Refined analysis of RGHWs of code pairs coming from Garcia-Stichtenoth’s second tower

O. Geil\textsuperscript{1}, S. Martin\textsuperscript{1}, U. Martínez-Peñas\textsuperscript{1}, D. Ruano\textsuperscript{1}

\textsuperscript{1} Aalborg University, Aalborg, Denmark, \{olav.stefano.umberto.diego\}@math.aau.dk

1 Introduction

Relative generalized Hamming weights (RGHW) of two linear codes are fundamental for evaluating the security of ramp secret sharing schemes and wire-tap channels of type II [3, 4]. Until few years ago only for MDS codes and a few other examples of codes the hierarchy of the RGHWs was known [6], but recently new results were discovered for one-point algebraic geometric codes [3], \(q\)-ary Reed-Muller codes [7] and cyclic codes [8]. In [2] it was discussed how to obtain asymptotically good sequences of ramp secret sharing schemes by using one-point algebraic geometric codes defined from good towers of function fields. The tools used here were the Goppa bound and the Feng-Rao bounds. In the present paper we focus on secret sharing schemes coming from the Garcia-Stichtenoth second tower [1]. We demonstrate how to obtain refined information on the RGHW’s when the codimension is small. For general co-dimension we give an improved estimate on the highest RGHW. The new results are obtained by studying in detail the sequence of Weierstrass semigroups related to a sequence of rational places [5].

We recall the definition of RGHWs and briefly mention their use in connection with secret sharing schemes.

\textbf{Definition 1} Let \( C_2 \subseteq C_1 \) be two linear codes. For \( m = 1, \ldots, \dim C_1 - \dim C_2 \) the \( m \)-th relative generalized Hamming weight (RGHW) of \( C_1 \) with respect to \( C_2 \) is

\[
M_m(C_1, C_2) = \min \{ \# \text{Supp} D \mid D \subseteq C_1 \text{ is a linear space}, \dim D = m, D \cap C_2 = \{ \vec{0} \} \}. \tag{1}
\]

Here \( \text{Supp} D = \{ i \in \mathbb{N} \mid \exists (c_1, \ldots, c_n) \in D \text{ with } c_i \neq 0 \} \).

For \( m = 1, \ldots, \dim C_1 \) the \( m \)-th generalized Hamming weight (GHW) \( d_m(C_1) \) is equal to \( M_m(C_1, \{ \vec{0} \}) \).

It was proved in [3, 4] that a secret sharing secret scheme obtained from two linear codes \( C_2 \subseteq C_1 \) has \( r_m = n - M_{\ell - m + 1}(C_1, C_2) + 1 \) reconstruction and \( t_m = M_m(C_2^+, C_1^+) - 1 \) privacy for \( m = 1, \ldots, \ell \). Here, \( r_m \) and \( t_m \) are the unique numbers such that the following holds: It is not possible to recover \( m \) \( q \)-bits of information
about the secret with only \( t_m \) shares, but it is possible with some \( t_m + 1 \) shares. With any \( r_m \) shares it is possible to recover \( m \) \( q \)-bits of information about the secret, but it is not possible to recover \( m \) \( q \)-bits of information with some \( r_m - 1 \) shares.

We shall focus on one-point algebraic geometric codes \( C_{\mathcal{L}}(D, G) \) where \( D = P_1 + \cdots + P_n, G = \mu Q \), and \( P_1, \ldots, P_n, Q \) are pairwise different rational places over a function field. By writing \( \nu_Q \) for the valuation at \( Q \), the Weierstrass semigroup corresponding to \( Q \) is

\[
H(Q) = -\nu_Q \left( \bigcup_{\mu=0}^{\infty} \mathcal{L}(\mu Q) \right) = \{ \mu \in \mathbb{N}_0 \mid \mathcal{L}(\mu Q) \neq \mathcal{L}((\mu-1)Q) \}. \tag{2}
\]

We denote by \( g \) the genus of the function field and by \( c \) the conductor of the Weierstrass semigroup.

We consider \( C_1 = C_{\mathcal{L}}(D, \mu_1 Q) \) and \( C_2 = C_{\mathcal{L}}(D, \mu_2 Q) \), with \(-1 \leq \mu_2 < \mu_1\). Observe that for \( \ell = \dim(C_1) - \dim(C_2) \) and \( \mu = \mu_1 - \mu_2 \) we have that \( \ell \leq \mu \), with equality if \( 2g \leq \mu_2 < \mu_1 \leq n - 1 \) holds.

