Hacettepe Journal of Mathematics & Statistics

Hacet. J. Math. Stat.
Volume 49 (2) (2020), 638 – 647
DOI : 10.15672/hujms.460348

Research Article

Construction of arithmetic secret sharing schemes by using torsion limits

Seher Tutdere*[1], Osmanbey Uzunkol[2,3]

[1] *Balıkesir University, Department of Mathematics, Altıeylül, 10145, Balıkesir*
[2] *FernUniversität in Hagen, Faculty of Mathematics and Computer Science, Germany*
[3] *Mathematical and Computational Sciences, TÜBİTAK BİLGEM, Turkey*

Abstract

Cascudo, Cramer, and Xing [Torsion limits and Riemann-Roch systems for function fields and applications, IEEE Trans. Inf. Theory, 2014] gave a construction of arithmetic secret sharing schemes by using the torsion limits of algebraic function fields and Riemann-Roch systems. In this work, we give some new conditions for the construction of arithmetic secret sharing schemes. Furthermore, we give new bounds on the torsion limits of certain towers of function fields over finite fields.

Mathematics Subject Classification (2010). 94A62, 11R58, 11T71

Keywords. algebraic function fields, torsion limits, arithmetic secret sharing schemes

1. Introduction

Secret sharing is a cryptographic mechanism allowing to distribute secret shares among different parties. This is achieved by a trusted dealer in such a way that only authorized subsets of the parties can determine the secret [3]. Secret sharing schemes have the advantage of enabling 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], oblivious transfers [23] to biometric authentication schemes [13].

The set of all subsets for a group of users authorized to access to some resources within a system is called its *access structure*. If the authorized subsets of a secret sharing scheme are exactly those sets whose cardinality is larger than a predetermined lower bound, then the secret sharing scheme is said to have a *threshold access structure* [10]. Moreover, a secret sharing scheme is called *ideal* if the shares have the same size as the 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 functions [18], it is also an example of a *linear secret sharing scheme* (LSSS). Moreover, an LSSS can be constructed for any access structure [17] following the notion of general access structures introduced in Ito *et al.* [16]. However, the shares grow exponentially in the number of parties, and the optimization of secret sharing schemes for arbitrary access structures is a difficult problem [3].

*Corresponding Author.
Email addresses: stutdere@gmail.com (S. Tutdere), osmanbey.uzunkol@gmail.com (O. Uzunkol)
Received: 16.09.2018; Accepted: 08.02.2019

Chen and Cramer [8] 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 MDS codes [8]) 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 algebraic curve. For LSSS over finite fields, in [5], an upper bound on the limit of t is given in some cases.

Cascudo, Cramer, and Xing [4, 6] introduced the notion of *arithmetic secret sharing schemes* based on AG-codes which are special quasi-threshold $\mathbb{F}_q$-linear secret sharing schemes. They can be used as the main algorithmic primitives in realizing information theoretically secure multi-party computation schemes (in particular, communication-efficient secure two-party computations) and verifiable secret sharing schemes [7,9]. More precisely, it is shown in [8] 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 appear if one instead uses Shamir's secret sharing scheme [21]. As argued in [6], as an important primitive, these schemes can also be used in plenty of other useful applications in cryptography including zero-knowledge for circuit satisfiability [14] and efficient oblivious transfer [15].

Constructing asymptotically good arithmetic secret sharing schemes is based on some special sequences of algebraic function fields. Besides the well-known notion of *Ihara limits* for constructing asymptotically good towers of function fields, the notion *torsion limits* for algebraic function fields is introduced in [6]. 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 tower of function fields with a given Ihara limit gives information on the size of $d-$torsion subgroups of the corresponding degree-zero divisor class groups. In [6], the authors give asymptotical results improving the classical bounds of Weil [24] 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 sequences 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 $A(q)$.

