

Improved constructions of nested code pairs

Carlos Galindo, Olav Geil, Fernando Hernando and Diego Ruano

Abstract

Two new constructions of linear code pairs $C_2 \subset C_1$ are given for which the codimension and the relative minimum distances $M_1(C_1, C_2)$, $M_1(C_2^\perp, C_1^\perp)$ are good. By this we mean that for any two out of the three parameters the third parameter of the constructed code pair is large. Such pairs of nested codes are indispensable for the determination of good linear ramp secret sharing schemes [40]. They can also be used to ensure reliable communication over asymmetric quantum channels [54]. The new constructions result from carefully applying the Feng-Rao bounds [21], [31] to a family of codes defined from multivariate polynomials and Cartesian product point sets.

Index Terms

asymmetric quantum code, CSS construction, Feng-Rao bound, nested codes, ramp secret sharing, relative generalized Hamming weight, relative minimum distance, wiretap channel of type II.

I. INTRODUCTION

In this paper we consider pairs of linear codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$ where \mathbb{F}_q is the finite field with q elements. We are interested in the codimension $\ell = \dim C_1 - \dim C_2$ and the relative minimum distances

$$M_1(C_1, C_2) = \min\{w_H(\vec{c}) \mid \vec{c} \in C_1 \setminus C_2\},$$

$$M_1(C_2^\perp, C_1^\perp) = \min\{w_H(\vec{c}) \mid \vec{c} \in C_2^\perp \setminus C_1^\perp\}.$$

Here $w_H(\vec{c})$ means the Hamming weight of \vec{c} . For any two out of three parameters we aim to construct code pairs such that the two parameters are equal to some prescribed values, whereas the last parameter is as large as possible. Our motivation for studying the above problem is applications in ramp secret sharing, communication over wiretap channels of type II, and asymmetric quantum coding.

We first explain the application in secret sharing. The application to wiretap channels of type II is analogue. A secret sharing scheme is a cryptographic method to encode a secret into a set of shares, later to be distributed among participants, so that only specified subsets of the participants can reconstruct the secret. The first secret sharing scheme, proposed by Shamir [52], was a perfect scheme, meaning that a set of participants unable to reconstruct the secret has no information on the secret. Later non-perfect secret sharing schemes were proposed [7], [56] in which there are sets of participants that have some information about the secret, but cannot fully reconstruct it. In this paper we use the term ramp secret sharing schemes for the general class of perfect or non-perfect schemes. Secret sharing has been applied, for example, to store confidential information at multiple locations that are placed geographically apart. When we use 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 are useful. In the perfect scheme the size of a share must be greater than or equal to that of the

Published in IEEE Transactions on Information Theory. Volume 64, Issue 4, pages 2444-2459 (2018).

The authors gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367), the support from the Spanish MINECO/FEDER (Grants No. MTM2015-65764-C3-2-P and MTM2015-69138-REDT), and the support from University Jaume I (Grant No. P1-1B2015-02).

C. Galindo and F. Hernando are with Instituto Universitario de Matemáticas y Aplicaciones de Castellón, and Departamento de Matemáticas, Jaume I University, Spain. e-mail: galindo@mat.uji.es, carrillf@mat.uji.es.

O. Geil and D. Ruano are with the Department of Mathematical Sciences, Aalborg University, Denmark. e-mail: olav@math.aau.dk, diego@math.aau.dk

secret [11]. In contrast ramp secret sharing schemes allow shares to be smaller than the secret which for instance is useful for storing bulk data [14].

A linear ramp secret sharing scheme can be described as a coset construction C_1/C_2 where $C_2 \subset C_1$ are linear codes [12]. More precisely, let $\dim C_2 = k_2$, $\dim C_1 = k_1$ and $\ell = k_1 - k_2$. Given a basis $\{\vec{b}_1, \dots, \vec{b}_{k_2}\}$ for C_2 as a vector space over \mathbb{F}_q and a corresponding basis $\{\vec{b}_1, \dots, \vec{b}_{k_2}, \vec{b}_{k_2+1}, \dots, \vec{b}_{k_1=k_2+\ell}\}$ for C_1 the encoding of a secret $(s_1, \dots, s_\ell) \in \mathbb{F}_q^\ell$ is done by choosing $a_1, \dots, a_{k_2} \in \mathbb{F}_q$ randomly from a uniform distribution and then constructing the codeword $\vec{c} = a_1\vec{b}_1 + \dots + a_{k_2}\vec{b}_{k_2} + s_1\vec{b}_{k_2+1} + \dots + s_\ell\vec{b}_{k_1}$. The shares are the entries of \vec{c} .

Definition 1. Given a ramp secret sharing scheme C_1/C_2 with $\ell = \dim C_1 - \dim C_2$ we say that it has (t_1, \dots, t_ℓ) -privacy and (r_1, \dots, r_ℓ) -reconstruction if the positive integers t_1, \dots, t_ℓ are chosen as large as possible and the positive integers r_1, \dots, r_ℓ are chosen as small as possible such that

- for $1 \leq v \leq \ell$, an adversary cannot obtain $v \log_2(q)$ bits of information about \vec{s} with any t_v shares,
- for $1 \leq v \leq \ell$, it is possible to recover $v \log_2(q)$ bits of information about \vec{s} with any collection of r_v shares.

We shall refer to the numbers r_1, \dots, r_ℓ as reconstruction numbers and similarly call the numbers t_1, \dots, t_ℓ privacy numbers. These parameters are motivated by the fact that the amount of information which an adversary can obtain is always an integer times $\log_2(q)$ bits and similar for the reconstruction. Of particular interest are the first privacy number $t = t_1$ and the last reconstruction number $r = r_\ell$, as t is the maximal number such that no set of this size leaks any information about the secret, and r equals the smallest number such that any set of this size can recover the entire secret. It was demonstrated in [5], [55], [40], [30] that the above numbers can be uniquely determined from the relative generalized Hamming weights, that we shall define now. For $v = 1, \dots, \ell$

$$M_v(C_1, C_2) = \min\{\#\text{Supp } U \mid U \text{ is a subspace of } C_1 \\ \text{of dimension } v, U \cap C_2 = \{\vec{0}\}\}$$

(and similar for the dual codes). Here, $\text{Supp } U$ is the set of entries where some codeword in U is non-zero and $\#$ is the cardinality. In our paper we shall adopt the tradition of sometimes referring to relative generalized Hamming weights $M_1(C_1, C_2)$ and $M_1(C_2^\perp, C_1^\perp)$ simply as relative minimum distances. Note that the relative minimum distance $M_1(C_1, C_2)$ can be lower bounded by the minimum distance of C_1 . Similarly, the relative minimum distance $M_1(C_2^\perp, C_1^\perp)$ is greater than or equal to the minimum distance of C_2^\perp . The following theorem corresponds to [30, Theorem 3].

Theorem 2. Let $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$ with $\ell = \dim C_1 - \dim C_2$ and consider the corresponding ramp secret sharing scheme C_1/C_2 . Then the reconstruction numbers and privacy numbers satisfy

$$r_v = n - M_{\ell-v+1}(C_1, C_2) + 1, \\ t_v = M_v(C_2^\perp, C_1^\perp) - 1,$$

for $v = 1, \dots, \ell$.

Hence, if for instance we want to construct a ramp secret sharing scheme over \mathbb{F}_q with n participants, secrets of length ℓ , first privacy number equal to some t , and last reconstruction number r as small as possible, what we need is exactly a pair of nested codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$ of codimension ℓ with $M_1(C_2^\perp, C_1^\perp) = t + 1$, and $M_1(C_1, C_2) = n - r + 1$ as large as possible.

Finally we explain in brief the use of nested codes in connection with asymmetric quantum error-correcting codes, introduced in [54]. The study of good quantum codes is by now a well-established research area. Some classical and recent references are [10], [8], [9], [4], [6], [3], [47], [39]. Recently, such theory has been extended to asymmetric quantum error-correcting codes which are useful in a model where the probabilities of qubit-flip and phase-shift errors are different [38], [51], [19], [42], [41], [16], [17],

[43], [44]. This generalization is motivated by the argument that dephasing will happen more frequently than relaxation [38]. A linear q -ary asymmetric quantum error-correcting code C is a q^k dimensional subspace of the Hilbert space \mathbb{C}^{q^n} whose error basis is defined by unitary operators usually denoted by X and Z . It is customary to write the parameters of C as $[[n, k, d_z/d_x]]_q$ which means that C corrects all phase-shift errors up to $\lfloor \frac{d_z-1}{2} \rfloor$, and all qudit-flip errors up to $\lfloor \frac{d_x-1}{2} \rfloor$.

In the present paper we concentrate on the Calderbank-Shor-Steane (CSS) construction of asymmetric quantum codes from a pair of nested linear codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$. We leave it for the reader to inspect [9], [39] for the actual construction. Here, we only give the following important result on the parameters of the resulting asymmetric quantum code (see [51, Lemma 3.1]).

Theorem 3. *Consider linear codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$. Then the asymmetric quantum code defined using the CSS construction has parameters*

$$[[n, \ell = \dim C_1 - \dim C_2, d_z/d_x]]_q$$

where $d_z = M_1(C_1, C_2)$ and $d_x = M_1(C_2^\perp, C_1^\perp)$.

Recall, that a stabilizer (symmetric) quantum code is the common eigenspace of a commutative subgroup of the error group associated to the error basis (see [9], [39] for details). The quantum codes in Theorem 3 can be considered as stabilizer asymmetric quantum codes [51, Lemma 3.1]. Studying asymmetric quantum codes rather than only symmetric codes is an important problem. For instance, already in [38] it was identified that large ratios d_z/d_x are relevant – phase-flip errors occurring tens, hundreds, or even thousands times more likely than bit-flips. From Theorem 3 it is clear that $d_z \geq d(C_1)$ and $d_x \geq d(C_2^\perp)$ where the expressions on the right sides are the minimum distance of the classical code. There is a clear physical significance of cases where strict inequality holds in at least one of these expressions. Such (asymmetric) quantum codes are called impure (or degenerate) [1], [35] and it is known that the impureness can be employed to obtain improved decoding.

As a measure for goodness of asymmetric quantum codes we shall use the Gilbert-Varshamov bound from [45, Theorem 4] which we now recall:

Theorem 4. *If*

$$\frac{1 - q^{-2\ell}}{1 - q^{-2n}} \cdot \frac{1}{q^{n-\ell}} \sum_{i=1}^{d_x-1} \binom{n}{i} (q-1)^i \cdot \sum_{i=1}^{d_z-1} \binom{n}{i} (q-1)^i < 1$$

then there exists an $[[n, \ell, d_z/d_x]]_q$ asymmetric quantum code.

The literature only reports few families of long asymmetric quantum codes, an exception being La Guardia's construction II in [44, Theorem 7.1] which we shall compare our codes with. In another direction Ezerman et al's works in [17], [18] explain how to derive good asymmetric quantum codes with d_x being very small and ℓ being moderate. As our constructions do not seem to generally compare well with these codes in the case of $d_x \in \{2, 3\}$ we omit such cases in our tables.

Having discussed both ramp secret sharing schemes and asymmetric quantum codes we include a remark relating them to each other.

Remark 5. There exists an asymmetric quantum code based on the CSS construction with parameters $[[n, \ell, d_z/d_x]]_q$ if and only there exists a linear ramp secret sharing scheme over \mathbb{F}_q with secrets in \mathbb{F}_q^ℓ , with $r = r_\ell = n - d_z + 1$ and $t = t_1 = d_x - 1$.

As the tradition for reporting numerical data on parameters of (asymmetric) quantum codes seems stronger than the tradition for reporting corresponding parameters of ramp secret sharing schemes, throughout this paper we shall often report our findings in the first setting. In such cases we leave it for the reader to apply Remark 5 to make the translation to secret sharing. On the other hand, higher relative weights give information on ramp secret sharing schemes, whereas no implication for asymmetric quantum codes

seems to be known. Hence, when treating them we shall do it in the setting of secret sharing.

In this paper we present two new families of long nested codes $C_2 \subset C_1$ with $M_1(C_1, C_2) + M_1(C_2^\perp, C_1^\perp)$ high. Such codes give rise to ramp secret sharing schemes with $r - t$ close to ℓ , and give rise to asymmetric quantum codes with $d_z + d_x$ close to $n - \ell + 2$. The code pairs are defined by evaluating multivariate polynomials at the points of Cartesian products of subsets of finite fields, and the above mentioned two families are found by carefully applying Feng-Rao theory [30]. Our first family is made by combining, for the first time in the literature, the Feng-Rao improved code constructions for dual and primary codes. This leads to good pairs of codes, however, it only works for relatively high codimension ℓ . The asymmetric quantum codes related to this first family of nested codes compare very favorably with known asymmetric quantum codes of similar length as well as the Gilbert-Varshamov bound. Moreover, the construction is very flexible and we can choose d_z/d_x very large, which as already mentioned can be desirable. Our second family is a completely new construction which produces very good parameters in the case of relatively small codimension ℓ . Again the corresponding asymmetric quantum codes compare favorably with the known codes of similar length and similarly with the Gilbert-Varshamov bound. Even more, we demonstrate a strong advantage of using our estimates on the relative minimum distances $M_1(C_1, C_2)$ and $M_1(C_2^\perp, C_1^\perp)$; rather than just using information on the minimum distances $d(C_1)$ and $d(C_2^\perp)$. Actually, using only information on the minimum distances $d(C_1)$ and $d(C_2^\perp)$ – which is often done in the literature – it seems in many cases impossible to establish the code parameters for asymmetric quantum codes, which we are able to obtain. These reflections are closely related to the fact that the corresponding asymmetric quantum codes of relatively small dimension are almost always impure, which as already mentioned is desirable. Again the construction is quite flexible in the sense that we can choose the ratio d_z/d_x very high if requested. For both families of codes we provide generator matrices, and we also describe a method for estimating higher relative weights $M_v(C_1, C_2)$, $M_v(C_2^\perp, C_1^\perp)$, $v = 2, \dots, \ell$, which sometimes leads to closed formula expressions. Recall, that such parameters express the information leakage and message recovery in connection with ramp secret sharing. As a result it is shown that for our second family of nested codes, the security of the related secret sharing schemes is much better than expected from studying only $t = t_1$. Furthermore, for certain choices of Cartesian product point sets also parity check matrices can easily be obtained, namely for the particular cases where the considered codes satisfy the conditions for being so-called J -affine variety codes [26]. Finally, all considered codes in this paper can be decoded up to half their designed minimum distance by applying known decoding algorithms. The dual codes can furthermore be decoded up to half the designed relative minimum distance. These observations lead to decoding algorithms for the corresponding asymmetric quantum codes.

