

Torsion Limits and Riemann-Roch Systems for Function Fields and Applications*

Ignacio Cascudo[†] Ronald Cramer[‡] Chaoping Xing[§]

Abstract

The Ihara limit (or constant) $A(q)$ has been a central problem of study in the asymptotic theory of global function fields (or equivalently, algebraic curves over finite fields). It addresses global function fields with many rational points and, so far, most applications of this theory do not require additional properties. Motivated by recent applications, we require global function fields with the additional property that their zero class divisor groups contain at most a small number of d -torsion points. We capture this with the notion of torsion limit, a new asymptotic quantity for global function fields. It seems that it is even harder to determine values of this new quantity than the Ihara constant. Nevertheless, some non-trivial upper bounds are derived. Apart from this new asymptotic quantity and bounds on it, we also introduce Riemann-Roch systems of equations. It turns out that this type of equation system plays an important role in the study of several other problems in each of these areas: arithmetic secret sharing, symmetric bilinear complexity of multiplication in finite fields, frameproof codes and the theory of error correcting codes. Finally, we show how our new asymptotic quantity, our bounds on it and Riemann-Roch systems can be used to improve results in these areas.

Keywords: Algebraic curves, Jacobian, torsion limit, Ihara limit, secret sharing, complexity of multiplication, frameproof codes

1 Introduction

Since the discovery of algebraic geometry codes by Goppa [30] and other applications such as low-discrepancy sequences [44], the study of algebraic curves with many rational points over finite fields or, equivalently, global function fields with many rational places, has attracted many researchers from various areas, such as pure mathematicians, coding theorists and algorithmically inclined mathematicians. In the last two decades, there have been tremendous research activities in this topic.

A crucial quantity in the asymptotic theory of global function fields with many rational places, namely the Ihara limit, plays an important role in coding theory and other topics. Precisely speaking, for a given prime power q , the Ihara limit is defined by

$$A(q) := \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g},$$

where $N_q(g)$ denotes the maximum number of rational places taken over all global function fields over $\mathbb{F}_q$ of genus g .

*Version accepted for publication in *IEEE Transactions on Information Theory*. DOI: 10.1109/TIT.2014.2314099, URL (early access version): <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6779612>. Copyright (c) 2012 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. This is an extended version of our paper [15] in Proceedings of 31st Annual IACR CRYPTO, Santa Barbara, Ca., USA, 2011. The results in Sections 5 and 6 did not appear in [15]. A first version of this paper has been widely circulated since November 2009. I. Cascudo was supported in part by the STW Sentinels program under Project 10532 and in part by Cramer’s NWO VICI Grant “Mathematics of Secure Computation”. R. Cramer was supported in part by NWO VICI Grant “Mathematics of Secure Computation.” C. Xing was supported by the Singapore Minister of Education under Tier 1 grant RG20/13.

[†]CWI Amsterdam, The Netherlands (at the time of this research; currently at Aarhus University, Denmark). Email: ignacio@cs.au.dk.

[‡]CWI Amsterdam & Mathematical Institute, Leiden University, The Netherlands. Email: cramer@cw.nl, cramer@math.leidenuniv.nl.

[§]Division of Mathematical Sciences, Nanyang Technological University, Singapore. Email: xingcp@ntu.edu.sg.

The Drinfeld-Vlăduţ bound states that $A(q) \leq \sqrt{q} - 1$. By Ihara [35], $A(q) = \sqrt{q} - 1$ if q is a square. By Serre’s Theorem [51], $A(q) \geq c \cdot \log q$ for some absolute real constant $c > 0$ (for which the current best lower bound [45] is approximately $\frac{1}{96}$).

So far, most applications of global function fields do not require additional properties. Motivated by recent applications (arithmetic secret sharing, see below), we require global function fields with the additional property that their zero divisor class groups contain at most a small number of d -torsion points. The exact same requirements are relevant for the study of the symmetric bilinear complexity of multiplication in finite fields. Although the latter topic started much earlier, the role of 2-torsion points in the zero class divisor groups was overlooked in [53, 2].

In this paper, we introduce two new primitives for function fields over finite fields, namely the torsion limit and systems of Riemann-Roch equations. Our torsion limit, which we believe is of independent interest, can in general be upper bounded using Weil’s classical theorem on torsion in Abelian varieties (and in many cases using the Weil-pairing).¹ However, the resulting bound is far too pessimistic, as we present a tower for which our torsion limit is *considerably smaller*, yet it attains the Drinfeld-Vlăduţ bound.

A system of Riemann-Roch equations consists of simultaneous equations whose variables are divisors. Although Riemann-Roch systems have been implicitly studied in coding theory [59, 62, 65, 64, 68, 40, 42] such a concept has not been formally introduced. Moreover, we are interested in systems of a more general type than the ones considered in those papers, as we will explain. In several interesting cases, the existence of solutions will depend very much on the torsion in the class group. Hence, in the asymptotic case, where we consider Riemann-Roch systems in a tower of function fields, its solvability will depend on our new torsion limit.

We give three applications in this paper that demonstrate the importance of such systems, in conjunction with our torsion limit and bounds on it. First, arithmetic secret sharing schemes are a special kind of codes arising in secure multi-party computation [23, 18]. Using optimal towers of function fields, Chen and Cramer [18] showed the existence of “asymptotically good” families of such schemes. Since then, the asymptotical results of [18] have had several important and surprising applications in *two-party* cryptography [37, 39, 31, 38, 24, 36]. The results of [18] were improved and extended in [20, 14]. We show how our torsion limits and Riemann-Roch equations allow to further improve those results.

In fact, the arguments from [18] also show the existence of linear codes such that both the duals and “powers” are simultaneously asymptotically good, where we define the d -th power C^{*d} of a linear code C to be the linear code spanned by all possible coordinate-wise products of d (not necessarily distinct) words in C . The results in [18] imply that for any fixed integer $d \geq 2$ and for any finite field $\mathbb{F}_q$ such that $A(q) > 2d$ there exist families of codes C such that both $C, C^\perp$ and the powers $C^{*d'}$ with $2 \leq d' \leq d$ are simultaneously asymptotically good. Interestingly, if we want to extend these results to other finite fields, the concatenation techniques of [14] come to no avail, as opposed to the case of secret sharing schemes. Our results in the paper show the existence of such asymptotically good families of codes for several small finite fields for which it was so far not yet established. For instance, for $d = 2$, we show that the result holds for any finite field $\mathbb{F}_q$, $q \geq 8$, except perhaps for $q = 11, q = 13$; in comparison, [18] only showed this result in the case $A(q) > 4$, which cannot hold when $q \leq 25$.

Second, we consider bounds in the context of extension field multiplication. Shparlinski, Tsfasman, and Vlăduţ [53] initiated study of asymptotics, finding upper bounds for the limits m_q, M_q defined in that paper. We start by noticing a gap in the proof of their main result: there is an implicit but unjustified assumption on the possibilities of positive Ihara limits in combination with the absence of non-trivial 2-torsion. The same gap exists in a more recent paper (2008) on the same subject by Ballet [2]. Therefore the upper bounds stated for m_q in those papers are not justified. On the other hand, Randriambololona recently proved in [47] that the bound for m_q in [53] can indeed be attained in the case $A(q) > 5$. We examine the connection of this extension field multiplication problem to the solvability of a system of Riemann-Roch equations, and obtain bounds that significantly improve the state of the art for some small fields by incorporating our limit and corresponding tower. In addition, we also show how to improve the state of the art [16] regarding the upper bounds for the other limit, M_q over small finite fields $\mathbb{F}_q$. Third, frameproof codes were introduced in the context of

¹We note that, independently, Randriambololona [46] introduced the same notion of torsion limit (for optimal families of function fields) in the context of an application to the construction of frameproof codes and proved the bounds that follow directly from Weil’s classical result.

digital fingerprinting by Boneh and Shaw in [13] although a slightly different definition, which we will be using, was proposed afterwards by Fiat and Tassa [25], see also [11]. The asymptotic properties of such codes have been studied in [46, 48, 63]. We show how to improve those bounds in some cases.

This paper is organized as follows. Our main contributions are captured in Definition 2.2 (the torsion limit), Theorem 2.3 (bounds for this limit), Theorem 3.2 (sufficient conditions for Riemann-Roch system solvability), Theorems 4.13 and 4.15 (claimed arithmetic secret sharing schemes), Theorems 5.9 and 5.18 (improvements on multiplication complexity of finite field extensions) and Theorem 6.16 (improvements on asymptotical constructions for frameproof codes). After giving some preliminaries in Section 2.1, we introduce our torsion limit in Section 2.2 and show our bounds. In Section 3 we introduce Riemann-Roch systems of equations and show how these may be solved using the bounds from Section 2. We also include a short discussion on efficient randomized solving strategies. In Section 4 we discuss how to obtain the claimed arithmetic secret sharing schemes and linear codes with good duals and powers. In Section 5 we show how our torsion limit and Riemann-Roch system can be applied to study the symmetric bilinear complexity of multiplication in finite fields. Finally in Section 6 we show our application to the asymptotical study of frameproof codes.

2 Torsion Limits

2.1 Preliminaries

For convenience of the reader, we start with some definitions and notations.

For a prime power q , let $\mathbb{F}_q$ be a finite field of q elements. An *algebraic function field* over $\mathbb{F}_q$ in one variable is a field extension $F \supset \mathbb{F}_q$ such that F is a finite algebraic extension of $\mathbb{F}_q(x)$ for some $x \in F$ that is transcendental over $\mathbb{F}_q$. It is assumed that $\mathbb{F}_q$ is its full field of constants, i.e., the algebraic closure of $\mathbb{F}_q$ in F is $\mathbb{F}_q$ itself.

The following notations will be used throughout the rest of the paper.

- $F/\mathbb{F}_q$ —a function field with full constant field $\mathbb{F}_q$;
- $g(F)$ —the genus of F ;
- $N(F)$ —the number of rational places of F ;
- $\mathbb{P}(F)$ —the set of places of F (note that $\mathbb{P}(F)$ is an infinite set);
- $\mathbb{P}^{(k)}(F)$ —the set of places of degree k of F (note that $\mathbb{P}^{(k)}(F)$ is a finite set);
- $N_i(F)$ —the number of $\mathbb{F}_{q^i}$ -rational places, i.e., $N_i(F) = \sum_{j|i} j |\mathbb{P}^{(j)}(F)|$ (note that $N(F) = N_1(F)$);
- $\text{Div}(F)$ —the divisor group of F ;
- $\text{Div}^0(F)$ —the divisor group of degree 0;
- $\text{Prin}(F)$ —the principal divisor group of F ;
- $\text{Cl}(F)$ —the divisor class group $\text{Div}(F)/\text{Prin}(F)$ of F ;
- $\text{Cl}_0(F) = \mathcal{J}_F$ —the degree zero divisor class group $\text{Div}^0(F)/\text{Prin}(F)$ of F (note that $\text{Cl}_0(F)$ is a finite group);
- $\mathcal{J}_F[r]$ —the group of r -torsion points in $\mathcal{J}_F$.
- $h(F) = |\text{Cl}_0(F)|$ —the zero divisor class number;
- $\mathcal{A}_r(F)$ —the set of effective divisors of degree $r \geq 0$ (note that $\mathcal{A}_r(F)$ is a finite set);
- $A_r(F)$ —the cardinality of $\mathcal{A}_r(F)$;
- $\text{Cl}_r(F)$ —the set $\{[D] : \deg(D) = r\}$, where $[D]$ stands for the divisor class containing D .

In case there is no confusion, we omit the function field F in some of the above notations. For instance, $A_r(F)$ is denoted by A_r if it is clear in the context.

For a divisor G of F , we define the Riemann-Roch space by

$$\mathcal{L}(G) := \{f \in F^* : \operatorname{div}(f) + G \geq 0\} \cup \{0\}.$$

Then $\mathcal{L}(G)$ is a finite dimensional space over $\mathbb{F}_q$ and its dimension $\ell(G)$ is determined by the Riemann-Roch theorem which gives

$$\ell(G) = \deg(G) + 1 - g(F) + \ell(K - G),$$

where K is a canonical divisor of degree $2g(F) - 2$. Therefore, we always have that $\ell(G) \geq \deg(G) + 1 - g(F)$ and the equality holds if $\deg(G) \geq 2g(F) - 1$.

The zeta function of F is defined by the following power series

$$Z_F(t) := \operatorname{Exp} \left(\sum_{i=1}^{\infty} \frac{N_i(F)}{i} t^i \right) = \sum_{i=0}^{\infty} A_i(F) t^i.$$

Then Weil showed that $Z_F(t)$ is in fact a rational function of the form

$$Z_F(t) = \frac{L_F(t)}{(1-t)(1-qt)},$$

where $L_F(t)$ is a polynomial of degree $2g(F)$ in $\mathbb{Z}[t]$, called *L-polynomial* of F . Furthermore, $L_F(0) = 1$. If we factorize $L_F(t)$ into a linear product $\prod_{i=1}^{2g(F)} (w_i t - 1)$ in $\mathbb{C}[t]$, then Weil showed that $|w_i| = \sqrt{q}$ for all $1 \leq i \leq 2g(F)$.

From the definition of zeta function, one obtains

$$N_m(F) = q^m + 1 - \sum_{i=1}^{2g(F)} w_i^m$$

for all $m \geq 1$. This gives the Hasse-Weil bound

$$N(F) = N_1(F) \leq q + 1 + 2g(F)\sqrt{q}.$$

Function fields F with a large number $N(F)$ of rational points have a bearing on problems in coding theory [57, 55] as well as, for instance, in low-discrepancy sequences [44] and several problems in cryptography [18, 43]. In particular, the following quantity is relevant:

$$N_q(g) = \max_F N(F),$$

where F ranges over all function fields of genus g over $\mathbb{F}_q$.

One can imagine that it is not easy at all to determine the exact value $N_q(g)$ for an arbitrary pair (q, g) . The complete solution to this problem has been found only for $g = 0, 1, 2$ [51]. The reader may refer to [29] for a table of values of $N_q(g)$ for some small values of q and g .

In order to study the asymptotic behavior of $N_q(g)$ when q is fixed and g tends to ∞ , we can define the following asymptotic quantity

$$A(q) := \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g}.$$

An upper bound on $A(q)$ was given by Vlăduț and Drinfeld [60]

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

For applications, we are more interested in finding lower bounds on this asymptotic quantity. Ihara [35] first showed by using modular curves that $A(q) \geq \sqrt{q} - 1$ for any square power q . This result determines the exact value $A(q)$ for all square powers, i.e.,

$$A(q) = \sqrt{q} - 1. \tag{2.1}$$

On the other hand, no single value of $A(q)$ is known if q is a non-square. However, some lower bounds have been obtained so far. For instance, by using modular curves and explicit function fields, Zink [69], Bezerra-Garcia-Stichtenoth [10] and Bassa-Garcia-Stichtenoth [8] showed that

$$A(q^3) \geq \frac{2(q^2 - 1)}{q + 2}. \quad (2.2)$$

Recently, Garcia-Stichtenoth-Bassa-Beelen [7] produced an explicit tower of function fields over finite fields $\mathbb{F}_{p^{2m+1}}$ for any prime p and integer $m \geq 1$ and showed that this tower gives

$$A(p^{2m+1}) \geq \frac{2(p^{m+1} - 1)}{p + 1 + \epsilon} \quad \text{with} \quad \epsilon = \frac{p - 1}{p^m - 1}.$$

Serre made use of class field theory to show that there is an absolute positive constant c such that

$$A(q) \geq c \cdot \log(q)$$

for every prime power q .

