On asymptotically good ramp secret sharing schemes

Olav Geil, Stefano Martin, Umberto Martínez-Peñas, Ryutaroh Matsumoto, Diego Ruano

On asymptotically good ramp secret sharing schemes

Olav Geil[1], Stefano Martin[1], Umberto Martínez-Peñas[1], Ryutaroh Matsumoto[2], and Diego Ruano[1]

[1] Department of Mathematical Sciences, Aalborg University, Denmark
{olav,stefano,umberto,diego}@math.aau.dk
[2] Department of Communications and Integrated Systems, Tokyo Institute of Technology, Japan
http://www.rmatsumoto.org/

Abstract. Asymptotically good sequences of ramp secret sharing schemes have been intensively studied by Cramer et al. in [1,2,3,4,5,6,7,8]. In those works the focus is on full privacy and full reconstruction. We propose an alternative definition of asymptotically good sequences of ramp secret sharing schemes where a small amount of information leakage is allowed (and possibly also non-full recovery). By a non-constructive proof we demonstrate the existence of sequences that – following our definition of goodness – have parameters arbitrary close to the optimal ones. Moreover – still using our definition – we demonstrate how to concretely construct asymptotically good sequences of schemes from sequences of algebraic geometric codes related to a tower of function fields. Our study involves a detailed treatment of the relative generalized Hamming weights of the involved codes.

1 Introduction

A ramp secret sharing scheme is a cryptographic method to encode a secret $\mathbf{s}$ into multiple shares $c_1, \ldots, c_n$ so that only from specified subsets of the shares one can recover $\mathbf{s}$. Often it is assumed that n participants each receive a share, no two different participants receiving the same. In that description, one talks about qualified and non-qualified sets of participants. The encoding is in general probabilistic, meaning that to each secret $\mathbf{s}$ there corresponds a collection of possible share vectors $\mathbf{c} = (c_1, \ldots, c_n)$.

A linear ramp secret sharing scheme can be understood as a coset construction of two linear codes [5]. Given linear codes $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ where $\dim C_1 = k_1$, $\dim C_2 = k_2$ and $\ell = k_1 - k_2$, let $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k_1}\}$ be a basis for C_1 as a vector space over $\mathbb{F}_q$ in such a way that $\{\mathbf{b}_1, \ldots, \mathbf{b}_{k_2}\}$ is also a basis for C_2. A secret $\mathbf{s} = (s_1, \ldots, s_\ell) \in \mathbb{F}_q^\ell$ is encoded to $\mathbf{c} = c_1\mathbf{b}_1 + \cdots + c_{k_2}\mathbf{b}_{k_2} + s_1\mathbf{b}_{k_2+1} + \cdots + s_\ell\mathbf{b}_{k_1} \in \mathbb{F}_q^n$, where $c_1, \ldots, c_{k_2}$ are chosen at random. The shares are then the elements of $\mathbf{c}$. The information leakage of the system is described by the parameters $t_1, \ldots, t_\ell$, $r_1, \ldots, r_\ell$ where for $m = 1, \ldots, \ell$, t_m and r_m are the unique numbers such that

- no group of t_m participants can recover m q-bits of information, but some group of size $t_m + 1$ can, and

– any group of size r_m can recover m q-bits of information, but some group of size $r_m - 1$ cannot.

From [13, Th. 4] and [12, Th. 3] we have that $t_m = M_m(C_2^\perp, C_1^\perp) - 1$ and $r_m = n - M_{\ell-m+1}(C_1, C_2) + 1$, for $m = 1, \ldots, \ell$, where $M_m(C_1, C_2)$ is the m-th relative generalized Hamming weight (RGHW) of C_1 with respect to C_2 [14]

$$M_m(C_1, C_2) = \min\{\#\mathrm{Supp}D \mid D \subseteq C_1 \text{ is a linear space}, \\ \dim D = m, D \cap C_2 = \{\mathbf{0}\}\}.$$

Here, Supp$D$ is the set of indices i such that for some $(c_1, \ldots, c_n) \in D$, $c_i \neq 0$. The generalized Hamming weights (GHW) $d_m(C_1)$ [20] are obtained by considering $C_2 = \{\mathbf{0}\}$, which serves as a lower bound for $M_m(C_1, C_2)$.

The parameters t_1 and r_ℓ give a first characterization of the ramp secret sharing schemes. One often says that a scheme has $t = t_1$ privacy and $r = r_\ell$ reconstruction.

Asymptotically good sequences of ramp secret sharing schemes have been intensively studied, e.g. in [1,2,3,4,5,6,7,8]. In these works the focus is on zero information leakage and full reconstruction. It seems natural to consider some small fraction of information leakage (and possibly allow non-full reconstruction). Since in this way there is a trade-off between information leakage and corruption and once a scheme is constructed and run, it may happen that more participants than expected are corrupted. We would like then to keep the information leakage as low as possible, and the recovery capability as high as possible.

