Relative generalized Hamming weights of one-point algebraic geometric codes

Olav Geil*, Stefano Martin*, Ryutaroh Matsumoto†, Diego Ruano* and Yuan Luo ‡
*Department of Mathematical Sciences, Aalborg University, Denmark
Email: {olav,stefano,diego}@math.aau.dk
†Department of Communications and Computer Engineering, Tokyo Institute of Technology, Japan
Email: ryutaroh@rmatsumoto.org
‡Computer Science and Engineering Department, Shanghai Jiao Tong University, China
Email: yuanluo@sjtu.edu.cn

Abstract

Security of linear ramp secret sharing schemes can be characterized by the relative generalized Hamming weights of the involved codes [30], [28]. In this paper we elaborate on the implication of these parameters and we devise a method to estimate their value for general one-point algebraic geometric codes. As it is demonstrated, for Hermitian codes our bound is often tight. Furthermore, for these codes the relative generalized Hamming weights are often much larger than the corresponding generalized Hamming weights.

Index Terms

linear code, Feng-Rao bound, Hermitian code, one-point algebraic geometric code, relative dimension/length profile, relative generalized Hamming weight, secret sharing, wiretap channel of type II.

I. Introduction

A secret sharing scheme is a cryptographic method to encode a secret into multiple shares later distributed to participants, so that only specified sets of participants can reconstruct the secret. The first secret sharing scheme was proposed by Shamir [39]. It was a perfect scheme, in which a set of participants unable to reconstruct the secret has absolutely no information on the secret. Later, non-perfect secret sharing schemes were proposed [4], [46] in which there are sets of participants that have non-zero amount of information about the secret but cannot reconstruct it. The term ramp secret sharing scheme is sometimes used for the latter mentioned type of schemes, sometimes for the union of the two types. In this paper we will apply the most general definition, but concentrate our investigation on non-perfect secret sharing schemes. Secret sharing has been used, for example, to store confidential information to multiple locations geographically apart. By using secret sharing schemes in such a scenario, the likelihoods of both data loss and data theft are decreased. As far as we know, in many applications both perfect and non-perfect ramp secret sharing schemes can be used. In the perfect scheme, the size of a share must be at least that of the secret [5]. On the other hand, ramp secret sharing schemes allow shares to be smaller than the secret, which is what we concentrate on in this paper. Such schemes are particularly useful for storing bulk data [7].

A linear ramp secret sharing scheme can be described as a coset construction C_1/C_2 where $C_2 \subsetneq C_1$ are linear codes [6]. It was shown in [2], [28], [41] that the corresponding relative dimension/length

Published in IEEE Transactions on Information Theory, vol. 60, no. 10, pages 5938–5949 (2014).
This research is supported by the Danish National Research Foundation, the National Natural Science Foundation of China (Grant No. 11061130539 – the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography), Japan Society for the Promotion of Science (Grant Nos. 23246071 and 26289116), the Danish Council for Independent Research (Grant No. DFF–4002-00367), the Spanish MINECO (Grant No. MTM2012-36917-C03-03), National Basic Research Program of China (Grant No. 2013CB338004), and National Natural Science Foundation of China (Grant No. 61271222).

profile (RDLP) expresses the worst case information leakage to unauthorized sets in such a system. The RDLP was proposed by Luo et al. [30]. They [30] also proposed the relative generalized Hamming weight (RGHW) and its equivalence to the RDLP, similar to the one demonstrated by Forney [13] between the dimension/length profile and the generalized Hamming weight. The m-th RGHW expresses the smallest size of unauthorized sets that can obtain m q-bits [2], [28], where q is the size of the alphabet of $C_2 \subsetneq C_1$. In order to investigate the potential of linear codes to construct useful ramp secret sharing schemes, it is indispensable to study the RGHW and the RDLP. However, not much research has been done so far, partly because the connection between the secret sharing and RGHW/RDLP was only recently reported. In particular, few classes of linear codes have been examined for their RGHW/RDLP. In this paper we study the RGHW of general linear codes by the Feng-Rao approach [17], and explore its consequences for one-point algebraic geometry (AG) codes [43], [22] and, in particular the Hermitian codes [42], [40], [47].

The present paper starts with a discussion of known results regarding linear ramp secret sharing schemes and it continues with demonstrating that the RGHWs can also be used to express the best case information leakage. The main result of the paper is a method to estimate RGHW of one-point algebraic geometric codes. This is done by carefully applying the Feng-Rao bounds [17] for primary [1] as well as dual [11], [12], [37], [22], [32], [21] codes. From this we derive a relatively simple bound which uses information on the corresponding Weierstrass semigroup [24], [8]. As shall be demonstrated for Hermitian codes the new bound is often sharp. Moreover, for the same codes the RGHW are often much larger than the corresponding generalized Hamming weights (GHW) [44] which means that studies of RGHW cannot be substituted by those of GHW.

The paper is organized as follows. Section II describes the use of RGHW in connection with linear ramp secret sharing schemes, and in connection with communication over the wiretap channel of type II. In Section III we apply the theory to the special case of MDS codes. In Section IV we show – at the level of general linear codes – how to employ the Feng-Rao bounds to estimate RGHW. This method is then applied to one-point algebraic geometric codes in Section V. We investigate Hermitian codes in Section VI, and treat the corresponding ramp secret sharing schemes in Section VII.

II. Ramp secret sharing schemes and wiretap channels of type II

Ramp secret sharing schemes were introduced in [4], [46]. Let $\mathbb{F}_q$ be the finite field with q elements. A ramp secret sharing scheme with t-privacy and r-reconstruction is an algorithm that, given an input $\vec{s} \in \mathbb{F}_q^\ell$, outputs a vector $\vec{x} \in \mathbb{F}_q^n$, the vector of shares that we want to share among n players, such that, given a collection of shares $\{x_i \mid i \in \mathcal{I}\}$ where $\mathcal{I} \subseteq \{1, \ldots, n\}$, one has no information about $\vec{s}$ if $\#\mathcal{I} \leq t$ and one can recover $\vec{s}$ if $\#\mathcal{I} \geq r$ [6]. We shall always assume that t is largest possible and that r is smallest possible such that the above hold. We say that one has a t-threshold secret sharing scheme if $t = r + 1$.

We consider the secret sharing schemes introduced in [6, Section 4.2], which was the first general construction of ramp secret sharing schemes using arbitrary linear codes: Let $C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ be two linear codes. Set $k_2 = \dim(C_2)$ and $k_1 = \dim(C_1)$ and let $L \subsetneq \mathbb{F}_q^n$ be such that $C_1 = L \oplus C_2$ (direct sum). That is, $L \cap C_2 = \{\vec{0}\}$ and the union of a basis for L and a basis for C_2 constitutes a basis for C_1. We denote by $\ell = \dim(L) = \dim(C_1/C_2) = k_1 - k_2$.

We consider a secret $\vec{s} \in \mathbb{F}_q^\ell$; note that $\ell > 0$ since $C_1 \neq C_2$. We fix a vector space isomorphism $\psi : \mathbb{F}_q^\ell \to L$ which maps the secret $\vec{s} \in \mathbb{F}_q^\ell$ to L, and choose $\vec{c}_2 \in C_2$ randomly (uniformly distributed). Finally, consider $\vec{x} = \psi(\vec{s}) + \vec{c}_2 \in C_1$. The n shares consist of the n coordinates of $\vec{x}$; this scheme is clearly $\mathbb{F}_q$-linear [6]. One may also consider that the secret $\vec{s}$ is represented by the coset $\psi(\vec{s}) + C_2$ in C_1/C_2. Note that there are q^ℓ different cosets in C_1/C_2 and there are q^{k_2} possible representatives for every coset, i.e. for generating the shares of a secret $\vec{s}$. The schemes in [9], [31] form a particular case of the above scheme with $\ell = 1$.

Remark 1: All linear ramp secret sharing schemes with shares in $\mathbb{F}_q$ are of the above type. For constructions that use puncturing [31], [6, Sec. 4.1] we can take C_1, C_2 to be the punctured codes.
Let $\mathcal{I} \subseteq \mathcal{J} = \{1, \ldots, n\}$. We consider that an unauthorized set of participants obtains the shares $\{x_i \mid i \in \mathcal{I}\}$. We represent the shares by a random variable $\vec{X}$, and the shares obtained by an unauthorized set of participants by $f_{\mathcal{I}}(\vec{x}) = (x_i \mid i \in \mathcal{I})$ where $f_{\mathcal{I}} : \mathbb{F}_q^n \to \mathbb{F}_q^{\#\mathcal{I}}$. The amount of information in q-bits that the unauthorized set obtains is measured by $I(\vec{S}; f_{\mathcal{I}}(\vec{X}))$, the mutual information, where $\vec{S}$ is the random variable that represents the secrets, and $f_{\mathcal{I}}(\vec{X})$ is the random variable that represents the shares that an unauthorized set may obtain. We assume that both $\vec{S}$ and $\vec{X}$ are uniformly distributed. In particular we have t-privacy and r-reconstruction if t is largest possible and r is smallest possible such that $I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = 0$ for all $\#\mathcal{I} \leq t$ and $I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = \ell$ for all $\#\mathcal{I} \geq r$. A (non sharp) bound for r and t was given in [6]: $r < n - d(C_1)$ and $t > d(C_2^\perp)$ where $d(C_i)$ denotes the minimum distance of C_i, for $i = 1, 2$. The exact values can be derived from [28, Proof of Theorem 4] as

$$\begin{aligned} I(\vec{S}; f_{\mathcal{I}}(\vec{X})) &= \ell - \dim((V_{\overline{\mathcal{I}}} \cap C_1)/(V_{\overline{\mathcal{I}}} \cap C_2)), & (1)\\ &= \dim((C_2^\perp \cap V_{\mathcal{I}})/(C_1^\perp \cap V_{\mathcal{I}})), & (2)\end{aligned}$$

where $\overline{\mathcal{I}} = \mathcal{J} \setminus I$ and $V_{\mathcal{I}} = \{\vec{x} \in \mathbb{F}_q^n \mid x_i = 0 \text{ for all } i \notin \mathcal{I}\}$.

