Construction of Arithmetic Secret Sharing Schemes by Using Torsion Limits

Seher Tutdere [*], and Osmanbey Uzunkol [†]

Abstract

Recent results of Cascudo, Cramer, and Xing on the construction of arithmetic secret sharing schemes are improved by using some new bounds on the torsion limits of algebraic function fields. Furthermore, new bounds on the torsion limits of certain towers of function fields are given.

Keywords: Algebraic function fields, torsion limits, Riemann-Roch systems of equations, arithmetic secret sharing schemes.

1 Introduction

Secret sharing is a cryptographic mechanism allowing to distribute shares among different parties. This is achieved by a trusted dealer in such a way that only authorized subset of parties can determine the secret [3]. Unlike conventional cryptographic schemes, secret sharing schemes enable the user to eliminate the root of trust problem [3, 21]. Furthermore, secret sharing has plenty of privacy preserving real-life applications ranging from access controls [20], oblivous transfers [23] to biometric authentication schemes [13].

If the authorized subset has the cardinality larger than a predetermined lower bound, then secret sharing schemes have the property of *threshold access structure* [9]. Moreover, a secret sharing scheme is called *ideal* if the shares have the same size as secrets [3]. Shamir's secret sharing scheme is a classical example of an ideal secret sharing scheme having threshold access structure. Since the shares are computed and reconstructed by using only linear algebra [18], it is also an example of *linear secret sharing schemes* (LSSS). Ito et al. [16] introduced secret sharing schemes for general access structures. Moreover, an LSSS can be constructed for any access structure [17]. However, the shares grow

[*]Department of Mathematics, Gebze Technical University, Turkey (stutdere@gmail.com) This paper was presented at the conference Arithmetic, Geometry, Cryptography and Coding Theory (AGCT-15.)

[†]Mathematical and Computational Sciences Labs, TÜBİTAK BİLGEM, Turkey (osmanbey.uzunkol@tubitak.gov.tr)

exponentially in the number of parties, and the optimization of secret sharing schemes for arbitrary access structures is a difficult problem [3].

Chen and Cramer [6] introduced an LSSS defined over a finite field using algebraic-geometry codes (AG-codes). Unlike the general case, this scheme has the advantage that shares are much smaller than the number of parties since one uses algebraic curves with many rational points. Therefore, this achieves larger information rate by generalizing Shamir's secret sharing scheme into an algebra-geometric setting. One inevitable disadvantage (due to the bounds on MDC [6]) is that this scheme is an ideal *ramp secret sharing scheme, i.e. a quasi-threshold scheme*. In particular, one has the property that the scheme has t-rejecting and $t + 1 + 2g$-accepting structure, where g is the genus of the underlying maximal algebraic curve.

Cascudo, Cramer, and Xing [4] introduced *arithmetic secret sharing schemes* which are special quasi-threshold $\mathbb{F}_q$-linear secret sharing schemes based on AG-codes. They can be used as the main algorithmic primitives in realizing information theoretically secure multi-party computation schemes (in particular, communication-efficient two-party cryptography) and verifiable secret sharing schemes [5, 7]. More precisely, it is shown in [6] that *asymptotically good* arithmetic secret sharing schemes can be used to achieve constant-rate communication in secure two-party communication by removing logarithmic terms which appears if one instead uses Shamir's secret sharing scheme [21]. As argued in [4], these schemes can be also used as an important primitive in plenty of other useful applications in cryptography including zero-knowledge for circuit satisfiability [14] and efficient oblivous transfers [15].

Constructing asymptotically good arithmetic secret sharing schemes is based on some special families of algebraic function fields. Besides the well-known notion of *Ihara limits* for constructing asymptotically good function field towers, the notion *torsion limits* for algebraic function fields is introduced in [4]. Geometrically, in order to construct arithmetic secret sharing schemes with asymptotically good properties, we need not only to have algebraic curves with many rational points but also to have jacobians (of corresponding algebraic curves) having comparably small d-torsion subgroups. On the algebraic side, the torsion limit for a function field tower with a given Ihara limit gives information on the size of $d-$torsion subgroups of the corresponding degree-zero divisor class groups. In [4], the authors give asymptotical results improving the classical bounds of Weil [26] on the size of torsion subgroups of abelian varieties over finite fields. For this purpose, the existence of solutions for certain Riemann-Roch systems of equations is investigated. The authors further give new bounds on the torsion limits of certain families of function fields. Consequently, they use these bounds in constructing asymptotically good arithmetic secret-sharing schemes by weakening the lower bound condition on the Ihara constant.

In this work, we made some modifications and improvements on their results by using the bound on class number given by [19]. Moreover, we estimated the torsion limit of an important class of towers of function fields introduced by

Bassa et al. depending on the Ihara limit given in [2]. For example for the case $d > 2$, these new bounds can easily be adapted to improve the communication complexity of zero knowledge protocols for multiplicative relations introduced in [8].

In Section 2 we revisit the preliminaries about algebraic function fields together with algebraic-geometry codes and Riemann-Roch systems of equations. We further investigate the bounds on the torsion limits in Section 2. Then, we apply the result for the bounds on the torsion limits for function field towers in Section 3. In Section 4 new conditions for the construction of arithmetic schemes are investifated and the results are proven. We construct families of arithmetic secret sharing schemes with uniformity in Section 5. Moreover, we give examples yielding to infinite families of arithmetic secret sharing schemes in Section 5. Finally, Section 6 concludes the paper.

2 Preliminaries

Let $F/\mathbb{F}_q$ be a function field over the finite field $\mathbb{F}_q$ with q elements, where q is a power of a prime number p. We denote by $g := g(F)$ its genus, by $B_i(F)$ its number of places of degree i for any $i \in \mathbb{N}$, and by $\mathbb{P}(F)$ its set of rational places.