On the other direction, lower bounds on $A(q)$ have already been obtained for small prime q such as $q = 2, 3, 5, 7, 11, 13, \dots$ etc. For instance, in [66], Xing and Yeo showed that

$$A(2) \geq 0.258.$$

For a family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \rightarrow \infty$ such that $\lim_{g(F) \rightarrow \infty} N(F)/g(F)$ exists, one can define this limit to be the *Ihara limit*, denoted by $A(\mathcal{F})$. It is clear that there exists a family $\mathcal{E} = \{E/\mathbb{F}_q\}$ of function fields such that $g(E) \rightarrow \infty$ and the Ihara limit $A(\mathcal{E})$ is equal to $A(q)$.

Remark 2.1. *In general, we can define the Ihara limit for any family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \rightarrow \infty$ by $\limsup_{g(F) \rightarrow \infty} N(F)/g(F)$. However, for convenience of this paper, we define the Ihara limit only for those families $\{E/\mathbb{F}_q\}$ whose limit $\lim_{g(E) \rightarrow \infty} N(E)/g(E)$ exists.*

2.2 Torsion Limits

Due to some recent applications to arithmetic secret sharing and multiplications in finite field extensions, we are interested in considering, in addition to the Ihara limit of a family of function fields, a limit for the number of torsion points of the zero divisor class groups of these function fields.

Let $F/\mathbb{F}_q$ be a function field. For a positive integer r larger than 1, we denote by $\mathcal{J}_F[r]$ the r -torsion point group in $\mathcal{J}_F$, i.e.,

$$\mathcal{J}_F[r] := \{[D] \in \mathcal{J}_F : r[D] = 0\}.$$

The cardinality of $\mathcal{J}_F[r]$ is denoted by $J_F[r]$.

For each family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \rightarrow \infty$, we define the asymptotic limit

$$J_r(\mathcal{F}) := \liminf_{F \in \mathcal{F}} \frac{\log_q |\mathcal{J}_F[r]|}{g(F)}.$$

We need to define an asymptotic notion involving both $J_r(\mathcal{F})$ and the Ihara limit $A(\mathcal{F})$.

Definition 2.2. *For a prime power q , an integer $r > 1$ and a real $a \leq A(q)$, let $\mathfrak{F}$ be the set of families $\{\mathcal{F}\}$ of function fields over $\mathbb{F}_q$ such that the genus in each family tends to ∞ and the Ihara limit $A(\mathcal{F}) \geq a$ for every $\mathcal{F} \in \mathfrak{F}$. Then the asymptotic quantity $J_r(q, a)$ is defined by*

$$J_r(q, a) = \liminf_{\mathcal{F} \in \mathfrak{F}} J_r(\mathcal{F}).$$

Thus, for a given family, our limit $J_r(\mathcal{F})$ measures the r -torsion against the genus. The corresponding constant $J_r(q, a)$ measures, for a given Ihara limit a and for given r , the “least possible r -torsion.” Note that $A(q)$, Ihara’s constant, is the supremum of $A(\mathcal{F})$ taken over all asymptotically good $\mathcal{F}$ over $\mathbb{F}_q$. For some applications such as multiplication in extension fields in Subsection 4.2, one may be interested in function fields with many places of higher degree and small torsion limit. The above definition could be modified by replacing the Ihara limit by the limit of number of places of higher degree against genus.

Now we are ready to state the main result of this section.

Theorem 2.3. *Let $\mathbb{F}_q$ be a finite field and let $r > 1$ be a prime.*

- (i) *If $r \mid (q - 1)$, then $J_r(q, A(q)) \leq \frac{2}{\log_r q}$.*
- (ii) *If $r \nmid (q - 1)$, then $J_r(q, A(q)) \leq \frac{1}{\log_r q}$.*
- (iii) *If q is square and $r \mid q$, then $J_r(q, \sqrt{q} - 1) \leq \frac{1}{(\sqrt{q}+1) \log_r q}$.*

The *first* part of Theorem 2.3, as well as the second part when, additionally, $r \mid q$, is proved directly using a theorem of Weil [61, 41] on torsion in Abelian varieties. For any non-zero integer m , this theorem, which holds over *algebraically closed* fields K , says that the m -torsion point group $A[m]$ of the variety, is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2g}$ if m is co-prime to the characteristic p of K ; and $A[p]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^a$ for a non-negative integer $a \leq g$, where g is the dimension of A . See also [50]. Clearly, this implies upper bounds when the field is not algebraically closed. The second part, in the case $r \nmid (q - 1)$, can be proved by using the Weil pairing for abelian varieties (see [15]). The most interesting part is the bound in the *third part*, which is substantially smaller (see Subsection 2.3 for the detailed proof). Note that this last bound applies to families which attain the Drinfeld-Vlăduț bound.

By using a lifting idea, we are able to obtain an upper bound on the size of the r^t -torsion point group of an abelian variety from its r -torsion point group, and hence we can derive the following result from Theorem 2.3 (see [15] for the detailed proof).

Theorem 2.4. *Let $\mathbb{F}_q$ be a finite field of characteristic p .*

- (i) *If $m \geq 2$ is an integer, then $J_m(q, A(q)) \leq \log_q(dm)$, where $d = \gcd(m, q - 1)$.*
- (ii) *Write m into $p^\ell m'$ for some $\ell \geq 0$ and an positive integer m' co-prime to p . If q is a square, then $J_m(q, \sqrt{q} - 1) \leq \frac{\ell}{\sqrt{q}+1} \log_q(p) + \log_q(cm')$, where $c = \gcd(m', q - 1)$.*

At the time when an earlier version of this paper was being prepared, Randriambololona independently introduced in [46] the limit $J_r(q, A(q))$, in the context of an application to the construction of frameproof codes. Moreover he stated the bounds in the first part of Theorem 2.3, the second part of Theorem 2.3 when $r \mid q$ and the first part of Theorem 2.4 when m is a power of p .

Like the Ihara-constant $A(q)$, it could be extremely difficult to determine the exact value of $J_r(q, a)$ for given a and q , and we would like to leave this as an open problem. Also, in the context of solving general Riemann-Roch systems (see Section 3) it makes sense to extend the definition of the limit above to the case of r -torsion for a finite set of positive integers r *simultaneously*.

Another particular interesting case is $q = 2$. The following result gives a bound on the 2-torsion limit for the family of function fields given in [66].

Theorem 2.5. *The family $\mathcal{F}$ of function fields over $\mathbb{F}_2$ with the Ihara's limit 97/376 given in [66] has 2-torsion limit $J_2(\mathcal{F})$ at most 216/376.*

The proof of Theorem 2.5 will be given in Subsection 2.3. Note that the bound in Theorem 2.3 gives only $J_2(\mathcal{F}) \leq 1$.

Finally, one can show existence of certain function field families that is essential for our applications of Sections 4 and 5.

Theorem 2.6. *For every prime power $q \geq 8$ except perhaps for $q = 11$ or 13, there exists a family $\mathcal{F}$ of function fields over $\mathbb{F}_q$ such that the Ihara limit $A(\mathcal{F})$ exists and it satisfies $A(\mathcal{F}) > 1 + J_2(\mathcal{F})$.*

Again we refer to [15] for the detailed proof of Theorem 2.6.

2.3 Proof of Theorems 2.3(iii) and 2.5

Let $\mathbb{F}_q$ be a finite field. Write p for its characteristic. For a function field F over $\mathbb{F}_q$, denote by $\gamma(F)$ the $\mathbb{F}_p$ -dimension of $\mathcal{J}_F[p]$, i.e., $\log_p |\mathcal{J}_F[p]|$.² Now, consider the constant field extension $\overline{F} = F \cdot \overline{\mathbb{F}}_q$ where $\overline{\mathbb{F}}_q$ denotes an algebraic closure of $\mathbb{F}_q$. Then the *Hasse-Witt* invariant i_F of F is defined to be the $\mathbb{F}_p$ -dimension of $\mathcal{J}_{\overline{F}}[p]$. It is clear that $\mathcal{J}_F[p]$ is an $\mathbb{F}_p$ -subspace of $\mathcal{J}_{\overline{F}}[p]$, and hence $i_F \geq \gamma(F)$.

²Note that in the definition of $\gamma(F)$ the logarithm of $\mathcal{J}_F[p]$ is taken in base p as opposed to the definition of $J_p(\mathcal{F})$, where it is taken in base q .

Note that, for any family $\mathcal{F}$ of function fields F over $\mathbb{F}_q$ with $g(F) \rightarrow \infty$,

$$J_p(\mathcal{F}) = \liminf_{F \in \mathcal{F}} \frac{\gamma(F)}{g(F) \log_p q} \leq \liminf_{F \in \mathcal{F}} \frac{i_F}{g(F) \log_p q}.$$

Before proving Theorems 2.3(iii) and 2.5, we need to introduce the Deuring-Shafarevich theorem.

Theorem 2.7 (Deuring-Shafarevich (see e.g. [34])). *Let E/F be a Galois extension of function fields over an algebraically closed field k of characteristic p . Suppose that the Galois group of the extension is a p -group. Then*

$$\gamma(E) - 1 = [E : F](\gamma(F) - 1) + \sum_{P \in \mathbb{P}(F)} \sum_{\substack{Q \in \mathbb{P}(E) \\ Q|P}} (e(Q|P) - 1).$$

From this theorem, we can obtain the following corollary for function fields over *finite* fields.

Corollary 2.8. *Let E/F be a Galois extension of function fields over a finite field $\mathbb{F}_q$ of characteristic p . Suppose that the Galois group of the extension is a p -group. Then*

$$i_E - 1 = [E : F](i_F - 1) + \sum_{P \in \mathbb{P}(F)} \sum_{\substack{Q \in \mathbb{P}(E) \\ Q|P}} (e(Q|P) - 1) \deg Q.$$

Proof. Let $\overline{E} = E \cdot \overline{\mathbb{F}_q}$, $\overline{F} = F \cdot \overline{\mathbb{F}_q}$ where $\overline{\mathbb{F}_q}$ denotes an algebraic closure of $\mathbb{F}_q$. By elementary algebra arguments we can see that since E/F is Galois and both E and F have the same full constant field $\mathbb{F}_q$, then $\overline{E}/\overline{F}$ is also Galois and the Galois groups of both extensions are the same.

We can therefore apply the Deuring-Shafarevich Theorem to $\overline{E}$ and $\overline{F}$, thereby obtaining:

$$\gamma(\overline{E}) - 1 = [\overline{E} : \overline{F}](\gamma(\overline{F}) - 1) + \sum_{P' \in \mathbb{P}(\overline{F})} \sum_{\substack{Q' \in \mathbb{P}(\overline{E}) \\ Q'|P'}} (e(Q'|P') - 1).$$

Note that $\gamma(\overline{E}) = i_E$, $\gamma(\overline{F}) = i_F$ and $[\overline{E} : \overline{F}] = [E : F]$, so all we are left to do is to analyse the last term.

Given a place $P \in \mathbb{P}(F)$ of degree k , and a place $Q \in \mathbb{P}(E)$ of degree m such that $Q|P$, there are exactly k places $P'_1, \dots, P'_k \in \mathbb{P}(\overline{F})$ lying over P and m places $Q'_1, \dots, Q'_m \in \mathbb{P}(\overline{E})$ lying over Q . Each of the places Q'_j lies above some P'_i . Moreover, all places of $\overline{E}$ lying above a place $P'_i \in \mathbb{P}(\overline{F})$ are among the Q'_j . It is well known that all places in $\overline{F}$ and $\overline{E}$ have degree 1. Given P' in $\{P'_1, \dots, P'_k\}$ and Q' in $\{Q'_1, \dots, Q'_m\}$, we have $e(P'|P) = 1$ and $e(Q'|Q) = 1$. Consequently if Q' lies above P' , we deduce $e(Q'|P') = e(Q|P)$ since $e(Q'|P')e(P'|P) = e(Q'|P) = e(Q'|Q)e(Q|P)$.

Thus

$$\begin{aligned} \sum_{P' \in \mathbb{P}(\overline{F})} \sum_{\substack{Q' \in \mathbb{P}(\overline{E}) \\ Q'|P'}} (e(Q'|P') - 1) &= \\ \sum_{P \in \mathbb{P}(F)} \sum_{\substack{Q \in \mathbb{P}(E) \\ Q|P}} (e(Q|P) - 1) \deg Q. \end{aligned}$$

□

Now we are ready to prove Theorem 2.3(iii).

Proof of Theorem 2.3(iii). Assume q is an even power of p . Consider the tower $\mathcal{F} = (F^{(0)} \subset F^{(1)} \subset \dots)$ over $\mathbb{F}_q$ introduced in [28] by Garcia and Stichtenoth, recursively defined by $F^{(0)} = \mathbb{F}_q(x_0)$ and $F^{(n+1)} = F^{(n)}(x_{n+1})$, where $x_n^{\sqrt{q}-1} x_{n+1}^{\sqrt{q}} + x_{n+1} = x_n^{\sqrt{q}}$.

Assuming for the moment that Theorems 2.9 and 2.10 stated below hold, the rest of the argument follows immediately: indeed,

$$\liminf_{n \rightarrow \infty} \frac{\gamma(F^{(n)})}{g(F^{(n)})} \leq \lim_{n \rightarrow \infty} \frac{i_{F^{(n)}}}{g(F^{(n)})} = \frac{1}{\sqrt{q} + 1}.$$

where the equality follows from part 3 of Theorem 2.9 and Theorem 2.10.

Therefore

$$J_p(\mathcal{F}) = \liminf_{n \rightarrow \infty} \frac{\gamma(F^{(n)})}{g(F^{(n)}) \log_p q} = \frac{1}{(\sqrt{q} + 1) \log_p q}.$$

On the other hand, $A(\mathcal{F}) = \sqrt{q} - 1$ by part 1 of Theorem 2.9. Therefore

$$J_p(q, \sqrt{q} - 1) = \frac{1}{(\sqrt{q} + 1) \log_p q}.$$

It only remains to show Theorems 2.9 and 2.10.

Theorem 2.9. 1. The tower $\mathcal{F}$ attains the Drinfeld-Vlăduț bound, i.e., its limit $A(\mathcal{F})$ is given by

$$A(\mathcal{F}) := \lim_{n \rightarrow \infty} \frac{N(F^{(n)})}{g(F^{(n)})} = \sqrt{q} - 1.$$

2. Every place $P \in \mathbb{P}(F^{(n-1)})$ is either unramified, i.e. for every place $Q \in \mathbb{P}(F^{(n)})$ such that $Q|P$ we have $e(Q|P) = 1$, where $e(Q|P)$ denotes the ramification index, or totally ramified, i.e., there exists a unique $Q \in \mathbb{P}(F^{(n)})$ such that $Q|P$, and the ramification index $e(Q|P)$ equals $[F^{(n)} : F^{(n-1)}] = \sqrt{q}$. In the latter case, it always holds that $\deg P = \deg Q$. Moreover for every $P \in \mathbb{P}(F^{(n-1)})$, $Q \in \mathbb{P}(F^{(n)})$ such that $Q|P$ we have

$$d(Q|P) = (\sqrt{q} + 2)(e(Q|P) - 1),$$

where $d(Q|P)$ denotes the different exponent.