From [2, Proposition 23 and its proof] we have the following result:

**Proposition 2** If \( 1 \leq m \leq \min\{\ell, c\} \), then

\[
M_m(C_1, C_2) \geq n - \mu_1 + (m - 1) + (m - c + g + h_{c-m}) \tag{3}
\]

where \( h_{c-m} = \#(H(Q) \cap (0, c-m)]. \) If \( 2g \leq \mu_1 \leq n - 1 \), then

\[
M_m(C_1, C_2) \geq n - \dim C_1 + 2m - c + h_{c-m} \tag{4}
\]

Applying Proposition 2 to code pairs coming from Garcia-Stichtenoth’s second tower [1] the following asymptotically result was obtained in [2, Corollary 40]:

**Corollary 3** Let \( q \) be an even power of a prime and \( 0 \leq \rho \leq \frac{1}{\sqrt{q-1}} \). There exists a sequence of one-point algebraic geometric codes \( C_i = C_{\mathcal{L}}(D, \mu_i Q) \) and a sequence of positive integers \( m_i \), such that for \( i \) going to infinity: \( n_i = n(C_i) \rightarrow \infty \), \( \dim C_i/n_i \rightarrow R \), \( \mu_i/n_i \rightarrow \bar{R} \), \( m_i/n_i \rightarrow \rho \). Let \( \delta = \liminf \frac{d_m(C_i)}{n_i} \), we have that:

\[
\delta \geq 1 - \bar{R} + 2\rho. \tag{5}
\]

If \( \frac{1}{\sqrt{q-1}} \leq R \leq 1 \), we have that:

\[
\delta \geq 1 - R + 2\rho - \frac{1}{\sqrt{q-1}}. \tag{6}
\]
From Garcia-Stichtenoth’s second tower [1] one obtains codes over any field $\mathbb{F}_q$ where $q$ is an even power of a prime. Garcia and Stichtenoth analyzed the asymptotic behavior of the number of rational places and the genus, from which it is clear that the codes beat the Gilbert-Varshamov bound for $q \geq 49$. Remarkably, a complete description of the Weierstrass semigroups corresponding to a sequence of rational places was given in [5]. This description is what allows us to refine in the present paper the analysis of the RGHWs.

2 Small codimension

In this section we give a sharper bound on the RGHWs of two one-point algebraic geometric codes coming from Stichtenoth-Garcia’s towers when the codimension is small.

**Proposition 4** Let $\nu$ be an even positive integer and $q$ an even power of a prime. Consider two one-point algebraic geometric codes $C_2 \subseteq C_1$ defined from the $\nu$-th Garcia-Stichtenoth function field over $\mathbb{F}_q$. For $\mu < \frac{q^{\frac{\nu+1}{2}}}{\nu} + 1$ and $m = 1, \ldots, \mu$, we have that:

$$M_m(C_1, C_2) \geq n - \mu + \min \left\{ (m - 1)q^{-\frac{1}{2}u} + \frac{u}{q^{\nu}} \left( 1 - q^{-\frac{1}{2}} \right) \right\} ;$$

$$u \in \left\{ \left\lfloor \log_q (m - 1) + \frac{1}{2} \right\rfloor, \left\lfloor \log_q (\mu - 1) + \frac{1}{2} \right\rfloor \right\} .$$

(7)

Note that there are some cases where the minimum is reached for $u = \left\lfloor \log_q (m - 1) + \frac{1}{2} \right\rfloor$ and other cases where it is reached for $u = \left\lfloor \log_q (\mu - 1) + \frac{1}{2} \right\rfloor$. For this reason in Proposition 4 the value $u$ is not univocal.

As Proposition 2, this result has an asymptotic implication:

**Corollary 5** Let $q$ be an even power of a prime, $0 \leq \tilde{R}_2 \leq \tilde{R}_1 < 1$, and $\tilde{R} = \tilde{R}_1 - \tilde{R}_2 < \frac{1}{\sqrt{q} - 1}$. There exists a sequence of pairs of one-point AG codes $C_{2,i} \subseteq C_{1,i} = C_{\tilde{R}}(D_{1,i}, \mu_{2,i}Q)$, such that: $n_i = n(C_{2,i}) = n(C_{1,i}) \to \infty$, $\mu_{j,i}/n_i \to \tilde{R}_j$ for $j = 1, 2$ for $i \to \infty$. For a given $\rho$ let $m_i$ be such that $m_i/n_i \to \rho$ for $i \to \infty$ and let $M = \liminf M_{m_i}(C_{1,i}, C_{2,i})/n_i$. The sequence of code pairs satisfies:

$$M \geq 1 - \tilde{R}_1 + \min_{u \in \{\rho, \tilde{R}\}} \left\{ \rho (u(q - \sqrt{q}))^{-\frac{1}{2}} + \frac{u}{q} (q - \sqrt{q}) \right\} .$$

(8)
Note that if we assume that $C_{2,i}$ are zero codes for all $i$, then $\lim M_{m_i}(C_{1,i}, \{\vec{0}\})$ is the asymptotically value of the $m_i$-th general Hamming weight of $C_{i,1}$. For $\bar{R} < \frac{1}{4(q-\sqrt{q})}$, the bound in Corollary 5 is sharper than the one obtained in Corollary 3.

