FAMILIES OF QUANTUM STABILIZER AND SUBSYSTEM CODES FROM ALGEBRO-GEOMETRIC TORIC CODES

ROY JOSHUA AND G. V. RAVINDRA

Abstract. We show how to construct large families of quantum stabilizer and subsystem codes from algebro-geometric toric codes extending the known construction of subsystem codes from cyclic codes and extending the construction of stabilizer codes from toric codes in an earlier work by one of the authors. Since algebro-geometric toric codes are higher dimensional extensions of cyclic codes, we obtain this way a new and rich source of quantum stabilizer and subsystem codes. The fact that these codes are produced from polytopes enable us to produce large families of codes by varying the shape of the polytopes. In fact, by varying the shape of the polytopes defining the toric varieties, we show that we obtain families of quantum codes whose parameters improve steadily and with several of these codes being either Quantum MDS codes or Near Quantum MDS codes.

Contents

1. Introduction 1
2. Toric and Generalized Toric evaluation codes as multicyclic codes 5
3. Quantum stabilizer codes and subsystem codes 9
4. Construction of sub-system codes from Generalized toric codes 10
5. Quantum stabilizer codes from toric varieties over \( \mathbb{F}_q \) 12
6. Examples 12
7. Appendix: Toric residue theorems over finite fields 20
References 23

1. Introduction

In prior work (see [JA11]), one of the authors had shown how to produce quantum stabilizer codes from higher dimensional algebraic varieties, especially from the class of higher dimensional toric varieties of arbitrary dimensions. The Toric residue theorems as well as a partial converse proved therein (see [JA11] Theorems 4.1 and 4.3), enable one to adapt the methods of [SHan02] and [JHan02] making use of intersection theory, to determine the parameters of such toric residue codes: see also [JHan13] for similar toric residue theorems, but restricted to toric surfaces. Though toric residue theorems have been available in the literature prior to [JA11] and [JHan13], (see [Gr], for example)), they were valid only for complex toric varieties. The extension to finite fields is not automatic since important ingredients used in the proofs of these theorems like the Kodaira vanishing theorems fail in positive characteristics in general: see for example, [Gr, (3.8) Theorem] for a proof of the converse residue theorem making use

The first author was supported by a grant from the NSF and the second author was supported by a grant from the Simons Foundation.
of Kodaira vanishing. As shown in [JA11], it is only because, toric varieties happen to be Frobenius split, that such theorems hold in positive characteristics.

By showing that one could produce quantum stabilizer codes from all such projective toric varieties of arbitrary dimensions, [JA11] provides an abundant supply of families of such quantum stabilizer codes. However, there were a few limitations and restrictions on the quantum codes that were considered in [JA11]: for example, only finite fields of characteristic 2 were considered for several reasons. Another aspect that was not considered in [JA11] was the construction of quantum codes over fields of the form \( F_{q^2} \), where \( q \) is any prime power; there the presence of the involution \( x \mapsto x^q, x \in F_{q^2} \) (and hence often called the Hermitian case) provides an extra ingredient that may yield better codes. In addition, the question of how to adapt the methods of toric residue codes to construct subsystem codes from projective toric varieties remained open: since subsystem codes have been shown to possess several advantages, (see §3 for more on this), this question is of central importance.

The goals of the present paper are as follows:

(i) address the limitations of our earlier work [JA11] as pointed out in the last paragraph, so that the techniques developed there apply much more generally and

(ii) produce large families of both stabilizer and subsystem quantum codes from toric varieties of varying dimensions with steadily improving parameters by varying the shape of the polytopes used, with several of these codes being either Quantum MDS codes or Near Quantum MDS codes.

In fact, we establish a framework, where it is possible to construct large families of subsystem and stabilizer codes from toric varieties of arbitrary dimension. The parameters of quantum codes we construct from toric varieties are computed making use of various functions we have written in Macaulay2: see [J18].

