \sigma(y_\ell))$ for $\ell = 1, \ldots, m$. Then $x = \sum_{\ell=1}^m \lambda_\ell x_\ell y_\ell$ and $\mathbf{0} = \sum_{\ell=1}^m \lambda_\ell \sigma(x_\ell) * \sigma(y_\ell)$. But since ψ is linear

$$\mathbf{0} = \psi(\sum_{\ell=1}^m \lambda_\ell \sigma(x_\ell) * \sigma(y_\ell)) = \sum_{\ell=1}^m \lambda_\ell \psi(\sigma(x_\ell) * \sigma(y_\ell)) = \sum_{\ell=1}^m \lambda_\ell x_\ell y_\ell$$

so $x = 0$. Hence C is a multiplication-friendly code. △

In fact, given a multiplication-friendly code, one can always consider a subcode which satisfies the condition in the statement of the theorem and consequently construct a multiplication-friendly embedding from it.

LEMMA 6.6 *Every (r, k)-multiplication-friendly code C over $\mathbb{F}_q$ contains a (r, k)-multiplication-friendly code C' over $\mathbb{F}_q$ such that $|C'| = q^k$.*

PROOF. Let C be an (r, k)-multiplication-friendly code and $\{e_1, \ldots, e_k\}$ be a basis of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Since $\pi_0(C) = \mathbb{F}_{q^k}$, there exist $\mathbf{c}_1, \ldots, \mathbf{c}_k$ with $\pi_0(\mathbf{c}_j) = e_j$, $j = 1, \ldots, k$. The words generate another multiplication-friendly code $C' = \mathbb{F}_q < \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k >$ with $C' \subseteq C$ and $|C'| = q^k$. △

We can now formulate upper bounds for the quantities $m(q, k)$.

THEOREM 6.7 *Let $\mathbb{F}_q$ be a finite field and $k \geq 2$ be an integer with $q \geq 2k-2$, then $m(q, k) \leq 2k - 1$.*

PROOF. We need to prove that in the conditions above there exists a $(2k-1, k)$-multiplication-friendly code C over $\mathbb{F}_q$.

Let $e \in \mathbb{F}_{q^k}$ be a primitive element in $\mathbb{F}_{q^k}$. Let $x_0, x_1, \ldots, x_{q-1}$ be all the elements of $\mathbb{F}_q$. For an integer $r \geq 0$ and $f \in \mathbb{F}_q[X]_{\leq r}$, denote $\gamma_r(f)$ the coefficient of X^r in f. Define the generalized linear code

$$C = \{(f(e), f(x_0), f(x_1), \ldots, f(x_{2k-3}), \gamma_{k-1}(f)) : f \in \mathbb{F}_q[X]_{\leq k-1}\}.$$

Note that this is well defined, since $q - 1 \geq 2k - 3$ by assumption. The map $\mathbb{F}_q[X]_{\leq k-1} \to \mathbb{F}_{q^k}$ given by $f \mapsto f(e)$ is a bijection, so $\pi_0(C) = \mathbb{F}_{q^k}$. On the other hand, the code $\widehat{C}$ is given by

$$\widehat{C} = \{(h(e), h(x_0), h(x_1), \ldots, h(x_{2k-3}), \gamma_{2k-2}(h)) : h \in \mathbb{F}_q[X]_{\leq 2k-2}\}.$$

Given a word of the form $\mathbf{c} = (x, \mathbf{0}) \in \widehat{C}$, where $x \in \mathbb{F}_{q^k}$, one can see that $x = 0$ as follows: let I^* denote the set of the last $2k-1$ indices of $\widehat{C}$. Then $\pi_{I^*}(\mathbf{c}) = \mathbf{0}$ implies that

$$\mathbf{c} = (h(e), h(x_0), h(x_1), \ldots, h(x_{2k-3}), \gamma_{2k-2}(h)),$$

for $h \in \mathbb{F}_q[X]_{\leq 2k-2}$ a multiple of $\prod_{i=0}^{2k-3}(X - x_i)$ such that $\gamma_{2k-2}(h) = 0$. This implies $h = 0$ and consequently $\pi_0(\mathbf{c}) = h(e) = 0$. Hence $(x, \mathbf{0}) \notin \widehat{C}$ for all $x \in \mathbb{F}_{q^k} \setminus \{0\}$ and all the conditions in Definition 6.4 have been verified, so C is a multiplication-friendly code.

△

Two particular cases will be especially interesting.

COROLLARY 6.8 *$m(q, 2) \leq 3$ for all finite field $\mathbb{F}_q$. Moreover $m(4, 3) \leq 5$*

In order to obtain the results of Section 6.5 we will need a construction of multiplication-friendly embeddings of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ without any constraint on q and k. The expansion in this case is worse, as it is quadratic in k, although for the particular case $k = 2$ it is exactly the same as above.

THEOREM 6.9 *For every finite field $\mathbb{F}_q$, and any integer $k \geq 2$, there exists a multiplication-friendly embedding of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ with expansion $\binom{k+1}{2}$. Therefore $m(q, k) \leq \binom{k+1}{2}$.*

PROOF. Let $\alpha \in \mathbb{F}_{q^m}$ such that $1, \alpha, \ldots, \alpha^{m-1}$ is a basis of $\mathbb{F}_{q^m}$ as an $\mathbb{F}_q$-vector space. Consider the map

$$\begin{array}{rcl} \sigma : \mathbb{F}_{q^m} & \to & (\mathbb{F}_q)^r \\ x & \mapsto & (x_0, \ldots, x_{m-1}, x_0 + x_1, \ldots, x_0 + x_{m-1}, \ldots, x_{m-2} + x_{m-1}), \end{array}$$

where $x = \sum_{i=0}^{m-1} x_i \alpha^i$. Given two elements $x, y \in \mathbb{F}_{q^m}$, the coordinates of $\sigma(x) * \sigma(y)$ precisely exhaust all possible expressions $x_i y_i$, as well as all possible expressions $x_i y_i + x_j y_j + x_i y_j + x_j y_i$ for $i \neq j$. Hence, for each pair of indices (i, j) with $i \neq j$, there exists an $\mathbb{F}_q$-linear map $\phi_{i,j}$ such that $\phi_{i,j}(\sigma(x) * \sigma(y)) = x_i y_j + x_j y_i$. Since

$$xy = \sum_{k=0}^{2m-2} \Big(\sum_{i+j=k} x_i y_j \Big) \alpha^k = \sum_{i=0}^{m-1} x_i y_i \alpha^{2i} + \sum_{k=0}^{2m-2} \Big(\sum_{i+j=k, i<j} x_i y_j + x_j y_i \Big) \alpha^k,$$

it follows that there exists an $\mathbb{F}_q$-linear map ψ such that $xy = \psi(\sigma(x) * \sigma(y))$. $\triangle$

Note that this construction does not rely on algebraic geometric techniques. In Chapter 12 we will see that we can obtain multiplication-friendly embeddings of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ for fixed q and arbitrarily large k with much better expansion than the one given in this theorem. However, those results will require the existence of asymptotically good families of function fields over $\mathbb{F}_q$.

6.2 Dedicated field descent technique

In the next theorem, we state the main technical tool of this chapter.

THEOREM 6.10 *Let (r, σ, ψ) be a multiplication-friendly embedding of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Then there exists a transformation $\vartheta_{r,\sigma} : \mathcal{C}^\dagger(\mathbb{F}_{q^k}) \to \mathcal{C}^\dagger(\mathbb{F}_q)$ such that for all $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^k})$, $n(\vartheta_{r,\sigma}(C)) = r \cdot n(C)$ and $\widehat{t}(\vartheta_{r,\sigma}(C)) \geq \widehat{t}(C)$ and consequently*

$$\widehat{\tau}(\vartheta_{r,\sigma}(C)) \geq \frac{1}{r}\widehat{\tau}(C)\left(1 - \frac{r-1}{rn(C)-1}\right).$$

PROOF. Let $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^k})$. Write $n = n(C)$. After permuting $\mathcal{I}(C)$, if necessary, we may assume without loss of generality that $i_s = 0$ (see Definition 4.28), i.e., $\widehat{t}(C)$ is attained for $i = 0$ (so in particular $0 \in I(\widehat{C})$). As usual we denote $\mathcal{P}(C, 0) = \mathcal{I}(C) \setminus \{0\}$.

Consider the $\mathbb{F}_q$-generalized linear code $G = C \cap (\mathbb{F}_q \bigoplus (\mathbb{F}_{q^k})^n)$, i.e., the elements of C whose 0-th coordinate is in $\mathbb{F}_q$.

Define the map

$$\chi : \mathbb{F}_q \bigoplus (\mathbb{F}_{q^k})^n \to (\mathbb{F}_q)^{1+rn}$$

$$(c_0, c_1, \ldots, c_n) \mapsto (c_0, \sigma(c_1), \ldots, \sigma(c_n)).$$

Note that this map is $\mathbb{F}_q$-linear. Now define $D = \chi(G) \subset \mathbb{F}_q^{rn+1}$, and note that D is an $\mathbb{F}_q$-linear code with $n(D) = rn$.

For the sake of notation, denote the set of indices of D as

$$\mathcal{I}(D) := \{(0,0)\} \cup \{(i,j), 1 \leq i \leq n, 1 \leq j \leq r\}.$$

Let $\mathcal{P}(D, (0,0)) = \mathcal{I}(D) \setminus \{(0,0)\}$. Let $\pi'_(i,j)$ denote the projection to the index $(i,j) \in \mathcal{I}(D)$ of a word in D. The notation for the indices of $\mathcal{I}(D)$

highlights the fact that every "parent" index $i \in \mathcal{P}(C,0)$ has r "children" indices (i,j), $j = 1,\ldots,r$ of $\mathcal{P}(D,(0,0))$, while $0 \in \mathcal{I}(C)$ has as only child $(0,0) \in \mathcal{I}(D)$. That is, the indices of $\mathcal{I}(D)$, are denoted in such a way that for a word in D of the form $\mathbf{w} = \chi(\mathbf{c})$, with $\mathbf{c} = (c_0, c_1, \ldots, c_n) \in G$, $\pi'_{(0,0)}(\mathbf{w}) := \pi_0(\mathbf{c}) = c_0$ and for $1 \leq i \leq n$, $1 \leq j \leq r$, $\pi_{(i,j)}(\mathbf{w})$ denotes the j-th coordinate of $\sigma(c_i)$.

Moreover, if $A \subset \mathcal{P}(D,(0,0))$ is a non-empty set, then $\beta(A) \subset \mathcal{P}(C,0)$ denotes the set of parent indices of the indices in A. Note that $|\beta(A)| \leq |A|$. Finally, $\alpha(A) \subset \mathcal{P}(D,(0,0))$ denotes the set of all children of the elements in $\beta(A)$ (the set of "siblings" of the indices in A). Note that $A \subset \alpha(A)$.

Next it is shown that $w^{\perp}_{(0,0)}(D) \geq w^{\perp}_0(C)$ and $w_{(0,0)}(\widehat{D}) \geq w_0(\widehat{C})$. That will prove $D \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ and $\widehat{t}(D) \geq t$ because $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ and $\widehat{t}(C) \geq t$.

In order to prove $w^{\perp}_{(0,0)}(D) \geq w^{\perp}_0(C)$ we first prove $(0,0) \in I(D)$ and $t(D,(0,0)) \geq t(C,0)$. Note that by definition, $0 \in I(C)$ and therefore $w_0(C) > 1$. By construction of D, and the fact that Ker $\sigma = \{0\}$ clearly $w_{(0,0)}(D) > 1$ so $(0,0) \in I(D)$ and $t(D,(0,0))$ is well defined. Now, let $A \subseteq \mathcal{P}(D,(0,0))$ with $|A| = t(C,0)$. Since $|\beta(A)| \leq t(C,0)$ and we have that $\beta(A) \in \mathcal{A}(C,0)$ and there exists $\mathbf{c} \in C_{0,1}$ such that $\pi_{\beta(A)}(\mathbf{c}) = \mathbf{0}$. Note that, since $\pi_0(\mathbf{c}) = 1$, $\mathbf{c}$ belongs to G. Then $\pi'_0(\chi(\mathbf{c})) = 1$, $\pi'_{\alpha(A)}(\chi(\mathbf{c})) = \mathbf{0}$, so $\alpha(A) \in \mathcal{A}(D,(0,0))$. Since $A \subset \alpha(A)$, we have $A \in \mathcal{A}(D,(0,0))$. Since this is valid for any set $A \subseteq \mathcal{P}(D,(0,0))$ with $|A| = t(C,0)$, we conclude that $t(D,(0,0)) \geq t(C,0)$. Finally, applying Proposition 4.18 we find out that $w^{\perp}_{(0,0)}(D) \geq w^{\perp}_0(C)$.

Now we prove that $w_{(0,0)}(\widehat{D}) \geq w_0(\widehat{C})$. Let $\mathbf{w} \in (\widehat{D})_{(0,0),1}$. Then we can write this word as $\mathbf{w} = \sum \lambda_\ell \mathbf{y}_\ell * \mathbf{y}'_\ell$, with $\lambda_\ell \in \mathbb{F}_q$, $\mathbf{y}_\ell, \mathbf{y}'_\ell \in D$. Let $\mathbf{y}_\ell = \chi(\mathbf{x}_\ell)$ and $\mathbf{y}'_\ell = \chi(\mathbf{x}'_\ell)$, with $\mathbf{x}_\ell, \mathbf{x}'_\ell \in G \subseteq C$. Then the word $\mathbf{c} = \sum \lambda_\ell \mathbf{x}_\ell * \mathbf{x}'_\ell$ belongs to $\widehat{C}$ as $\lambda_\ell \in \mathbb{F}_q \subseteq \mathbb{F}_{q^k}$. It is immediate to see from the definition of χ that $\pi_0(\mathbf{c}) = \pi_{(0,0)}(\mathbf{w}) = 1$ so $\mathbf{c} \in (\widehat{C})_{0,1}$.

Next we prove $w_{Ham}(\mathbf{w}) \geq w_{Ham}(\mathbf{c})$. For this we prove that for all indices $i \in \mathcal{P}(C,0)$, such that $\pi_i(\mathbf{c}) \neq 0$, there exists $1 \leq j \leq r$ such that $\pi'_{(i,j)}(\mathbf{w}) \neq 0$. Suppose on the contrary that $\pi'_{(i,j)}(\mathbf{w}) = 0$ for all $1 \leq j \leq r$ or, in the notation above, $\pi'_{\alpha(\{(i,j)\})}(\mathbf{w}) = \mathbf{0}$. Note that by definition of $\mathbf{w}$, this is the same as saying

$$\mathbf{0} = \sum_{\ell} \lambda_\ell \sigma(\pi_i(\mathbf{x}_\ell)) * \sigma(\pi_i(\mathbf{x}'_\ell))$$

and by Definition 6.1,

$$\psi(\sigma(\pi_i(\mathbf{x}_\ell)) * \sigma(\pi_i(\mathbf{x}'_\ell))) = \pi_i(\mathbf{x}_\ell)\pi_i(\mathbf{x}'_\ell)$$

and as ψ is linear,

$$\pi_i(\mathbf{c}) = \sum_\ell \lambda_\ell \pi_i(\mathbf{x}_\ell)\pi_i(\mathbf{x}'_\ell) = \sum_\ell \lambda_\ell \psi(\sigma(\pi_i(\mathbf{x}_\ell)) * \sigma(\pi_i(\mathbf{x}'_\ell))) =$$

$$= \psi(\sum_\ell \lambda_\ell \sigma(\pi_i(\mathbf{x}_\ell)) * \sigma(\pi_i(\mathbf{x}'_\ell))) = \psi(\mathbf{0}) = 0,$$

which is a contradiction. Summing up, it has been proved that for all $\mathbf{w} \in (\widehat{D})_{(0,0),1}$ we can associate a word $\mathbf{c} \in (\widehat{C})_{0,1}$ with $w_{Ham}(\mathbf{c}) \leq w_{Ham}(\mathbf{w})$. Hence $w_{(0,0)}(\widehat{D}) \geq w_0(\widehat{C})$.

We have proved $D \in \mathcal{C}^\dagger(\mathbb{F}_q)$ and $\widehat{t}(D) \geq \widehat{t}(C)$. Therefore

$$\widehat{\tau}(D) \geq \frac{3\widehat{t}(D)}{n(D)-1} = \frac{3\widehat{t}(C)}{rn(C)-1} = \frac{1}{r}\widehat{\tau}(C)\left(1 - \frac{r-1}{rn(C)-1}\right).$$

Therefore we can define a map $\vartheta_{r,\sigma} : \mathcal{C}^\dagger(\mathbb{F}_{q^k}) \to \mathcal{C}^\dagger(\mathbb{F}_q)$ satisfying the properties of the statement. For $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^k})$, $\vartheta_{r,\sigma}(C) := D$ where D is constructed from C as we have described at the beginning of this proof.

△

6.3 Explicit lower bounds

Finally, we are prepared to prove that $\widehat{\tau}(q) > 0$ for all finite fields $\mathbb{F}_q$. First note the following fact.

THEOREM 6.11 *For any finite field $\mathbb{F}_q$ and any integer $k \geq 2$,*

$$\widehat{\tau}(q) \geq \frac{1}{m(q,k)}\widehat{\tau}(q^k).$$

PROOF. There is an infinite family of codes $\{C^{(\ell)}\}_{\ell>0} \subseteq \mathcal{C}^\dagger(\mathbb{F}_{q^k})$ such that $n(C^{(i)}) < n(C^{(j)})$ for $i < j$ and $\widehat{\tau}(C^{(\ell)}) \to \widehat{\tau}(q^k)$. Applying Theorem 6.10 to $C^{(\ell)}$ using a multiplication-friendly embedding $(m(q,k), \sigma, \psi)$ (which exists by definition of $m(q,k)$) gives a code $D^{(\ell)} = \vartheta_{m(q,k),\sigma}(C^{(\ell)}) \in \mathcal{C}^\dagger(\mathbb{F}_q)$ with

$\widehat{\tau}(D^{(\ell)}) \geq \frac{1}{m(q,k)}\widehat{\tau}(C^{(\ell)})\left(1 - \frac{m(q,k)-1}{m(q,k)n(C^{(\ell)})-1}\right)$. Note $n(D^{(\ell)}) = m(q,k)n(C^{(\ell)})$ so $n(D^{(i)}) < n(D^{(j)})$ for $i < j$.

Finally, even though $\lim_{\ell\to\infty}\widehat{\tau}(D^{(\ell)})$ might not exist, we can ensure that

$$\limsup_{\ell\to\infty}\widehat{\tau}(D^{(\ell)}) \geq \frac{1}{m(q,k)}\lim_{\ell\to\infty}\widehat{\tau}(C^{(\ell)})\left(1 - \frac{m(q,k)-1}{m(q,k)n(C^{(\ell)})-1}\right) =$$

$$= \frac{1}{m(q,k)}\widehat{\tau}(q^k)$$

since $\widehat{\tau}(C^{(\ell)}) \to \widehat{\tau}(q^k)$ and $n(C^{(\ell)}) \to \infty$. This is enough to verify the statement of the theorem. △

In particular, in the case of square extensions we can apply Corollary 6.8 and we have:

COROLLARY 6.12 *For any finite field $\mathbb{F}_q$, $\widehat{\tau}(q) \geq \frac{1}{3}\widehat{\tau}(q^2)$*

It is useful to define now the following function:

DEFINITION 6.13 *For every finite field $\mathbb{F}_q$, let $\nu(q)$ be as follows:*

$$\nu(q) := \begin{cases} 1/35 \approx 2.86\% & \text{if } q = 2 \\ 1/18 \approx 5.56\% & \text{if } q = 3 \\ 3/35 \approx 8.57\% & \text{if } q = 4 \\ 5/54 \approx 9.26\% & \text{if } q = 5 \\ 1 - \frac{4}{\sqrt{q}-1} & \text{if } q \text{ square, } q \geq 49 \\ \frac{1}{3}(1 - \frac{4}{q-1}) & \text{in all the other cases } (5 < q < 49 \text{ or} \\ & q \geq 49,\ q \text{ non-square}) \end{cases}$$

And finally we prove the main result of this chapter.

THEOREM 6.14 *Let $\mathbb{F}_q$ be a finite field. Then $\widehat{\tau}(q) \geq \nu(q) > 0$.*

PROOF. The result for q square, $q \geq 49$ is Theorem 5.10. From these bounds and the descent method one can derive the results for the rest of

cases. First, applying Corollary 6.12 to any $\mathbb{F}_q$ such that $q \geq 7$ and noticing $q^2 \geq 49$ gives

$$\widehat{\tau}(q) \geq \frac{1}{3}\widehat{\tau}(q^2) \geq \frac{1}{3}\left(1 - \frac{4}{\sqrt{q^2}-1}\right) = \frac{1}{3}\left(1 - \frac{4}{q-1}\right).$$

For the cases $q = 3, 5$ one uses the descent method again, this time on the results for $\mathbb{F}_9$ and $\mathbb{F}_{25}$ obtained above. This gives

$$\widehat{\tau}(q) \geq \frac{1}{3}\widehat{\tau}(q^2) \geq \frac{1}{9}\left(1 - \frac{4}{q^2-1}\right)$$

which corresponds to the bounds above. In the case $q = 4$ we could apply the descent method to $\mathbb{F}_{16}$ but in fact it is better to apply it to $\mathbb{F}_{64}$. Then $\widehat{\tau}(4) \geq \frac{1}{m(4,3)}\widehat{\tau}(64)$ and as remarked above $m(4,3) \leq 5$ so one obtains $\widehat{\tau}(4) \geq 3/35$. Finally applying once more the descent technique to $\mathbb{F}_2$ and $\mathbb{F}_4$ one gets $\widehat{\tau}(2) \geq \frac{1}{3}\widehat{\tau}(4) \geq 1/35$. △

6.4 A remark on the dual distance

In this section we address a limitation of the dedicated field descent method. As we have seen, if we apply this technique to a code $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^k})$, we obtain another code $\vartheta_{r,\sigma}(C) \in \mathcal{C}^\dagger(\mathbb{F}_q)$ such that $\widehat{t}(\vartheta_{r,\sigma}(C)) \geq \widehat{t}(C)$ and in particular $w_j^\perp(\vartheta_{r,\sigma}(C)) \geq w_i^\perp(C)$ for some $i \in \mathcal{I}(C)$, $j \in \mathcal{I}(\vartheta_{r,\sigma}(C))$. However in this section, we will see that the field descent technique "does not preserve the dual distance". In fact the dual distance of $\vartheta_{r,\sigma}(C)$ is upper bounded by a constant independent of the length of C.

We first need the following observation

LEMMA 6.15 *If (r, σ, ψ) is a multiplication-friendly embedding of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, $k \geq 2$, then $\sigma : \mathbb{F}_{q^k} \to (\mathbb{F}_q)^r$ cannot be surjective.*

PROOF. Assume σ were a surjection, then it would also be bijective by Lemma 6.2. Then $r = k$. Note however that when considering $(\mathbb{F}_q)^k$ as a ring with the multiplication given by Schur's product $*$, when $k \geq 2$, $(\mathbb{F}_q)^k$ has divisors of zero, so there exist $\mathbf{0} \neq \mathbf{x}, \mathbf{y} \in (\mathbb{F}_q)^k$ with $\mathbf{x} * \mathbf{y} = \mathbf{0}$. Then, if x', y' are the only elements in $\mathbb{F}_{q^k}$ with $\sigma(x') = \mathbf{x}$, $\sigma(y') = \mathbf{y}$. Then we have $x'y' = \psi(\sigma(x') * \sigma(y')) = \psi(\mathbf{x} * \mathbf{y}) = \psi(\mathbf{0}) = 0$ but then either $x' = 0$ (and in that case $\mathbf{x} = 0$) or $y' = 0$ (so $\mathbf{y} = 0$). So we get a contradiction. △

REMARK 6.16 *As an aside remark, this means that for all finite field $\mathbb{F}_q$ and any $k \geq 2$, we have $m(q,k) > k$. In particular, if we combine this with Corollary 6.8, we deduce that $m(q,2) = 3$ for any finite field $\mathbb{F}_q$.*

Now we prove the fact that the field descent technique does not preserve dual distances, even though it preserves the minimal weight at some index of the dual code.

PROPOSITION 6.17 *Let $k \geq 2$, $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^k})$, and (r, σ, ψ) be a multiplication-friendly embedding of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ and $\vartheta_{r,\sigma} : \mathcal{C}^\dagger(\mathbb{F}_{q^k}) \to \mathcal{C}^\dagger(\mathbb{F}_q)$ be as in Theorem 6.10. Then $w^\perp_{(0,0)}(\vartheta_{r,\sigma}(C)) \geq w^\perp_0(C)$ and $d(\vartheta_{r,\sigma}(C)^\perp) \leq r$.*

PROOF. The first part was proved in Theorem 6.10. As for the second part, Im $\sigma \neq (\mathbb{F}_q)^r$(by Lemma 6.15) so $(\text{Im } \sigma)^\perp \neq \emptyset$. Let $\mathbf{0} \neq \mathbf{v} \in (\text{Im } \sigma)^\perp$. Then by construction of $\vartheta_{r,\sigma}(C)$, it holds that $\mathbf{c} = (0, \mathbf{v}, \mathbf{0}, \ldots, \mathbf{0}) \in \vartheta_{r,\sigma}(C)^\perp$ and $w_{Ham}(\mathbf{c}) \leq r$. △

We can now examine the asymptotical consequences of this. It is not surprising that there exist families of linear codes C over a finite field such that $w^\perp_i(C) - d(C^\perp)$ can be made arbitrarily large for some $i \in \mathcal{I}(C)$ (one can come up with trivial examples of this fact). But we can now prove that this also holds for families of codes *with asymptotically good corruption tolerance.*

PROPOSITION 6.18 *For every finite field $\mathbb{F}_q$, there exists an infinite family of codes $\{D^{(m)}\}_{m>0} \subseteq \mathcal{C}^\dagger(\mathbb{F}_q)$ with $n(D^{(m)}) \to \infty$ such that*

$$\widehat{\tau}(D^{(m)}) \to \tau > 0$$

but

$$\frac{d((D^{(m)})^\perp)}{n(D^{(m)})} \to 0.$$

PROOF. Let $k \geq 2$. As we know that $\widehat{\tau}(q^k) > 0$, there exists an infinite sequence of codes $C^{(m)} \in \mathcal{C}^\dagger(\mathbb{F}_{q^k})$ such that $n(C^{(m)}) \to \infty$ and

$$\widehat{\tau}(C^{(m)}) \to \widehat{\tau}(q^k) > 0.$$

Let (r, σ, ψ) be a multiplication-friendly embedding of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ and for all m define $D^{(m)} = \vartheta_{r,\sigma}(C^{(m)}) \in \mathcal{C}^\dagger(\mathbb{F}_q)$. Note that $n(D^{(m)}) = r \cdot n(C^{(m)})$. By Theorem 6.10, we can assume without loss of generality that

$$\widehat{\tau}(D^{(m)}) \to \tau \geq \frac{1}{r}\widehat{\tau}(q^k) > 0.$$

On the other hand, by Proposition 6.17, $d((D^{(m)})^{\perp}) \leq r$ *for all* m. Therefore $\frac{d((D^{(m)})^{\perp})}{n(D^{(m)})} \to 0$. $\triangle$

In Chapter 7, we will prove non-trivial upper bounds for $\widehat{\tau}(q)$. Proposition 6.18 tells us, however, that in order to do that we cannot use, at least in a straightforward manner, the asymptotical upper bounds for the relative distance of codes stated in Chapter 1.

Another consequence is that these families of codes are not suitable for one of the applications mentioned in the Introduction to this thesis, namely the constructions of correlation extractors of [47], since one of the conditions required by these constructions is that the relative distance of the family of linear codes used is asymptotically non-vanishing.

6.5 Note on elementary constructions

We have shown that a combination of strong methods from algebraic geometry with a dedicated field-descent method leads to asymptotically good schemes over any finite field.

We now show an *elementary* construction of families of codes that we can define for any finite field $\mathbb{F}_q$. It is asymptotically bad. Yet it gives t-strong multiplication for $t = \Omega(n/((\log\log n)\log n))$.