3. The genus $g(F^{(n)})$ of the function field $F^{(n)}$ is given by

$$g(F^{(n)}) = \begin{cases} g_1(q, n) & \text{if } n \equiv 0 \pmod{2}, \\ g_2(q, n) & \text{if } n \equiv 1 \pmod{2}. \end{cases}$$

where

$$\begin{aligned} g_1(q, n) &:= q^{\frac{n+1}{2}} + q^{\frac{n}{2}} - q^{\frac{n+2}{4}} - 2q^{\frac{n}{4}} + 1, \\ g_2(q, n) &:= q^{\frac{n+1}{2}} + q^{\frac{n}{2}} - \frac{1}{2}q^{\frac{n+3}{4}} - \frac{3}{2}q^{\frac{n+1}{4}} - q^{\frac{n-1}{4}} + 1. \end{aligned}$$

Proof. See [28]. □

Theorem 2.10. The Hasse-Witt invariant of the function field $F^{(n)}$ is given by

$$i_{F^{(n)}} = \begin{cases} (q^{n/4} - 1)^2 & \text{if } n \equiv 0 \pmod{2}, \\ (q^{(n-1)/4} - 1)(q^{(n+1)/4} - 1) & \text{if } n \equiv 1 \pmod{2}. \end{cases}$$

In particular

$$\liminf_{n \rightarrow \infty} \frac{\gamma(F^{(n)})}{g(F^{(n)})} \leq \lim_{n \rightarrow \infty} \frac{i_{F^{(n)}}}{g(F^{(n)})} = \frac{1}{\sqrt{q} + 1}.$$

Proof. Fix some $n \geq 1$ and for the sake of notation let $E := F^{(n)}$, $F := F^{(n-1)}$. Consider the extension E/F . This is an Artin-Schreier extension, hence its Galois group is a p -group. By the theorem of Riemann-Hurwitz (see e.g. [55]) and part 2) of Theorem 2.9 above,

$$2 \cdot g(E) - 2 = \sqrt{q} \cdot (2g(F) - 2) + (\sqrt{q} + 2) \cdot \sum_{P \in \mathbb{P}(F)} \sum_{\substack{Q \in \mathbb{P}(E) \\ Q|P}} (e(Q|P) - 1) \deg Q. \quad (2.3)$$

By Corollary 2.8

$$i_E - 1 = \sqrt{q} \cdot (i_F - 1) + \sum_{P \in \mathbb{P}(F)} \sum_{\substack{Q \in \mathbb{P}(E) \\ Q|P}} (e(Q|P) - 1) \deg Q. \quad (2.4)$$

Combining equations (2.3) and (2.4), we find

$$i_E = \sqrt{q} \cdot i_F + \frac{2 \cdot g(E) - 2\sqrt{q} \cdot g(F) - \sqrt{q}^2 + \sqrt{q}}{\sqrt{q} + 2}$$

This, of course, holds for any $n \geq 1$, $E := F^{(n)}$, $F := F^{(n-1)}$. Using the fact that $i_{F^{(0)}} = 0$ and applying induction, the result follows. $\square$

This concludes the proof of Theorem 2.3(iii). $\square$

We can use the same kind of argument applied to a different tower to prove Theorem 2.5:

Proof of Theorem 2.5: In [66], Xing and Yeo gave an example of a tower $\mathcal{F} = (F^{(0)} \subset F^{(1)} \subset \dots)$ of function fields over $\mathbb{F}_2$ with the Ihara limit $97/376 = 0.257979\dots$. Using cyclotomic function fields, they constructed a function field $F = F^{(0)}$ over $\mathbb{F}_2$ of genus 377, which admits an infinite $(2; S)$ -Hilbert class field tower for a set $S \subset \mathbb{P}_F$ of places of F , such that $S' = \mathbb{P}_F \setminus S$ consists of 97 rational places of F . At each step $F^{(i+1)}/F^{(i)}$, it is unramified. Hence, to compute the Hasse-Witt invariant of $F^{(i)}$, it is sufficient to compute the Hasse-Weil invariant of $F^{(0)}$ by using the formula of Deuring-Shafarevich.

To do so, we briefly recall the construction of the function field F . For more details, the reader may refer to [66]. Let $k = \mathbb{F}_2(x)$ be the rational function field over $\mathbb{F}_2$. Let $M = (x^4 + x^3 + x^2 + x + 1)^2 \in \mathbb{F}_2[x]$ and let $N := x^4$. Denote by k_M (resp. k_N) the cyclotomic function field over k with modulus M (resp. modulus N). Let K be the subfield of k_M fixed by the cyclic subgroup $\langle x \rangle$ of $\text{Gal}(k_M/k) = (\mathbb{F}_2[x]/M)^*$ and let L be the subfield of k_N that is fixed by the cyclic subgroup $\langle (x+1)^2 \rangle$ of $\text{Gal}(k_N/k) = (\mathbb{F}_2[x]/N)^*$. We have $[K : k] = 24$ and $[L : k] = 4$. Define $F := KL$, the composite of the fields K and L . The only ramified place in K/k is the place corresponding to the irreducible polynomial $x^4 + x^3 + x^2 + x + 1$. It is totally ramified with different exponent 44. In the extension L/k the only ramified place is the zero of x . It is totally ramified with different exponent 10.

From the ramification in K/k and L/k , it follows that K and L are linearly disjoint over k . We have $[F : k] = 2^5 \times 3$. The fixed field of the 2-Sylow subgroup of $\text{Gal}(F/k)$ is generated over k by an element w , whose irreducible polynomial over k is given by

$$T^3 + (x^4 + x^3 + x^2 + x + 1)T^2 + (x^5 + 1)T + (x^4 + x^3 + x^2 + x + 1) \in k[T].$$

Let $F' = k(w)$. We have $k \subset F' \subset K$. The only ramified place in F'/k is the place corresponding to the irreducible polynomial $x^4 + x^3 + x^2 + x + 1$. It is tamely ramified with ramification index 3. Hence the genus of F' is 2. Next by computing the Hasse-Witt invariant of F we know that in the degree 32 extension F/F' the only ramified places are the places lying over the places of k associated to the irreducible polynomials x and $x^4 + x^3 + x^2 + x + 1$. The corresponding ramification indices are 4 and 8, respectively. So we have

$$i_F - 1 = 32(2 - 1) + 4 \times 4 \times (8 - 1) + 3 \times 8 \times (4 - 1) = 216.$$

For the $(2; S)$ -Hilbert class field tower of $F = F^{(0)}$, we hence have

$$g(F^{(n)}) - 1 = [F^{(n)} : F^{(0)}](g(F^{(0)}) - 1) = 376[F^{(n)} : F^{(0)}]$$

and

$$i_{F^{(n)}} - 1 = [F^{(n)} : F^{(0)}](i_{F^{(0)}} - 1) = 216[F^{(n)} : F^{(0)}].$$

Therefore,

$$\lim_{n \rightarrow \infty} \frac{i_{F^{(n)}}}{g(F^{(n)})} = \frac{216}{376} = 0.574468\dots$$

$\square$

The Deuring-Shafarevich theorem has been used in [6] to analyze the p -rank of the function fields for other optimal towers over $\mathbb{F}_q$, for q square. However, the resulting bounds for the torsion limits for those towers are worse (for our applications) than that of the first Garcia-Stichtenoth tower, obtained above.

3 Riemann-Roch Systems of Equations

Let $\mathbb{F}_q$ be a finite field and let F be an algebraic function field over $\mathbb{F}_q$.

Definition 3.1. Let $u \in \mathbb{Z}_{>0}$ and let $Y_i \in \text{Cl}(F)$, $m_i \in \mathbb{Z} \setminus \{0\}$ for $i = 1, \dots, u$. The Riemann-Roch system of equations in the indeterminate X is the system $\{\ell(m_i X + Y_i) = 0\}_{i=1}^u$ determined by these data. A solution is some $[G] \in \text{Cl}(F)$ which satisfies all equations when substituted for X .

While Riemann-Roch systems have been (implicitly) used before in the construction of codes with good asymptotic properties, for instance in [59, 62, 65, 64, 68, 40, 42], they were of a less general type. Namely, $m_i = \pm 1$ for all i . As we shall see soon, dealing with the more general case where $m_i \neq \pm 1$ leads us to consider m_i -torsion in the class group.

One observation about the systems is that X is a solution of the equation $\ell(m_i X + Y_i) = 0$ as long as $\deg(m_i X + Y_i) < 0$ since we have $\ell(m_i X + Y_i) = 0$ in this case. This suggests that, if we want to prove the existence of solutions of certain fixed degree, we should only consider those equations $\ell(m_i X + Y_i) = 0$ in the Riemann-Roch system with $\deg(m_i X + Y_i) \geq 0$.

The following theorem shows that a solution of degree d exists if a certain numerical condition is satisfied that involves the class number, the number A_{r_i} of effective divisors of degree r_i and the cardinality of the m_i -torsion subgroups of the degree-zero divisor class group, where the m_i are determined by the system and the r_i are determined by d and the m_i .

Theorem 3.2. Consider the Riemann-Roch system of equations

$$\{\ell(m_i X + Y_i) = 0\}_{i=1}^u.$$

Let $d_i = \deg Y_i$ for $i = 1, \dots, u$. Write $h := h(F)$ the class number. Denote by A_r the number of effective divisors of degree r in $\text{Div}(F)$ for $r \geq 0$, and 0 for $r < 0$. Let $s \in \mathbb{Z}$ and define $r_i = m_i s + d_i$ for $i = 1, \dots, u$. If

$$h > \sum_{i=1}^u A_{r_i} \cdot |\mathcal{J}_F[m_i]|,$$

then the Riemann-Roch system has a solution $[G] \in \text{Cl}_s(\mathbb{F})$.

We refer to [15] for the detailed proof of Theorem 3.2.

Remark 3.3. (“Solving by taking any divisor X of large enough degree”)

- (i) If $r_i < 0$ for all $i = 1, \dots, u$, then the inequality in Theorem 3.2 is automatically satisfied and hence the Riemann-Roch system always has a solution.
- (ii) In many scenarios in algebraic geometry codes, one can simply argue for a solution of the Riemann-Roch system by assuming that $r_i < 0$ for all $i = 1, \dots, u$.
- (iii) For instance, in [18], it was also simply assumed $r_i < 0$ to obtain strongly multiplicative linear secret sharing schemes. But this does not always give the best results. In particular, in Section 4, we will show how we can employ Theorem 3.2 to get improvements, especially for small finite fields.

It will often be more convenient to write systems as defined over $\text{Div}(F)$ rather than $\text{Cl}(F)$.

The condition in Theorem 3.2 involves the number of positive divisors of certain degrees and the class number. The following bound will be useful in the applications. The proof is based on careful manipulations with the zeta function of $\mathbb{F}$.

Proposition 3.4. Let F be an algebraic function field over $\mathbb{F}_q$. Write g for the genus $g(F)$ and h for the class number $h(F)$. For $r \in \mathbb{Z}_{\geq 0}$, write A_r for the number of effective divisors of degree r in $\text{Div}(\mathbb{F})$. Suppose $g \geq 1$. Then, for any integer r with $0 \leq r \leq g - 1$,

$$\frac{A_r}{h} \leq \frac{g}{q^{g-r-1}(\sqrt{q} - 1)^2}.$$

A very brief proof of Proposition 3.4 was given in [15]. Here we give a detailed proof.

Proof. For $i \geq 2g - 1$ the value of A_i is known as a function of q, g, h, i (see Lemma 5.1.4 and Corollary 5.1.11 in [55]). This has been exploited in Lemma 3 (ii) from [44], to show that

$$\sum_{i=0}^{g-2} A_i t^i + \sum_{i=0}^{g-1} q^{g-1-i} A_i t^{2g-2-i} = \frac{L(t) - ht^g}{(1-t)(1-qt)}$$

by manipulations of power series, where $L(t)$ is the L -polynomial in the zeta function of F .

The claim 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 RHS, then finding an expression for $L'(1/q)$ (the “left-over term”), and substituting that back in.

Taking this limit,

$$\sum_{i=0}^{g-2} \frac{A_i}{q^i} + \sum_{i=0}^{g-1} \frac{A_i}{q^{g-1-i}} = \lim_{t \rightarrow 1/q} \frac{L(t) - ht^g}{(1-t)(1-qt)},$$

and applying l'Hôpital's rule ($((f(t))'|_{t=a}$ denotes the derivative of f evaluated at $t = a$), it follows that

$$\begin{aligned} \frac{(L(t) - ht^g)'|_{t=1/q}}{((1-t)(1-qt))'|_{t=1/q}} &= \frac{L'(1/q) - gh/q^{g-1}}{-q(1-1/q)} = \\ &= \frac{gh - q^{g-1}L'(1/q)}{(q-1)q^{g-1}}. \end{aligned}$$

The term $L'(1/q)$ can be evaluated as follows. By differentiation,

$$L'(t) = \sum_{i=1}^{2g} L(t) \cdot \frac{-\omega_i}{1 - \omega_i t},$$

and hence,

$$L'\left(\frac{1}{qt}\right) = L\left(\frac{1}{qt}\right) \cdot \sum_{i=1}^{2g} (qt) \cdot \frac{-\omega_i}{qt - \omega_i}.$$

Evaluation of $L(1/q)$ is straightforward by combining the Functional Equation for L -polynomials and the fact that $L(1) = h$ (see [55]). Namely,

$$L\left(\frac{1}{q}\right) = q^g \left(\frac{1}{q}\right)^{2g} L(1) = \frac{h}{q^g}.$$

Therefore,

$$L'\left(\frac{1}{q}\right) = \frac{h}{q^{g-1}} \cdot \sum_{i=1}^{2g} \frac{-\omega_i}{q - \omega_i}.$$

Substituting the expression for $L'(1/q)$ back in, it follows that

$$\sum_{i=0}^{g-2} \frac{A_i}{q^i} + \sum_{i=0}^{g-1} \frac{A_i}{q^{g-1-i}} = \frac{h}{q^{g-1}(q-1)} \cdot \left(g + \sum_{i=0}^{2g} \frac{\omega_i}{q - \omega_i}\right).$$

Note that, trivially, 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 $|\omega_i| = \sqrt{q}$ for $i = 1, \dots, 2g$, it holds, for $0 \leq r \leq g-1$, that

$$\begin{aligned} \frac{A_r}{q^r} &\leq \sum_{i=0}^{g-2} \frac{A_i}{q^i} + \sum_{i=0}^{g-1} \frac{A_i}{q^{g-1-i}} = \frac{h}{q^{g-1}(q-1)} \cdot \left|g + \sum_{i=0}^{2g} \frac{\omega_i}{q - \omega_i}\right| \\ &\leq \frac{h}{q^{g-1}(q-1)} \cdot \left(g + \sum_{i=0}^{2g} \frac{|\omega_i|}{q - |\omega_i|}\right) = \frac{gh}{q^{g-1}(q-1)} \cdot \left(1 + \frac{2}{\sqrt{q}-1}\right) \\ &= \frac{gh}{q^{g-1}(q-1)} \cdot \left(\frac{\sqrt{q}+1}{\sqrt{q}-1}\right) = \frac{gh}{q^{g-1} \cdot (\sqrt{q}-1)^2}. \end{aligned}$$

and the claimed result follows. $\square$

Remark 3.5 (Efficient randomized solving strategy). *Except in the cases where Remark 3.3 applies, we are not aware of any efficient deterministic strategy to solve efficiently the Riemann-Roch systems of equations appearing in our applications. However, in many circumstances, there is an efficient randomized strategy that produces a divisor that is a solution with high probability. Namely, if the number of non-solutions (which is bounded by the right hand side of the inequality in Theorem 3.2) is negligible as a function of the class number, then a uniformly random element from $Cl_s(\mathbb{F})$ will be a solution with overwhelming probability. Assuming both means for efficient sampling in $Cl_s(\mathbb{F})$ according to a distribution sufficiently close to uniform and for efficient construction of generator matrices of the algebraic geometric codes associated to the sampled divisors, there exist efficient probabilistic constructions of the asymptotically good families of codes in our applications. As for the sampling issue, we note that it can be done under mild conditions (see [12, Section 5.3.2.] or [33, Theorem 5]). As for the construction of generator matrices, not much is known in full generality but results for the construction of bases of Riemann-Roch spaces of general divisors can be found in [33]. Generator matrices for algebraic geometric codes on function fields of a tower of Garcia-Stichtenoth were explicitly constructed in [54] although only one-point divisors are considered.*

4 Application 1: Arithmetic Secret Sharing

Our first application concerns the asymptotic study of *arithmetic secret sharing schemes*, which was first considered in [23, 18] in the context of secure multi-party computation. Since then, the asymptotical results from [18] have had important and surprising applications in *two-party* cryptography as well [37, 39, 31, 38, 24, 36]. For a more detailed discussion of the motivation, results and applications, please refer to [15].