For the convenience of the reader we include the computation of the previous mutual information: since the variables $\vec{S}$ and $\vec{X}$ are uniformly distributed one has that $H_q(f_{\mathcal{I}}(\vec{X})) = \log_q \#f_{\mathcal{I}}(C_1) = \dim(f_{\mathcal{I}}(C_1)) = k_1 - \dim(\ker(f_{\mathcal{I}}) \cap C_1)$, and $H_q(f_{\mathcal{I}}(\vec{X})|S) = \log_q \#f_{\mathcal{I}}(C_2) = \dim(f_{\mathcal{I}}(C_2)) = k_2 - \dim(\ker(f_{\mathcal{I}}) \cap C_2)$. Here, H_q is the entropy function to base q. Therefore $I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = k_1 - k_2 - \big(\dim(\ker(f_{\mathcal{I}}) \cap C_1) - \dim(\ker(f_{\mathcal{I}}) \cap C_2)\big)$ and we obtain equation (1). Equation (2) follows from (1) and an extension of Forney's second duality lemma [27, Lemma 25]: Let $V \subseteq \mathbb{F}_q^n$, then

$$\begin{aligned} &\dim((C_2^\perp \cap V^\perp)/(C_1^\perp \cap V^\perp)) \\ = \;& \dim(C_1/C_2) - \dim((C_1 \cap V)/(C_2 \cap V)).\end{aligned}$$

In order to characterize the security of secret sharing schemes, one considers the jth relative dimension/length profile (RDLP) of two codes $C_2 \subsetneq C_1$ with $j \in \{1, \ldots, n\}$ [30]:

$$K_j(C_1, C_2) = \max_{\mathcal{I} \subseteq \mathcal{J}, \#\mathcal{I} = j} \dim((C_1 \cap V_{\mathcal{I}})/(C_2 \cap V_{\mathcal{I}})),$$

and the mth relative generalized Hamming weight (RGHW) with $m \in \{1, \ldots, \ell\}$ [30]:

$$M_m(C_1, C_2) = \min_{\mathcal{I} \subseteq \mathcal{J}} \{\#\mathcal{I} \mid \dim((C_1 \cap V_{\mathcal{I}})/(C_2 \cap V_{\mathcal{I}})) = m\}. \quad (3)$$

In this way the worst amount of information leakage of $\vec{s}$ from j shares is precisely characterized by the jth relative dimension/length profile of $C_2^\perp$ and $C_1^\perp$ [28, Theorem 4]:

$$\begin{aligned} &\max_{\mathcal{I} \subseteq \mathcal{J}, \#\mathcal{I} = j} I(\vec{S}; f_{\mathcal{I}}(\vec{X})) \\ = \;& \max_{\mathcal{I} \subseteq \mathcal{J}, \#\mathcal{I} = j} \dim((C_2^\perp \cap V_{\mathcal{I}})/(C_1^\perp \cap V_{\mathcal{I}})) \\ = \;& K_j(C_2^\perp, C_1^\perp).\end{aligned}$$

The smallest possible number of shares for which an unauthorized set of participants can determine m q-bits of information is

$$\begin{aligned} &\min_{\mathcal{I} \subseteq \mathcal{J}} \{\#\mathcal{I} \mid I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = m\} \\ = \;& \min_{\mathcal{I} \subseteq \mathcal{J}} \{\#\mathcal{I} \mid \dim((C_2^\perp \cap V_{\mathcal{I}})/(C_1^\perp \cap V_{\mathcal{I}})) = m\} \\ = \;& M_m(C_2^\perp, C_1^\perp).\end{aligned}$$

In particular $t = M_1(C_2^\perp, C_1^\perp) - 1$ [28, Theorem 9]. (See also [2, Th. 6.7] and for the special case of $\ell = 1$ [9, Cor. 1.7]). We now generalize the notion of t-privacy and r-reconstruction.

Definition 2: We say that a ramp secret sharing scheme has $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction if $t_1, \ldots, t_\ell$ are chosen largest possible and $r_1, \ldots, r_\ell$ are chosen smallest possible such that:

- an adversary cannot obtain m q-bits of information about $\vec{s}$ with any t_m shares,
- it is possible to recover m q-bits of information about $\vec{s}$ with any collection of r_m shares.

In particular, one has $t = t_1$ and $r = r_\ell$.

By our previous discussion one has that $t_m = M_m(C_2^\perp, C_1^\perp) - 1$ since $M_m(C_2^\perp, C_1^\perp)$ is the smallest size of a set of shares that can determine m q-bits of information about $\vec{s}$ [28, Theorem 4]. We will show that $(r_1, \ldots, r_\ell)$ can be characterized in terms of the RGHWs as well. Let r'_m be the largest size of a set of shares that cannot determine m q-bits of information about $\vec{s}$, i.e.

$$r'_m = \max_{\mathcal{I} \subseteq \mathcal{J}} \{ \#\mathcal{I} \mid I(\vec{S}; f(\vec{X})) < m \}. \tag{4}$$

This value is closely related to r_m since any strictly larger set of shares will determine m q-bits of information about $\vec{s}$ and thus

$$\begin{aligned}
& r_m \\
= \; & r'_m + 1 \\
= \; & \max_{\mathcal{I} \subseteq \mathcal{J}} \{ \#\mathcal{I} \mid I(\vec{S}; f_{\mathcal{I}}(\vec{X})) < m \} + 1 \\
= \; & \max_{\mathcal{I} \subseteq \mathcal{J}} \{ \#\mathcal{I} \mid I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = m - 1 \} + 1 \\
= \; & \max_{\mathcal{I} \subseteq \mathcal{J}} \{ \#\mathcal{I} \mid \dim((C_1 \cap V_{\overline{\mathcal{I}}})/(C_2 \cap V_{\overline{\mathcal{I}}})) = \\
& \quad \ell - m + 1 \} + 1, \text{ by (1)} \\
= \; & n - \min_{\overline{\mathcal{I}} \subseteq \mathcal{J}} \{ \#\overline{\mathcal{I}} \mid \dim((C_1 \cap V_{\overline{\mathcal{I}}})/(C_2 \cap V_{\overline{\mathcal{I}}})) = \\
& \quad \ell - m + 1 \} + 1 \\
= \; & n - M_{\ell - m + 1}(C_1, C_2) + 1.
\end{aligned} \tag{5}$$

In particular one has that $r = r_\ell = n - M_1(C_1, C_2) + 1$ [28, Theorem 9] (see also [9, Cor. 1.7] for the special case $\ell = 1$). We note that r'_m corresponds to the $(m-1)$th conjugate relative length/dimension profile in [48].

Theorem 3: Let C_1/C_2, where $\dim(C_1) - \dim(C_2) = \ell$, be a linear ramp secret sharing scheme with $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction. Then for $m = 1, \ldots, \ell$ we have $t_m = M_m(C_2^\perp, C_1^\perp) - 1$ and $r_m = n - M_{\ell - m + 1}(C_1, C_2) + 1$.

We shall relate the above concept of $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction to the literature: let $D_1 \subsetneq D_2 \subseteq \mathbb{F}_q^n$ be vector spaces of codimension ℓ and define for $1 \leq m \leq \ell$,

$$A_m(D_1, D_2) = \{ \mathcal{I} \subseteq \mathcal{J} \mid m = \dim(D_1 \cap V_{\mathcal{I}})/(D_2 \cap V_{\mathcal{I}}) \}.$$

Since $I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = \dim((C_2^\perp \cap V_{\mathcal{I}})/(C_1^\perp \cap V_{\mathcal{I}}))$ we have that, for $D_1 = C_2^\perp$ and $D_2 = C_1^\perp$, $A_m(D_1, D_2)$ is the collection of shares that give m q-bits of information about $\vec{S}$. In addition, $A_\ell(D_1, D_2)$ is the access structure in the sense of [25], and $A_m(D_1, D_2)$ is equivalent to A_m in [26, Definition 1].

In particular we are interested in the largest and smallest element of such a collection of shares

$$\begin{aligned}
& A_m^{\min}(D_1, D_2) \\
= \; & \{ \mathcal{I} \in A_m(D_1, D_2) \mid \nexists \mathcal{K} \in A_m(D_1, D_2) \text{ s.t. } \mathcal{K} \subsetneq \mathcal{I} \} \\
& A_m^{\max}(D_1, D_2) \\
= \; & \{ \mathcal{I} \in A_m(D_1, D_2) \mid \nexists \mathcal{K} \in A_m(D_1, D_2) \text{ s.t. } \mathcal{K} \supsetneq \mathcal{I} \}
\end{aligned}$$

and, as we are interested in its size, we define

$$\begin{aligned} A_m^d(D_1, D_2) &= \{\mathcal{I} \in A_m(D_1, D_2) \mid d = \#\mathcal{I}\} \\ A_m^{\min,d}(D_1, D_2) &= \{\mathcal{I} \in A_m^{\min}(D_1, D_2) \mid d = \#\mathcal{I}\} \\ A_m^{\max,d}(D_1, D_2) &= \{\mathcal{I} \in A_m^{\max}(D_1, D_2) \mid d = \#\mathcal{I}\}. \end{aligned}$$

Moreover, we are interested in the smallest and the largest size of a collection of shares that reveal m q-bits of information: the first one being the smallest $d \in \{1, \ldots, n\}$ such that $A_m^{\min,d}(D_1, D_2)$ is non-empty and it is equal to $M_m(D_1, D_2) = t_m + 1$. Analogously, the largest size of a collection of shares that reveals m q-bits of information is the largest $d \in \{1, \ldots, n\}$ such that $A_m^{\max,d}(D_1, D_2)$ is non-empty and it is equal to $n - M_{\ell-m+1}(C_1, C_2) + 1 = r_m$.

Ramp secret sharing schemes with $\ell > 1$ are relevant in the situation where the set of possible secrets is large but one wants to keep the size of each share small. A further motivation for considering $\ell > 1$ is the analogy to the wiretap channels of type II [45], [36]. Recall that this model involves a main channel from Alice to Bob which is assumed to be error and erasure free, and a secondary channel from Alice to the eavesdropper Eve which is a q-ary erasure channel. Consider the slightly more general situation where also the main channel is a q-ary erasure channel [41]. Assuming that the probability of erasure is much smaller on the main channel than on the secondary channel we see that to achieve reliable and secure communication we should use long codes $C_2 \subsetneq C_1$. To retain a positive information rate on the main channel we therefore need $\ell > 1$. The exact values of the mutual information on the main and the secondary channel could be calculated from $A_m(D_1, D_2)$, $m = 1, \ldots, \ell$ and the erasure probabilities of the two channels; but it seems a difficult task to determine $A_m(D_1, D_2)$ even for simple codes. Finding $M_m(D_1, D_2) = t_m + 1$ and $n - M_{\ell-m+1}(C_1, C_2) + 1 = r_m$, however, would be a first step in this direction. As we shall see in the following, for many codes we can easily estimate these last mentioned parameters.

In the remaining part of this paper we shall concentrate on methods to estimate RGHW. We shall need the following definition which by [29] is equivalent to (3) (see also [2, Def. 6.2]).

Definition 4: Let $C_2 \subsetneq C_1$ be linear codes over $\mathbb{F}_q$. For $m = 1, \ldots, \dim(C_1) - \dim(C_2)$ the mth relative generalized Hamming weight is defined as

$$\begin{aligned} M_m(C_1, C_2) = \min\{&\#\text{Supp}\, D \mid D \text{ is a subspace of } C_1, \\ &\dim(D) = m, D \cap C_2 = \{\vec{0}\}\}. \end{aligned}$$

From this definition the connection between the RGHW and the generalized Hamming weight (GHW) becomes clear – the latter being $d_m(C_1) = M_m(C_1, C_2)$ with $C_2 = \{\vec{0}\}$. Before embarking with more general classes of codes in the next section we discuss the parameters t_m, r_m in the case of MDS codes.