The paper is organized as follows. In Section II we start by recalling the Feng-Rao bounds for primary and dual linear codes and we apply them to the general class of codes derived by evaluating multivariate polynomials at Cartesian product point sets. In this section we provide all needed background on Feng-Rao theory – for basic results on multivariate polynomials and related concepts we refer the reader to [13]. The section concludes with a discussion on how to decode the related asymmetric quantum codes. Then, in Section III, we explain how to employ the Feng-Rao improved code constructions for primary and dual codes simultaneously to obtain good families of nested codes with relatively high codimension. We then study the corresponding ramp secret sharing schemes and asymmetric quantum codes. In Section IV we present the new good construction of nested codes with relatively small codimension and we study the corresponding ramp secret sharing schemes and asymmetric quantum codes. Section V gives concluding remarks on the connection to J -affine variety codes. The paper contains a number of examples, the end of which we indicate by \diamond s.

II. CODES DEFINED FROM CARTESIAN PRODUCT POINT SETS

In this paper we consider families of code pairs $C_2 \subset C_1$ defined by evaluating multivariate polynomials at the points of Cartesian products of subsets of finite fields. For the applications described in the previous

section, we are interested in the parameters $M_v(C_1, C_2)$ (the primary case) as well as $M_v(C_2^\perp, C_1^\perp)$ (the dual case) – with a special focus on the relative minimum distances $M_1(C_1, C_2)$ and $M_1(C_2^\perp, C_1^\perp)$. To handle the primary case only it would be natural to use the language of Gröbner basis theory and to apply the so-called footprint bound [50], [36], [28]. However, in this language it is more difficult to treat the dual case and we therefore give a coherent description of both cases using the Feng-Rao bounds for general linear codes instead. The Feng-Rao bounds come in two versions, namely one for primary codes [2], [32], [31], [30] and another for dual codes [20], [21], [22], [48], [37], [46], [30].

Our exposition follows the presentation in [30, Section IV] and is illustrated with a continued example. This continued example, at the end of the present section, leads to the introduction of a general class of code pairs for which we have a simple description of generator matrices, where we know the codimension, and where we can easily estimate the relative minimum distances and also the higher relative weights (Theorem 16). It is from this class of code pairs we, in the following sections, show how to choose optimal pairs when the codimension is relatively large (Section III), and when it is relatively small (Section IV).

Consider a fixed basis $\mathcal{B} = \{\vec{b}_1, \dots, \vec{b}_n\}$ for \mathbb{F}_q^n as a vector space over \mathbb{F}_q and let $\mathcal{I} = \{1, \dots, n\}$.

Definition 6. Define $\bar{\rho} : \mathbb{F}_q^n \rightarrow \mathcal{I} \cup \{0\}$ to be the function given as follows. For non-zero \vec{c} we have $\bar{\rho}(\vec{c}) = i$ where i is the unique integer such that

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

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

Throughout the paper by \prec_{deg} we shall always mean the degree lexicographic ordering given by the rule that for two different monomials we have $X_1^{i_1} \dots X_m^{i_m} \prec_{\text{deg}} X_1^{j_1} \dots X_m^{j_m}$ if one of the following conditions holds:

- 1) $i_1 + \dots + i_m < j_1 + \dots + j_m$
- 2) $i_1 + \dots + i_m = j_1 + \dots + j_m$, but the rightmost non-zero entry of $(j_1 - i_1, \dots, j_m - i_m)$ is positive.

In case of two variables X and Y , we shall always think of X as X_1 and Y as X_2 . In the paper we shall also need other monomial orderings \prec , however, the degree lexicographic ordering will play a particular important role.

Example 1. Consider the ideal $I = \langle X^6 - 1, Y^6 - 1 \rangle \subset \mathbb{F}_7[X, Y]$ and the residue class ring $R = \mathbb{F}_7[X, Y]/I$. We have that the corresponding variety consists of all pairs of non-zero elements of \mathbb{F}_7 , hence we may write $\mathcal{V}_{\mathbb{F}_7}(I) = \{P_1, \dots, P_{36}\}$. Let $\text{ev} : R \rightarrow \mathbb{F}_7^{36}$ be the vector space homomorphism given by $\text{ev}(F + I) = (F(P_1), \dots, F(P_{36}))$. Therefore, the set $\mathcal{B} = \{\text{ev}(X^i Y^j + I) \mid 0 \leq i, j < 6\}$ constitutes a basis for \mathbb{F}_7^{36} as a vector space over \mathbb{F}_7 . To see this, we first observe that

$$\begin{aligned} \text{ev}(F(X, Y) + I) &= \text{ev}\left(F(X, Y) - A(X, Y)(X^6 - 1) \right. \\ &\quad \left. - B(X, Y)(Y^6 - 1) + I\right) \end{aligned}$$

for any $A(X, Y), B(X, Y) \in \mathbb{F}_7[X, Y]$, which implies that we may, without loss of generality, assume that $\deg_X F, \deg_Y F < 6$. Using Lagrange interpolation it holds that ev is surjective, and as $\#\mathcal{B}$ equals the dimension of the image \mathbb{F}_7^{36} \mathcal{B} is indeed a basis – and consequently ev is an isomorphism. We next enumerate \mathcal{B} according to the degree lexicographic ordering \prec_{deg} . The enumeration is illustrated in Fig. 1. As an example we obtain $\bar{\rho}(\text{ev}(2X^5 Y^4 + 5X^3 Y^2 + 4 + I)) = 34$. \diamond

Recall, that the component wise product of two vectors in \mathbb{F}_q^n is given by

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

Using this product we can now introduce the concept of one-way well-behaving pairs.

Y^5	XY^5	X^2Y^5	X^3Y^5	X^4Y^5	X^5Y^5	\vec{b}_{21}	\vec{b}_{26}	\vec{b}_{30}	\vec{b}_{33}	\vec{b}_{35}	\vec{b}_{36}
Y^4	XY^4	X^2Y^4	X^3Y^4	X^4Y^4	X^5Y^4	\vec{b}_{15}	\vec{b}_{20}	\vec{b}_{25}	\vec{b}_{29}	\vec{b}_{32}	\vec{b}_{34}
Y^3	XY^3	X^2Y^3	X^3Y^3	X^4Y^3	X^5Y^3	\vec{b}_{10}	\vec{b}_{14}	\vec{b}_{19}	\vec{b}_{24}	\vec{b}_{28}	\vec{b}_{31}
Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	X^5Y^2	\vec{b}_6	\vec{b}_9	\vec{b}_{13}	\vec{b}_{18}	\vec{b}_{23}	\vec{b}_{27}
Y	XY	X^2Y	X^3Y	X^4Y	X^5Y	\vec{b}_3	\vec{b}_5	\vec{b}_8	\vec{b}_{12}	\vec{b}_{17}	\vec{b}_{22}
1	X	X^2	X^3	X^4	X^5	\vec{b}_1	\vec{b}_2	\vec{b}_4	\vec{b}_7	\vec{b}_{11}	\vec{b}_{16}

Fig. 1. The enumeration of \mathcal{B} in Example 1

Definition 7. An ordered pair $(i, j) \in \mathcal{I} \times \mathcal{I}$ 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 $i' \in \mathcal{I}$ with $i' < i$.

Example 2. This is a continuation of Example 1. Consider $\vec{b}_i = \text{ev}(X^\alpha Y^\beta + I)$ and $\vec{b}_j = \text{ev}(X^\gamma Y^\delta + I)$ (where, by assumption, $0 \leq \alpha, \beta, \gamma, \delta < 6$). The pair (i, j) is OWB if and only if $\alpha + \gamma < 6$ and $\beta + \delta < 6$ hold simultaneously. To see the “if” part note that if $X^\eta Y^\lambda \prec_{\text{deg}} X^\alpha Y^\beta$ then the leading monomial M of the remainder of $X^{\eta+\gamma} Y^{\lambda+\delta}$ after division with $\{X^6 - 1, Y^6 - 1\}$ satisfies $M \preceq_{\text{deg}} X^{\eta+\gamma} Y^{\lambda+\delta} \prec_{\text{deg}} X^{\alpha+\gamma} Y^{\beta+\delta}$ which follows from the properties of a monomial ordering and those of the division algorithm. The “only if” part has to do with the special form of the ideal I coming from a variety which is a Cartesian product. If for instance, $\alpha + \gamma \geq 6$ then letting $\eta = 6 - \gamma - 1$ we obtain $X^\eta Y^\beta \prec_{\text{deg}} X^\alpha Y^\beta$, but the leading monomial N of $X^{\eta+\gamma} Y^{\beta+\delta}$ after division with $\{X^6 - 1, Y^6 - 1\}$ has the same Y -part as the leading monomial of $X^{\alpha+\gamma} Y^{\beta+\delta}$ after division with $\{X^6 - 1, Y^6 - 1\}$, but higher X -part. \diamond

To formulate the Feng-Rao bound for primary codes we shall need the following set.

Definition 8. For $i \in \mathcal{I}$ define

$$\Lambda_i = \{l \in \mathcal{I} \mid \exists j \in \mathcal{I} \text{ s.t. } (i, j) \text{ is OWB and } \bar{\rho}(\vec{b}_i * \vec{b}_j) = l\}.$$

Given a v -dimensional vector space $U \subseteq \mathbb{F}_q^n$ then $\bar{\rho}(U \setminus \{\vec{0}\})$ is of size v . The following proposition, known as the Feng-Rao bound for primary codes [30, Proposition 8], therefore is operational.

Proposition 9. Let $U \subseteq \mathbb{F}_q^n$ be a vector space of dimension at least 1. The support size of U satisfies

$$\#\text{Supp}(U) \geq \#\cup_{i \in \bar{\rho}(U \setminus \{\vec{0}\})} \Lambda_i. \quad (1)$$

Example 3. This is a continuation of the previous examples. We have $\vec{b}_{28} = \text{ev}(X^4 Y^3 + I)$ and therefore

$$\#\Lambda_{28} = \#\{X^4 Y^3, X^5 Y^3, X^4 Y^4, X^5 Y^4, X^4 Y^5, X^5 Y^5\} = 6.$$

In general, for $\vec{b}_i = \text{ev}(X^\alpha Y^\beta + I)$ (with $0 \leq \alpha, \beta < 6$) we have $\#\Lambda_i = (6 - \alpha)(6 - \beta)$. The situation is depicted in Fig. 2.

6	5	4	3	2	1
12	10	8	6	4	2
18	15	12	9	6	3
24	20	16	12	8	4
30	25	20	15	10	5
36	30	24	18	12	6

Fig. 2. $\#\Lambda_i$ from Example 1 (enumeration with respect to Fig. 1)

Let $F(X, Y)$ be a polynomial whose leading monomial with respect to \prec_{deg} is $X^\alpha Y^\beta$ for some $0 \leq \alpha, \beta < 6$. Consider $\vec{c} = \text{ev}(F + I)$, then, by Proposition 9, $w_H(\vec{c}) \geq (6 - \alpha)(6 - \beta)$. In general, Fig. 2 gives upper bounds on the Hamming weights of all possible words in \mathbb{F}_7^{36} . \diamond

We now turn to relative generalized Hamming weights. Note that although $C_2 \subset C_1$ implies $\bar{\rho}(C_2) \subset \bar{\rho}(C_1)$, it does not always hold that $\vec{c} \in C_1 \setminus C_2$ implies $\bar{\rho}(\vec{c}) \in \bar{\rho}(C_1) \setminus \bar{\rho}(C_2)$. Nevertheless, the Feng-Rao bound for primary codes [30, Theorem 9] still gives us useful information.

Theorem 10. Consider two linear codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$ with $\dim(C_1) = k_1$ and $\dim(C_2) = k_2$. Let u be the smallest element in $\bar{\rho}(C_1)$ that is not in $\bar{\rho}(C_2)$. For $v = 1, \dots, \ell = k_1 - k_2$ we have

$$M_v(C_1, C_2) \geq \min \left\{ \# \cup_{s=1}^v \Lambda_{i_s} \mid u \leq i_1 < \dots < i_v \text{ and } i_1, \dots, i_v \in \bar{\rho}(C_1 \setminus \{\vec{0}\}) \right\}.$$

Example 4. This is a continuation of the previous examples. If $C_2 = \text{Span}\{\vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_5\}$ and $C_1 = \text{Span}\{\vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_4, \vec{b}_5\}$ then

$$M_1(C_1, C_2) \geq \min\{\#\Lambda_4, \#\Lambda_5\} = \min\{24, 25\} = 24.$$

However, if $C_2 = \text{Span}\{\vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_4\}$, while C_1 is unchanged, then $M_1(C_1, C_2) \geq \#\Lambda_5 = 25$. \diamond

To treat dual codes we shall need the following definitions, where the first can be considered as the counterpart of Definition 8, and the last as the counterpart of Definition 6.