Clearly, $M_1(C_2^\perp, C_1^\perp)$ is greater than or equal to the minimum distance $d(C_2^\perp)$. Hence, an asymptotically good sequence of codes can be used to construct a sequence of secret sharing schemes where, concerning privacy, we have that t/n goes to some number greater than 0 when n goes to infinity. In particular one can construct schemes with $r/n - t/n < 1$ asymptotically. This technique has been extensively exploited by Cramer et al. in [1,2,3,4,5,6,7]. When dealing with fractions of information leakage (and possibly non-full reconstruction) asymptotically good codes still play a key-role. The relevant parameters, however, are no longer the first relative generalized Hamming weights, but higher relative generalized Hamming weights.

Our proposals for a new definition of asymptotically good sequence of ramp secret sharing schemes involves an infinite sequence of linear ramp secret sharing schemes $(S_1, S_2, \ldots)$, where the shares belong to $\mathbb{F}_q$, a variable Ω, and:

(S.1) The number of participants for S_i is n_i, where $n_i \to \infty$, as $i \to \infty$.
(S.2) The space of secrets for S_i is $\mathbb{F}_q^{\ell_i}$, where $\ell_i/n_i \to L$, as $i \to \infty$.
(S.3) The space of shares for S_i has dimension $k_{1,i}$, where $k_{1,i}/n_i \to \Omega$, as $i \to \infty$.

Definition 1. *Let $0 < L < \Omega \leq 1$, $0 \leq \varepsilon \leq 1$ and $-\varepsilon L \leq \Lambda \leq \Omega - L$. We say that a sequence $(S_1, S_2, \ldots)$ is asymptotically good with deficiency Λ and defect ε if it satisfies (S.1), (S.2) and there exists a sequence of positive integers $(m_1, m_2, \ldots)$ such that $1 \leq m_i \leq \ell_i$, $m_i/n_i \to \varepsilon L$ and:*

$$\liminf_{i\to\infty} \frac{t_{m_i}}{n_i} \geq \Omega - L - \Lambda, \quad \text{and} \quad \limsup_{i\to\infty} \frac{r_{\ell_i - m_i + 1}}{n_i} \leq \Omega + \Lambda.$$

This means that for large enough i, a fraction $\Omega - L - \Lambda$ of the participants can recover at most a fraction εL q-bits of the secret, and a fraction $\Omega + \Lambda$ of the participants can recover at least a fraction $(1-\varepsilon)L$ q-bits of the secret. The condition $-\varepsilon L \leq \Lambda$ means that, when we relax the constrains on privacy and reconstruction of the secret, then the optimal value of the deficiency can possibly be negative, instead of at least zero.

In some other cases, some participants may be corrupted and thus there may be some information leakage, but we can still use their shares to recover the entire secret. Thus, we include the following definition:

Definition 2. *Let $0 < L < \Omega \leq 1$, $0 \leq \varepsilon \leq 1$, $-\varepsilon L \leq \Lambda \leq \Omega - L$ and $0 \leq \Lambda_r \leq \Omega - L$. We say that a sequence $(S_1, S_2, \ldots)$ is asymptotically good with deficiencies Λ and Λ_r, and defect ε if it satisfies (S.1), (S.2) and there exists a sequence of positive integers $(m_1, m_2, \ldots)$ such that $1 \leq m_i \leq \ell_i$, $m_i/n_i \to \varepsilon L$ and:*

$$\liminf_{i\to\infty} \frac{t_{m_i}}{n_i} \geq \Omega - L - \Lambda, \quad \textit{and} \quad \limsup_{i\to\infty} \frac{r_{\ell_i}}{n_i} \leq \Omega + \Lambda_r.$$

In this paper we follow two different tracks. First we extend a result from [15] and then prove the existence of asymptotically good sequences for any Ω and L, with arbitrarily small ϵ and $\Lambda > -\varepsilon L$. Our proof of the existence of the above good sequences is non-constructive. We therefore next turn to demonstrate how to construct sequences of ramp secret sharing schemes with low deficiency and low defect for many different values of Ω and L. The tool for doing this is to apply asymptotically good towers of function fields, in particular Garcia-Stichtenoth's tower in [10], and to employ bounds on corresponding relative generalized Hamming weights. Due to the space limitation, all proofs are omitted in the present extended summary. The full version is available at [11].

2 Asymptotically good sequences

In this section we present the main results of the paper, which are five theorems stating the existence of asymptotically good sequences of ramp secret sharing schemes with low deficiency and defect. The proof of the first theorem is not constructive. It states that it is possible to obtain values of deficiency and defect as close to the optimal ones as wanted.