III. Ramp schemes based on MDS codes

Let C be an MDS code of dimension k. Then $C^\perp$ is also MDS and consequently

$$d_m(C) = n - k + m, \qquad m = 1, \ldots, k \tag{6}$$

$$d_m(C^\perp) = k + m, \qquad m = 1, \ldots, n - k \tag{7}$$

which means that all generalized Hamming weights attain the Singleton bound. Consider two MDS codes $C_2 \subsetneq C_1$ with $\dim(C_1) = k_1$ and $\dim(C_2) = k_2$. By definition, $M_m(C_1, C_2) \geq d_m(C_1)$, $m = 1, \ldots, \ell = k_1 - k_2$. However, the Singleton bound for RGHW is identical to the Singleton bound for GHW [30, Sec. IV] and therefore $M_m(C_1, C_2) = d_m(C_1)$ and $M_m(C_2^\perp, C_1^\perp) = d_m(C_2^\perp)$ [41]. Based on (6) and (7) one can show that

$$M_m(C_2^\perp, C_1^\perp) = n - M_{\ell-m+1}(C_1, C_2) + 1, \tag{8}$$

and from Theorem 3 it now follows that if we base a ramp scheme on two MDS codes then the size of a group uniquely determines how much information it can reveal:

$$t_m = r_m - 1, \;\; t_{m+1} = t_m + 1, \;\; t_1 = k_2, \;\; r_\ell = k_1.$$

When the number of participants is larger than two times the field size minus 1 then by [23, Cor. 7.4.4] C_1 and C_2 cannot be MDS – unless $k_1 = n-1$ and $k_2 = 1$ – and consequently we can no longer assume (8). What is obviously needed is a method to estimate the left and the right side of (8) for codes of any length. As shall be demonstrated in the following the Feng-Rao method makes this possible.

IV. The Feng-Rao bounds for RGHW

The Feng-Rao bounds come in two versions: One for primary codes [1], [18], [17] and the other for dual codes [10], [11], [12], [37], [22], [32]. The most general formulations deal with arbitrary linear codes, whereas more specialized formulations – such as the order bounds – require that the code construction is supported by certain types of algebraic structures. The bounds have been applied to the minimum distance, the generalized Hamming weights – and for the case of dual codes of co-dimension 1 – also the relative minimum distance [9]. It is not difficult to extend the method for estimating GHW to a method for estimating RGHW. In the following we give the details for primary codes in the language of general linear codes. The details for dual codes are similar, hence for these codes we shall give a more brief description.

We start by introducing some terminology that shall be used throughout the section. Let $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ be a fixed basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$ and write $\mathcal{J} = \{1, \ldots, n\}$.

Definition 5: The function $\bar{\rho} : \mathbb{F}_q^n \to \mathcal{J} \cup \{0\}$ is given as follows. For non-zero $\vec{c}$ we have $\bar{\rho}(\vec{c}) = i$ where i is the unique integer such that

$$\vec{c} \in \text{Span}\{\vec{b}_1, \ldots, \vec{b}_i\} \backslash \text{Span}\{\vec{b}_1, \ldots, \vec{b}_{i-1}\}.$$

Here we used the convention that $\text{Span}\,\emptyset = \{\vec{0}\}$. Finally, $\bar{\rho}(\vec{0}) = 0$.

The component wise product of two vectors in $\mathbb{F}_q^n$ plays a fundamental role in our exposition. This product is given by

$$(\alpha_1, \ldots, \alpha_n) * (\beta_1, \ldots, \beta_n) = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n).$$

Definition 6: An ordered pair $(i, j) \in \mathcal{J} \times \mathcal{J}$ is said to be one-way well-behaving (OWB) if $\bar{\rho}(\vec{b}_{i'} * \vec{b}_j) < \bar{\rho}(\vec{b}_i * \vec{b}_j)$ holds true for all $i' \in \mathcal{J}$ with $i' < i$.

Definition 7: For $i \in \mathcal{J}$ define

$$\begin{aligned} \Lambda_i \;\; = \;\; & \{l \in \mathcal{J} \mid \exists\, j \in \mathcal{J} \text{ such that } (i, j) \text{ is OWB and} \\ & \bar{\rho}(\vec{b}_i * \vec{b}_j) = l\}. \end{aligned}$$

As is easily seen – if $D \subseteq \mathbb{F}_q^n$ is a vector space of dimension m then it holds that $\#\bar{\rho}\big(D\backslash\{\vec{0}\}\big) = m$. (Actually, any set $\{\vec{d}_1, \ldots, \vec{d}_m\} \subseteq D\backslash\{\vec{0}\}$ with $\bar{\rho}(\vec{d}_1) < \cdots < \bar{\rho}(\vec{d}_m)$ constitutes a basis for D). The following result is a slight modification of the material in [1].

Proposition 8: Let $D \subseteq \mathbb{F}_q^n$ be a vector space of dimension at least 1. The support size of D satisfies

$$\#\text{Supp}(D) \geq \# \cup_{i \in \bar{\rho}(D\backslash\{\vec{0}\})} \Lambda_i. \tag{9}$$

Proof: Let $l_1 < \cdots < l_\sigma$ be the elements in $\cup_{i \in \bar{\rho}(D\backslash\{\vec{0}\})} \Lambda_i$ and let $i_1, \ldots, i_\sigma$ and $j_1, \ldots, j_\sigma$ be such that for $s = 1, \ldots, \sigma$ it holds that:

- $i_s \in \bar{\rho}(D\backslash\{\vec{0}\})$,
- (i_s, j_s) is OWB and $\bar{\rho}(\vec{b}_{i_s} * \vec{b}_{j_s}) = l_s$.

Choose $\vec{d}_1, \ldots \vec{d}_\sigma \in D$ with $\bar{\rho}(\vec{d}_s) = i_s$, $s = 1, \ldots, \sigma$. Clearly $\bar{\rho}(\vec{d}_s * \vec{b}_{j_s}) = l_s$ and therefore $\vec{d}_1 * \vec{b}_{j_1}, \ldots, \vec{d}_\sigma * \vec{b}_{j_\sigma}$ are linearly independent. In conclusion $D * \mathbb{F}_q^n = \{\vec{d} * \vec{c} \mid \vec{d} \in D, \vec{c} \in \mathbb{F}_q^n\}$ is of dimension at least σ. The dimension of $D * \mathbb{F}_q^n$ equals the size of the support of D and the proposition follows. ■

We now turn to RGHW. Observe that although $C_2 \subsetneq C_1$ implies $\bar{\rho}(C_2) \subsetneq \bar{\rho}(C_1)$, it does not always hold that $\vec{c} \in C_1 \backslash C_2$ implies $\bar{\rho}(\vec{c}) \in \bar{\rho}(C_1) \backslash \bar{\rho}(C_2)$. However, some observations can still be made.

Theorem 9: Consider linear codes $C_2 \subsetneq C_1$, $\dim(C_1) = k_1$, $\dim(C_2) = k_2$. Let u be the smallest element in $\bar{\rho}(C_1)$ that is not in $\bar{\rho}(C_2)$. For $m = 1, \ldots, k_1 - k_2$ we have

$$\begin{aligned} M_m(C_1, C_2) \;\; \geq \;\; & \min \big\{ \# \cup_{s=1}^{m} \Lambda_{i_s} \mid u \leq i_1 < \cdots < i_m, \\ & i_1, \ldots, i_m \in \bar{\rho}(C_1 \backslash \{\vec{0}\}) \big\}. \end{aligned}$$

Proof: If D is an m-dimensional subspace of C_1 with $D \cap C_2 = \{\vec{0}\}$ then we can write $\bar{\rho}(D \backslash \{\vec{0}\}) = \{i_1, \ldots, i_m\} \subseteq \bar{\rho}(C_1 \backslash \{\vec{0}\})$ with $u \leq i_1 < \cdots < i_m$. The theorem now follows from Proposition 8. ■

Corollary 10: Consider a k_1-dimensional code C_1, say $C_1 = \text{Span}\{\vec{f}_1, \ldots, \vec{f}_{k_1}\}$, where without loss of generality we assume $\bar{\rho}(\vec{f}_1) < \cdots < \bar{\rho}(\vec{f}_{k_1})$. For $k_2 < k_1$ let $C_2 = \text{Span}\{\vec{f}_1, \ldots, \vec{f}_{k_2}\}$. We have

$$\begin{aligned} M_m(C_1, C_2) \;\; \geq \;\; & \min \big\{ \# \cup_{s=1}^{m} \Lambda_{i_s} \mid i_1 < \cdots < i_m, \\ & i_1, \ldots, i_m \in \{\bar{\rho}(\vec{f}_{k_2+1}), \ldots, \bar{\rho}(\vec{f}_{k_1})\} \big\}. \end{aligned}$$

Next we treat dual codes.

Definition 11: For $\vec{c} \in \mathbb{F}_q^n \backslash \{\vec{0}\}$ define $M(\vec{c})$ to be the smallest number $i \in \mathcal{J}$ such that $\vec{c} \cdot \vec{b}_i \neq 0$. Here $\vec{a} \cdot \vec{b}$ means the usual inner product between $\vec{a}$ and $\vec{b}$.

It is clear that for an m-dimensional space D we have $\# M(D \backslash \{\vec{0}\}) = m$. Also it is clear that if $D \subseteq C^\perp$, where C is a linear code, then $M(D \backslash \{\vec{0}\}) \cap \bar{\rho}(C) = \emptyset$.

Definition 12: For $l \in \mathcal{J}$ define

$$V_l = \{i \in \mathcal{J} \mid \bar{\rho}(\vec{b}_i * \vec{b}_j) = l \text{ for some } \vec{b}_j \in \mathcal{B} \text{ with } (i, j) \text{ OWB}\}.$$

The following result is proved by slightly modifying the proof of [21, Prop. 3.12] and [20, Th. 5].

Proposition 13: Let $D \subseteq \mathbb{F}_q^n$ be a space of dimension at least 1. We have

$$\#\text{Supp}(D) \geq \# \cup_{l \in M(D \backslash \{\vec{0}\})} V_l.$$

From the above discussion we derive

Theorem 14: Consider linear codes $C_2 \subsetneq C_1$. Let u be the largest element in $\bar{\rho}(C_1 \backslash \{\vec{0}\})$. For $m = 1, \ldots, \dim(C_1) - \dim(C_2) = \dim(C_2^\perp) - \dim(C_1^\perp)$ we have

$$\begin{aligned} & M_m(C_2^\perp, C_1^\perp) \geq \min\{ \# \cup_{s=1}^{m} V_{i_s} \mid \\ & \quad 1 \leq i_1 < \cdots < i_m \leq u, i_1, \ldots, i_m \notin \bar{\rho}(C_2) \}. \end{aligned} \tag{10}$$

To apply Theorem 9, Corollary 10 and Theorem 14 we need information on which pairs are OWB. This suggests the use of a supporting algebra. One class of algebras that works well is the order domains [22], [35], [19]. In the present paper we will concentrate on the most prominent example of order domain codes – namely one-point algebraic geometric codes.

Remark 15: In our exposition we used a single (but arbitrary) basis $\mathcal{B}$ for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. Following [37] one could reformulate all the above results in a more general setting that uses three bases $\mathcal{U}$, $\mathcal{V}$, and $\mathcal{W}$. This point of view is important when one considers affine variety codes [38], but it does not improve the results for order domain codes. In [14] and [15], the concept of OWB was relaxed giving new improved Feng-Rao bounds. All the above results could be reformulated in this setting – but again – for order domain codes the results stay unchanged.