Definition 11. For $l \in \mathcal{I}$ define

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

Definition 12. For $\vec{c} \in \mathbb{F}_q^n \setminus \{\vec{0}\}$ define $\eta(\vec{c})$ to be the smallest number $l \in \mathcal{I}$ such that $\vec{c} \cdot \vec{b}_l \neq 0$. Here $\vec{a} \cdot \vec{b}$ means the Euclidean inner product between \vec{a} and \vec{b} .

Given a v -dimensional space U , $\eta(U \setminus \{\vec{0}\})$ is of size v . The following proposition, known as the Feng-Rao bound for dual codes [30, Proposition 13], therefore is operational.

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

$$\#\text{Supp}(U) \geq \# \cup_{l \in \eta(U \setminus \{\vec{0}\})} V_l.$$

Example 5. This is a continuation of the previous examples. For $\vec{b}_l = \text{ev}(X^\alpha Y^\beta + I)$ (with $0 \leq \alpha, \beta < 6$) we have $\#V_l = (\alpha + 1)(\beta + 1)$. Given \vec{c} with $\eta(\vec{c}) = l$, from Proposition 13 we obtain $w_H(\vec{c}) \geq (\alpha + 1)(\beta + 1)$. By Proposition 13, Fig. 3 gives upper bounds on the Hamming weights of all possible words in \mathbb{F}_7^{36} . \diamond

6	12	18	24	30	36
5	10	15	20	25	30
4	8	12	16	20	24
3	6	9	12	15	18
2	4	6	8	10	12
1	2	3	4	5	6

Fig. 3. $\#V_l$ from Example 4 (enumeration with respect to Fig. 1)

We next treat relative generalized Hamming weights. Note that for $C_2 \subset C_1$ it does not in general hold that $\vec{c} \in C_2^\perp \setminus C_1^\perp$ implies $\eta(\vec{c}) \in \bar{\rho}(C_1 \setminus \{\vec{0}\})$. Nevertheless, the Feng-Rao bound for dual codes [30, Theorem 14] still gives us useful information.

Theorem 14. Consider linear codes $C_2 \subset C_1 \subseteq \mathbb{F}_q^n$. Let u^\perp be the largest element in $\bar{\rho}(C_1 \setminus \{\vec{0}\})$. For $v = 1, \dots, \dim(C_1) - \dim(C_2) = \dim(C_2^\perp) - \dim(C_1^\perp)$ we have

$$M_v(C_2^\perp, C_1^\perp) \geq \min\{\#\cup_{s=1}^v V_{i_s} \mid 1 \leq i_1 < \dots < i_v \leq u^\perp, \\ i_1, \dots, i_v \notin \bar{\rho}(C_2)\}.$$

Example 6. This is a continuation of the previous examples. If $C_2 = \text{Span}\{\vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_4\}$ and $C_1 = \text{Span}\{\vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_4, \vec{b}_5, \vec{b}_6\}$, then

$$M_1(C_2^\perp, C_1^\perp) \geq \min\{\#V_5, \#V_6\} = \min\{4, 3\} = 3.$$

However, if $C_1 = \text{Span}\{\vec{b}_1, \vec{b}_2, \vec{b}_3, \vec{b}_4, \vec{b}_5\}$ while C_2 is unchanged then $M_1(C_2^\perp, C_1^\perp) \geq \#V_5 = 4$. \diamond

The above theorems and examples lead us to consider the following family of codes, which have a good behavior with respect to the applications described in the introduction. Consider a Cartesian product $S = S_1 \times \dots \times S_m \subseteq \mathbb{F}_q^m$. For $i = 1, \dots, m$ define the one-variable polynomial

$$F_i(X_i) = \prod_{\alpha \in S_i} (X_i - \alpha), \quad (2)$$

and consider the vanishing ideal of S , $I = \langle F_1(X_1), \dots, F_m(X_m) \rangle \subset \mathbb{F}_q[X_1, \dots, X_m]$. We write $R = \mathbb{F}_q[X_1, \dots, X_m]/I$ and enumerate S as $S = \{\alpha_1, \dots, \alpha_n\}$, where $n = \#S = \prod_{i=1}^m s_i$. Here, we use the notation $s_i = \#S_i$. As in the above examples we then obtain a vector space homomorphism $\text{ev} : R \rightarrow \mathbb{F}_q^n$ defined by $\text{ev}(F + I) = (F(\alpha_1), \dots, F(\alpha_n))$. Now let

$$\Delta(s_1, \dots, s_m) = \{X_1^{i_1} \dots X_m^{i_m} \mid 0 \leq i_t < s_t, t = 1, \dots, m\} \\ = \{N_1, \dots, N_n\},$$

where the enumeration of the N_i 's is with respect to an arbitrary (but fixed) monomial ordering \prec . For general $L \subseteq \Delta(s_1, \dots, s_m)$ define

$$C(L) = \text{Span}\{\text{ev}(X_1^{i_1} \dots X_m^{i_m} + I) \mid X_1^{i_1} \dots X_m^{i_m} \in L\},$$

which is clearly a code of length n . For the purpose of applying the Feng-Rao bounds to the codes $C(L)$ and $C(L)^\perp$ we introduce functions D and D^\perp .

Definition 15. Given $X_1^{i_1} \dots X_m^{i_m} \in \Delta(s_1, \dots, s_m)$, define

$$D(X_1^{i_1} \dots X_m^{i_m}) = \prod_{t=1}^m (s_t - i_t) \text{ and}$$

$$D^\perp(X_1^{i_1} \dots X_m^{i_m}) = \prod_{t=1}^m (i_t + 1).$$

More generally, for $K \subseteq \Delta(s_1, \dots, s_m)$ let

$$D(K) = \#\{N \in \Delta(s_1, \dots, s_m) \mid \\ N \text{ is divisible by some } M \in K\}, \\ D^\perp(K) = \#\{N \in \Delta(s_1, \dots, s_m) \mid \\ N \text{ divides some } M \in K\}.$$

Observe that $D(X_1^{i_1}, \dots, X_m^{i_m}) = D(\{X_1^{i_1}, \dots, X_m^{i_m}\})$ and $D^\perp(X_1^{i_1}, \dots, X_m^{i_m}) = D^\perp(\{X_1^{i_1}, \dots, X_m^{i_m}\})$.

We are now ready to describe the relative parameters of the evaluation codes introduced above.

Theorem 16. Consider $S = S_1 \times \dots \times S_m \subseteq \mathbb{F}_q^m$ and $L_2 \subset L_1 \subseteq \Delta(s_1, \dots, s_m) = \{N_1, \dots, N_n\}$ where the enumeration of the N_i 's is with respect to an arbitrary (but fixed) monomial ordering \prec . Then the

codes $C(L_1)$ and $C(L_2)$ are of length n and their codimension equals $\#L_1 - \#L_2$. Furthermore, for $v = 1, \dots, \#L_1 - \#L_2$ we have

$$M_v(C(L_1), C(L_2)) \geq \min\{D(K) \mid K \subseteq \{N_u, \dots, N_n\} \cap L_1, \#K = v\}, \quad (3)$$

$$M_v(C(L_2)^\perp, C(L_1)^\perp) \geq \min\{D^\perp(K) \mid K \subseteq \{N_1, \dots, N_{u^\perp}\} \setminus L_2, \#K = v\}, \quad (4)$$

where $u = \min\{i \mid N_i \in L_1 \setminus L_2\}$ and $u^\perp = \max\{i \mid N_i \in L_1\}$.

Proof. We start by proving that $\{\text{ev}(N_1 + I), \dots, \text{ev}(N_n + I)\}$ is a basis for \mathbb{F}_q^n as a vector space over \mathbb{F}_q . This fact implies that the dimension of $C(L_i)$ equals $\#L_i$, $i = 1, 2$, and the formula for the codimension follows. Observe that $\text{ev}(F(X_1, \dots, X_m) + I)$ is equal to

$$\begin{aligned} & \text{ev}(F(X_1, \dots, X_m) - A_1(X_1, \dots, X_m)F_1(X_1) - \dots \\ & \quad - A_m(X_1, \dots, X_m)F_m(X_1, \dots, X_m) + I) \end{aligned}$$

for any polynomials A_1, \dots, A_m in the variables X_1, \dots, X_m with coefficients in \mathbb{F}_q . Hence, we may assume that $\deg_{X_1} F < \deg F_1 = s_1, \dots, \deg_{X_m} F < \deg F_m = s_m$. Using Lagrange-interpolation we next see that ev is surjective and, as $\Delta(s_1, \dots, s_m)$ is of the same size as the image \mathbb{F}_q^n , the considered set is indeed a basis for \mathbb{F}_q^n . As in the above examples we enumerate the basis elements $\{\vec{b}_1 = \text{ev}(N_1 + I), \dots, \vec{b}_n = \text{ev}(N_n + I)\}$ (meaning that we order it according to the monomial ordering \prec).

Notice that, regardless of the choice of monomial ordering \prec , $D(N_i) \leq \#L_i$, and that in larger generality¹ $D(\{N_{i_1}, \dots, N_{i_m}\}) \leq \#\cup_{t=1}^m \Lambda_{i_t}$. Therefore (3) follows from Theorem 10. Similarly, regardless of the choice of monomial ordering \prec , $D^\perp(N_i) \leq \#V_i$ and in larger generality² $D^\perp(\{N_{i_1}, \dots, N_{i_m}\}) \leq \#\cup_{t=1}^m V_{i_t}$. Hence, (4) follows from Theorem 14. \square

In the next two sections we show a way to choose $L_2 \subset L_1$ such that the parameters $\ell = \dim C(L_1) - \dim C(L_2) = \#L_1 - \#L_2$, $M_1(C(L_1), C(L_2))$, and $M_1(C(L_2)^\perp, C(L_1)^\perp)$ are good. We study two separate cases. The first case, which we treat in Section III, deals with relatively large codimension. The second case, which we treat in Section IV, concerns relatively small codimensions.

Before studying these two families of codes we briefly discuss the decoding of the related asymmetric quantum codes. Observe that the decoding algorithm for order domain codes described in [37, Section 6.3] can be applied in the more general setting of linear codes with Feng-Rao designed minimum distance. Hence, it can be applied to all codes of the present paper. This holds both for dual codes [46] and primary codes [31]. The decoding algorithm which corrects errors up to half the designed minimum distance uses $\mathcal{O}(n^3)$ operations, where n is the length of the code. In [15, Appendix A] Duursma and Park provided a similar algorithm correcting errors up to half the designed *relative* minimum distance. This was done at the general level of linear codes described by means of their parity check matrix. The application in connection with decoding of asymmetric quantum codes is as follows. To decode both phase-shift and qudit-flip errors up to half the designed values of d_z and d_x one will need two decoding algorithms, namely one which decodes up to $\lfloor (M_1(C_1, C_2) - 1)/2 \rfloor$ errors in connection with $C_2 \subset C_1$, and another which corrects up to $\lfloor (M_1(C_2^\perp, C_1^\perp) - 1)/2 \rfloor$ errors in connection with $C_1^\perp \subset C_2^\perp$ [10], [9]. Duursma and Park's algorithm applies to the last task, but not to the first in its present form. It is an open research problem to modify the decoding algorithm from [15] for general nested dual codes, so that it also works for nested *primary* codes. This probably could be done using the material in [31]. In the absence of such a translation one may instead apply the algorithm from [31] to correct only up to $\lfloor (d(C_1) - 1)/1 \rfloor$ errors in connection with the primary nested codes.

¹Actually equalities hold – which can be seen by applying similar arguments as in Example 2 – but we shall not need this fact.

²Actually again equalities hold, but we shall not need this fact.

III. RELATIVELY LARGE CODIMENSION

One of the nice features of the Feng-Rao bounds is that they come with improved code constructions. In the setting of the codes in the previous section, by applying the improved construction for primary codes [2], we obtain a code $C(L_1)$ of designed distance δ and maximal dimension if we choose

$$L_1 = \{X_1^{i_1} \cdots X_m^{i_m} \in \Delta(s_1, \dots, s_m) \mid D(X_1^{i_1} \cdots X_m^{i_m}) \geq \delta\}. \quad (5)$$

Similarly, by applying the improved construction for dual codes [21], [22] we obtain a code $C(L_2)^\perp$ of designed distance δ^\perp and maximal dimension if we choose

$$L_2 = \{X_1^{i_1} \cdots X_m^{i_m} \in \Delta(s_1, \dots, s_m) \mid D^\perp(X_1^{i_1} \cdots X_m^{i_m}) < \delta^\perp\}. \quad (6)$$

Our first proposal for constructing good pairs of nested codes is to choose L_1 and L_2 as in (5) and (6) with $L_2 \subset L_1$. We then obtain

$$M_1(C(L_1), C(L_2)) \geq d(C(L_1)) \geq \delta, \quad (7)$$

$$M_1(C(L_2)^\perp, C(L_1)^\perp) \geq d(C(L_2)^\perp) \geq \delta^\perp. \quad (8)$$

The codimension $\ell = \#L_1 - \#L_2$ is the largest possible with these designed parameters as, by Proposition 9 and Proposition 13, L_1 is as large as possible and L_2 is as small as possible, such that (7) and (8) hold. Observe that (7) and (8) are independent of the choice of monomial ordering \prec in Theorem 16, as the integers u and u' from that theorem play no role here. Note that $D(X_1^{i_1} \cdots X_m^{i_m}) = \delta$ is a concave function on the domain under consideration, while $D^\perp(X_1^{i_1} \cdots X_m^{i_m}) = \delta^\perp$ is a convex function. Therefore the necessary condition that $L_2 \subset L_1$ creates a restriction on how small a codimension can be for each fixed value of δ (low codimensions require another method which we describe in the next section). The following theorem summarizes the method described.