In the following graph we compare the bound from Corollary 3 (the dashed curve) with the bound from Corollary 5 (the solid curve). The first axis represents $\rho = \lim m_i/n_i$, and the second axis represents $\delta = \liminf M_{m_i}(C_{1,i}, \{\vec{0}\})$.

3 The highest RGHW

In this section for $2g \leq \mu_2 < \mu_1 < n - 1$, we obtain a new bound for the highest RGHW of two one-point algebraic geometric codes obtained from Stichtenoth-Garcia’s second tower.

Proposition 6 Let $\nu$ be an even positive integer and $2g \leq \mu_2 < \mu_1 < n - 1$. Consider two one-point algebraic geometric codes $C_2 \subsetneq C_1$ built on the $\nu$-th Garcia-Stichtenoth tower. We have that:

$$M_\ell(C_1, C_2) = n - \dim C_2 \quad \text{if } \ell \geq q^{\nu - 1}$$

$$M_\ell(C_1, C_2) \geq n - \dim C_2 - \left( q^{\nu - \frac{1}{2}} - q^{-\frac{1}{2}} \right) \sum_{i=1}^{\left\lfloor \frac{\nu+1}{2} - \log_q(\ell) \right\rfloor - 1} (q^{1 - \frac{1}{2}} - q^{-\frac{1}{2}}) +$$

$$+ (q^{\nu - \frac{1}{2}} - \left\lfloor \frac{\nu+1}{2} - \log_q(\ell) \right\rfloor)q^{-\frac{1}{2}}$$

if $\ell < q^{\nu - 1}$

For $\ell \geq q^{\nu - 1}$, the Singleton bound is reached. For $\ell < q^{\nu - 1}$ it is still an interesting bound because we are able to estimate $h_{c-m}$. This bound has an asymptotically implication as well:
Corollary 7  Let \( q \) be an even power of a prime, \( \frac{2}{\sqrt{q} - 1} \leq \tilde{R}_2 \leq \tilde{R}_1 < 1 \), and \( \hat{R} = \tilde{R}_1 - \tilde{R}_2 \). There exists a sequence of one-point algebraic geometric codes \( C_{2,i} = C_{\tilde{g}}(D_i, \mu_{2,i}Q) \subseteq C_{1,i} = C_{\tilde{g}}(D_i, \mu_{1,i}Q) \), \( \mu_i = \mu_{1,i} - \mu_{2,i} \), such that: \( n_i = n(C_{2,i}) = n(C_{1,i}) \to \infty \), \( \mu_{j,i}/n_i \to \tilde{R}_j \) for \( j = 1, 2 \) for \( i \to \infty \). Let \( \ell_i = \dim C_{1,i} - \dim C_{2,i} \), \( M = \liminf \frac{M_{\ell_i}(C_{1,i}, C_{2,i})}{n_i} \), \( R_j = \lim \frac{\dim C_i}{n_i} \) for \( j = 1, 2 \), and \( \hat{R} = R_1 - R_2 \), we have that:

\[
M = 1 - R_2 \quad \text{if} \quad R \geq \frac{1}{q - \sqrt{q}}
\]

and

\[
M \geq 1 - R_2 - \left( \frac{1}{q - \sqrt{q}} \left( -\frac{\log_q(R_1 - \frac{1}{\sqrt{q}}))}{\log_q(1 - \frac{1}{\sqrt{q}})} \right)^{-1} \sum_{j=1}^{\frac{\log_q(R_1 - \frac{1}{\sqrt{q}})}{\log_q(1 - \frac{1}{\sqrt{q}})}} (q^{1 - \frac{1}{2j}} q^{-\frac{1}{2j}}) + q^{1 + \frac{1}{2} \log_q(R_1 - \frac{1}{\sqrt{q}}))} \right) - R q^{-\frac{1}{2} \log_q(R_1 - \frac{1}{\sqrt{q}}))} \right) \quad \text{if} \quad R < \frac{1}{q - \sqrt{q}}.
\]

In Corollary 3, \( \rho \) is smaller than or equal to \( \frac{1}{\sqrt{q} - 1} \). If we assume \( C_{2,i} \) to be the zero codes for all \( i \), then the value \( M \) of Corollary 7 represents the asymptotically value of the highest generalized Hamming weight of \( C_{1,1} \). By using Corollary 3 for \( R = \frac{1}{\sqrt{q} - 1} \) it is possible to obtain a similar value, but for the other values of \( R \) it is a new bound.

References