V. One-point algebraic geometric codes

Given an algebraic function field F of transcendence degree one, let $P_1, \ldots, P_n$, Q be distinct rational places. For $f \in F$ write $\rho(f) = -\nu_Q(f)$, where ν_Q is the valuation at Q, and denote by $H(Q)$ the Weierstrass semigroup of Q. That is, $H(Q) = \rho\big(\cup_{\mu=0}^{\infty} \mathcal{L}(\mu Q)\big)$. In the following let $\{f_\lambda \mid \lambda \in H(Q)\}$ be any fixed basis for $R = \cup_{\mu=0}^{\infty}\mathcal{L}(\mu Q)$ with $\rho(f_\lambda) = \lambda$ for all $\lambda \in H(Q)$. Let $D = P_1 + \cdots + P_n$ and define

$$\begin{aligned} H^*(Q) &= \{\mu \mid C_{\mathcal{L}}(D, \mu Q) \neq C_{\mathcal{L}}(D, (\mu-1)Q)\} \\ &= \{\gamma_1, \ldots, \gamma_n\} \subsetneq H(Q). \end{aligned} \tag{11}$$

Here, the enumeration is chosen such that $\gamma_1 < \cdots < \gamma_n$. Consider the map $\mathrm{ev} : F \to \mathbb{F}_q^n$ given by $\mathrm{ev}(f) = (f(P_1), \ldots, f(P_n))$. The set

$$\{\vec{b}_1 = \mathrm{ev}(f_{\gamma_1}), \ldots, \vec{b}_n = \mathrm{ev}(f_{\gamma_n})\} \tag{12}$$

clearly is a basis for $\mathbb{F}_q^n$ and by [1, Pro. 27] a pair (i, j) is OWB if $\rho(f_{\gamma_i}) + \rho(f_{\gamma_j}) = \rho(f_{\gamma_l})$, i. e. $\gamma_i + \gamma_j = \gamma_l$, in which case of course $\bar{\rho}(\vec{b}_i * \vec{b}_j) = l$. From [1, Pro. 28] we know that if $\delta \in H^*(Q)$ and $\alpha, \beta \in H(Q)$ satisfy $\alpha + \beta = \delta$ then we have $\alpha, \beta \in H^*(Q)$. We therefore get the following lemma.

Lemma 16: Let $\{\vec{b}_1, \ldots, \vec{b}_n\}$ be as above. For $i \in \mathcal{J}$ it holds that

$$\{l \in \mathcal{J} \mid \gamma_l - \gamma_i \in H(Q)\} \subseteq \Lambda_i$$

where Λ_i is as in Definition 7.

Proposition 17: Let $D \subseteq \mathbb{F}_q^n$ be a vector space of dimension m. There exist unique numbers $\gamma_{i_1} < \cdots < \gamma_{i_m}$ in $H^*(Q)$ such that $\bar{\rho}(D \backslash \{\vec{0}\}) = \{i_1, \ldots, i_m\}$. The support of D satisfies

$$\#\mathrm{Supp}(D) \geq \#\Big(H^*(Q) \cap \big(\cup_{s=1}^{m} (\gamma_{i_s} + H(Q))\big)\Big) \tag{13}$$

$$\begin{aligned} &\geq n - \gamma_{i_m} + \#\{\lambda \in \cup_{s=1}^{m-1}(\gamma_{i_s} + H(Q)) \mid \\ &\qquad \lambda \notin \gamma_{i_m} + H(Q)\}. \end{aligned} \tag{14}$$

Proof: By Lemma 16 the right side of (13) is lower than or equal to $\#\cup_{s=1}^{m} \Lambda_{i_s}$, and (13) therefore follows from Proposition 8. Another way of writing the right side of (13) is $n - \#\big(H^*(Q) \backslash \cup_{s=1}^{m} (\gamma_{i_s} + H(Q))\big)$. This number is greater than or equal to

$$\begin{aligned} & n - \#\big(H(Q) \backslash \cup_{s=1}^{m} (\gamma_{i_s} + H(Q))\big) \\ = \; & n - \#\big(H(Q) \backslash (\gamma_{i_m} + H(Q))\big) \\ & \quad + \#\left\{\lambda \in \cup_{s=1}^{m-1}(\gamma_{i_s} + H(Q)) \mid \lambda \notin \gamma_{i_m} + H(Q)\right\}. \end{aligned}$$

From [22, Lem. 5.15] we know that for any numerical semigroup Γ and $\lambda \in \Gamma$, one has $\lambda = \#\big(\Gamma \backslash (\lambda + \Gamma)\big)$. In particular $\#\big(H(Q) \backslash (\gamma_{i_m} + H(Q))\big) = \gamma_{i_m}$ and (14) follows. ∎

From (14) we can obtain a manageable bound on the RGHWs of one-point algebraic geometric codes as we now explain. This bound can even be used when one does not know $H^*(Q)$. Given non-negative integers $\lambda_1 < \cdots < \lambda_m$ (note that we make no assumptions that $\lambda_1, \ldots, \lambda_m \in H(Q)$) let $i_j = \lambda_j - \lambda_m$, $j = 1, \ldots, m-1$ and observe that

$$\begin{aligned} &\#\{\lambda \in \cup_{s=1}^{m-1}(\lambda_i + H(Q) \mid \lambda \notin \lambda_m + H(Q)\} \\ &\qquad = \#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\} \end{aligned} \tag{15}$$

since λ is in the first set if and only if $\lambda - \lambda_m$ is in the second set. The function Z in the definition below shall help us estimate the last expression in (14).

Definition 18: Consider a numerical semigroup Γ and a positive integer μ. Define $Z(\Gamma,\mu,1)=0$ and for $1<m\leq\mu$

$$\begin{aligned} Z(\Gamma,\mu,m) &= \min\big\{\#\{\alpha\in\cup_{s=1}^{m-1}(i_s+\Gamma)\mid\alpha\notin\Gamma\}\mid \\ &\quad -\mu+1\leq i_1<\cdots<i_{m-1}\leq -1\big\}. \end{aligned} \tag{16}$$

We are now ready for the main result of the section.

Theorem 19: Let μ_1,μ_2 be positive integers with $\mu_2<\mu_1$.
For $m=1,\ldots,\dim(C_{\mathcal{L}}(D,\mu_1Q))-\dim(C_{\mathcal{L}}(D,\mu_2Q))$ we have

$$\begin{aligned} & M_m(C_{\mathcal{L}}(D,\mu_1Q),C_{\mathcal{L}}(D,\mu_2Q)) \\ \geq\ & \min\Big\{\#\big(H^*(Q)\cap\big(\cup_{s=1}^{m}(\gamma_{i_s}+H(Q))\big)\big)\mid \\ & \gamma_{i_1},\ldots,\gamma_{i_m}\in H^*(Q),\mu_2<\gamma_{i_1}<\cdots<\gamma_{i_t}\leq\mu_1\Big\} \end{aligned} \tag{17}$$

$$\begin{aligned} \geq\ & \min\Big\{n-\gamma_{i_m}+ \\ & \#\{\lambda\in\cup_{s=1}^{m-1}(\gamma_{i_s}+H(Q))\mid\lambda\notin\gamma_{i_m}+H(Q)\}\mid \\ & \gamma_{i_1},\ldots,\gamma_{i_m}\in H^*(Q),\mu_2<\gamma_{i_1}<\cdots<\gamma_{i_t}\leq\mu_1\Big\} \end{aligned} \tag{18}$$

$$\geq\ n-\mu_1+Z(H(Q),\mu,m), \tag{19}$$

where $\mu=\mu_1-\mu_2$.

Proof: Consider an m-dimensional vector space $D\subseteq C_{\mathcal{L}}(D,\mu_1Q)$ with $D\cap C_{\mathcal{L}}(D,\mu_2Q)=\{\vec{0}\}$. Let $\gamma_{i_1}<\cdots<\gamma_{i_m}$ be as described in Theorem 17. By the definition of the codes we have $\gamma_{i_1},\ldots,\gamma_{i_m}\in\{\mu_2+1,\ldots,\mu_1\}$ (this is the situation of Corollary 10). Consequently (17) and (18), respectively, follow from (13) and (14), respectively. We have $-\mu_1\leq-\gamma_{i_m}$. Similarly, by (15) $Z(H(Q),\mu,m)$ is smaller than or equal to the last term in (14). These observations prove (19). ■

Note that (19) may be strictly smaller than (18). Firstly, μ_1 may not belong to $H^*(Q)$. Secondly, when applying the function $Z(H(Q),\mu,m)$ we do not discard the numbers in $\{\mu_2+1,\ldots,\mu_1-1\}$ that are gaps of $H(Q)$, and least of all the numbers in the interval that are not present in $H^*(Q)$. The connection to the usual Goppa bound for primary codes is seen from the expression in (19): letting $m=1$ we get by Definition 18 $Z(H(Q),\mu,m)=0$ and the formula simplifies to the well-known bound on the minimum distance $d\big(C_{\mathcal{L}}(D,\mu_1Q)\big)\geq n-\mu_1$.

For duals of one-point algebraic geometric codes we have a bound similar to (17), but no bounds similar to (18) or (19).

Theorem 20: Let μ_1,μ_2 and m be as in Theorem 19. We have

$$\begin{aligned} & M_m(C_{\mathcal{L}}^{\perp}(D,\mu_2Q),C_{\mathcal{L}}^{\perp}(D,\mu_1Q)) \\ \geq\ & \min\Big\{\#\big(H(Q)\cap\big(\cup_{s=1}^{m}(\gamma_{i_s}-H(Q))\big)\big)\mid \\ & \gamma_{i_1},\ldots,\gamma_{i_m}\in H^*(Q),\mu_2<\gamma_{i_1}<\cdots<\gamma_{i_m}\leq\mu_1\Big\}. \end{aligned} \tag{20}$$

VI. RGHWs of Hermitian codes

In this section we apply the results of Section V to the case of Hermitian codes [42], [40]. Our main result is that (19) is often tight. The Hermitian function field over $\mathbb{F}_{q^2}$ (q a prime power) is given by the equation $x^{q+1} - y^q - y$ and it possesses exactly $q^3 + 1$ rational places which we denote $P_1, \ldots, P_{q^3}, Q$ – the last being the pole of x. The Weierstrass semigroup of Q, $H(Q) = \langle \rho(x) = q, \rho(y) = q + 1 \rangle$, has $g = q(q-1)/2$ gaps and conductor $c = q(q-1)$. Let $D = P_1 + \cdots + P_{q^3}$. In the following by a Hermitian code we mean a code of the form $C_{\mathcal{L}}(D, \mu Q)$. Clearly, this code is of length $n = q^3$. As is well-known the dual of a Hermitian code is a Hermitian code. This fact will be useful when in a later section we consider ramp schemes based on Hermitian codes. We start our investigation with a lemma that treats a slightly more general class of semigroups than the semigroup $\langle q, q+1 \rangle$ relevant to us.