Theorem 1. *For any $0 < L < \Omega \leq 1$, any $0 < \varepsilon_t, \varepsilon_r < 1$ and any Λ_t, Λ_r with $-\varepsilon_j L < \Lambda_j \leq \Omega - (1+\varepsilon_j)L$, $j = t, r$, there exists an asymptotically good sequence of secret sharing schemes $(S_1, S_2, \ldots)$ with deficiencies Λ_t, Λ_r and defects $\varepsilon_t, \varepsilon_r$.*

On the other hand, the sequences obtain in the following results can be obtained in a constructive way from pairs of algebraic geometric codes.

Theorem 2. *Let q be a power of a prime, $1/A(q) \leq \Omega \leq 1$, $\max\{0, \Omega - 1 + 1/A(q)\} \leq L \leq \Omega$ and*

$$\frac{q}{(q-1)}\frac{1}{A(q)} - \frac{1}{q-1}\min\{\Omega, 1 - \Omega + L\} \leq \varepsilon L \leq \Omega - L.$$

Then, there exists an asymptotically good sequence $(S_1, S_2, \ldots)$, based on one-point algebraic geometric codes, with deficiency $\Lambda = -\varepsilon L$ and defect ε.

Theorem 3. *Let q be a power of a prime, $0 < L < \Omega \leq 1$ and $0 \leq \varepsilon_t, \varepsilon_r \leq \Omega/L - 1$. Then, there exists an asymptotically good sequence $(S_1, S_2, \ldots)$, based on one-point algebraic geometric codes, with deficiencies*

$$\Lambda_t = -\frac{1}{q-1}(\Omega - L) + \frac{q}{q-1}\frac{1}{A(q)} - \varepsilon_t L, \text{ and}$$

$$\Lambda_r = -\frac{1}{q-1}(1 - \Omega) + \frac{q}{q-1}\frac{1}{A(q)} - \varepsilon_r L,$$

and defects ε_t and ε_r.

Theorem 4. *Let q be an even power of a prime, $1/(\sqrt{q}-1) \leq \Omega \leq 1$, $\max\{0, \Omega - 1 + 1/(\sqrt{q}-1)\} \leq L \leq \Omega$ and $0 \leq \varepsilon L \leq 1/(\sqrt{q}-1)$. There exists an asymptotically good sequence $(S_1, S_2, \ldots)$, based on one-point algebraic geometric codes, with deficiency $\Lambda = -2\varepsilon L + 1/(\sqrt{q}-1)$ and defect ε.*

Theorem 5. *Let q be an even power of a prime, $1/(\sqrt{q}-1) \leq \Omega \leq 1$, $\max\{0, \Omega - 1 + 1/(\sqrt{q}-1)\} \leq L \leq \Omega$, $0 \leq V \leq 1/(\sqrt{q}-1)$ and $\max\{0, 1/(\sqrt{q}-1) - 2V\} \leq \varepsilon L \leq \Omega - L$. There exists an asymptotically good sequence $(S_1, S_2, \ldots)$, based on one-point algebraic geometric codes, with deficiency $\Lambda = -\varepsilon L + V$ and defect ε.*

3 The existence of sequences with arbitrarily low Λ and ε

We need a more complete version of [15, Th. 9] to prove Theorem 1. The following results extends [15, Th. 9] and states that the RGHWs of both primary and dual nested code pairs can get asymptotically as close to the Singleton bound.

Theorem 6. *For $0 < R_2 < R_1 \leq 1$, $0 \leq \delta \leq 1$, $0 \leq \delta^\perp \leq 1$, $0 < \tau \leq \min\{\delta, R_1 - R_2\}$ and $0 < \tau^\perp \leq \min\{\delta^\perp, R_1 - R_2\}$, if $R_1 + \delta < 1 + \tau$ and $(1 - R_2) + \delta^\perp < 1 + \tau^\perp$, then for any prime power q and sufficiently large n, there exist $C_2 \subset C_1 \subset \mathbb{F}_q^n$ such that $\dim C_1 = \lfloor nR_1 \rfloor$, $\dim C_2 = \lceil nR_2 \rceil$, $M_{\lceil n\tau \rceil}(C_1, C_2) \geq \lfloor n\delta \rfloor$, and $M_{\lceil n\tau^\perp \rceil}(C_2^\perp, C_1^\perp) \geq \lfloor n\delta^\perp \rfloor$.*

4 Schemes from algebraic geometric codes

The proof of Theorem 1 being non-constructive, we cannot specify the sequence of secret sharing schemes. Also, the RGHWs related to these schemes can get as close as we want to the Singleton bound, but they do not actually reach it. In the remaining part of the paper we shall therefore concentrate on algebraic geometric codes, for which these problems can be overcome.