An asymptotically exact sequence of algebraic function fields $\mathcal{F} = F_{i\,i \geq 0}$ over a finite field $\mathbb{F}_q$ is a sequence of function fields such that for all $m \geq 1$ the following limit exists:

$$\beta_m(\mathcal{F}) = \lim_{i \to \infty} \frac{B_m(F_i)}{g_i}.$$

It is well-known that any tower of function fields over any finite field is an exact sequence, see for instance [11].

We will use the following notations frequently:

- A_n: The number of effective divisors of degree n, for $n \geq 1$.
- h_i: The class number of $F_i/\mathbb{F}_q$ for any family of function fields $\mathcal{F} = (F_i)_{i \geq 1}$.
- $\mathbb{P}^{(k)}(F)$: The set of places of $F/\mathbb{F}_q$ having degree $k \in \mathbb{N}$.
- $\log := \ln$.
- $CI(F) := \mathrm{Div}(F)/\mathrm{Prin}(F)$: The divisor class group of $F/\mathbb{F}_q$.
- $CI_s(F) := \{[D] \ : \deg D = s\}$, where $[D] \in CI(F)$ stands for the divisor class containing D.
- $\mathrm{Div}^0(F)$: The group of divisors of F with degree zero,

- $\mathcal{J}_F = \mathrm{Div}^0(F)/\mathrm{Prin}(F)$: The zero divisor class group of F with cardinality $|\mathcal{J}_F| = h(F)$, which is called the *class number*.
- $C(D,G)_L$: The image of the map $\phi : \mathcal{L}(G) \to \mathbb{F}_q^k \times \mathbb{F}_q^n$, $f \mapsto (f(Q_1), \cdots f(Q_k), f(P_1), \cdots f(P_n))$, where $\mathcal{L}(G)$ is the Riemann-Roch space of G, $k, n \in \mathbb{N}$, $n \geq k$, G is a divisor of F, $Q_1, \cdots, Q_k, P_1, \cdots P_n \in \mathbb{P}^{(1)}(F)$ are pairwise distinct $\mathbb{F}_q$-places with $D = \sum_{j=1}^{k} Q_j + \sum_{i=1}^{n} P_i$ and $\mathrm{supp}\, D \cap \mathrm{supp}\, G = \emptyset$.

For a positive integer r, let

$$\mathcal{J}_F[r] := \{[D] \in \mathcal{J}_F : r \cdot [D] = \mathcal{O}\}$$

be the r-torsion subgroup of $\mathcal{J}_F$, where $\mathcal{O}$ denotes the identity element of $\mathcal{J}_F$. For each family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \to \infty$, the limit

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

is called the *r-torsion limit* of the family $\mathcal{F}$. Let $a \in \mathbb{R}$ and $\mathfrak{F}$ be the set of families $\{\mathcal{F}\}$ of function fields over $\mathbb{F}_q$ such that in each family genus tends to infinity and the Ihara limit

$$A(\mathcal{F}) = \lim_{g(F) \to \infty} \frac{B_1(F)}{g(F)} \geq a \text{ for every } \mathcal{F} \in \mathfrak{F}.$$

Then the asymptotic quantity $J_r(q,a)$ is defined by

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

We note that we only consider the Ihara limit for function field families $\mathcal{F}$ for which this limit exists following the lines of [4, Remark 2.1].

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 $t \geq 1$, $d \geq 2$, C is t-disconnected, the d powering C^{*d} is an n-code for $\mathbb{F}_q^k$, and C^{*d} is r-reconstructing. For further details, the relation of these codes with $C(D,G)_L$, and the concept of uniformity we refer to [4, pp. 3873-3875].

Firstly, we investigate the bounds on torsion limits in the following theorem by combining the bounds in Theorems 2.3 and 2.4 of [4]:

Theorem 1. *Let $\mathbb{F}_q$ be a finite field of characteristic p. For any integer $r \geq 2$, set $J_r := J_r(q, A(q))$. Write r as $r = p^l r'$ for some $l \geq 0$ and a positive integer r' coprime to p. Let $c := \gcd(r', q-1)$ and $k := \frac{l\sqrt{q}}{\sqrt{q}+1}$.*

(i) If $r \mid q$ and q is a square, then $J_r \leq \frac{1}{\sqrt{q}+1} \log_q r$.

(ii) If $r \mid (q-1)$, then $J_r \leq 2 \log_q r$.

(iii) If $r \nmid (q-1)$ and, q is non-square or $c > p^k$, then $J_r \leq \log_q r$.

(iv) If $r \nmid q$, $r \nmid (q-1)$, q is a square, and $c \leq p^k$, then

$$J_r \leq \frac{l}{\sqrt{q}+1} \log_q p + \log_q(cr').$$

Proof. We give a complete proof by comparing the results of [4]:

(i) Applying [4, Theorem 2.4(ii)] with $r = p^l$ and $r' = c = 1$ we obtain the inequality

$$J_r \leq \frac{l}{\sqrt{q}+1} \log_q p.$$

(ii) This assertion is a direct consequence of [4, Theorems 2.3 and 2.4].