One motivation of this section is to show an important application of our torsion limits and Riemann-Roch systems introduced in the previous sections. As the proofs of most results in this section can be found in [15], we state our results without detailed proof.

We first define arithmetic secret sharing schemes and then show how our torsion limits help to improve prior results significantly.

Let k, n be integers with $k, n \geq 1$. Consider the $\mathbb{F}_q$ -vector space $\mathbb{F}_q^k \times \mathbb{F}_q^n$, where $\mathbb{F}_q$ is an arbitrary finite field.

Definition 4.1. *The $\mathbb{F}_q$ -vector space morphism*

$$\pi_0 : \mathbb{F}_q^k \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q^k$$

is defined by the projection

$$(s_1, \dots, s_k, c_1, \dots, c_n) \mapsto (s_1, \dots, s_k).$$

For each $i \in \{1, \dots, n\}$, the $\mathbb{F}_q$ -vector space morphism

$$\pi_i : \mathbb{F}_q^k \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$$

is defined by the projection

$$(s_1, \dots, s_k, c_1, \dots, c_n) \mapsto c_i.$$

For $\emptyset \neq A \subset \{1, \dots, n\}$, the $\mathbb{F}_q$ -vector space morphism

$$\pi_A : \mathbb{F}_q^k \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{|A|}$$

is defined by the projection

$$(s_1, \dots, s_k, c_1, \dots, c_n) \mapsto (c_i)_{i \in A}.$$

For $\mathbf{v} \in \mathbb{F}_q^k \times \mathbb{F}_q^n$, it is sometimes convenient to denote $\pi_0(\mathbf{v}) \in \mathbb{F}_q^k$ by $\mathbf{v}_0$ and $\pi_A(\mathbf{v}) \in \mathbb{F}_q^{|A|}$ by $\mathbf{v}_A$. We write $\mathcal{I}^ = \{1, \dots, n\}$. It is also sometimes convenient to refer to $\mathbf{v}_0$ as the secret-component of $\mathbf{v}$ and to $\mathbf{v}_{\mathcal{I}^*}$ as its shares-component.*

Definition 4.2. *An n -code for $\mathbb{F}_q^k$ (over $\mathbb{F}_q$) is an $\mathbb{F}_q$ -vector space $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ such that*

- (i) $\pi_0(C) = \mathbb{F}_q^k$
- (ii) $(\text{Ker } \pi_{\mathcal{I}^*}) \cap C \subset (\text{Ker } \pi_0) \cap C$.

For $\mathbf{c} \in C$, $\mathbf{c}_0 \in \mathbb{F}_q^k$ is the secret and $\mathbf{c}_{\mathcal{I}^*} \in \mathbb{F}_q^n$ the shares.

The first condition means that, in C , the secret can take any value in $\mathbb{F}_q^k$. More precisely, for a uniformly random vector $\mathbf{c} \in C$, the secret $\mathbf{c}_0$ is uniformly random in $\mathbb{F}_q^k$. This follows from the fact that the projection $(\pi_0)|_C$ is regular (since it is a surjective $\mathbb{F}_q$ -vector space morphism).

The second condition means that the shares uniquely determine the secret. Indeed, the shares do not always determine the secret uniquely if and only if there are $\mathbf{c}, \mathbf{c}' \in C$ such that their shares coincide but not their secrets. Therefore, by linearity, the shares determine the secret uniquely if and only if the shares being zero implies the secret being zero. Moreover these two conditions imply that $k \leq n$. Note that an n -code with the stronger condition $(\text{Ker } \pi_{\mathcal{I}^*}) \cap C = (\text{Ker } \pi_0) \cap C$ is a k -dimensional error correcting code of length n .

Definition 4.3 (r -reconstructing). An n -code C for $\mathbb{F}_q^k$ is r -reconstructing ($1 \leq r \leq n$) if

$$(\text{Ker } \pi_A) \cap C \subset (\text{Ker } \pi_0) \cap C$$

for each $A \subset \mathcal{I}^*$ with $|A| = r$.

In other words, r -reconstructing means that any r shares uniquely determine the secret. Note that an n -code is n -reconstructing by definition.

Definition 4.4 (t -Disconnected). An n -code C for $\mathbb{F}_q^k$ is t -disconnected if $t = 0$ or else if $1 \leq t < n$, the projection

$$\begin{aligned} \pi_{0,A} : C &\longrightarrow \mathbb{F}_q^k \times \pi_A(C) \\ \mathbf{c} &\mapsto (\pi_0(\mathbf{c}), \pi_A(\mathbf{c})) \end{aligned}$$

is surjective for each $A \subset \mathcal{I}^*$ with $|A| = t$.

If, additionally, $\pi_A(C) = \mathbb{F}_q^t$, we say C is t -uniform.

If $t > 0$, then t -disconnectedness means the following. Let $A \subset \mathcal{I}^*$ with $|A| = t$. Then, for uniformly randomly $\mathbf{c} \in C$, the secret $\mathbf{c}_0$ is independently distributed from the t shares $\mathbf{c}_A$. Indeed, for the same reason that the secret $\mathbf{c}_0$ is uniformly random in $\mathbb{F}_q^k$, it holds that $(\mathbf{c}_0, \mathbf{c}_A)$ is uniformly random in $\mathbb{F}_q^k \times \pi_A(C)$. Since the uniform distribution on the Cartesian-product of two finite sets corresponds to the uniform distribution on one set, and independently, the uniform distribution on the other, the claim follows. Uniformity means that, in addition, $\mathbf{c}_A$ is uniformly random in $\mathbb{F}_q^t$.

Definition 4.5 (Powers of an n -Code). Let $m \in \mathbb{Z}_{>0}$. For $\mathbf{x}, \mathbf{x}' \in \mathbb{F}_q^m$, their product $\mathbf{x} * \mathbf{x}' \in \mathbb{F}_q^m$ is defined as $(x_1 x'_1, \dots, x_m x'_m)$.

Let d be a positive integer. If C is an n -code for $\mathbb{F}_q^k$, then $C^{*d} \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ is the $\mathbb{F}_q$ -linear subspace generated by all terms of the form $\mathbf{c}^{(1)} * \dots * \mathbf{c}^{(d)}$ with $\mathbf{c}^{(1)}, \dots, \mathbf{c}^{(d)} \in C$. For $d = 2$, we use the abbreviation $\hat{C} := C^{*2}$. Powers of linear codes (instead of n -codes) are defined analogously and will be useful later.

Remark 4.6 (Powering Need Not Preserve n -Code). Suppose $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ is an n -code for $\mathbb{F}_q^k$. It follows immediately that the secret-component in C^{*d} takes any value in $\mathbb{F}_q^k$. However, the shares-component in C^{*d} need not determine the secret-component uniquely. Thus, C^{*d} need not be an n -code for $\mathbb{F}_q^k$.

Definition 4.7 (Arithmetic secret sharing scheme). An (n, t, d, r) -arithmetic secret sharing scheme for $\mathbb{F}_q^k$ (over $\mathbb{F}_q$) is an n -code C for $\mathbb{F}_q^k$ such that

- (i) $t \geq 1$, $d \geq 2$
- (ii) C is t -disconnected,
- (iii) C^{*d} is in fact an n -code for $\mathbb{F}_q^k$ and
- (iv) C^{*d} is r -reconstructing.

C has uniformity if, in addition, it is t -uniform.

For example, the case $k = 1$, $d = 2$, $n = 3t + 1$, $r = n - t$, $q > n$ obtained from Shamir's secret sharing scheme [52] (taking into account that degrees sum up when taking products of polynomials) corresponds to the secret sharing scheme used in [9, 17]. The properties are easily proved using Lagrange's Interpolation Theorem. The generalization to $k > 1$ of this Shamir-based approach is due to [26]. The abstract notion is due to [23], where also constructions for $d = 2$ were given based on general linear secret sharing. See also [18, 19, 20]. On the other hand the following limitations are easy to establish.

Proposition 4.8. *Let C be an (n, t, d, r) -arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. As a linear secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$, C has t -privacy and $(r - (d - 1)t)$ -reconstruction. Hence, $dt + k \leq r$. Particularly, if $k = 1$, $d = 2$, $r = n - t$, then $3t + 1 \leq n$.*

We are now ready to state the asymptotical results from [18] in full generality.³ Let $F/\mathbb{F}_q$ be an algebraic function field (in one variable, with $\mathbb{F}_q$ as field of constants). Let g denote the genus of F . Let $k, t, n \in \mathbb{Z}$ with $n > 1$, $1 \leq t \leq n$, $1 \leq k \leq n$. Suppose $Q_1, \dots, Q_k, P_1, \dots, P_n \in \mathbb{P}^{(1)}(F)$ are pairwise distinct $\mathbb{F}_q$ -rational places. Write $Q = \sum_{j=1}^k Q_j \in \text{Div}(F)$ and $D = Q + \sum_{i=1}^n P_i \in \text{Div}(F)$. Let $G \in \text{Div}(F)$ be such that $\text{supp } D \cap \text{supp } G = \emptyset$, i.e., they have disjoint support. Consider the AG-code $C(D, G)_L \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$, given by the image of the map

$$\begin{aligned} \phi : \mathcal{L}(G) &\rightarrow \mathbb{F}_q^k \times \mathbb{F}_q^n \\ f &\mapsto (f(Q_1), \dots, f(Q_k), f(P_1), \dots, f(P_n)). \end{aligned}$$

Theorem 4.9. (from [18]). *Let $t \geq 1, d \geq 2$. Let $C = C(D, G)_L$ with $\deg G \geq 2g + t + k - 1$. If $n > 2dg + (d + 1)t + dk - d$, then C is an $(n, t, d, n - t)$ -arithmetic sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity.*

Theorem 4.10. (from [18]). *Fix $d \geq 2$ and a finite field $\mathbb{F}_q$. Suppose $A(q) > 2d$, where $A(q)$ is Ihara's constant. Then there is an infinite family of $(n, t, d, n - t)$ -arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity such that n is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$. Moreover, for every C in the family, a generator for C is $\text{poly}(n)$ -time computable and C^{*i} has $\text{poly}(n)$ -time reconstruction of a secret in the presence of t faulty shares ($i = 1, \dots, d - 1$).*

Since $A(q) = \sqrt{q} - 1$ if q is a square, it holds that $A(q) > 2d$ if q is a square with $q > (2d + 1)^2$. Also, since by Serre's Theorem, $A(q) > c \log q$ for some absolute constant $c > 0$, it also holds that $A(q) > 2d$ if q is (very) large. We will now apply our results on the torsion limit in combination with appropriate Riemann-Roch systems in order to relax the condition $A(q) > 2d$ considerably. As a result, we attain the result of [18] but this time over *nearly all finite fields*.

Theorem 4.11. *Let $t \geq 1, d \geq 2$. Define $\mathcal{I}^* = \{1, \dots, n\}$. For $A \subset \mathcal{I}^*$ with $A \neq \emptyset$, define $P_A = \sum_{j \in A} P_j \in \text{Div}(F)$. Let $K \in \text{Div}(F)$ be a canonical divisor. If the system*

$$\{\ell(dX - D + P_A + Q) = 0, \ell(K - X + P_A + Q) = 0\}_{A \subset \mathcal{I}^*, |A|=t}$$

is solvable, then there is a solution $G \in \text{Div}(F)$ such that $C(D, G)_L$ is an $(n, t, d, n - t)$ -arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ (with uniformity).

The reader may refer [15] for a detailed proof of 4.11.

And now as a corollary of Theorems 3.2 and 4.11 we get the following:

Corollary 4.12. *Let $F/\mathbb{F}_q$ be an algebraic function field. Let $d, k, t, n \in \mathbb{Z}$ with $d \geq 2$, $n > 1$ and $1 \leq t < n$. Suppose $Q_1, \dots, Q_k, P_1, \dots, P_n \in \mathbb{P}^{(1)}(F)$ are pairwise distinct. If there is $s \in \mathbb{Z}$ such that*

$$h > \binom{n}{t} (A_{r_1} + A_{r_2} |\mathcal{J}_F[d]|)$$

where $r_1 := 2g - s + t + k - 2$ and $r_2 := ds - n + t$, then there exists an $(n, t, d, n - t)$ -arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity.

³In fact, we state a version that is proved by exactly the same arguments as in [18].

Theorem 4.13. *Let $\mathbb{F}_q$ be a finite field and $d \in \mathbb{Z}_{\geq 2}$. If there exists $0 < A \leq A(q)$ such that $A > d - 1 + J_d(q, A)$, then there is an infinite family of $(n, t, d, n - t)$ -arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with t -uniformity where n is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$.*

Remark 4.14. *Note that in [15, Main Theorem 1] this result was announced but only proved in the case $d = 2$. However, the general condition is incorrectly written there as $A > 1 + J_d(q, A)$ instead of $A > d - 1 + J_d(q, A)$. Note that in the case $d = 2$ (which is the main concern of [15]) both expressions coincide.*

Theorem 4.13 will follow from the more precise statement in Theorem 4.16 below. Combining Theorem 4.13 with Theorem 2.6 we obtain, in the special case $d = 2$:

Theorem 4.15. *For $q = 8, 9$ and for all prime powers $q \geq 16$ there is an infinite family of $(n, t, 2, n - t)$ -arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with t -uniformity where n is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$.*

More precisely, we have the following result (for $d > 2$ there is a similar analysis).

Theorem 4.16. *Let $\mathbb{F}_q$ be a finite field. Suppose $\kappa \in [0, \frac{1}{3})$ and $\tau \in (0, 1]$ and $0 < A \leq A(q)$ are real numbers such that*

$$A > \frac{1 + \kappa}{1 - 3\kappa} (1 + J_2(q, A))$$

and

$$\tau + \frac{H_2(\tau)}{\log q} < \frac{1}{3} \left(1 - 3\kappa - \frac{(1 + J_2(q, A))(1 + \kappa)}{A} \right).$$

Then there is an infinite family of $(n, t, 2, n - t)$ -arithmetic secret sharing schemes for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity where n is unbounded, $k = \lfloor \kappa n \rfloor + 1$ and $t = \lfloor \tau n \rfloor$.