The construction is as follows:

For every integer $k > 0$ define $r_k = (q^k)^{\lfloor \frac{q^k}{2} \rfloor}$. Define $t_k = \lfloor \frac{1}{3}(r_k - 2) \rfloor$. Consider a $RS_{r_k}[r_k - 1, t_k]$-code C_k. Since $3t_k < r_k$, we can show, using the arguments as in Theorem 4.43, that $C_k \in \mathcal{C}^{\dagger}(\mathbb{F}_{r_k})$ and $\widehat{t}(C_k) = t_k$.

We apply now the descent technique (Theorem 6.10). Note that we cannot use the multiplication-friendly embeddings in Theorem 6.7 to descend from $\mathbb{F}_{r_k}$ to $\mathbb{F}_q$ since it is not true in general that $q \geq 2k\lfloor q^k/2 \rfloor - 2$. We could use the construction in Theorem 6.9 but instead what we do is combining both approaches.

First, we apply Theorem 6.10 to descend from $\mathbb{F}_{r_k}$ to $\mathbb{F}_{q^k}$ using the multiplication-friendly embedding $(r_k^{(1)}, \sigma_k^{(1)}, \psi_k^{(1)})$ from Theorem 6.7, which we can construct because $q^k \geq 2\lfloor \frac{q^k}{2} \rfloor - 2$. Note that $r_k^{(1)} = 2\lfloor \frac{q^k}{2} \rfloor - 1$. This yields a code $C'_k := \vartheta_{r_k^{(1)}, \sigma_k^{(1)}}(C_k) \in \mathcal{C}^{\dagger}(\mathbb{F}_{q^k})$ with

$$n(C'_k) = (2\lfloor \frac{q^k}{2} \rfloor - 1) n(C_k)$$

and

$$\widehat{t}(C'_k) \geq t_k.$$

Then we descend from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$ applying again Theorem 6.10 but now using the multiplication-friendly embedding $(r_k^{(2)}, \sigma_k^{(2)}, \psi_k^{(2)})$ in Theorem 6.9, where $r_k^{(2)} = \binom{k+1}{2}$. This gives us a code $D_k = \vartheta_{r_k^{(2)}, \sigma_k^{(2)}}(C'_k) \in \mathcal{C}^\dagger(\mathbb{F}_q)$ with

$$n(D_k) = \binom{k+1}{2} n(C'_k) = \binom{k+1}{2} (2\lfloor \frac{q^k}{2} \rfloor - 1) n(C_k) =$$

$$= \binom{k+1}{2} (2\lfloor \frac{q^k}{2} \rfloor - 1)(r_k - 1)$$

and

$$\widehat{t}(D_k) \geq t_k = \lfloor \frac{1}{3}(r_k - 2) \rfloor.$$

Consequently

$$\widehat{t}(D_k) = \Omega(n(D_k)/((\log\log n(D_k)) \log n(D_k)).$$

Unfortunately, we cannot prove $\widehat{\tau}(q) > 0$ for any field $\mathbb{F}_q$ using this construction. In fact, we still do not know if we can prove this fact without the use of asymptotically good families of function fields. A well known result of coding theory, proved by Pellikaan, Shen and van Wee ([65]) states that every linear code over $\mathbb{F}_q$ is an AG-code defined over some function field $\mathbb{F}/\mathbb{F}_q$. Therefore for any infinite family of codes $\{C^{(m)}\}_{m>0} \subseteq \mathcal{C}^\dagger(\mathbb{F}_q)$ with $n(C^{(m)}) \to \infty$ there exists an infinite family $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$ of function fields $\mathbb{F}^{(m)}/\mathbb{F}_q$ such that $C^{(m)}$ is an AG-code defined over the function field $\mathbb{F}^{(m)}/\mathbb{F}_q$ and consequently $|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| \to \infty$ and $g(\mathbb{F}^{(m)}) \to \infty$. Assume now that in addition the codes satisfy $\widehat{\tau}(C^{(m)}) \to \tau > 0$. An interesting question is whether this implies $A(\mathcal{F}) > 0$, i.e., if it is a necessary condition that these codes are defined over an asymptotically good family of function fields.

We can compare this aspect of our problem with the code-theoretic problem of asymptotically good codes. Xing [82] proved that given a finite field $\mathbb{F}_q$ and *any* real number $0 < a \leq A(q)$ there exist families of AG-codes defined over a family $\mathcal{F}$ of function fields over $\mathbb{F}_q$ with $A(\mathcal{F}) = a$ and attaining the Gilbert-Varshamov bound. And in fact, if we examine the arguments given in [82], the same result is true if one uses asymptotically bad families $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$ (i.e. $A(\mathcal{F}) = 0$) as long as $|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| \to \infty$. So $A(\mathcal{F}) > 0$

is not a necessary condition for the construction of families of linear codes attaining the Gilbert-Varshamov bound.

However the techniques in [82] do not seem to yield a similar result for our problem.

Summary of the chapter: We have proved that $\widehat{\tau}(q) > 0$ for *all* finite fields $\mathbb{F}_q$. In order to do this we have introduced multiplication-friendly embeddings (r, σ, ψ) with expansion r of an extension field $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ and the parameter $m(q,k)$ as the smallest expansion among all these embeddings. We have proved that for every $C \in \mathcal{C}^{\dagger}(\mathbb{F}_{q^k})$ we can construct a code $D \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $\widehat{\tau}(D) \geq \frac{1}{m(q,k)}\widehat{\tau}(C)$. After that we have combined this with the results by Chen and Cramer [20] and found explicit lower bounds for $\widehat{\tau}(q)$ for every finite field $\mathbb{F}_q$. We have remarked that although the descent method does not degrade the parameter $\widehat{t}(C)$, it does not behave so well with $d(C^{\perp})$. Finally we have shown an elementary construction of families of LSSS with t-strong multiplication, where $t = \Omega(n/((\log\log n)\log n))$.

Chapter 7

$\widehat{\tau}(q) < 1$ for all q

In this chapter we prove that $\widehat{\tau}(q) < 1$ for all finite fields $\mathbb{F}_q$ and give explicit upper bounds for $\widehat{\tau}(q)$. We already know from Chapter 4 that $\widehat{\tau}(C) \leq 1$ for every code $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ (which trivially implies $\widehat{\tau}(q) \leq 1$) and that $T_q(n) < 1$ for all integers $n > \frac{3q-4}{2}$ (Corollary 4.42). But, in principle, this fact does not rule out the possibility that there exists an infinite family of linear codes $\{C_m\}_{m \in \mathbb{N}} \subseteq \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $n(C_m) \to \infty$ and $\widehat{\tau}(C_m) \to 1$ and, therefore, the equality $\widehat{\tau}(q) = 1$ might still be attained for some finite field $\mathbb{F}_q$.

However, we will show in this chapter that this is indeed impossible, so $\widehat{\tau}(q) < 1$ for all finite fields $\mathbb{F}_q$. In fact, we will derive explicit (non-trivial) upper bounds for $\widehat{\tau}(q)$.

Many of the results in this chapter appeared in [17].

7.1 Upper bounding $w_i(C)$ as a function of n, q and $w_i^{\perp}(C)$

In Proposition 4.20, we stated an upper bound for $w_i(C)$ as a function of $n(C)$ and $w_i^{\perp}(C)$. This led to the fact that $\widehat{\tau}(C) \leq 1$ for every code $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ (Proposition 4.35) and implied $\widehat{\tau}(q) \leq 1$ for any finite field $\mathbb{F}_q$. The proof of this result combined the aforementioned bound for the weights $w_i(C)$ with the fact that there exists some index $i \in \mathcal{I}(C)$ such that not only $w_i^{\perp}(C) \geq \widehat{t}(C) + 2$ and $w_i(\widehat{C}) \geq \widehat{t}(C) + 2$, but also, by Propositions 4.17 and 4.33, $w_i(C) \geq 2\widehat{t}(C) + 2$.

In order to find *non-trivial* upper bounds for $\widehat{\tau}(q)$ we will first obtain, for any $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$, upper bounds for $w_i(C)$ involving not only the parameters

$n(C)$ and $w_i^\perp(C)$ but also q. More concretely, in this section, we prove the following result:

THEOREM 7.1 *Let $C \in \mathcal{C}(\mathbb{F}_q)$, $i \in I(C)$. Assume that $t(C,i) > 0$ and $r(C,i) < n(C)$. Then $r(C,i) - t(C,i) \geq \frac{1}{2q-1}(n(C)+2)$.*

Note that by Propositions 4.17 and 4.18, we have $r(C,i) = n(C) - w_i(C) + 2$ and $t(C,i) = w_i^\perp(C) - 2$, so the bound above is indeed an upper bound for $w_i(C)$ in terms of $n(C)$, $w_i^\perp(C)$ and q. But the statement highlights the fact that it is also an upper bound for the "gap" between the thresholds of the LSSS $\Sigma(C,i)$. The theorem implies that this threshold gap must grow *linearly* with $n(C)$. This bound is valid for any $C \in \mathcal{C}(\mathbb{F}_q)$, not only for $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$, and the results of this section do not assume any multiplication property of the corresponding LSSS. We need to state first the following technical lemma.

LEMMA 7.2 *Let C be a linear code over $\mathbb{F}_q$, $\emptyset \neq A \subseteq \mathcal{I}(C)$. Then*

$$\pi_A(C) = \mathbb{F}_q^{|A|} \iff \nexists \mathbf{c}^* \in C^\perp \setminus \{\mathbf{0}\} \text{ such that } \operatorname{supp} \mathbf{c}^* \subseteq A.$$

Moreover, for all $\mathbf{x} \in \pi_A(C)$, $|C_{A,\mathbf{x}}| = \frac{|C|}{|\pi_A(C)|}$.

PROOF. Note that $\pi_A(C) \subseteq \mathbb{F}_q^{|A|}$ is also a linear code over $\mathbb{F}_q$. Hence its dual code $(\pi_A(C))^\perp$ is well defined, and $(\pi_A(C))^\perp \subseteq \mathbb{F}_q^{|A|}$, too. We have

$$\pi_A(C) \neq \mathbb{F}_q^{|A|} \iff (\pi_A(C))^\perp \neq \{\mathbf{0}\} \iff \exists \mathbf{x} \in (\pi_A(C))^\perp \setminus \{\mathbf{0}\}.$$

Now note that if there exists $\mathbf{x} \in (\pi_A(C))^\perp \setminus \{\mathbf{0}\}$ then the vector $\mathbf{c}^* \in \mathbb{F}_q^{n(C)+1}$ defined by $\pi_A(\mathbf{c}^*) = \mathbf{x}, \pi_{\mathcal{I}(C)\setminus A}(\mathbf{c}^*) = \mathbf{0}$ belongs to $C^\perp \setminus \{\mathbf{0}\}$ and $\operatorname{supp} \mathbf{c}^* \subseteq A$. On the other hand if there exists $\mathbf{c}^* \in C^\perp \setminus \{\mathbf{0}\}$ such that $\operatorname{supp} \mathbf{c}^* \subseteq A$ then define $\mathbf{x} = \pi_A(\mathbf{c}^*)$. We have $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{x} \in (\pi_A(C))^\perp$ since $\mathbf{c}^*$ is in $C^\perp$ and is zero outside A. This proves the first part.

The second is a consequence of the fact that, if $C_{A,\mathbf{x}}$ is non-empty (which happens if and only if $\mathbf{x} \in \pi_A(C)$), then it is a coset of $C_{A,\mathbf{0}}$ and consequently $|C_{A,\mathbf{x}}| = |C_{A,\mathbf{0}}|$ for all $\mathbf{x} \in \pi_A(C)$. Therefore $|C_{A,\mathbf{x}}| = \frac{|C|}{|\pi_A(C)|}$ for all $\mathbf{x} \in \pi_A(C)$.

△

We proceed now to determine upper bounds for $w_i(C)$.

DEFINITION 7.3 *Write* $\theta(q) := \frac{q-1}{q}$

THEOREM 7.4 *If C is a linear code over $\mathbb{F}_q$ with $w_i^\perp(C) \neq 2$, then*

$$w_i(C) \leq 1 + \lfloor \theta(q) \cdot n(C) \rfloor.$$

PROOF. If $w_i^\perp(C) \leq 1$, then, by Lemma 4.7, $w_i(C) = 1 - w_i^\perp(C)$. Therefore, $w_i(C) \leq 1 \leq 1 + \lfloor \theta(q) \cdot n(C) \rfloor$. So assume $w_i^\perp(C) \geq 3$.

Let $S = \sum_{\mathbf{c} \in C_{i,1}} w_{Ham}(\mathbf{c})$. On the one hand $S \geq w_i(C) \cdot |C_{i,1}| = w_i(C) \cdot \frac{|C|}{q}$.

On the other hand we can rewrite S as a sum of the "contribution" of every coordinate $j \in \mathcal{I}(C)$: $S = \sum_{j \in \mathcal{I}(C)} |\{\mathbf{c} \in C_{i,1}, \pi_j(\mathbf{c}) \neq 0\}|$.

In order to compute the summands we separate several cases:

If an index $j \in \mathcal{I}(C) \setminus \{i\}$ satisfies $w_j^\perp(C) = 1$, then $w_j(C) = 0$ and every $c \in C$ satisfies $\pi_j(\mathbf{c}) = 0$ so

$$|\{\mathbf{c} \in C_{i,1}, \pi_j(\mathbf{c}) \neq 0\}| = 0.$$

Fix now $j \in \mathcal{I}(C) \setminus \{i\}$ with $w_j^\perp(C) \neq 1$ and define $A = \{i, j\}$. We will apply now Lemma 7.2. Assume there existed $\mathbf{c}^* \in C^\perp \setminus \{0\}$ with $\operatorname{supp} \mathbf{c}^* \subseteq A$. Since $w_j^\perp(C) \neq 1$, $\pi_i(\mathbf{c}^*) \neq 0$, and we could choose this word $\mathbf{c}^*$ such that $\mathbf{c}^* \in (C^\perp)_{i,1}$. But then $w_i^\perp(C) \leq 2$ which is a contradiction. Consequently, such word $\mathbf{c}^*$ does not exist, and therefore by the first part of Lemma 7.2, $\pi_A(C) = \mathbb{F}_q^2$. Now, by the second part of the same lemma,

$$|\{\mathbf{c} \in C_{i,1}, \pi_j(\mathbf{c}) = 0\}| = \frac{|C|}{q^2}.$$

It is easy to see, using the same reasoning based on Lemma 7.2 applied now to $B = \{i\}$ and considering the fact that $w_i^\perp(C) > 1$, that $|C_{i,1}| = \frac{1}{q} \cdot |C|$. Therefore

$$|\{\mathbf{c} \in C_{i,1}, \pi_j(\mathbf{c}) \neq 0\}| = \frac{(q-1)}{q^2} \cdot |C|.$$

So, for any $j \in \mathcal{I}(C) \setminus \{i\}$,

$$|\{\mathbf{c} \in C_{i,1}, \pi_j(\mathbf{c}) \neq 0\}| \leq \frac{(q-1)}{q^2} \cdot |C|.$$

Finally, we have

$$|\{\mathbf{c} \in C_{i,1}, \pi_i(\mathbf{c}) \neq 0\}| = |C_{i,1}| = \frac{1}{q} \cdot |C|.$$

Therefore $S \leq \frac{(q-1)}{q^2} \cdot |C| \cdot n(C) + \frac{1}{q} \cdot |C|$.
Therefore both inequalities for S imply

$$w_i(C) \leq 1 + \frac{(q-1)}{q} \cdot n(C)$$

and now considering $w_i(C)$ must be an integer we get the result.

It should be remarked, however, that if $w_i^{\perp}(C) = 2$, the result might not hold. For example, given any finite field $\mathbb{F}_q$, take an integer $n > 1$ and consider the code $C = \mathbb{F}_q < (1, 1, \ldots, 1) >$ such that $n(C) = n$. Then $w_i(C) = n(C) + 1 > 1 + \lfloor \theta(q) \cdot n(C) \rfloor$ for any $i \in \mathcal{I}(C)$. Note however that $w_i^{\perp}(C) = 2$ also for any $i \in \mathcal{I}(C)$.

$\triangle$

This theorem and its proof bear some similarity with the *Norse bounds* for covering radius from coding theory, see for instance [66].

In the next results, the bound obtained in the previous theorem is refined by applying this same bound to *shortened codes* constructed from C instead of the whole code C. Recall the definition of shortening C at the set $A \subseteq \mathcal{I}(C)$ (see Definition 1.10). We will assume, without loss of generality, that A is the set of the $|A|$ last indices of C. Then if D is the code that results from shortening C at A, we have $\mathcal{I}(D) = \mathcal{I}(C) \setminus A$.

LEMMA 7.5 *Let $C \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(C)$ such that $w_i^{\perp}(C) \geq 3$. Let $\emptyset \neq A \subseteq \mathcal{P}(C, i)$, with $|A| \leq w_i^{\perp}(C) - 3$. Let D be obtained from C by shortening at A. Then $D \in \mathcal{C}(\mathbb{F}_q)$ and $w_i^{\perp}(D) \geq w_i^{\perp}(C) - |A|$.*

PROOF. By Proposition 4.18, $t(C, i) = w_i^{\perp}(C) - 2$. Hence $A \in \mathcal{A}(C, i)$ and therefore there exists a word $\mathbf{w} \in C_{i,1}$, such that $\pi_A(\mathbf{w}) = \mathbf{0}$. By construction of the code D, the existence of $\mathbf{w}$ guarantees that $D_{i,1} \neq \emptyset$, so $w_i(D) \neq 0$ and $w_i^{\perp}(D) \neq 1$.

Assume now that $w_i^{\perp}(D) = 0$. Then $w_i(D) = 1$. That means there is a word $\mathbf{c} \in D$ with $\pi_i(\mathbf{c}) = 1$ and $\pi_j(\mathbf{c}) = 0$ for all $j \in \mathcal{I}(D) \setminus \{i\}$. But by construction of D, there exists a word $\mathbf{w} \in C$, with $\pi_A(\mathbf{w}) = \mathbf{0}$ and $\pi_{\mathcal{I}(C) \setminus A}(\mathbf{w}) = \mathbf{c}$. But then $w_i(C) = 1$, and this contradicts the fact that $i \in I(C)$.

Hence $w_i^{\perp}(D) > 1$ and therefore $i \in I(D)$, so $D \in \mathcal{C}(\mathbb{F}_q)$. We can define $t(D, i)$ and again by Proposition 4.18, $t(D, i) = w_i^{\perp}(D) - 2$, so we need to prove $t(D, i) \geq t(C, i) - |A|$. Fix any $B \subseteq \mathcal{I}(D) \setminus \{i\}$, such that

$|B| = t(C,i) - |A| \geq 1$. The set $A \cup B \subseteq \mathcal{I}(C)$, satisfies $|A| + |B| = t(C,i)$ so $A \cup B \in \mathcal{A}(C,i)$. Consequently, there exists $\mathbf{c} \in C_{i,1}$ with $\pi_{A\cup B}(\mathbf{c}) = \mathbf{0}$. This implies the existence of $\mathbf{w} \in D_{i,1}$ with $\pi_B(\mathbf{w}) = \mathbf{0}$ and hence $B \in \mathcal{A}(D,i)$. This proves $t(D,i) \geq t(C,i) - |A|$. △

THEOREM 7.6 *Let C be a linear code over $\mathbb{F}_q$ such that $w_i^\perp(C) \neq 2$. Then*

$$w_i(C) \leq 1 + \lfloor \theta(q) \cdot (n(C) - w_i^\perp(C) + 3) \rfloor$$

PROOF. Again we can assume $w_i^\perp(C) \geq 3$, since otherwise $w_i(C) \leq 1$ holds trivially (and $\lfloor \theta(q) \cdot (n(C) - w_i^\perp(C) + 3) \rfloor \geq 0$ always).

In fact, if $w_i^\perp(C) = 3$, the statement is exactly that of Theorem 7.4. So we can assume then that $w_i^\perp(C) > 3$. Select a set $\emptyset \neq A \subseteq \mathcal{P}(C,i)$, with $|A| \leq w_i^\perp(C) - 3$. Let D be obtained from C by shortening at A. Then $w_i^\perp(D) \geq w_i^\perp(C) - |A| \geq 3$ by Lemma 7.5.

Now, since $w_i^\perp(D) \neq 2$, one can apply Theorem 7.4 to D. Then

$$w_i(D) \leq 1 + \lfloor \theta(q) \cdot n(D) \rfloor = 1 + \lfloor \theta(q) \cdot (n(C) - w_i^\perp(C) + 3) \rfloor.$$

But clearly, $w_i(C) \leq w_i(D)$, since, by construction of the code D, for any word $\mathbf{w} \in D_{i,1}$ there is a word in $C_{i,1}$ that coincides with $\mathbf{w}$ in the indices of $\mathcal{I}(D)$ and has zeros in the rest of the indices. △

In fact we can use this theorem to give an straightforward proof of the fact that, for a fixed field $\mathbb{F}_q$, there do not exist *threshold* LSSS $\Sigma(C,i)$ with arbitrary number of shares $n(C)$ (except in the trivial cases where $t(C,i) = 0$ or $t = n(C) - 1$). Indeed, if for some $C \in \mathcal{C}(\mathbb{F}_q)$ and $i \in I(C)$, $\Sigma(C,i)$ is threshold and $t(C,i) = t$ with $t \neq 0$ and $t \neq n(C) - 1$ then $w_i^\perp(C) = t + 2 \neq 2$ and $w_i(C) = n(C) - t + 1 \neq 2$. Therefore one can apply Theorem 7.6 to both C and $C^\perp$. One obtains the bound $q \geq \max\{n(C) - t + 1, t + 2\}$, which is precisely Corollary 4.40. Note that so far the only way to prove this result was using the equivalence between "non-trivial" threshold LSSS and non-trivial MDS codes (Corollary 4.39) and then use the bounds on the length of non-trivial codes (Theorem 1.19). Actually, one can also give an alternative proof of Theorem 1.19 by applying Theorem 7.6 to an MDS code and its dual (which is also an MDS code).

PROPOSITION 7.7 *Let $C \in \mathcal{C}(\mathbb{F}_q)$, $i \in I(C)$, such that $w_i(C) > 2$ and $w_i^\perp(C) > 2$. Then*

$$w_i(C) + w_i^\perp(C) \leq \frac{2 + 2 \cdot \theta(q) \cdot (n(C) + 3)}{1 + \theta(q)}$$

PROOF. We can apply Theorem 7.6 to both C and $C^\perp$. We obtain

$$w_i(C) \leq 1 + \theta(q) \cdot (n(C) - w_i^\perp(C) + 3)$$

and

$$w_i^\perp(C) \leq 1 + \theta(q) \cdot (n(C) - w_i(C) + 3)$$

Summing both inequalities, we achieve

$$(1 + \theta(q))(w_i(C) + w_i^\perp(C)) \leq 2 + 2 \cdot \theta(q) \cdot (n(C) + 3).$$

This leads to the result. △

Now we can prove the main result of this section.

PROOF. (Proof of Theorem 7.1) Propositions 4.17 and 4.18 state that $t(C,i) = w_i^\perp(C) - 2$ and $r(C,i) = n(C) - w_i(C) + 2$. Then

$$r(C,i) - t(C,i) = n(C) - w_i(C) - w_i^\perp(C) + 4.$$

Furthermore note that $t(C,i) > 0$ implies $w_i^\perp(C) > 2$ and $r(C,i) < n(C)$ implies $w_i(C) > 2$, so we can apply the previous bound for $w_i(C) + w_i^\perp(C)$ and after some algebraic manipulation we get the result. △

7.2 First non-trivial upper bounds for $\widehat{\tau}(q)$

The previous result also implies an upper bound for $\widehat{t}(C)$.

LEMMA 7.8 *Let $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ such that $\widehat{t}(C) \geq 1$. Then*

$$3\widehat{t}(C) \leq (1 - \frac{1}{2q-1})n(C) - \frac{2}{2q-1}.$$

PROOF. Let i_s be the index where the maximum in the definition of $\widehat{t}(C)$ is attained. Then $t(C,i_s) \geq \widehat{t}(C)$ and, by Proposition 4.33, we have $r(C,i_s) \leq n(C) - 2 \cdot \widehat{t}(C)$. Then $r(C,i_s) - t(C,i_s) \leq n(C) - 3\widehat{t}(C)$. Applying Theorem 7.1 to (C,i_s), we get $r(C,i_s) - t(C,i_s) \geq \frac{1}{2q-1}(n(C)+2)$. Considering both inequalities we get the result. △

This implies a first nontrivial upper bound for $\widehat{\tau}(q)$.

THEOREM 7.9 $\widehat{\tau}(q) \leq 1 - \frac{1}{2q-1} < 1$ *for all finite field $\mathbb{F}_q$.*

In order to give a better upper bound for the parameter $\widehat{t}(C)$, some bound involving not only $w_i^{\perp}(C)$ but also $w_i(\widehat{C})$ is needed. In order to use the previous results it is convenient to bound $w_i(\widehat{C})$ in terms of $w_i(C)$ and $w_i^{\perp}(C)$. The first approach is the following.

THEOREM 7.10 *Let $C \in \mathcal{C}(\mathbb{F}_q)$ with $w_i^{\perp}(C) \geq 3$. Then:*

- *If $w_i(C) + 1 \leq w_i^{\perp}(C)$, then $w_i(\widehat{C}) = 1$.*
- *If $w_i(C) + 1 > w_i^{\perp}(C)$, then $w_i(\widehat{C}) \leq w_i(C) - w_i^{\perp}(C) + 2$.*

PROOF. Let $\mathbf{c} \in C_{i,1}$ of minimal weight, that is $w_{Ham}(\mathbf{c}) = w_i(C)$. Write $B = \text{supp } \mathbf{c} \setminus \{i\}$ and note $|B| = w_i(C) - 1$.

If $w_i(C) + 1 \leq w_i^{\perp}(C)$ (and consequently $w_i^{\perp}(C) - 2 \geq |B|$), then by Proposition 4.18, $B \in \mathcal{A}(C, i)$ and there exists a word $\mathbf{w} \in C_{i,1}$ such that $\pi_B(\mathbf{w}) = \mathbf{0}$. Take the word $\mathbf{x} = \mathbf{c} * \mathbf{w} \in \widehat{C}$. Clearly $\pi_i(\mathbf{x}) = 1$ and $\pi_j(\mathbf{x}) = 0$ for all $j \in \mathcal{P}(C, i)$ (because either $j \notin B$ and in that case $\pi_j(\mathbf{c}) = 0$ or $j \in B$ and then $\pi_j(\mathbf{w}) = 0$). So $w_i(\widehat{C}) = w_{Ham}(\mathbf{x}) = 1$.

Otherwise if $w_i(C) + 1 > w_i^{\perp}(C)$, take $A \subseteq B$, with $|A| = w_i^{\perp}(C) - 2$. By Proposition 4.18, $A \in \mathcal{A}(C, i)$ and therefore there exists a word $\mathbf{w} \in C_{i,1}$ such that $\pi_A(\mathbf{w}) = \mathbf{0}$. Now the word $\mathbf{x} = \mathbf{c} * \mathbf{w} \in \widehat{C}$ satisfies $\pi_i(\mathbf{x}) = 1$, and we have that $\pi_A(\mathbf{x}) = \mathbf{0}$ (because $\pi_A(\mathbf{w}) = \mathbf{0}$) and for any $j \in \mathcal{P}(C, i) \setminus B$, $\pi_j(\mathbf{x}) = 0$ because $\pi_j(\mathbf{c}) = 0$. So supp $\mathbf{x} \subseteq (B \setminus A) \cup \{i\}$. Then

$$w_{Ham}(\mathbf{x}) \leq 1 + |B| - |A| = w_i(C) - w_i^{\perp}(C) + 2.$$

△

REMARK 7.11 *This result is in fact a generalization of Proposition 4.33 (more precisely, of the fact that $\widehat{t}(C) \geq t$ implies $w_i(C) \geq 2t + 2$)*

This approach leads to the following bounds:

THEOREM 7.12 *Let $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $w_i^{\perp}(C) \geq 3$. Then*

$$w_i(\widehat{C}) \leq \theta(q) \cdot n(C) - (1 + \theta(q))(w_i^{\perp}(C) - 3).$$

Moreover $\widehat{t}(C) \leq \frac{\theta(q) \cdot n(C) - \theta(q) - 1}{2 + \theta(q)}$.