(iii) and (iv) When $r \nmid (q-1)$, [4, Theorem 2.3(ii)] yields to $J_r \leq \log_q r$. Furthermore, when q is a square, we obtain

$$J_r \leq \frac{l}{\sqrt{q}+1} log_q r, \tag{1}$$

by [4, Theorem 2.3(iii)]. Using [4, Theorem 2.4(ii)], also the following inequality holds:

$$J_r \leq \frac{l}{\sqrt{q}+1} log_q p + log_q(cr'). \tag{2}$$

Hence, by inequalities (1), (2), and substituting the value $r = p^l r'$, we get

$$\begin{aligned} A &:= \frac{l}{\sqrt{q}+1} log_q p + log_q(cr') - \log_q r \\ &= \frac{-l\sqrt{q}}{\sqrt{q}+1} \log_q p + \log_q c. \end{aligned}$$

Since $A \geq 0$ if and only if $c \geq p^k$, assertion (iv) follows.

□

We remark that for Theorem 1(iv) with $c < p^k$, [4, Theorem 2.4] gives a better upper bound on J_r than [4, Theorem 2.3].

Remark 1. *It is well-known from Weil [26] that for any function field $F/\mathbb{F}_q$ with genus g one has $|J_F[r]| \leq r^{2g}$, and hence Theorem 1(ii) always holds.*

The following definition and theorems will be used in the subsequent sections:

Definition 1. *Let $u \in \mathbb{N}$, $m_i \in \mathbb{Z} \setminus \{0\}$, and $Y_i \in Cl(F)$ for $i = 1, \ldots, u$. The Riemann-Roch system of equations in the indeterminate X is the system of equations*

$$\{\ell(m_i X + Y_i) = 0\}_{i=1}^{u} \tag{3}$$

determined by these data. A solution is some divisor class $[G] \in Cl(F)$ satisfying all equations when substituted for X.

Theorem 2. *[4, Theorem 3.2] Consider the Riemann-Roch system (3). For $i = 1, \ldots, u$ and $s \in \mathbb{Z}$, let*

$$d_i := \deg Y_i \quad \text{and} \quad r_i := m_i s + d_i.$$

If one has

$$h(F) > \sum_{i=1}^{u} A_{r_i} \cdot |J_F[m_i]|,$$

then the system (3) has a solution $[G] \in Cl_s(F)$.

Theorem 3. *[4, Theorem 4.11] Let $t \geq 1$, $d \geq 2$. Define $I^* := \{1, \ldots, n\}$. For $\emptyset \neq A \subset I^*$ define*

$$P_A := \sum_{j \in A} P_j \in Div(F).$$

Let further a canonical divisor $K \in Div(F)$ be given. If the system

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

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

3 Torsion-limits of towers

We begin with an application of Theorem 1 when q is a square:

Proposition 1. *Suppose that $q = p^k$ is a square (with $k \geq 1$ and p prime) and $r = p^l r'$ where $\gcd(r', p) = 1$. We set $c := \gcd(r', q-1)$ and $k := \frac{l\sqrt{q}}{\sqrt{q}+1}$. Then there exists a recursive tower of function fields $\mathcal{F}$ over $\mathbb{F}_q$ such that one has*

$$A(\mathcal{F}) \geq \sqrt{q} - 1 - B + J_r(\mathcal{F}),$$

where

$$B = \begin{cases} \frac{1}{\sqrt{q}+1} \log_q r & \text{if } r \mid q \\ 2 \log_q r & \text{if } r \nmid q \text{ but } r \mid (q-1) \\ log_q r & \text{if } r \nmid q, r \nmid (q-1),\ c \geq p^k \\ \frac{l}{\sqrt{q}+1} \log_q p + \log(cr') & \text{otherwise.} \end{cases}$$

Proof. We know from [10] that there exists a recursive tower of function fields $\mathcal{F}$ over $\mathbb{F}_q$ with $A(\mathcal{F}) = \sqrt{q} - 1$. As q is a square, the proof follows easily from Theorem 1.

□

We now need the following result of Bassa et al. [2]:

Theorem 4. *[2, Theorem 1.2] Let $n = 2m + 1 \geq 3$ be an integer and $q = p^n$ with a prime p. There exists a recursive tower of function fields $\mathcal{F}$ over $\mathbb{F}_q$ such that*

$$A(\mathcal{F}) \geq \frac{2(p^{m+1} - 1)}{p + 1 + \epsilon}, \text{ where } \epsilon = \frac{p-1}{p^m - 1}.$$

Next, the torsion limit of the tower given in Theorem 4 can be estimated by using the lower bound on the Ihara limit $A(\mathcal{F})$:

Proposition 2. *Let n and q be given as in Theorem 4. There exists a recursive tower of function fields $\mathcal{F}$ over $\mathbb{F}_q$ with the following properties:*

(i) If p is odd, then $A(\mathcal{F}) \geq A + J_2(\mathcal{F})$, where

$$A = \frac{2(p^{m+1} - 1)}{p + 1 + \epsilon} - 2\log_q 2 \text{ with } \epsilon = \frac{p-1}{p^m - 1}. \tag{4}$$

(ii) If p is even, then $A(\mathcal{F}) \geq A + \log_q 2 + J_2(\mathcal{F})$, where A is given as in Eqn. (4).

The proof of Proposition 2 is obvious; it follows from Theorems 1 and 4, and Remark 1.