The proof of this fact relies on showing that the conditions in Corollary 4.12 are satisfied asymptotically for a family of function field with Ihara's limit A , if the requirements of Theorem 4.16 are met. It is easy to show why Theorem 4.16 implies Theorem 4.15: if $0 < A \leq A(q)$ is such that $A > 1 + J_2(q, A)$ we can always select $\kappa \in (0, \frac{1}{3})$ and $\tau \in (0, 1]$ satisfying the conditions in Theorem 4.16. Note that in order to obtain the result in Theorem 4.15 we require $\kappa > 0$. The reader may refer to [15] for the detailed proof of Theorem 4.16.

Finally, using our paradigm we also improve the explicit lower bounds for the parameter $\hat{\tau}(q)$ from [18] and [14] for all q with $q \leq 81$ and q square, as well as for all q with $q \leq 9$. Recall $\hat{\tau}(q)$ is defined as the maximum value of $3t/(n - 1)$ which can be obtained asymptotically (when n tends to infinity) when t, n are subject to the condition that an $(n, t, 2, n - t)$ -arithmetic secret sharing for $\mathbb{F}_q$ over $\mathbb{F}_q$ exists (no uniformity required here). The new bounds are shown in the upper row of Table 1. All the new bounds marked with a star (*) are obtained by applying Theorem 4.16 in the case $\kappa = 0$ and using the upper bounds given in Theorem 2.3 for the torsion limits. To obtain the rest of the new upper bounds, for each q , we apply the field descent technique in [14] to $\mathbb{F}_{q^2}$ (in the special case of $\mathbb{F}_9$, even though Theorem 4.16 can be applied directly, as remarked in Main Theorem 4.15, it is better to apply Theorem 4.16 to $\mathbb{F}_{81}$ and then use the descent technique). These are compared with the previous bounds: the ones obtained in [18] (marked also with the symbol *), and the rest, which were obtained in [14] by means of the aforementioned field descent technique.

q	2	3	4	5	7	8
New bounds	0.034	0.057	0.104	0.107	0.149	0.173*
Prev. bounds	0.028	0.056	0.086	0.093	0.111	0.143

q	9	16	25	49	64	81
New bounds	0.173	0.298*	0.323*	0.448*	0.520*	0.520*
Prev. bounds	0.167	0.244	0.278	0.333*	0.429*	0.500*

Table 1: Lower bounds for $\hat{\tau}(q)$

We end this section with the remark that the results above can be adapted to prove a statement about linear codes, namely the existence of families of codes C such that both their duals and their powers are asymptotically good.

Theorem 4.17. *If there exists $0 < A \leq A(q)$ such that $A > d - 1 + J_d(q, A)$, then there exists an asymptotically good family of linear codes C over $\mathbb{F}_q$ such that both the duals $C^\perp$ and, for each $1 \leq d' \leq d$, the powers $C^{*d'}$, are simultaneously asymptotically good. In particular, for $d = 2$, this holds for $q = 8, 9$ and for all prime powers $q \geq 16$.*

In order to show this, we need to adapt the construction of algebraic geometric codes and the proofs of Theorem 4.11 and the subsequent theorems above. The bottomline is to take the case $k = 0$ of those results. Then the same arguments as above prove that both $C^\perp$ and C^{*d} have minimum distance linear in the length. The remainder of the claim follows easily from the observations below. First, it is easy to show then that for all $1 \leq d' \leq d$, the codes $C^{*d'}$ also have minimum distance linear in their length, as it must be larger than the minimum distance of C^{*d} . Second, we have (by Singleton's bound) $\dim C \geq d_{\min}(C^\perp) - 1$, which proves that the codes C are asymptotically good, and analogously we can prove that $C^\perp$ are asymptotically good. Finally, it is obvious that if $d' > d''$ then $\dim C^{*d'} \geq \dim C^{*d''}$, which proves the rest of the statement.

In comparison, if we adapt the results from [18] similarly, we can only prove the existence of these families of codes under the stronger condition $A(q) > 2d$. In the case $d = 2$, this means $A(q) > 4$, which by the Drinfeld-Vlăduţ bound implies $q \geq 25$. The field descent technique based on concatenation of codes from [14], which establishes the existence of asymptotically good arithmetic secret sharing over any finite field when no uniformity is required, does not work here: first, it is not guaranteed that the squares of the resulting codes are asymptotically good and second, the duals cannot be asymptotically good. To the best of our knowledge our present paper is the first to establish, for several finite fields $\mathbb{F}_q$, the existence of linear codes C over $\mathbb{F}_q$ such that both C , C^{*2} and $C^\perp$ are simultaneously asymptotically good. The existence of such families over $\mathbb{F}_q$ for $2 \leq q \leq 13$ is currently an open question except in the cases $q = 8, 9$.

Finally, we remark that the case where just C , C^{*2} are considered (so the dual $C^\perp$ is left out of consideration) has been shown to hold for all finite fields [49], using an algebraic geometric argument in combination with a refined descent method. The construction applies this field descent method to algebraic geometric codes over a suitable extension field such that not only their square but also certain higher powers are asymptotically good. The minimum distance of these powers is bounded in [49] based solely on the degree of the divisors. It seems a plausible avenue to try and improve the parameters (dimension, minimum distance) of the resulting codes C and C^{*2} using the torsion limit but we do not elaborate further on this here.

5 Application 2: Bilinear Complexity of Multiplication

Since the 1980's, many interesting applications of algebraic curves (or algebraic function fields of one variable) over finite fields have been found. One of these applications, which was due to D.V. Chudnovsky and G.V. Chudnovsky [21], is the study of multiplication bilinear complexity in extension fields through algebraic curves. Following the brilliant work by D.V. Chudnovsky and G.V. Chudnovsky, Shparlinski, Tsfasman and Vlăduţ [53] systematically studied this idea and extended the result in [21]. After the above pioneer research, Ballet et al. [1, 2, 3, 4] further investigated and developed the idea and obtained improvements.

Before we formulate the problem, we need to adapt some of the definitions in the previous section.

Definition 5.1. *The $\mathbb{F}_q$ -vector space morphism*

$$\pi_0 : \mathbb{F}_{q^k} \times \mathbb{F}_q^n \rightarrow \mathbb{F}_{q^k}$$

is defined by the projection

$$(s, c_1, \dots, c_n) \mapsto s.$$

For each $i \in \{1, \dots, n\}$, the $\mathbb{F}_q$ -vector space morphism

$$\pi_i : \mathbb{F}_{q^k} \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q$$

is defined by the projection

$$(s, c_1, \dots, c_n) \mapsto c_i.$$

For $\emptyset \neq A \subset \{1, \dots, n\}$, the $\mathbb{F}_q$ -vector space morphism

$$\pi_A : \mathbb{F}_{q^k} \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{|A|}$$

is defined by the projection

$$(s, c_1, \dots, c_n) \mapsto (c_i)_{i \in A}.$$

For $\mathbf{v} \in \mathbb{F}_{q^k} \times \mathbb{F}_q^n$, it is sometimes convenient to denote $\pi_0(\mathbf{v}) \in \mathbb{F}_{q^k}$ by $\mathbf{v}_0$ and $\pi_A(\mathbf{v}) \in \mathbb{F}_q^{|A|}$ by $\mathbf{v}_A$. We write $\mathcal{I}^* = \{1, \dots, n\}$.

Definition 5.2. An n -code for $\mathbb{F}_{q^k}$ (over $\mathbb{F}_q$) is an $\mathbb{F}_q$ -vector space $C \subset \mathbb{F}_{q^k} \times \mathbb{F}_q^n$ such that

- (i) $\pi_0(C) = \mathbb{F}_{q^k}$
- (ii) $(\text{Ker } \pi_{\mathcal{I}^*}) \cap C \subset (\text{Ker } \pi_0) \cap C$.

Definition 5.3. Let $\mathbb{F}_q$ be a finite field, $k > 0$ an integer. For two vectors $\mathbf{x} = (x_0, x_1, \dots, x_m), \mathbf{x}' = (x'_0, x'_1, \dots, x'_m) \in \mathbb{F}_{q^k} \times \mathbb{F}_q^m$ their product $\mathbf{x} * \mathbf{x}' \in \mathbb{F}_{q^k} \times \mathbb{F}_q^m$ is defined as $(x_0 x'_0, x_1 x'_1, \dots, x_m x'_m)$ where $x_0 x'_0$ is the product in the extension field $\mathbb{F}_{q^k}$ and $x_i x'_i$ is the product in $\mathbb{F}_q$ for $i = 1, \dots, m$.

Let d be a positive integer. If C is a $\mathbb{F}_q$ -vector subspace of $\mathbb{F}_{q^k} \times \mathbb{F}_q^n$, then $C^{*d} \subset \mathbb{F}_{q^k} \times \mathbb{F}_q^n$ is the $\mathbb{F}_q$ -linear subspace generated by all terms of the form $\mathbf{c}^{(1)} * \dots * \mathbf{c}^{(d)}$ with $\mathbf{c}^{(1)}, \dots, \mathbf{c}^{(d)} \in C$. For $d = 2$, we use the abbreviation $\widehat{C} := C^{*2}$.

Now we can introduce the notion of multiplication-friendly code.

Definition 5.4. Let $n, k \in \mathbb{Z}$. An (n, k) -multiplication-friendly code C over $\mathbb{F}_q$ is an n -code for $\mathbb{F}_{q^k}$ (over $\mathbb{F}_q$) such that

- (i) $n, k \geq 1$.
- (ii) $\widehat{C}$ is also an n -code for $\mathbb{F}_{q^k}$.

Remark 5.5. Since $\pi_0(C) = \mathbb{F}_{q^k}$ implies $\pi_0(\widehat{C}) = \mathbb{F}_{q^k}$ we can replace (ii) by

$$(ii')(x, \mathbf{0}) \notin \widehat{C} \text{ for all } x \in \mathbb{F}_{q^k} \setminus \{0\}$$

and we get an equivalent definition.

Multiplication-friendly codes are also considered in [53] and are called *supercodes* there. By [53, Corollary 1.13], an (n, k) -multiplication-friendly code C over $\mathbb{F}_q$ yields a bilinear multiplication algorithm of multiplicative complexity n over $\mathbb{F}_q$. Therefore, we are interested in the smallest n for fixed q and k .

Definition 5.6. We define the quantity

$$\mu_q(k) = \min_{n \in \mathbb{Z}_{>0}} \{n : \text{there exists an } (n, k)\text{-multiplication-friendly code over } \mathbb{F}_q\}$$

To measure how $\mu_q(k)$ behaves when q is fixed and k tends to ∞ , we define two asymptotic quantities

$$M_q = \limsup_{k \rightarrow \infty} \frac{\mu_q(k)}{k}$$

and

$$m_q = \liminf_{k \in \mathbb{N}} \frac{\mu_q(k)}{k}.$$

D.V. Chudnovsky and G.V. Chudnovsky [21] first employed algebraic curves over finite fields to construct bilinear multiplication algorithms implicitly through multiplication-friendly codes in 1986 (please refer to [5] for more background). This idea was further developed in [53] in order to study the quantities m_q and M_q . The main idea in [53] is to solve a special Riemann-Roch system, stated in Theorem 5.7. However, the role of 2-torsion points in divisor class group was neglected in [53], and it turns out that there is a gap in the proof of the main result in [53]. Namely, the mistake is in the proof of their Lemma 3.3, page 161, the paragraph following formulas about the degrees of

the divisors. It reads: “Thus the number of linear equivalence classes of degree a for which either Condition α or Condition β fails is at most $D_{b'} + D_b$ ”. This is incorrect. D_b should be multiplied by the torsion. Hence the proof of their asymptotic bound is incorrect, as there is an implicit but (so far) unjustified assumption on $J_2 = 0$ being possible, or rather even the stronger assumption that $\mathcal{J}[2] = \{0\}$ is possible at all levels in an asymptotically good (optimal) family. Therefore, their claim that $m_q \leq 2(1 + \frac{1}{A(q)-1})$ is unjustified. Moreover, some other results [2, 3] use the same approach and have the same gap (the asymptotical results in their precursor [1] are based on the conjecture that a tower exists attaining certain properties). In [2] the mistake is at the very beginning of page 1801 (the sentence starts on the previous page): “Hence, the number of linear equivalence classes of divisors of degree $n + g - 1$ for which either the condition (5) or the condition (6) fails is at most $2D_{g-1}$ where D_{g-1} denotes...”. Hence the proof of the asymptotic bound is incorrect. We will now give an upper bound for m_q which involves the 2-torsion limit introduced in this paper. We first need to state the problem in a way that we can use the results in Section 3.

Theorem 5.7. *Let $F/\mathbb{F}_q$ be an algebraic function field and $N, k > 1$ be integers. Suppose there exist $P_1, \dots, P_N \in \mathbb{P}^{(1)}(F)$ with $P_i \neq P_j$ ($i \neq j$) and $Q \in \mathbb{P}^{(k)}(F)$. Let $D = \sum_{i=1}^N P_i + Q \in \text{Div}(F)$ and $D^- = \sum_{i=1}^N P_i \in \text{Div}(F)$. Let $K \in \text{Div}(F)$ be a canonical divisor.*

If the Riemann-Roch system

$$\begin{cases} \ell(-X + K + Q) = 0 \\ \ell(2X - D^-) = 0 \end{cases}$$

has some solution, then there exists a solution $G \in \text{Div}(F)$ such that $\text{supp } G \cap \text{supp } D = \emptyset$, and $C = C(D, G)_L$ is an (N, k) -multiplication friendly code over $\mathbb{F}_q$. Furthermore, write $r = \ell(2G) - \ell(2G - D^-)$. Then there exist r indices $i_1, \dots, i_r \in \{1, \dots, N\}$, such that $\tilde{C} = C(\tilde{D}, G)_L$ is a (r, k) -multiplication-friendly code, where $\tilde{D} = \sum_{j=1}^r P_{i_j} + Q \in \text{Div}(F)$. Therefore $\mu_q(k) \leq r \leq \ell(2G)$.

Proof. If there exists a solution, any divisor in its class of equivalence is also a solution. By the Weak Approximation Theorem, we can take an element G of this class in such a way that $\text{supp } G \cap \text{supp } D = \emptyset$.

Suppose G is a solution. We prove $C = C(D, G)_L$ is a multiplication-friendly code. We need to verify $\pi_0(C) = \mathbb{F}_{q^k}$ and $(x, \mathbf{0}) \notin \hat{C}$ for all $0 \neq x \in \mathbb{F}_{q^k}$.

Since $\deg Q = k$, it follows by the Riemann-Roch Theorem and $\ell(K - G + Q) = 0$ that $\ell(G) = \ell(G - Q) + k$. This is enough to ensure that $\pi_0(C) = \mathbb{F}_{q^k}$, as follows: Consider the map

$$\rho : \mathcal{L}(G) \rightarrow \mathbb{F}_{q^k},$$

$$f \mapsto f(Q).$$

Its kernel is $\mathcal{L}(G - Q)$. So its image is isomorphic to $\mathcal{L}(G)/\mathcal{L}(G - Q)$, and this has dimension (over $\mathbb{F}_q$) $\ell(G) - \ell(G - Q) = k$. So $\pi_0(C) = \mathbb{F}_{q^k}$.

Second, as $\hat{C} \subset C(D, 2G)_L$, it suffices to prove that $(x, \mathbf{0}) \notin C(D, 2G)_L$ 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 $i = 1, \dots, N$ satisfies $f(Q) = 0$. But this is trivially true as in these conditions, $f \in \mathcal{L}(2G - D^-) = \{0\}$. We have proved C is a multiplication-friendly code.