Theorem 17. *With the above notation, fix two positive integers δ and δ^\perp such that the monomial sets L_1 and L_2 described in (5) and (6), respectively, satisfy that $L_2 \subset L_1$. Then the evaluation codes $C(L_2) \subset C(L_1)$ are of codimension $\ell = \#L_1 - \#L_2$, and the relative minimum distances satisfy $M_1(C(L_1), C(L_2)) \geq \delta$ and $M_1(C(L_2)^\perp, C(L_1)^\perp) \geq \delta^\perp$.*

Remark 18. The case $\delta = \delta^\perp$ and $S = \mathbb{F}_q^m$ is studied in [25], [27] in connection with symmetric quantum codes. There it is characterized when the corresponding sets L_1 and L_2 satisfy the inclusion $L_2 \subset L_1$.

Remark 19. It is possible to show that $d(C(L_1)) = M_1(C(L_1), C(L_2))$, but for general Cartesian product point sets it is unsettled if

$$d(C(L_2)^\perp, C(L_1)^\perp) = M_1(C(L_2)^\perp, C(L_1)^\perp),$$

leaving it undecided if the related asymmetric quantum codes are pure or not.

Below we analyze the parameters of the nested code pairs in Theorem 17 when the sets S_1, \dots, S_m are all of the same size, but first we illustrate the theorem with an example.

Example 7. This is a continuation of the examples in Section II where we considered $S = \mathbb{F}_7^* * \mathbb{F}_7^*$. From Fig. 2 we see that for $\delta = 12$ the set L_1 in (5) becomes

$$L_1 = \{1, X, Y, X^2, XY, Y^2, X^3, X^2Y, XY^2, Y^3, X^4, X^3Y, X^2Y^2, XY^3, Y^4, X^3Y^2, X^2Y^3\}. \quad (9)$$

Hence, $\#L_1 = 17$. According to Fig. 3, $\delta^\perp = 6$ is the highest possible value of δ^\perp such that all $X^\alpha Y^\beta \in \Delta(6, 6)$ with $D^\perp(X^\alpha Y^\beta) < \delta^\perp$ also belong to L_1 . The corresponding set L_2 in (6) then becomes

$$L_2 = \{1, X, Y, X^2, XY, Y^2, X^3, Y^3, X^4, Y^4\} \quad (10)$$

ℓ	2	1	3	1	3	5	3	5	7	2	5	7	9
δ	30	25	25	24	24	24	20	20	20	18	18	18	18
δ^\perp	2	3	2	4	3	2	4	3	2	5	4	3	2
ℓ	3	6	8	10	5	8	10	12	7	9	12	14	16
δ	16	16	16	16	15	15	15	15	12	12	12	12	12
δ^\perp	5	4	3	2	5	4	3	2	6	5	4	3	2
ℓ	9	11	14	16	18	10	12	15	17	19	12	14	17
δ	10	10	10	10	10	9	9	9	9	9	8	8	8
δ^\perp	6	5	4	3	2	6	5	4	3	2	6	5	4
ℓ	19	21	16	18	21	23	25	20	23	25	27	26	28
δ	8	8	6	6	6	6	6	5	5	5	5	4	4
δ^\perp	3	2	6	5	4	3	2	5	4	3	2	4	3
ℓ	30	30	32	34									
δ	4	3	3	2									
δ^\perp	2	3	2	2									

TABLE I
PARAMETERS FROM EXAMPLE 7.

which is of size 10. Hence, the codimension between $C(L_1)$ and $C(L_2)$ is 7, and $M_1(C(L_1), C(L_2)) \geq 12$ and $M_1(C(L_2)^\perp, C(L_1)^\perp) \geq 6$. In a similar fashion we obtain the remaining parameters in Table I. Note that if we have a code pair $C(L_2) \subset C(L_1)$ with designed parameters $\delta = a$, $\delta^\perp = b$ and $\#L_1 - \#L_2 = \ell$ then there exist $L'_2 \subset L'_1$ with designed parameters of $C(L'_2) \subset C(L'_1)$ being $\delta = b$, $\delta^\perp = a$ and $\#L'_1 - \#L'_2 = \ell$. Hence, in Table I we only list parameters with $\delta \geq \delta^\perp$. We also exclude cases with $\delta^\perp = 1$ (corresponding to $C_2 = \{\vec{0}\}$).

◇

In the following we find closed formula expressions for the parameters of the coset construction in Theorem 17 when S_1, \dots, S_m are all of the same size. We start with a lemma explaining for which choices of δ and δ^\perp the theorem works.

Lemma 20. *Assume $s = s_1 = \dots = s_m$ and consider $\delta \in \{1, \dots, s^m\}$. Let $v \in \{0, \dots, m-1\}$ be such that $s^v \leq \delta \leq s^{v+1}$. If $\delta^\perp \leq \lfloor (s - \frac{\delta}{s^v} + 1)s^{m-v-1} \rfloor$ then the set L_2 from (6) is contained in the set L_1 from (5).*

Proof. Define functions $\tilde{D} : \mathbb{Q}^m \rightarrow \mathbb{Q}$ and $\tilde{D}^\perp : \mathbb{Q}^m \rightarrow \mathbb{Q}$ by $\tilde{D}((i_1, \dots, i_m)) = \prod_{t=1}^m (s - i_t)$ and $\tilde{D}^\perp((i_1, \dots, i_m)) = \prod_{t=1}^m (i_t + 1)$. Let $i = s - \delta/s^v$ and note that $0 \leq i \leq s-1$ as well as

$$\tilde{D}(\underbrace{(0, \dots, 0)}_{v \text{ times}}, i, \underbrace{(s-1, \dots, s-1)}_{m-1-v \text{ times}}) = \delta$$

hold true. Finally we observe that

$$\tilde{D}^\perp(\underbrace{(0, \dots, 0)}_{v \text{ times}}, i, \underbrace{(s-1, \dots, s-1)}_{m-1-v \text{ times}}) = (s - \frac{\delta}{s^v} + 1)s^{m-v-1}$$

and the lemma follows. □

The next step in our analysis is to establish an estimate from below on the dimension of the code $C(L_1)$ and $C(L_2)^\perp$ when L_1 is as in (5), L_2 is as in (6) and $s = s_1 = \dots = s_m$. In [29, Theorem 1] a bound was given for the special case $S_1 = \dots = S_m = \mathbb{F}_q$ and $q^{m-1} \leq \delta, \delta^\perp \leq q^m$. With the last mentioned condition we do not obtain $L_2 \subset L_1$ and we therefore now generalize the result from [29] to arbitrary $1 \leq \delta^\perp, \delta \leq s^m$ and $s = s_1 = \dots = s_m$. We start with a technical lemma, whose proof we give in Appendix A.

Lemma 21. For $m \geq 2$, $1 \leq i \leq m$ it holds that

$$\begin{aligned} & \int_0^{s-\frac{\tau}{s^{m-i}(s-x_1)\cdots(s-x_{i-1})}} \int_0^{s-\frac{\tau}{s^{m-i-1}(s-x_1)\cdots(s-x_i)}} \cdots \\ & \int_0^{s-\frac{\tau}{(s-x_1)\cdots(s-x_{m-1})}} dx_m \cdots dx_{i+1} dx_i \\ &= s^{m-i+1} - \sum_{t=0}^{m-i} \left[\frac{1}{t!} \frac{\tau}{(s-x_1)\cdots(s-x_{i-1})} \right. \\ & \quad \left. \cdot \left(\ln \left(\frac{(s-x_1)\cdots(s-x_{i-1})s^{m-i+1}}{\tau} \right) \right)^t \right]. \end{aligned}$$

From this lemma we obtain information on the dimensions of the codes as follows.

Theorem 22. Let $s = s_1 = \cdots = s_m$ and consider L_1 and L_2 as in (5) and (6), respectively with $\delta = \delta^\perp = \tau \in \{1, \dots, s^m\}$. The dimensions of $C(L_1)$ and $C(L_2)^\perp$ are at least

$$s^m - \sum_{t=1}^m \frac{1}{(t-1)!} \tau \left(\ln \left(\frac{s^m}{\tau} \right) \right)^{t-1}. \quad (11)$$

If $1 \leq \tau < s$ then the dimensions are at least

$$s^m - \sum_{t=1}^m \frac{1}{(t-1)!} \tau ((m-1) \ln(\tau))^{t-1} \quad (12)$$

which is sharper than (11).

Proof. By symmetry it is enough to prove the result for $C(L_1)$. The dimension of $C(L_1)$, i.e. the number of integer tuples $(i_1, \dots, i_m) \in \{0, \dots, s-1\}^m$ with $(s-i_1)\cdots(s-i_m) \geq \tau$, is at least that of the volume of

$$\{(x_1, \dots, x_m) \in [0, s]^m \mid (s-x_1)\cdots(s-x_m) \geq \tau\}$$

which corresponds to the integral in Lemma 21 when i is chosen to be equal to 1. This proves (11). Next, assume $1 \leq \tau < s$. The above mentioned set of integer tuples can be divided into two sets, the first set consisting of those tuples satisfying $0 \leq i_v < s - \tau$ for some $v \in \{1, \dots, m\}$, and the second set consisting of those tuples satisfying $s - \tau \leq i_v$ for $v = 1, \dots, m$. The number of elements in the first set equals $s^m - \tau^m$. The cardinality of the second set is estimated from below by the volume of

$$\{(x_1, \dots, x_m) \in [0, \tau]^m \mid (\tau-x_1)\cdots(\tau-x_m) \geq \tau\}.$$

The last part of the theorem now follows by applying Lemma 21 with $i = 1$ and $s = \tau$. \square

Remark 23. From Theorem 22 one obtains for each choice of m closed formula lower bounds on the rate k/n as a function of the relative minimum distance³ d/n . Such estimates are independent of the actual value of s . From the proof it is clear that these estimates become more and more precise as s increases. Computer experiments reveal that with $m = 2$ and $m = 3$ already for $s = 32$ the true values of the rate is almost the same as the estimated.

Using the constructions described in Section I we get by applying Lemma 20 in combination with (11) from Theorem 22 the following result on the existence of ramp secret sharing schemes and asymmetric quantum codes.

³Here, the relative minimum distance should not be confused with the first relative generalized Hamming weight.

Theorem 24. Consider integers $m \geq 2$ and $s \leq q$, where q is a prime power. Given $\delta \in \{1, \dots, s^m\}$ let $v \in \{0, \dots, m-1\}$ be such that $s^v \leq \delta \leq s^{v+1}$ and choose an integer $\delta^\perp \leq \lfloor (s - \frac{\delta}{s^v} + 1)s^{m-v-1} \rfloor$. From Theorem 17 we obtain ramp secret sharing schemes over \mathbb{F}_q with $n = s^m$ participants, shares in \mathbb{F}_q^ℓ where

$$\ell \geq s^m - \sum_{t=1}^m \frac{1}{(t-1)!} \left(\delta \left(\ln \left(\frac{s^m}{\delta} \right) \right)^{t-1} + \delta^\perp \left(\ln \left(\frac{s^m}{\delta^\perp} \right) \right)^{t-1} \right),$$

the first privacy number satisfying $t = t_1 \geq \delta^\perp - 1$ and the last reconstruction number satisfying $r = r_\ell \leq s^m - \delta + 1$. Similarly, we obtain asymmetric quantum codes with parameters

$$[[n = s^m, \ell, d_z \geq \delta/d_x \geq \delta^\perp]]_q.$$

Remark 25. The lower bound on ℓ in Theorem 24 can be improved in the case $1 \leq \delta < s$ or $1 \leq \delta^\perp < s$ by applying (12) instead of (11).

Recall from Remark 5 that studying asymmetric quantum codes derived from the CSS construction is equivalent to studying linear ramp secret sharing schemes. Therefore, the following discussion on asymmetric quantum codes imposed by Theorem 17 can be directly translated into results on ramp secret sharing schemes. We leave the details for the reader. It seems relevant to compare in some concrete cases what can be derived from Theorem 17 in combination with Theorem 3 with other general constructions in the literature of asymmetric quantum codes of similar length. Applying Theorem 17 to polynomials in two variables and to a Cartesian product $S = S_1 \times S_2$ we obtain from Theorem 3 asymmetric stabilizer codes of length $s_1 s_2$, where $s_1 = \#S_1$ and $s_2 = \#S_2$. For comparison La Guardia's Construction II of asymmetric quantum generalized Reed-Solomon codes [44, Theorem 7.1] gives codes of length $m_1 m_2$ as follows:

Theorem 26. Let q be a prime power. Then there exist asymmetric quantum generalized Reed-Solomon codes with parameters

$$[[m_1 m_2, \ell = m_1(2k - m_2 + c), d_z \geq d/d_x \geq (d - c)]]_q,$$

where $1 < k < m_2 < 2k + c \leq q^{m_1}$, $k = m_2 - d + 1$, and $m_2, d > c + 1$, $c \geq 1$, $m_1 \geq 1$ are integers.