4 New conditions for the construction of arithmetic secret sharing schemes

For an algebraic function field $F/\mathbb{F}_q$ with genus g, we set

$$\Delta := \{i \ : \ 1 \leq i \leq g - 1 \text{ and } B_i \geq 1\} \quad \text{with } \delta := |\Delta|, \tag{5}$$

fix an integer $n \geq 0$, and further set

$$U_n := \{b = (b_i)_{i \in \Delta} \ : \ b_i \geq 0 \text{ and } \sum_{i \in \Delta} i \cdot b_i = n\}. \tag{6}$$

It is well-known that the number of effective divisors of degree n of an algebraic function field $F/\mathbb{F}_q$ is given as follows:

$$A_n = \sum_{b \in U_n} \left[\prod_{i \in \Delta} \binom{B_i + b_i - 1}{b_i} \right],$$

see for instance [1]. By combining this formula for A_n with some results of [4] and the bound on class number given in [19] we obtained the following theorem. This improves the sufficient conditions on the existence of arithmetic secret sharing schemes with uniformity:

Theorem 5. *Let $F/\mathbb{F}_q$ be a function field of genus g, $d, k, t, n \in \mathbb{N}$ with $d \geq 2$, $n > 1$, and $1 \leq t < n$. Let $1 \leq m \leq g-1$ be given such that $B_m \geq B_i$ for all $i \in \{1, \dots, g-1\}$. Moreover, set $f := \lfloor \frac{g-1}{m} \rfloor$. Suppose that $Q_1, Q_2, \dots, Q_k, P_1, P_2, \dots, P_n \in \mathbb{P}^{(1)}(F)$ are pairwise distinct rational places and*

$$d^{2g} \leq \frac{H - 2g\sqrt{q} - q - 1}{\binom{B_m+f}{f}^{\delta}}, \tag{7}$$

where

$$H := \frac{q^{g-1} \cdot (q-1)^2}{(q+1) \cdot (g+1)}$$

and δ is given as in (5). Assume further that there exists an element $s \in \mathbb{Z}$ such that

$$2g - s + t + k - 2 = 1 \quad \text{and} \quad 1 \leq ds - n + t \leq g - 1. \tag{8}$$

Then there exists an $(n, t, d, n-t)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity.

Proof. We first note that $|J_F[d]| \leq d^{2g}$ by Remark 1. Let A be a subset of $\{1, 2, \dots, n\}$ with t elements, and

$$P_A := \sum_{i \in A} P_i, \; Q := \sum_{i=1}^{k} Q_i, \; \text{ and } \; D := Q + \sum_{i=1}^{n} P_i$$

be divisors of $F/\mathbb{F}_q$. Let K be a canonical divisor of $F/\mathbb{F}_q$. Consider the following system of Riemann-Roch equations:

$$\{\ell(dX - D + P_A + Q) = 0, \ell(K - X + P_A + Q) = 0\}. \tag{9}$$

We apply Theorems 2 and 3 with

$$r_1 = 2g - s + t + k - 2, \; r_2 = ds - n + t, \; m_1 = -1, \; m_2 = d,$$

and an $s \in \mathbb{Z}$ satisfying that $r_i := m_i s + d_i$ for $i = 1, 2$. Hence, it is enough to show that

$$h = h(F) > A_{r_1} \cdot |\mathcal{J}_F[m_1]| + A_{r_2} \cdot |\mathcal{J}_F[m_2]|.$$

This guarantees that there exists a solution $G \in Div(F)$ of (9) with $deg(G) = s$. Again by Theorems 2 and 3, this solution yields to an AG-code $C(G, D)_L \subseteq \mathbb{F}_q^k \times \mathbb{F}_q^n$ which is an $(n, t, d, n-t)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity. We now set

$$H := \frac{q^{g-1}(q-1)^2}{(q+1)(g+1)}.$$

It follows from [19] that $h \geq H$. We set $u_j := |U_{r_j}|$, with U_{r_j} as in (6), for $j = 1, 2$. Let $m \in \Delta$ such that

$$\binom{B_m + \lfloor \frac{g-1}{m} \rfloor}{\lfloor \frac{g-1}{m} \rfloor} := \max \Big\{ \binom{B_i + \lfloor \frac{g-1}{i} \rfloor}{\lfloor \frac{g-1}{i} \rfloor} | \, i \in \Delta \Big\}. \tag{10}$$

Note that $r_1 = 1$ implies $A_{r_1} = A_1 = B_1$. We obtain the following inequality by using the bound on A_{r_2} given in [1, Theorem 3.5]:

$$\begin{aligned} A_{r_1} + A_{r_2} \cdot J_F[d] &\leq B_1 + \prod_{i \in \Delta} \binom{B_i + \lfloor \frac{g-1}{i} \rfloor}{\lfloor \frac{g-1}{i} \rfloor} \cdot |\mathcal{J}_F[d]| \\ &\leq B_1 + \binom{B_m + f}{f}^{\delta} \cdot |\mathcal{J}_F[d]| \\ &\leq B_1 + \binom{B_m + f}{f}^{\delta} \cdot d^{2g} \\ &\leq H. \end{aligned} \tag{11}$$

Hence, Inequality (11) holds by the assumption (7) due to Hasse-Weil bound [22]. □

Firstly, we give an estimatition for A_n. Our aim is to estimate the cardinality of U_n. We know that the partitions of a number n is correspond to the set of solutions $(j_1, j_2, ..., j_n)$ to the Diophantine equation

$$1j_1 + 2j_2 + 3j_3 + ... + nj_n = n.$$

For example, two distinct partitions of 4 can be given by $(1, 1, 1, 1)$, $(1, 1, 2)$ corresponding to the solutions $(j_1, j_2, j_3, j_4) = (4, 0, 0, 0)$, $(2, 1, 0, 0)$, respectively. To compute $|U_n|$, we need to find the number of partitions $p(n, \delta)$ of n into at most δ partitions, where $\delta = |\Delta|$. It follows from [12, p.9] that $p(n, \delta) = p_\delta(n + \delta)$, where $p_\delta(n + \delta)$ is defined to be the number of partitions of $n + \delta$ into exactly δ partitions. Each δ parts must contain at least 1 item. Thus, it remains n which needs to be distribute into the δ parts. It is enough to choose how many to put in the first $\delta - 1$ parts, since the number going into the last part is fixed. Hence, there are $\delta - 1$ choices, within the range $[0, n]$. This means we have $n + 1$ choices. Therefore,