In order to state our main results, we need to introduce a few key technical terms. The vector space \( F_q^n \) will have the standard inner product defined by \( \langle v, w \rangle = \sum_{i=1}^{n} v_i w_i \), where \( v = (v_1, \cdots, v_n) \) and \( w = (w_1, \cdots, w_n) \). As mentioned above, the field \( F_{q^2} \) comes equipped with the involution \( x \mapsto x^q \). The vector space \( F_{q^2}^n \), therefore also has the inner product defined by \( \langle v, w \rangle_h = \sum_{i=1}^{n} v_i^q w_i \). (In the literature, these are often called the Euclidean case and the Hermitian case, perhaps for want of better names.) If \( V \) is a vector space over the finite field \( F_q (F_{q^2}) \), and \( W \) is a subspace of \( V \), we let \( W^\perp = \{ v \in V | \langle v, w \rangle = 0, \text{ for all } w \in W \} \) \( (W^h)^\perp = \{ v \in V | \langle v, w \rangle_h = 0, \text{ for all } w \in W \} \), respectively.

In addition, we need to formulate the notion of defining sets for the toric codes we consider. In the case where the toric variety is one dimensional, the defining set is often defined as the zero-set of a generating polynomial for the code. This is extended to higher dimensions in Definition 2.3 but this extension requires that we carefully re-examine the definitions even in the one dimensional case. Our toric codes will be defined by polytopes of dimension \( m \), in the character lattice \( \mathbb{Z}[M] \) of a split torus of dimension \( m \) defined over \( F_q \). The box \( H = \{0, \cdots, q-2\}^m \) will be identified with a subset of the above lattice: the importance of the box \( H \) is that the evaluation function that sends a monomial to the tuple obtained by evaluating at all the \( F_q \)-rational points of the split torus \( G_m^m \) is injective when restricted to \( H \). In view
of this, we will often restrict to codes defined by subsets $U$ of $H$. (A similar discussion applies to codes defined over $\mathbb{F}q^2$.)

A linear code $C$ over $\mathbb{F}_q$ ($\mathbb{F}q^2$) will be said to be self-orthogonal if $C \subseteq C^\perp$ ($C \subseteq C^\perp_h$, respectively). Then the following is one of the main results of the paper where $wt(w)$ denotes the Hamming weight of the word $w$, and where for a subset $T \subseteq H = \{0, \cdots , q-2\}^m$, $T^\perp := \{v \in H \mid v \equiv -v' \text{mod} ((q-1)\mathbb{Z})^m \text{ for some } v' \in T\}$: see Definition 2.3. For a generalized toric code $C_U$ defined by a subset $U \subseteq H$, we define its defining set to be $H \setminus U^\perp$. We denote this by $D(C_U)$.

**Theorem 1.1.** Let $C_U$ denote a $k$-dimensional generalized toric code that is self-orthogonal and of length $n$ over $\mathbb{F}_q$. Let $T$ denote a subset of $D(C_U) \setminus D(C_U^\perp)$. Then

(i) $T^\perp \subseteq D(C_U) \setminus D(C_U^\perp)$.

(ii) The generalized toric code $F := C_{U \cup T \cup T^\perp}$ satisfies the property that $F \cap F^\perp = C_U$.

(iii) If $r := |T \cup T^\perp|$ satisfies $0 \leq r < n - 2k$ and $d = \min \{wt(w) \mid w \in C_U^\perp \setminus F\}$, then there exists a sub-system code with parameters $[n, n - 2k - r, r, d]_q$.

Over $\mathbb{F}_q^2$, for a subset $T \subseteq H = \{0, \cdots , q^2 - 2\}^m$, we let $T^\perp := \{v \in H \mid v \equiv -qv' \text{mod} ((q^2 - 1)\mathbb{Z})^m \text{ for some } v' \in T\}$: see Definition 2.3. For a generalized toric code $C_U$ defined by a subset $U \subseteq H$, we define its defining set to be $H \setminus U^\perp$ and we denote it by $D_h(C_U)$. Then we obtain the following variant of the last theorem.

**Theorem 1.2.** Let $C_U$ denote a $k$-dimensional generalized toric code that is self-orthogonal and of length $n$ over $\mathbb{F}_q^2$. Let $T$ denote a subset of $D_h(C_U) \setminus D_h(C_U^\perp)$. Then

(i) $T^\perp \subseteq D_h(C_U) \setminus D_h(C_U^\perp)$.

(ii) The generalized toric code $F := C_{U \cup T \cup T^\perp}$ satisfies the property that $F \cap F^\perp = C_U$.