In the remaining part of the paper, by a function field we shall always mean an algebraic function field of transcendence degree one. As is well-known, the related algebraic geometric codes $C_{\mathcal{L}}(D, G)$ and $C_{\Omega}(D, G)$ are dual to each other. The Goppa bound treats both classes of codes.

Throughout the paper, for a function field F over $\mathbb{F}_q$, we denote by $N(F)$ the number of rational places and by $g(F)$, the genus. Also recall the parameter

$$A(q) = \limsup_{g(F)\to\infty} \frac{N(F)}{g(F)},$$

the limit is taken over all function fields over $\mathbb{F}_q$ of genus $g(F) > 0$. By [19],

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

holds for any prime power q (Drinfeld-Vlăduţ bound).

From the Goppa bound, we can derive a first simple result on asymptotically good sequences of secret sharing schemes, when $\varepsilon = 0$:

Corollary 1. *For any $0 < L < \Omega \leq 1$, there exists a sequence of secret sharing schemes $(S_1, S_2, \ldots)$ with deficiency $\Lambda \leq 1/A(q)$ and defect $\varepsilon = 0$.*

On the other hand, sometimes it is enough to treat the so-called threshold gap $r - t$ [3], and from the previous theorem we immediately get:

Theorem 7. *Let $C_2 \subsetneq C_1$ be algebraic geometric codes defined from a function field of genus g. Write $\dim C_1 = k_1$, $\dim C_2 = k_2$ and $\ell = k_1 - k_2$. The corresponding secret sharing scheme has t privacy and r construction where $t \geq k_2 - g$ and $r \leq k_1 + g$. In particular $r - t \leq \ell + 2g$.*

The Singleton upper bound, $M_m(C_1, C_2) \leq n - \dim C_1 + m$, the Goppa lower bound on the relative generalized Hamming weights of algebraic geometric codes and the Wei's duality theorem [20] give the following

Proposition 1. *If $\ell \geq 2g$, then $1 \leq r_m - t_m \leq g + 1$, for $m = 1, 2, \ldots, \ell$, and, if $g + 1 \leq m \leq \ell - g$, then $r_m - t_m = 1$.*

4.1 Non-asymptotic bounds for one-point algebraic geometric codes

In the remaining part of the paper we shall concentrate on one-point algebraic geometric codes. Hence, for the codes $C_{\mathcal{L}}(D, G)$ and $C_{\Omega}(D, G)$ we shall always assume that $D = P_1 + \cdots + P_n$ and that $G = \mu Q$ where $P_1, \ldots, P_n, Q$ are pairwise different rational places. Writing ν_Q for the valuation at Q the Weierstrass semigroup corresponding to Q is

$$H(Q) = -\nu_Q \left(\bigcup_{\mu=0}^{\infty} \mathcal{L}(\mu Q) \right) = \{\mu \in \mathbb{N}_0 \mid \mathcal{L}(\mu Q) \neq \mathcal{L}((\mu - 1)Q)\}.$$

Consider the related subset

$$H^*(Q) = \{\mu \in \mathbb{N}_0 \mid C_{\mathcal{L}}(D, \mu Q) \neq C_{\mathcal{L}}(D, (\mu - 1)Q)\}.$$

From now on we consider a pair of codes $C_1 = C_{\mathcal{L}}(D, \mu_1 Q)$ and $C_2 = C_{\mathcal{L}}(D, \mu_2 Q)$ with $0 \leq \mu_2 < \mu_1$. Write $k_1 = \dim C_1$ and $k_2 = \dim C_2$, respectively, and $\ell = \dim(C_1/C_2) = k_1 - k_2$. Observe that $\mu = \mu_1 - \mu_2 \leq \ell$ with equality if simultaneously $2g \leq \mu_2 \leq n$ and $\mu_1 \leq n$ hold. We have the following bounds on RGHWs from [12, Theorems 19, 20]:

Theorem 8. *For $1 \leq m \leq \ell$, we have*

1. $M_m(C_1, C_2) \geq n - \mu_1 + \min\{\#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\} \mid -\mu + 1 \leq i_1 < i_2 < \ldots < i_{m-1} \leq -1\}$.
2. $M_m(C_2^\perp, C_1^\perp) \geq \min\{\#\{\alpha \in \cup_{s=1}^{m}(i_s + (\mu_1 - H(Q))) \mid \alpha \in H(Q)\} \mid -\mu + 1 \leq i_1 < i_2 < \ldots < i_m \leq 0\}$.