$$p_\delta(n + \delta) \leq (n + 1)^{\delta - 1}. \tag{12}$$

Theorem 6. *Let $F/\mathbb{F}_q$ be a function field, $d, k, t, n \in \mathbb{N}$ with $d \geq 2$, $n > 1$, and $1 \leq t < n$. Let $1 \leq m \leq g - 1$, be such that $B_m \geq B_i$ for all $i \in \{1, \ldots, g - 1\}$. Suppose that $Q_1, Q_2, \ldots, Q_k, P_1, P_2, \ldots, P_n \in \mathbb{P}^{(1)}(F)$ are pairwise distinct rational places and*

$$d^{2g} \leq \frac{H - B_1}{(r_2 + 1)^{\delta - 1} \cdot \left(e \cdot \left(1 + \frac{r_2 - 1}{B_m - 1} \right)^{r_2} \right)^{\delta}}, \tag{13}$$

where

$$H := \frac{q^{g-1}\cdot(q-1)^2}{(q+1)\cdot(g+1)}$$

and δ is given as in (5). Assume further that there exists an $s\in\mathbb{Z}$ such that

$$2g-s+t+k-2=1 \qquad \textit{and} \qquad ds-n+t\geq 1.$$

Then there exists an $(n,t,d,n-t)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity.

Proof. The proof is similar to that of Theorem 5. The main difference is that instead of (refmax) we the bound (14) for binomial coefficients. Note that $b_i\leq n$ for all $i\in\Delta$. By applying induction on n the following inequality can be proven:

$$\begin{aligned}\binom{B_m+n-1}{n} &= \binom{B_m+n-1}{B_m-1} \\ &\leq \left(\frac{e\cdot(B_m+n-1)}{n}\right)^n.\end{aligned} \tag{14}$$

Hence, by using (12) with $n=r_2$ and (14) and definition of A_n, we obtain that

$$\begin{aligned} A_{r_1}+A_{r_2}\cdot J_F[d] &\leq B_1+\sum_{b\in U_{r_2}}\prod_{i\in\Delta}\binom{B_i+b_i-1}{B_i-1}\cdot|\mathcal{J}_F[d]| \\ &\leq B_1+\sum_{b\in U_{r_2}}\binom{B_m+n-1}{B_m-1}^{\delta}\cdot|\mathcal{J}_F[d]| \\ &\leq B_1+(n+1)^{\delta-1}\binom{B_m+n-1}{B_m-1}^{\delta}\cdot d^{2g} \\ &= B_1+\frac{[(n+1)\binom{B_m+n-1}{B_m-1}]^{\delta}}{n+1}\cdot d^{2g} \\ &= B_1+\frac{((n+1)e(1+\frac{n-1}{B_m-1})^n)^{\delta}}{n+1}\cdot d^{2g} \\ &\leq H.\end{aligned}$$

This inequality holds by Assumption (13). □

5 Construction of families of schemes with uniformity

We now consider exact sequences of function fields over finite fields. The sufficient conditions on the existence of families of arithmetic secret sharing schemes with uniformity [4, Theorems 4.15 and 4.16] can be given by imposing certain conditions on the sequences of $\mathcal{F}=\{F_i/\mathbb{F}_q\}_{i\geq 1}$ of function fields. We first need the following results:

Proposition 3. *[25, Corollary 2] Let $\mathcal{F} = \{F_i\}_{i\geq 0}$ be an exact sequence of function fields over a finite field $\mathbb{F}_q$. Then the following limit exists:*

$$h(\mathcal{F}) := \lim_{i\to\infty} \frac{\log h_i}{g_i}.$$

Theorem 7. *[25, Theorem 6] The following limit exists for an asymptotically exact family of function fields $\mathcal{F}$ over any finite field $\mathbb{F}_q$:*

$$\Delta(\mu) := \lim_{i\to\infty} \frac{A_{n_i}}{g_i},$$

where $n_i := \lfloor \mu g_i \rfloor$ and $\mu \in \mathbb{R}^{\geq 0}$. Moreover, for

$$\mu_0 := \sum_{m=1}^{\infty} \frac{m\beta_m(\mathcal{F})}{q^m - 1} \quad \text{and} \quad \mu \geq \mu_0 \tag{15}$$

we have

$$\Delta(\mu) = h(\mathcal{F}) - (1-\mu)\cdot \log q.$$

The main result concerning exact sequences of function fields and good artihmetic secret sharing schemes is given with the following theorem.

Theorem 8. *Let $d \geq 2$ be a positive integer and $\mathcal{F} = \{F_i\}_{i\geq 0}$ be an asymptotically exact family of function fields over $\mathbb{F}_q$. Let further μ be given as in Condition (15). For any $n_i, k_i \in \mathbb{N}$, with $i \geq 0$, suppose that the following assertions hold:*

(i) $J_d(\mathcal{F}) \leq (1-\mu)\log q$,

(ii) $B_1(F_i) \geq n_i + k_i$.

Then there exist $t_i \in \mathbb{N}$ depending on n_i satisfying $1 \leq t_i < n_i$, and an infinite family of $\{(n_i, t_i, d, n_i - t_i)\}_{i\geq 0}$ arithmetic secret sharing schemes for $\mathbb{F}_q^{k_i}$ over $\mathbb{F}_q$ with uniformity.