Lemma 21: Let a be an integer, $a \geq 2$. Define $\Gamma = \langle a, a+1 \rangle$. For integers m, μ with $1 \leq m \leq \mu \leq a+1$ it holds that

$$Z(\Gamma, \mu, m) = \sum_{s=0}^{m-2} (a - s) = a(m-1) - (m-2)(m-1)/2. \tag{21}$$

Proof: Recall that a positive integer λ is called a gap of Γ if $\lambda \notin \Gamma$. All other non-negative integers are called non-gaps. For the given semigroup Γ the set of non-negative integers consists of one non-gap followed by $a-1$ gaps, then two non-gaps followed by $a-2$ gaps and so on up to $a-1$ non-gaps followed by $a-(a-1) = 1$ gap. All the following numbers are non-gaps. We denote the above maximal sequences of consecutive gaps $G_1, \ldots, G_{a-1}$ with $\#G_v = a - v$, $v = 1, \ldots, a-1$ (such sequences are called deserts in [34, Ex. 3]).
First assume $1 \leq m \leq \mu \leq a+1$. Let $-\mu \leq i_1 < \ldots < i_{m-1} \leq -1$. We have

$$\#G_v \cap \left(\cup_{s=1}^{m-1} (i_s + \Gamma) \right) \geq \min\{\#G_v, m-1\}$$

with equality when $i_{m-1} = -1, i_{m-2} = -2, \ldots, i_1 = -(m-1)$. Summing up the contribution from all G_v accounts for $\sum_{s=1}^{m-2}(a-s)$. The term in (21) corresponding to $s = 0$, namely a, comes from considering the number of negative integers in $\sum_{s=1}^{m-1}(i_s + \Gamma)$. Thus we have established (21). ∎

Recall from Theorem 19 that we have three bounds on the RGHW of which (19) is the weakest. Using Lemma 21, for Hermitian codes of codimension at most $q+1$, (19) translates into a closed-formula expression in (22). Surprisingly, this expression is often equal to the true value of the RGHW.

Theorem 22: Consider the Hermitian curve $x^{q+1} - y^q - y$ over $\mathbb{F}_{q^2}$. Let $P_1, \ldots, P_{n=q^3}$, and Q be the rational places and $D = P_1 + \cdots + P_n$. Let μ_1, μ_2 be non-negative integers with $1 \leq \mu_1 - \mu_2 \leq q+1$. For $1 \leq m \leq \dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q))$ we have

$$\begin{aligned} & M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \\ \geq \; & n - \mu_1 + \sum_{s=0}^{m-2} (q - s) \\ = \; & n - \mu_1 + q(m-1) - (m-2)(m-1)/2. \end{aligned} \tag{22}$$

If

$$c - 1 \leq \mu_2 \text{ and } \mu_1 < n - c. \tag{23}$$

(recall that $c = q(q-1)$) then we have $\dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q)) = \mu_1 - \mu_2$ and equality in (22).

Proof: Equation (22) is a consequence of the last part of Theorem 19 and the first part of Lemma 21. The result concerning the dimensions is well-known. That equality holds in (22) under condition (23) follows from Lemma 23 below. ∎

Lemma 23: Let μ_1 and m be positive integers with $m \leq q+1$, $\mu_1 < n-c$ and $c-1 < \mu_1 - (m-1)$. Then there exist m functions $f_0, \ldots, f_{m-1}$ such that

- $f_i \in \mathcal{L}((\mu_1 - i)Q) \backslash \mathcal{L}((\mu_1 - (i+1))Q)$, $i = 0, \ldots, m-1$.
- The number of common zeros of $f_0, \ldots, f_{m-1}$ is exactly $\mu_1 - \sum_{i=0}^{m-2}(q-i)$.

Proof: As is well-known $\cup_{\mu=0}^{\infty}\mathcal{L}(\mu Q)$ is isomorphic to $\mathbb{F}_{q^2}[X,Y]/I$, where $I = \langle X^{q+1} - Y^q - Y \rangle$. The isomorphism is given by $\varphi(x) = X + I$ and $\varphi(y) = Y + I$. We call $X^{q+1} - Y^q - Y = \mathrm{N}(X) - \mathrm{Tr}(Y)$ the Hermitian polynomial – N being the norm and Tr the trace corresponding to the field extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. In this description the rational places $P_1, \ldots, P_{q^3}$ correspond to the affine points of the Hermitian polynomial. We remind the reader of the following few facts which play a crucial role in the below induction proofs:

- For any $\delta \in \mathbb{F}_{q^2}$ we have $\mathrm{N}(\delta), \mathrm{Tr}(\delta) \in \mathbb{F}_q$.
- For every $\epsilon \in \mathbb{F}_q$ there exists exactly q different δ such that $\mathrm{Tr}(\delta) = \epsilon$.
- There exist exactly $q+1$ different δ such that $\mathrm{N}(\delta) = 1$.

We start by fixing some notation. Let $\{\alpha_1, \ldots, \alpha_q\}$ be the elements in $\mathbb{F}_{q^2}$ that map to 1 under Tr. Let $\{\beta_1, \ldots, \beta_{q^2-(q+1)}\}$ be the elements that do not map to 1 under N and $\{\gamma_1, \ldots, \gamma_{q+1}\}$ the elements that do.

Write $\mu_1 = iq + j(q+1)$ with $0 \leq j < q$. First assume $1 \leq m \leq j+1$ and that $i < q^2 - q$. By induction on m (in this interval) one can show that the set $\{F_0, F_1, \ldots, F_{m-1}\}$ where

$$F_0 = \big(\prod_{s=1}^{i}(X-\beta_s)\big)\big(\prod_{s=1}^{j}(Y-\alpha_s)\big), \tag{24}$$

$$F_1 = \big(\prod_{s=1}^{i}(X-\beta_s)\big)(X-\gamma_1)\big(\prod_{s=1}^{j-1}(Y-\alpha_s)\big), \tag{25}$$

$$\vdots$$

$$F_{m-1} = \big(\prod_{s=1}^{i}(X-\beta_s)\big)\big(\prod_{s=1}^{m-1}(X-\gamma_s)\big)\big(\prod_{s=1}^{j-m+1}(Y-\alpha_s)\big), \tag{26}$$

has exactly $iq + j(q+1) - \sum_{s=0}^{m-2}(q-s)$ zeros in common with the Hermitian polynomial $X^{q+1} - Y^q - Y$ (we leave the technical details for the reader).

Finally, assume $j+1 \leq m \leq j+q$. By induction on m (in this interval) one can show that the set

$\{F_0, F_1, \ldots, F_{m-1}\}$ where

$$
\begin{aligned}
F_0 &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-j}(X-\gamma_s)\Big) \\
&\quad \Big(\prod_{s=1}^{j}(Y-\alpha_s)\Big), \qquad (27)\\
F_1 &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-j+1}(X-\gamma_s)\Big) \\
&\quad \Big(\prod_{s=1}^{j-1}(Y-\alpha_s)\Big), \qquad (28)\\
&\vdots \\
F_j &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q}(X-\gamma_s)\Big), \qquad (29)\\
F_{j+1} &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-1}(Y-\alpha_s)\Big), \\
F_{j+2} &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-2}(Y-\alpha_s)\Big)(X-\gamma_1), \\
&\vdots \\
F_{m-1} &= \Big(\prod_{s=1}^{i-q+j}(X-\beta_s)\Big)\Big(\prod_{s=1}^{q-m+j+1}(Y-\alpha_s)\Big) \\
&\quad \Big(\prod_{s=1}^{m-j-2}(X-\gamma_s)\Big),
\end{aligned}
$$

has exactly $iq+j(q+1)-\sum_{s=0}^{m}(q-s)$ zeros in common with the Hermitian polynomial $X^{q+1}-Y^q-Y$ (again we leave the technical details for the reader). For simplicity we covered the case $m=j+1$ and $i<q^2-q$ in both induction proofs. Observe that the basis step $m=j+1$ of the last induction proof corresponds to the terms in (27), (28), (29) which are different from (24), (25), (26) with $m=j+1$. ■

For $1 \le m \le \mu_1-\mu_2 \le q+1$ but with μ_1 and μ_2 not satisfying the condition in (23) we can often derive much better estimates than (22).

For $\mu_2 < c-1$ it may happen that not all of the numbers $\mu_1, \mu_1-1, \ldots, \mu_1-(m-1)$ belong to $H(Q)$, and so the worst case in the proof of Theorem 19 may not be realized. Hence, we should rather apply (18) or (17) (which in this situation are equivalent).

For $n-c \le \mu_1$ it may happen that $H^*(Q)\backslash(\mu_1+H(Q))$ is strictly smaller than $H(Q)\backslash(\mu_1+H(Q))$ (this will happen if $\mu_1 = iq+j(q+1)$, with $q^2-q \le i < q^2$ and $0<j<q$). In such a case $\#\big(H^*(Q)\cap(\mu_1+H(Q))\big)$ will be strictly larger than $n-\mu_1$. Moreover, all the numbers $\mu_1, \mu_1-1, \ldots, \mu_1-(m-1)$ need not belong to $H^*(Q)$ (this may happen if $\mu_1 \ge n$) and again the worst case considered in the proof of Theorem 19 may not be realizable. In this situation we should rather apply (17).

We illustrate our observations with three examples. The first two are concerned with $\mu_2 < c-1$ and the last with $n-c \le \mu_1$.

Example 1: In this example we consider codes over $\mathbb{F}_{q^2} = \mathbb{F}_{16}$. Hence, $q = 4$, $H(Q) = \langle 4, 5\rangle$ and $n = 64$. The first numbers of $H^*(Q)$ (and $H(Q)$) are $0, 4, 5, 8, 9, 10, 12$. Hence, $dimC_{\mathcal{L}}(D, 8Q) = 4$, $dimC_{\mathcal{L}}(D, 12Q) = 7$. Theorem 22 tells us that $M_m(C_{\mathcal{L}}(D, 12Q), C_{\mathcal{L}}(D, 8Q))$ is at least 52, 56 and 59, for m equal to 1, 2 and 3, respectively. Using (18) we now show that for $m = 2$ and $m = 3$ the true values are at least 58 and 60, respectively. We first concentrate on $m = 2$. Using the notation from Proposition 17 we must investigate all $\gamma_{i_1}, \gamma_{i_2} \in \{9, 10, 12\}$ with $\gamma_{i_1} < \gamma_{i_2}$, We have three different choices of $(\gamma_{i_1}, \gamma_{i_2})$ to consider, namely $(10, 12)$, $(9, 12)$ and $(9, 10)$. We first observe that

$$\begin{aligned} 12 + H(Q) &= \{12, 16, 17, 20, 21, 22, 24, \ldots\} \\ 10 + H(Q) &= \{10, 14, 15, 18, 19, 20, 22, 23, 24, \ldots\} \\ 9 + H(Q) &= \{9, 13, 14, 17, 18, 19, 21, 22, 23, 24, \ldots\}. \end{aligned}$$

Note that if $\alpha \in H(Q)\backslash(\lambda + H(Q))$ for $\lambda \in \{9, 10, 12\}$ then also $\alpha \in H^*(Q)$.