PROOF. $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ implies that $w_i(\widehat{C}) > 1$ and hence the second case in Theorem 7.10 must hold. So $w_i(\widehat{C}) \leq w_i(C) - w_i^{\perp}(C) + 2$ and now applying the bound in Theorem 7.6,

$$w_i(\widehat{C}) \leq \theta(q) \cdot (n(C) - w_i^{\perp}(C) + 3) - w_i^{\perp}(C) + 3 =$$

$$= \theta(q) \cdot n(C) - (1 + \theta(q))(w_i^{\perp}(C) - 3).$$

If $\widehat{t}(C) = t \geq 1$, then for the index i_s where the maximum in the definition of $\widehat{t}(C)$ is attained, $w_{i_s}^{\perp}(C) \geq t + 2 \geq 3$. So

$$w_{i_s}(\widehat{C}) \leq \theta(q) \cdot n(C) - (1 + \theta(q))(w_{i_s}^{\perp}(C) - 3).$$

Applying that $w_{i_s}(\widehat{C}) \geq t + 2$ and $w_{i_s}^{\perp}(C) \geq t + 2$, we get

$$t + 2 \leq \theta(q) \cdot n(C) - (1 + \theta(q))(t - 1).$$

The result follows from here. △

The following theorem follows by immediate application of Theorem 7.12, in combination with Definition 5.2.

THEOREM 7.13

$$\widehat{\tau}(q) \leq \frac{3\theta(q)}{2 + \theta(q)} = 1 - \frac{2}{3q - 1}$$

for all finite field $\mathbb{F}_q$.

7.3 Refinement using code shortening

While the previous approaches lead to non trivial upper bounds for $\widehat{\tau}(q)$, the following refinement will yield better bounds. It consists in applying the bounds in the previous results to a shortened code constructed from $\widehat{C}$.

LEMMA 7.14 *Let* $C \in \mathcal{C}(\mathbb{F}_q)$ *with* $w_i^{\perp}(C) \geq 3$. *Let* $\mathbf{c}$ *be a word of minimal weight* $w_i(C)$ *in* $C_{i,1}$. *Let* $A = \mathcal{I}(C) \setminus \operatorname{supp} \mathbf{c}$. *Let* M^A *be obtained by shortening* $\widehat{C}$ *at* A. *Then*

- $n(M^A) + 1 = w_i(C)$.
- $w_i(M^A) \geq w_i(\widehat{C})$.

- *If $w_i^\perp(C) \geq w_i(C) + 1$, then $w_i(\widehat{C}) = 1$.*
- *If $w_i^\perp(C) < w_i(C) + 1$, then $w_i^\perp(M^A) \geq w_i^\perp(C)$.*

PROOF. The first claim is trivial. For the second, note that, if $(M^A)_{i,1}$ is nonempty, then the claim can be easily verified, since for every $\mathbf{x} \in (M^A)_{i,1}$, the word $\mathbf{w} \in \mathbb{F}_q^{\mathfrak{k}(C)}$ given by $\pi_{\mathcal{I}(C)\setminus A}(\mathbf{w}) = \mathbf{x}$ and $\pi_A(\mathbf{w}) = \mathbf{0}$ is in $(\widehat{C})_{i,1}$ (by definition of M^A) and therefore $w_i(\widehat{C}) \leq w_i(M^A)$. Now note that $(M^A)_{i,1}$ is nonempty since we can construct the following word: Since $\mathbf{c} \in C_{i,1}$, $\pi_A(\mathbf{c}) = \mathbf{0}$, we have $\mathbf{c} * \mathbf{c} \in (\widehat{C})_{i,1}$ and $\pi_A(\mathbf{c} * \mathbf{c}) = \mathbf{0}$. Then the vector $\pi_{\mathcal{I}(C)\setminus A}(\mathbf{c} * \mathbf{c})$ belongs to $(M^A)_{i,1}$.

The third claim was proven in Theorem 7.10. As for the last one, first note that $w_i^\perp(C) - 2 < w_i(C) - 1 = n(M^A)$ and we can apply the following reasoning. Since $t(M^A, i) = w_i^\perp(M^A) - 2$ and $t(C, i) = w_i^\perp(C) - 2$ by Proposition 4.18, we need to prove that $t(M^A, i) \geq t(C, i)$.

Let $B \subseteq \mathcal{P}(M^A, i)$ with $|B| = t(C, i)$. Since $B \in \mathcal{A}(C, i)$ there is a word $\mathbf{d}$ in $C_{i,1}$ with $\pi_B(\mathbf{d}) = \mathbf{0}_B$. Now take $\mathbf{v}' = \mathbf{c} * \mathbf{d} \in (\widehat{C})_{i,1}$. Clearly this word has zeros in $A \cup B$. Therefore the vector $\mathbf{v}$ obtained by removing the coordinates in A is a word in $(M^A)_{i,1}$ such that $\pi_B(\mathbf{v}) = \mathbf{0}_B$ and consequently $B \in \mathcal{A}(M^A, i)$. Therefore $t(M^A, i) \geq t(C, i)$. △

THEOREM 7.15 *Suppose $C \in \mathcal{C}(\mathbb{F}_q)$ with $w_i^\perp(C) \geq 3$. Then*

- *$w_i(\widehat{C}) = 1$ if $w_i^\perp(C) \geq w_i(C) + 1$.*
- *$w_i(\widehat{C}) \leq 1 + \lfloor \theta(q) \cdot (w_i(C) - w_i^\perp(C) + 2) \rfloor$ if $w_i^\perp(C) < w_i(C) + 1$.*

So in particular if $C \in \mathcal{C}^\dagger(\mathbb{F}_q)$ (and $w_i^\perp(C) \geq 3$), then $w_i^\perp(C) < w_i(C) + 1$ and $w_i(\widehat{C}) \leq 1 + \lfloor \theta(q) \cdot (w_i(C) - w_i^\perp(C) + 2) \rfloor$.

PROOF. The first case has already been proven. In the second case, take A as in the previous theorem and then apply Theorem 7.6 to M^A. By Lemma 7.14, $w_i^\perp(M^A) \geq w_i^\perp(C) \geq 3$ so Theorem 7.6 applied to M^A gives

$$w_i(M^A) \leq 1 + \lfloor \theta(q) \cdot (n(M^A) - w_i^\perp(M^A) + 3) \rfloor.$$

Now Lemma 7.14 implies

$$w_i(\widehat{C}) \leq w_i(M^A) \leq 1 + \lfloor \theta(q) \cdot (n(M^A) - w_i^\perp(M^A) + 3) \rfloor \leq$$

$$\leq 1 + \lfloor \theta(q) \cdot (w_i(C) - w_i^{\perp}(C) + 2) \rfloor.$$

If $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$, by definition $w_i(\widehat{C}) > 1$, so only the second case can hold. △

REMARK 7.16 *Note that self-dual codes $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $w_i(C) \geq 3$ must satisfy $w_i(\widehat{C}) \leq 1 + \lfloor 2\theta(q) \rfloor = 2$. Therefore for any such code, we have $\widehat{t}(C) = 0$.*

THEOREM 7.17 *Let $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ and suppose $\widehat{t}(C) = t \geq 1$ and the maximum is achieved in index i_s. Then*

$$t + 2 \leq 1 + \lfloor \theta(q) \cdot (w_{i_s}(C) - t) \rfloor.$$

PROOF. By definition of $\widehat{t}(C)$, we have that $t + 2 \leq w_{i_s}(\widehat{C})$ and $t + 2 \leq w_{i_s}^{\perp}(C)$. Combining this and Theorem 7.15 (note $w_i^{\perp}(C) \geq 3$), we get

$$t+2 \leq w_{i_s}(\widehat{C}) \leq 1+\lfloor \theta(q) \cdot (w_{i_s}(C) - w_{i_s}^{\perp}(C)+2) \rfloor \leq 1+\lfloor \theta(q) \cdot (w_{i_s}(C) - t) \rfloor.$$

△

COROLLARY 7.18 *Let $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ and suppose $\widehat{t}(C) = t \geq 1$. Then*

$$t + 2 \leq 1 + \lfloor \theta(q) \cdot (1 + \lfloor \theta(q) \cdot (n(C) - t + 1) \rfloor - t) \rfloor.$$

PROOF. The first bound is obtained using Theorem 7.17 and the bound in Theorem 7.6 for $w_{i_s}(C)$, in addition to the fact that $w_{i_s}^{\perp}(C) \geq t + 2$. △

So, finally we have the following upper bound for $\widehat{\tau}(q)$.

THEOREM 7.19 *For all finite field $\mathbb{F}_q$,*

$$\widehat{\tau}(q) \leq \frac{3\theta(q)}{1 + \theta(q) + (\theta(q))^2} = 1 - \frac{3q - 2}{3q^2 - 3q + 1}.$$

PROOF. Let $\{C^{(m)}\}_{m>0} \subseteq \mathcal{C}^{\dagger}(\mathbb{F}_q)$ be an infinite family of linear codes such that $n_m = n(C^{(m)}) \xrightarrow[m\to\infty]{} \infty$ and $\widehat{\tau}(C^{(m)}) \xrightarrow[m\to\infty]{} \widehat{\tau}(q)$. By Corollary 7.18, we know that for every m, if we write $t_m = \widehat{t}(C^{(m)})$ it holds that either, $t_m = 0$ or $t_m \leq \theta(q) \cdot (1 + \theta(q) \cdot (n_m - t_m + 1) - t_m) - 1$. Since by the previous lower

bounds on $\widehat{\tau}(q)$, we know this parameter is bigger than 0, $t_m = 0$ can only happen for a finite number of m. For the rest of m, note that the inequality above can also be written as $t_m(1+\theta(q)+\theta(q)^2) \leq \theta(q)^2 n_m + (\theta(q)^2+\theta(q)-1)$. Then for those m,

$$\widehat{\tau}(C^{(m)}) = \frac{3t_m}{n_m - 1} \leq \frac{3(\theta(q)^2 n_m + \theta(q)^2 + \theta(q) - 1)}{(1+\theta(q)+\theta(q)^2)(n_m - 1)}.$$

When $m \to \infty$, $n_m \to \infty$, and the limit of the rightmost expression is $\frac{3\theta(q)^2}{1+\theta(q)+\theta(q)^2}$. Hence

$$\widehat{\tau}(q) \leq \frac{3\theta(q)^2}{1+\theta(q)+\theta(q)^2} = \frac{3(q-1)^2}{3q^2-3q+1} = 1 - \frac{3q-2}{3q^2-3q+1}$$

as can be checked by elementary algebraic manipulation. △

Finally we collect the explicit bounds for some finite fields in the following table.

q	Upper bounds
2	0.429
3	0.632
4	0.730
5	0.787
7	0.850
9	0.885
16	0.936
25	0.959
49	0.979

Table 7.1: Upperbounds

Note that for small fields $\mathbb{F}_q$ the upper bound for $\widehat{\tau}(q)$ is quite far away from 1.

Summary of the chapter: We have proved that $\widehat{\tau}(q) \leq 1 - \frac{3q-2}{3q^2-3q+1} < 1$ for *all* finite fields $\mathbb{F}_q$. The proof requires only combinatorial techniques, and does not rely on any algebraic geometric result.

Part III

Codes based on Riemann-Roch systems

Chapter 8

Riemann-Roch systems of equations

In this chapter, Riemann-Roch systems of equations are introduced. Riemann-Roch systems of equations consist of a finite number of equations defined over the class-group of a function field. There is a single *indeterminate* X for the whole system, to be viewed as an unknown divisor class. In each such equation there is a fixed scalar $m_i \in \mathbb{Z}$, and two fixed divisor classes T_i and Y_i. The i-th equation is the condition that the dimension of the Riemann-Roch space of the general affine combination $m_i X + Y_i$ does not change when the "off-set" T_i is added. More formally, $\ell(m_i X + Y_i + T_i) - \ell(m_i X + Y_i) = 0$. This concept is not entirely new. Previously, Riemann-Roch systems of equations had been used in [54, 60, 79, 81, 82, 83, 85] to construct special types of AG-codes. The desired properties of the codes are captured as a system of equations: any solution to this system yields an AG-code with those properties. The systems that appear in all these works are however of a less general type, namely $m_i = \pm 1$ for all i. Equations of this form allow us to set conditions on the code and its dual. The novelty of this work is that we will also consider systems where m_i can take (integer) values different from ± 1, for some of the equations i. This enables us to impose conditions on the *Schur product transforms* of the code as well.

In this chapter, we give a short indication of how solutions to special kinds of Riemann-Roch equations yield linear codes with special combinatorial properties (Theorem 8.5). In the sequel (Chapters 11 and 12) more specific applications are studied.

The main results in this chapter concern sufficient conditions of solvability

of Riemann-Roch systems of equations. There are different ways to ensure that a certain Riemann-Roch system of equations has a solution. For some systems, we can prove that there exists $r \in \mathbb{Z}$, such that any class of divisors of degree r is a solution to the system. However, in order to be solvable in this way, systems must satisfy certain somewhat strong properties. These sufficient conditions will be stated in Theorem 8.6.

A different approach consists on upper bounding, for each equation of the system, the number of classes of divisors of certain degree that do not satisfy that equation. This gives an upper bound on the total number of classes that do not satisfy some of the equations. We can compare this number with the number of classes of that degree (the class number) and if the former is smaller than the latter, we know that there exists a class of that degree that satisfies all of the equations. This argumentation leads to weaker sufficient conditions of solvability, stated in the main result of this chapter, Theorem 8.12.

Many of the definitions and results in this part of the thesis appeared in [16].

8.1 Definitions

Let $\mathbb{F}_q$ be a finite field and let $\mathbb{F}/\mathbb{F}_q$ be an algebraic function field.

DEFINITION 8.1 *For each $T \in \mathrm{Cl}(\mathbb{F})$, we define the map*

$$\Delta_T : \mathrm{Cl}(\mathbb{F}) \to \mathbb{Z}$$

$$X \mapsto \ell(X+T) - \ell(X).$$

REMARK 8.2 *Given a* divisor $T \in \mathrm{Div}(\mathbb{F})$, *we can also define the map Δ_T applied to divisors, i.e., $\Delta_T : \mathrm{Div}(\mathbb{F}) \to \mathbb{Z}$ by $X \mapsto \ell(X+T) - \ell(X)$. In the following, both definitions of the function Δ_T (applied to divisors and to divisor classes) will be used indistintly.*

Now a general type of systems of equations can be defined. From now on, these will be known as Riemann-Roch systems of equations.

DEFINITION 8.3 *Let $s > 0$ an integer and let $T_i, Y_i \in \mathrm{Cl}(\mathbb{F})$, $m_i \in \mathbb{Z} \setminus \{0\}$ for $i = 1, \ldots, s$. The* Riemann-Roch system of equations *in the indeterminate X is the system*

$$\{\Delta_{T_i}(m_i X + Y_i) = 0\}_{i=1}^{s}$$

determined by these data. A solution is some $G \in \mathrm{Cl}(\mathbb{F})$ *which satisfies all equations when substituted for* X*.*

REMARK 8.4 *Again, Riemann-Roch systems of equations can be defined with respect to divisors instead of classes of divisors (i.e., in the notation above,* $T_i, Y_i \in \mathrm{Div}(\mathbb{F})$*). In this case the solutions are defined as divisors (but in fact any divisor in the same class as a solution is a solution as well).*

The applications of Chapters 11 and 12 will be based on the fact that if a divisor G is a solution to a Riemann-Roch systems of equations of a certain form, then this implies some conditions on the distribution of the zeros of an algebraic geometric code $C_L(D, G)$. Although more will be explained later, we can now state the following:

THEOREM 8.5 *Let* $P_0, P_1, \ldots, P_n \in \mathbb{P}(\mathbb{F})$ *with* $P_i \neq P_j$ *for* $i \neq j$*. Write* $D = \sum_{i=0}^{n} P_i$*. Let* $G \in \mathrm{Div}(\mathbb{F})$ *be such that* $\mathrm{supp}\ G \cap \mathrm{supp}\ D = \emptyset$ *and consider the (generalized) linear code* $C := C_L(D, G)$ *over* $\mathbb{F}_q$*. For any* $A \subseteq \mathcal{I}(C)$*, we write* $P_A := \sum_{i \in A} P_i \in \mathrm{Div}(\mathbb{F})$*.*
Let $A \subseteq \mathcal{I}(C)$*,* $B \subseteq \mathcal{I}(C) \setminus A$ *such that* $\Delta_{P_B}(G - P_A - P_B) = 0$*. Then for any* $\mathbf{c} \in C$ *with* $\pi_A(\mathbf{c}) = \mathbf{0}$*, we have* $\pi_B(\mathbf{c}) = \mathbf{0}$*.*

PROOF. $\Delta_{P_B}(G - P_A - P_B) = 0$ means $\ell(G - P_A - P_B) = \ell(G - P_A)$ but, since $G - P_A - P_B \leq G - P_A$, we have $\mathcal{L}(G - P_A - P_B) = \mathcal{L}(G - P_A)$. Then for every $f \in \mathcal{L}(G)$ such that $f(P_j) = 0$ for all $j \in A$, it also happens that $f(P_i) = 0$ for all $i \in B$. Therefore one gets the result. △

8.2 Solving systems by reasoning with the degree of divisors

There are several ways to ensure the existence of a solution to a given Riemann-Roch system of equations. In some cases, the parameters of the system are such that any class of divisors of a certain degree is a solution, as we will see in this section.

THEOREM 8.6 *Consider the Riemann-Roch system of equations*

$$\{\Delta_{T_i}(m_i X + Y_i) = 0\}_{i=1}^{s},$$

Write $d_i = \deg T_i$ *and* $d'_i = \deg Y_i$ *for* $i = 1, \ldots, s$. *If there exists* $d \in \mathbb{Z}$ *such that* $m_i d + d'_i < 0$ *and* $m_i d + d_i + d'_i < 0$ *for* $i = 1, \ldots, s$, *then any class* $G \in \mathrm{Cl}(\mathbb{F})$ *with* $\deg G = d$ *is a solution to the Riemann-Roch system.*

PROOF. Let $G \in \mathrm{Cl}(\mathbb{F})$ with $\deg G = d$. Then

$$\deg m_i G + Y_i + T_i = m_i d + d_i + d'_i < 0$$

and

$$\deg m_i G + Y_i = m_i d + d'_i < 0$$

for every $i = 1, \ldots, s$ by assumption. Consequently $\ell(m_i G + Y_i + T_i) = 0$ and $\ell(m_i G + Y_i) = 0$ for every $i = 1, \ldots, s$ and

$$\Delta_{T_i}(m_i X + Y_i) = \ell(m_i G + Y_i + T_i) - \ell(m_i G + Y_i) = 0$$

for all $i = 1, \ldots, s$ so G is a solution to the system. △

The Riemann-Roch systems that we will consider in the applications in forthcoming chapters are of the kind considered in Theorem 8.5. In that case, it holds that $\deg T_i > 0$ for all the classes T_i, $i = 1, \ldots, s$ in the theorem above and we can give a simpler version of the previous theorem.

COROLLARY 8.7 *Consider the Riemann-Roch system of equations*

$$\{\Delta_{T_i}(m_i X + Y_i) = 0\}_{i=1}^{s},$$

Write $d_i = \deg T_i$ *and* $d'_i = \deg Y_i$ *for* $i = 1, \ldots, s$ *and assume* $d_i > 0$ *for all* $i = 1, \ldots, s$. *If there exists* $d \in \mathbb{Z}$ *such that* $m_i d + d_i + d'_i < 0$ *for* $i = 1, \ldots, s$, *then any class* $G \in \mathrm{Cl}(\mathbb{F})$ *with* $\deg G = d$ *is a solution to the Riemann-Roch system.*

8.3 Solvability based on the size of the torsion group $\mathrm{Cl}_0(\mathbb{F})[m]$ and the number of effective divisors

In this section we show more general sufficient conditions for a Riemann-Roch system to be solvable. The argumentation is the following: Given certain degree $r \in \mathbb{Z}$, we know $|\mathrm{Cl}_r(\mathbb{F})| = h$. For each equation of the system, there

may be a fraction of these classes in $\mathrm{Cl}_r(\mathbb{F})$ that do *not* satisfy the equation. The crucial observation is that an upper bound (which depends on r) for this number can be actually given. So the union bound can then be used to give an upper bound for the number of classes that do not satisfy *at least one* of the equations. If for some r, this number of "bad" classes is strictly smaller than h, then there is a solution in $\mathrm{Cl}_r(\mathbb{F})$ to the system.

We need to introduce the following notation.

DEFINITION 8.8 *Let* $\mathrm{Cl}^+(\mathbb{F}) := \{Y : Y \in \mathrm{Cl}(\mathbb{F})$ *and* $\exists G \in Y, G \geq 0\}$. *For any* $r \geq 0$, *let* $\mathrm{Cl}^+_r(\mathbb{F}) := \mathrm{Cl}^+(\mathbb{F}) \cap \mathrm{Cl}_r(\mathbb{F})$.

As we have remarked before, we are especially interested in the kind of Riemann-Roch systems appearing in Theorem 8.5. In those cases we have that $T_i \in \mathrm{Cl}^+(\mathbb{F})$ for all $i = 1, \ldots, s$, since the classes T_i contain sums of places of the function field, which are effective divisors. The following simplification, which can be made in that case, will be useful. If $T \in \mathrm{Cl}^+(\mathbb{F})$, then $\ell(mX + Y + T) \geq \ell(mX + Y) \geq 0$. Hence:

PROPOSITION 8.9 *Consider the Riemann-Roch system of equations*

$$\{\Delta_{T_i}(m_i X + Y_i) = 0\}_{i=1}^s.$$

Suppose that $T_i \in \mathrm{Cl}^+(\mathbb{F})$ *for* $i = 1, \ldots, s$. *Then any solution* $G \in \mathrm{Cl}(\mathbb{F})$ *to the system of equations*

$$\{\ell(m_i X + Y_i + T_i) = 0\}_{i=1}^s$$

is a solution to the above Riemann-Roch system.

PROOF. Let $i \in \{1, \ldots, s\}$. If $T_i \in \mathrm{Cl}^+(\mathbb{F})$, then clearly

$$0 \leq \ell(m_i X + Y_i) \leq \ell(m_i X + Y_i + T_i)$$

for all $X \in \mathrm{Cl}(\mathbb{F})$. Therefore if $\ell(m_i G + Y_i + T_i) = 0$ for $G \in \mathrm{Cl}(\mathbb{F})$, then also $\ell(m_i G + Y_i) = 0$ and

$$\Delta_{T_i}(m_i G + Y_i) = \ell(m_i G + Y_i + T_i) - \ell(m_i G + Y_i) = 0.$$

△

It follows from the definition of Riemann-Roch space that:

LEMMA 8.10 *$\ell(Y) > 0$ if and only if $Y \in \mathrm{Cl}^+(\mathbb{F})$*

PROOF. If $Y \in \mathrm{Cl}^+(\mathbb{F})$ there exists $G \in Y$, $G \geq 0$. Then for any element $f \in \mathbb{F}_q \setminus \{0\} \subseteq \mathbb{F}$, we have $(f) + G \geq 0$ (since $(f) = 0$) and this is equivalent to saying that $\mathbb{F}_q \subseteq \mathcal{L}(G)$, so $\ell(Y) = \ell(G) > 0$. On the other hand assume $\ell(Y) > 0$, then given a divisor $G \in Y$, there exists $0 \neq f \in \mathcal{L}(G)$, so $(f) + G \geq 0$. But the divisor $G' = (f) + G$ is also in Y and $G' \geq 0$ so $Y \in \mathrm{Cl}^+(\mathbb{F})$. △

Before we state the main result of this chapter, we introduce the following notation.

DEFINITION 8.11 *For any $m \in \mathbb{Z} \setminus \{0\}$, denote the m-*torsion subgroup *of the group $\mathrm{Cl}_0(\mathbb{F})$ as $\mathrm{Cl}_0(\mathbb{F})[m] := \{X \in \mathrm{Cl}_0(\mathbb{F}), mX = 0\}$. When $\mathbb{F}$ is clear by the context, we write $\mathrm{Cl}_0[m]$ for the sake of notation. Note that $\mathrm{Cl}_0[m] = \mathrm{Cl}_0[-m]$.*

Finally, we can state the general sufficient conditions for a Riemann-Roch system of equations of a certain form to be solvable. The conditions are in terms of the size of some of the torsion groups introduced in the previous definition and of the numbers A_{r_i} (see Definition 2.68).

THEOREM 8.12 *Consider the Riemann-Roch system of equations*

$$\{\Delta_{T_i}(m_i X + Y_i) = 0\}_{i=1}^{s},$$

where $T_i \in \mathrm{Cl}^+(\mathbb{F})$ for $i = 1, \ldots, s$. Write $d_i = \deg T_i$ and $d_i' = \deg Y_i$ for $i = 1, \ldots, s$. Let $d \in \mathbb{Z}$ and define $r_i = m_i d + d_i + d_i'$ for $i = 1, \ldots, s$. If

$$h > \sum_{i=1}^{s} A_{r_i} \cdot |\mathrm{Cl}_0[m_i]|,$$

then the Riemann-Roch system has a solution $G \in \mathrm{Cl}_d(\mathbb{F})$.

PROOF. By Proposition 8.9, it suffices to prove it for the system

$$\{\ell(m_i X + Y_i + T_i) = 0\}_{i=1}^{s}.$$

For $i = 1, \ldots, s$, argue in the following way. Define the maps

$$\phi_i : \mathrm{Cl}_d(\mathbb{F}) \to \mathrm{Cl}_{m_i d}(\mathbb{F})$$

$$X \mapsto m_i X$$

and

$$\psi_i : \mathrm{Cl}_{m_i d}(\mathbb{F}) \to \mathrm{Cl}_{r_i}(\mathbb{F})$$
$$X' \mapsto X' + Y_i + T_i.$$

Then ψ_i is clearly a bijection and each image under ϕ_i has exactly $|\mathrm{Cl}_0[m_i]|$ pre-images. This last claim is a consequence of the fact that ϕ_i is the restriction to the set $\mathrm{Cl}_d(\mathbb{F})$ of the homomorphism

$$\overline{\phi}_i : \mathrm{Cl}(\mathbb{F}) \to \mathrm{Cl}(\mathbb{F})$$

$$X \mapsto m_i X.$$

The kernel of this homomorphism is $\mathrm{Cl}_0[m_i]$ (since any preimage of 0 must have degree zero so it must be in $\mathrm{Cl}_0(\mathbb{F})$). Then every image under $\overline{\phi}_i$ has exactly $|\mathrm{Cl}_0[m_i]|$ pre-images and the same happens to the restriction ϕ_i because any preimage under $\overline{\phi}_i$ of an element in $\mathrm{Cl}_{m_i d}(\mathbb{F})$ is in $\mathrm{Cl}_d(\mathbb{F})$.