Instead of computing these minimums, in the following two propositions we bound them for some values of m. For $0 \leq \gamma \leq c$, let $h_\gamma = \#\left(H(Q) \cap (0, \gamma]\right)$.

Proposition 2. *If $2g \leq \mu_1 \leq n-1$ and $1 \leq m \leq \min\{\ell, c\}$, then*

$$M_m(C_1, C_2) \geq n - k_1 + 2m - c + h_{c-m}.$$

Note that C_2 could be $\{\mathbf{0}\}$, since we are allowing $\mu_2 = -1$, and thus we obtain bounds on the GHWs of C_1.

Now, let $g_\gamma = \#([\gamma, \infty) \setminus H(Q))$, for $\gamma \geq 1$.

Proposition 3. *If $2g \leq \mu_2 \leq n-1$ and $1 \leq m \leq \min\{\ell, c\}$, then*

$$M_m(C_2^\perp, C_1^\perp) \geq k_2 + 2m - c + g_{\mu_2 - c + m}.$$

Note that C_1 could be $\mathbb{F}_q^n$, since we are allowing $\mu_1 = n + 2g - 1$, and thus $C_1^\perp = \{\mathbf{0}\}$ and we obtain bounds on the GHWs of $C_2^\perp$.

4.2 RGHWs versus GHWs for one-point algebraic geometric codes

In this subsection we compare the RGHWs with the GHWs of the pair of primary one-point algebraic geometric codes $C_2 \subsetneq C_1$, where the notation is as in the previous section. After that, we treat the dual case. In this way we can see how much we are losing by considering GHWs instead of RGHWs.

For that purpose, we also use the notation from [12, Sections IV and V]. First write $H^*(Q) = \{\gamma_1, \gamma_2, \ldots, \gamma_n\}$, with $\gamma_1 < \gamma_2 < \ldots < \gamma_n$. Now, fix functions f_i in the function field such that $-\nu_Q(f_i) = \gamma_i$, and write $\mathbf{b}_i = (f_i(P_1), f_i(P_2), \ldots, f_i(P_n))$, which constitute a basis of $\mathbb{F}_q^n$. Then, we define the function $\overline{\rho} : \mathbb{F}_q^n \to \{0, 1, 2, \ldots, n\}$ by

$$\overline{\rho}(\mathbf{c}) = \min\{i : \mathbf{c} \in \operatorname{span}(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_i)\},$$

if $\mathbf{c} \neq \mathbf{0}$, and we define $\overline{\rho}(\mathbf{0}) = 0$.

We state the result [12, Proposition 17] as a lemma and then the main result:

Lemma 1. *Let $D \subset \mathbb{F}_q^n$ be a linear subspace of dimension m, with $\overline{\rho}(D \setminus \{\mathbf{0}\}) = \{i_1, i_2, \ldots, i_m\}$, where $i_1 < i_2 < \ldots < i_m$. The support of D satisfies*

$$\#SuppD \geq n - \gamma_{i_m} + \#\{\alpha \in \cup_{s=1}^{m-1}(\gamma_{i_s} - \gamma_{i_m} + H(Q)) : \alpha \notin H(Q)\}.$$

Proposition 4. *Using the same notation as in the previous section, assume that $0 \leq \mu_2 < \mu_1$, $2g \leq \mu_1 \leq n-1$, and $\ell = k_1 - k_2$. If $D \subset C_1$ is a linear subspace of dimension $\dim D = m \leq \ell$ such that $D \cap C_2 \neq \{\mathbf{0}\}$, then $\#SuppD \geq n - k_1 + m - \max\{0, c - \ell\}$.*

As a direct consequence, we obtain an upper bound on the difference between RGHWs and GHWs:

Corollary 2. *Under the same hypotheses of the previous proposition, and for* $1 \leq m \leq \ell$, *it holds that* $M_m(C_1, C_2) - d_m(C_1) \leq c - \ell$, *if* $\ell < c$, *and* $M_m(C_1, C_2) = d_m(C_1)$ *if* $\ell \geq c$ *or if* $m > g$.

We can also treat dual codes and obtain an upper bound:

Corollary 3. *Under the same hypotheses of the previous proposition, and for* $1 \leq m \leq \ell$, *it holds that* $M_m(C_2^\perp, C_1^\perp) - d_m(C_2^\perp) \leq c - \ell$, *if* $\ell < c$, *and* $M_m(C_2^\perp, C_1^\perp) = d_m(C_2^\perp)$ *if* $\ell \geq c$ *or if* $m > g$.