Following the lines of [6], the contributions of this work are given as follows:

- We give a necessary condition on the asymptotic constructions of arithmetic secret sharings which is helpful for the security of the construction (i.e. how many adversaries it can tolerate) by using an important class of towers of function fields introduced by Bassa *et al.* depending on the Ihara limit given in [2].
- We then give a simplification of Theorem 2.2 [6, Corollary 4.12] in Theorems 4 and 5 under some conditions which eliminate not only the requirements of computing the class number h, but also the number of effective divisors with degree r_1, r_2 (A_{r_1}, A_{r_2}, resp.). These new conditions are much easier to verify for a given function field though making the results less general than [6]. For this purpose, we mainly use the bound on class number [19] and the bound on the number of effective divisors [1, Theorem 3.5]. In Theorem 2.2, one needs to know both the class number h and the values A_{r_1}, A_{r_2} of a given function field. In particular, our improvements imply that it is enough to know the genus g and the number of

places of degree $n \leq g-1$ (which are much easier to estimate) to obtain a sufficient condition.

In Section 2, we first introduce the preliminaries and notations. We then give definitions and some results regarding arithmetic-secret sharing schemes (based on AG-codes). We further investigate the bounds on the torsion limits in this section. In Section 3, we give an application of these bounds for a family of towers of function fields over finite fields introduced by Bassa *et al.* [2]. Finally, Section 4 concludes the paper with new conditions for the construction of arithmetic secret sharing schemes.

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 with $g_i := g(F_i) \to \infty$ 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 asymptotically exact sequence, see for instance [12].

Throughout this paper, we will use the following notations frequently:

- $F/\mathbb{F}_q$: A function field with full constant field $\mathbb{F}_q$.
- $A_n = A_n(F)$: The number of effective divisors of F with degree n, for $n \geq 1$. Set $A_n := 0$ for $n < 0$.
- $\mathbb{P}^{(k)}(F)$: The set of places of F with degree $k \in \mathbb{N}$.
- $\log := \ln$.
- $\mathrm{Div}(F)$: The group of divisors of F with $\mathrm{Div}(F) \supset \mathrm{Div}^0(F) \supset \mathrm{Princ}(F)$, where $\mathrm{Div}^0(F)$ denotes the group of divisors of F with degree zero and $\mathrm{Princ}(F)$ denotes the group of principal divisors of F.
- $\mathcal{J}_F = \mathrm{Div}^0(F)/\mathrm{Prin}(F)$: The zero divisor class group of F with cardinality $|\mathcal{J}_F| = h(F)$, which is called the *class number*.

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 sequences $\{\mathcal{F}\}$ 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

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

It is well-known that the Ihara constant is given by $A(q) = \limsup_{\mathcal{F}} A(\mathcal{F})$, where $\mathcal{F}$ runs over all infinite families of function fields over $\mathbb{F}_q$. We note that we here only consider asymptotically exact sequences of function fields over finite fields.

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. This means that the secret sharing scheme is linear with the secret in $\mathbb{F}_q^k$ for every share in $\mathbb{F}_q$ such that

- no set of $\leq t$ parties has any information about the secret,
- if d secrets are shared with the scheme, then for any set of r parties, the product of the d secrets is a linear function of the vector containing the products of the d shares which correspond to each party.

These schemes are secret sharing schemes with additional properties regarding the reconstruction of the product of d secrets given the local products of the respective shares. For further details and how such schemes may be constructed using function fields with many places of degree one, see [6]. The results of [6] can be divided into two main categories; results related to the asymptotic existence of arithmetic secret sharing schemes, and the conditions for the existence of arithmetic secret sharing schemes.

Firstly, we investigate the bounds on torsion limits, which are only related to the results in [6] on asymptotically good arithmetic secret sharing and will be revisited in Section 3, in the following theorem by combining the bounds in Theorems 2.3 and 2.4 of [6]:

Theorem 2.1. *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 $\gamma := \frac{l\sqrt{q}}{\sqrt{q}+1}$.*

(i) *For any r one has $J_r \leq 2\log_q r$.*
(ii) *If $r \mid q$ and q is a square, then $J_r \leq \frac{1}{\sqrt{q}+1}\log_q r$.*
(iii) *If $r \nmid (q-1)$ and, q is non-square or $c > p^\gamma$, then $J_r \leq \log_q r$.*
(iv) *If $r \nmid q$, $r \nmid (q-1)$, q is a square, and $c \leq p^\gamma$, 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 [6]:

(i) It is well-known from a result of Weil [24] that for any function field $F/\mathbb{F}_q$ with genus g one has $|\mathcal{J}_F[r]| \leq r^{2g}$, and hence assertion (i) always holds.