(iii) If $r := |T \cup T^\perp|$ satisfies $0 \leq r < n - 2k$ and $d = \min \{wt(w) \mid w \in C_U^\perp \setminus F\}$, then there exists a sub-system code with parameters $[n, n - 2k - r, r, d]_q$.

The proof of these theorems are discussed in §4 making intrinsic use of defining sets. The main results of [JA11] were stated only for fields of the form $\mathbb{F}_q$ and with the standard inner product $< , >$ to define the dual of a code. The second theorem above, valid for fields of the form $\mathbb{F}_q^2$, requires that the techniques of [JA11] be extended to cover the use of the inner product $< , >_h$. This is carried out in an appendix.

As discussed above, in [JA11], the authors were also forced to restrict to fields of characteristic 2, though the main theorems there, i.e. [JA11] Theorems 4.1 and 4.3] were already stated for fields of arbitrary characteristics. The next result of the present paper is the following theorem, which removes the above restrictions.

**Theorem 1.3.** Let $U_1, U_2 \subseteq H$ denote polytopes so that $U_2 \subseteq U_1 \subseteq U_1^\uparrow$. Assume that both of these polytopes define toric codes of length $n$. Let $D_i = C_{U_i}^\perp$, $i = 1, 2$ and assume moreover that both $U_1$ and $U_2$ are the translates of polytopes that satisfy the hypotheses discussed in §7.1, i.e. in [JA11] 3.4].
Then $D_2 \supseteq D_1 \supseteq D_1^\perp$. If $n$ is as above, $k'_1 = |U_1|$, $k'_2 = |U_2|$ and $d_1 = \text{distance}(D_1)$, $d_2 = \text{distance}(D_2)$, then there exists a quantum stabilizer code with parameters $[[n, k'_1 + k'_2 - n, \min(d_1, d_2)]]_q$. Moreover, there exist toric residue codes $E_i$, $i = 1, 2$, so that $\text{distance}(E_i) \leq \text{distance}(D_i)$.

Here is an overview of the paper. In §2, we review the background material on toric and generalized toric codes carefully. In fact, we provide a more conceptual understanding of the notion of defining sets for cyclic codes, making it possible to define such objects for higher dimensional toric codes.

§3 reviews quantum codes and subsystem codes and extends the construction of quantum stabilizer codes in [JA11] to finite fields of arbitrary characteristic. §4 and §5 discuss the main theorems of the paper, i.e. the proofs of Theorems 1.1, 1.2 and 1.3. After discussing a proof of Theorem 1.3, we show that the techniques of [JA11] may be invoked to compute the distance of the dual of toric codes.

§6 is devoted to constructing families of quantum codes from projective toric varieties invoking the theorems worked out in earlier sections. We discuss families of codes constructed from toric surfaces of all types, the projective spaces of dimensions 2, projective spaces of dimension 2 with a point blown-up as well as families of Hirzebruch surfaces. In dimensions 3 and higher, the only toric varieties we consider are projective spaces.

(i) In all these examples, we produce families of quantum codes by varying the shape of the polytopes and show that the parameters of the resulting codes can be improved steadily by fine-tuning these parameters, and that in fact several of the quantum codes we produce are either Quantum MDS codes or Near Quantum MDS codes.

(ii) A feature that was discovered by running a computer program computing the parameters of the quantum codes, was that these parameters are quite sensitive to the shape of the polytope and that, it is in fact possible to select polytopes so that the parameters of the resulting quantum codes improve steadily, approaching the quantum singleton bound.

(iii) It may be important to point out that the families of quantum codes we construct here from the projective spaces of dimension 3 and higher may be the only examples of quantum codes constructed from algebraic varieties of dimension higher than 2 and also among the few quantum codes of length of order at least $q^3$ over the base field $\mathbb{F}_q$.

These families are produced by computer calculations using various functions we have written using the Macaulay2 package (in fact using the NormalToricVarieties sub-package), without which it would be very difficult to compute the resulting code parameters by hand. Tables 1 through 3 list examples of such families of quantum codes constructed.