It is often enough to study the GHWs rather than the RGHWs for constructing asymptotically good sequences of secret sharing schemes:

Proposition 5. *Consider a sequence of pairs of one-point algebraic geometric codes* $C_{j,i} = C_{\mathcal{L}}(D_i, \mu_j Q_i)$, $j = 1, 2$, $\mu_{2,i} < \mu_{1,i}$ *related to a tower of function fields* $(F_1, F_2, \ldots)$ *over* $\mathbb{F}_q$. *By* c_i *we denote the conductor of the Weierstrass semigroup related to* Q_i, *and by* g_i *the genus. Assume that the length* n_i *of the codes* $C_{j,i}$ *satisfies* $n_i \to \infty$ *and that* $\mu_{1,i}$ *and* $\mu_{2,i}$ *are chosen such that* $(\mu_{j,i} - g_i)/(n_i) \to R_j$, $j = 1, 2$, *which implies that* $(\dim C_{j,i})/(n_i) \to R_j$, $j = 1, 2$. *Let* $(m_1, m_2, \ldots)$ *be a sequence of integers such that* $(m_i)/(n_i) \to \rho$, *where* $0 \leq \rho \leq R = R_1 - R_2$. *Assume that* $M_{m_i}(C_{1,i}, C_{2,i})/n_i \to M$, $d_{m_i}(C_{1,i})/n_i \to \delta$, $c_i/n_i \to \gamma$ *and* $R_1 \geq \lim_i (g_i/n_i)$. *Then it holds that* $0 \leq M - \delta \leq \gamma - R$, *if* $R < \gamma$, *and* $M = \delta$ *if* $R \geq \gamma$.

5 Asymptotic analysis for AG-codes over general fields

From [18, Th. 5.9] we have the following theorem

Theorem 9. *Let* q *be a fixed prime power. For any pair* (δ, R) *and any* $\rho \leq R$ *such that* $\rho \leq \delta \leq 1$, $\delta + R \leq 1 + \rho$, *and any growing sequence* $m_i \to \infty$, *there exists an infinite sequence of linear* q*-ary codes* $(C_1, C_2, \ldots)$ *with* $n_i = n(C_i) \to \infty$, $m_i/n_i \to \rho$, $\dim C_i/n_i \to R$ *and* $d_{m_i}(C_i)/n_i \to \delta$.

The proof given in [18] of Theorem 9 uses a sequence of asymptotically good algebraic geometric codes, which suggests that one could attain the Singleton bound for any ρ and R with $0 \leq \rho \leq R \leq 1$ by using codes from an optimal tower of function fields over $\mathbb{F}_q$. For instance, this could be done in a constructive way for q being a square by using one of Garcia-Stichtenoth's tower, see [17]. Unfortunately, as we explain below, the proof given in [18] imposes an unnoticed restriction on ρ and R which leaves many cases undecided. This restriction is $1/A(q) \leq \rho \leq R$ which in particular by (1) means that $1/(\sqrt{q} - 1) \leq \rho$. Plugging in for instance $q = 4$ we obtain $1 \leq \rho \leq R$, leaving Theorem 9 empty. For $q = 9$ the restriction is $\frac{1}{2} \leq \rho \leq R$, leaving many cases undecided.

We now show that it is possible to replace the condition $1/A(q) \leq \rho \leq R$ with the less restrictive condition that

$$\frac{q}{q-1}\frac{1}{A(q)} - \frac{1}{q-1}R \leq \rho \leq R, \ \tfrac{1}{A(q)} \leq R. \tag{2}$$

Theorem 10. *Given a power of a prime q, $1/A(q) \leq R \leq 1$ and $\frac{q}{q-1}\frac{1}{A(q)} - \frac{1}{q-1}R \leq \rho \leq R$, let $(C_1, C_2, \ldots)$ be a sequence of algebraic geometric codes defined from a tower of function fields $(F_1, F_2, \ldots)$, with $g(F_i) \to \infty$, $N(F_i)/g(F_i) \to A(q)$, $n_i = n(C_i) = N(F_i) - 1$ and $\dim C_i/n_i \to R$. There exists a sequence $(m_1, m_2, \ldots)$ of positive integers such that $m_i/n_i \to \rho$, $d_{m_i}(C_i)/n_i \to \delta$ and $\delta = 1 - R + \rho$.*

The next proposition can give us some information in the interval where the above theorem fails to provide such.