Write $\sigma_i = \psi_i \circ \phi_i$. Then, for any element $Z \in \mathrm{Cl}^+_{r_i}(\mathbb{F})$,

$$|\sigma_i^{-1}(\{Z\})| \leq |\mathrm{Cl}_0[m_i]|.$$

Hence (using $|\mathrm{Cl}^+_{r_i}(\mathbb{F})| \leq A_{r_i}$),

$$|\sigma_i^{-1}(\mathrm{Cl}^+_{r_i}(\mathbb{F}))| \leq A_{r_i} \cdot |\mathrm{Cl}_0[m_i]|.$$

Thus,

$$|\bigcup_{i=1}^{s} \sigma_i^{-1}(\mathrm{Cl}^+_{r_i}(\mathbb{F}))| \leq \sum_{i=1}^{s} A_{r_i} \cdot |\mathrm{Cl}_0[m_i]|.$$

Since

$$|\mathrm{Cl}_d(\mathbb{F})| = h > \sum_{i=1}^{s} A_{r_i} \cdot |\mathrm{Cl}_0[m_i]|,$$

there is an element

$$[G] \in \mathrm{Cl}_d(\mathbb{F}) \setminus \bigcup_{i=1}^{s} \sigma_i^{-1}(\mathrm{Cl}^+_{r_i}(\mathbb{F})).$$

Since $\sigma_i([G]) \in \mathrm{Cl}_{r_i}(\mathbb{F})$ but $\sigma_i([G]) \notin \mathrm{Cl}^+_{r_i}(\mathbb{F})$, it follows (Lemma 8.10) that $\ell(\sigma_i([G])) = 0$ for $i = 1, \ldots, s$, as desired. $\triangle$

Note that in the previous section we had already argued (Corollary 8.7) that if $r_i < 0$ for all $i = 1, \ldots, s$ then the Riemann-Roch system has a solution in $\mathrm{Cl}_d(\mathbb{F})$ (and in fact any class in $\mathrm{Cl}_d(\mathbb{F})$ would be a solution in that case). Note that we can also prove this fact as a particular case of Theorem 8.12. Indeed, assume $r_i < 0$ for all $i = 1, \ldots, s$. Then $A_{r_i} = 0$ as there cannot be positive divisors of negative degree. Since $h > 0$, the sufficient condition of Theorem 8.12 always holds in this case and consequently the system has a solution of degree d.

REMARK 8.13 *As it can be easily derived from the proof, the previous result also holds if we substitute the condition by the possibly weaker following one:*

$$h > \sum_{i=1}^{s} |\mathrm{Cl}_{r_i}^{+}| \cdot |\mathrm{Cl}_0[m_i]|$$

An open question is to determine if there are asymptotically stronger upper bounds for $|\mathrm{Cl}_{r_i}^{+}|$ than the ones that will be shown for A_{r_i}.

The following two chapters will be devoted to obtain upper bounds for the size of the parameters $A_{r_i}(\mathbb{F})$ and $|\mathrm{Cl}_0(\mathbb{F})[m_i]|$ for an algebraic function field $\mathbb{F}/\mathbb{F}_q$, which only involve the parameters $g(\mathbb{F})$, $|\mathbb{P}^{(1)}(\mathbb{F})|$ and q.

Summary of the chapter: We have introduced Riemann-Roch systems of equations. We have proved that a solution to a system of a certain form yields an algebraic geometric code with certain combinatorial properties. We have given sufficient conditions for a system to have a solution. First, we give sufficient conditions for *every* class of divisors of a certain degree to be a solution. Afterwards, we have given a more general sufficient condition for the system to have *a* solution of certain degree. This last condition depends on certain parameters of the function field $\mathbb{F}$ where the system is defined: the number A_{r_i} of positive divisors of degree r_i and $|\mathrm{Cl}_0(\mathbb{F})[m_i]|$, the size of the m_i-torsion subgroup of the degree zero divisor class group of the function field, for certain integers m_i, r_i dependant on the system.

Chapter 9

Upper bounds for effective divisors of given degree

In this chapter, we provide upper bounds for the number $A_r(\mathbb{F})$ of effective of divisors of certain fixed degree r of a function field $\mathbb{F}/\mathbb{F}_q$. These upper bounds depend on parameters of the function field such as the class number and the genus and also on the size of the finite field. The proof of these bounds uses several properties of the zeta function and L-polynomial of a function field and the Hasse-Weil Theorem. These techniques are not new, since they have been used to state similar bounds in several works (see for instance [51], [61], [81]), although the precise result stated here does not seem to have been proved before.

PROPOSITION 9.1 *Let $\mathbb{F}/\mathbb{F}_q$ be a function field with $g \geq 1$. Then, for any integer r with $0 \leq r \leq g-1$,*

$$A_r/h \leq \frac{g}{q^{g-r-1}(\sqrt{q}-1)^2}.$$

PROOF. For $i \geq 2g-1$, $A_i = \frac{h}{q-1}(q^{i+1-g}-1)$(see Lemma 5.1.4 and Corollary 5.1.11 in [75]). This has been exploited in Lemma 3 (ii) from [61], to show that

$$\sum_{i=0}^{g-2} A_i T^i + \sum_{i=0}^{g-1} q^{g-1-i} A_i T^{2g-2-i} = \frac{L(T) - hT^g}{(1-T)(1-qT)}$$

where $L(T)$ is the polynomial associated to the zeta function of $\mathbb{F}$ (Definition 2.76).

The claim from Proposition 9.1 will be derived from a relation that is obtained by taking the limit as T tends to $1/q$ on both sides of the equation above, where l'Hôpital's Rule is applied on the right hand side, then finding an expression for $L'(1/q)$ and substituting that back in.

Taking this limit,

$$\sum_{i=0}^{g-2} \frac{A_i}{q^i} + \sum_{i=0}^{g-1} \frac{A_i}{q^{g-1}} = \lim_{T \to 1/q} \frac{L(T) - hT^g}{(1-T)(1-qT)},$$

and applying l'Hôpital's rule ($(f(T))'|_{T=a}$ denotes the derivative of f evaluated at $T = a$), it follows that

$$\frac{(L(T) - hT^g)'|_{T=1/q}}{((1-T)(1-qT))'|_{T=1/q}} = \frac{L'(1/q) - gh/q^{g-1}}{-q(1-1/q)} = \frac{gh - q^{g-1}L'(1/q)}{(q-1)q^{g-1}}.$$

The term $L'(1/q)$ can be evaluated as follows. By differentiation,

$$L'(T) = \sum_{i=1}^{2g} L(T) \cdot \frac{-\alpha_i}{1 - \alpha_i T},$$

and hence,

$$L'(\frac{1}{qT}) = L(\frac{1}{qT}) \cdot \sum_{i=1}^{2g} (qT) \cdot \frac{-\alpha_i}{qT - \alpha_i}.$$

Evaluation of $L(1/q)$ is straightforward by combining the Functional Equation (see Proposition 2.77) for L-polynomials and the fact that $L(1) = h$ (see [75]). Namely,

$$L(1/q) = q^g (1/q)^{2g} L(1) = h/q^g.$$

Therefore,

$$L'(1/q) = \frac{h}{q^{g-1}} \cdot \sum_{i=1}^{2g} \frac{-\alpha_i}{q - \alpha_i}.$$

Substituting the expression for $L'(1/q)$ back in, it follows that

$$\sum_{i=0}^{g-2} \frac{A_i}{q^i} + \sum_{i=0}^{g-1} \frac{A_i}{q^{g-1}} = \frac{h}{q^{g-1}(q-1)} \cdot (g + \sum_{i=0}^{2g} \frac{\alpha_i}{q - \alpha_i}).$$

Note that, by writing it appropriately as a fraction of the other expressions in the equation, the expression between brackets on the right-most side must be a positive number. Using this and the fact $|\alpha_i| = \sqrt{q}$ for $i = 1, \ldots, 2g$ (this is Hasse-Weil Theorem, Theorem 2.80), it holds, for $0 \leq r \leq g-1$, that

$$\frac{A_r}{q^r} \leq \sum_{i=0}^{g-2} \frac{A_i}{q^i} + \sum_{i=0}^{g-1} \frac{A_i}{q^{g-1}} = \frac{h}{q^{g-1}(q-1)} \cdot |g + \sum_{i=0}^{2g} \frac{\alpha_i}{q-\alpha_i}| \leq$$

$$\leq \frac{h}{q^{g-1}(q-1)} \cdot (g + \sum_{i=0}^{2g} \frac{|\alpha_i|}{q-|\alpha_i|}) = \frac{gh}{q^{g-1}(q-1)} \cdot (1 + \frac{2}{\sqrt{q}-1}) =$$

$$= \frac{gh}{q^{g-1}(q-1)} \cdot (\frac{\sqrt{q}+1}{\sqrt{q}-1}) = \frac{gh}{q^{g-1} \cdot (\sqrt{q}-1)^2}.$$

and the claimed result follows. △

Chapter 10

Asymptotic upper bounds for r-torsion in $\mathrm{Cl}_0(\mathbb{F})$

In this chapter we obtain, for any function field $\mathbb{F}/\mathbb{F}_q$ and any integer $r \neq -1, 0, 1$, upper bounds for the size of the r-torsion subgroups $\mathrm{Cl}_0(\mathbb{F})[r]$. These numbers appeared in the sufficient condition for the existence of a solution of a Riemann-Roch system of equations given in Theorem 8.12.

Moreover, since our goal in next chapters will be to ensure the solvability of certain Riemann-Roch systems of equations in infinite families $\mathcal{F}$ of function fields, we will define and study a torsion limit that measures asymptotically the size of $\mathrm{Cl}_0(\mathbb{F})[r]$ against $g(\mathbb{F})$ for the elements $\mathbb{F} \in \mathcal{F}$.

First we will define the limit $J_r(q, a)$ that measures how small can the groups $\mathrm{Cl}_0(\mathbb{F})[r]$ be asymptotically, for the function fields $\mathbb{F}$ of a family $\mathcal{F}$ of function fields over $\mathbb{F}_q$ with Ihara's limit $A(\mathcal{F}) = a$. In the next sections, we will give upper bounds for $J_r(q, a)$ in several cases. First, we will apply classical results by Weil on the size of the torsion subgroups of abelian varieties to derive some first bounds for any r. Afterwards, we use Weil Pairing to derive tighter bounds in the case that r is a prime which does not divide $q - 1$. Finally, we use a theorem by Deuring and Shafarevich to give some improved bounds for $J_r(q, \sqrt{q} - 1)$ when q is square (recall that in the case that q is square, Ihara's constant $A(q)$ of the field is exactly $\sqrt{q} - 1$) and r equals the characteristic of $\mathbb{F}_q$.

It should be remarked that for the applications in this thesis, the interesting case is $r = 2$. In particular, the bound from Weil Pairing will not be applied (since we can only obtain bounds for fields of characteristic 2, but in this case the bounds are not better than the ones we obtain with the more

elementary approach), and the one from Deuring-Shafarevich will only be used in the case that the characteristic of the field is 2. However, proving bounds for other values of r may be interesting for future applications.

10.1 Torsion limits

In this section we will define the notion of torsion limit and give some properties.

DEFINITION 10.1 *Let $\mathbb{F}_q$ be a finite field and $a > 0$ a real number. Then $\mathfrak{F}(q,a)$ denotes the set of all asymptotically good families (see Definition 2.93) $\mathcal{F}$ over $\mathbb{F}_q$ with $A(\mathcal{F}) \geq a$.*

We define now the concept of r-torsion limit.

DEFINITION 10.2 *Let $a > 0$ a real number, $r \in \mathbb{Z}$ with $r \neq -1, 0, 1$. If $\mathfrak{F}(q,a) \neq \emptyset$, then we define*

$$J_r(q,a) := \inf_{\mathcal{F} \in \mathfrak{F}(q,a)} J_r(\mathcal{F}),$$

where if $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$,

$$J_r(\mathcal{F}) := \liminf_{m \to \infty} \frac{\log_q(|\mathrm{Cl}_0(\mathbb{F}^{(m)})[r]|)}{g(\mathbb{F}^{(m)})}.$$

For a given family $\mathcal{F}$, $J_r(\mathcal{F})$ measures (asymptotically) the logarithm of the r-torsion against the genus. The corresponding constant $J_r(q,a)$ measures, for a given Ihara limit and for given r, the "least possible r-torsion." Note that $J_r(\mathcal{F}) = J_{-r}(\mathcal{F})$, so we only consider $r > 1$ from now on.

Also note that $J_r(q,a)$ is defined (for any integer $r \neq -1, 0, 1$) if and only if $0 < a \leq A(q)$. Moreover by definition we have

REMARK 10.3 *$J_r(q,a) \leq J_r(q, A(q))$ for any $0 < a \leq A(q)$ and any integer $r > 1$.*

All the bounds proved in this chapter apply to the values $J_r(q, A(q))$ and hence are also upper bounds for $J_r(q,a)$ for any $0 < a < A(q)$. It is not known whether the actual values of $J_r(q,a)$ coincide with $J_r(q, A(q))$ for $0 < a < A(q)$.

OPEN QUESTION 10.4 *Is there any finite field $\mathbb{F}_q$, any integer $r > 1$ and any $0 < a < A(q)$ for which $J_r(q, a) < J_r(q, A(q))$?*

Moreover, we will only bound the values $J_r(q, A(q))$ for r prime (except for the bounds in Section 10.2, which are easy to state for any integer $r > 1$). In the following results, we show how to prove bounds for general r from the case where r is prime.

LEMMA 10.5 *Let $\mathbb{F}$ be a function field over $\mathbb{F}_q$ and $r > 1$ and $t \geq 1$ be integers. Then $|\mathrm{Cl}_0(\mathbb{F})[r^t]| \leq |\mathrm{Cl}_0(\mathbb{F})[r]|^t$*

PROOF. We prove this by induction on t. The result is true for $t = 1$. Assume now that it is true for $t-1$, $|\mathrm{Cl}_0(\mathbb{F})[r^{t-1}]| \leq |\mathrm{Cl}_0(\mathbb{F})[r]|^{t-1}$. Clearly $\mathrm{Cl}_0(\mathbb{F})[r] \subseteq \mathrm{Cl}_0(\mathbb{F})[r^t]$ and we can define the group homomorphism

$$\phi : \mathrm{Cl}_0(\mathbb{F})[r^t] \to \mathrm{Cl}_0(\mathbb{F})[r^{t-1}]$$

$$D \mapsto rD$$

whose kernel is $\mathrm{Cl}_0(\mathbb{F})[r]$. Then

$$|\mathrm{Cl}_0(\mathbb{F})[r^t]| = |\mathrm{Ker}\ \phi||\mathrm{Im}\ \phi| \leq |\mathrm{Cl}_0(\mathbb{F})[r]||\mathrm{Cl}_0(\mathbb{F})[r^{t-1}]| \leq |\mathrm{Cl}_0(\mathbb{F})[r]|^t$$

△

THEOREM 10.6 *Let r be an integer which factors as a product of primes as $r = \prod_{i=1}^{s} p_i^{e_i}$. Then $|\mathrm{Cl}_0(\mathbb{F})[r]| \leq \prod_{i=1}^{s} |\mathrm{Cl}_0(\mathbb{F})[p_i]|^{e_i}$ and consequently*

$$J_r(q, A(q)) \leq \sum_{i=1}^{s} e_i J_{p_i}(q, A(q))$$

PROOF. This is a consequence of the fact that $\mathrm{Cl}_0(\mathbb{F})[r]$ is isomorphic to $\bigoplus_{i=0}^{s} \mathrm{Cl}_0(\mathbb{F})[p_i^{e_i}]$ and of the previous Lemma. △

10.2 Bounds from Weil's Torsion Theorem

For function fields $\mathbb{F}$ over *algebraically closed fields*, there are classical results that allow for the computation of the size of these subgroups. We have the following result by Weil([80], see also [59, 68]):

THEOREM 10.7 (A. WEIL) *Let $\mathbb{E}$ be a function field over an algebraically closed field K of characteristic $p > 0$. Then for a positive integer $r > 1$, $|\mathrm{Cl}_0(\mathbb{E})[r]| = r^{2g}$ if r is prime to p and $|\mathrm{Cl}_0(\mathbb{E})[p]| = p^\gamma$, for some $0 \leq \gamma \leq g$.*

The following definition will be useful later

DEFINITION 10.8 *Let $\mathbb{E}$ be a function field over an algebraically closed field K of characteristic $p > 0$. The p-*rank *of $\mathbb{E}$, $\gamma(\mathbb{E})$, is defined as the integer γ such that $|\mathrm{Cl}_0(\mathbb{E})[p]| = p^\gamma$.*

We are interested in considering function fields over *finite fields*. Let $\mathbb{F}/\mathbb{F}_q$ and fix $\overline{\mathbb{F}_q}$ an algebraic closure of $\mathbb{F}_q$. Then one can consider the constant field extension $\mathbb{E}/\overline{\mathbb{F}_q}$ of $\mathbb{F}/\mathbb{F}_q$ where $\mathbb{E} = \overline{\mathbb{F}_q}\mathbb{F}$ in order to apply Weil's results.

We have the following facts, that follow from [75], Definition 3.1.8 and Theorem 3.6.3:

LEMMA 10.9 *If $\mathbb{F}$ and $\mathbb{E}$ are defined as above,*

1. *There exists an injective homomorphism $Con_{\mathbb{E}/\mathbb{F}} : \mathrm{Cl}(\mathbb{F}) \to \mathrm{Cl}(\mathbb{E})$ that preserves the degree of every element and consequently*

$$|\mathrm{Cl}_0(\mathbb{F})[r]| \leq |\mathrm{Cl}_0(\mathbb{E})[r]|$$

   for any integer $r > 1$.

2. *$g(\mathbb{E}) = g(\mathbb{F})$.*

As a consequence of this and Weil's bounds:

THEOREM 10.10 *Let $\mathbb{F}$ be a function field over $\mathbb{F}_q$ and $r > 1$ be an integer. Then $|\mathrm{Cl}_0(\mathbb{F})[r]| \leq r^{2g}$. Moreover, if $r = char(\mathbb{F}_q)$, then $|\mathrm{Cl}_0(\mathbb{F})[r]| \leq r^g$.*

The bounds in Theorem 10.10 imply the following asymptotical fact:

THEOREM 10.11 *Let $\mathbb{F}_q$ be a finite field of characteristic p and let $r > 1$. If $p \neq r$, then $J_r(q, A(q)) \leq \frac{2}{\log_r q}$. If $p = r$, then $J_r(q, A(q)) \leq \frac{1}{\log_r q}$*

10.3 Bounds from Weil Pairing

We use now properties of Weil Pairing in order to prove better bounds in some cases[1].

Let $\mathbb{F}_q$ be a finite field of characteristic p. We can associate, to every function field $\mathbb{F}$ over $\mathbb{F}_q$, an abelian variety over the algebraic closure $\overline{\mathbb{F}_q}$, its jacobian $\mathcal{J}$. We know that, for an integer r, $\mathcal{J}[r]$ is isomorphic to $(\mathbb{Z}/r\mathbb{Z})^{2g}$ if r is co-prime to p; and $\mathcal{J}[p]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^a$ for a non-negative integer $a \leq g$, where g is the dimension of $\mathcal{J}$ (see [80, 59]). This is in fact a more general way to state Theorem 10.7.

The subgroup of $\mathbb{F}_q$-rational points of this variety, $\mathcal{J}(\mathbb{F}_q)$ is isomorphic as a group to $Cl_0(\mathbb{F})$. Given an integer r which is prime to p, let $G_r \simeq \mathbb{Z}/r\mathbb{Z}$ be the group of r-th roots of unity in $\overline{\mathbb{F}_q}$. We can define Weil Pairing

$$e_r : \mathcal{J}[r] \times \mathcal{J}[r] \to G_r$$

which is a bilinear map which satisfies the following properties:

(i) $e_r(S_1 + S_2, T) = e_r(S_1, T)e_r(S_2, T)$ for all $S_1, S_2, T \in \mathcal{J}[r]$
$e_r(S, T_1 + T_2) = e_r(S, T_1)e_r(S, T_2)$ for all $S, T_1, T_2 \in \mathcal{J}[r]$;

(ii) If there exists $T \in \mathcal{J}[r]$ such that $e_r(S, T) = 1$ for all $S \in \mathcal{J}[r]$, then $T = 0$;

(iii) $e_r(S^\sigma, T^\sigma) = e_r(S, T)^\sigma$ for every $\sigma \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$.

See [58] for more information about Weil Pairings on abelian varieties.

We examine now the consequence of these properties. Let

$$\mathcal{J}(\mathbb{F}_q)[r] = \mathcal{J}[r] \cap \mathcal{J}(\mathbb{F}_q)$$

be the m-torsion subgroup of the group of $\mathbb{F}_q$-rational points of $\mathcal{J}$. The fact that e_r commutes with any element of the Galois group $Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ allows us to derive the following fact.

LEMMA 10.12 *The image of the restriction of e_r to $\mathcal{J}(\mathbb{F}_q)[r] \times \mathcal{J}(\mathbb{F}_q)[r]$ is a subgroup of G_r contained in $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. In particular, if r is a prime not dividing $q - 1$ then this image is the trivial subgroup.*

[1] I would like to thank Bas Edixhoven for suggesting this idea in the first place

PROOF. For any $S, T \in \mathcal{J}(\mathbb{F}_q)[r]$ and any $\sigma \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, we have that S and T are fixed by the action of σ, i.e., $S^\sigma = S$ and $T^\sigma = T$, but by Property (iii), $e_r(S,T) = e_r(S^\sigma, T^\sigma) = e_r(S,T)^\sigma$ so $e_r(S,T)$ is also fixed by σ and, since this holds for any $\sigma \in Gal(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, it implies $e_r(S,T) \in \mathbb{F}_q$.

Finally if r is a prime that does not divide $q-1$, the only r-th root of the unity in $\mathbb{F}_q$ is 1. Indeed, assume that $1 \neq x$ is a r-th root of the unity in $\mathbb{F}_q$. Then the subgroup of $\mathbb{F}_q^*$ generated by x has order r (since r is prime) and hence r divides the order of $\mathbb{F}_q^*$, which is $q-1$, contradicting the hypothesis. △

Now, if a certain bilinear form vanishes in certain subspace of its domain, we can bound the dimension of such subspace.

LEMMA 10.13 *For a prime r, consider an $\mathbb{F}_r$-vector space W of dimension n and a non-degenerate bilinear map e from $W \times W$ to $\mathbb{F}_r$, i.e.,*

(i) $e(\mathbf{x}+\mathbf{z}, \mathbf{y}) = e(\mathbf{x}, \mathbf{y}) + e(\mathbf{z}, \mathbf{y})$, $e(\mathbf{x}, \mathbf{y}+\mathbf{z}) = e(\mathbf{x}, \mathbf{y}) + e(\mathbf{x}, \mathbf{z})$ *for all* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in W$;

(ii) If $e(\mathbf{x}, \mathbf{u}) = 0$ *for all* $\mathbf{x} \in W$, *then* $\mathbf{u} = \mathbf{0}$.

If V is an $\mathbb{F}_r$-subspace of W such that $e(\mathbf{x}, \mathbf{y}) = 0$ for all $\mathbf{x}, \mathbf{y} \in V$, then $\dim_{\mathbb{F}_r} V \leq \frac{n}{2}$.

PROOF. Without loss of generality we can write $W = \mathbb{F}_r^n$. Then, there is a matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{F}_r)$, such that $e(\mathbf{x}, \mathbf{y}) =< \mathbf{x}A, \mathbf{y} >$ for all $\mathbf{x}, \mathbf{y} \in W$. Furthermore this matrix has rank n because e is non-degenerate, so the following is a vector space isomorphism

$$\begin{array}{rccc} \phi: & W & \to & W \\ & \mathbf{x} & \mapsto & \mathbf{x}A. \end{array}$$

Then $\phi(V)$ is a vector subspace of V and $\dim_{\mathbb{F}_r} \phi(V) = \dim_{\mathbb{F}_r} V$ because ϕ is an isomorphism. Moreover, by the assumption on V, we have $\phi(V) \subseteq V^\perp$ where $V^\perp$ denotes, as it is usual in this text, the orthogonal space to V inside W with respect to the inner product $< \cdot, \cdot >$. Then we have

$$\dim_{\mathbb{F}_r} V = \dim_{\mathbb{F}_r} \phi(V) \leq \dim_{\mathbb{F}_r} V^\perp = n - \dim_{\mathbb{F}_r} V.$$

Therefore $\dim_{\mathbb{F}_r} V \leq \frac{n}{2}$.

Actually, if e is a reflexive (symmetric or alternate) non-degenerate bilineal form, this is a well known result about the maximal dimension of isotropic subspaces of (V, e), i.e., the Witt index of e. △

COROLLARY 10.14 *Let r be a prime. If V is an $\mathbb{F}_r$-subspace of $\mathcal{J}[r]$ such that $e_r(P,Q) = 1$ for all $P, Q \in V$, then $\dim_{\mathbb{F}_r}(V) \leq g$.*

PROOF. Let ζ be a r-th primitive root of unity and consider the bilinear map $(P,Q) \mapsto r \in \mathbb{Z}/r\mathbb{Z}$, where r satisfies $\zeta^r = e_r(P,Q)$. The desired result follows from Lemma 10.13 and the fact that $\dim_{\mathbb{F}_r} \mathcal{J}[r] = 2g$. △

THEOREM 10.15 *Assume that a prime r does not divide $q-1$. Then*

$$\dim_{\mathbb{F}_r} \mathcal{J}(\mathbb{F}_q)[r] \leq g$$

PROOF. If r is the characteristic of $\mathbb{F}_q$, then it is trivial. Now assume that r is not the characteristic of $\mathbb{F}_q$. It is easy to verify that $\mathcal{J}(\mathbb{F}_q)[r]$ is an $\mathbb{F}_r$-subspace of $\mathcal{J}[r]$. By Lemma 10.12 $e_r(S,T) = 1$ for any $S, T \in \mathcal{J}(\mathbb{F}_q)[r]$ and by Corollary 10.14 $\dim_{\mathbb{F}_r} \mathcal{J}(\mathbb{F}_q)[r] \leq g$ △

We have proved

THEOREM 10.16 *Let $\mathbb{F}$ be a function field over $\mathbb{F}_q$ and r be a prime not dividing $q-1$. Then $|\mathrm{Cl}_0(\mathbb{F})[r]| \leq r^g$.*

And as a consequence we have:

THEOREM 10.17 *Let r be a prime not dividing $q-1$. Then*

$$J_r(q, A(q)) \leq \frac{1}{\log_r q}.$$

10.4 Bounds from Deuring-Shafarevich Theorem

We can improve the results in the second case of Theorem 10.11 for specific families (in fact towers) of function fields[2]. For this we use a theorem by Deuring and Shafarevich. We first need to recall some notions and results about extensions of function fields, which can also be found in [75].

[2]I would like to thank Alp Bassa and Peter Beelen for suggesting this approach

10.4.1 Algebraic extensions of function fields

Let $\mathbb{F}'|K'$ be an algebraic extension of $\mathbb{F}|K$ (recall Definition 2.94).

DEFINITION 10.18 *We say that a place $P' \in \mathbb{P}(\mathbb{F}')$ lies above $P \in \mathbb{P}(\mathbb{F})$ (or that P lies below P', or that P' is an extension of P) if $P \subseteq P'$. We write $P'|P$ to denote this fact.*

PROPOSITION 10.19 *For any $P' \in \mathbb{P}(\mathbb{F}')$, there is exactly one place of $\mathbb{F}$ lying below P', and this is given by $P = P' \cap \mathbb{F}$. For any $P \in \mathbb{P}(\mathbb{F})$, there is at least one but only finitely many places of $\mathbb{F}'$ lying above P.*

PROPOSITION 10.20 *Given an extension $P'|P$ with $P' \in \mathbb{P}(\mathbb{F}')$, $P \in \mathbb{P}(\mathbb{F})$ there exists an integer $e \geq 1$ such that $v_{P'}(x) = e \cdot v_P(x)$ for all $x \in \mathbb{F} \subseteq \mathbb{F}'$*

DEFINITION 10.21 *The integer e in the previous proposition is called the* ramification index *of the extension $P'|P$ and denoted $e(P'|P)$. We say $P'|P$ is* ramified *if $e(P'|P) > 1$,* unramified *otherwise.*

We say P is ramified if there exists at least one P' over P such that $P'|P$ is ramified, and unramified otherwise

PROPOSITION 10.22 *Let $\mathbb{F}''|K''$ be an algebraic extension of $\mathbb{F}'|K'$ and $\mathbb{F}'|K'$ be an algebraic extension of $\mathbb{F}|K$. Let $P'' \in \mathbb{P}(\mathbb{F}'')$, $P' \in \mathbb{P}(\mathbb{F}')$ and $P \in \mathbb{P}(\mathbb{F})$ such that $P''|P'$ and $P'|P$. Then $e(P''|P) = e(P''|P')e(P'|P)$.*

10.4.2 Results

If $\mathbb{F}'/K$ is an algebraic extension of $\mathbb{F}/K$ such that K is an *algebraically closed field* and certain conditions are satisfied, the theorem by Deuring and Shafarevich allows for the computation of the p-rank of $\mathbb{F}'$ (see Definition 10.8) from that of $\mathbb{F}$.