Proof. For a fixed $i \geq 0$ let

$$Q_{i,1}, Q_{i,2}, \ldots, Q_{i,k}, P_{i,1}, P_{i,2}, \ldots, P_{i,n_i}$$

be distinct rational places of $F_i/\mathbb{F}_q$. For simplicity we write $k := k_i$, $n := n_i$, and $t := t_i$. Assume that $I = \{1, 2, \ldots n_i\}$ and $A \subseteq I$ with $|A| = t$. Define

$$P_{i,A} := \sum_{j\in A} P_{i,j} \in Div(F_i) \text{ and } Q_i := \sum_{j=1}^{k} Q_{i,j} \in Div(F_i).$$

Let $K_i \in Div(F_i)$ be a canonical divisor of $F_i/\mathbb{F}_q$ and

$$D_i := Q_i + \sum_{j=1}^{n} P_{i,j} \in Div(F_i).$$

By [4, Theorem 4.11] it is enough to show that the system of Riemann-Roch equations

$$\begin{aligned} \ell(K_i - X + P_{i,A} + Q_i) &= 0, \\ \ell(dX - D_i + P_{i,A} + Q_i) &= 0 \end{aligned} \tag{16}$$

has a solution $G_i \in Div(F_i)$ such that $\deg G_i = s_i$ so that the AG-code $C(G_i, D)_L \subseteq \mathbb{F}_q^k \times \mathbb{F}_q^n$ is an $(n, t, d, n-t)$ arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with uniformity. We have the property that

$$d_{1,i} := 2g_i + t_i + k - 2 = \deg(K_i + P_{i,A} + Q_i) \text{ and}$$

$$d_{2,i} := t_i - n_i = \deg(-D_i + P_{i,A} + Q_i).$$

Notice that $A_1(F_i) = B_1(F_i)$ and $|J_{F_i}[-1]| = 1$. We set $h_i := h(F_i)$ for all $i \geq 1$. We now apply Theorems 2 and 3 with $m_1 = -1$, $m_2 = d$, and choose $s_i \in \mathbb{Z}$ so that

$$r_{1,i} := m_1 + d_{1,i} = 2g_i - s_i + t_i + k - 2 = 1 \text{ and}$$

$$r_{2,i} := m_2 s_i + d_{2,i} = ds_i - n_i + t_i = \lfloor \mu g_i \rfloor \geq 1.$$

This implies that if

$$h_i \geq 2A_{r_2}(F_i)|J_{F_i}[d]| > B_1(F_i) + A_{r_2}(F_i)|J_{F_i}[d]| \tag{17}$$

holds, then the system of equations (9) has a desired solution $G_i \in Div(F_i)$. To finish the proof, we need to verify Inequality (17). Taking $\log_q$ of both sides of (17) and dividing them by g_i yield to

$$\frac{\log_q h_i}{g_i} \geq \frac{\log_q 2}{g_i} + \log_q \frac{A_{r_2}(F_i)}{g_i} + \frac{\log_q |J_{F_i}[d]|}{g_i}. \tag{18}$$

Since the sequence $\mathcal{F} = \{F_i\}_{i \geq 0}$ is exact, it follows from Proposition 3 and Theorem 7 that taking limit infimum of both sides of Inequality (18) gives that

$$\begin{aligned} h(\mathcal{F}) &= \lim_{i \to \infty} \frac{\log_q h_i}{g_i} \\ &\geq \lim_{i \to \infty} \frac{\log_q A_{r_{2,i}(F_i)}}{g_i} + \liminf_{i \to \infty} \frac{\log_q |J_{F_i}[d]|}{g_i} \\ &= \Delta(\mu) + J_d(\mathcal{F}). \end{aligned} \tag{19}$$

We know from [24, Proposition 4.1] that the following inequality holds:

$$\begin{aligned} \Delta(\mu) = \liminf_{i \to \infty} \frac{\log A_{r_{2,i}}}{g_i} &= \mu \log q + \sum_{m=1}^{\infty} \beta_m \log \frac{q^m}{q^m - 1} \\ &\geq \mu \log q. \end{aligned} \tag{20}$$

Now it follows from Theorem 7 and Assertion (ii) that Equation (19) holds, which implies that Inequality (17) holds for sufficiently large i. □

Remark 2. *Suppose that q is a square. Then there are many function field towers $\mathcal{F} = \{F_i\}_{i\geq 0}$ over $\mathbb{F}_q$ with*

$$\beta_1(\mathcal{F}) = A(\mathcal{F}) = \sqrt{q} - 1 \ \text{ and}$$

$$\beta_i(\mathcal{F}) = \lim_{i\to\infty} \frac{B_i(F_i)}{g_i} = 0 \ \text{ for all } \ i \neq 1,$$

see for instance [10]. Moreover, we know from [25, Corollary 2] that for any asymptotically exact sequence $\mathcal{F} = \{F_i\}_{i\geq 0}$ of function fields (which includes towers), the following equality holds:

$$\lim_{i\to\infty} \frac{\log h_i}{g_i} = \log q + \sum_{i=1}^{\infty} \beta_i(\mathcal{F}) \log\big(\frac{q^i}{q^i - 1}\big).$$

By Remark 2 and Theorem 8, we obtain:

Proposition 4. *Suppose that q is a square and $d \geq 2$ is a positive integer. Let further μ be given as in Condition (15). There exists a tower $\mathcal{F} = \{F_i\}_{i\geq 0}$ of function fields over $\mathbb{F}_q$ with $n_i, k_i \in \mathbb{N}$ such that the following conditions hold:*

(i) $\mu + J_d(\mathcal{F}) \leq \sqrt{q} + (\sqrt{q} - 1)\log\big(\frac{q-1}{q}\big)$,