**Comparison with other codes in the literature.** The very fact that several of the codes produced in this paper are either Quantum MDS codes or near Quantum MDS codes show that, for a given length and dimension, several of these codes have the best possible or nearly the best possible minimum distance. This should be hardly surprising once one realizes that among classical codes, several of the codes produced from toric varieties had been shown to be MDS or near MDS codes: see [Joyn]. Our results show that these advantages carry over also to the quantum codes produced this way.
Acknowledgments. Both authors thank the reviewers of an earlier draft for helpful comments that have enabled us to improve the exposition as well as sharpen the results of the paper considerably.

2. Toric and Generalized Toric evaluation codes as multicyclic codes

Let $F_q$ denote a fixed finite field, where $q = p^m$ for some prime $p$. We start with cyclic codes over $F_q$, which are well-known in coding theory: see, for example, [HP, Chapter 4]. Observe that cyclic codes may be viewed as toric codes constructed from one dimensional toric varieties.

2.1. Toric and Generalized Toric Evaluation and Residue codes. Let $T \cong (F^*)^m$ denote a split $r$-dimensional torus over $k = F_q$. Then the correspondence between rational convex polytopes in $\mathbb{R}^m$ and projective toric varieties with dense torus isomorphic to $T$, along with the choice of an ample Cartier divisor is well-known: see [Oda] or [CLS], for example. Let $M$ denote the lattice of characters of $T$ and let $M_R = M \otimes \mathbb{Z}$. Let $P$ denote such a lattice polytope in $M_R$ and let $X_P$ denote the associated projective toric variety together with the choice of an ample Cartier divisor $D_P$. By subdividing the corresponding fan if necessary, we will always assume that the toric variety $X_P$ is in fact smooth. Let $L(D_P) = H^0(X_P, O(D_P))$ denote the space of global sections of the line bundle $O(D_P)$. If $K(X_P)$ denotes the set of rational functions of $X_P$, then one has an identification $H^0(X_P, O(D_P)) \cong \{f \in K(X_P) \mid \text{div}(f) + D_P \geq 0\}$.

Now recall that the toric evaluation code $C_P$ is defined to be the image of the $F_q$-linear map $ev : H^0(X, O(D_P)) \to F_q^n, f \mapsto (f(t))_{t \in T}$, i.e. one sends sections of the line bundle $O(D_P)$ to their evaluations at the rational points of the dense torus $T$, i.e. under the assumptions that the rational points in $T$ are not among the poles of the rational functions in $H^0(X_P, O(D_P))$. Therefore, the code $C_P$ has length $n = (q - 1)^m = |T|$. Let $H = \{0, \cdots, q - 2\}^m$. Then the dimension of the above code is given by the cardinality of the set $\bar{P}$ which is the image of $P$ in $H$ modulo $((q - 1)\mathbb{Z})^m$. The techniques in [SHan02], [JHan02] to compute the minimum distance of the resulting code have been extended to higher dimensional toric varieties provided the intersection number calculations are carried out with computer help, for example as in [J18].

Any subset $U \subseteq H$ defines what is called a generalized toric evaluation code as follows: let $F_q[U]$ denote the $F_q$-vector space with basis vectors $\{Y^u = \Pi Y_i^{u_i} \mid u \in U\}$. Then one has a natural injective map $ev : F_q[U] \to F_q^n, f \mapsto (f(t))_{t \in T}$, obtained by evaluating the monomials corresponding to $U$ at the points of the dense torus $T$. The image of this map is the generalized toric code and is denoted $C_U$. This construction specializes to provide toric evaluation codes if one takes the subsets $U$ to be $\bar{P}$ defined above.

Recall that for the codes considered above, the code parameters $[n, k, d]$ are defined as follows: $n$ denotes the number of $F_q$-rational points on $T$, $k$ denotes the dimension of the $F_q$-linear subspace which is the image of the evaluation map $ev$ and $d$ denotes the minimum distance of the resulting code.
Next we observe the multi-cyclic nature of toric and generalized toric evaluation codes which will be a key property we exploit in this paper in constructing subsystem codes.