Observe that the bound $d_z \geq m_2 - k + 1$ in Theorem 26 suggests that to obtain the widest variety of code parameters for a given code length one should choose m_1 smallest possible and m_2 largest possible, such that the conditions in the theorem are satisfied. The surprising consequence – which we illustrate in the following example – is that sometimes one obtains better parameters from Theorem 26 by considering a shorter code length. Adding 0s to the code words of the shorter code, we then obtain bounds on codes of the right length.

Example 8. We first consider asymmetric quantum codes with $q = 7$ and of length 49. Applying Theorem 26 directly to the case of $n = 49$ we obtain six different sets of parameters. However, we can actually derive better information on codes of length 49 by applying Theorem 26 to codes of length $n = 48$. In Table II a selection of such parameters are compared with examples of what can be achieved by applying Theorem 17 instead. In the table, by “—” we indicate that no comparable parameters can be derived. The advantage of our method is clear in most cases. Furthermore, all the codes in Table II coming from Theorem 17 strictly exceed the Gilbert-Varshamov bound (Theorem 4).

We next consider asymmetric quantum codes with $q = 8$ and of length 64. Our theorem treats many more constellations of d_z/d_x with $d_z \geq d_x$ than does Theorem 26. For instance, the highest value of d_z treated by Theorem 26 is $d_z = 31$, whereas Theorem 17 describes 35 different nested code pairs with $d_z \geq 32$. In most cases the code parameters guaranteed by Theorem 17 are much better than the parameters described in Theorem 26. However, there are also cases where the situation is the opposite. From the huge amount of obtainable values d_z/d_x we display in Table III some representative examples that illustrate the situation. Again all listed codes coming from Theorem 17 strictly exceed the Gilbert-Varshamov bound. \diamond

Theorem 26 ([44, Theorem 7.1])	Theorem 17
—	$[[49, 3, 30/4]]_7$
—	$[[49, 8, 24/4]]_7$
—	$[[49, 5, 24/5]]_7$
—	$[[49, 9, 20/5]]_7$
$[[49, 10, 14/7]]_7$	$[[49, 10, 14/7]]_7$
$[[49, 12, 14/6]]_7$	$[[49, 14, 14/6]]_7$
$[[49, 16, 12/6]]_7$	$[[49, 18, 12/6]]_7$
$[[49, 18, 10/7]]_7$	$[[49, 16, 10/7]]_7$

TABLE II

COMPARISON OF CODE PARAMETERS IN EXAMPLE 8. PARAMETERS FROM APPLYING THEOREM 26 TO CODES OF LENGTH $n = 48$ ON THE LEFT, AND PARAMETERS FROM THEOREM 17 ON THE RIGHT.

Theorem 26 ([44, Theorem 7.1])	Theorem 17
—	$[[64, 5, 35/5]]_8$
—	$[[64, 12, 30/4]]_8$
—	$[[64, 9, 30/5]]_8$
—	$[[64, 7, 30/6]]_8$
$[[64, 6, 25/6]]_8$	$[[64, 10, 25/6]]_8$
$[[64, 6, 24/7]]_8$	$[[64, 10, 24/7]]_8$
$[[64, 50, 5/4]]_8$	$[[64, 51, 5/4]]_8$

TABLE III

COMPARISON OF CODE PARAMETERS IN EXAMPLE 8. PARAMETERS FROM THEOREM 26 ON THE LEFT AND PARAMETERS FROM THEOREM 17 ON THE RIGHT.

Example 9. In this example we consider $S_1, S_2 \subseteq \mathbb{F}_7$ with $\#S_1 = 6$ and $\#S_2 = 7$ and apply Theorem 17 and Theorem 26 to construct asymmetric quantum codes of length $n = 42$. In most cases Theorem 17 is much better than Theorem 26, however, there also exists a number of cases where the latter is the best. Table IV displays some illustrative examples. As in the previous example all displayed cases coming from Theorem 17 strictly exceed the Gilbert-Varshamov bound. \diamond

Example 10. This is a continuation of Example 7. From Table I one can show that all related asymmetric quantum codes strictly exceed the Gilbert-Varshamov bound (Theorem 4). The details are left for the reader.

We conclude this section with an example illustrating how to derive relative generalized Hamming weights of the considered codes. Recall from Section I that such information directly translates into information on the privacy numbers and the reconstruction numbers of the corresponding ramp secret sharing schemes.

Example 11. In this example we apply Theorem 16 to estimate the parameters $M_v(C(L_1), C(L_2))$,

Theorem 26 ([44, Theorem 7.1])	Theorem 17
—	$[[42, 4, 20/5]]_7$
$[[42, 2, 18/4]]_7$	$[[42, 9, 18/4]]_7$
$[[42, 6, 16/4]]_7$	$[[42, 10, 16/4]]_7$
$[[42, 10, 14/4]]_7$	$[[42, 13, 14/4]]_7$
$[[42, 14, 10/6]]_7$	$[[42, 14, 10/6]]_7$
$[[42, 16, 9/6]]_7$	$[[42, 15, 9/6]]_7$
$[[42, 24, 7/4]]_7$	$[[42, 23, 7/4]]_7$
$[[42, 28, 5/4]]_7$	$[[42, 29, 5/4]]_7$

TABLE IV

COMPARISON OF CODE PARAMETERS IN EXAMPLE 9. PARAMETERS FROM THEOREM 26 ON THE LEFT AND PARAMETERS FROM THEOREM 17 ON THE RIGHT.

v	1	2	3	4	5	6	7
$M_v(C(L_1), C(L_2)) \geq$	12	15	16	18	20	22	23
$M_v(C(L_2)^\perp, C(L_1)^\perp) \geq$	6	8	9	11	12	14	15

TABLE V

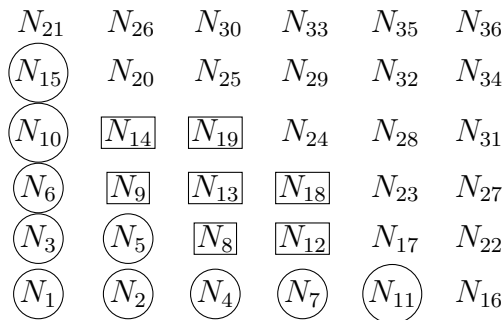
ESTIMATED RELATIVE GENERALIZED HAMMING WEIGHTS OF THE CODE PAIR IN EXAMPLE 11.

v	1	2	3	4	5	6	7
$t_v \geq$	5	7	8	10	11	13	14
$r_v \leq$	25	22	21	19	17	15	14

TABLE VI

PRIVACY NUMBERS AND RECONSTRUCTION NUMBERS OF THE RAMP SECRET SHARING SCHEME DESCRIBED IN EXAMPLE 11.

$M_v(C(L_2)^\perp, C(L_1)^\perp)$, $v = 1, \dots, \#L_1 - \#L_2 = 7$ where L_1 and L_2 are as in (9) and (10), respectively. See Fig. 4. Recall that the monomial ordering, that we use in this example, is the degree lexicographic

Fig. 4. The situation in Example 11: L_2 corresponds to the circled monomials and L_1 equals L_2 plus the boxed monomials.

ordering \prec_{deg} . We therefore obtain $u = \min\{i \mid N_i \in L_1 \setminus L_2\} = 8$ and $u^\perp = \max\{i \mid N_i \in L_1\} = 19$. Hence, (3) becomes

$$M_v(C(L_1), C(L_2)) \geq \min \{D(K) \mid K \subseteq \{N_8, N_9, N_{10}, N_{11}, N_{12}, N_{13}, N_{14}, N_{15}, N_{18}, N_{19}\}, \#K = v\},$$

and (4) becomes

$$M_v(C(L_2)^\perp, C(L_1)^\perp) \geq \min \{D^\perp(K) \mid K \subseteq \{N_8, N_9, N_{12}, N_{13}, N_{14}, N_{16}, N_{17}, N_{18}, N_{19}\}, \#K = v\}.$$

Going through all possible combinations we obtain the information in Table V. Hence, we can construct a ramp secret sharing scheme over \mathbb{F}_7 with $n = 36$ participants, with the secrets belonging to \mathbb{F}_7^7 and with the privacy numbers being as in Table VI. ◇

IV. RELATIVELY SMALL CODIMENSION

In the former section we demonstrated how to construct good pairs of nested codes having relatively large codimension. We now show how to obtain good pairs of nested codes with relatively small codimension. To explain the idea behind our method, we start with an example which leads to a formal statement in Theorem 27 below.

Example 12. This is a continuation of the series of examples where we consider codes over $\mathbb{F}_7^* \times \mathbb{F}_7^*$, and where we use the degree lexicographic ordering \prec_{deg} . Consider

$$L_1 = \{X^\alpha Y^\beta \in \Delta(6, 6) \mid X^\alpha Y^\beta \preceq_{\text{deg}} XY^3\}, \quad (13)$$

$$L_2 = \{X^\alpha Y^\beta \in \Delta(6, 6) \mid X^\alpha Y^\beta \prec_{\text{deg}} X^3 Y\}. \quad (14)$$

$$\begin{array}{c} v \\ M_v(C(L_1), C(L_2)) \geq \\ M_v(C(L_2)^\perp, C(L_1)^\perp) \geq \end{array} \left| \begin{array}{ccc} 1 & 2 & 3 \\ 15 & 19 & 22 \\ 8 & 11 & 13 \end{array} \right.$$

TABLE VII

ESTIMATED RELATIVE GENERALIZED HAMMING WEIGHTS OF THE FIRST CODE PAIR IN EXAMPLE 12

$$\begin{array}{c} \ell = \#L_1 - \#L_2 \\ M_1(C(L_1), C(L_2)) \geq \\ d(C(L_1)) \geq \\ M_1(C(L_2)^\perp, C(L_1)^\perp) \geq \\ d(C(L_2)^\perp) \geq \end{array} \left| \begin{array}{cccccc} 1 & 2 & 3 & 1 & 4 & 2 \\ 25 & 20 & 15 & 16 & 10 & 12 \\ 24 & 18 & 12 & 12 & 6 & 6 \\ 4 & 6 & 8 & 9 & 10 & 12 \\ 3 & 4 & 5 & 5 & 6 & 6 \end{array} \right.$$

TABLE VIII

THE FIRST WEIGHTS IN EXAMPLE 12.

The situation is described in Fig. 5

$$\begin{array}{cccccc} N_{21} & N_{26} & N_{30} & N_{33} & N_{35} & N_{36} \\ N_{15} & N_{20} & N_{25} & N_{29} & N_{32} & N_{34} \\ \textcircled{N_{10}} & \boxed{N_{14}} & N_{19} & N_{24} & N_{28} & N_{31} \\ \textcircled{N_6} & \textcircled{N_9} & \boxed{N_{13}} & N_{18} & N_{23} & N_{27} \\ \textcircled{N_3} & \textcircled{N_5} & \textcircled{N_8} & \boxed{N_{12}} & N_{17} & N_{22} \\ \textcircled{N_1} & \textcircled{N_2} & \textcircled{N_4} & \textcircled{N_7} & \textcircled{N_{11}} & N_{15} \end{array}$$

Fig. 5. The situation in Example 12: The circled monomials correspond to L_2 . The circled and the boxed monomials correspond to L_1 .

The codimension is 3 and the values of u and u^\perp in Theorem 16 become $u = \min\{i \mid N_i \in L_1 \setminus L_2\} = 12$ (corresponding to $N_u = X^3Y$), and $u^\perp = \max\{i \mid N_i \in L_1\} = 14$ (corresponding to $N_{u^\perp} = XY^3$). By inspection we see that, due to the particular choice of L_1 and L_2 , in (3) and (4) of Theorem 16 we need only to consider monomials in $L_1 \setminus L_2$. That is, we obtain

$$\begin{aligned} M_v(C(L_1), C(L_2)) &\geq \min\{D(K) \mid \\ &K \subseteq \{X^3Y, X^2Y^2, XY^3\}, \#K = v\}, \end{aligned}$$

$$\begin{aligned} M_v(C(L_2)^\perp, C(L_1)^\perp) &\geq \min\{D^\perp(K) \mid \\ &K \subseteq \{X^3Y, X^2Y^2, XY^3\}, \#K = v\}, \end{aligned}$$

for $v = 1, 2, 3$. From this we easily obtain the parameters in Table VII.

In a similar way we have in (3) and (4) only monomials from $L_1 \setminus L_2$, if in (13) and (14) we replace (XY^3, X^3Y) with (XY, XY) , (XY^2, X^2Y) , (X^2Y^2, X^2Y^2) , (XY^4, X^4Y) , (X^2Y^3, X^3Y^2) , (X^2Y^4, X^4Y^2) , (X^3Y^3, X^3Y^3) , (X^3Y^4, X^4Y^3) , or (X^4Y^4, X^4Y^4) . However, due to symmetry, we only need to consider the first five cases (in addition to the case that we have already considered). For instance from (X^4Y^4, X^4Y^4) we derive the same estimates for $M_v(C(L_1), C(L_2))$ and $M_v(C(L_2)^\perp, C(L_1)^\perp)$, respectively, as we would derive from (XY, XY) for $M_v(C(L_2)^\perp, C(L_1)^\perp)$ and $M_v(C(L_1), C(L_2))$, respectively (the order of parameters being reversed). In Table VIII we list our estimates of relative minimum distances and these are compared to the estimates of minimum distances to demonstrate the advantage of the proposed code construction. In this example we did in (13) and (14), not consider replacing XY^3 and X^3Y , respectively, with Y^a and X^a , respectively. The arguments of the example surely would apply also in this case, however, the corresponding nested codes are of Reed-Muller type, and such codes do not have impressive parameters. \diamond

The method of Example 12 can be applied to any point set $S_1 \times S_2$ with $s = \#S_1 = \#S_2$. The idea is to consider the intersection of a line with slope -1 and the lattice $\Delta(s, s)$. From either direction, both values $D(X^i Y^j)$ and $D^\perp(X^i Y^j)$ strictly increase, while moving on the line segment toward its middle. Hence, choosing $L_2 \subset L_1$ in such a way that $L_1 \setminus L_2$ is equal to a center part of a line segment of slope -1 produces good relative minimum distances.