(ii) $B_1(F_i) \geq n_i + k_i$ *for sufficiently large i.*

An immediate consequence of Proposition 4 is the following corollary whose proof follows from Remark 2, and is similar to that of Theorem 8:

Corollary 1. *Suppose that q is a square and $d, k_i, n_i \in \mathbb{N}$ with $d \geq 2$. Then there exist $t_i \in \mathbb{N}$ depending on n_i satisfying $1 \leq t_i < n_i$, and an infinite family of $\{(n_i, t_i, d, n_i - t_i)\}_{i\geq 0}$ arithmetic secret sharing schemes for $\mathbb{F}_q^{k_i}$ over $\mathbb{F}_q$ with uniformity.*

Example 1. *Let $q = \ell^2$, where ℓ is a prime power. Consider the tower $\mathcal{F} = \{F_i\}_{i\geq 0}$ over $\mathbb{F}_q$ defined by the equation*

$$f(x, y) = y^\ell x^{\ell-1} + y - x^\ell \in \mathbb{F}_q[x, y].$$

This tower is optimal [10], i.e. $\beta_1(\mathcal{F}) = \ell - 1$ and $\beta_i(\mathcal{F}) = 0$ for all $i \geq 2$. Thus, the value of μ_0 defined in Condition (15) is

$$\mu_0 = \frac{1}{\ell + 1}.$$

Choose $\mu = \mu_0$, $d = 2$. By[10, Theorem 2.10] we have

$$g(F_i) = \begin{cases} (q+1)q^i - (q+2)q^{i/2} + 1 & \text{if } i \text{ is even} \\ (q+1)q^i - \frac{1}{2}(q^2 + 3q + 2)q^{(i-1)/2} + 1 & \text{if } i \text{ is odd.} \end{cases}$$

Moreover, by [10, Proposition 3.1], we have

$$B_1(F_i) \geq (q-1)\ell^i + 2\ell \quad \text{for all } i \geq 4.$$

For each $i \geq 4$ we choose $n_i, k_i \in \mathbb{N}$ in such a way that $B_1 \geq n_i + k_i$. Then Proposition 4 is satisfied by Theorem 1. Therefore, the tower $\mathcal{F}$ can be used to construct an infinite family of $\{(n_i, t_i, d, n_i - t_i)\}_{i\geq 0}$ arithmetic secret sharing schemes for $\mathbb{F}_{\ell^2}^{k_i}$ over $\mathbb{F}_{\ell^2}$ with uniformity.

Example 2. *Consider the example from [1, Proposition 5.20]. Let $\mathcal{F} = \{F_i\}_{i\geq 0}$ be the tower over $\mathbb{F}_9$ defined by the polynomial*

$$f(X,Y) = Y^2 + (X+b)^2 - 1 \in \mathbb{F}_9[X,Y], b \in \mathbb{F}_3^* \tag{21}$$

and $F_0 = \mathbb{F}_9(x_0)$ be the rational function field. Let $E = F_0(z)$ with z is a root of the polynomial

$$\varphi(T) = (T^2 + \alpha^7)(T^9 - T) - \frac{1}{x_0} \in F_0[T],$$

where α is a primitive element for $\mathbb{F}_9$. Then the sequence $\mathcal{E} = \{E_i\}_{i\geq 0}$, with $E_i := EF_i$, over $\mathbb{F}_9$ is a composite quadratic tower such that for all $i \geq 0$,

(i) $B_1(E_i) \geq 9 \cdot 2^i$ *and* $B_2(E_i) \geq 2^i$,

(ii)
$$g_i = \begin{cases} 21 \cdot 2^{i-1} - 33 \cdot 2^{(i-2)/2} + 6 & \text{if } i \equiv 0 \bmod 2, \\ 21 \cdot 2^{i-1} - 11 \cdot 2^{(i+1)/2} + 6 & \text{if } i \equiv 1 \bmod 2, \end{cases}$$

where $g_i = g(E_i)$.

(iii) $\beta_1(\mathcal{E}) = \frac{6}{7}$, $\beta_2(\mathcal{E}) = \frac{2}{21}$ *and* $\beta_j(\mathcal{E}) = 0$ *for all* $j \geq 3$.

Thus, the value of μ_0 defined in Condition (15) is

$$\mu_0 = \frac{23}{210} \approx 0.12.$$

Choose $\mu = 0.5 \geq \mu_0$ and for simplicity choose $k_i = 2, t_i = 50$ for all $i = 1, 2, 3, 4$. From the proof of Theorem 1 we obtain

$$r_{1,i} = 1, \ r_{2,1} = 2, \ r_{2,2} = 7, \ r_{2,3} = 23, \ r_{2,4} = 54$$

for all $d = 2, 3, 4, 5$. We now have the following table by using the relations given in the proof of Theorem 1:

$$s_i = 2g_i + t + k - 3 \ \text{ and } \ n_i = ds_i + t - r_{2,i} \text{ for } i = 1, 2, 3, 4.$$

Table 1: Some parameters of Example 2

d	$j_d \leq$	n_1	n_2	n_3	n_4
2	0.8	166	201	309	525
3	0.8	225	280	450	791
4	0.8	288	363	595	1060
5	0.2	343	438	732	1321

Notice that for $d = 2, 3, 4, 5$ and $q = 9$ we have

$$J_d(\mathcal{E}) \leq \sqrt{q} + (\sqrt{q} - 1) \log\big(\frac{q-1}{q}\big) - \mu \approx 1.9.$$

6 Conclusion

In this work some bounds [4] on the construction of arithmetic secret sharing schemes are improved by using bounds on class number [19]. We here estimated the torsion limit of an important class of towers of function fields [2] depending on the Ihara limit. In the case $d \geq 2$, these new bounds can easily be adapted to improve several applications of torsion limits ranging from improving the communication complexity of zero knowledge protocols for multiplicative relations [8] and bilinear complexity of finite field multiplication to obtain new results on the asymptotics of frameproof codes.