Finally, consider the $\mathbb{F}_q$ -linear code $C(D^-, 2G)_L$. It has dimension r by definition. Let $i_1, \dots, i_r \in \{1, \dots, N\}$ be such that the code $C(\tilde{D}^-, 2G)_L$ of length r equals $\mathbb{F}_q^r$, where $\tilde{D}^- = \sum_{j=1}^r P_{i_j}$. Note that $\tilde{C} = C(\tilde{D}, G)_L$ satisfies $\pi_0(\tilde{C}) = \mathbb{F}_{q^k}$ 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, $r = \ell(2G) - \ell(2G - \tilde{D}^-)$. Since, by definition, it also holds that $r = \ell(2G) - \ell(2G - D^-)$, it follows that $\mathcal{L}(2G - D^-) = \mathcal{L}(2G - \tilde{D}^-)$. So if $f \in \mathcal{L}(2G - \tilde{D}^-)$, then $f \in \mathcal{L}(2G - D^-)$. This implies $f(Q) = 0$, as shown before. $\square$

Combining Theorem 5.7 with Theorem 3.2, we get

Theorem 5.8. *Let $F/\mathbb{F}_q$ be an algebraic function field and $N, k > 1$ be integers. Suppose $|\mathbb{P}^{(1)}(F)| \geq N$ and $\mathbb{P}^{(k)}(F)$ is not empty. If there is a positive integer d such that*

$$h > A_{2g-2-d+k} + A_{2d-N}|\mathcal{J}[2]|$$

then $\mu_q(k) \leq \max\{\ell(2G) : G \in \text{Div}(F), \deg G = d\}$. In particular, if in addition $d \geq g$, then $\mu_q(k) \leq 2d - g + 1$.

Note that the last part is a consequence of the fact that if $\deg G = d \geq g$, then $\deg 2G = 2d \geq 2g$ and by Riemann-Roch, $\ell(2G) = 2d - g + 1$

Theorem 5.9. *Let $\mathbb{F}_q$ be a finite field. If there exists a real number $a \leq A(q)$ with $a \geq 1 + J_2(q, a)$ then*

$$m_q \leq 2 \left(1 + \frac{1}{a - J_2(q, a) - 1} \right).$$

In particular, if $A(q) \geq 1 + J_2(q, A(q))$, then

$$m_q \leq 2 \left(1 + \frac{1}{A(q) - J_2(q, A(q)) - 1} \right).$$

Proof. Let $\mathcal{F} = \{F_s/\mathbb{F}_q\}_{s=1}^\infty$ be an infinite family of function fields with limit $A(\mathcal{F}) = A \geq a$ and such that $J_2(\mathcal{F}) = J_2(q, a)$, which exists by definition. Let $\kappa > 0$ be a real number. The precise value of κ will be determined later. And define, for every s , $g_s = g(F_s)$, $n_s = N_1(F_s)$, $k_s = \lfloor \kappa g_s \rfloor$ and $j_s = \log_q |\mathcal{J}_{F_s}[2]|$. Note $\lim_{s \rightarrow \infty} n_s/g_s = A$ and $\liminf j_s/g_s = J_2(q, a)$.

We will apply 5.8 to all large enough function fields F_s . It is enough to verify that there exists a place Q of degree k_s in F_s and that

$$h(F_s) > A_{2g_s-2-d_s+k_s} + |\mathcal{J}[2]|A_{2d_s-n_s} \quad (5.1)$$

holds for some d_s .

First note that [55, Corollary 5.2.10(c)] states that for any function field F and any positive integer k with $q^{(k-1)/2}(q^{1/2} - 1) \geq 2g(F) + 1$, there is at least one place of degree k . In our setting, since $\lim_{s \rightarrow \infty} k_s/g_s = \kappa > 0$, a place of degree k_s exists in F_s for large enough s .

Suppose that for any $\epsilon > 0$, there exists a value of s such that

$$k_s \leq \frac{n_s - g_s - j_s}{2} - \epsilon g_s - 1. \quad (5.2)$$

Then it is easy to see that we can choose an integer d_s with

$$d_s \geq k_s + g_s + \frac{\epsilon}{2}g_s \quad (5.3)$$

and

$$2d_s \leq n_s + g_s - j_s - \epsilon g_s. \quad (5.4)$$

Then for this selection of d_s we can apply Proposition 3.4 to get

$$\frac{A_{2g_s-2-d_s+k_s}}{h} \leq \frac{g_s}{q^{g_s-(2g_s-2-d_s+k_s)-1}(\sqrt{q}-1)^2} \quad (5.5)$$

and

$$|\mathcal{J}[2]| \frac{A_{2d_s-n_s}}{h} \leq \frac{g_s q^{j_s}}{q^{g_s-(2d_s-n_s)-1}(\sqrt{q}-1)^2} \quad (5.6)$$

Now if s is large enough, equations 5.3 and 5.5 imply that

$$A_{2g_s-2-d_s+k_s} \leq h/3$$

and equations 5.4 and 5.6 imply that

$$|\mathcal{J}[2]|A_{2d_s-n_s} \leq h/3,$$

so equation 5.1 holds, and we can apply Theorem 5.8 and (since in addition $d_s \geq g_s - 1$ by equation 5.3), this gives $\mu_q(k_s) \leq 2d_s - g_s + 1$. In particular, since we can take ϵ arbitrarily small, we can choose $d_s = k_s + g_s + 1$, and this yields the bound $\mu_q(k_s) \leq 2k_s + g_s + 3$.

So all is left is to determine when we can fulfill condition 5.2. It is not difficult to see that if $\kappa < \frac{A-1-J_2(q,a)}{2}$, then for an infinite number of values of s , and for small enough (but constant) ϵ , the condition holds.

Therefore, for those values of s , we have

$$\frac{\mu_q(k_s)}{k_s} \leq \frac{2k_s + g_s + 3}{k_s} \leq \frac{(2 + \frac{1}{\kappa})k_s + o(1)}{k_s} \rightarrow 2 + \frac{1}{\kappa}$$

for any $\kappa < \frac{A-1-J_2(q,a)}{2}$.

Hence

$$m_q = \liminf_{k \rightarrow \infty} \frac{\mu_q(k)}{k} \leq 2 + \frac{2}{A-1-J_2(q,a)} \leq 2 \left(1 + \frac{1}{a-J_2(q,a)-1} \right)$$

which finishes the proof. $\square$

Remark 5.10. Recently in [47], H. Randriambololona proved that the original result claimed in [53], i.e. $m_q \leq 2(1 + \frac{1}{A(q)-1})$, can indeed be attained in the case $A(q) > 5$.⁴

From Theorem 2.6, we can apply Theorem 5.9 to all fields $\mathbb{F}_q$ with $q \geq 8$, except perhaps $q = 11$ and 13. These include several fields for which the result in Remark 5.10 cannot be applied directly. However, we must also take into account the following descent lemma which, combined with any of these results, allows to obtain upper bounds for m_q for all fields $\mathbb{F}_q$.

Lemma 5.11. [53, Corollary 1.3] For every finite field $\mathbb{F}_q$ and every positive integer k , we have

$$m_q \leq \frac{\mu_q(k)}{k} m_{q^k}.$$

In order to obtain explicit results, we need some values of $\mu_q(k)$ for small values of k . We can use the following lemma, which for example can be found in [16, Example III.5].

Lemma 5.12. [16, Example III.5] Let q be a prime power and k be an integer with $2 \leq k \leq q/2 + 1$. Then $\mu_q(k) = 2k - 1$. In particular $\mu_q(2) = 3$ for every q and $\mu_q(3) = 5$ for every $q \geq 4$.

Corollary 5.13. For every prime power q , we have $m_q \leq \frac{3}{2}m_{q^2}$ and if $q \geq 4$, then $m_q \leq \frac{5}{3}m_{q^3}$.

These observations allow us to compare the bounds which result from Theorem 5.9 with those implied by the result in Remark 5.10. We find then that our Theorem 5.9 gives the best bound in the cases $q = 16, 25, 32$ while for the rest of cases, applying Remark 5.10 in a suitable extension and then using the descent results above is preferable, given the current knowledge about $A(q)$ and the bounds for the torsion limit given in Theorem 2.3. We give some examples in Table 2. For $q = 8, 9, 27$, the results are found by applying Theorem 5.9 and Remark 5.10 to $\mathbb{F}_{q^2}$ (followed by Corollary 5.13). Note in particular that it would be possible to apply Theorem 5.9 directly in these cases, yet it would give a worse bound. For $q = 4, 5$, we apply Theorem 5.9 and Remark 5.10 to $\mathbb{F}_{q^3}$. For $q = 2, 3$ we use the bounds for m_{q^2} that we have just computed. Finally, for $q = 16, 25, 32$ we apply Theorem 5.9 directly on $\mathbb{F}_q$, while we apply Remark 5.10 on $\mathbb{F}_{q^2}$. For the case $q = 16$, the fact that we can prove an improved torsion bound (we are in the case (iii) of Theorem 2.3) using the theorem of Deuring-Shafarevich is significant, as otherwise we would only be able to prove the bound $m_{16} \leq 3.334$ this way.

In the rest of this section, we improve the state of the art [16] regarding lower bounds on the limit M_q , for small values of q such as $q = 2, 3, 4, 5$. The following result can be found in [16].

Proposition 5.14. Let $F/\mathbb{F}_q$ be a function field with r distinct places $P_1, \dots, P_r$. Let Q be a place of degree k . If there exists a divisor G such that the following two conditions are satisfied

(i) $\ell(G) - \ell(G - Q) = \deg(Q);$

(ii) $\ell(2G - \sum_{i=1}^r P_i) = 0$

⁴Note that in [47], our notion m_q is denoted by m_q^{sym} .

q	2	3	4	5	8
Thm. 5.9	5.836	5.174	3.891	3.932	3.501
Rem. 5.10	5.834	5.143	3.889	3.903	3.5
q	9	16	25	27	32
Thm. 5.9	3.449	3.026	2.779	3.121	2.667
Rem. 5.10	3.429	3.215	3.131	3.12	3.1

Table 2: Upper bounds for m_q

then

$$\mu_q(k) \leq \sum_{i=1}^r \mu_q(s_i),$$

where $s_i = \deg(P_i)$ for all $1 \leq i \leq r$.

The two conditions of Proposition 5.14 can be replaced by the solvability of certain Riemann-Roch system as shown below.

Corollary 5.15. *Let $F/\mathbb{F}_q$ be a function field with r distinct places $P_1, \dots, P_r$. Let Q be a place of degree k . If the Riemann-Roch system*

$$\begin{cases} \ell(K - X + Q) = 0 \\ \ell(2X - \sum_{i=1}^r P_i) = 0 \end{cases}$$

has solutions for a canonical divisor K , then

$$\mu_q(k) \leq \sum_{i=1}^r \mu_q(s_i),$$

where $s_i = \deg(P_i)$ for all $1 \leq i \leq r$.

Proof. Suppose that G is a solution. Then we have $\mathcal{L}(K - G + Q) = 0$, and hence $\mathcal{L}(K - G) = 0$. Thus, we have

$$\ell(G) - \ell(G - Q) = \deg(Q) + \ell(K - G) - \ell(K - G + Q) = \deg(Q).$$

The desired result follows from Proposition 5.14. $\square$

Now combining Corollary 5.15 with Theorem 3.2, we obtain a numerical condition.

Theorem 5.16. *Let $F/\mathbb{F}_q$ be a function field with r distinct places $P_1, \dots, P_r$. Let Q be a place of degree k . Denote by A_r the number of effective divisors of degree r in $\text{Div}(F)$. If there is a positive integer d such that*

$$h > A_{2g-2-d+k} + |\mathcal{J}[2]| A_{2d-\sum_{i=1}^r s_i},$$

then

$$\mu_q(k) \leq \sum_{i=1}^r \mu_q(s_i),$$

where $s_i = \deg(P_i)$ for all $1 \leq i \leq r$.

To derive a lower bound on M_q , we need a family of Shimura curves with genus in this family growing slowly (see [16, Lemma IV.4]).

Lemma 5.17. *For any prime power q and integer $t \geq 1$, there exists a family $\{\mathcal{X}_s\}_{s=1}^\infty$ of Shimura curves over $\mathbb{F}_q$ such that*

- (i) *The genus $g(F_s) \rightarrow \infty$ as s tends to ∞ , where F_s stands for the function field $\mathbb{F}_q(\mathcal{X}_s)$.*
- (ii) *$\lim_{s \rightarrow \infty} g(F_s)/g(F_{s-1}) = 1$.*

- (iii) $\lim_{s \rightarrow \infty} B_{2t}(F_s)/g(F_s) = (q^t - 1)/(2t)$, where $B_{2t}(F_s)$ stands for the number of places of degree $2t$ in F_s .

Now we are ready to derive the following result.

Theorem 5.18. *For a prime power q , one has*

$$M_q \leq \begin{cases} \mu_q(2t) \frac{q^t - 1}{t(q^t - 2 - \log_q 2)} & \text{if } 2|q \\ \mu_q(2t) \frac{q^t - 1}{t(q^t - 2 - 2\log_q 2)} & \text{otherwise} \end{cases}$$

for any $t \geq 1$ as long as $q^t - 2 - \log_q 2 > 0$ for even q ; and $q^t - 2 - 2\log_q 2 > 0$ for odd q .

Proof. We prove the theorem only for the case where q is a power of 2. For the odd characteristic case, the only difference is the size of $\mathcal{J}[2]$.

Let $\{F_s/\mathbb{F}_q\}_{s=1}^\infty$ be a family of function fields with the three properties in Lemma 5.17. For every $k \geq 2$, let $s(k)$ be the smallest positive integer such that

$$B_{2t}(F_{s(k)}) \geq r := \left\lceil \left(\frac{1}{2}g_{s(k)}(1 + \log_q 2) + k + \frac{3}{2}\log_q \left(\frac{3qg_{s(k)}}{(\sqrt{q} - 1)^2} \right) + 1 \right) / t \right\rceil, \quad (5.7)$$

where $g_{s(k)}$ is the genus $g(F_{s(k)})$ of $F_{s(k)}$.