(ii) Applying [6, Theorem 2.4(ii)] with $r = p^l$ and $r' = c = 1$ we obtain the inequality

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

(iii) and (iv) When $r \nmid (q-1)$, [6, Theorem 2.3(ii)] yields to $J_r \leq \log_q r$. Furthermore, when q is a square, we obtain

$$J_r \leq \frac{l}{\sqrt{q}+1} log_q r, \tag{2.1}$$

by [6, Theorem 2.3(iii)]. Using [6, Theorem 2.4(ii)], also the following inequality holds:

$$J_r \leq \frac{l}{\sqrt{q}+1}\log_q p + \log_q(cr'). \tag{2.2}$$

Hence, by inequalities (2.1), (2.2), and substituting the value $r = p^l r'$, we get

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

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

□

We remark that for Theorem 2.1(iv) with $c < p^\gamma$, [6, Theorem 2.4] gives a better upper bound on J_r than [6, Theorem 2.3].

Secondly, we revisit the following theorem from [6] which is about the general conditions required for the existence of arithmetic secret sharing which will be improved in Section 4, under some conditions.

Theorem 2.2 ([6, 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 $Q_1, \ldots, Q_k, P_1, \ldots, P_n \in \mathbb{P}^{(k)}(F)$ are pairwise distinct. If there is an integer s such that*

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

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.

3. Torsion-limits of towers

For some cryptographic applications [6], one is interested in the families of function fields $\mathcal{F}$ with positive limit $A(\mathcal{F})$ and small torsion limit $J_r(\mathcal{F})$. To determine the torsion limit seems to be much harder than determining the Ihara limit. In [6, Theorem 2.6], it is proved that for all $q \geq 8$ except perhaps for $q = 11$ or 13, $A(\mathcal{F}) > 1 + J_2(\mathcal{F})$. We here give a discussion on these limits. We begin with an application of Theorem 2.1 when q is a square:

Proposition 3.1. *Suppose that $q = p^m$ is a square (with $m \geq 1$ and p prime) and $r = p^l r'$ where $\gcd(r', p) = 1$. We set $c := \gcd(r', q-1)$ and $\gamma := \frac{l\sqrt{q}}{\sqrt{q}+1}$. 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

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

Proof. We know from [11] 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 2.1. □

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

Theorem 3.2 ([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 3.2 can be estimated by using the lower bound on the Ihara limit $A(\mathcal{F})$:

Proposition 3.3. *Let n and q be given as in Theorem 3.2. 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*

$$A = \frac{2(p^{m+1}-1)}{p+1+\epsilon} - 2\log_q 2 \text{ with } \epsilon = \frac{p-1}{p^m-1}. \tag{3.1}$$

(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. (3.1).*

The proof of Proposition 3.3 is obvious; it follows from Theorems 2.1 and 3.2. Alternatively, the proposition follows from Theorem 3.2 and the fact that $J_2(F) \leq \log_q 2$ if $2 \mid q$ and $J_2(F) \leq 2\log_q 2$ if $2 \nmid q$, which is immediate since for any function field F of genus g one has $\mathcal{J}_F[2] \leq 2^{2g}$ in general, and $\mathcal{J}_F[2] \leq 2^g$ in case $char(F) = 2$.

Remark 3.4. More concretely, [6, Theorem 4.16] implies that parameters of the asymptotic constructions of arithmetic secret sharings improve depending on the ratio $A(\mathcal{F})/(1 + J(\mathcal{F}))$. In particular, a larger κ corresponding to the length of the secret and the τ corresponding to the security of the construction (how many adversaries it can tolerate) can be obtained by using Proposition 3.3.