Theorem 27. Consider $S_1, S_2 \subseteq \mathbb{F}_q$ with $s = \#S_1 = \#S_2$. Let $I = \langle F_1(X), F_2(Y) \rangle \subset \mathbb{F}_q[X, Y]$, where F_1 and F_2 are as in (2). Consider $X^i Y^j \in \Delta(s, s)$ with $i \leq j$ and let

$$L_1 = \{N \in \Delta(s, s) \mid N \preceq_{\text{deg}} X^i Y^j\}, \quad (15)$$

$$L_2 = \{N \in \Delta(s, s) \mid N \prec_{\text{deg}} X^j Y^i\}. \quad (16)$$

The codes $C(L_1)$ and $C(L_2)$ are of length $n = s^2$ and their codimension equals $\ell = j - i + 1$. The relative minimum distances satisfy

$$M_1(C(L_1), C(L_2)) = (s - i)(s - j), \quad (17)$$

$$M_1(C(L_2)^\perp, C(L_1)^\perp) \geq (i + 1)(j + 1), \quad (18)$$

and for $v = 2, \dots, \ell$

$$\begin{aligned} M_v(C(L_1), C(L_2)) &= (s - i)(s - j) \\ &\quad + \sum_{t=2}^v ((s - i) - (t - 1)) \\ &= (s - i)(s - j + v - 1) \\ &\quad - \frac{v(v - 1)}{2}, \end{aligned} \quad (19)$$

$$\begin{aligned} M_v(C(L_2)^\perp, C(L_1)^\perp) &\geq (i + 1)(j + 1) + \\ &\quad \sum_{t=2}^v ((j + 1) - (t - 1)) \\ &= (i + v)(j + 1) - \frac{v(v - 1)}{2}. \end{aligned} \quad (20)$$

Proof. We first establish the bounds

$$\begin{aligned} M_v(C(L_1), C(L_2)) &\geq \min \{D(K) \mid \\ &\quad K \subseteq \{X^j Y^i, X^{j-1} Y^{i+1}, \dots, X^i Y^j\}, \#K = v\}, \end{aligned} \quad (21)$$

$$\begin{aligned} M_v(C(L_2)^\perp, C(L_1)^\perp) &\geq \min \{D^\perp(K) \mid \\ &\quad K \subseteq \{X^j Y^i, X^{j-1} Y^{i+1}, \dots, X^i Y^j\}, \#K = v\}. \end{aligned} \quad (22)$$

We do this by applying Theorem 16 with \prec_{deg} as the chosen monomial ordering. In particular $\Delta(s, s) = \{N_1, \dots, N_{s^2}\}$ where the enumeration of the N_i s is with respect to \prec_{deg} . Consider $u = \min\{i \mid N_i \in L_1 \setminus L_2\}$ and $u^\perp = \max\{i \mid N_i \in L_1\}$. The u th element of $\Delta(s, s)$ now is $N_u = X^j Y^i$ and the u^\perp th element is $N_{u^\perp} = X^i Y^j$. By (3) and (4) the right-hand sides of (21) and (22) therefore serve as lower bounds on their respective left-hand sides.

We next prove (17) and (18). From (21) we have

$$\begin{aligned} &M_1(C(L_1), C(L_2)) \\ &\geq \min\{D(X^j Y^i), D(X^{j-1} Y^{i+1}), \dots, D(X^i Y^j)\} \\ &= \min\{(s - (i + v))(s - (j - v)) \mid \\ &\quad v = 0, \dots, \ell - 1 = j - i\} \\ &= (s - i)(s - j) \end{aligned}$$

(equality of the convex function is attained for $v = 0$ and $v = \ell - 1$). This proves that the right-hand side of (17) is larger than or equal to the left-hand side. In a similar fashion we establish the inequality (18). To establish equality in (17) we only need to find a codeword in $C(L_1) \setminus C(L_2)$ with $(s-i)(s-j)$ non-zeros. To this end, write $S_1 = \{\alpha_1, \dots, \alpha_s\}$ and $S_2 = \{\beta_1, \dots, \beta_s\}$ and consider

$$F(X, Y) = \prod_{w=1}^i (X - \alpha_w) \prod_{r=1}^j (Y - \beta_r)$$

which has exactly the prescribed number of non-zeros in $S_1 \times S_2$. The codeword $\vec{c} = \text{ev}(F(X, Y) + I)$ clearly belongs to $C(L_1) \setminus C(L_2)$ and therefore we have established equality in (17).

In a similar way we can show that equality actually holds in (21). This is done by considering for each possible set $K \subseteq \{X^j Y^i, X^{j-1} Y^{i+1}, \dots, X^i Y^j\}$ the corresponding set of $\#K$ polynomials as above. The number of elements in $S_1 \times S_2$, that are non-zeros of at least one of these polynomials, equals $D(K)$.

It remains to show that the right-hand side of (21) equals the right-hand side of (19), and that the right-hand side of (22) equals the right-hand side of (20). For convenience, we will explain the case in (19) for $v = 2$. The cases $v \geq 3$ can be proved with the same reasoning by using the principle of inclusion and exclusion. A similar and straightforward reasoning, where one should replace $(s-i)(s-j)$ with $(i+1)(j+1)$ gives the corresponding formula for the case in (20).

Indeed, note that we are considering sets $K = \{X^{j-x} Y^{i+x}, X^{j-y} Y^{i+y}\}$, where one can assume $0 \leq x < y \leq j-i = \ell-1$. Then $D(K)$ equals the cardinality of the set of monomials which are divisible by either $X^{j-x} Y^{i+x}$ or $X^{j-y} Y^{i+y}$. So, we have to compute the sum of the cardinalities of the set of monomials divisible by $X^{j-x} Y^{i+x}$ plus that of the set of monomials divisible by $X^{j-y} Y^{i+y}$ minus that of the set of monomials divisible by both of them. Therefore,

$$\begin{aligned} D(K) &= ((s-j) + x)((s-i) - x) \\ &\quad + ((s-j) + y)((s-i) - y) \\ &\quad - ((s-j) + x)((s-i) - y). \end{aligned}$$

We are looking for the minimum of that function within the above mentioned region. Derivatives show that the minimum will appear on the boundary. As a consequence we find it for the values $x = 0$ and $y = 1$ which give the value $(s-i)(s-j) + (s-i-1)$ in the statement. This concludes the proof. \square

Proposition 28. *Let the notation be as in Theorem 27 and consider $\sigma \in \{0, \dots, s-1\}$. Then for any positive integer $\ell \leq \sigma + 1$ such that ℓ is even if and only if σ is odd we obtain nested code pairs $C(L_2) \subset C(L_1)$ of codimension ℓ with*

$$M_1(C(L_1), C(L_2)) = \binom{s - \frac{\sigma - \ell + 1}{2}}{s - \frac{\sigma + \ell - 1}{2}} \quad (23)$$

$$M_1(C(L_2)^\perp, C(L_1)^\perp) \geq \binom{\frac{\sigma - \ell + 3}{2}}{\frac{\sigma + \ell + 1}{2}} \quad (24)$$

and if $\ell \leq \sigma - 1$ then

$$d(C(L_1)) = s(s - \sigma) < M_1(C(L_1), C(L_2)). \quad (25)$$

Similarly we obtain code pairs of codimension ℓ with

$$M_1(C(L_1), C(L_2)) = \binom{\frac{\sigma - \ell + 3}{2}}{\frac{\sigma + \ell + 1}{2}} \quad (26)$$

$$\begin{aligned} M_1(C(L_2)^\perp, C(L_1)^\perp) \\ \geq \binom{s - \frac{\sigma - \ell + 1}{2}}{s - \frac{\sigma + \ell - 1}{2}} \end{aligned} \quad (27)$$

and if $\ell \leq \sigma - 1$ then

$$d(C(L_1)) = \sigma + 1 < M_1(C(L_1), C(L_2)).$$

Proof. We only prove (23), (24) and (25). The other results follow by symmetry. Choose $0 \leq i \leq j < s$ with $i + j = \sigma < s$ and $\ell = j - i + 1$. Then $i = \frac{\sigma - \ell + 1}{2}$, $j = \frac{\sigma + \ell - 1}{2}$ and the first two results follow from Theorem 27. Finally, $d(C(L_1)) = M_1(C(L_1), \{\vec{0}\}) = D(X^\sigma) = s(s - \sigma)$. \square

Corollary 29. Consider integers $1 < s \leq q$, where q is a prime power and let $\sigma \in \{0, \dots, s - 1\}$. Then for any $\ell \leq \sigma + 1$ such that ℓ is even if and only if σ is odd we obtain from Proposition 28 ramp secret sharing schemes over \mathbb{F}_q with $n = s^2$ participants, shares in \mathbb{F}_q^ℓ and either

$$\begin{aligned} t = t_1 &\geq \left(\frac{\sigma - \ell + 3}{2}\right) \left(\frac{\sigma + \ell + 1}{2}\right) - 1 \\ r = r_\ell &= s^2 - \left(s - \frac{\sigma - \ell + 1}{2}\right) \left(s - \frac{\sigma + \ell - 1}{2}\right) + 1 \end{aligned}$$

or

$$\begin{aligned} t = t_1 &\geq \left(s - \frac{\sigma - \ell + 1}{2}\right) \left(s - \frac{\sigma + \ell - 1}{2}\right) - 1 \\ r = r_\ell &= s^2 - \left(\frac{\sigma - \ell + 3}{2}\right) \left(\frac{\sigma + \ell + 1}{2}\right) + 1. \end{aligned}$$

Similarly we obtain asymmetric quantum codes with parameters

$$[[n = s^2, \ell, d_z/d_x]]_q$$

where d_z equals the right hand side of (23) and d_x is greater than or equal to the right hand side of (24) (and similarly with (26) and (27)). If $\ell \leq \sigma - 1$ then the asymmetric quantum codes are impure.

Remark 30. As mentioned in the introduction it is often desirable to have asymmetric quantum codes with d_z much larger than d_x . One such family is obtained from Corollary 29 with parameters $[[n = s^2, \ell, d_z \geq s(s - \ell + 1)/d_x = \ell]]_q$ for any $\ell \in \{1, \dots, s - 1\}$. For $q = 7, 8, 9$ and $\ell = 1, 2, 3, 4, 5$ these codes strictly exceed the Gilbert-Varshamov bound (Theorem 4). Similarly for $q = 5, 11, 13, 16, 17, 19, 23, 25$ and $\ell = 1, 2, 3, 4$.

Example 13. In this example we consider asymmetric quantum codes as in Corollary 29 with $d_z = \delta$ being equal to the right hand side of (23) and d_x being greater than or equal to δ^\perp which we define as the right hand side of (24). We treat the cases $n = q^2$, where $q = 3, 4, 5, 7, 8, 9$. In the literature e.g. [42], [17], [44] one can find extensive tables of quantum stabilizer code parameters derived by applying Theorem 3, however, they only use the bound $d_z \geq d(C_1)$ and $d_x \geq d(C_2^\perp)$, where $d(C_1)$ and $d(C_2^\perp)$ are the minimum distances of concrete code pairs with $C_2 \subset C_1$. The present example illustrates the huge advantage of using instead the relative minimum distances (which is what is behind the bounds in Corollary 29). This is done by investigating for each ℓ and δ what is the highest value $g(\ell, \delta)$ such that the tables of best known linear codes in [34] guarantee the existence of linear code pairs A, B^\perp satisfying $\dim A - \dim B = \ell$, $d(A) \geq \delta$, and $d(B^\perp) \geq g(\ell, \delta)$ (this is in the spirit of [18, Theorem 2]). Observe, that we make no assumption whatsoever that $B \subset A$. Actually, such inclusion is very unlikely to hold when one chooses two codes A and B^\perp which are optimal with respect to the tables of best known linear codes in [34]. In Table IX we list values of $(\ell, \delta, \delta^\perp, g(\ell, \delta))$. The many cases where δ^\perp is close to $g(\ell, \delta)$ illustrate the huge advantage of using the construction in Theorem 27 and taking into account the relative minimum distances. Note that, there are even two cases where δ^\perp exceeds the corresponding $g(\ell, \delta)$, namely for $q = 7$ and $(\ell, \delta, \delta^\perp, g(\ell, \delta))$ equal to $(3, 15, 15, 14)$ or $(2, 30, 6, 5)$. All displayed code parameters coming from Theorem 27 strictly exceed the Gilbert-Varshamov bound (Theorem 4). \diamond

q	$(\ell, \delta, \delta^\perp, g(\ell, \delta))$
3	(1,4,4,4)
4	(2,6,6,6) (1,9,4,4)
5	(3,8,9,9) (1,9,9,9) (2,12,6,6) (1,16,4,4)
7	(5,12,12,18) (3,15,15,14) (1,16,16,17) (4,18,10,13) (2,20,12,12) (3,24,8,9) (1,25,9,10) (2,30,6,5) (1,36,4,4)
8	(5,21,12,19) (3,24,15,16) (1,25,16,16) (4,18,18,21) (2,20,20,22) (4,28,10,13) (2,30,12,13) (3,35,8,8) (1,36,9,10) (2,42,6,6) (1,49,4,4)
9	(3,24,24,26) (1,25,25,26) (5,21,21,27) (4,28,18,21) (2,30,20,22) (5,32,12,18) (3,35,15,16) (1,36,16,16) (4,40,10,13) (2,42,12,14) (3,48,8,8) (1,49,9,9) (2,56,6,6) (1,64,4,4)

TABLE IX

CORRESPONDING VALUES OF $(\ell, \delta, \delta^\perp, g(\ell, \delta))$ FROM EXAMPLE 13. THE MANY CASES WITH δ^\perp CLOSE TO $g(\ell, \delta)$ (AND EVEN **TWO** CASES WITH $\delta^\perp > g(\ell, \delta)$) DEMONSTRATE THE ADVANTAGE OF THE CONSTRUCTION IN THEOREM 27 AND OF USING RELATIVE MINIMUM DISTANCES.