THEOREM 10.23 (DEURING-SHAFAREVICH) *Let $\mathbb{F}'|\mathbb{F}$ be a Galois extension of function fields over $\overline{\mathbb{F}}_q$ of characteristic p. Suppose that the Galois group of the extension is a p-group. Then*

$$\gamma(\mathbb{F}') - 1 = [\mathbb{F}' : \mathbb{F}](\gamma(\mathbb{F}) - 1) + \sum_{P \in \mathbb{P}(\mathbb{F})} \sum_{\substack{Q \in \mathbb{P}(\mathbb{F}') \\ Q|P}} (e(Q|P) - 1).$$

The towers for which we prove tighter bounds are in fact the Garcia-Stichtenoth towers, which we introduced in Definition 2.96. Recall (Theorem 2.97) that these towers are optimal, that is, they attain the Drinfeld-Vlăduţ bound.

Assume q is a square, and let p be the characteristic of $\mathbb{F}_q$. Consider the first Garcia-Stichtenoth tower $\mathcal{F}$ over $\mathbb{F}_q$.

All fields $\mathbb{F}$ in this tower have as field of constants the same finite field $\mathbb{F}_q$ and hence, in order to apply Deuring-Shafarevich theorem it will be necessary to consider constant field extensions of these elements over the algebraic closure $\overline{\mathbb{F}_q}$. Consequently, for each n, we define the function field $\mathbb{E}^{(n)}/\overline{\mathbb{F}_q}$ with $\mathbb{E}^{(n)} = \overline{\mathbb{F}_q}\mathbb{F}^{(n)}$. Then we have a family of function fields $\mathcal{E} = \{\mathbb{E}^{(n)}\}$ over $\overline{\mathbb{F}_q}$.

We prove the following theorem about this tower $\mathcal{E}$.

THEOREM 10.24 *The p-rank of the function field $\mathbb{E}^{(n)}$ is given by*

$$\gamma(\mathbb{E}^{(n)}) = \begin{cases} (\sqrt{q}^{n/2} - 1)^2 & \text{if } n \text{ even,} \\ (\sqrt{q}^{(n-1)/2} - 1)(\sqrt{q}^{(n+1)/2} - 1) & \text{if } n \text{ odd.} \end{cases}$$

In particular

$$\lim_{n\to\infty} \frac{\gamma(\mathbb{E}^{(n)})}{g(\mathbb{E}^{(n)})} = \frac{1}{\sqrt{q}+1}$$

PROOF.

We will apply the theorem of Deuring-Shafarevich to every extension $\mathbb{E}^{(n)}|\mathbb{E}^{(n-1)}$. First, in order to apply Deuring-Shafarevich we need some data about this extension and we can compute this from what we know of the extension $\mathbb{F}^{(n)}|\mathbb{F}^{(n-1)}$.

As $\mathbb{F}^{(n)}|\mathbb{F}^{(n-1)}$ is an *Artin-Schreier extension*, it is Galois and its Galois group is a p-group (see [75], 3.7.8(a)). Then, $\mathbb{E}^{(n)}|\mathbb{E}^{(n-1)}$ is also Galois and, since $\mathbb{F}^{(n)}$ and $\mathbb{F}^{(n-1)}$ have the same field of constants $\mathbb{F}_q$, we can apply [75], 3.6.6. to deduce that $|\mathbb{E}^{(n)} : \mathbb{E}^{(n-1)}| = |\mathbb{F}^{(n)} : \mathbb{F}^{(n-1)}|$, and therefore $|\mathbb{E}^{(n)} : \mathbb{E}^{(n-1)}| = \sqrt{q}$.

It remains to compute

$$\sum_{P' \in \mathbb{P}(\mathbb{E}^{(n-1)})} \sum_{\substack{Q' \in \mathbb{P}(\mathbb{E}^{(n)}) \\ Q'|P'}} (e(Q'|P') - 1).$$

In order to do this, we first prove some facts about the constant field extensions $\mathbb{E}^{(n-1)}|\mathbb{F}^{(n-1)}$ and $\mathbb{E}^{(n)}|\mathbb{F}^{(n)}$, since we want to apply some results about the extension $\mathbb{F}^{(n)}|\mathbb{F}^{(n-1)}$ which appeared in [37].

For every $P' \in \mathbb{P}(\mathbb{E}^{(n-1)})$ there exists exactly one place $P \in \mathbb{P}(\mathbb{F}^{(n-1)})$ below it (Proposition 10.19), and $e(P'|P) = 1$ for all such P' above P (see [75], 3.6.3(a)).

Moreover, for every $P \in \mathbb{P}(\mathbb{F}^{(n-1)})$ there exist exactly $\deg P$ places in $\mathbb{E}^{(n-1)}$ above P. To see this, fix $P \in \mathbb{P}(\mathbb{F}^{(n-1)})$ and note that

$$\deg P = \sum_{\substack{P' \in \mathbb{P}(\mathbb{E}^{(n-1)}) \\ P'|P}} e(P'|P) \deg P$$

by [75], 3.6.3(c). But $e(P'|P) = 1$ and $\mathbb{E}^{(n-1)}$ is a function field over an algebraically closed field so $\deg P' = 1$ for all $P' \in \mathbb{P}(\mathbb{E}^{(n-1)})$ (recall Remark 2.20). Therefore

$$|\{P' \in \mathbb{P}(\mathbb{E}^{(n-1)}) : P'|P\}| = \deg P.$$

All these results for $\mathbb{E}^{(n-1)}|\mathbb{F}^{(n-1)}$ also hold for the extension $\mathbb{E}^{(n)}|\mathbb{F}^{(n)}$, as well.

Let $P \in \mathbb{P}(\mathbb{F}^{(n-1)})$, $P' \in \mathbb{P}(\mathbb{E}^{(n-1)})$, $Q \in \mathbb{P}(\mathbb{F}^{(n)})$, $Q' \in \mathbb{P}(\mathbb{E}^{(n)})$ such that $Q'|Q$, $Q'|P'$, $Q|P$ and $P'|P$. Note Q' is above P and we can compute $e(Q'|P)$ in two different ways: on the one hand $e(Q'|P) = e(Q'|P')e(P'|P)$ and on the other $e(Q'|P) = e(Q'|Q)e(Q|P)$. But by the observation in the previous parragraph $e(Q'|Q) = e(P'|P) = 1$ and therefore $e(Q|P) = e(Q'|P')$.

Therefore we have:

$$\sum_{P \in \mathbb{P}(\mathbb{E}^{(n-1)})} \sum_{\substack{Q' \in \mathbb{P}(\mathbb{E}^{(n)}) \\ Q'|P'}} (e(Q'|P') - 1) = \sum_{P \in \mathbb{P}(\mathbb{F}^{(n-1)})} \sum_{\substack{Q \in \mathbb{P}(\mathbb{F}^{(n)}) \\ Q|P}} \deg P(e(Q|P) - 1)$$

This quantity was computed in [37] in order to obtain the genus of $\mathbb{F}^{(n)}$ from the genus of $\mathbb{F}^{(n-1)}$ by the use of Hurwitz' Lemma (see again [75]). We have

$$\sum_{P \in \mathbb{P}(\mathbb{F}^{(n-1)})} \sum_{\substack{Q \in \mathbb{P}(\mathbb{F}^{(n)}) \\ Q|P}} \deg P(e(Q|P) - 1) = \sqrt{q}^{\lfloor \frac{n-1}{2} \rfloor}(\sqrt{q} - 1)$$

Therefore applying Deuring-Shafarevich,

$$\gamma(\mathbb{E}^{(n)}) - 1 = \sqrt{q}(\gamma(\mathbb{E}^{(n-1)}) - 1) + \sqrt{q}^{\lfloor \frac{n-1}{2} \rfloor}(\sqrt{q} - 1)$$

Now we use that $\gamma(\mathbb{E}^{(0)}) = 0$ because $\mathbb{E}^{(0)} = \overline{\mathbb{F}_q}(x_0)$ is the rational function field over the algebraic closure of $\mathbb{F}_q$ and hence $\mathrm{Cl}_0(\mathbb{E}^{(0)}) = \{0\}$.

We apply induction and get the formula we stated for the p-rank of $\mathbb{E}^{(n)}$. The computation of the limit is straightforward. △

THEOREM 10.25 *Let $\mathbb{F}_q$ be a finite field of characteristic p. If q is square then*

$$J_p(q, \sqrt{q} - 1) \leq \frac{1}{(\sqrt{q} + 1)\log_p q}.$$

PROOF. If q is an square we may define the Garcia-Stichtenoth tower of function fields $\mathcal{F} = \{\mathbb{F}^{(n)}\}_{n\geq 0}$ over $\mathbb{F}_q$ and the tower $\mathcal{E} = \{\mathbb{E}^{(n)}\}_{n\geq 0}$ over $\overline{\mathbb{F}_q}$ containing the constant field extensions $\mathbb{E}^{(n)} = \overline{\mathbb{F}_q}\mathbb{F}^{(n)}$. We have $|\mathrm{Cl}_0(\mathbb{F}^{(n)})[p]| \leq |\mathrm{Cl}_0(\mathbb{E}^{(n)})[p]|$ for every n.

Since $|\mathrm{Cl}_0(\mathbb{E}^{(n)})[p]| = p^{\gamma(\mathbb{E}^{(n)})}$, $\log_q |\mathrm{Cl}_0(\mathbb{F}^{(n)})[p]| \leq \gamma(\mathbb{E}^{(n)}) \log_q p$. Note that also $g(\mathbb{E}^{(n)}) = g(\mathbb{F}^{(n)})$ so

$$J_p(\mathbb{F}^{(n)}) = \liminf_{n\to\infty} \frac{\log_q |\mathrm{Cl}_0(\mathbb{F}^{(n)})[p]|}{g(\mathbb{F}^{(n)})} \leq \lim_{n\to\infty} \frac{\gamma(\mathbb{E}^{(n)})}{g(\mathbb{E}^{(n)})\log_p q} = \frac{1}{(\sqrt{q}+1)\log_p q}$$

and, since $A(\mathbb{F}^{(n)}) = \sqrt{q} - 1$,

$$J_p(q, \sqrt{q} - 1) \leq \frac{1}{(\sqrt{q} + 1)\log_p q}.$$

△

To conclude, the bounds obtained in this chapter for $J_r(q, A(q))$ for r prime are enumerated next.

MAIN THEOREM 10.26 *Let $\mathbb{F}_q$ be a finite field and let $r > 1$ be a prime.*

1. *If $r \mid (q-1)$, then $J_r(q, A(q)) \leq \frac{2}{\log_r q}$.*
2. *If $r \nmid (q-1)$, then $J_r(q, A(q)) \leq \frac{1}{\log_r q}$.*
3. *If q is square and $r \mid q$, then $J_r(q, \sqrt{q} - 1) \leq \frac{1}{(\sqrt{q}+1)\log_r q}$.*

Summary of the chapter: We have defined the r-torsion limit $J_r(q,a)$ of a function field $\mathbb{F}_q$ and a real number $a \in (0, A(q)]$ which measures the ratio $\log_q(|\mathrm{Cl}_0(\mathbb{F}^{(m)})[r]|)/g(\mathbb{F}^{(m)})$ asymptotically, that is, for families $\mathcal{F}$ of function fields $\mathbb{F}^{(m)}$ with $g(\mathbb{F}^{(m)}) \to \infty$ and Ihara's limit $A(\mathcal{F}) \geq a$. Then we have given upper bounds for the values $J_r(q,a)$ in different scenarios using algebraic geometric results. First, we have used some classical results by Weil to upper bound $|\mathrm{Cl}_0(\mathbb{F})[r]|$ as a function of $g(\mathbb{F})$ and derived upper bounds for $J_r(q,a)$ for any r, q, a from there. Afterwards we have used Weil Pairing and the restriction of the dimension of a self orthogonal subspace to derive bounds in the case where r is a prime and does not divide $q-1$. Finally, we have used Deuring-Shafarevich p-rank formula for algebraic extensions of function fields to prove bounds for specific families of function fields (Garcia Stichtenoth towers) which imply upper bounds for $J_r(q, A(q))$ in the case that r is prime.

Chapter 11

Application 1: Improved lower bounds on $\widehat{\tau}(q)$ for q small

In this chapter we use the results of Chapters 8, 9 and 10 to deduce new lower bounds for $\widehat{\tau}(q)$ which, for small values of q, are better than the ones obtained in Part II. First, we show how to pose Riemann-Roch systems of equations whose solutions yield algebraic geometric codes with large corruption tolerance. We find out that if we apply the degree based conditions for the solvability of these systems that were explained in Chapter 8.2 we obtain precisely the lower bounds for $\widehat{\tau}(q)$ of [20]. However, as we have seen in Chapter 8.3, we can argue about the solvability of a Riemann-Roch system in a more general way. We can then combine these results with the upper bounds given in Chapters 9 and 10 and derive the new lower bounds $\widehat{\tau}(q)$.

11.1 Codes with large corruption tolerance from solutions to Riemann-Roch systems

Given an AG-code $C = C_L(D, G)$ over $\mathbb{F}_q$, a straightforward application of Theorem 8.5 is that one can pose a Riemann-Roch system of equations such that, if G is a solution for that system, then $w_i(C)$ is large. The same can be done for the dual of this code (which is also an AG whose parameters are known) and for $\widehat{C}$, using the fact that $\widehat{C} \subseteq C_L(D, 2G)$. Hence one has a Riemann-Roch set of equations in such a way that, given a solution G, the secret sharing scheme $\Sigma(C)$ defined from the code $C = C_L(D, G)$ has t-strong multiplication for large t. This is done in the next theorem.

THEOREM 11.1 *Let $\mathbb{F}/\mathbb{F}_q$ be an algebraic function field. Let $t, N \in \mathbb{Z}$ with $N > 1$ and $1 \leq t \leq N$. Suppose there are $P_0, P_1, \ldots, P_N \in \mathbb{P}^{(1)}(\mathbb{F})$ with $P_i \neq P_j$ for $i \neq j$. Write $D = \sum_{i=1}^{N} P_i + P_0 \in \mathrm{Div}(\mathbb{F})$ and $\mathcal{I}^* = \{1, \ldots, N\}$. For $A \subset \mathcal{I}^*$ with $A \neq \emptyset$, define $P_A = \sum_{j \in A} P_j$. Let $K \in \mathrm{Div}(\mathbb{F})$ be a canonical divisor. If the system*

$$\{\Delta_{P_0}(-X + K + P_A) = 0,\ \Delta_{P_0}(2X - D + P_A) = 0\}_{A \subset \mathcal{I}^*, |A| = t}$$

has some solution, then there is a solution $G \in \mathrm{Div}(\mathbb{F})$ such that $\mathrm{supp}\ G \cap \mathrm{supp}\ D = \emptyset$, and that the code $C = C_L(D, G)$ satisfies $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$, $n(C) = N$ and $\widehat{t}(C) \geq t$.

PROOF. If there is a solution, then any divisor in its class of equivalence is also a solution and by the Weak Approximation Theorem (Corollary 2.47) such solution $G \in \mathrm{Div}(\mathbb{F})$ can be selected such that $\mathrm{supp}\ G \cap \mathrm{supp}\ D = \emptyset$.

We can now define $C = C_L(D, G)$. We show that $w_0^{\perp}(C) \geq t + 2$ and $w_0(\widehat{C}) \geq t + 2$.

The code $C^{\perp}$ equals $C_L(D, G')$ with $G' = K - G + D$ for a canonical divisor K such that $\mathrm{supp}\ G' \cap \mathrm{supp}\ D = \emptyset$. We can assume that this is the canonical divisor that appears in the definition of the system, as any other canonical divisor is in the same class of equivalence and defines a system with the same solutions.

Let $A \subseteq \mathcal{I}^*$ with $|A| = t$. Let $A^c = \mathcal{I}^* \setminus A$ (so we can write $D = P_A + P_{A^c} + P_0$). Note that

$$\Delta_{P_0}(K - G + P_A) = \Delta_{P_0}(K - G + D - P_{A^c} - P_0) = \Delta_{P_0}(G' - P_{A^c} - P_0).$$

Hence, by Theorem 8.5 (applied to $C^{\perp}$), $\Delta_{P_0}(K - G + P_A) = 0$ implies there is no word $\mathbf{c} \in (C^{\perp})_{0,1}$ with $\pi_{A^c}(\mathbf{c}) = \mathbf{0}$ so $A \notin \Gamma(C, 0)$ (see Definition 4.11) and consequently $A \in \mathcal{A}(C, 0)$. This holds for all $A \subseteq \mathcal{I}^*$ with $|A| = t$. Hence $t(C, 0) \geq t$ and Proposition 4.18 implies $w_0(C^{\perp}) \geq t + 2$.

The proof that $w_0(\widehat{C}) \geq t + 2$ is obtained as follows. First, note that $\widehat{C} \subset C_L(D, 2G)$, so it is enough to prove $w_0(C_L(D, 2G)) \geq t + 2$. For all $A \subseteq \mathcal{I}^*$ with $|A| = t$, we can write the condition $\Delta_{P_0}(2G - D + P_A) = 0$ as

$$\Delta_{P_0}(2G - P_0 - \sum_{i \in A^c} P_i) = 0$$

and by Theorem 8.5 this means there is no word $\mathbf{c} \in (C_L(D, 2G))_{0,1}$ with $\pi_{A^c}(\mathbf{c}) = \mathbf{0}$. This holds for any $A \subseteq \mathcal{I}^*$ with $|A| = t$, and therefore we have $w_0(C_L(D, 2G)) \geq t + 2$. △

In Chapter 8 we have given some sufficient conditions in order to ensure the existence of solutions to general Riemann-Roch systems of equations. We will now combine those conditions with Theorem 11.1 to obtain sufficient conditions for the existence of codes with a certain corruption tolerance. We start by applying the degree based reasoning in Section 8.2 (Corollary 8.7), and we will find out that this leads to the lower bounds for $\widehat{\tau}(q)$ from [20], which were described in Chapter 5.2.

THEOREM 11.2 *Let $\mathbb{F}/\mathbb{F}_q$ be an algebraic function field. Let $t, N \in \mathbb{Z}$ with $N > 1$ and $1 \leq t \leq N < |\mathbb{P}^{(1)}(\mathbb{F})|$. If there exists $d \in \mathbb{Z}$ such that $d > 2g+t-1$ and $2d < N - t$, then there exists $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$, with $n(C) = N$, $\widehat{t}(C) \geq t$ and consequently $\widehat{\tau}(C) \geq \frac{3t}{N-1}$.*

Now it is not hard to verify that there exists an integer d satisfying the conditions of this theorem if and only if $N \geq 4g + 3t + 1$ (as in this case we can take $d = 2g + t$). If we take $N = 4g + 3t + 1$ we get exactly Theorem 5.8. Note again that this imposes the restriction $|\mathbb{P}^{(1)}(\mathbb{F})| \geq 4g + 3t + 2$ on the parameters of the function field in order to be able to prove $\widehat{t}(C) \geq t$.

Now we use Theorem 8.12, which provides more general sufficient conditions for the existence of a solution to a general Riemann-Roch set of equations, in the particular case of the system in Theorem 11.1. We get:

THEOREM 11.3 *Let $\mathbb{F}/\mathbb{F}_q$ be an algebraic function field. Let $t, N \in \mathbb{Z}$ with $N > 1$ and $1 \leq t \leq N$. Suppose there are $P_0, P_1, \ldots, P_N \in \mathbb{P}^{(1)}(\mathbb{F})$ with $P_i \neq P_j$ for $i \neq j$. Let $d \in \mathbb{Z}$ and define $r_1 = 2g-d+t-1$ and $r_2 = 2d-N+t$. If*

$$h > \binom{N}{t}(A_{r_1} + A_{r_2} \cdot |\mathrm{Cl}_0[2]|),$$

then there exists $G \in \mathrm{Div}_d(\mathbb{F})$ such that $C = C_L(D, G) \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$, $n(C) = N$, and $\widehat{t}(C) \geq t$

The results of Theorem 11.2 are obtained if we impose that both $r_1 < 0$ and $r_2 < 0$. Note that in that case the condition $h > \binom{N}{t}(A_{r_1} + A_{r_2} \cdot |\mathrm{Cl}_0[2]|)$ in Theorem 11.3 is automatically fulfilled since $A_{r_1} = A_{r_2} = 0$. But on the other hand, in order to be able to select an integer d such that $r_1 < 0$, $r_2 < 0$, we have to impose some restrictions on the parameters of the function field and the integer t for which we prove $\widehat{t}(C) \geq t$. Concretely, as we have said, we need that $|\mathbb{P}^{(1)}(\mathbb{F})| \geq 4g + 3t + 2$.

Alternatively, we can accept that $r_1 \geq 0$ or $r_2 \geq 0$ and then we eliminate this restriction on $|\mathbb{P}^{(1)}(\mathbb{F})|$. However, this also means that the condition $h > \binom{N}{t}(A_{r_1} + A_{r_2} \cdot |\mathrm{Cl}_0[2]|)$ may in principle not be satisfied. Still, using the upper bounds for A_{r_1} and A_{r_2} given in Chapter 9 and the ones for $|\mathrm{Cl}_0[2]|$ given in Chapter 10 we can in turn give some sufficient conditions for this to hold.

11.2 The improved lower bounds

In this section we use the upper bounds given in Chapters 9 and 10 in order to give sufficient conditions that imply the ones in Theorem 11.3 in the cases where it does not hold that both $r_1, r_2 < 0$. As we shall see this leads to new lower bounds for $\widehat{\tau}(q)$.

11.2.1 Results from the bounds in Chapter 9 and 10

We will assume now that *both* $r_1 \geq 0$ and $r_2 \geq 0$. The other two cases $r_1 < 0, r_2 \geq 0$ and $r_1 \geq 0, r_2 < 0$ will be examined afterwards. In order to impose new restrictions that imply the conditions of Theorem 11.3 we use the bounds for the number of positive divisors of degrees r_1 and r_2 and torsion bounds for $|\mathrm{Cl}_0[2]|$ which were obtained in Chapters 9 and 10. We get:

COROLLARY 11.4 *Let $\mathbb{F}/\mathbb{F}_q$ be an algebraic function field. Let $t, N \in \mathbb{Z}$ with $N > 1$ and $1 \leq t \leq N$. Assume there are $P_0, P_1, \ldots, P_N \in \mathbb{P}^{(1)}(\mathbb{F})$ with $P_i \neq P_j$ for $i \neq j$. Assume also that there exists $d \in \mathbb{Z}$ such that if we define $r_1 = 2g - d + t - 1$ and $r_2 = 2d - N + t$, the following conditions hold:*

1. $0 \leq r_1, r_2 \leq g - 1$,
2. $\binom{N}{t} \frac{g}{q^{g-r_1-1}(\sqrt{q}-1)^2} < \frac{1}{2}$, *and*
3. $\binom{N}{t} \frac{g}{q^{g-r_2-1}(\sqrt{q}-1)^2} \cdot |\mathrm{Cl}_0[2]| < \frac{1}{2}$.

Then there exists $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $n(C) = N$ and $\widehat{t}(C) \geq t$.

PROOF. If $0 \leq r_1 \leq g - 1$ and $0 \leq r_2 \leq g - 1$ then we can apply the bounds in Proposition 9.1 to conclude that $A_{r_1}/h \leq \frac{g}{q^{g-r_1-1}(\sqrt{q}-1)^2}$ and

$A_{r_2}/h \leq \frac{g}{q^{g-r_2-1}(\sqrt{q}-1)^2}$. Then

$$(A_{r_1} + A_{r_2} \cdot |\mathrm{Cl}_0[2]|) \leq \frac{gh}{q^{g-r_1-1}(\sqrt{q}-1)^2} + \frac{gh}{q^{g-r_2-1}(\sqrt{q}-1)^2} \cdot |\mathrm{Cl}_0[2]|.$$

Using assumptions 2) and 3) we get $\binom{N}{t}(A_{r_1} + A_{r_2} \cdot |\mathrm{Cl}_0[2]|) < h$. Finally we apply Theorem 11.3 to get the result. △

REMARK 11.5 *If $2g \geq (\sqrt{q}-1)^2$, then 2) and 3) imply 1) in Corollary 11.4.*

We will now analyze the asymptotical implications of this result. The following known lemma, which can be found in [53], will be helpful.

LEMMA 11.6 *Let $n \in \mathbb{N}$ and $0 < \tau < \frac{1}{2}$ be a real number. Then*

$$\binom{n}{\lfloor \tau n \rfloor} \leq \sum_{k=0}^{\lfloor \tau n \rfloor} \binom{n}{k} \leq 2^{H_2(\tau)n}$$

where $H_2(\cdot)$ denotes the binary entropy (see Definition 1.29).

Now we can state the main theorem of this section, which provides new lower bounds for $\widehat{\tau}(q)$ for some finite fields $\mathbb{F}_q$. They depend on torsion limits $J_2(q, A)$(see Definition 10.2) with $0 < A \leq A(q)$. We can use the upper bounds for these torsion limits given in Chapter 10 in order to state explicit lower bounds for $\widehat{\tau}(q)$.

THEOREM 11.7 *Let $\mathbb{F}_q$ be a finite field. If there exists $0 < A \leq A(q)$ such that $A > 1 + J_2(q, A)$, then $\widehat{\tau}(q) \geq 3\tau$ for any $\tau \in [0, 1]$ with*

$$\tau + \frac{H_2(\tau)}{\log q} < \frac{1}{3}(1 - \frac{1 + J_2(q, A)}{A}).$$

Hence, if q is a square and $q \geq 9$, then $\widehat{\tau}(q) \geq 3\tau$ for any τ such that

$$\tau + \frac{H_2(\tau)}{\log q} < \frac{(\sqrt{q}-2)\log q - 2}{3(\sqrt{q}-1)\log q}.$$

If, in addition, $q = 4^e$, $e \in \mathbb{Z}_{>1}$, then $\widehat{\tau}(q) \geq 3\tau$ for any τ with

$$\tau + \frac{H_2(\tau)}{\log q} < \frac{(q-\sqrt{q}-2)\log q - 1}{3(q-1)\log q}.$$

PROOF. Let $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$ be an infinite family of algebraic function fields over $\mathbb{F}_q$ with $g(\mathbb{F}^{(m)}) \to \infty$ such that $A(\mathcal{F}) \geq A$ and $J_2(\mathcal{F}) = J_2(q, A)$ (recall Definitions 2.93 and 10.2). Write $J = J_2(\mathcal{F})$. Fix some real number τ satisfying the hypothesis. Define $g_m = g(\mathbb{F}^{(m)})$, $j_m = \log_q(|\mathrm{Cl}_0(\mathbb{F}^{(m)})[2]|)$ and $d_m = \lfloor \delta g_m \rfloor$, where $\delta = 1 + \frac{A-1-J}{3}$. Also define N_m an integer with $N_m \leq |\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| - 1$ to be determined later and $t_m = \lfloor \tau N_m \rfloor$. Define $(r_1)_m = 2g_m - d_m + t_m - 1$ and $(r_2)_m = 2d_m - N_m + t_m$. The goal is to prove that for all sufficiently large m we can apply Corollary 11.4 to $\mathbb{F}^{(m)}$, N_m and d_m. We only need to verify conditions 2) and 3) which can be written as

$$2)\ \log_q \binom{N_m}{t_m} + (r_1)_m - g_m + 1 < \log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right)$$

and

$$3)\ \log_q \binom{N_m}{t_m} + (r_2)_m - g_m + j_m + 1 < \log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right).$$

We have $\delta g_m - 1 \leq d_m \leq \delta g_m$ and since $\tau < \frac{1}{2}$ (which is ensured by the condition on τ), $\log_q \binom{N_m}{t_m} < \frac{H_2(\tau)}{\log q} N_m$. Fix any $0 < \epsilon \in \mathbb{R}$ such that

$$\frac{H_2(\tau)}{\log q} + \tau < \frac{1}{3} - \frac{1+J}{3A} - \frac{4\epsilon}{A}.$$

For large enough m, by definition of J, $j_m < (J+\epsilon)g_m$, and by elementary calculus $\log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right) > -\epsilon g_m$. Moreover by definition of A we can take $(A-\epsilon)g_m < N_m < Ag_m$. Then

$$\log_q \binom{N_m}{t_m} + (r_1)_m - g_m + 1 = \log_q \binom{N_m}{t_m} + g_m - d_m + t_m <$$

$$< \left(\frac{H_2(\tau)}{\log q} + \tau\right) N_m + (1-\delta)g_m < \left(\frac{1}{3} - \frac{1+J}{3A} - \frac{4\epsilon}{A}\right) A g_m + (1-\delta)g_m$$

and using $\delta = 1 + \frac{A-1-J}{3}$,

$$\log_q \binom{N_m}{t_m} + g_m - d_m + t_m < \left(\frac{A}{3} - \frac{1+J}{3} - 4\epsilon\right) g_m - \frac{A-1-J}{3} g_m =$$

$$= -4\epsilon g_m < \log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right).$$

On the other hand,

$$\log_q \binom{N_m}{t_m} + (r_2)_m - g_m + j_m + 1 = \log_q \binom{N_m}{t_m} + 2d_m - N_m + t_m - g_m + j_m + 1 <$$

$$< (\frac{H_2(\tau)}{\log q} + \tau)N_m - N_m + 2\delta g_m + (J+\epsilon)g_m - g_m + 1 <$$

$$< (\frac{1}{3} - \frac{1+J}{3A} - \frac{4\epsilon}{A})Ag_m - (A-\epsilon)g_m + 2\delta g_m + (J+\epsilon)g_m - g_m + 1 =$$

$$= (-\frac{2A}{3} + \frac{2J}{3} + 2\delta - \frac{4}{3} - 2\epsilon)g_m + 1.$$

Since $2\delta = 2 + \frac{2(A-1-J)}{3} = \frac{4}{3} + \frac{2A-2J}{3}$,

$$\log_q \binom{N_m}{t_m} + (r_2)_m - g_m + j_m + 1 < -2\epsilon g_m + 1 < \log_q \left(\frac{(\sqrt{q}-1)^2}{2g_m} \right).$$

Then Corollary 11.4 can be applied, and there exists a sequence of codes $C^{(m)}$ with $n(C^{(m)}) = N_m \to \infty$ and $\widehat{t}(C^{(m)}) \geq t_m$. Clearly this implies $\widehat{\tau}(q) \geq 3\tau$. This proves the first part of the theorem.