Proposition 6. *Given a power of a prime q, $0 \leq R \leq 1$ and $0 \leq \rho \leq R$, let $(C_1, C_2, \ldots)$ be a sequence of algebraic geometric codes defined from a tower of function fields $(F_1, F_2, \ldots)$, with $g(F_i) \to \infty$, $N(F_i)/g(F_i) \to A(q)$, $n_i = n(C_i) = N(F_i) - 1$ and $\dim C_i/n_i \to R$. For any sequence $(m_1, m_2, \ldots)$ of positive integers such that $m_i/n_i \to \rho$, with $\delta = \liminf_{i\to\infty} d_{m_i}(C_i)/n_i$, we have that*

$$\delta \geq \frac{q}{q-1}\left(1 - R - \frac{1}{A(q)}\right) + \rho.$$

6 Asymptotic analysis over $\mathbb{F}_q$ when q is a square

Garcia and Stichtenoth gave two towers [9,10] of function fields over quadratic finite fields attaining the Drinfeld-Vlăduţ bound. The tower in [10] is given by:

- $F_1 = \mathbb{F}_q(x_1)$,
- for $\nu > 1$, $F_\nu = F_{\nu-1}(x_\nu)$ with x_ν satisfying $x_\nu^{\sqrt{q}} + x_\nu = \frac{x_{\nu-1}^{\sqrt{q}}}{x_{\nu-1}^{\sqrt{q}-1}+1}$,

where q is an even power of a primer number.

The number of its rational places is $N(F_\nu) \geq q^{\frac{\nu-1}{2}}(q - \sqrt{q})$ and its genus is $g_\nu = g(F_\nu) = (q^{\frac{1}{2}\left\lfloor\frac{\nu+1}{2}\right\rfloor} - 1)(q^{\frac{1}{2}\left\lceil\frac{\nu+1}{2}\right\rceil} - 1)$. From [16, Sec. 2], we have that the conductor of $H(Q)$ when Q is the pole at $x_1 \in F_m$: $c_\nu = q^{\nu/2} - q^{\nu/4}$, if ν is even, and $q^{\nu/2} - q^{(\nu+1)/4}$, otherwise.

In this section, we apply Proposition 2 and Proposition 3 to derive new asymptotic results that we then compare with the general ones in the previous section.

Corollary 4. *If q is an even power of a prime, $\frac{1}{\sqrt{q}-1} \leq R \leq 1$ and $0 \leq \rho \leq \frac{1}{\sqrt{q}-1}$, there exists a sequence of one-point algebraic geometric codes C_i and a sequence of positive integers m_i such that: $n_i = n(C_i) \to \infty$, $\dim C_i/n_i \to R$, $m_i/n_i \to \rho$, $\delta = \liminf_{i\to\infty} d_{m_i}(C_i)/n_i$ and $\delta^\perp = \liminf_{i\to\infty} d_{m_i}(C_i^\perp)/n_i$, with $\delta \geq 1 - R + 2\rho - \frac{1}{\sqrt{q}-1}$, and $\delta^\perp \geq R + 2\rho - \frac{1}{\sqrt{q}-1}$.*

We next use Wei's duality theorem to improve the previous asymptotic bound. We only consider primary one-point algebraic geometric codes. The case of duals of one-point algebraic geometric codes is analogous.

Corollary 5. *If q is an even power of a prime, $\frac{1}{\sqrt{q}-1} \leq R \leq 1$, $0 \leq V \leq \frac{1}{\sqrt{q}-1}$ and $\max\{0, \frac{1}{\sqrt{q}-1} - 2V\} \leq \rho \leq R$, there exists a sequence of one-point algebraic geometric codes C_i and a sequence of positive integers m_i such that: $n_i = n(C_i) \to \infty$, $\dim C_i/n_i \to R$, $m_i/n_i \to \rho$ and $\delta = \liminf_{i\to\infty} d_{m_i}(C_i)/n_i$, with $\delta \geq 1 - R + \rho - V$.*

We observe that Corollary 5 simplifies to Theorem 9 (with the necessary restriction $1/A(q) \leq \rho \leq R$) when $V = 0$, and improves the asymptotic Goppa bound when $2V = 1/(\sqrt{q} - 1)$.

7 Asymptotically good sequences of ramp secret sharing schemes from algebraic geometric codes

The strategy to obtain asymptotically good sequences of schemes is analogous in all the cases. It consists in defining a suitable sequence of pairs of codes $C_2(i) \subset C_1(i) \subset \mathbb{F}_q^{n_i}$ such that: $\dim C_1(i)/n_i \to \Omega$, $(\dim C_1(i) - \dim C_2(i))/n_i = \ell_i/n_i \to L$, $(\varepsilon\ell_i)/n_i \to \varepsilon L = \rho$, for $i \to \infty$, and choosing Λ appropriately so that

$$\liminf_{i\to\infty} \frac{d_{m_i}(C_2(i)^\perp)}{n_i} \geq \Omega - L - \Lambda, \text{ and} \tag{3}$$

$$\liminf_{i\to\infty} \frac{d_{m_i}(C_1(i))}{n_i} \geq 1 - \Omega - \Lambda. \tag{4}$$

In this way, one can prove Theorem 2, Theorem 3, Theorem 4 and Theorem 5, which are consequences of Theorem 10, Proposition 6, Corollary 4 and Corollary 5, respectively.