8	7	6	5	4	3	2	1	5	10	15	20	25	30	35	40
16	14	12	10	8	6	4	2	4	8	12	16	20	24	28	32
24	21	18	15	12	9	6	3	3	6	9	12	15	18	21	24
32	28	24	20	16	12	8	4	2	4	6	8	10	12	14	16
40	35	30	25	20	15	10	5	1	2	3	4	5	6	7	8

Fig. 6. Example 14: $D(N)$ to the left, and $D^\perp(N)$ to the right

It is not straightforward to generalize Theorem 27 to point ensembles $S_1 \times S_2$ with $\#S_1$ not necessarily equal to $\#S_2$. The problem lies in the choice of monomial ordering (and the corresponding definition of L_1 and L_2). More concretely, for $\#S_1 \neq \#S_2$ there simply is no monomial ordering which simultaneously optimizes the relative minimum distance of the corresponding primary codes and the relative minimum distance of the corresponding dual codes. However, our method can still be applied as the following example illustrates.

Example 14. In this example we consider $S_1, S_2 \subseteq \mathbb{F}_q$ with $s_1 = \#S_1 = 8$, $s_2 = \#S_2 = 5$ and consider codes defined from $S_1 \times S_2$. Here q is any prime power greater than or equal to 8. In Fig. 6 we depict on the left $D(\Delta(s_1, s_2))$ and on the right $D^\perp(\Delta(s_1, s_2))$.

Concentrating first on the lower left corner of $\Delta(s_1, s_2)$ we see that on a line segment of slope -1 the values $D^\perp(X^i Y^j)$ indeed still increase when moving from either direction toward the middle of the segment. This, however, does not at all hold for $D(X^i Y^j)$. For instance if we choose

$$L_1 = \{N \in \Delta(s_1, s_2) \mid N \preceq_{\text{deg}} XY^2\},$$

$$L_2 = \{N \in \Delta(s_1, s_2) \mid N \prec_{\text{deg}} X^2Y\},$$

then in (3) and (4) of Theorem 16 we only need to consider monomials in $L_1 \setminus L_2 = \{X^2Y, XY^2\}$. Hence, we obtain the estimates $M_1(C(L_1), C(L_2)) \geq \min\{21, 24\} = 21$ and $M_1(C(L_2)^\perp, C(L_1)^\perp) \geq 6$. But this seems somewhat not a perfect choice of $L_2 \subset L_1$ as now $\min\{D(M) \mid M \in L_1\} = \min\{D(M) \mid M \in L_1 \setminus L_2\}$. Hence, we optimized the relative minimum distance of the dual codes, but did not obtain any improvement for the primary codes. Turning to the right upper corner of $\Delta(s_1, s_2)$ the situation is similar, however, with the role of the primary and dual codes interchanged. We finally consider the remaining

middle part of $\Delta(s_1, s_2)$. We first choose as monomial ordering the weighted degree lexicographic ordering \prec_w defined by the rule that $X^{i_1}Y^{i_2} \prec_w X^{j_1}Y^{j_2}$ if either $i_1 + 2i_2 < j_1 + 2j_2$, or $i_1 + 2i_2 = j_1 + 2j_2$ with $i_2 < j_2$. Then define

$$\begin{aligned} L_1 &= \{N \in \Delta(s_1, s_2) \mid N \preceq_w X^2Y^2\}, \\ L_2 &= \{N \in \Delta(s_1, s_2) \mid N \prec_w X^4Y\}. \end{aligned}$$

Again this renders the nice property that in (3) and (4) we only need to consider the monomials of $L_1 \setminus L_2$, which in this case becomes $\{X^4Y, X^2Y^2\}$. We obtain

$$\begin{aligned} M_1(C(L_1), C(L_2)) &\geq \min\{16, 18\} = 16, \\ M_1(C(L_2)^\perp, C(L_1)^\perp) &\geq \min\{9, 10\} = 9. \end{aligned}$$

Choosing on the other hand the degree lexicographic ordering and defining

$$\begin{aligned} L_1 &= \{N \in \Delta(s_1, s_2) \mid N \preceq_{\text{deg}} X^2Y^2\}, \\ L_2 &= \{N \in \Delta(s_1, s_2) \mid N \prec_{\text{deg}} X^3Y\}, \end{aligned}$$

we only need to consider monomials in $L_1 \setminus L_2 = \{X^3Y, X^2Y^2\}$, from which we obtain $M_1(C(L_1), C(L_2)) \geq \min\{18, 20\} = 18$ and $M_1(C(L_2)^\perp, C(L_1)^\perp) \geq \min\{8, 9\} = 8$. As a consequence, there seems to be no general rule for which (weighted) degree lexicographic ordering to choose. \diamond

We now return to the case of the point set being a Cartesian product of subsets $S_i \subseteq \mathbb{F}_q$ of the same size. Theorem 27 treated the two-dimensional case, the theorem below treats higher dimensions.

Theorem 31. Consider $S_1, \dots, S_m \subseteq \mathbb{F}_q$ with $s = \#S_1 = \dots = \#S_m$ and let $\langle F_1(X_1), \dots, F_m(X_m) \rangle \subset \mathbb{F}_q[X_1, \dots, X_m]$, where F_1, \dots, F_m are as in (2). Consider $X_1^{i_1}X_2^{i_2} \dots X_m^{i_m} \in \Delta(s, \dots, s)$ with $i_1 \leq i_2$ and let

$$\begin{aligned} L_1 &= \{N \in \Delta(s, \dots, s) \mid N \preceq_{\text{deg}} X_1^{i_1}X_2^{i_2} \dots X_m^{i_m}\}, \\ L_2 &= \{N \in \Delta(s, \dots, s) \mid N \prec_{\text{deg}} X_1^{i_2}X_2^{i_1}X_3^{i_3} \dots, X_m^{i_m}\}. \end{aligned}$$

The codes $C(L_1)$ and $C(L_2)$ are of length $n = s^m$ and their codimension equals $\ell = i_2 - i_1 + 1$. The relative minimum distances satisfy

$$\begin{aligned} M_1(C(L_1), C(L_2)) &= (s - i_1) \dots (s - i_m) \\ M_1(C(L_2)^\perp, C(L_1)^\perp) &\geq (i_1 + 1) \dots (i_m + 1), \end{aligned}$$

and for $v = 2, \dots, \ell$

$$\begin{aligned} M_v(C(L_1), C(L_2)) &= \min \{D(K) \mid \\ &K \subseteq \{X_1^{i_2}X_2^{i_1}X_3^{i_3} \dots X_m^{i_m}, \dots, X_1^{i_1}X_2^{i_2} \dots X_m^{i_m}\}, \\ &\#K = v\}, \\ M_v(C(L_2)^\perp, C(L_1)^\perp) &\geq \min \{D^\perp(K) \mid \\ &K \subseteq \{X_1^{i_2}X_2^{i_1}X_3^{i_3} \dots X_m^{i_m}, \dots, X_1^{i_1}X_2^{i_2} \dots X_m^{i_m}\}, \\ &\#K = v\}. \end{aligned}$$

Proof. The proof is similar to that of Theorem 27. The details are left for the reader. \square

We next return to the two-dimensional case, comparing in an example asymmetric quantum codes from Corollary 29 with La Guardia's Construction II of asymmetric quantum generalized Reed-Solomon codes (Theorem 26). Recall from Remark 5 that parameters of asymmetric quantum codes based on the CSS construction can be directly translated into parameters of ramp secret sharing schemes.

Theorem 26 ([44, Theorem 7.1])	Theorem 27
—	$[[49, 1, 31/4]]_7$
—	$[[49, 2, 30/6]]_7$
—	$[[49, 1, 25/9]]_7$
$[[49, 2, 23/2]]_7$	$[[49, 3, 24/8]]_7$
$[[49, 2, 20/5]]_7$	$[[49, 2, 20/12]]_7$
$[[49, 2, 18/7]]_7$	$[[49, 4, 18/10]]_7$
$[[49, 2, 16/9]]_7$	$[[49, 1, 16/16]]_7$
$[[49, 2, 15/10]]_7$	$[[49, 3, 15/15]]_7$
$[[49, 6, 12/11]]_7$	$[[49, 5, 12/12]]_7$

TABLE X

COMPARISON OF CODE PARAMETERS IN EXAMPLE 15. TO THE RIGHT ALL POSSIBLE PARAMETERS DERIVED USING THEOREM 27. TO THE LEFT A SELECTION OF PARAMETERS DERIVED BY APPLYING THEOREM 26 TO CODES OF LENGTH 48. AN EMPTY ENTRY MEANS THAT THERE ARE NO COMPARABLE PARAMETER.

Theorem 26 ([44, Theorem 7.1])	Theorem 27
—	$[[64, 1, 49/4]]_8$
—	$[[64, 2, 42/6]]_8$
—	$[[64, 1, 36/9]]_8$
—	$[[64, 3, 35/8]]_8$
$[[64, 2, 30/3]]_8$	$[[64, 2, 30/12]]_8$
$[[64, 4, 28/4]]_8$	$[[64, 4, 28/10]]_8$
$[[64, 2, 25/8]]_8$	$[[64, 1, 25/16]]_8$
$[[64, 2, 24/9]]_8$	$[[64, 3, 24/15]]_8$
$[[64, 2, 21/12]]_8$	$[[64, 5, 21/12]]_8$
$[[64, 2, 20/13]]_8$	$[[64, 2, 20/20]]_8$
$[[64, 4, 18/14]]_8$	$[[64, 4, 18/18]]_8$

TABLE XI

COMPARISON OF CODE PARAMETERS IN EXAMPLE 15. TO THE RIGHT ALL POSSIBLE PARAMETERS FROM THEOREM 27. TO THE LEFT A SELECTION OF PARAMETERS RESULTING FROM THEOREM 26.

Example 15. We first consider the case of asymmetric quantum codes with $q = 7$ and of length 49. The parameters produced by Theorem 26 for the code length 49 all satisfy that $d_z, d_x \leq 6$. To produce higher values of d_z (as usual we shall assume $d_z \geq d_x$), we can instead apply Theorem 26 to codes of length 48 and thereby derive information on codes of length 49. We then compare these values with what is produced from Theorem 27 in combination with Theorem 3 for codes of length 49. As is seen in Table X, most often Theorem 27 produces the best results. All displayed codes coming from Theorem 27 strictly exceed the Gilbert-Varshamov bound (Theorem 4).

We next consider asymmetric quantum codes with $q = 8$ and of length 64. In Table XI we compare representative examples of what can be derived from Theorem 26 with what can be obtained from Theorem 27 in combination with Theorem 3. Again the advantage of our method is distinct in most cases, however, with a clear exception when $d_z = 14$. For $d_z > 31$, Theorem 26 does not produce any information, which in Table XI is marked with “—”. All displayed codes coming from Theorem 27 strictly exceed the Gilbert-Varshamov bound (Theorem 4).

◇

We conclude this section with discussing higher weights and their use in secret sharing.

Remark 32. Inspecting (19) and (20) it is clear that the $(v + 1)$ th relative weights are typically much larger than the v th relative weights, for $v \in \{1, \dots, \ell - 1\}$. In particular the second relative weights are often much larger than the first relative weights. The consequence for the related ramp secret sharing schemes is that the security is much better than what is reflected only by the parameter $t = t_1$, in that t_{v+1} is much larger than t_v for $v \in \{1, \dots, \ell - 1\}$. Hence, if a small amount of information leakage can be accepted, then one can tolerate many more leaked symbols. In the other direction, reconstruction corresponds to solving a system of linear equations. Hence, the fact that r_v is much smaller than r_{v+1} for

ℓ	t_1	t_2	t_3	t_4	r_1	r_2	r_3	r_4
1	24	-	-	-	33	-	-	-
2	19	23	-	-	29	31	-	-
3	14	18	21	-	24	26	29	-
1	15	-	-	-	28	-	-	-
4	9	13	16	18	18	20	23	27
1	8	-	-	-	21	-	-	-
3	7	10	12	-	15	18	22	-
2	5	7	-	-	13	17	-	-
1	3	-	-	-	12	-	-	-

TABLE XII
RAMP SECRET SHARING SCHEMES FROM EXAMPLE 16

$v \in \{1, \dots, \ell - 1\}$, and in particular that $r_{\ell-1}$ is much smaller than $r = r_\ell$, means that if one is willing to guess some of the indeterminates of the system then one needs much fewer shares to reconstruct the secret.