Now if $A(q) > 1 + J_2(q, A(q))$, we have $\widehat{\tau}(q) \geq 3\tau$ for any $\tau \in [0,1]$ with

$$\tau + \frac{H_2(\tau)}{\log q} < \frac{1}{3}(1 - \frac{1 + J_2(q, A(q))}{A(q)}).$$

Assume q is square. Applying that, in this case, $A(q) = \sqrt{q} - 1$, and using the upper bounds for $J_2(q, \sqrt{q}-1)$ obtained in Chapter 10.4, we find that $A(q) > 1 + J_2(q, A(q))$ for all q square, $q \geq 9$ and we can derive the explicit bounds in the statement.

△

11.2.2 Combining the bound in Chapter 9 and the large degree strategy

We examine now the intermediate case between the results in Chapter 5 and Section 11.2.1 where we impose that one of the integers r_1, r_2 in the formula of Theorem 11.3 is negative, while the other is positive. It turns out that the case $r_1 < 0$ and $r_2 \geq 0$ does not provide new lower bounds for $\widehat{\tau}(q)$ for any field, at least with the techniques we use. Hence we will study the case where $r_1 \geq 0$ and $r_2 < 0$.

First we rewrite Theorem 11.3 in the case that we already assume $r_2 < 0$.

THEOREM 11.8 *Let $t, N \in \mathbb{Z}$ with $N > 1$ and $1 \leq t \leq N$. Suppose there exist $P_0, P_1, \ldots, P_N \in \mathbb{P}^{(1)}(\mathbb{F})$ and let K be a canonical divisor. Let $d \in \mathbb{Z}$. If*

$$2d < N - t$$

and

$$h > \binom{N}{t} A_{r_1}$$

where $r_1 = 2g - d + t - 1$ then the Riemann-Roch system of equations

$$\{\Delta_{P_0}(-X + K + P_A) = 0,\ \Delta_{P_0}(2X - D + P_A) = 0\}_{A \subset \mathcal{I}^*, |A| = t}$$

has a solution $G \in \mathrm{Cl}_d$

PROOF. By Theorem 11.3, it is enough to verify that

$$h > \binom{N}{t}(A_{r_1} + A_{r_2} \cdot |\mathrm{Cl}_0[2]|)$$

where $r_2 = 2d - N + t$. But since now we are assuming $2d < N - t$, we have that $r_2 < 0$ and $A_{r_2} = 0$. Since by assumption, $h > \binom{N}{t} A_{r_1}$, then also $h > \binom{N}{t}(A_{r_1} + A_{r_2} \cdot |\mathrm{Cl}_0[2]|)$. Hence we apply Theorem 11.3. △

We assume now also that $r_1 \geq 0$. A sufficient condition for the fact that $h > \binom{N}{t} A_{r_1}$ can be given by using the bounds for the number of positive divisors of degree r_1.

THEOREM 11.9 *Let $t, N \in \mathbb{Z}$ with $N > 1$ and $1 \leq t \leq N$. Let $d \in \mathbb{Z}$ and define $r_1 = 2g - d + t - 1$. Suppose that*

1. $0 \leq r_1 \leq g - 1$,
2. $\binom{N}{t} \frac{g}{q^{g - r_1 - 1}(\sqrt{q} - 1)^2} < 1$, *and*
3. $2d < N - t$.

Then there is a code $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ such that $n(C) = N$, $\widehat{t}(C) \geq t$

Therefore, we have again basically two conditions that we need to verify in order to apply this theorem. Condition 2) (together with 1)) implies $h > \binom{N}{t} A_{r_1}$ and Condition 3) implies $r_2 < 0$. Note also that in this case we do not need to use the upper bounds for $|\mathrm{Cl}_0(\mathbb{F})[2]|$.

Finally, using the same techniques as in Section 11.2.1, we derive lower bounds for $\widehat{\tau}(q)$.

THEOREM 11.10 *Let $\mathbb{F}_q$ be a finite field with Ihara's constant $A(q) > 2$. For any $\tau \in (0, 1]$ with*

$$3\tau + 2\frac{H_2(\tau)}{\log q} < 1 - \frac{2}{A(q)}$$

we have $\widehat{\tau}(q) \geq 3\tau$.

In particular, if q is a square, for any $\tau \in (0, 1]$ with

$$3\tau + 2\frac{H_2(\tau)}{\log q} < 1 - \frac{2}{\sqrt{q} - 1}$$

we have $\widehat{\tau}(q) \geq 3\tau$.

PROOF. This result is proved in a similar way to Theorem 11.7. We can prove that there exists a family $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m\in\mathbb{N}}$ of algebraic function fields over $\mathbb{F}_q$ such that $g(\mathbb{F}^{(m)}) \to \infty$, $A(\mathcal{F}) = A(q)$ and that for any m sufficiently large, if we take $N_m = |\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| - 1$ (we know this value is asymptotically close to $A(\mathcal{F})g(\mathbb{F}^{(m)})$) and $t_m = \lfloor \tau N_m \rfloor$, there exists an integer d_m such that the conditions in Theorem 11.9 are satisfied.

△

REMARK 11.11 *The most remarkable difference between Theorems 11.7 and 11.10 is that in the latter, the bounds do not involve the value of the torsion limits $J_2(q, A)$. However, note that in order to apply Theorem 11.10, we require that $A(q) > 2$, while Theorem 11.7 requires the weaker condition $A(q) > 1 + J_2(q, A(q))$ (more precisely, we only require $A > 1 + J_2(q, A)$ for some $0 < A \leq A(q)$). Moreover, as we will see next, Theorem 11.7 gives the best lower bounds for $\widehat{\tau}(q)$ than Theorem 11.10 for many small finite fields $\mathbb{F}_q$ and consequently, the best lower bounds on $\widehat{\tau}(q)$ given in this text depend in many cases on the value of the* torsion limit *$J_2(q, A(q))$.*

11.3 Comparison with the lower bounds from Part II

The first two columns of Table 11.1 collect the bounds for $\widehat{\tau}(q)$ for small fields that follow from Theorem 11.7 and Theorem 11.10, respectively. For very

q	New lower bounds from Theorem 11.7	New lower bounds from Theorem 11.10	Prev. lower bounds ([20], Th. 5.9)	Upper bounds
2	**0.034**(*)	0.033(*)	0.028(*)	*0.429*
3	0.057(*)	**0.059**(*)	0.056(*)	*0.632*
4	**0.104**(*)	0.099(*)	0.086(*)	*0.730*
5	**0.107**(*)	0.099(*)	0.093(*)	*0.787*
7	**0.150**(*)	0.149(*)	0.111(*)	*0.850*
9	0.172(!)	**0.178**(*)	0.167(*)	*0.885*
16	**0.298**	0.224(!)	0.244(*)	*0.936*
25	**0.323**	0.298	0.278(*)	*0.959*
49	**0.450**	0.449	0.333	*0.979*
64	**0.521**	0.498	0.429	*0.984*
81	0.520	**0.536**	0.500	*0.988*
121	0.568	0.592	**0.600**	*0.990*

Table 11.1: Lower bounds

small fields $\mathbb{F}_q$, we cannot use directly the theorems on $\mathbb{F}_q$ and the results are a consequence of applying them in an extension field $\mathbb{F}_{q^k}$ and then using the descent method from Chapter 6. The entries of the two first columns corresponding to these cases are denoted with the symbol (*). We always descend from the extension $\mathbb{F}_{q^2}$, except when $q = 4$, where we descend from $\mathbb{F}_{64}$

In some special cases, even though direct application of Theorem 11.7 does give non trivial lower bounds, stronger ones are obtained if we apply this result to an extension field and then use the field descent method. We use the symbol (!) to mark these cases in the table. Again, we apply the descent method to the extension $\mathbb{F}_{q^2}$ in these cases.

These bounds are compared with the ones in Theorem 6.14, which appear in the third column of Table 11.1. Recall that these bounds result from applying the more elementary reasoning in [20], as described in Chapter 5, combined also with the field descent in some cases, which we also mark in the table with the symbol (*).

The best bound obtained for each finite field is highlighted in boldface. Note that in the case of $\mathbb{F}_{121}$, the best bound is obtained via the "old" approach of [20] and in fact this happens for all larger fields of square cardinality. So the improvements of $\widehat{\tau}(q)$ in this section are achieved for *small* values of q. Also note that the bounds in Theorem 11.7, which depend on the upper

bounds for the torsion limit $J_2(q, A(q))$, are tighter than the ones in Theorem 11.10, which do not depend on the value of this torsion limit. Therefore, proving better upper bounds for $J_2(q, A(q))$ would improve the best known lower bounds for $\widehat{\tau}(q)$ in many cases.

In the last column of Table 11.1 the upper bounds for $\widehat{\tau}(q)$ obtained in Chapter 7 are enumerated in italics.

Note that the techniques in this chapter allow for the obtention of direct algebraic geometric constructions over some fields (q square, $9 \leq q < 49$) for which it was previously necessary to use the field descent method.

Summary of the chapter: We have posed certain Riemann-Roch systems of equations whose solutions yield algebraic geometric code with a certain corruption tolerance. We have combined this fact with the conditions of solvability of Riemann-Roch systems of equations found in Chapter 8 in order to find sufficient conditions for the existence of linear codes with a given corruption tolerance. We have found out that one of the two approaches in Chapter 8, the "degree-based conditions of solvability" of Section 8.2 lead to the results of [20]. We have then studied the application to this problem of the more general conditions of system solvability in Section 8.3. Combining them with the bounds in Chapters 9 and 10, we have found new lower bounds for $\widehat{\tau}(q)$, which are better than the bounds of [20] for some finite fields. We have compared all lower and upper bounds for $\widehat{\tau}(q)$ obtained in this thesis.

Chapter 12

Application 2: Complexity of extension field multiplication

12.1 Motivation and previous work

Riemann-Roch systems of equations have another interesting application. This is in the context of *extension field multiplication*. D.V. Chudnovsky and G.V. Chudnovsky [23] first employed algebraic curves over finite fields to construct low complexity algorithms for the multiplication of two elements in an extension field $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$. Later Shparlinski, Tsfasman and Vlăduţ [73] studied the asymptotic complexity of these algorithms.

We can describe the multiplication algorithm in terms of multiplication-friendly embeddings, which were introduced in Chapter 6. Given a multiplication friendly embedding (r, σ, ψ) of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, the algorithm for the multiplication of two elements x,y in $\mathbb{F}_{q^k}$ consists on the evaluation of

$$xy = \psi(\sigma(x) * \sigma(y)).$$

The computation of this formula requires two evaluations of σ, r products in $\mathbb{F}_q$ and a evaluation of ψ.

The complexity of such an algorithm is defined as the number of products of elements in $\mathbb{F}_q$ that are calculated in the second step, which equals the expansion of the multiplication-friendly embedding.

Thus, for a given q,k, it is interesting to know the smallest possible expansion of a multiplication friendly embedding of $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$. Recall that this is the definition of the parameter $m(q,k)$ (Definition 6.3). The proof of the upper bound in Theorem 6.7 made use of an algebraic-geometric code defined over the rational function field. However this construction requires that $q \geq 2k-2$. D.V. Chudnovsky and G.V. Chudnovsky considered this construction generalized to other types of function fields.

Shparlinski, Tsfasman and Vlăduţ (see [73]) studied the complexity of such construction asymptotically, that is, when the base field is fixed and the degree k of the extension grows. They defined Riemann-Roch systems of equations over the function fields of asymptotically good towers and giving conditions for solutions to exist asymptotically (in a similar way to Theorem 11.7 does in the case of secret sharing with strong multiplication). However, they make one unjustified claim, when the role of the two torsion subgroup $\mathrm{Cl}_0(\mathbb{F})[2]$ is neglected.

Later, more authors, especially Ballet, contributed with more results in the papers [1], [2], [3], [4], [5], [6], [7]. The results up to 2006 are summarized in the survey [8] and do *not* suffer from this gap with the exception of the aforementioned [73]. The result in [2] is not affected either, but the part of the contribution regarding asymptotical results is based on a conjecture. However, the more recent (2008) asymptotical results in [3] and [4] are affected by the same problem as in [73].

In this chapter, the results are corrected, using the techniques presented in the previous sections and obtaining the results below.

12.2 Multiplication-friendly embeddings from Riemann-Roch systems

The following theorem summarizes part of the ideas of [23] and [73] in the language of Riemann-Roch systems of equations. Recall that, as we have seen in Chapter 6.1, multiplication-friendly embeddings are equivalent in certain sense to special kinds of codes that we called multiplication-friendly codes

(see Proposition 6.5). We show that we can obtain multiplication-friendly codes from solutions to certain Riemann-Roch systems of equations.

THEOREM 12.1 *Let $\mathbb{F}/\mathbb{F}_q$ be an algebraic function field, $N, k > 1$ integers. Suppose there exist $P_1, \ldots, P_N \in \mathbb{P}^{(1)}(\mathbb{F})$ with $P_i \neq P_j$ $(i \neq j)$ and $P_0 \in \mathbb{P}^{(k)}(\mathbb{F})$. Let $D = \sum_{i=1}^{N} P_i + P_0 \in \mathrm{Div}(\mathbb{F})$ and $D^- = \sum_{i=1}^{N} P_i \in \mathrm{Div}(\mathbb{F})$. Let $K \in \mathrm{Div}(\mathbb{F})$ be a canonical divisor.*

If the Riemann-Roch system $\{\Delta_{P_0}(-X + K) = 0, \Delta_{P_0}(2X - D) = 0\}$ has some solution, then there exists a solution $G \in \mathrm{Div}(\mathbb{F})$ such that supp $G \cap$ supp $D = \emptyset$, *and $C = C_L(D, G)$ is an (N, k)-multiplication friendly code over $\mathbb{F}_q$.*

Furthermore, write $r = \ell(2G) - \ell(2G - D^-)$. Then there exist r indices $i_1, \ldots, i_r \in \{1, \ldots, N\}$, such that $\widetilde{C} = C_L(\widetilde{D}, G)$ is a (r, k)-multiplication-friendly code, where $\widetilde{D} = \sum_{j=1}^{r} P_{i_j} + P_0 \in \mathrm{Div}(\mathbb{F})$. In particular, we have $m(q, k) \leq \ell(2G)$.

PROOF. If there exists a solution, any divisor in its class of equivalence is also a solution. By the Weak Approximation Theorem (Corollary 2.47), we can take an element G of this class in such a way that supp $G \cap$ supp $D = \emptyset$.

Suppose G is a solution. We prove $C = C_L(D, G)$ is a multiplication-friendly code. We need to verify $\pi_0(C) = \mathbb{F}_{q^k}$ and $(x, \mathbf{0}) \notin \widehat{C}$ for all $0 \neq x \in \mathbb{F}_{q^k}$.

$\Delta_{P_0}(K - G) = 0$ implies $\ell(K - G + P_0) = \ell(K - G)$. Since $\deg P_0 = k$, it follows by the Riemann-Roch Theorem that $\ell(G) = \ell(G - P_0) + k$. This is enough to ensure that $\pi_0(C) = \mathbb{F}_{q^k}$, as follows: Consider the map

$$\rho : \mathcal{L}(G) \to \mathbb{F}_{q^k},$$

$$f \mapsto f(P_0).$$

Its kernel is $\mathcal{L}(G - P_0)$. So its image is isomorphic to $\mathcal{L}(G)/\mathcal{L}(G - P_0)$, and this has dimension (over $\mathbb{F}_q$) $\ell(K - G + P_0) - \ell(K - G) = k$. So $\pi_0(C) = \mathbb{F}_{q^k}$.

Second, as $\widehat{C} \subseteq C_L(D, 2G)$, it suffices to prove that $(x, \mathbf{0}) \notin C_L(D, 2G)$ for any $0 \neq x \in \mathbb{F}_{q^k}$. Or equivalently, that any $f \in \mathcal{L}(2G)$ with $f(P_i) = 0$ for

$i = 1, \ldots, N$ satisfies $f(P_0) = 0$. But this is also equivalent to the equality of Riemann-Roch spaces $\mathcal{L}(2G - D^-) = \mathcal{L}(2G - D)$, and this is precisely the condition $\Delta_{P_0}(2G - D) = 0$ which holds because G is a solution of the system. We have proved C is a multiplication-friendly code.

Finally, consider the $\mathbb{F}_q$-linear code $C_L(D^-, 2G)$. It has dimension r by definition. Let $i_1, \ldots, i_r \in \{1, \ldots, N\}$ be such that the code $C_L(\widetilde{D}^-, 2G)$ of length r equals $\mathbb{F}_q^r$, where $\widetilde{D}^- = \sum_{j=1}^r P_{i_j}$. Note that $\widetilde{C} = C_L(\widetilde{D}, G)$ satisfies $\pi_0(\widetilde{C}) = \mathbb{F}_{q^k}$ trivially, since $\pi_0(C) = \mathbb{F}_{q^k}$ as it is obtained from C by puncturing ("erasing coordinates") outside the 0-th coordinate.

By construction, $r = \ell(2G) - \ell(2G - \widetilde{D}^-)$. Since, by definition, it also holds that $r = \ell(2G) - \ell(2G - D^-)$, it follows that $\mathcal{L}(2G - D^-) = \mathcal{L}(2G - \widetilde{D}^-)$. So if $f \in \mathcal{L}(2G - \widetilde{D}^-)$, then $f \in \mathcal{L}(2G - D^-)$. This implies $f(P_0) = 0$, as shown before. △

Next we give sufficient conditions for the solvability of such systems. Recall that in Chapter 8.2 we showed that in some cases we can arrange the parameters of the system in such a way that all divisors of some fixed degree are solutions. If we do that, then we get the following result

THEOREM 12.2 *Let $\mathbb{F}_q$ be a finite field and $k > 1$ an integer. If there exists a function field $\mathbb{F}/\mathbb{F}_q$ such that $|\mathbb{P}^{(k)}(\mathbb{F})| > 0$ and $|\mathbb{P}^{(1)}(\mathbb{F})| \geq 4g + 2k - 1$, then $m(q, k) \leq 3g + 2k - 1$*

PROOF. Take $P_0 \in \mathbb{P}^{(k)}(\mathbb{F})$ and $P_1, \ldots, P_N \in \mathbb{P}^{(1)}(\mathbb{F})$ with $N = |\mathbb{P}^{(1)}(\mathbb{F})|$ and $P_i \neq P_j$ for $i \neq j$. Take $D = \sum_{i=1}^N P_i + P_0$.

We consider the Riemann-Roch system of equations

$$\{\Delta_{P_0}(-X + K) = 0, \Delta_{P_0}(2X - D) = 0\}.$$

We apply Corollary 8.7. The integer $d = 2g + k - 1$ satisfies that

$$-d + \deg K + \deg P_0 = -d + 2g - 2 + k = -1 < 0$$

and

$$2d - \deg D + \deg P_0 = 2d - (N + k) + k = 2d - N < 0$$

since $N = |\mathbb{P}^{(1)}(\mathbb{F})| \geq 4g + 2k - 1 > 2d$. Consequently, by Corollary 8.7 any divisor $G \in \mathrm{Div}_{2g+k-1}(\mathbb{F})$ is a solution to the Riemann-Roch set of equations.

Hence, by Theorem 12.1, $m(q,k) \leq \ell(2G)$. Note that

$$\deg 2G = 4g + 2k - 2 \geq 2g - 1,$$

so Riemann-Roch Theorem implies

$$\ell(2G) = \deg 2G - g + 1 = 3g + 2k - 1.$$

So $m(q,k) \leq 3g + 2k - 1$. △

But instead, one can use the more general Theorem 8.12 in order to obtain a sufficient condition for the solvability of the system in Theorem 12.1

THEOREM 12.3 *Let $\mathbb{F}/\mathbb{F}_q$ be an algebraic function field. Let $N, k > 1$ be integers. Suppose there are $P_1, \ldots, P_N \in \mathbb{P}^{(1)}(\mathbb{F})$ with $P_i \neq P_j$ $(i \neq j)$ Let $d \geq 0$ be an integer and define $r_1 = 2g - 2 - d + k$ and $r_2 = 2d - N$.*

If

$$h > A_{r_1} + A_{r_2}|\mathrm{Cl}_0[2](\mathbb{F})|$$

then the system $\{\Delta_{P_0}(-X + K) = 0, \Delta_{P_0}(2X - D) = 0\}$ has some solution $G \in \mathrm{Div}(\mathbb{F})$ with $\deg G = d$.

PROOF. This is exactly Theorem 8.12 applied to the system

$$\{\Delta_{P_0}(-X + K) = 0, \Delta_{P_0}(2X - D) = 0\}.$$

△

REMARK 12.4 (THE GAP IN [73]) *It is at this point when [73] takes an unjustified step, as it is claimed that the condition $h > A_{r_1} + A_{r_2}$ (instead of $h > A_{r_1} + A_{r_2}|\mathrm{Cl}_0[2]|$) suffices to ensure the existence of a solution to the corresponding Riemann-Roch system of equations. This jeopardizes the correction of the asymptotical bounds.*

We apply now the bounds in Chapter 9 in order to get a set of conditions which imply $h > A_{r_1} + A_{r_2}|\mathrm{Cl}_0[2](\mathbb{F})|$ and consequently the existence of a solution G of certain degree to the system in Theorem 12.1. When these conditions are satisfied we can give an upper bound for $m(q,k)$.

THEOREM 12.5 *Let $\mathbb{F}/\mathbb{F}_q$ be a function field and $N, k > 1$ be integers. Suppose there are $P_1, \ldots, P_N \in \mathbb{P}^{(1)}(\mathbb{F})$ with $P_i \neq P_j$ $(i \neq j)$ and there is $P_0 \in \mathbb{P}^{(k)}(\mathbb{F})$. Let $d \in \mathbb{Z}$ with $d \geq 0$ and define $r_1 = 2g - 2 - d + k$ and $r_2 = 2d - N$. Suppose the following conditions hold:*

1. $0 \leq r_1 \leq g-1$,
2. $0 \leq r_2 \leq g-1$,
3. $\frac{g}{q^{g-r_1-1}(\sqrt{q}-1)^2} < \frac{1}{2}$,
4. $\frac{g}{q^{g-r_2-1}(\sqrt{q}-1)^2} \cdot |\mathrm{Cl}_0[2]| < \frac{1}{2}$.

Then $m(q,k) \leq 2d-g+1$.

PROOF. By Proposition 9.1, the conditions imply $h > A_{r_1} + A_{r_2}|\mathrm{Cl}_0[2]|$. By Theorem 12.3, there is a solution $G \in \mathrm{Div}_d(\mathbb{F})$ to the system

$$\{\Delta_{P_0}(-X+K) = 0, \Delta_{P_0}(2X-D) = 0\}.$$

Therefore, by Theorem 12.1, there is an (n,k)-multiplication friendly code over $\mathbb{F}_q$ with $n \leq \ell(2G)$.

By condition i) and by the definition of r_1, it holds that $d \geq g+k-1 > g$. Hence, $\deg 2G = 2d > 2g$ and by Riemann-Roch Theorem,

$$\ell(2G) = \deg 2G - g + 1 = 2d - g + 1,$$

and the claim follows by the last statement in Theorem 12.1.

△

12.3 The asymptotical minimal multiplication complexity $\mu(q)$

12.3.1 Definition and known results

We introduce now the asymptotical quantity $\mu(q)$ that we are interested to upper bound.

DEFINITION 12.6 $\mu(q) := \liminf_{k \in \mathbb{N}} \frac{m(q,k)}{k}$.

The results in [23] and [73] (the ones which do not suffer from the aforementioned problem) imply the following facts [1]:

[1] Note that there is a typo in the statement of [73] of the lower bound for $\mu(q)$, which appears stated as $\mu(q) \geq 2(1+\frac{1}{(q-1)})$, but the lower bound stated here is the one that follows logically from the argument in that paper

THEOREM 12.7 *We have:*

- $\mu(2) \geq 3.52$ *and* $\mu(q) \geq 2(1 + \frac{1}{2(q-1)})$ *for any finite field* $\mathbb{F}_q$ *with* $q > 2$
- *For any finite field* $\mathbb{F}_q$ *with* q *square with* $q \geq 25$, $\mu(q) \leq 2(1 + \frac{1}{\sqrt{q}-3})$
- *For any finite field* $\mathbb{F}_q$ *and any integer* $k \geq 2$, $\mu(q) \leq \frac{m(q,k)}{k}\mu(q^k)$. *In particular* $\mu(q) \leq \frac{3}{2}\mu(q^2)$

The two last assertions imply that $\mu(q)$ is finite because, as we know, $m(q, 2) = 3$.

The problematic bound from [73] states that $\mu(q) \leq 2(1 + \frac{1}{A(q)-1})$ when $A(q) > 1$ (and in particular $\mu(q) \leq 2(1 + \frac{1}{\sqrt{q}-2})$ for q square, $q \geq 9$).

On the other hand, the asymptotic results that follow from [8] improve in certain cases the upper bounds in Theorem 12.7.

12.3.2 Upper bounds for $\mu(q)$

In order to study the behaviour of $\mu(q)$, one first needs to ensure that given an extension field of large enough degree there are function fields over the base field with at least one place of that degree. We need to use the following known fact:

THEOREM 12.8 ([75], 5.2.10(3)) *If* $1 < k \in \mathbb{Z}$ *satisfies*

$$2g + 1 \leq q^{\frac{k-1}{2}}(\sqrt{q} - 1),$$

then $\mathbb{P}^{(k)}(\mathbb{F}) \neq \emptyset$.

Next, the result of applying the simple argument in Theorem 12.2 is given. This is stated merely as an example, as it does not improve any previously known result.