4. New conditions for the construction of arithmetic secret sharing schemes

In this part, we give an improvement of [6, Corollary 4.12] under some conditions. Before this, we need the following: For an algebraic function field $F/\mathbb{F}_q$ with genus g, we set

$$\Delta := \{i \ : \ 1 \leq i \leq g-1 \text{ and } B_i \geq 1\} \quad \text{with } \delta := |\Delta|, \tag{4.1}$$

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

$$U_n := \{b = (b_i)_{i\in\Delta} \ : \ b_i \geq 0 \text{ and } \sum_{i\in\Delta} i \cdot b_i = n\}. \tag{4.2}$$

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:

$$A_n = \sum_{b\in U_n} \Big[\prod_{i\in\Delta} \binom{B_i + b_i - 1}{b_i} \Big], \tag{4.3}$$

see for instance [1]. By combining this formula for A_n with some results of [6] and the bound on class number given in [19] we obtain the following theorem. This improves the sufficient conditions on the existence of arithmetic secret sharing schemes with uniformity:

Theorem 4.1. *Let $F/\mathbb{F}_q$ be a function field of genus $g \geq 2$, $d, k, t, n \in \mathbb{N}$ with $d \geq 2$ and $1 \leq t < n$. Set*

$$M := \max\Big\{ \binom{B_i + \lfloor \frac{g-1}{i} \rfloor}{\lfloor \frac{g-1}{i} \rfloor} \Big| \ i \in \Delta \Big\}. \tag{4.4}$$

Suppose that $Q_1, \ldots, Q_k, P_1, \ldots, P_n \in \mathbb{P}^{(1)}(F)$ are pairwise distinct rational places and

$$H > \binom{n}{t} (2g\sqrt{q} + q + 1 + M^\delta \cdot d^{2g}), \tag{4.5}$$

where

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

and δ is given as in (4.1). Assume further that

$$1 \leq ds - n + t \leq g - 1, \tag{4.6}$$

where $s = 2g + t + k - 3$. 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 $|\mathcal{J}_F[d]| \leq d^{2g}$ by Theorem 2.1.

Choose an $s \in \mathbb{Z}$ such that

$$r_1 := 2g - s + t + k - 2 = 1,\ r_2 := ds - n + t.$$

Note that $r_1 = 1$ implies $A_{r_1} = A_1 = B_1$. Using the Hasse-Weil bound [22, Theorem 5.2.3] on B_1 and the bound on A_{r_2} given in [1, Theorem 3.5] one obtains

$$\begin{aligned}
\binom{n}{t}(A_{r_1} + A_{r_2}|\mathcal{J}_F[d]|) &\leq \binom{n}{t}\left(B_1 + \prod_{i\in\Delta}\binom{B_i + \lfloor\frac{g-1}{i}\rfloor}{\lfloor\frac{g-1}{i}\rfloor}|\mathcal{J}_F[d]|\right) \\
&\leq \binom{n}{t}(B_1 + M^\delta|\mathcal{J}_F[d]| \leq B_1 + M^\delta d^{2g}) \\
&\leq \binom{n}{t}(2g\sqrt{q} + q + 1 + M^\delta d^{2g}) \\
&< H \leq h,
\end{aligned}$$

by assumption (4.5) and the bound $H \leq h$ shown in [19]. Now by Theorem 2.2, the proof follows. □

We now give an example satisfying the conditions of Theorem 4.1. Note that the parameters in the following example satisfy the conditions in [6, Proposition 4.8].

Example 4.2. Let $q := 3^8$, $n = 9$, $d = t = 2$, $k = 1$, and $F := \mathbb{F}_q(x)$ be the rational function field over $\mathbb{F}_q$. Consider the extension field $E := F(y)$ of F where $y^2+x^6+x+1 = 0$. It has genus $g(E) = 2$ and $\Delta = \{1\}$, so $\delta = 1$. Using Magma[†], one obtains $B_1(F) = 6481$, hence $M = 6482$, and

$$H = \frac{2^9 \cdot 3^7 \cdot 5^2 \cdot 41^2}{17 \cdot 193} > 14342347.$$

Hence, H satisfies condition (4.5):

$$H \geq \binom{n}{t}(2g\sqrt{q} + q + 1 + M^\delta \cdot d^{2g}) = 3981528.$$

The condition (4.6) is clearly satisfied. Thus, by Theorem 4.1, we obtain an $(9, 2, 2, 7)$-arithmetic secret sharing scheme over $\mathbb{F}_{3^8}$ with uniformity. Note that $E/\mathbb{F}_q$ is a hyperelliptic function field.