Thus, we can find r places of degree $2t$ in $F_{s(k)}$. By the definition of r in Equation (5.7), we have

$$g_{s(k)} + k + \log_q \left(\frac{3qg_{s(k)}}{(\sqrt{q} - 1)^2} \right) \leq \frac{1}{2}g_{s(k)}(1 - \log_q 2) + rt - \frac{1}{2}\log_q \left(\frac{3qg_{s(k)}}{(\sqrt{q} - 1)^2} \right) - 1. \quad (5.8)$$

Therefore, we can find an integer d between $g_{s(k)} + k + \log_q \left(\frac{3qg_{s(k)}}{(\sqrt{q} - 1)^2} \right)$ and $\frac{1}{2}g_{s(k)}(1 - \log_q 2) + rt - \frac{1}{2}\log_q \left(\frac{3qg_{s(k)}}{(\sqrt{q} - 1)^2} \right)$, i.e., we have

$$\frac{g_{s(k)}}{q^{g_{s(k)} - (2g_{s(k)} - d + k) - 1}(\sqrt{q} - 1)^2} \leq \frac{1}{3} \quad (5.9)$$

and

$$\frac{g_{s(k)}2^{g_{s(k)}}}{q^{g_{s(k)} - (2d - 2rt) - 1}(\sqrt{q} - 1)^2} \leq \frac{1}{3} \quad (5.10)$$

Using the fact that $|\mathcal{J}[2]| \leq q^{g_{s(k)}}$ and combining Equations (5.9), (5.10) and Proposition 3.4, we get

$$h > \frac{2h}{3} \geq A_{2g_{s(k)} - d + k} + |\mathcal{J}[2]|A_{2d - 2rt},$$

where h is the zero divisor class number of $F_{s(k)}$. By Theorem 5.16, we have

$$\mu_q(k) \leq r\mu_q(2t).$$

On the other hand, by choice of $s(k)$, we know that

$$B_{2t}(F_{s(k)-1}) \leq \left\lceil \left(\frac{1}{2}g_{s(k)-1}(1 + \log_q 2) + k + \frac{3}{2}\log_q \left(\frac{3qg_{s(k)-1}}{(\sqrt{q} - 1)^2} \right) + 1 \right) / t \right\rceil - 1, \quad (5.11)$$

By the property (iii) in Lemma 5.17, the inequality (5.11) gives

$$k \geq \frac{1}{2}g_{s(k)-1}(q^t - 2 - \log_q 2) + o(g_{s(k)-1}). \quad (5.12)$$

Finally by Theorem 5.16, we have

$$\begin{aligned} \frac{\mu_q(k)}{k} &\leq \frac{r\mu_q(2t)}{k} \leq \mu_q(2t) \left(\frac{(1 + \log_q 2)g_{s(k)} + o(g_{s(k)})}{2kt} + \frac{1}{t} \right) \\ &= \mu_q(2t) \left(\frac{(1 + \log_q 2)g_{s(k)} + o(g_{s(k)})}{t(g_{s(k)-1}(q^t - 2 - \log_q 2) + o(g_{s(k)-1}))} + \frac{1}{t} \right) \\ &\rightarrow \mu_q(2t) \frac{q^t - 1}{t(q^t - 2 - \log_q 2)} \quad \text{as } k \rightarrow \infty. \end{aligned}$$

This finishes the proof. $\square$

Note that in [16], a trivial solution of the Riemann-Roch system in Corollary 5.15 was used due to the fact that torsion limit was not considered, and hence a weaker bound on M_q was derived in [16].

With help of the torsion-limit technique and Riemann-Roch system, we can bring down the upper bound derived in Theorem [16, Theorem IV.5] and hence we get further improvements on M_q for small values of q . Here we only provide upper bounds for a few small q to demonstrate our improvements.

Corollary 5.19. *One has the upper bounds on M_q for $q = 2, 3, 4, 5$ as shown in the following table*

q	2	3	4	5
M_q	7.23	5.45	4.44	4.34

Proof. (i) For $q = 2$, the desired result follows from Theorem 5.18 by taking $t = 6$ and applying $\mu_2(12) \leq 42$.

(ii) For $q = 3$, the desired result follows from Theorem 5.18 by taking $t = 5$ and applying $\mu_3(10) \leq 27$.

(iii) For $q = 4$, the desired result follows from Theorem 5.18 by taking $t = 2$ and applying $\mu_4(4) = 8$.

(iv) For $q = 5$, the desired result follows from Theorem 5.18 by taking $t = 2$ and applying $\mu_5(4) = 8$. $\square$

6 Application 3: Asymptotic Bounds for Frameproof Codes

6.1 Definitions and basic results

Let S be a finite set of q elements (we denote by $\mathbb{F}_q$ the finite field with q elements if q is a prime power) and let n be a positive integer. Define the i -th projection:

$$\pi_i : S^n \rightarrow S, \quad (a_1, \dots, a_n) \mapsto a_i.$$

Definition 6.1. *For a subset $A \subset S^n$, we define the descendants of A , $\text{desc}(A)$, to be the set of all words $\mathbf{x}$ such that for each $1 \leq i \leq n$, there exists $\mathbf{a} \in A$ satisfying $\pi_i(\mathbf{x} - \mathbf{a}) = 0$.*

Definition 6.2. *Let $s \geq 2$ be an integer. A q -ary s -frameproof code of length n is a subset $C \subset S^n$ such that for all $A \subset C$ with $|A| \leq s$, the intersection $\text{desc}(A) \cap C$ is the same as A .*

Note that 1-frameproof codes are uninteresting, since any $C \subset S$ would satisfy the resulting condition. From the definition of frameproof codes, it is clear that a q -ary s -frameproof code C is a q -ary s_1 -frameproof code for any $2 \leq s_1 \leq s$.

Following the notation from [56], we denote a q -ary s -frameproof code in S^n of size M by $s\text{-FPC}(n, M)$. As usual, we denote a q -ary error-correcting code of length n , size M and minimum distance d by (n, M, d) -code, or $[n, \log_q M, d]$ -linear code if the code is linear.

We want to look at the asymptotic behavior of s -frameproof codes in the sense that q and s are fixed and the length n tends to infinity.

Definition 6.3. *For fixed integers $q \geq 2$, $s \geq 2$ and $n \geq 2$, let $M_q(n, s)$ denote the maximal size of q -ary s -frameproof codes of length n , i.e.,*

$$M_q(n, s) := \max\{M : \text{there exists a } q\text{-ary } s\text{-FPC}(n, M)\}.$$

For fixed q and s , define the asymptotic quantity

$$R_q(s) = \limsup_{n \rightarrow \infty} \frac{\log_q M_q(n, s)}{n}.$$

It seems that the exact values of $R_q(s)$ are not easy to be determined for any given q and s . Instead, we will get some lower bounds on $R_q(s)$. Before looking at lower bounds, we first derive an upper bound on $R_q(s)$ from [11].

Theorem 6.4.

$$R_q(s) \leq \frac{1}{s}.$$

Proof. By Theorem 1 of [11], we have

$$M_q(n, s) \leq \max\{q^{\lceil \frac{n}{s} \rceil}, r \left(q^{\lceil \frac{n}{s} \rceil} - 1 \right) + (s - r) \left(q^{\lfloor \frac{n}{s} \rfloor} - 1 \right)\},$$

where $r \in \{0, 1, \dots, s - 1\}$ and r is the remainder of n divided by s . Thus, we have

$$M_q(n, s) \leq sq^{\lceil \frac{n}{s} \rceil}.$$

The desired result follows. $\square$

From now on we will concentrate on lower bounds on $R_q(s)$. Let us first recall the constructions from [22].

Proposition 6.5. *Let q be a prime power. Then a q -ary $[n, k, d]$ -linear code C is a q -ary s -FPC(n, q^k) with $s = \lfloor (n - 1)/(n - d) \rfloor$.*

Remark 6.6. *This construction shows that the crucial parameter s is determined only by the minimum distance of C if the length is given.*

From the above relationship between linear codes and frameproof codes, we immediately obtain a lower bound on $R_q(s)$ from the Gilbert-Varshamov bound.

Theorem 6.7. *Let q be a prime power and $2 \leq s < q$ an integer. Then*

$$R_q(s) \geq 1 - H_q\left(1 - \frac{1}{s}\right),$$

where

$$H_q(\delta) = \delta \log_q(q - 1) - \delta \log_q \delta - (1 - \delta) \log_q(1 - \delta)$$

is the q -ary entropy function.

Proof. The desired result follows directly from the Gilbert-Varshamov bound and Proposition 6.5. $\square$

Remark 6.8. *The bound in Theorem 6.7 is only an existence result as the Gilbert-Varshamov bound is not constructive.*

6.2 Lower Bounds from AG Codes

In this section, we introduce two lower bounds on $R_q(s)$ from algebraic geometry codes. One bound can be obtained by directly applying Proposition 6.5 and the Tsfasman-Vlăduț-Zink bound [58]. However, the second bound employs our torsion limits.

Theorem 6.9. *For a prime power q and an integer $s \geq 2$, we have*

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)}.$$

Proof. Let $\delta = 1 - 1/s$. Combining Proposition 6.5 with the TVZ bound, we obtain the desired result. $\square$

Remark 6.10. (i) *The bound in Theorem 6.9 is constructive as long as sequences of curves attaining $A(q)$ are explicit.*

(ii) *It is easy to check that for every $s \geq 2$, the bound in Theorem 6.9 is better than the one in Theorem 6.7 for sufficiently large square q . For instance, for $s = 2$, and a square $q \geq 49$, the bound in Theorem 6.9 is always better than the one in Theorem 6.7.*

(iii) Comparing with the upper bound in Theorem 6.4, we find that

$$\frac{1}{s} - \frac{1}{A(q)} \leq R_q(s) \leq \frac{1}{s}.$$

Since $1/A(q) \rightarrow 0$ as $q \rightarrow \infty$ (see [45]), $R_q(s)$ is getting closer to $1/s$ as $q \rightarrow \infty$. The result $R_q(s) \approx 1/s$ is also implicitly stated in [22] by combining Propositions 2 and 3 there.

The bound in Theorem 6.9 has been further improved in [63, 46, 48].

Theorem 6.11. (i) [63] For every $2 \leq s \leq A(q)$, one has

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)} + \frac{1 - 2\log_q s}{sA(q)}.$$

(ii) [46] Let s be the characteristic of $\mathbb{F}_q$, then one has

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)} + \frac{1 - \log_q s}{sA(q)}.$$

(iii) [48] For $A(q) > 5$, one has

$$R_q(2) \geq \frac{1}{2} - \frac{1}{2A(q)}.$$

For the rest of this section, we derive a lower bound on $R_q(s)$ by making use of the idea from [63] and our torsion limit. In particular, the bounds (i) and (ii) of Theorem 6.11 can be deduced from our lower bound in Theorem 6.16. Furthermore, we improve the above bounds in the following two cases: (i) when q is a square and s is the characteristic of $\mathbb{F}_q$, the bound in Theorem 6.11(ii) can be improved significantly (see Corollary 6.17(i)); (ii) when s does not divide $q-1$, the bound in Theorem 6.11(i) can be improved (see Corollary 6.17(ii)).

Let $P_1, P_2, \dots, P_n$ be n distinct rational points of a function field F over the finite field $\mathbb{F}_q$. Choose a positive divisor G such that $\mathcal{L}(G - \sum_{i=1}^n P_i) = \{0\}$. Let $\nu_{P_i}(G) = v_i \geq 0$ and t_i be a local parameter at P_i for each i .

Consider the map

$$\begin{aligned} \phi : \mathcal{L}(G) &\longrightarrow \mathbb{F}_q^n \\ f &\mapsto ((t_1^{v_1} f)(P_1), (t_2^{v_2} f)(P_2), \dots, (t_n^{v_n} f)(P_n)). \end{aligned}$$

Then the image of ϕ forms a subspace of $\mathbb{F}_q^n$ that is defined as an algebraic geometry code. The image of ϕ is denoted by $C(\sum_{i=1}^n P_i, G)_L$. The map ϕ is an embedding since $\mathcal{L}(G - \sum_{i=1}^n P_i) = \{0\}$ and the dimension of $C(\sum_{i=1}^n P_i, G)_L$ is equal to $\ell(G)$.

Remark 6.12. Notice that the above construction is a modified version of algebraic geometry codes defined by Goppa. The advantage of the above construction is to make it possible to get rid of the condition $\text{Supp}(G) \cap \{P_1, P_2, \dots, P_n\} = \emptyset$. This is crucial for our construction of frameproof codes in this section.

When the condition $\text{Supp}(G) \cap \{P_1, P_2, \dots, P_n\} = \emptyset$ is satisfied, i.e., $v_i = 0$ for all $i = 1, \dots, n$, then the above construction of algebraic geometry codes is consistent with Goppa's construction.

Theorem 6.13. Let $F/\mathbb{F}_q$ be an algebraic function field of genus g and let $P_1, P_2, \dots, P_n$ be n distinct rational points of F . Let G be a positive divisor such that $\deg(G) < n$. Let $s \geq 2$ satisfy $\mathcal{L}(sG - \sum_{i=1}^n P_i) = \{0\}$. Then $C(\sum_{i=1}^n P_i, G)_L$ is an s -FPC($n, q^{\ell(G)}$).

Proof. For all $f \in \mathcal{L}(G)$, denote by $\mathbf{c}_f$ the codeword

$$\phi(f) = ((t_1^{v_1} f)(P_1), (t_2^{v_2} f)(P_2), \dots, (t_n^{v_n} f)(P_n)).$$

Let $A = \{\mathbf{c}_{f_1}, \dots, \mathbf{c}_{f_r}\}$ be a subset of $C := C(\sum_{i=1}^n P_i, G)_L$ with $|A| = r \leq s$. Let $\mathbf{c}_g \in \text{desc}(A) \cap C$ for some $g \in \mathcal{L}(G)$. Then by the definition of descendant, for each $1 \leq i \leq n$ we have

$$\prod_{j=1}^r \pi_i(\mathbf{c}_{f_j} - \mathbf{c}_g) = 0,$$

where $\pi_i(\mathbf{c}_{f_j} - \mathbf{c}_g)$ stands for i th coordinate of $\mathbf{c}_{f_j} - \mathbf{c}_g$. This implies that

$$\prod_{j=1}^r (t_i^{v_i} f_j - t_i^{v_i} g)(P_i) = 0,$$

i.e.,

$$\nu_{P_i} \left(\prod_{j=1}^r (t_i^{v_i} f_j - t_i^{v_i} g) \right) \geq 1.$$

This is equivalent to

$$\nu_{P_i} \left(\prod_{j=1}^r (f_j - g) \right) \geq -rv_i + 1.$$

Hence,

$$\prod_{j=1}^r (f_j - g) \in \mathcal{L}(rG - \sum_{i=1}^n P_i) \subset \mathcal{L}(sG - \sum_{i=1}^n P_i) = \{0\}.$$

Thus, the function $\prod_{j=1}^r (f_j - g)$ is the zero function. So, $f_l - g = 0$ for some $1 \leq l \leq r$. Hence $\mathbf{c}_g = \mathbf{c}_{f_l} \in A$. $\square$

From Theorem 6.13, we know that it is crucial to find a divisor G such that $\mathcal{L}(sG - \sum_{i=1}^n P_i) = \{0\}$. Again we can apply our Theorem 3.2 to show

Lemma 6.14. *Let $F/\mathbb{F}_q$ be an algebraic function field of genus g with at least one rational point P_0 .*

Let s, m, n be three integers satisfying $s \geq 2$ and $g \leq m \leq n < sm$ and H a fixed positive divisor of degree n . Then there exists a positive divisor G of degree m such that $\mathcal{L}(sG - H) = \{0\}$ provided that $A_{sm-n}|\mathcal{J}[s]| < h$.

Lemma 6.15. *Let $F/\mathbb{F}_q$ be an algebraic function field of genus g with at least one rational point.*

Let s, m, n be three integers satisfying $s \geq 2$ and $g \leq m \leq n < sm$ and $sm - n < g - \log_q |\mathcal{J}[s]| - \log_q \frac{qg}{(\sqrt{q}-1)^2}$. Let D be a fixed positive divisor of degree n . Then there exists a positive divisor G of degree m such that $\mathcal{L}(sG - D) = \{0\}$.

Proof. By Proposition 3.4 we have (note $1 \leq sm - n \leq g - 1$)

$$\frac{A_{sm-n}}{h} \leq \frac{g}{q^{g-(sm-n)-1}(\sqrt{q}-1)^2}.$$

The condition in Lemma 6.14 is satisfied and the desired result follows. $\square$

Theorem 6.16. *Suppose that q is a prime power and s is an integer such that $A(q) \geq s \geq 2$ and $J_s(q, A(q)) < 1$. Then we have*

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)} + \frac{1 - J_s(q, A(q))}{sA(q)}.$$

Proof. Choose a family of function fields $F/\mathbb{F}_q$ with growing genus such that $\lim_{g(F) \rightarrow \infty} N(F)/g(F) = A(q)$ and $\lim_{g(F) \rightarrow \infty} \log_q |\mathcal{J}[s]|/g(F) = J_s(q, A(q))$. Put $n = N(F)$, $g = g(F)$. Let $D = \sum_{P \in \mathbb{P}(1)(F)} P$.