Acknowledgements: The authors wish to thank Ignacio Cascudo and Ronald Cramer for valuable feedback on the manuscript. Also the authors gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367), from the Spanish MINECO (Grant No. MTM2012-36917-C03-03), from Japan Society for the Promotion of Science (Grant Nos. 23246071 and 26289116), from the Villum Foundation through their VELUX Visiting Professor Programme 2013-2014, and from the "Program for Promoting the Enhancement of Research Universities" at Tokyo Institute of Technology.

References

1. Cascudo, I., Chen, H., Cramer, R., Xing, C.: Asymptotically good ideal linear secret sharing with strong multiplication over *any* fixed finite field. In: Advances in cryptology—CRYPTO 2009, Lecture Notes in Comput. Sci., vol. 5677, pp. 466–486. Springer, Berlin (2009)
2. Cascudo, I., Cramer, R., Mirandola, D., Zemor, G.: Squares of random linear codes. IEEE Trans. Inform. Theory 61(3), 1159–1173 (March 2015)
3. Cascudo, I., Cramer, R., Xing, C.: Bounds on the threshold gap in secret sharing and its applications. IEEE Trans. Inform. Theory 59(9), 5600–5612 (2013)

4. Cascudo, I., Cramer, R., Xing, C.: Torsion limits and Riemann-Roch systems for function fields and applications. IEEE Trans. Inform. Theory 60(7), 3871–3888 (2014)
5. Chen, H., Cramer, R., Goldwasser, S., de Haan, R., Vaikuntanathan, V.: Secure computation from random error correcting codes. In: Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, pp. 291–310. Springer, Berlin (2007)
6. Chen, H., Cramer, R., de Haan, R., Cascudo, I.: Strongly multiplicative ramp schemes from high degree rational points on curves. In: Advances in cryptology—EUROCRYPT 2008, Lecture Notes in Comput. Sci., vol. 4965, pp. 451–470. Springer, Berlin (2008)
7. Chen, H., Cramer, R.: Algebraic geometric secret sharing schemes and secure multiparty computations over small fields. In: Advances in cryptology—CRYPTO 2006, Lecture Notes in Comput. Sci., vol. 4117, pp. 521–536. Springer, Berlin (2006)
8. Cramer, R., Damgård, I., Döttling, N., Fehr, S., Spini, G.: Linear secret sharing schemes from error correcting codes and universal hash functions. In: To appear in EUROCRYPT 2015, pp. 1–24 (2015)
9. Garcia, A., Stichtenoth, H.: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-vlăduţ bound. Inventiones Mathematicae 121(1), 211–222 (1995)
10. Garcia, A., Stichtenoth, H.: On the asymptotic behaviour of some towers of function fields over finite fields. Journal of Number Theory 61(2), 248–273 (1996)
11. Geil, O., Martin, S., Martínez-Peñas, U., Matsumoto, R., Ruano, D.: On asymptotically good ramp secret sharing schemes. ArXiv: 1502.05507 (2015)
12. Geil, O., Martin, S., Matsumoto, R., Ruano, D., Luo, Y.: Relative generalized Hamming weights of one-point algebraic geometric codes. IEEE Trans. Inform. Theory 60(10), 5938–5949 (2014)
13. Kurihara, J., Uyematsu, T., Matsumoto, R.: Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. IEICE Trans. Fundamentals E95-A(11), 2067–2075 (Nov 2012)
14. Luo, Y., Mitrpant, C., Vinck, A.J.H., Chen, K.: Some new characters on the wiretap channel of type II. IEEE Trans. Inform. Theory 51(3), 1222–1229 (2005)
15. Matsumoto, R.: New asymptotic metrics for relative generalized Hamming weight. Proceedings of IEEE International Symposium on Information Theory pp. 3142–3144 (2014)
16. Pellikaan, R., Stichtenoth, H., Torres, F.: Weierstrass semigroups in an asymptotically good tower of function fields. Finite fields and their applications 4(4), 381–392 (1998)
17. Shum, K.W., Aleshnikov, I., Kumar, P.V., Stichtenoth, H., Deolaikar, V.: 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)
18. Tsfasman, M.A., Vlăduţ, S.G.: Geometric approach to higher weights. IEEE Trans. Inform. Theory 41(6, part 1), 1564–1588 (1995), special issue on algebraic geometry codes
19. Vlăduţ, S.G., Drinfel′d, V.G.: The number of points of an algebraic curve. Funktsional. Anal. i Prilozhen. 17(1), 68–69 (1983)
20. Wei, V.K.: Generalized Hamming weights for linear codes. IEEE Trans. Inform. Theory 37(5), 1412–1418 (1991)