THEOREM 12.9 *Let* $\mathbb{F}_q$ *be a finite field. Suppose* $A(q) > 4$. *Then*

$$\mu(q) \leq 2(1 + \frac{3}{A(q) - 4}).$$

The proof of this theorem is similar to the following one and is omitted

MAIN THEOREM 12.10 *Let $\mathbb{F}_q$ be a finite field. If there exists $0 < A \leq A(q)$ such that $A > 1 + J_2(q, A)$, then*

$$\mu(q) \leq 2(1 + \frac{1}{A - J(q, A) - 1}).$$

Consequently, for any q square, $q \geq 9$,

$$\mu(q) \leq 2(1 + \frac{\log q}{(\sqrt{q} - 2)\log q - 2}).$$

If in addition $q = 4^e$, $e \in \mathbb{Z}_{>1}$, then

$$\mu(q) \leq 2(1 + \frac{(\sqrt{q} + 1)\log q}{(q - \sqrt{q} - 2)\log q - 1}).$$

PROOF. Let $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$ be an infinite family of function fields over $\mathbb{F}_q$ be an infinite family of function fields over $\mathbb{F}_q$ with $g(\mathbb{F}^{(m)}) \to \infty$ and such that $A(\mathcal{F}) \geq A$ and $J_2(\mathcal{F}) = J_2(q, A)$. Write $J = J_2(\mathcal{F})$. Define $g_m = g(\mathbb{F}^{(m)})$, $N_m = |\mathbb{P}^{(1)}(\mathbb{F}^{(m)})|$, $j_m = \log_q(|\mathrm{Cl}_0(\mathbb{F}^{(m)})[2]|)$, and $d_m = \lceil \delta g_m \rceil$, $k_m = \lfloor \kappa g_m \rfloor$ for some real numbers δ, $\kappa > 0$ to be determined next. Also define $(r_1)_m = 2g_m - 2 - d_m + k_m$ and $(r_2)_m = 2d_m - N_m$. The idea is to apply Theorem 12.5 to $\mathbb{F}^{(m)}$.

For all m selected large enough, we can argue as follows. First note that $\mathbb{P}^{(k_m)}(\mathbb{F}^{(m)}) \neq \emptyset$ by Theorem 12.8 and because $\kappa > 0$. According to Remark 11.5, all that remains to prove in order to apply Theorem 12.5 are conditions *iii*) and *iv*). These can be written as

$$iii)(r_1)_m - g_m + 1 \leq \log_q \left(\frac{(\sqrt{q} - 1)^2}{2g_m} \right)$$

and

$$iv)(r_2)_m - g_m + 1 + j_m \leq \log_q \left(\frac{(\sqrt{q} - 1)^2}{2g_m} \right).$$

Fix any $0 < \epsilon \in \mathbb{R}$ such that $4\epsilon < A - (1 + J)$, which is possible by the condition $A - J > 1$. Define $\delta = \frac{A-J+1}{2} - \epsilon$ and $\kappa = \delta - 1 - \epsilon$. The condition $4\epsilon < A - (1 + J)$ ensures $\delta > 1$ and $\kappa > 0$. The definition of A

ensures $N_m > (A-\frac{\epsilon}{3})g_m$. Moreover, by definition of J we might assume that $j_m < (J+\frac{\epsilon}{3})g_m$ (otherwise we might take an infinite subfamily where this is satisfied). By elementary calculus, we have $\log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right) > -\frac{\epsilon}{3}g_m$. Now note that

$$(r_1)_m - g_m + 1 = g_m - d_m + k_m - 1 \leq g_m - \lceil \delta g_m \rceil + \lfloor \kappa g_m \rfloor - 1.$$

Now, by substituting the value of κ,

$$(r_1)_m - g_m + 1 \leq -\epsilon g_m - 1 < -\frac{\epsilon}{3}g_m < \log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right).$$

On the other hand

$$(r_2)_m - g_m + 1 + j_m = 2d_m - N_m - g_m + 1 + j_m <$$

$$< 2(\delta g_m + 1) - (A - \frac{\epsilon}{3})g_m - g_m + (J + \frac{\epsilon}{3})g_m + 1$$

by applying the previous bounds on N_m and j_m. Now, by definition of δ we get

$$(r_2)_m - g_m + 1 + j_m \leq -\frac{4\epsilon}{3}g_m + 3 < -\frac{\epsilon}{3}g_m < \log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right).$$

Hence we have proved

$$(r_1)_m - g_m + 1 < \log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right)$$

and

$$(r_2)_m - g_m + 1 + j_m < \log_q\left(\frac{(\sqrt{q}-1)^2}{2g_m}\right).$$

Application of Theorem 12.5 for large m shows that $m(q,k) \leq 2d_m - g_m + 1$ and therefore $\mu(q) \leq \frac{2\delta-1}{\kappa}$. If we substitute κ and δ by the values given before, we get

$$m_q \leq 2\frac{A - J - 2\epsilon}{A - J - 1 - 4\epsilon}.$$

This holds for any $\epsilon > 0$ small enough so by letting $\epsilon \to 0$,

$$\mu(q) \leq 2\frac{A-J}{A-J-1} = 2(1 + \frac{1}{A-J-1}).$$

The concrete bounds are obtained by applying the bounds for $J_2(q, A(q))$ in the previous section. $\triangle$

Hence we have that $\mu(q) \leq 2(1+\frac{1}{A(q)-J_2(q,A(q))-1})$ if $A(q) > 1+J_2(q, A(q))$. This improves the results in Theorem 12.7. It also improves many cases of the bounds that follow from [8]. It is always worse however than the problematic statement in [73] (we could only reach this bound if we could prove that $J_2(q, A(q)) = 0$).

12.3.3 Table of explicit upper bounds on $\mu(q)$ and comparison with previous results

In the following Table we compare the upper bounds for $\mu(q)$ implied by Main Theorem 12.10 with the best previous bounds stated in [8] for some finite fields $\mathbb{F}_q$.

REMARK 12.11 *Note that the improvement that we get in characteristic 2 by applying the bounds of Main Theorem 12.10 which are specific for powers of* 4 *(which use the theorem by Deuring-Shafarevich) is significant. If we did not use this improvement, we would only be able to prove the bounds* $\mu(16) \leq 3.33$ *and* $\mu(64) \leq 2.35$.

q	New bounds	Previous bounds
9	7.419	9
16	3.026	3.924
25	2.779	4
49	2.431	3
64	2.335	2.800
81	2.300	2.667

Bounds for smaller finite fields $\mathbb{F}_q$ can be obtained applying for example that $\mu(q) \leq \frac{3}{2}\mu(q^2)$ or the more general version $\mu(q) \leq \frac{m(q,k)}{k}\mu(q^k)$ for any $k \geq 2$ (Theorem 12.7).

Summary of the chapter: We have studied the problem of complexity of multiplication in extension fields, first considered by Chudnovsky and Chudnovsky. We have explained how to pose a Riemann-Roch system of

equations whose solutions yield a multiplication algorithm. We have defined the asymptotical best multiplication complexity $\mu(q)$ of a finite field $\mathbb{F}_q$. We have identified a gap in one of the proofs of [73] that implied incorrect (or at least unjustified) upper bounds for this value. We used the results of solvability about Riemann-Roch systems of equations in Chapter 8 together with the bounds in Chapters 9, 10 in order to obtain new upper bounds for $\mu(q)$.

Conclusions

In this thesis the asymptotical behaviour of families of ideal linear secret sharing schemes with strong multiplication has been analyzed. The problem has been studied from a code-theoretic perspective. We have introduced the notion of minimal weight $w_i(C)$ at an index i of a linear code C and the class $\mathcal{C}(\mathbb{F}_q)$ of linear codes over $\mathbb{F}_q$ such that one can define a linear secret sharing scheme $\Sigma(C,i)$ from any index $i \in I(C)$. We have characterized the privacy and reconstruction thresholds of $\Sigma(C,i)$ in terms of $w_i(C)$ and $w_i^{\perp}(C)$. In order to study the multiplication of $\Sigma(C,i)$, we have introduced the notion of Schur square $\widehat{C}$ of a linear code C as the linear span of the set of Schur products of every pair of words in C. We have defined a subclass $\mathcal{C}^{\dagger}(\mathbb{F}_q) \subseteq \mathcal{C}(\mathbb{F}_q)$ that contains all codes C such that some LSSS $\Sigma(C,i)$ has t-strong multiplication for some integer t. We have introduced the corruption tolerance $\widehat{\tau}(C)$ of a code $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$. This is the ratio $\widehat{\tau}(C) = \frac{3t}{n-1}$ where t is the largest integer for which there exists a linear secret sharing scheme constructed from C which has t-strong multiplication and n shares. It is immediate to verify that $0 \leq \widehat{\tau}(C) \leq 1$ for any $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$. We have introduced the asymptotical optimal corruption tolerance $\widehat{\tau}(q)$ of the field $\mathbb{F}_q$ which represents the best possible limit for the corruption tolerance of an infinite family of codes $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$. We have recast the results of Chen and Cramer [20] in our language. These results stated that $\widehat{\tau}(q) > 1 - \frac{4}{A(q)} > 0$ for an infinite number of finite fields $\mathbb{F}_q$, concretely those such that Ihara's constant $A(q)$ satisfies $A(q) > 4$.

The first main result of this thesis assures that $\widehat{\tau}(q) > 0$ for every finite field $\mathbb{F}_q$. In the LSSS terminology this means that for any finite field $\mathbb{F}_q$ there is an infinite family of ideal LSSS such that the number of shares n tends to infinity and they have t-strong multiplication for $t = \Omega(n)$. In particular it has been shown that $\widehat{\tau}(2) \geq 0.034$ so, for an arbitrarily large n, there exist ideal binary linear secret sharing schemes with n shares and t-strong multiplication for $t = 0.01n$. In order to show this we have introduced a dedicated field descent technique, which allowed us to prove $\widehat{\tau}(q) \geq \frac{1}{3}\widehat{\tau}(q^2)$ and then we have combined it with the results of Chen and Cramer.

On the other hand, we have also proved $\widehat{\tau}(q) < 1$. It was easy to verify that the optimal value $\widehat{\tau}(C) = 1$ could only be achieved for the case of MDS codes. Since the length of these codes is bounded by some function of q, the size of the field, it is not possible to have $\widehat{\tau}(C) = 1$ for codes of arbitrary length over a fixed finite field $\mathbb{F}_q$. But, by proving $\widehat{\tau}(q) < 1$, we have also ruled out the possibility that the corruption tolerance of an infinite family of

ideal LSSS *tends* to 1. In fact we have obtained upper bounds for $\widehat{\tau}(q)$ which in some cases (for very small finite fields) are quite far from 1. For example, in the binary case, we have proved $\widehat{\tau}(2) < 0.429$. The proof of some of the results that lead to these bounds are somewhat reminiscent of the techniques used to prove the Norse upper bound for the covering radius and the Plotkin upper bound for the dimension and distance of a linear code. However, more sophisticated techniques have been proposed for these coding theory problems, for example linear programming bounds. So an open question is: Can some of these more sophisticated techniques be adapted to the problem of upper bounding $\widehat{\tau}(q)$?

We have also improved the lower bounds for $\widehat{\tau}(q)$ that appeared in [20] by means of more involved algebraic geometric techniques. We have considered certain system of equations defined on the set of divisors of the function field, that have been named Riemann-Roch systems of equations in this text, whose solutions yield linear codes with good properties. The equations consist on equalities of the Riemann-Roch dimensions of some pairs of divisors. In our case, we can pose a certain Riemann-Roch system such that whenever it has a solution there is an ideal linear secret sharing scheme with certain corruption tolerance. Although the idea of Riemann-Roch systems of equations had already been used in previous works [54, 60, 79, 81, 82, 83, 85], the systems considered in this thesis are of a more general type and this affects the analysis of the existence of solutions.

In order to guarantee the existence of a solution to a system of this kind, we have given upper bounds for two kinds of parameters of the algebraic function field. The first parameter is the number of effective divisors of certain degree. Bounds for this parameter had already been found in other works concerning Riemann-Roch systems of equations. We have adapted the bounding techniques in those papers, which make use of results about the zeta function of the function field. The novelty was the necessity to bound a second parameter: the size of the m-torsion subgroup $\mathrm{Cl}_0(\mathbb{F})[m]$ of the degree zero divisor class group $\mathrm{Cl}_0(\mathbb{F})$. This does not seem to have been studied before in relation to the problem of proving the existence of a system of equations of the considered type.

We have defined, for every finite field $\mathbb{F}_q$ and $0 < a \leq A(q)$, the torsion limits $J_m(q, a)$, which are an asymptotic measure of $|\mathrm{Cl}_0(\mathbb{F})[m]|$ for families $\mathcal{F}$ of function fields $\mathbb{F}$ with "Ihara's limit" $A(\mathcal{F}) \geq a$. We have shown that we can derive some upper bounds for $J_m(q, a)$ from several known results in algebraic geometry. General bounds for any a, m, q follow from results due

to Weil, but we have improved this bounds in some cases using two different strategies, based on properties of Weil Pairing and on a theorem of Deuring and Shafarevich about the computation of the p-rank in extensions of algebraic function fields. The latter idea has led to a particularly good upper bound for $J_2(q, \sqrt{q}-1)$ in the case where q is a square. It is an interesting and crucial open problem to determine the actual value of $J_m(q, a)$ for some finite field $\mathbb{F}_q$, real number $0 < a \leq A(q)$ and integer $m \neq -1, 1$; in particular, it is an intriguing question to determine whether $J_m(q, a) = 0$ in some case. Another interesting question is to determine if it helps to consider *non-optimal* families $\mathcal{F}$ of function fields over $\mathbb{F}_q$; that is, if $J_m(q, a) < J_m(q, A(q))$ for some m, q and $0 < a < A(q)$.

We have shown, as an application of the results obtained for a particular kind of Riemann-Roch systems of equations, new lower bounds for $\widehat{\tau}(q) > 0$. These are achieved in the case $a > 1 + J_2(q, a)$ for some $0 < a \leq A(q)$ and depend on the ratio $\frac{1+J_2(q,a)}{a}$. The bounds are stronger if we can guarantee that this value is small. So another open question is, even if $J_m(q, a) < J_m(q, A(q))$ holds for some m,q and $0 < a < A(q)$, we can also prove $\frac{1+J_2(q,a)}{a} < \frac{1+J_2(q,A(q))}{A(q)}$; in other words, we wonder if the best bounds for $\widehat{\tau}(q)$ obtained by means of this argumentation may be attained for a *non-optimal* family of function fields.

Another related interesting question would be if it is possible at all to prove $\widehat{\tau}(q) > 0$ without the use of asymptotically *good* families of function fields. A well known result of coding theory, proved by Pellikaan, Shen and van Wee([65]) states that every linear code over $\mathbb{F}_q$ is an AG-code defined over some function field $\mathbb{F}/\mathbb{F}_q$. Therefore for any infinite family of codes $\{C^{(m)}\}_{m>0} \subseteq \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $n(C^{(m)}) \to \infty$ there exists an infinite family $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$ of function fields $\mathbb{F}^{(m)}/\mathbb{F}_q$ such that $C^{(m)}$ is an AG-code defined over the function field $\mathbb{F}^{(m)}/\mathbb{F}_q$ and consequently $|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| \to \infty$ and $g(\mathbb{F}^{(m)}) \to \infty$. Assume now that we have a family of linear codes $\{C^{(m)}\}_{m>0} \subseteq \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $n(C^{(m)}) \to \infty$ such that in addition the corruption tolerance tends to a positive number, that is, $\widehat{\tau}(C^{(m)}) \to \tau > 0$. The question is if this family of codes may be defined as AG-codes over some *asymptotically bad* family $\mathcal{F}$ of function fields over $\mathbb{F}_q$ (i.e. a family $\mathcal{F}$ such that $A(\mathcal{F}) = 0$).

Note that in this thesis whenever we have constructed a family of codes directly as AG-codes over some family of function fields $\mathcal{F}$ we required at least the condition $A(\mathcal{F}) > 1$ in order to ensure that the corruption tolerance

of the codes is asymptotically non-vanishing. However we know that this condition is not necessary for every finite field because we have also obtained, by means of the field descent technique, families of codes over $\mathbb{F}_2$ and $\mathbb{F}_3$ with asymptotically non-vanishing corruption tolerance. Since $A(q) < 1$ for $q = 2, 3$, and on account of the aforementioned result in [65], the codes in these families must be defined as AG-codes on an infinite family of function fields with $A(\mathcal{F}) < 1$.

We can compare this aspect of our problem with the code-theoretic problem of asymptotically good codes. Xing [82] proved that given a finite field $\mathbb{F}_q$ and *any* real number $0 < a \leq A(q)$ there exist families of AG-codes defined over a family $\mathcal{F}$ of function fields over $\mathbb{F}_q$ with $A(\mathcal{F}) = a$ and attaining the Gilbert-Varshamov bound (interestingly those results are also based on the Riemann-Roch systems approach). And in fact, if we examine the arguments given in [82], the same result is true if one uses asymptotically bad families $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$ (i.e. $A(\mathcal{F}) = 0$) as long as $|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| \to \infty$. However we do not seem to be able to use the same techniques as a successful approach to our problem.

We have also applied the "Riemann-Roch systems approach" to a problem in the context of multiplication complexity in finite fields. More precisely, given a base field $\mathbb{F}_q$ and an extension field $\mathbb{F}_{q^k}$ an algorithm by D. V. Chudnovsky and G. V. Chudnovsky allows for the transformation of the task of multiplying two elements in $\mathbb{F}_{q^k}$ into the computation of a certain number of products of elements in $\mathbb{F}_q$. The complexity of the product is the minimal necessary number of products in the base field, which we have denoted $m(q, k)$. Shparlinski, Tsfasman and Vladut[73] extended this work and studied the problem asymptotically, that is, when q is fixed and k grows. Concretely, one of the quantities they considered was the limit inferior of $m(q, k)/k$ for $k \in \mathbb{N}$, which we have denoted $\mu(q)$. They computed lower and upper bounds for this value, however as we have seen, there was a gap in one of their proofs, where they did not take into account the role of the group $\mathrm{Cl}_0(\mathbb{F})[2]$, and this error affected the upper bounds. We have identified and this problem and proved new bounds using the aforementioned bounding techniques. The bounds obtained are worse (although relatively close) than the ones claimed in [73]. It is still an open problem to determine whether the bounds clamed in [73] are valid, which may still happen, since the known *lower* bounds for $\mu(q)$ are smaller than the claimed upper bounds. In fact, our argumentation here proves that these bounds would be true if $J_2(q, A(q)) = 0$ holds.

To conclude, we remark that the techniques explained in this thesis can also be applied to a number of extensions of the problems studied here and this is the subject of current and future work. In first place, we can analyze the case of (non-perfect) LSSS with n shares where the secret is not one single element of $\mathbb{F}_q$ but a vector of length κn for some real number κ. The study of multiplication of these kind of schemes was initiated by Franklin and Yung, who considered in [36] a variation of Shamir's scheme where the secret consists on the evaluations of a polynomial on several elements of the field, and discussed its applications in multiparty computation. We can define an appropiate generalization $\mathcal{C}_\kappa(\mathbb{F}_q)$ of the class $\mathcal{C}(\mathbb{F}_q)$, and for a code C in this class and an appropiate set $T \subseteq \mathcal{I}(C)$, with $|T| = \kappa n(C)$, we take as secret the *subvector* $\pi_T(\mathbf{c})$, and as shares the remaining coordinates $\pi_i(\mathbf{c})$, $i \notin T$, for a word $\mathbf{c}$ taken uniformly at random in C. We can generalize all the notions given in Chapters 4 and 5, which now depend also on the extra parameter κ (the "relative length of the secret") and apply the same kind of techniques explained in the rest of the thesis. In particular we can also estimate the "*multisecret* asymptotical optimal corruption tolerance" $\widehat{\tau}(q, \kappa)$. We can also study the case of secret sharing schemes where the secret is an element of an extension field $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$, the shares are elements of $\mathbb{F}_q$ and the strong multiplication property is defined with respect to the products in the respective fields. Cramer,Damgård and de Haan first studied a scheme with these properties (see [26]). Some results on this problem also appeared in [18]. In this case, we need to apply the techniques of this thesis to generalized linear codes, where one coordinate lies in the extension field.

Other extensions are interesting as well: we can consider the more general problem of secret sharing schemes with r-fold multiplication, for $r \geq 2$, where the product of r secrets is determined by the products of the corresponding sets of r shares. Then we need to study the weight at an index of the r-th order Schur product transform $C^{\circledast r}$ of a code C. We can apply the strategy consisting of Riemann-Roch systems of equations as explained in Part III. In this case, we will have equations of the form $\Delta_{P_0}(rX - D + P_A)$ and therefore we will need the upper bounds for the size of r-torsion limits $J_r(q, a)$ that were obtained in Chapter 10 (note again that for the applications considered in this thesis we only needed bounds for the particular case $r = 2$, but the results in Chapter 10 are more general).

Finally, we can also analyze which of our constructions enjoy the property of t-independence of shares, required by the application to correlation extractors of [47] mentioned in the introduction. It turns out that this property

can be captured imposing a condition on the dual distance of the codes and that all techniques we have used in this thesis yield secret sharing schemes with t-independence of shares for $t = \Omega(n)$ except for the ones resulting from the application of the descent technique presented in Chapter 6 where, on account of the observations of Section 6.4, the dual distances of all codes of the family are upper bounded by certain constant. It is still an unanswered question to determine whether for all finite fields $\mathbb{F}_q$ there is a family of codes $\{C^{(m)}\}_{m>0} \subseteq \mathcal{C}^{\dagger}(\mathbb{F}_q)$ with $n(C^{(m)}) \to \infty$ such that not only $\widehat{\tau}(C^{(m)}) \to \tau > 0$ but also $d((C^{(m)})^{\perp})/n(C^{(m)}) \to \delta > 0$. Currently we can only prove this fact for finite fields for which we can prove $\widehat{\tau}(q) > 0$ without resorting to the descent technique, in particular for every finite field $\mathbb{F}_q$ with q square and $q \geq 9$, as we can deduce from the results stated in Table 11.1.

Conclusiones

En esta tesis se ha analizado el comportamiento asintótico de familias de esquemas de compartición de secretos lineales ideales con multiplicación fuerte. El problema se ha estudiado desde la perspectiva de la teoría de códigos. Hemos introducido el concepto de peso mínimo $w_i(C)$ en un índice i de un código lineal C y la clase $\mathcal{C}(\mathbb{F}_q)$ de códigos lineales sobre $\mathbb{F}_q$ tales que podemos definir un esquema de compartición de secretos $\Sigma(C,i)$ a partir de cualquier índice $i \in I(C)$. Hemos caracterizado los umbrales de privacidad y reconstrucción de $\Sigma(C,i)$ en función de $w_i(C)$ y $w_i^{\perp}(C)$. Para estudiar la multiplicación de $\Sigma(C,i)$, hemos introducido el concepto de cuadrado de Schur $\widehat{C}$ de un código lineal C como el código generado por el conjunto de productos de Schur de todo par de palabras de C. Hemos definido una subclase $\mathcal{C}^{\dagger}(\mathbb{F}_q) \subseteq \mathcal{C}(\mathbb{F}_q)$ que contiene todos los códigos C tal que algún esquema $\Sigma(C,i)$ tiene t-multiplicación fuerte para algún entero t. Se ha usado la noción de tolerancia de corrupción $\widehat{\tau}(C)$ de un código $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$. Es el cociente $\widehat{\tau}(C) = \frac{3t}{n-1}$ donde t es el mayor entero para el cual existe un esquema de compartición de secretos construido a partir de C que tiene t-multiplicación fuerte y n fragmentos. Es inmediato comprobar que $0 \leq \widehat{\tau}(C) \leq 1$ para cualquier $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$. Hemos introducido la tolerancia de corrupción asintótica $\widehat{\tau}(q)$ del cuerpo $\mathbb{F}_q$ que representa el mejor límite posible para la tolerancia de corrupción de una familia infinita de códigos $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$. Hemos reformulado los resultados de Chen y Cramer [20] en nuestro lenguaje. Estos resultados implican que $\widehat{\tau}(q) > 1 - \frac{4}{A(q)} > 0$ para un número infinito de cuerpos finitos $\mathbb{F}_q$, concretamente para aquellos cuya constante de Ihara $A(q)$ satisface $A(q) > 4$.

Un resultado a resaltar de esta tesis es el que asegura que $\widehat{\tau}(q) > 0$ para todo cuerpo finito $\mathbb{F}_q$. En términos de esquemas de compartición de secretos esto significa que para todo cuerpo finito $\mathbb{F}_q$ existe una familia de esquemas de compartición de secretos lineales ideales tal que el número de fragmentos n tiende a infinito y tienen t-multiplicación fuerte para $t = \Omega(n)$. En particular se ha demostrado que $\widehat{\tau}(2) \geq 0.034$ así que, para n arbitrariamente grande, existe un esquema de compartición de secretos lineal ideal con n fragmentos y t-multiplicación fuerte para $t = 0.01n$. Para probar esto, hemos introducido una técnica de descenso de cuerpo, que nos ha permitido demostrar que $\widehat{\tau}(q) \geq \frac{1}{3}\widehat{\tau}(q^2)$ y luego la hemos combinado con los resultados de Chen y Cramer.

Por otro lado, hemos demostrado que $\widehat{\tau}(q) < 1$. Es fácil verificar que el valor óptimo $\widehat{\tau}(C) = 1$ sólo se puede alcanzar cuando C es un código MDS.

Como la longitud de este tipo de códigos está acotada por cierta función de q, el tamaño del cuerpo, no es posible tener que $\widehat{\tau}(C) = 1$ para códigos de longitud arbitraria sobre un determinado cuerpo finito $\mathbb{F}_q$. Pero, demostrando que $\widehat{\tau}(q) < 1$, también hemos eliminado la posibilidad de que la tolerancia de corrupción de una familia infinita de esquemas de compartición de secretos lineales ideales *tienda* a 1. De hecho, hemos obtenido cotas superiores para $\widehat{\tau}(q)$ que en algunos casos (para cuerpos muy pequeños) están bastante lejos de 1. Por ejemplo, en el caso binario, hemos demostrado que $\widehat{\tau}(2) < 0.429$. La demostración de algunos de los resultados que nos llevan a estas cotas se parecen, en cierto modo, a las técnicas que se utilizan para demostrar la denominada cota noruega para el radio de cobertura y la cota de Plotkin para la dimensión y distancia de un código lineal. Sin embargo, en la teoría de códigos se han utilizado técnicas más sofisticadas para estos problemas, por ejemplo programación lineal. Así que una pregunta que nos podemos plantear es: ¿se puede adaptar alguna de estas técnicas más sofisticadas para mejorar las cotas superiores que hemos encontrado para $\widehat{\tau}(q)$?

Además hemos mejorado las cotas inferiores para $\widehat{\tau}(q)$ que aparecieron en [20] por medio de técnicas más elaboradas de geometría algebraica. Hemos considerado ciertos sistemas de ecuaciones definidos en el conjunto de divisores de un cuerpo de funciones algebraicas, sistemas que hemos denominado de Riemann-Roch, cuyas soluciones permiten obtener códigos lineales con buenas propiedades. Las ecuaciones consisten en igualdades de las dimensiones de Riemann-Roch de algunos pares de divisores. En nuestro caso, podemos plantear un sistema de Riemann-Roch de forma que si tiene solución, entonces existe un esquema de compartición de secretos lineal ideal con cierta tolerancia de corrupción. Aunque la idea de los sistemas de ecuaciones de Riemann-Roch había sido utilizada ya anteriormente en [54, 60, 79, 81, 82, 83, 85], los sistemas considerados en esta tesis son de un tipo más general y esto afecta al análisis de la existencia de soluciones.