$\underline{(\gamma_{i_1}, \gamma_{i_2}) = (10, 12)}$: We have

$$\begin{aligned} \#(H^*(Q) \cap (12 + H(Q)) = n - 12 = 52, \\ \#((10 + H(Q))\backslash(12 + H(Q)) = 6. \end{aligned} \tag{30}$$

Hence, we get the value $52 + 6 = 58$.

$\underline{(\gamma_{i_1}, \gamma_{i_2}) = (9, 12)}$: Combining (30) with

$$\#((9 + H(Q))\backslash(12 + H(Q)) = 6$$

again give us the value $52 + 6 = 58$.

$\underline{(\gamma_{i_1}, \gamma_{i_2}) = (9, 10)}$: We have

$$\begin{aligned} \#(H^*(Q) \cap (10 + H(Q)) = n - 10 = 54, \\ \#((9 + H(Q))\backslash(10 + H(Q)) = 4 \end{aligned}$$

producing the value $54 + 4 = 58$.

The minimum of the above three values is 58 which is then our estimate on $M_2(C_{\mathcal{L}}(D, 12Q), C_{\mathcal{L}}(D, 8Q))$.

Finally consider $m = 3$. There is only one choice of $(\gamma_{i_1}, \gamma_{i_2}, \gamma_{i_3})$ namely $(9, 10, 12)$. By inspection there are exactly 8 numbers that are in either $9 + H(Q)$ or $10 + H(Q)$ but not in $12 + H(Q)$. Hence, our estimate on $M_3(C_{\mathcal{L}}(D, 12Q), C_{\mathcal{L}}(D, 8Q))$ becomes $n - 12 + 8 = 60$.

Example 2: This is a continuation of Example 1. The dimension of $C_{\mathcal{L}}(D, 10Q)$ and $C_{\mathcal{L}}(D, 5Q)$ are 6 and 3, respectively. Theorem 22 tells us that
$M_m(C_{\mathcal{L}}(D, 10Q), C_{\mathcal{L}}(D, 5Q))$ is at least $n - 10 = 54$, $n - 10 + 4 = 58$ and $n - 10 + 4 + 3 = 61$, for m equal to 1, 2 and 3, respectively. The possible values of γ_{i_s} to consider are $8, 9, 10$, which constitute a sequence without gaps. Hence, according to our discussion prior to Example 1 in this case we cannot improve upon Theorem 19.

Example 3: This is a continuation of Examples 1 and 2. The last numbers of $H^*(Q)$ are $\{65, 66, 67, 69, 70, 71, 74, 7$
Hence, $\dim(C_{\mathcal{L}}(D, 69Q)) = 64 - 5 = 59$ and $\dim(C_{\mathcal{L}}(D, 65Q)) = 64 - 8 = 56$. Theorem 22 gives no information on the first two RGHWs and only tells us that the third relative weight is larger than or equal to 2. This, however, is useless information as any space D of dimension 3 has a support of size at least 3.

As we will now demonstrate (17) guarantees that the three RGHWs are at least 3, 6, and 8, respectively. We first observe that

$$\begin{aligned} H^*(Q) \cap (69 + H(Q)) &= \{69, 74, 79\} \\ H^*(Q) \cap (67 + H(Q)) &= \{67, 71, 75, 79\} \\ H^*(Q) \cap (66 + H(Q)) &= \{66, 70, 71, 74, 75, 79\}. \end{aligned}$$

The smallest set is of size 3 and we get $M_1(C_{\mathcal{L}}(D, 69Q), C_{\mathcal{L}}(D, 65Q)) = 3$.
The smallest union of two sets is the union of the first two. This union is of size 6 giving us $M_2(C_{\mathcal{L}}(D, 69Q), C_{\mathcal{L}}(D, 65$
6.
The union of all three sets is of size 8. Hence, $M_3(C_{\mathcal{L}}(D, 69Q), C_{\mathcal{L}}(D, 65Q)) \geq 8$.

A. A comparison between RGHW and GHW

In [33] and [3], respectively, Munuera & Ramirez and Barbero & Munuera determined the GHWs of any Hermitian code. To state all their results is too extensive. However, already from their master theorem [33, Prop. 12], [3, Prop. 2.3], one can deduce that the RGHWs are often much larger than the corresponding GHWs.

Definition 24: Let $\text{ev} : \cup_{\mu=0}^{\infty} C_{\mathcal{L}}(D, \mu Q) \to \mathbb{F}_q^n$ be the map $\text{ev}(f) = (f(P_1), \ldots, f(P_n))$. The abundance $\alpha(\mu)$ is the dimension of $\ker \text{ev}$ when ev is restricted to $C_{\mathcal{L}}(D, \mu Q)$.
The following is the master theorem from [33], [3]. Here, and throughout the rest of this section, we use the notation $H(Q) = \{\rho_1, \rho_2, \ldots\}$ with $\rho_i < \rho_j$ for $i < j$.

Theorem 25: For $m = 1, \ldots, \dim(C_{\mathcal{L}}(D, \mu Q))$

$$d_m(C_{\mathcal{L}}(D, \mu Q)) \geq n - \mu + \rho_m + \alpha(\mu). \tag{31}$$

Equality holds under the following conditions:

1) $\mu \in H^*(Q)$
2) $n - \mu + \rho_{m+\alpha(\mu)} \in H(Q)$, in which case we write $n - \mu + \rho_{m+\alpha(\mu)} = iq + j(q+1)$, where i, j are non-negative integers with $j < q$.
3) $i \leq q^2 - q - 1$ or $j = 0$.

Observe that Theorem 25 and Theorem 22, respectively, produce similar estimates for the minimum distance and the relative minimum distance. Similarly for the second GHW and the second RGHW. From the last part of Theorem 22 we conclude that for $m = 1, 2$, whenever $m \leq \mu_1 - \mu_2 \leq q+1$, $c-1 \leq \mu_2$ and $\mu_1 < n-c$ holds, then $M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) = d_m(C_{\mathcal{L}}(D, \mu_1 Q))$ (recall that c is the conductor). As shall be demonstrated in the following, for higher values of m, $M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q))$ is often much larger than $d_m(C_{\mathcal{L}}(D, \mu_1 Q))$.

Proposition 26: For $q > 2$, $1 \leq m \leq q+1$ and $2q^2 - q \leq \mu \leq n - c$ we have $d_m(C_{\mathcal{L}}(D, \mu Q)) = n - \mu + \rho_m$.

Proof: It is well-known [42] that for $\mu \leq q^3 - 1$ we have $\alpha(\mu) = 0$. Therefore (31) simplifies to $d_m(C_{\mathcal{L}}(D, \mu Q)) \geq n - \mu + \rho_m$ under the conditions of the proposition. To prove the proposition it suffices to demonstrate the conditions 1, 2, and 3 of Theorem 25. As is well-known $\mu \in H^*(Q)$ when $c \leq \mu < n$. However, $c < 2q^2 - q$ and therefore condition 1 follows. To see that condition 2 is satisfied note that by assumption $c \leq n - \mu$ and so $n - \mu + \rho_{m+\alpha(\mu)} \geq c$. To demonstrate condition 3 it suffices to show

$$n - \mu + \rho_m \leq q^3 - q^2. \tag{32}$$

Observe that $\rho_m \leq q(q-1)$ which holds because of the assumption that $m \leq q+1$ and $q > 2$ and because the number of gaps in $H(Q)$ equals $q(q-1)/2$. As a consequence the assumption $2q^2 - q \leq \mu$ implies $q^2 + \rho_m \leq \mu$ from which we derive (32). ■

TABLE I
DIFF(m, q) IS THE VALUE OF (33).

m	3	4	5	6	7	8	9	10
Diff(m,4)	2	1	1					
Diff(m,5)	3	2	3	3				
Diff(m,7)	5	4	7	9	6	6		
Diff(m,8)	6	5	9	12	9	10	10	
Diff(m,16)	14	13	25	36	33	42	50	57

m	11	12	13	14	15	16	17
Diff(m,16)	51	56	60	63	65	55	55

Proposition 27: Consider the field $\mathbb{F}_{q^2}$, with $q > 2$. Let $3 \leq \widetilde{\mu} \leq q+1$ be fixed. For $m = 3, \ldots, \widetilde{\mu}$ there are at least $q^3 - 3q^2 + 1$ different codes $C_{\mathcal{L}}(D, \mu Q)$ for which $d_m(C_{\mathcal{L}}(D, \mu Q)) = n - \mu + \rho_m$ and simultaneously $M_m(C_{\mathcal{L}}(D, \mu Q), C_{\mathcal{L}}(D, (\mu - \widetilde{\mu})Q)) = n - \mu + \sum_{i=0}^{m-2}(q-i)$ hold. For these codes we have

$$M_m(C_{\mathcal{L}}(D, \mu Q), C_{\mathcal{L}}(D, (\mu - \widetilde{\mu})Q)) - d_m(C_{\mathcal{L}}(D, \mu Q)) = \big(\sum_{s=0}^{m-2}(q-s)\big) - \rho_m > 0. \tag{33}$$

Proof: Follows from Theorem 25, Theorem 22 and a study of $H(Q)$. ∎

Note that if for fixed $\widetilde{\mu}$ we divide the number of different codes $C_{\mathcal{L}}(D, \mu Q)$ for which (33) holds by the number of different codes, which is q^3, then we get the ratio $R(q) \geq (q^3 - 3q^2 + 1)/q^3 \geq 1 - 3/q$. This ratio approaches 1 as q approaches infinity. For $q = 4, 5, 7, 8, 9, 16$, and 32, respectively, $R(q)$ is at least 0.25, 0.4, 0.57, 0.62, 0.66, 0.81, and 0.9, respectively. In Table I for different values of m and q we list the difference between the parameters as expressed in (33).