Next, we give an estimation for the cardinality of U_n (see (4.2)), which will be used in Theorem 4.5. For this, 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 in summands 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. The cardinalities of the summands in the partition $(1, 1, 2)$ are $j_1 = 2$ and $j_2 = 1$. We now fix $\delta = |\Delta|$, as in (4.1). We need to count the number of partitions of n in summands whose cardinalities are in Δ. We choose the values $j_i's$ for the $\delta - 1$ largest indices i in Δ. Those indices are all at least 2 (notice that if $1 \in \Delta$, then it is necessarily the smallest index in Δ). Thus, each j_i is at most $n/2$, i.e., it is within the range $[0, \frac{n}{2}]$. This means, we have $\frac{n}{2} + 1$ choices for each j_i. Therefore, we have the following lemma:

Lemma 4.3. $|U_n| \leq \left(\frac{n}{2} + 1\right)^{\delta-1}$.

[†]Magma Computational Algebra System: Magma Online Calculator, available under http://magma.maths.usyd.edu.au/calc/

Remark 4.4. For the applications in arithmetic secret sharing schemes, it is highly desired to construct other examples with $q < n$ (i.e., improving Shamir's secret sharing scheme). In order to find such examples we need algebraic function fields for which B_1 is large, however, almost all B_i, $2 \leq i \leq g-1$, are zero so that Conditions (4.5) and (4.6) of Theorem 4.1 simultaneously hold. However, finding such examples may not be easy. For example, the function field $\mathbb{F}_3(x,y) \supset \mathbb{F}_3(x)$, with $y^3 - y - x^4 + x^2 = 0$, over $\mathbb{F}_3$ has genus $g = 3$ and $B_2 = 0$. Similarly, the function field $\mathbb{F}_5(x,y) \supset \mathbb{F}_5(x)$, with $(x^4-1)y^4+x^3y^3+3xy-x^4 = 0$, over $\mathbb{F}_5$ has $g = 4$ and $B_2 = 0$ (but $B_3 = 40$). When $B_e = 0$ with e a *prime* number would imply that the corresponding curve attains no new points over the extension $\mathbb{F}_q$ of degree e. For a fixed genus g and e prime, assuming $B_e = 0$ and comparing a Hasse-Weil lower bound over $\mathbb{F}_{q^e}$ to an upper bound over $\mathbb{F}_q$ yields

$$q^e - 2g\sqrt{q^e} \leq q + 2g\sqrt{q}.$$

For instance, for $g = 3$ (which makes $e = 2$ the only relevant case to consider) this leads to $q \leq 9$.

Theorem 4.5. *Let $F/\mathbb{F}_q$ be a function field, $d, k, t, n \in \mathbb{N}$ with $d \geq 2$ 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*

$$H > \binom{n}{t}\left(B_1 + \left(\frac{n}{2}+1\right)^{\delta-1}\left(\frac{e\cdot(B_m+n-1)}{n}\right)^{n\delta} d^{2g}\right) \tag{4.7}$$

where H is as in Theorem 4.1, δ is as in (4.1), and e is Euler's constant. Assume further that

$$ds - n + t \geq 1,$$

where $s = 2g + t + k - 3$. 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 4.1. The main difference is that instead of M, we use the assumption that $B_m \geq B_i$ and the bound (4.8) 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:

$$\begin{aligned}\binom{B_m+n-1}{n} &= \binom{B_m+n-1}{B_m-1} \\ &\leq \left(\frac{e\cdot(B_m+n-1)}{n}\right)^n.\end{aligned} \tag{4.8}$$

Hence, by applying Lemma 4.3 with $n = r_2$, using (4.3) and (4.8), we obtain that

$$\begin{aligned}A_1 + A_{r_2}|\mathcal{J}_F[d]| &= B_1 + \sum_{b\in U_n}\prod_{i\in\Delta}\binom{B_i+b_i-1}{B_i-1}|\mathcal{J}_F[d]| \\ &\leq B_1 + \sum_{b\in U_n}\binom{B_m+n-1}{B_m-1}^{\delta}|\mathcal{J}_F[d]| \\ &\leq B_1 + \left(\frac{n}{2}+1\right)^{\delta-1}\binom{B_m+n-1}{B_m-1}^{\delta} d^{2g} \\ &\leq B_1 + \left(\frac{n}{2}+1\right)^{\delta-1}\left(\frac{e(B_m+n-1)}{n}\right)^{n\delta} d^{2g}.\end{aligned}$$

Thus, the desired results follows by the assumption (4.7). □

Acknowledgment. We thank the referee for providing constructive suggestions which improve the presentation of the paper. Uzunkol's work was supported by the project (114C027) funded by EU FP7-The Marie Curie Action and TÜBİTAK (2236-CO-FUNDED Brain Circulation Scheme).