Let $\alpha \in \mathbb{F}_q^*$ be a primitive element, i.e. $\mathbb{F}_q^* = \{\alpha^0, \alpha^1, \ldots, \alpha^{q-2}\}$. Therefore, the $\mathbb{F}_q$-rational points of $T = \mathbb{G}_m^n$ are given by $\{\alpha^i = (\alpha^{i_1}, \ldots, \alpha^{i_m})\}$, and their cardinality is $n = (q-1)^m$. We will order such multi-exponents $\{i = (i_1, \ldots, i_m)\}$ by $\{i_0, \ldots, i_{n-1}\}$. The box $H$ also has $n = (q-1)^m$ elements which we will order and enumerate as $\{u_0, \ldots, u_{n-1}\}$. We denote by

$$Y^u(a^i) = \alpha^{u_1 i_1} \cdots \alpha^{u_m i_m} = \alpha^{<u,i>},$$

where $Y^u = Y_{1}^{u_1} \cdots Y_{m}^{u_m}$ is the monomial associated to each point $u = (u_1, \ldots, u_m) \in H$.

We next consider the isomorphism

$$\phi : \mathbb{F}_q^n \rightarrow \frac{\mathbb{F}_q[x_1, \ldots, x_m]}{(x_1^{q-1} - 1, \ldots, x_m^{q-1} - 1)}, \quad (c_1, \ldots, c_n) \mapsto \sum c_jx^i,$$

where $x^i = x_1^{i_1} \cdots x_m^{i_m}$. In particular, the map sends

$$(\alpha^{<u,i>} : i \in \{0, 1, \ldots, q-2\}^m) \mapsto \sum_i \alpha^{<u,i>} x^i,$$

where the sum on the right hand side is over all $i \in \{0, 1, \ldots, q-2\}^m$.

A code $C \subset \mathbb{F}_q^n$ is called multi-cyclic if its image under the above map is an ideal. The image of a generalized toric evaluation code $C_U$ for a subset $U \subseteq H$ under the above map is an ideal in $\mathbb{F}_q[x_1, \ldots, x_m]/(x_1^{q-1} - 1, \ldots, x_m^{q-1} - 1)$, and hence a generalized toric evaluation code $C_U$ is a multi-cyclic code. To summarize the discussion above, we have isomorphisms

$$\begin{align*}
\mathbb{F}_q[H] & \rightarrow \mathbb{F}_q^n \rightarrow \frac{\mathbb{F}_q[x_1, \ldots, x_m]}{(x_1^{q-1} - 1, \ldots, x_m^{q-1} - 1)} \\
Y^u & \mapsto (\alpha^{<u,i>})_{i \in \{0,1,\ldots,q-2\}^m} \mapsto \sum_{i \in \{0, 1, \ldots, q-2\}^m} \alpha^{<u,i>} x^i, \\
\mathbb{F}_q[U] & \rightarrow C_U \rightarrow \phi(C_U).
\end{align*}$$

In [JA11], it is also shown that instead of evaluating sections of a line bundle $O(D_P)$ at the $k$-rational points of the (split) torus $T$, one may start with $H^0(X_P, \omega(D_P))$, which is a set of differential forms and take their residues at (most of the) $k$-rational points on the dense torus $T$. It is shown that this construction produces codes that are close to the duals of toric evaluation codes and may be combined with the Calderbank-Shor-Steane technique (see [CS] and [SU]) to produce quantum stabilizer codes.

### 2.2. Cyclic codes as Generalized 1-dimensional toric codes

In this subsection, we pause to review and reformulate the notion of defining sets of cyclic codes, so that we are able to extend the definition suitably to higher dimensional toric and generalized toric codes.

A cyclic code over $\mathbb{F}_q$ is a linear subspace $C$ of the vector space $\mathbb{F}_q^n$ which is stable under cyclic shifts, $(c_0, c_1, \cdots, c_{n-1}) \mapsto (c_{n-1}, c_0, \cdots, c_{n-2})$. The map

$$\mathbb{F}_q^n \rightarrow \frac{\mathbb{F}_q[x]}{(x^n - 1)}, \quad (c_0, \cdots, c_{n-1}) \mapsto \sum_{i=0}^{n-1} c_i x^i,$$
induces a bijection between cyclic codes in $\mathbb{F}_q^n$ and ideals in the ring $\mathbb{F}_q[x]/(x^n - 1)$. Thus we see that 1-dimensional multi-cyclic codes are cyclic codes in the above sense. Furthermore, since every ideal in $\mathbb{F}_q[x]$ and $\mathbb{F}_q[x]/(x^n - 1)$ is a principal ideal, it follows that each cyclic code in $\mathbb{F}_q^n$ in fact corresponds to a principal ideal in $\mathbb{F}_q[x]/(x^n - 1)$.