We illustrate Remark 32 with an example.

Example 16. This is a continuation of Example 12. Applying Theorem 27 we obtain ramp secret sharing schemes with $n = 36$ participants, with secrets in \mathbb{F}_q^ℓ where ℓ and the privacy and reconstruction numbers are as in Table XII.

◇

V. CONCLUDING REMARKS

In a series of works [26], [24], [27], [25], [23] the authors of the present paper investigated linear codes over \mathbb{F}_q defined by evaluating multivariate polynomials at Cartesian products $S_1 \times \dots \times S_m$, where for $i = 1, \dots, m$, S_i is the set of roots of

$$X_i^{N_i} - X_i \quad \text{or} \quad X_i^{N_i-1} - 1. \quad (28)$$

Here $N_i > 1$ satisfies that $N_i - 1$ divides $q - 1$. Such codes were then used in [26], [24], [27], [25], [23] for the construction of symmetric quantum codes. In the terminology used in these papers a set $J \subseteq \{1, \dots, m\}$ indicates for which indices the second case in (28) occurs – and the corresponding codes are called J -affine variety codes, and if $N_i - 1 = q - 1$, $J = \{1, \dots, m\}$ generalized toric codes [49]. One of the advantages of such codes is that they come with an efficient method for finding parity check matrices. More precisely, when each row in the generator matrix is made by evaluating a monomial at the points of the point set, then [27, Proposition 1] provides a description of a corresponding parity check matrix. The codes of the present paper clearly are J -affine variety codes when S_i , $i = 1, \dots, m$ is of the form (28). This is in particular the case in all the examples we have given, implying that for these codes we can easily establish parity check matrices.

Another advantage of J -affine variety codes is that they are suited for the construction of subfield subcodes. It is an interesting topic of future research to investigate if the method from the present paper can be successfully combined with such subfield subcode construction.

For q an even power of a prime, Theorem 3 is also true if one replaces the Euclidean duality with the Hermitian duality [19, Theorem 4.5]. It is also an interesting research problem to investigate if this product can be successfully combined with the methods of the present paper.

APPENDIX A PROOF OF LEMMA 21

Proof. Let $m \geq 2$ be an arbitrary integer. The proof is by induction on $i = m, \dots, 1$. For $i = m$ the formula reduces to

$$\int_0^{s - \frac{\tau}{(s-x_1)\cdots(s-x_{m-1})}} dx_m = s - \frac{\tau}{(s-x_1)\cdots(s-x_{m-1})}$$

which is indeed true. Next let $1 \leq i < m$ and assume that the formula in the lemma holds when i is substituted with $i + 1$. We must show that it also holds for i . The left hand side becomes

$$\begin{aligned}
& \int_0^{s - \frac{\tau}{s^{m-i}(s-x_1)\cdots(s-x_{i-1})}} s^{m-i} \\
& \quad - \sum_{t=0}^{m-i-1} \left[\frac{1}{t!} \frac{\tau}{(s-x_1)\cdots(s-x_i)} \right. \\
& \quad \quad \left. \cdot \left(\ln \left(\frac{(s-x_1)\cdots(s-x_i)s^{m-i}}{\tau} \right) \right)^t \right] dx_i \\
& = s^{m-i+1} - \frac{\tau}{(s-x_1)\cdots(s-x_{i-1})} \\
& \quad + \sum_{t=0}^{m-i-1} \int_0^{s - \frac{\tau}{s^{m-i}(s-x_1)\cdots(s-x_{i-1})}} \\
& \quad \quad \frac{1}{t!} \frac{\tau}{(s-x_1)\cdots(s-x_{i-1})} \frac{-1}{(s-x_i)} \\
& \quad \quad \cdot \left(\ln \left(\frac{(s-x_1)\cdots(s-x_i)s^{m-i}}{\tau} \right) \right)^t dx_i. \tag{29}
\end{aligned}$$

We continue with the last term, which after the substitution,

$$u = \ln((s-x_1)\cdots(s-x_i)s^{m-i}/\tau),$$

becomes

$$\begin{aligned}
& \sum_{t=0}^{m-i-1} \int_0^0 \left(\frac{(s-x_1)\cdots(s-x_{i-1})s^{m-i+1}}{\tau} \right) \\
& \quad \quad \frac{1}{t!} \frac{\tau}{(s-x_1)\cdots(s-x_{i-1})} u^t du \\
& = - \sum_{t=0}^{m-i-1} \left[\frac{1}{(t+1)!} \frac{\tau}{(s-x_1)\cdots(s-x_{i-1})} \right. \\
& \quad \quad \left. \cdot \left(\ln \left(\frac{(s-x_1)\cdots(s-x_{i-1})s^{m-i+1}}{\tau} \right) \right)^{t+1} \right].
\end{aligned}$$

Shifting the index by 1 in the last sum and collecting terms in (29) prove the lemma. \square

ACKNOWLEDGMENT

The authors thank Ryutaroh Matsumoto for pleasant discussions and the anonymous reviewers for insightful comments and suggestions.

REFERENCES

- [1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Remarkable degenerate quantum stabilizer codes derived from duadic codes. *Information Theory, 2006 IEEE International Symposium on*, IEEE: 1105–1108, 2006.
- [2] H. E. Andersen and O. Geil. Evaluation codes from order domain theory. *Finite Fields Appl.*, 14(1):92–123, 2008.
- [3] A. Ashikhmin and E. Knill. Non-binary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.
- [4] A. E. Ashikhmin, A. M. Barg, E. Knill, and S. N. Litsyn. Quantum error detection. I. Statement of the problem. *IEEE Trans. Inform. Theory*, 46(3):778–788, 2000.
- [5] T. Bains. Generalized Hamming weights and their applications to secret sharing schemes. Master's thesis, Univ. Amsterdam, 2008.
- [6] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Combin. Des.*, 8(3):174–188, 2000.

- [7] G. R. Blakley and C. Meadows. Security of ramp schemes. In *Advances in cryptology (Santa Barbara, Calif., 1984)*, volume 196 of *Lecture Notes in Comput. Sci.*, pages 242–268. Springer, Berlin, 1985.
- [8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405, 1997.
- [9] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $GF(4)$. *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.
- [10] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54(2):1098, 1996.
- [11] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptology*, 6(3):157–167, 1993.
- [12] 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*, volume 4515 of *Lecture Notes in Comput. Sci.*, pages 291–310. Springer, Berlin, 2007.
- [13] D. A. Cox, J. Little, and D. O’Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, volume 10. Springer, 1997.
- [14] L. Csirmaz. Ramp secret sharing and secure information storage. *Preprint*, 2009.
- [15] I. M. Duursma and S. Park. Coset bounds for algebraic geometric codes. *Finite Fields Appl.*, 16(1):36–55, 2010.
- [16] M. F. Ezerman, S. Jitman, H. M. Kiah, and S. Ling. Pure asymmetric quantum MDS codes from CSS construction: A complete characterization. *Int. J. Quantum Inf.*, 11(03): 1350027, 2013.
- [17] M. F. Ezerman, S. Jitman, S. Ling, and D. V. Pasechnik. CSS-like constructions of asymmetric quantum codes. *IEEE Trans. Inform. Theory*, 59(10):6732–6754, 2013.
- [18] M. F. Ezerman, S. Jitman, and P. Sole. Xing-Ling codes, duals of their subcodes, and good asymmetric quantum codes. *Des. Codes Cryptogr.*, 75(1):21–42, 2015.
- [19] M. F. Ezerman, S. Ling, and P. Sole. Additive asymmetric quantum codes. *IEEE Trans. Inform. Theory*, 57(8):5536–5550, 2011.
- [20] G. L. Feng and T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Trans. Inform. Theory*, 39(1):37–45, 1993.
- [21] G. L. Feng and T. R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Trans. Inform. Theory*, 40(4):1003–1012, 1994.
- [22] G. L. Feng and T. R. N. Rao. Improved geometric Goppa codes part I: Basic theory. *IEEE Trans. Inform. Theory*, 41(6):1678–1693, 1995.
- [23] C. Galindo, O. Geil, F. Hernando, and D. Ruano. On the distance of stabilizer quantum codes from J -affine variety codes. *Quantum Inf. Process.*, 14(4):111, 2017.
- [24] C. Galindo and F. Hernando. Quantum codes from affine variety codes and their subfield-subcodes. *Des. Codes Cryptogr.*, 76(1):89–100, 2015.
- [25] C. Galindo, F. Hernando, and D. Ruano. New quantum codes from evaluation and matrix-product codes. *Finite Fields Appl.*, 36:98–120, 2015.
- [26] C. Galindo, F. Hernando, and D. Ruano. Quantum codes with bounded minimum distance. In *21st Conference on Applications of Computer Algebra*, 2015.
- [27] C. Galindo, F. Hernando, and D. Ruano. Stabilizer quantum codes from J -affine variety codes and a new Steane-like enlargement. *Quantum Inf. Process.*, 14(9):3211–3231, 2015.
- [28] O. Geil and T. Høholdt. Footprints or generalized Bezout’s theorem. *IEEE Trans. Inform. Theory*, 46(2):635–641, 2000.
- [29] O. Geil, and T. Høholdt. On hyperbolic type codes. *Information Theory, 2003. Proceedings. IEEE International Symposium on*, 331–331, 2003.
- [30] O. Geil, S. Martin, R. Matsumoto, D. Ruano, and Y. Luo. Relative generalized Hamming weights of one-point algebraic geometric codes. *IEEE Trans. Inform. Theory*, 60(10):5938–5949, 2014.
- [31] O. Geil, R. Matsumoto, and D. Ruano. Feng-Rao decoding of primary codes. *Finite Fields Appl.*, 23:35–52, 2013.
- [32] O. Geil, C. Munuera, D. Ruano, and F. Torres. On the order bounds for one-point AG codes. *Adv. Math. Commun.*, 5(3):489–504, 2011.
- [33] O. Geil and C. Thomsen. Weighted Reed-Muller codes revisited. *Des. Codes Cryptogr.*, 66(1-3):195–220, 2013.
- [34] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at <http://www.codetables.de>, 2007. Accessed on 2016-09-15.
- [35] M. Grassl, S. Lu, and B. Zeng. Codes for simultaneous transmission of quantum and classical information. *arXiv preprint arXiv:1701.06963*, 2017.
- [36] T. Høholdt. On (or in) Dick Blahut’s’ footprint’. In A. Vardy, editor, *Codes, Curves and Signals: Common Threads in Communications*, pages 3–9, Springer, 1998.
- [37] T. Høholdt, J. H. van Lint, and R. Pellikaan. Algebraic geometry codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, volume 1, pages 871–961. Elsevier, Amsterdam, 1998.
- [38] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75(3):032345, 2007.
- [39] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.
- [40] 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*, E95-A(11):2067–2075, Nov. 2012.
- [41] G. G. La Guardia. Asymmetric quantum product codes. *Int. J. Quantum Inf.*, 10(01):1250005, 2012.
- [42] G. G. La Guardia. Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes. *Quantum Inf. Process.*, 11(2):591–604, 2012.
- [43] G. G. La Guardia. Asymmetric quantum codes: New codes from old. *Quantum Inf. Process.*, 12(8):2771–2790, 2013.
- [44] G. G. La Guardia. On the construction of asymmetric quantum codes. *Int. J. Theor. Phys.*, 53:2312–2322, 2014.

- [45] R. Matsumoto. Two Gilbert-Varshamov type existential bounds for asymmetric quantum error-correcting codes. *arXiv preprint arXiv:1705.04087*, 2017.
- [46] R. Matsumoto and S. Miura. On the Feng-Rao bound for the \mathcal{L} -construction of algebraic geometry codes. *IEICE Trans. Fundamentals*, E83-A(5):926–930, May 2000.
- [47] R. Matsumoto and T. Uyematsu. Lower bound for the quantum capacity of a discrete memoryless quantum channel. *J. Math. Phys.*, 43(9):4391–4403, 2002.
- [48] R. Pellikaan. On the efficient decoding of algebraic-geometric codes. In P. Camion, P. Charpin, and S. Harari, editors, *Eurocode '92 International Symposium on Coding Theory and Applications*, number 339 in CISM Courses and Lectures, pages 231–253. CISM International Centre for Mechanical Sciences, Springer, 1993.
- [49] D. Ruano. On the structure of generalized toric codes. *J. Symbolic Comput.*, 44(5):499–506, 2009.
- [50] S. Sakata. Extension of the Berlekamp-Massey algorithm to N dimensions. *Inform. and Comput.*, 84(2):207–239, 1990.
- [51] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler. Asymmetric quantum codes: constructions, bounds and performance. In *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.*, volume 465, pages 1645–1672. The Royal Society, 2009.
- [52] A. Shamir. How to share a secret. *Comm. ACM*, 22(11):612–613, 1979.
- [53] A. B. Sørensen. Weighted Reed-Muller codes and algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 38(6):1821–1826, 1992.
- [54] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A*, 54(6):4741, 1996.
- [55] A. Subramanian and S. W. McLaughlin. MDS codes on the erasure-erasure wiretap channel. *arXiv preprint arXiv:0902.3286*, 2009.
- [56] H. Yamamoto. Secret sharing system using (k, L, n) threshold scheme. *Electron. Comm. Japan Part I Comm.*, 69(9):46–54, 1986.