VII. RAMP SCHEMES BASED ON HERMITIAN CODES

In this section we consider ramp secret sharing schemes D_1/D_2 where $D_1 = C_2^{\perp}$, $D_2 = C_1^{\perp}$, and $C_2 \subsetneq C_1$ are Hermitian codes over $\mathbb{F}_{q^2}$, with $\dim(C_1) - \dim(C_2) = \widetilde{\mu}$. Recall from Theorem 3 in Section II that $t_m + 1 = M_m(C_1, C_2)$, $m = 1, \ldots, \widetilde{\mu}$ is the size of the smallest group that can reveal m q^2-bits of information. Also recall that $r_m = n - M_{\widetilde{\mu}-m+1}(D_1, D_2) + 1$ is the smallest number such that any group of this size can reveal m q^2-bits of information. From Section VI we know how to determine/estimate $M_m(C_1, C_2)$. Now [42, Th. 1] tells us that for $\mu \in H^*(Q)$ we have $C_{\mathcal{L}}(D, \mu Q)^{\perp} = C_{\mathcal{L}}(D, (n+c-2-\mu)Q)$. To establish information on r_m we therefore need not apply Theorem 20 (the theorem for duals of one-point algebraic geometric codes), but can instead use the already established information on the RGHW of $C_2 \subseteq C_1$. From Theorem 22 we get the following result:

Theorem 28: Let $\mu, \widetilde{\mu}$ be positive integers satisfying

$$\widetilde{\mu} \leq q+1, \;\; c - 1 + \widetilde{\mu} \leq \mu \leq n - 1. \tag{34}$$

Consider the ramp secret sharing scheme $D_1/D_2 = C_2^{\perp}/C_1^{\perp}$ where $C_1 = C_{\mathcal{L}}(D, \mu Q)$ and $C_2 = C_{\mathcal{L}}(D, (\mu - \widetilde{\mu})Q)$. The codimension (and thereby the length of the secret) equals $\widetilde{\mu}$. Furthermore for $m = 1, \ldots, \widetilde{\mu}$ it holds that

$$t_m \;\; \geq \;\; n - \mu + \sum_{s=0}^{m-2}(q-s) - 1, \tag{35}$$

$$r_m \;\; \leq \;\; n - \mu + c + \widetilde{\mu} - 1 - \sum_{s=0}^{\widetilde{\mu}-m-1}(q-s). \tag{36}$$

TABLE II
PARAMETERS OF THE RAMP SCHEMES IN EXAMPLE 4.

m	1	2	3	4	5	6	7	8	9
$G_1(m,8)$	0	8	15	21	26	30	33	35	36
$G_2(m,9,8)$	28	29	31	34	38	43	49	56	64

TABLE III
PARAMETERS OF THE RAMP SCHEMES IN EXAMPLE 5.

m	1	2	3	4	5	6	7	8
$G_1(m,16)$	0	16	31	45	58	70	81	91
$G_2(m,16,16)$	120	122	125	129	134	140	147	155

m	9	10	11	12	13	14	15	16
$G_1(m,16)$	100	108	115	121	126	130	133	135
$G_2(m,16,16)$	164	174	185	197	210	224	239	255

Equality holds simultaneously in (35) and (36) when the second condition in (34) is replaced with

$$2c - 2 + \widetilde{\mu} < \mu < n - c. \tag{37}$$

Example 4: In this example we consider schemes over $\mathbb{F}_{64}$. That is, $q = 8$ and the number of participants is $n = 512$. The assumption (34) for (35) and (36) to hold is $\widetilde{\mu} \leq 9$, $55 + \widetilde{\mu} \leq \mu \leq 511$, the latter corresponding to $1 \leq n - \mu \leq 457 - \widetilde{\mu}$. By (37) equality holds simultaneously in (35) and (36) when $56 < n - \mu < 402 - \widetilde{\mu}$ holds. In Table II we list for $\widetilde{\mu} = q + 1$ the values of $G_1(m,q) = \sum_{s=0}^{m-2}(q-s)$ (which is our lower bound on $(t_m + 1) - (n - \mu)$) and $G_2(m,\widetilde{\mu},q) = c + \widetilde{\mu} - 1 - \sum_{s=0}^{\widetilde{\mu}-m-1}(q-s)$ (which is our upper bound on $r_m - (n - \mu)$). Note that $G_1(m,q) = Z(H(Q),\mu,m)$ (Lemma 21). For the considered choice of $\widetilde{\mu}$ the secret is of size equal to 9 q^2-bits. One can get much information from Table II. Assume for instance $n - \mu = 130$. Then the smallest group that can derive some information is of size $130 + 0 = 130$, hence $t_1 = 129$. The smallest group size for which any group can derive some information is $r_1 = 130 + 28 = 158$. Groups of size 158 on the other hand can never obtain more than 5 q^2-bits of information as $G_1(5,8) \leq 158 - 130 < G_1(6,8)$. Some group of size $t_3 + 1 = 130 + 15 = 145$ can derive at least 3 q^2-bits of information, however, $r_3 = 130 + 31 = 161$ is the smallest group size guaranteed to reveal 3 q^2-bits of information. Any group of size $r_9 = 130 + 64 = 194$ can reveal the entire secret. Some group of size $t_9 + 1 = 130 + 36 = 166$ can reveal the entire secret whereas other groups of size 166 can reveal no more than 4 q^2-bits of information.

Example 5: In this example we consider schemes over $\mathbb{F}_{256}$. That is, $q = 16$ and the number of participants is $n = 4096$. Assumption (34) is $1 \leq n - \mu < 3857 - \widetilde{\mu}$ and by (37) equality holds in (35) and (36) simultaneously if

$$240 < n - \mu < 3618 - \widetilde{\mu} \tag{38}$$

In Table III we list values of $G_1(m,16)$ and $G_2(m,16,16)$ where the functions G_1 and G_2 are as in Example 4. Assuming (38), then from the table we get the following information: Some groups of size $t_1 + 1 = n - \mu$ may reveal 1 q^2-bit of information whereas other groups of size $n - \mu + 119$ cannot as $r_1 = n - \mu + 120$. Some group of size $t_{11} + 1 = n - \mu + 115$ can reveal 11 q^2-bits of information whereas some group of the same size can not reveal anything. Any group of size $n - \mu + 135$ can for sure reveal 5 q^2-bits of information and some group of the same size can reveal everything. Any group of size $r_{16} = n - \mu + 255$ can reveal the entire secret.

Remark 29: Assume that (34) holds and let $m \leq \widetilde{\mu}$. The difference between the smallest size for which any group can reveal m q^2-bits of information and the smallest size for which some group can reveal m

q^2-bits of information equals $(n - M_{\widetilde{\mu}+1-m}(C_2^{\perp}, C_1^{\perp}) + 1) - M_m(C_1, C_2)$ which is at most

$$c + \widetilde{\mu} - 1 - \sum_{s=0}^{\widetilde{\mu}-m-1} (q-s) - \sum_{s=0}^{m-2} (q-s) \tag{39}$$

(with equality if $2c - 2 + \widetilde{\mu} < \mu < n - c$). The maximum of (39) is attained at $m = 1$ and $m = \widetilde{\mu}$. The corresponding "worst-case" difference equals $c + \widetilde{\mu} - 1 - \frac{\widetilde{\mu}-1}{2}(2q - \widetilde{\mu} + 2)$. This number is highest possible when $\widetilde{\mu} = q$ and $\widetilde{\mu} = q + 1$, in which case it equals the genus $g = (q^2 - q)/2$.
We conclude the section with an example in which we show how to improve upon (35) and (36) when the condition (37) is not satisfied.

Example 6: In this example we consider schemes over $\mathbb{F}_{16}$. That is, $q = 4$ and the number of participants is $n = 64$. We consider secrets of length 3. Hence, we require that

$$\dim(C_1 = C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_2 = C_{\mathcal{L}}(D, \mu_2 Q)) = 3.$$

We have

$$\begin{aligned} H^*(Q) &= \{0, 4, 5, 8, 9, 10, 12, 13, \cdots, \\ &\qquad 62, 63, 65, 66, 67, 70, 71, 75\} \end{aligned}$$

and therefore without loss of generality the possible choices of (μ_1, μ_2) are $\{(\mu_1^{(1)}, \mu_2^{(1)}), \ldots, (\mu_1^{(62)}, \mu_2^{(62)})\} = \{(5, -1), (8, 0), (9, 4), (10, 5), (12, 8), (13, 9), (14, 10), (15, 12), \ldots, (63, 60), (65, 61), (66, 62), (67, 63), (70, 65), (71, 66), (75, 67)\}$, where for $(5, -1)$ we mean that C_2 equals $\{\vec{0}\}$. In the following we calculate

$$\begin{aligned} t_m &= M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) - 1, \\ r_m &= n - M_{\mu_2 - \mu_1 - m + 1}(C_{\mathcal{L}}(D, (n + c - 2 - \mu_2)Q), \\ &\qquad C_{\mathcal{L}}(D, (n - c + 2 - \mu_1)Q)) + 1 \\ &= n - M_{\mu_2 - \mu_1 - m + 1}(C_{\mathcal{L}}(D, (74 - \mu_2)Q), \\ &\qquad C_{\mathcal{L}}(D, (74 - \mu_1)Q)) + 1, \end{aligned}$$

$m = 1, 2, 3$, for all the above choices of (μ_1, μ_2).

Recall from the discussion prior to Example 1 in Section VI that for some choices of (μ_1, μ_2) we may achieve better estimates on the RGHW than (22). This is done by applying the method of Example 1 and Example 3 which corresponds to (18) and (17), respectively. Specifically for $\mu_1 = 5, 8, 9, 10, 12, 13$ we do not have

$$\{\mu_1, \mu_1 - 1, \mu_1 - 2\} \subseteq H^*(Q) \tag{40}$$

and to calculate t_m we therefore apply the method of Example 1. By inspection, for $\mu_1 = 53$, 57, 58, 61, 62, 63, 65, 66, 67, 70, 71, 75 we have that $H^*(Q) \backslash (\mu_1 + H(Q))$ is strictly smaller than $H(Q) \backslash (\mu_1 + H(Q))$ and also for some of these values, (40) does not hold either. Hence, we apply the method of Example 3. In conclusion the values of μ_1 for which we can potentially obtain improved information on t_m are

$$\begin{aligned} S_1 &= \{\mu_1^{(1)}, \mu_1^{(2)}, \ldots, \mu_1^{(6)}, \\ &\qquad \mu_1^{(46)}, \mu_1^{(50)}, \mu_1^{(51)}, \mu_1^{(54)}, \mu_1^{(55)}, \ldots, \mu_1^{(62)}\} \\ &= \{5, 8, 9, 10, 12, 13, \\ &\qquad 53, 57, 58, 61, 62, 63, 65, 66, 67, 70, 71, 75\}. \end{aligned} \tag{41}$$

We next discuss r_m. Here, a little care is needed in the analysis: as an example for $(\mu_1, \mu_2) = (\mu_1^{(4)}, \mu_2^{(4)}) = (10, 5)$ we have $C_2^{\perp} = C_{\mathcal{L}}(D, (74 - \mu_2)Q) = C_{\mathcal{L}}(D, 69Q)$, but this code is the same as $C_{\mathcal{L}}(D, 67Q)$

TABLE IV
LOWER BOUNDS ON t_m AND UPPER BOUNDS ON r_m FOR THE SCHEMES IN EXAMPLE 6.