Now for any fixed $0 < \varepsilon < 1 - J_s(q, A(q))$, put

$$m = \lfloor \frac{n + (1 - J_s(q, A(q)) - \varepsilon)g}{s} \rfloor.$$

Then we obtain

$$\lim_{g \rightarrow \infty} \frac{m}{g} = \frac{A(q) + 1 - J_s(q, A(q)) - \varepsilon}{s} > \frac{A(q)}{s} \geq 1,$$

and

$$\lim_{n \rightarrow \infty} \frac{m}{n} = \frac{A(q) + 1 - J_s(q, A(q)) - \varepsilon}{sA(q)} < \frac{A(q) + 1}{sA(q)} < \frac{2A(q)}{sA(q)} \leq 1,$$

and

$$\lim_{n \rightarrow \infty} \frac{sm}{n} = 1 + \frac{1 - J_s(q, A(q)) - \varepsilon}{A(q)} > 1,$$

and

$$\lim_{n \rightarrow \infty} \frac{sm - n - (1 - J_s(q, A(q)))g}{g} = -\varepsilon < 0.$$

Therefore, for all sufficiently large g we have $g \leq m < n < sm$ by (2), (3) and (4). It follows from (5) that for all sufficiently large g we have

$$sm - n < g - \log_q |\mathcal{J}[s]| - \log_q \frac{qg}{(\sqrt{q} - 1)^2}.$$

By Lemma 6.15, there exists a divisor G of degree m of F such that $\mathcal{L}(sG - D) = \{0\}$ for each sufficiently large g . Thus, by Theorem 6.13 the code $C(D, G)_L$ is an s -FPC($n, q^{\ell(G)}$). Hence,

$$\begin{aligned} R_q(s) &\geq \lim_{g \rightarrow \infty} \frac{\log_q q^{\ell(G)}}{n} \\ &\geq \lim_{g \rightarrow \infty} \frac{m - g + 1}{n} \\ &= \frac{1}{s} - \frac{1}{A(q)} + \frac{1 - J_s(q, A(q))}{sA(q)} - \frac{\varepsilon}{sA(q)}. \end{aligned}$$

Since the above inequality holds for any $0 < \varepsilon < 1 - J_s(q, A(q))$, we get

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)} + \frac{1 - J_s(q, A(q))}{sA(q)}$$

by letting ε tend to 0. This completes the proof. $\square$

Corollary 6.17. *Suppose that q is a prime power and s is an integer such that $A(q) \geq s \geq 2$. Then we have*

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)} + \frac{1 - 2 \log_q s}{sA(q)}. \quad (6.1)$$

Moreover, we obtain an improvement to the bounds in Theorem 6.11 for the following two cases.

(i) *If q is a square and s is the characteristic of $\mathbb{F}_q$ with $\sqrt{q} - 1 \geq s \geq 2$, then*

$$R_q(s) \geq \frac{1}{s} - \frac{1}{\sqrt{q} - 1} + \frac{(1 - (\log_q s)/(\sqrt{q} + 1))}{s(\sqrt{q} - 1)}. \quad (6.2)$$

(ii) *If s does not divide $q - 1$, then*

$$R_q(s) \geq \frac{1}{s} - \frac{1}{A(q)} + \frac{1 - \log_q s}{sA(q)}. \quad (6.3)$$

Proof. The bounds (6.1), (6.2) and (6.3) follow from Theorems 6.16 and Theorem 2.3(i), 2.3(iii) and 2.3(ii), respectively. $\square$

7 Acknowledgments

We are grateful for valuable contributions to the refinements on the bounds for the torsion limit in Theorem 2.3. Bas Edixhoven and Hendrik Lenstra suggested the generic approach we used in its second part. Alp Bassa and Peter Beelen confirmed our hope that stronger bounds should be attainable from certain *specific* recursive towers, by contributing the proof of its third part. We also thank Hendrik for many helpful discussions, and for his encouragement since the paper was first circulated in the Fall of 2009. We are thankful to Florian Hess for valuable discussions. Finally, we thank the referees for their helpful comments.

References

- [1] 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) 293-305.
- [2] S. Ballet. On the tensor rank of the multiplication in the finite fields. *Journal of Number Theory* 128 (2008) 1795-1806.
- [3] S. Ballet. A note on the tensor rank of the multiplication in certain finite fields. *Algebraic geometry and its applications*, 332–342, Ser. Number Theory Appl., 5, World Sci. Publ., Hackensack, NJ, 2008.
- [4] S. Ballet and J. Pielant. On the tensor rank of multiplication in any extension of $\mathbb{F}_2$. *Journal of Complexity* 27(2): 230–245 (2011).
- [5] S. Ballet, R. Rolland. On the bilinear complexity of the multiplication in finite fields. *Séminaires et Congrès* 11, 2005, 179-188.
- [6] A. Bassa, P. Beelen. The Hasse-Witt invariant in some towers of function fields over finite fields *Bull. Braz. Math. Soc.*, Volume 41, Number 4 (2010), 567-582.
- [7] A. Bassa, P. Beelen, A. Garcia, H. Stichtenoth. Towers of function fields over non-prime finite fields. Preprint, 2012. See <http://arxiv.org/abs/1202.5922>.
- [8] 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.
- [9] M. Ben-Or, S. Goldwasser, A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proceedings of STOC 1988*, pp. 1-10. ACM Press, 1988.
- [10] J. Bezerra, A. Garcia, and H. Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink's lower bound. *J. Reine Angew. Math.*, vol. 589, pp. 159–199, December 2005.
- [11] S. Blackburn. Frameproof codes. *SIAM J. Discrete Math.*, Vol. 16, 499-510 (2003).
- [12] M. Boettler. Berechnung von Zetafunktionen algebraischer Kurven über endlichen Körpern. Diplomarbeit. Institut für Mathematik der Technischen Universität Berlin, 2008.
- [13] D. Boneh, J. Shaw. Collusion-secure finger printing for digital data. *IEEE Trans. on Inf. Theory*, Vol. 44, 1897-1905 (1998).
- [14] I. Cascudo, H. Chen, R. Cramer, C. Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over *Any* Finite Field. *Proceeding of 29th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5677, pp. 466-486, August 2009.
- [15] I. Cascudo, R. Cramer, C. Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. *Proceeding of 31st Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 6842, pp. 685-705, August 2011.
- [16] I. Cascudo, R. Cramer, C. Xing, A. Yang. Asymptotic Bound for Multiplication Complexity in the Extensions of Small Finite Fields. *IEEE Transactions on Information Theory*, Vol. 58, Issue 7, pp. 4930 - 4935, 2012.
- [17] D. Chaum, C. Crépeau, I. Damgaard. Multi-party unconditionally secure protocols. *Proceedings of STOC 1988*, pp. 11-19. ACM Press, 1988.
- [18] H. Chen, R. Cramer. Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computation over Small Fields. *Proceedings of 26th Annual IACR CRYPTO*, Springer Verlag LNCS, vol. 4117, pp. 516-531, Santa Barbara, Ca., USA, August 2006.
- [19] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, V. Vaikuntanathan. Secure Computation from Random Error Correcting Codes. *Proceedings of 26th Annual IACR EUROCRYPT*, Barcelona, Spain, Springer Verlag LNCS, vol. 4515, pp. 329-346, May 2007.

- [20] H. Chen, R. Cramer, R. de Haan, I. Cascudo Pueyo. Strongly multiplicative ramp schemes from high degree rational points on curves. *Proceedings of 27th Annual IACR EUROCRYPT*, Istanbul, Turkey, Springer Verlag LNCS, vol. 4965, pp. 451-470, April 2008.
- [21] D.V. Chudnovsky, G.V. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Proc. Natl. Acad. Sci. USA*, vol. 84, no. 7, pp. 1739-1743, April 1987.
- [22] G. Cohen and S. Encheva, *Efficient constructions of frameproof codes*, Electronics Letters, Vol. 36 (2000), 1840-1842.
- [23] R. Cramer, I. Damgaard, U. Maurer. General secure multi-party computation from any linear secret sharing scheme. *Proceedings of 19th Annual IACR EUROCRYPT*, Brugge, Belgium, Springer Verlag LNCS, vol. 1807, pp. 316-334, May 2000.
- [24] I. Damgaard, Y. Ishai, M. Krøigaard. Perfectly Secure Multiparty Computation and the Computational Overhead of Cryptography. *Proceedings of 29th Annual IACR EUROCRYPT*, Nice, France, Springer Verlag LNCS, vol. 6110, pp. 445-465, May 2010.
- [25] A. Fiat, T. Tassa. Dynamic traitor tracing. *Journal of Cryptology* 14, pp. 211-223, 2001.
- [26] M. Franklin, M. Yung. Communication Complexity of Secure Computation. *ACM STOC 1992*: 699-710.
- [27] A. Garcia, H. Stichtenoth (Ed.). Topics in Geometry, Coding Theory and Cryptography. Algebra and Applications Series, Springer Verlag, 2007.
- [28] A. Garcia, H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduț bound. *Invent. Math.* 121, pp. 211-222, 1995.
- [29] G. van der Geer. manYPoints - Table of Curves with Many Points. Online webpage: <http://www.manypoints.org/>
- [30] V. D. Goppa. Codes on algebraic curves. *Soviet Math. Dokl.* 24:170-172, 1981.
- [31] D. Harnik, Y. Ishai, E. Kushilevitz, J. Nielsen. OT-Combiners via Secure Computation. *Proceedings of TCC 2008*: 393-411.
- [32] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comp.* 33(4): 425-445, 2002.
- [33] F. Hess. Generalised Jacobians in Cryptography and Coding Theory. In *WAIFI 2012*, LNCS 7369, p. 1-15, Springer-Verlag, Berlin-Heidelberg-New York, 2012.
- [34] J.W.P. Hirschfeld, G. Korchmáros, F. Torres. Algebraic Curves over a Finite Field. Princeton Series in Applied Mathematics, 2008.
- [35] 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.
- [36] Y. Ishai, E. Kushilevitz, R. Ostrovsky, M. Prabhakaran, A. Sahai, J. Wullschleger. Constant-rate OT from Noisy Channels. *Proceeding of 31st Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 6842, pp. 667-684, August 2011.
- [37] 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.
- [38] Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai. Extracting Correlations. *Proc. 50th IEEE FOCS*, pp. 261-270, 2009.
- [39] Y. Ishai, M. Prabhakaran, A. Sahai. Founding Cryptography on Oblivious Transfer-Efficiently. *Proceedings of 28th Annual IACR CRYPTO*, Santa Barbara, Ca., USA, Springer Verlag LNCS, vol. 5157, pp. 572-591, August 2008.

- [40] H. Maharaj. A Note on Further Improvements of the TVZ-Bound. *IEEE Trans. Inform. Theory* 53(3): 1210-1214 (2007).
- [41] D. Mumford. *Abelian Varieties*. Oxford University Press, 1970.
- [42] 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).
- [43] H. Niederreiter, H. Wang, C. Xing. Applications to Cryptography. In [27].
- [44] H. Niederreiter, C. Xing. Low-Discrepancy Sequences and Global Function Fields with Many Rational Places. *Finite Fields and Their Applications* 2, 241-273 (1996).
- [45] H. Niederreiter and C. Xing. *Rational Points on Curves over Finite Fields: Theory and Applications*. Cambridge University Press, LMS 285, 2001.
- [46] H. Randriambololona. Hecke operators with odd determinant and binary frame-proof codes beyond the probabilistic bound? In *Proc. of ITW 2010 Dublin IEEE Information Theory Workshop*, Dublin, Ireland, 2010.
- [47] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky-Chudnovsky interpolation method. *Journal of Complexity* 28(4): 489-517 (2012).
- [48] H. Randriambololona. $(2, 1)$ -separating systems beyond the probabilistic bound. *Israel Journal of Mathematics*, Volume 195, Issue 1, pp. 171-186 (2013).
- [49] H. Randriambololona. Asymptotically good binary linear codes with asymptotically good self-intersection spans. *IEEE Trans. Inform. Theory* 59(5): 3038-3045 (2013).
- [50] M. Rosen. *Number Theory in Function Fields*. GTM, Springer, 2001.
- [51] J. -P. Serre. *Rational points on curves over finite fields*. Notes of lectures at Harvard University, 1985.
- [52] A. Shamir. How to share a secret. *Comm. of the ACM*, 22(11):612-613, 1979.
- [53] I. Shparlinski, M. Tsfasman, S. Vlăduț. Curves with many points and multiplication in finite fields. *Lecture Notes in Math.*, vol. 1518, Springer-Verlag, Berlin, 1992, pp. 145-169.
- [54] K.W. Shum, I. Aleshnikov, P.V. Kumar, H. Stichtenoth, V. Deolalikar. A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound. *IEEE Trans. Inform. Theory* 47(6): 2225-2241 (2001).
- [55] H. Stichtenoth. *Algebraic function fields and codes*. Springer Verlag, 1993. (New edition: 2009).
- [56] D. R. Stinson and R. Wei, *Combinatorial properties and constructions of traceability schemes and frameproof codes*, *SIAM J. Discrete Math.*, Vol. 11 (1998), 41-53.
- [57] M. Tsfasman, S. Vlăduț, D. Nogin. *Algebraic geometric codes: Basic Notions*. AMS, Mathematical Surveys and Monographs, Vol. 139, 2007.
- [58] M. Tsfasman, S. Vlăduț, Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov Gilbert bound. *Math. Nachr.* 109, 21-28, 1982.
- [59] S. G. Vlăduț. An exhaustion bound for algebraic-geometric modular codes. *Probl. Inf. Transm.*, vol. 23, pp. 22-34, 1987.
- [60] S. G. Vlăduț, V. G. Drinfeld. Number of points of an algebraic curve. *Funct. Anal. Appl.* vol. 17, pp. 53-54, 1983.
- [61] A. Weil. *Variétés Abéliennes et Courbes Algébriques*. Hermann, Paris, 1948.
- [62] C. Xing. Algebraic geometry codes with asymptotic parameters better than the Gilbert-Varshamov and the Tsfasman-Vlăduț-Zink bounds. *IEEE Trans. Inform. Theory*, 47(1): 347-352. (2001).

- [63] C. Xing. Asymptotic bounds on frameproof codes. *IEEE Trans. Inform. Theory*, 48(11): 2991-2995. (2002)
- [64] C. Xing. Goppa Geometric Codes Achieving the Gilbert-Varshamov Bound. *IEEE Trans. Inform. Theory*, 51(1): 259-264 (2005).
- [65] C. Xing, H. Chen. Improvements on parameters of one-point AG codes from Hermitian curves. *IEEE Trans. Inform. Theory*, 48(2): 535-537 (2002).
- [66] C. Xing, S. L. Yeo. Algebraic curves with many points over the binary field. *J. of Algebra*, 311: 775-780, (2007).
- [67] C. Xing, S. L. Yeo. Algebraic curves over finite fields with good asymptotic behavior. Preprint, 2010.
- [68] L. Xu. Improvement on parameters of Goppa geometry codes from maximal curves using the Vlăduț-Xing method. *IEEE Trans. Inform. Theory*, 51(6): 2207-2210 (2005).
- [69] T. Zink. Degeneration of Shimura surface and a problem in coding theory. *Fundamentals of Computation Theory, Lecture Notes in Computer Science Vol. 199*, pp. 503-511, 1985.