Acknowledgment

We thank Mehmet Sabır Kiraz for his comments during the preparation of this research. O. Uzunkol is partly supported by a research project funded by Bundesministerium für Bildung und Forschung (BMBF), Germany (01DL12038) and TÜBİTAK, Turkey (TBAG-112T011). Uzunkol's research is also partially supported by the project (114C027) funded by EU FP7-The Marie Curie Action and TÜBİTAK (2236-CO-FUNDED Brain Circulation Scheme).

References

[1] Ballet, S., Rolland, R., and Tutdere, S.: Lower Bounds on the Number of Rational Points of Jacobians over Finite Fields and Application to Algebraic Function Fields in Towers, preprint arXiv:1303.5822.

[2] Bassa, A., Beelen P., Garcia, A., and Stichtenoth, H.: Towers of Function Fields over Non-Prime Finite Fields, Moscow Math J. 15(1), 1–29, (2015).

[3] Beimel A., Secret-Sharing Schemes: A Survey, IWCC 2011, LNCS 6639, 11–46, Springer Verlag, (2011).

[4] Cascudo, I., Cramer, R., and Xing, C.: Torsion Limits and Riemann-Roch Systems for Function Fields and Applications, IEEE Transactions on Information Theory, 60(7): 3871–3888, (2012).

[5] Chaum, D., Crépeau, C., Damgaard, I.: Multi-Party Unconditionally Secure Protocols, Proceedings of STOC 1988, ACM Press, New York 11–19, (1988).

[6] Chen, H. and Cramer, R.: Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields, CRYPTO 2006. LNCS, Springer, Heidelberg, 4117, 516-531, (2006).

[7] Cramer, R., Damgaard, I., Maurer, U.: General Secure Multi-Party Computation from any Linear Secret Sharing Scheme. EUROCRYPT 2000, LNCS 1807, Springer, Heidelberg 316–334, (2000).

[8] Cramer, R., Damgaard, I., Pastro, V.: On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations, ICITS'12 Proceedings of the 6th international conference on Information Theoretic Security, 62–79, (2012).

[9] Farràs O., Padró C., Xing C., and Yang A.: Natural Generalizations of Threshold Secret Sharing, IEEE Tran. on Information Theory 60, No. 3, 1652–1664, (2014).

[10] Garcia, A., and Stichtenoth, H.: A Tower of Artin-Schreier Extensions of Function Fields Attaining the Drinfeld-Vladut Bound, Invent Math, 121, 211–222, (1995).

[11] Hess, F., Stichtenoth, H., and Tutdere, S.: On Invariants of Towers of Function Fields over Finite Fields, J. of Algebra and Its Appl, 12(4), (2013).

[12] Gupta, H.: Partitions A Survey, Journal of Res. of Nat. Bur. Standards-B Math. Sciences B 74, 1–29, (1970).

[13] Ignatenko, T., and Willems F. M. J.: Biometric Systems: Privacy and Secrecy Aspects, IEEE Trans. Inf. Forensics Security, 4(4), 956–973, (2009).

[14] Ishai, Y., Kushilevitz, E., Ostrovsky, R., Sahai, A.: Zero-Knowledge from Secure Multi-Party Computation, Proceedings of 39th STOC, San Diego, Ca., USA, 21–30, (2007).

[15] Ishai, Y., Prabhakaran, M., Sahai, A.: Founding Cryptography on Oblivious Transfer-Efficiently, CRYPTO 2008, LNCS 157, Springer, Heidelberg, 572–591, (2008).

[16] Ito, M., Saito, A., Nishizeki, T.: Multiple Assignment Scheme for Sharing Secret, Journal of Cryptology, 6(1), 15–20, (1993).

[17] Ito, M., Saito, A., Nishizeki, T.: Secret Sharing Scheme Realizing any Access Structure, in Proc. IEEE Globecom, 99–102, (1987).

[18] Karnin E. D., Greene J. W., and Hellman M. E: On Secret Sharing Systems, IEEE Trans. Inf. Theory, 29(1), 35–41, (1983).

[19] Lachaud, G. and Martin-Deschamps, M.: Nombre de points des jacobiennes sur un corps finis, Acta Arithmetica, 56(4), 329-340, (1990).

[20] Naor, M., Wool, A.: Access Control and Signatures via Quorum Secret Sharing, IEEE Transactions on Parallel and Distributed Systems 9(1), 909–922, (1998).

[21] Shamir, A.: How to Share a Secret, Comm. of the ACM 22(11), 612–613, (1979).

[22] Stichtenoth, H.: Algebraic Function Fields and Codes, 2nd Ed. Springer-Verlag 254, (2009).

[23] Tassa, T.: Generalized Oblivious Transfer by Secret Sharing, Designs, Codes and Cryptography 58(1), 11–21, (2011).

[24] Tsfasman, M. A. and Vladut, S.G.: Asymptotic Properties of Zeta-Functions, Journal of Mathematical Sciences, 84(5), 1445–1467, (1997).

[25] Tsfasman, M. A.: Some Remarks on The Asymptotic Number of Points, Coding Theory and Algebraic Geometry, Lecture Notes in Mathematics Springer Berlin Heidelberg, 178–192, (1992).

[26] Weil, A.: Vari*é*t*é*s Ab*é*liennes et Courbes Alg*é*briques. Hermann, Paris, (1948).