μ_1	5	8	9	10	12	13	14	15
$[t_1, r_1]$	[58,62]	[55,61]	[54,60]	[53,59]	[51,58]	[50,57]	[49,56]	[48,56]
$[t_2, r_2]$	[62,63]	[59,62]	[58,61]	[57,60]	[57,60]	[54,59]	[53,58]	[52,58]
$[t_3, r_3]$	[63,64]	[62,63]	[61,63]	[60,62]	[59,62]	[58,62]	[56,61]	[55,61]

μ_1	16	19	20	24	53	57	58	61
$[t_1, r_1]$	[47,55]	[44,52]	[43,51]	[39,47]	[11,18]	[7,14]	[7,13]	[3,10]
$[t_2, r_2]$	[51,58]	[48,54]	[47,54]	[43,50]	[14,21]	[10,17]	[10,16]	[6,13]
$[t_3, r_3]$	[54,61]	[51,57]	[50,57]	[46,53]	[17,25]	[13,21]	[12,20]	[9,17]

μ_1	62	63	65	66	67	70	71	75
$[t_1, r_1]$	[3,9]	[3,8]	[2,6]	[2,5]	[2,4]	[1,3]	[1,2]	[0,1]
$[t_2, r_2]$	[6,12]	[6,11]	[5,10]	[4,7]	[4,7]	[3,6]	[2,5]	[1,2]
$[t_3, r_3]$	[8,16]	[8,15]	[7,14]	[6,13]	[5,11]	[4,10]	[3,9]	[2,6]

because 68 and 69 do not belong to $H^*(Q)$. This phenomenon corresponds to the fact that actually $C_{\mathcal{L}}(D, \mu_2^{(s)}Q)^{\perp} = C_{\mathcal{L}}(D, \mu_1^{(63-s)}Q)$, $s = 1, \ldots, 62$. Hence, from (41) we see that the values of μ_1 for which we can potentially derive improved information regarding r_m are

$$\begin{aligned} S_2 &= \{\mu_1^{(63-1)}, \ldots, \mu_1^{(63-6)}, \mu_1^{(63-46)}, \mu_1^{(63-50)}, \mu_1^{(63-51)}, \\ &\quad \mu_1^{(63-54)}, \ldots, \mu_1^{(63-62)}\} \\ &= \{5, 8, 9, 10, 12, 13, 14, 15, 16, \\ &\quad 19, 20, 24, 65, 66, 67, 70, 71, 75\}. \end{aligned}$$

Applying a mixture of the method from Example 1 and Example 3 plus (22) we derive for $\mu_1 \in S_1 \cup S_2$ the information given in Table IV.

For the remaining values of μ_1, that is for

$$\begin{aligned} \mu_1 &\in \{5, 8, 9, 10, 12, \ldots, 63, 65, 66, 67, 70, 71, 75\} \\ &\quad \setminus (S_1 \cup S_2) \\ &= \{17, 18, 21, 22, 23, 25, 26, 27, \ldots, \\ &\quad 51, 52, 54, 55, 56, 59, 60\} \end{aligned}$$

we have $\mu_2 = \mu_1 - 3$, and the best bounds (sometimes tight) are obtained from (22). They are: $[t_1 \geq n - \mu_1 - 1, r_1 \leq n - \mu_1 + 7]$, $[t_2 \geq n - \mu_1 + 3, r_2 \leq n - \mu_1 + 10]$ and $[t_3 \geq n - \mu_1 + 6, r_3 \leq n - \mu_1 + 14]$.

ACKNOWLEDGMENTS

The authors would like to thank Ignacio Cascudo, Hao Chen, Ronald Cramer and Carlos Munuera for pleasant discussions. Also the authors would like to thank the anonymous reviewers for valuable comments that helped us improve the paper.

REFERENCES

[1] H. E. Andersen and O. Geil, "Evaluation codes from order domain theory," *Finite Fields Appl.*, vol. 14, no. 1, pp. 92–123, 2008.
[2] T. Bains, "Generalized Hamming weights and their applications to secret sharing schemes," Master's thesis, Univ. Amsterdam, 2008.
[3] A. I. Barbero and C. Munuera, "The weight hierarchy of Hermitian codes," *SIAM J. Discrete Math.*, vol. 13, no. 1, pp. 79–104, 2000. [Online]. Available: http://dx.doi.org/10.1137/S089548019834342X
[4] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Advances in cryptology (Santa Barbara, Calif., 1984)*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 1985, vol. 196, pp. 242–268.
[5] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, "On the size of shares for secret sharing schemes," *Journal of Cryptology*, vol. 6, no. 3, pp. 157–167, 1993.

[6] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, "Secure computation from random error correcting codes," in *Advances in cryptology—EUROCRYPT 2007*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 2007, vol. 4515, pp. 291–310.

[7] L. Csirmaz, "Ramp secret sharing and secure information storage," 2009, presented at IntelliSec'09. Available from http://eprints.renyi.hu/19/.

[8] A. Del Centina, "Weierstrass points and their impact in the study of algebraic curves: a historical account from the lückensatz to the 1970s," *Annali dell'Università di Ferrara*, vol. 54, no. 1, pp. 37–59, 2008.

[9] I. M. Duursma and S. Park, "Coset bounds for algebraic geometric codes," *Finite Fields Appl.*, vol. 16, no. 1, pp. 36–55, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.ffa.2009.11.006

[10] G. L. Feng and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, no. 1, pp. 37–45, 1993.

[11] ——, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1003–1012, 1994.

[12] ——, "Improved geometric Goppa codes part I: Basic theory," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1678–1693, 1995.

[13] G. D. J. Forney, "Dimension/length profiles and trellis complexity of linear block codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 1741–1752, Nov 1994.

[14] O. Geil and S. Martin, "Further improvements on the Feng-Rao bound for dual codes," *Finite Fields Appl.*, vol. 30, pp. 33–48, 2014.

[15] ——, "An improvement of the Feng–Rao bound for primary codes," *Des. Codes Cryptogr.*, 2014, dOI: 10.1007/s10623-014-9983-z. To appear. [Online]. Available: arXiv:1307.3107

[16] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and L. Yuan, "Relative generalized Hamming weights of one-point algebraic geometric codes," Apr. 2014, to appear in Proc. IEEE Information Theory Workshop (ITW 2014).

[17] O. Geil, R. Matsumoto, and D. Ruano, "Feng-Rao decoding of primary codes," *Finite Fields Appl.*, vol. 23, pp. 35–52, 2013.

[18] O. Geil, C. Munuera, D. Ruano, and F. Torres, "On the order bounds for one-point AG codes," *Adv. Math. Commun.*, vol. 5, no. 3, pp. 489–504, 2011. [Online]. Available: http://dx.doi.org/10.3934/amc.2011.5.489

[19] O. Geil and R. Pellikaan, "On the structure of order domains," *Finite Fields Appl.*, vol. 8, no. 3, pp. 369–396, 2002.

[20] O. Geil and C. Thommesen, "On the Feng-Rao bound for generalized Hamming weights," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. Lecture Notes in Computer Science, M. P. C. Fossorier, H. Imai, S. Lin, and A. Poli, Eds. Springer, 2006, vol. 3857, pp. 295–306.

[21] P. Heijnen and R. Pellikaan, "Generalized Hamming weights of q-ary Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 181–196, 1998.

[22] T. Høholdt, J. H. van Lint, and R. Pellikaan, "Algebraic geometry codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam: Elsevier, 1998, vol. 1, pp. 871–961.

[23] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*. Cambridge university press Cambridge, 2003, vol. 22.

[24] A. Hürwitz, "Über algebraische Gebilde mit eindeutigen Transformationen in sich," *Math. Ann*, vol. 41, no. 3, pp. 403–442, 1892.

[25] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electron. Comm. Jpn. Pt. III*, vol. 72, no. 9, pp. 56–63, 1989. [Online]. Available: doi:10.1002/ecjc.4430720906

[26] M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," *Inform. Process. Lett.*, vol. 97, no. 2, pp. 52–57, Jan. 2006. [Online]. Available: doi:10.1016/j.ipl.2005.09.012

[27] J. Kurihara, R. Matsumoto, and T. Uyematsu, "Relative generalized rank weight of linear codes and its applications to network coding," 2013. [Online]. Available: arxiv:1301.5482

[28] J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight," *IEICE Trans. Fundamentals*, vol. E95-A, no. 11, pp. 2067–2075, Nov. 2012. [Online]. Available: doi:10.1587/transfun.E95.A.2067

[29] Z. Liu, W. Chen, and Y. Luo, "The relative generalized Hamming weight of linear q-ary codes and their subcodes," *Des. Codes Cryptogr.*, vol. 48, no. 2, pp. 111–123, 2008. [Online]. Available: http://dx.doi.org/10.1007/s10623-008-9170-1

[30] Y. Luo, C. Mitrpant, A. J. H. Vinck, and K. Chen, "Some new characters on the wire-tap channel of type II," *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 1222–1229, 2005. [Online]. Available: http://dx.doi.org/10.1109/TIT.2004.842763

[31] J. L. Massey, "Some applications of coding theory in cryptography," in *Codes and Ciphers: Cryptography and Coding IV*, 1995, pp. 33–47.

[32] R. Matsumoto and S. Miura, "On the Feng-Rao bound for the $\mathcal{L}$-construction of algebraic geometry codes," *IEICE Trans. Fundamentals*, vol. E83-A, no. 5, pp. 926–930, May 2000. [Online]. Available: http://www.rmatsumoto.org/repository/e83-a_5_923.pdf

[33] C. Munuera and D. Ramirez, "The second and third generalized Hamming weights of Hermitian codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 709–712, 1999. [Online]. Available: http://dx.doi.org/10.1109/18.749019

[34] W. Olaya-León and C. Munuera, "On the minimum distance of castle codes," *Finite Fields Appl.*, vol. 20, pp. 55–63, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.ffa.2012.12.001

[35] M. E. O'Sullivan, "New codes for the Berlekamp-Massey-Sakata algorithm," *Finite Fields Appl.*, vol. 7, no. 2, pp. 293–317, 2001. [Online]. Available: http://dx.doi.org/10.1006/ffta.2000.0283

[36] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," in *Advances in cryptology (Paris, 1984)*, ser. Lecture Notes in Comput. Sci. Berlin: Springer, 1985, vol. 209, pp. 33–50. [Online]. Available: http://dx.doi.org/10.1007/3-540-39757-4_5

[37] R. Pellikaan, "On the efficient decoding of algebraic-geometric codes," *Eurocode*, vol. 92, pp. 231–253, 1993.

[38] G. Salazar, D. Dunn, and S. B. Graham, "An improvement of the Feng-Rao bound on minimum distance," *Finite Fields Appl.*, vol. 12, pp. 313–335, 2006.

[39] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[40] H. Stichtenoth, "A note on Hermitian codes over GF(q^2)," *Information Theory, IEEE Transactions on*, vol. 34, no. 5, pp. 1345–1348, 1988.
[41] A. Subramanian and S. W. McLaughlin, "MDS codes on the erasure-erasure wiretap channel," *arXiv preprint arXiv:0902.3286*, 2009.
[42] H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Inform. Theory*, vol. 33, no. 4, pp. 605–609, 1987. [Online]. Available: http://dx.doi.org/10.1109/TIT.1987.1057327
[43] M. Tsfasman and S. G. Vladut, *Algebraic-geometric codes*. Kluwer Academic Publishers, 1991.
[44] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 5, pp. 1412–1418, 1991.
[45] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[46] H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme," *Electron. Comm. Jpn. Pt. I*, vol. 69, no. 9, pp. 46–54, 1986. [Online]. Available: doi:10.1002/ecja.4410690906
[47] K. Yang and P. V. Kumar, "On the true minimum distance of Hermitian codes," in *Coding theory and algebraic geometry*. Springer, 1992, pp. 99–107.
[48] Z. Zhuang, Y. Luo, and B. Dai, "Code constructions and existence bounds for relative generalized Hamming weight," *Des. Codes Cryptogr.*, vol. 69, no. 3, pp. 275–297, dec 2013.