References

[1] S. Ballet, R. Rolland, and S. Tutdere, *Lower bounds on the number of rational points of Jacobians over finite fields and application to algebraic function fields in towers*, Moscow Math. J. **15** (3), 1–9, 2015.

[2] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth, *Towers of function fields over non-prime finite fields*, Moscow Math. J. **15** (1), 1–29, 2015.

[3] A. Beimel, *Secret-sharing schemes: A survey*, IWCC 2011: LNCS **6639** Springer Verlag: 11–46, 2011.

[4] I. Cascudo, R. Cramer, and C. Xing, *The torsion-limit for algebraic function fields and its application to arithmetic secret sharing*, CRYPTO 2011: LNCS **6841** Springer Verlag: 685–705, 2011.

[5] I. Cascudo, R. Cramer, and C. Xing, *Bounds on the threshold gap in secret sharing and its applications*, IEEE Trans. Inf. Theory **59** (9), 5600–5612, 2013.

[6] I. Cascudo, R. Cramer, and C. Xing, *Torsion limits and Riemann-Roch systems for function fields and applications*, IEEE Trans. Inf. Theory **60** (7), 3871–3888, 2014.

[7] D. Chaum, C. Crépeau, and I. Damgaard, *Multi-Party unconditionally secure protocols*, Proceedings of STOC 1988: ACM Press, New York, 11–19, 1988.

[8] H. Chen and R. Cramer, *Algebraic geometric secret sharing schemes and secure multi-party computations over small fields*, CRYPTO 2006: LNCS **4117** Springer Verlag: 516–531, 2006.

[9] R. Cramer, I. Damgaard, and U. Maurer, *General secure multi-party computation from any linear secret sharing scheme*, EUROCRYPT 2000: LNCS **1807** Springer Verlag: 316–334, 2000.

[10] O. Farràs, C. Padró, C. Xing, and A. Yang, *Natural generalizations of threshold secret sharing* IEEE Trans. Inf. Theory **60** (3), 1652–1664, 2014.

[11] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121**, 211–222, 1995.

[12] F. Hess, H. Stichtenoth, and S. Tutdere, *On invariants of towers of function fields over finite fields*, J. Algebra Appl. **12** (4), 1250190, 2013.

[13] T. Ignatenko and F.M.J. Willems, *Biometric systems: Privacy and secrecy aspects*, IEEE Trans. Inf. Forensics Secur. **4** (4), 956–973, 2009.

[14] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, *Zero-knowledge from secure multi-party computation*, Proceedings of 39th STOC: San Diego, Ca., USA: 21–30, 2007.

[15] Y. Ishai, M. Prabhakaran, and A. Sahai, *Founding cryptography on oblivious transfer-efficiently* CRYPTO 2008: LNCS **157** Springer Verlag: 572–591, 2008.

[16] M. Ito, A. Saito, and T. Nishizeki, *Multiple assignment scheme for sharing secret*, J. Cryptol. **6** (1), 15–20, 1993.

[17] M. Ito, A. Saito, and T. Nishizeki, *Secret sharing scheme realizing any access structure*, Proc IEEE Globecom: 99–102, 1987.

[18] E.D. Karnin, J.W. Greene, and M.E. Hellman, *On secret sharing systems*, IEEE Trans. Inf. Theory **29** (1), 35–41, 1983.

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

[20] M. Naor and A. Wool, *Access control and signatures via quorum secret sharing* IEEE Trans. Parallel Distrib. Syst. **9(1)**, 909–922, 1998.

[21] A. Shamir, *How to share a secret*, Comm. ACM. **22** (11), 612–613, 1979.
[22] H. Stichtenoth, *Algebraic function fields and codes*, 2nd Ed. Springer-Verlag **254**, 2009.
[23] T. Tassa, *Generalized oblivious transfer by secret sharing*, Design Code Cryptogr. **58** (1), 11–21, 2011.
[24] A. Weil, *Variétés abéliennes et courbes algébriques*, Hermann, Paris, 1948.