Para garantizar la existencia de solución en un sistema de este tipo, hemos necesitado cotas superiores para dos tipos de parámetros del cuerpo de funciones algebraicas. El primer parámetro es el número de divisores positivos de cierto grado. Se habían obtenido cotas para este parámetro en trabajos anteriores que utilizaban el planteamiento de sistemas de Riemann-Roch. En esta tesis se han adaptado las técnicas utilizadas, que hacen uso de algunos resultados acerca de la función zeta del cuerpo de funciones algebraicas. La novedad de este trabajo con respecto a trabajos anteriores es la necesidad de acotar un segundo parámetro: el tamaño del subgrupo de

m-torsión $\mathrm{Cl}_0(\mathbb{F})[m]$ del grupo de clases de divisores de grado cero $\mathrm{Cl}_0(\mathbb{F})$. Este problema no parece haber sido tratado anteriormente en relación con el de asegurar la existencia de un sistema de ecuaciones de Riemann-Roch.

A este respecto, hemos definido para todo cuerpo finito $\mathbb{F}_q$ y todo número real a con $0 < a \leq A(q)$ los límites de torsión $J_m(q,a)$, que son una medida asintótica de $|\mathrm{Cl}_0(\mathbb{F})[m]|$ para cuerpos de funciones algebraicas $\mathbb{F}$ de una familia $\mathcal{F}$ con "límite de Ihara" $A(\mathcal{F}) \geq a$. Hemos demostrado que podemos obtener cotas superiores para los valores $J_m(q,a)$ a partir de resultados conocidos de geometría algebraica. Algunos resultados clásicos de Weil acerca de torsión en variedades abelianas permiten deducir cotas generales para cualesquiera a, m, q, pero hemos mejorado estas cotas en algunos casos utilizando dos estretegias distintas, que se basan respectivamente en propiedades de los pares de Weil y en un teorema de Deuring y Shafarevich acerca de la computación del p-rango de extensiones de cuerpos de funciones algebraicas. Esta última idea nos ha llevado a obtener cotas superiores particularmente buenas para $J_2(q, \sqrt{q}-1)$ en el caso en el que q es un cuadrado. Determinar el verdadero valor de $J_m(q,a)$ para algún cuerpo finito $\mathbb{F}_q$, número real $0 < a \leq A(q)$ y entero $m \neq -1, 1$ es un problema interesante; en particular, sería importante determinar si $J_m(q,a) = 0$ puede ocurrir en algún caso. Otra cuestión interesante es la de determinar si permitir familias *no óptimas* $\mathcal{F}$ de cuerpos de funciones algebraicas sobre $\mathbb{F}_q$ puede ayudar a mejorar las cotas superiores para resolver este problema; es decir, si $J_m(q,a) < J_m(q, A(q))$ para algunos m, q y algún $0 < a < A(q)$.

Hemos encontrado nuevas cotas inferiores para $\widehat{\tau}(q)$ como aplicación de los resultados obtenidos para un tipo particular de sistemas de ecuaciones de Riemann-Roch. Estas cotas se alcanzan siempre que $a > 1 + J_2(q,a)$ para algún $0 < a \leq A(q)$ y dependen del cociente $\frac{1+J_2(q,a)}{a}$. Las cotas son mejores si podemos garantizar que este valor es pequeño. Así que otra cuestión abierta es si, incluso en el caso de que $J_m(q,a) < J_m(q,A(q))$ para algunos m, q y $0 < a < A(q)$, se cumple que $\frac{1+J_2(q,a)}{a} < \frac{1+J_2(q,A(q))}{A(q)}$; en otras palabras, nos preguntamos si las mejores cotas para $\widehat{\tau}(q)$ obtenidas por medio de estos argumentos se pueden alcanzar para una familia *no óptima* de cuerpos de funciones algebraicas.

Otra cuestión interesante relacionada con lo anterior que nos podemos plantear es la de determinar si es posible demostrar que $\widehat{\tau}(q) > 0$ sin utilizar familias *buenas* de cuerpos de funciones algebraicas. Un resultado conocido de teoría de códigos, demostrado por Pellikaan, Shen y van Wee([65]) afirma

que todo código lineal sobre $\mathbb{F}_q$ es un código algebraico-geométrico definido sobre algún cuerpo de funciones algebraicas $\mathbb{F}/\mathbb{F}_q$. Por tanto para cualquier familia infinita de códigos $\{C^{(m)}\}_{m>0} \subseteq \mathcal{C}^{\dagger}(\mathbb{F}_q)$ con $n(C^{(m)}) \to \infty$ existe una familia infinita $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$ de cuerpos de funciones $\mathbb{F}^{(m)}/\mathbb{F}_q$ tal que $C^{(m)}$ es un código algebraico-geométrico definido sobre un cuerpo de funciones $\mathbb{F}^{(m)}/\mathbb{F}_q$ y por tanto $|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| \to \infty$ y $g(\mathbb{F}^{(m)}) \to \infty$. Supongamos ahora que tenemos una familia $\{C^{(m)}\}_{m>0} \subseteq \mathcal{C}^{\dagger}(\mathbb{F}_q)$ de códigos lineales con $n(C^{(m)}) \to \infty$ y además la tolerancia de corrupción tiende a un número positivo, es decir, $\widehat{\tau}(C^{(m)}) \to \tau > 0$. La pregunta que nos planteamos es si esta familia de códigos se puede definir como códigos algebraico-geométricos sobre alguna familia asintóticamente mala $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ (es decir una familia $\mathcal{F}$ tal que $A(\mathcal{F}) = 0$).

Notemos que, en esta tesis, siempre que hemos construido una familia de códigos directamente como códigos algebraico-geométricos sobre alguna familia de cuerpos de funciones $\mathcal{F}$ exigimos que se cumpla al menos la condición $A(\mathcal{F}) > 1$ para asegurar que la tolerancia de corrupción de los códigos no tienda a cero. Sin embargo, sabemos que esta condición no es necesaria para todo cuerpo finito porque también hemos obtenido, por medio del método de descenso de cuerpo, familias de códigos sobre $\mathbb{F}_2$ y $\mathbb{F}_3$ con tolerancia de corrupción asintóticamente positiva. Como $A(q) < 1$ para $q = 2, 3$, teniendo en cuenta el resultado antes mencionado de [65], los códigos de estas familias deben ser códigos algebraico-geométricos sobre una familia infinita de cuerpos de funciones $\mathcal{F}$ tal que $A(\mathcal{F}) < 1$.

Podemos comparar este aspecto de nuestro problema con el de construir códigos lineales asintóticamente buenos. Xing [82] demostró que dado un cuerpo finito $\mathbb{F}_q$ y *cualquier* número real $0 < a \leq A(q)$ existen familias de códigos algebraico-geométricos definidos sobre una familia $\mathcal{F}$ de cuerpos de funciones algebraicas sobre $\mathbb{F}_q$ con $A(\mathcal{F}) = a$ que alcanzan la cota de Gilbert-Varshamov (es interesante que estos resultados también se basan en el planteamiento de sistemas de Riemann-Roch). Y de hecho, si examinamos los argumentos dados en [82], este resultado también es cierto si utilizamos familias asintóticamente malas $\mathcal{F} = \{\mathbb{F}^{(m)}\}_{m>0}$ (es decir, $A(\mathcal{F}) = 0$) siempre que $|\mathbb{P}^{(1)}(\mathbb{F}^{(m)})| \to \infty$. Sin embargo, estas técnicas no parecen ser efectivas para aproximarnos a nuestro problema.

Hemos aplicado también el "enfoque de los sistemas de Riemann-Roch" a un problema en el contexto de la complejidad de la multiplicación en cuerpos finitos. De forma más precisa, dado un cuerpo base $\mathbb{F}_q$ y una extensìón suya $\mathbb{F}_{q^k}$, un algoritmo de D.V. Chudnovsky y G.V. Chudnovsky permite trans-

formar el problema de multiplicar dos elementos de $\mathbb{F}_{q^k}$ en la computación de cierto número de productos de elementos de $\mathbb{F}_q$. La complejidad del producto es el número mínimo necesario de productos en el cuerpo base, que hemos denotado por $m(q,k)$. Shparlinski, Tsfasman y Vladut [73] extendieron este trabajo y estudiaron el problema asintóticamente, es decir, cuando q está fijo y k crece. Concretamente, uno de los valores que estudiaron fue el límite inferior de $m(q,k)/k$ para $k \in \mathbb{N}$, que hemos denotado por $\mu(q)$. Calcularon cotas inferiores y superiores para este valor, pero como hemos visto, había un paso injustificado en una de sus demostraciones, ya que no tuvieron en cuenta el papel del grupo $\mathrm{Cl}_0(\mathbb{F})[2]$, lo que afecta a las cotas superiores. Hemos identificado este error y hallado nuevas cotas utilizando las cotas obtenidas previamente para $|\mathrm{Cl}_0(\mathbb{F})[2]|$. Estas nuevas cotas superiores para $\mu(q)$, aunque relativamente cercanas, son peores que las presentadas en [73]. Es todavía un problema abierto el decidir si las cotas de [73] son válidas, lo que no es descartable, ya que las cotas *inferiores* conocidas para $\mu(q)$ son más pequeñas que ellas. De hecho, nuestra argumentación demuestra que las cotas de [73] serían válidas si $J_2(q, A(q)) = 0$.

Para concluir, queremos destacar que las técnicas empleadas en esta tesis también se pueden aplicar a algunas extensiones de los problemas estudiados aquí, de lo que nos ocuparemos en futuros trabajos. En primer lugar, podemos analizar el caso de los esquemas de compartición de secretos no perfectos con n fragmentos donde el secreto no es un único elemento de $\mathbb{F}_q$ sino un vector de longitud κn para cierto número real κ. El estudio de la multiplicación de este tipo de esquemas fue iniciado por Franklin y Yung, que consideraron en [36] una variación del esquema de Shamir en la que el secreto consiste en las evaluaciones de un polinomio en varios elementos del cuerpo y discutieron sus aplicaciones en computación multiparte. Podemos definir una generalización $\mathcal{C}_\kappa(\mathbb{F}_q)$ de la clase $\mathcal{C}(\mathbb{F}_q)$, y para un código C de esta clase y un conjunto de índices $T \subseteq \mathcal{I}(C)$, con $|T| = \kappa n(C)$, tomar como secreto el *subvector* $\pi_T(\mathbf{c})$, y como fragmentos el resto de coordenadas $\pi_i(\mathbf{c})$, $i \notin T$, para una palabra $\mathbf{c}$ tomada uniformemente al azar en C. Podremos generalizar entonces las nociones dadas en los capítulos 4 y 5, que ahora dependerán también del parámetro κ (la "longitud relativa del secreto") y aplicar el mismo tipo de técnicas explicadas en el resto de la tesis. En particular, será posible estimar la "tolerancia de corrupción *multisecreto* asintótica óptima" $\widehat{\tau}(q,\kappa)$. También queremos estudiar el caso de los esquemas de compartición de secretos en los que el secreto es un elemento de una extensión $\mathbb{F}_{q^k}$ de $\mathbb{F}_q$, los fragmentos son elementos de $\mathbb{F}_q$ y la propiedad de multiplicación fuerte se

define con respecto a los productos en los respectivos cuerpos. Un esquema con estas propiedades fue estudiado por primera vez por Cramer, Damgård y de Haan (ver [26]). En este caso, necesitaremos aplicar las técnicas de esta tesis a códigos lineales generalizados, donde una coordenada pertenece a la extensión del cuerpo. Algunos resultados relacionados con este problema han sido publicados en [18].

Hay otras extensiones del problema que son interesantes: podemos considerar el problema más general de esquemas de compartición de secretos en los que el producto de r secretos está determinado por los productos de los correspondientes conjuntos de r fragmentos, con $r \geq 2$. Necesitamos estudiar entonces el peso mínimo en un índice de la transformada del producto de Schur $C^{\circledast r}$ de un código C. Podemos aplicar la estrategia que consiste en plantear sistemas de ecuaciones de Riemann-Roch explicada en la parte III de esta tesis. En este caso, tendremos ecuaciones de la forma $\Delta_{P_0}(rX - D + P_A)$ y por tanto necesitaremos las cotas superiores para el tamaño de los límites de r-torsión $J_r(q, a)$ que obtuvimos en el capítulo 10 (notemos de nuevo que para las aplicaciones consideradas en esta tesis sólo hemos necesitado cotas para el caso particular $r = 2$, pero, de hecho, los resultados del capítulo 10 son más generales).

Finalmente, podemos analizar cuáles de nuestras construcciones disfrutan de la propiedad de t-independencia de fragmentos, que requiere la aplicación a la construcción de extractores de correlaciones de [47] que fue mencionada en la introducción. Esta propiedad se puede capturar imponiendo una condición sobre la distancia dual de los códigos. Todas las técnicas utilizadas en esta tesis dan lugar a esquemas de compartición de secretos con t-independencia de fragmentos para $t = \Omega(n)$ excepto aquellas que resultan de la aplicación de la técnica de descenso presentada en el capítulo 6, ya que como hemos visto en la sección 6.4, en este caso la distancia dual está acotada por cierta constante para todos los códigos de las familias que obtenemos. Todavía es una cuestión abierta determinar si para todo cuerpo finito $\mathbb{F}_q$ hay una familia de códigos $\{C^{(m)}\}_{m>0} \subseteq \mathcal{C}^{\dagger}(\mathbb{F}_q)$ con $n(C^{(m)}) \to \infty$ verificando no sólo que $\widehat{\tau}(C^{(m)}) \to \tau > 0$ sino también que $d((C^{(m)})^{\perp})/n(C^{(m)}) \to \delta > 0$. Actualmente, sólo podemos demostrar este hecho para cuerpos finitos para los que es posible probar que $\widehat{\tau}(q) > 0$ sin recurrir a la técnica del descenso, lo que es el caso para todos los cuerpos finitos $\mathbb{F}_q$ con q cuadrado y $q \geq 9$ (se puede comprobar en los resultados detallados en la Tabla 11.1).

Bibliography

[1] S. Ballet. Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$. *Finite Fields Appl.* 5 (1999), pp. 364–377.

[2] S. Ballet. An improvement of the construction of the D. V. and G. V. Chudnovsky algorithm for multiplication in finite fields. *Theoret. Comput. Sci.* 352 (2006), pp. 293–305.

[3] S. Ballet. On the tensor rank of the multiplication in the finite fields. *Journal of Number Theory* 128 (2008), pp. 1795–1806.

[4] S. Ballet. A note on the tensor rank of the multiplication in certain finite fields. *Algebraic geometry and its applications*, pp. 332–342, Ser. Number Theory Appl., 5, World Sci. Publ., Hackensack, NJ, 2008.

[5] S. Ballet and D. Le Brigand On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$. *J. Number Theory* 116 (2006), no. 2, pp. 293–310.

[6] S. Ballet, J. Chaumine. On the bounds of the bilinear complexity of multiplication in some finite fields. *Appl. Algebra Engrg. Comm. Comput.* 15 (2004), pp. 205–211.

[7] S. Ballet, R. Rolland. Multiplication algorithm in a finite field and tensor rank of the multiplication. *J. Algebra*, 272 (1) (2004), pp. 173–185.

[8] S. Ballet, R. Rolland. On the bilinear complexity of the multiplication in finite fields. *Séminaires & Congrès* 11 (2005), pp. 179–188.

[9] A. Bassa, A. Garcia and H. Stichtenoth. A new tower over cubic finite fields. *Moscow Mathematical Journal*, Vol. 8, No. 3, September 2008, pp. 401–418.

[10] M. Ben-Or, S. Goldwasser and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proceedings of STOC 1988*, pp. 1–10. ACM Press, 1988.

[11] J. Bezerra, A. Garcia and H. Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink's lower bound. *Journal für die reine und angewandte Mathematik*, vol. 589, December 2005, pp. 159–199.

[12] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings*, 48 (1979), pp. 313–317.

[13] G.R. Blakley and G.A. Kabatianski. Ideal Perfect Threshold Schemes and MDS Codes *IEEE Conference Proc., Internation Symposium on Information Theory, ISIT 95* (1995), p.488.

[14] P. Bogetoft, D.L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, M. Schwartzbach, T. Toft. Secure Multiparty Computation Goes Live Report available at: `http://eprint.iacr.org/2008/068.pdf`

[15] I. Cascudo, H. Chen, R. Cramer, C. Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over *Any* Fixed Finite Field. *Advances in Cryptology- CRYPTO 2009*, Springer Verlag LNCS, vol. 5677, pp. 466–486, August 2009.

[16] I. Cascudo, R. Cramer, C. Xing. Torsion-limits for towers and asymptotically good special codes in secure computation and complexity. Manuscript, 2010.

[17] I. Cascudo, R. Cramer, C. Xing. Upper bounds on asymptotic optimal corruption tolerance in strongly multiplicative linear secret sharing. Manuscript, 2010.

[18] H. Chen, R. Cramer, R. de Haan, I. Cascudo Pueyo. Strongly multiplicative ramp schemes from high degree rational points on curves. *Advances in Cryptology- EUROCRYPT 2008*, Springer Verlag LNCS, vol. 4965, pp. 451–470, April 2008.

[19] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan. Secure Computation from Random Error Correcting Codes. *Advances*

in Cryptology- EUROCRYPT 2007, Springer Verlag LNCS, vol. 4515, pp. 329–346, May 2007.

[20] H. Chen and R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computation over Small Fields. *Advances in Cryptology- CRYPTO 2006*, Springer Verlag LNCS, vol. 4117, pp. 516–531, August 2006.

[21] D. Chaum, C. Crépeau and I. Damgård. Multi-party unconditionally secure protocols. *Proceedings of STOC 1988*, pp. 11–19. ACM Press, 1988.

[22] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults. *Proceedings of 26th Annual IEEE FOCS 1985*, pp. 383–395, 1985.

[23] D.V. Chudnovsky, G.V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Proceedings of the National Academy of Sciences of the United States of America*, vol. 84, no. 7, pp. 1739–1743, April 1987.

[24] T. M. Cover, J. A. Thomas. Elements of Information Theory. Wiley-Interscience, 2006.

[25] R. Cramer and I. Damgård. Zero-Knowledge Proofs for Finite Field Arithmetic; or: Can Zero-Knowledge be for Free? *Advances in Cryptology- CRYPTO 1998*, Springer-Verlag, vol. 1462, pp. 424–441, August 1998.

[26] R. Cramer, I. Damgård and R. de Haan. Atomic secure multi-party multiplication with low communication. In *Advances in Cryptology- EUROCRYPT 2007*, volume 4515, pp. 329–346. Springer Verlag LNCS, May 2007.

[27] R. Cramer, I. Damgård and J. B. Nielsen. Multiparty Computation, an Introduction. Lecture Notes, available at `http://www.daimi.au.dk/~ivan/smc.pdf`.

[28] R. Cramer, V. Daza, I. Gracia, J. Jimenez Urroz, G. Leander, J. Martí-Farré and C. Padró. On codes, matroids and secure multi-party computation from linear secret sharing schemes. *Advances in Cryptology- CRYPTO 2005*, Springer-Verlag, vol. 3621, pp. 327–343, August 2005.

[29] R. Cramer, S. Fehr, M. Stam. Primitive Sets over Number Fields and Black-Box Secret Sharing. *Advances in Cryptology- CRYPTO 2005*, Springer Verlag LNCS, vol. 3621, pp. 344–360, August 2005.

[30] R. Cramer and S. Fehr. Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups. *Advances in Cryptology- CRYPTO 2002*, Springer Verlag LNCS, vol. 2442, pp. 272–287, August 2002.

[31] R. Cramer, I. Damgård and S. Dziembowski. On the complexity of verifiable secret sharing and multi-party computation. *Proceedings of STOC 2000*, pp. 325–334. ACM Press, 2000.

[32] R. Cramer, I. Damgård and U. Maurer. General secure multi-party computation from any linear secret sharing scheme. *Advances in Cryptology- EUROCRYPT 2000*, Springer Verlag LNCS, vol. 1807, pp. 316–334, May 2000.

[33] I. Damgård, Y. Ishai. Scalable Secure Multiparty Computation. *Advances in Cryptology- CRYPTO 2006*, Springer Verlag LNCS, vol. 4117, pp. 501–520, August 2006.

[34] I. Damgård, J. Buus Nielsen, D. Wichs. Isolated Proofs of Knowledge and Isolated Zero Knowledge. *Advances in Cryptology- EUROCRYPT 2008*, Springer Verlag LNCS, vol. 4965, pp. 509–526, May 2008.

[35] Y. Desmedt and Y. Frankel. Threshold Cryptosystems. *Advances in Cryptology- CRYPTO 89*, Springer Verlag LNCS, vol. 435 , pp. 307–315, August 1989.

[36] M. Franklin and M. Yung. Communication complexity of secure computation. *Proceedings of STOC 1992*, pages 699–710. ACM Press, 1992.

[37] A. Garcia and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound. *Invent. Math.* 121, pp. 211–222, 1995.

[38] A. Garcia, H. Stichtenoth. On the asymptotic behavior of some towers of function fields over finite fields. *J. Number Theory*, 61 (1996), pp. 248–273.

[39] G. van der Geer and M. van der Vlugt. An asymptotically good tower of function fields over the field with eight elements. *Bull. London Math. Soc.* 34 (2002), pp. 291–300.

[40] O. Goldreich, S. Micali and A. Wigderson. How to Play any Mental Game or a Completeness Theorem for Protocols with Honest Majority. In *Proceedings of ACM STOC 1987*, pp. 218–229, 1987.

[41] V. D. Goppa. Codes on algebraic curves. *Soviet Math. Dokl*, 24 (1981), pp. 170–172.

[42] R. de Haan. Algebraic Techniques for Low Communication Secure Protocols. PhD. Thesis. Leiden University, 2009. Available at `http://www.bsik-bricks.nl/documents/2009_PhD_Haan.pdf`.

[43] M. Hirt, U. Maurer. Player Simulation and General Adversary Structures in Perfect Multiparty Computation. *Journal of Cryptology*, Springer-Verlag, vol. 13, no. 1, pp. 31–60, Apr 2000.

[44] W. G. Huffman, V. Pless. Fundamentals of Error Correcting Codes. Cambridge University Press, 2003.

[45] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Tokyo* 28 (1981), 3:721–724.

[46] Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. Zero-knowledge from secure multiparty computation. *Proceedings of 39th STOC*, San Diego, Ca., USA, pp. 21–30, 2007.

[47] Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. Extracting Correlations. *Proceedings of 50th Annual IEEE FOCS, 2009*, to appear.

[48] Y. Ishai, M. Prabhakaran, A. Sahai. Founding Cryptography on Oblivious Transfer–Efficiently. *Advances in Cryptology- CRYPTO 2008*, Springer Verlag LNCS, vol. 5157, pp. 572–591, August 2008.

[49] M. Karchmer and A. Wigderson. On span programs. *Proceedings of the Eigth Annual Structure in Complexity Theory Conference*, pp. 102–111, IEEE, 1993.

[50] E.D. Karnin, J.W. Greene and M. Hellman. On Secret Sharing Systems. *IEEE Transactions on Information Theory*, Vol. IT-29, January 1983, pp. 35–41.

[51] G. Lachaud and M. Martin-Deschamps. Nombre de points des jacobiennes sur un corps fini. *Acta Arith.* 56 (1990), pp. 329–340.

[52] J. H. van Lint. *Introduction to Coding Theory.* Graduate Texts in Mathematics. Springer Verlag, 1999.

[53] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*(11th impression), North Holland, 2003.

[54] H. Maharaj. A Note on Further Improvements of the TVZ-Bound. *IEEE Trans. Inf. Theory* 53(3):1210–1214 (2007).

[55] Y. I. Manin. What is the maximal number of points on a curve over $\mathbb{F}_2$? *J. Fac. Sci. Univ. Tokyo* 28, pp. 715–720 (1981).

[56] J. L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6-th Joint Swedish-Russian Workshop on Information Theory*, pp. 269–279, Molle, Sweden, August 1993.

[57] J. L. Massey. Some applications of coding theory in cryptography. *Codes and Ciphers: Cryptography and Coding IV*, pp. 33–47, 1995.

[58] J. S. Milne. Abelian Varities. Online lecture notes, 2009.

[59] D. Mumford. Abelian Varieties. Oxford University Press, 1970.

[60] H. Niederreiter, F. Özbudak. Improved Asymptotic Bounds for Codes Using Distinguished Divisors of Global Function Fields. *SIAM J. Discrete Math.* 21(4): 865–899 (2007).

[61] H. Niederreiter, C. Xing. Low-Discrepancy Sequences and Global Function Fields with Many Rational Places. *Finite Fields and Their Applications* 2 (1996), pp. 241–273.

[62] H. Niederreiter, C. Xing. Towers of global function fields with asymptotically many rational places and an improvement on Gilbert-Varshamov bound. *Mathematische Nachrichten* 195, pp. 171–186 (1998).

[63] H. Niederreiter, C. Xing. Rational points on curves over finite fields: theory and applications. Cambridge University Press, 2001.

[64] R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.*, vol. 106/107 (1992), pp. 369–381.

[65] R. Pellikaan, B.-Z. Shen, G. J. M. van Wee. Which linear codes are algebraic-geometric? *IEEE Transactions on Information Theory* 37(3): 583–602 (1991)

[66] V. Pless and W. C. Huffman. Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003.

[67] E. M. Rains and N. J. A. Sloane. Self-Dual Codes. Survey written for the Handbook of Coding Theory, 1998. Available at `http://www.research.att.com/~njas/`

[68] M. Rosen. Number Theory in Function Fields. GTM, Springer, 2001.

[69] G. Seroussi, A. Lempel. Factorization of Symmetric Matrices and Trace-Orthogonal Bases in Finite Fields. *SIAM J. Comput.* 9(4): 758–767, 1980.

[70] J. -P. Serre. Sur le nombre des points rationnels d'une courbe algébraique sur une corps fini. *C.R.Acad.Sci* Paris 296, pp. 397–402, 1983.

[71] J. -P. Serre. Rational points on curves over finite fields. 1985, notes of lectures at Harvard University.

[72] A. Shamir. How to share a secret. *Comm. of the ACM*, 22(11):612–613, 1979.

[73] I. Shparlinski, M. Tsfasman, S. Vlăduţ. Curves with many points and multiplication in finite fields. *Coding Theory and Algebraic Geometry*, 145–169, Springer Verlag, 1992.

[74] J. H. Silverman. The Arithmetic of Elliptic Curves. Springer Verlag, 2009.

[75] H. Stichtenoth. Algebraic function fields and codes, 2nd edition. Springer Verlag, 2008.

[76] M. Tsfasman, S. G. Vlăduţ. Algebraic-geometric codes. Kluwer Academic Publishers, 1991.

[77] M. Tsfasman, S. G. Vlăduţ, D. Nogin. Algebraic-geometric codes: Basic Notions. *AMS, Mathematical Surveys and Monographs*, Vol. 139, 2007.

[78] M. Tsfasman, S. G. Vlăduţ, T. Zink. Modular curves, Shimura curves and Goppa codes, better than the Gilbert-Varshamov bound *Mathematische Nachrichten*, vol. 109 (1982), pp.21–28.

[79] S. G. Vlăduţ. An exhaustion bound for algebro-geometric modular codes. *Probl. Inf. Transm.*, vol. 23 (1987), pp. 22–34.

[80] A. Weil. Variétés Abéliennes et Courbes Algébriques. Hermann, Paris, 1948.

[81] C. Xing. Algebraic geometry codes with asymptotic parameters better than the Gilbert-Varshamov and the Tsfasman-Vlăduţ-Zink bounds. *IEEE Trans. on Inf. Theory*, 47(1): 347–352 (2001).

[82] C. Xing. Goppa Geometric Codes Achieving the Gilbert-Varshamov Bound. *IEEE Trans. on Inf. Theory*, 51(1): 259–264 (2005).

[83] C. Xing and H. Chen. Improvements on parameters of one-point AG codes from Hermitian curves. *IEEE Trans. on Inf. Theory*, 48(2): 535–537 (2002).

[84] C. Xing and S. L. Yeo. Algebraic curves with many points over the binary field. *Journal of Algebra*, Volume 311, Issue 2 (2007), pp. 775–780.

[85] L. Xu. Improvement on parameters of Goppa geometry codes from maximal curves using the Vlăduţ-Xing method. *IEEE Trans. on Inf. Theory*, 51(6): 2207–2210 (2005).

[86] T. Zink. Degeneration of Shimura surfaces and a problem in coding theory. *Fundamentals of Computation Theory*, Springer Verlag LCNS, vol. 199 (1985), pp. 503–511.