Recall that $\mathbb{F}_q$ is the splitting field for the polynomial $x^q - x$ over $\mathbb{F}_p$, and hence $\mathbb{F}_q^*$ may be identified with the set of roots of the polynomial $f(x) := x^{q^2 - 1} - 1$. Let $H := \{0, 1, \ldots, q - 2\}$ and let $\alpha$ be a primitive generator of the multiplicative subgroup $H^* := \mathbb{F}_q^* \setminus \{0\}$, so that $H^* = \{\alpha^i \mid i \in H\}$. We will also use the identification $H \cong \mathbb{Z}/(q - 1)\mathbb{Z}$, when we need to use the (additive) group structure on $H$. Thus, for a subset $D \subseteq H$, we let

$$D^-(1) := \{d \in H \mid d \equiv -d' \text{ mod}(q - 1) \text{ for some } d' \in D\}.$$

Next we consider the case where the field $\mathbb{F}_q$ is replaced by $\mathbb{F}_{q^2}$. In this case, observe that $H = \{0, 1, \ldots, q^2 - 2\}$. For a subset $D \subseteq H$, we define

$$D^{-q}(2) := \{d \in H \mid d \equiv -qd' \text{ mod}(q^2 - 1) \text{ for some } d' \in D\}.$$

There exists a bijective correspondence between (principal) ideals in $\mathbb{F}_q[x]/(x^{q^2 - 1} - 1)$ and the monic polynomial factors of $(x^{q^2 - 1} - 1)$. Since any monic polynomial in one variable is determined by its roots, the generator polynomial of any cyclic code is determined by its roots which lie in $\mathbb{F}_q$. Using the correspondence between such roots and powers of the primitive element $\alpha \in \mathbb{F}_q^*$, these correspond to elements in $H$. The set of roots of any such generator polynomial is called the defining set of the cyclic code $C$.

We proceed to obtain a clearer understanding of the defining sets. The following two results seem to be well-known, and therefore we skip their proof.

**Lemma 2.1.** Let $e(x) := \sum_{i \in H} x^i$, and for any $a \in H$, let $e_a(x) := e(\alpha^a x) \in \mathbb{F}_q[x]$. Then $e_a(\alpha^b) = 0$ if and only if $a + b \neq q - 1$. In the Hermitian case, i.e. over $\mathbb{F}_{q^2}$, $e_a(\alpha^{qb}) = 0$ if and only if $a + qb \neq q^2 - 1$.

**Proposition 2.2.** (i) For a subset $U \subseteq H$, the image of $\mathbb{F}_q[U]$ under the evaluation isomorphism

$$\text{ev} : \mathbb{F}_q[H] \to \mathbb{F}_q[x]/(x^{q^2 - 1} - 1)$$

is the principal ideal generated by the monic polynomial $g(x)$ whose roots are elements of the set $\{\alpha^b \mid b \in H \setminus U^\perp\}$. Conversely, any principal ideal in $\mathbb{F}_q[x]/(x^{q^2 - 1} - 1)$ generated by a polynomial whose roots are $\{\alpha^a \mid a \in D\}$ for $D \subseteq H$, is the image of the cyclic code $H \setminus D^\perp$.

(ii) Over $\mathbb{F}_{q^2}$, the corresponding statements hold when $U^\perp (D^\perp)$ is replaced by $U^{-q}(D^{-q}, \text{respectively})$.

**2.3. Defining sets for higher dimensional multi-cyclic codes.** Over the field $\mathbb{F}_q$, we let $H = \{0, 1, \ldots, q - 2\}^m$ and over $\mathbb{F}_{q^2}$, we let $H = \{0, 1, \ldots, q^2 - 2\}^m$ as before. In view of Proposition 2.2 we make the following definition.

**Definition 2.3.** (i) Over $\mathbb{F}_q$, for a subset $V \subseteq H$, we let

$$V^- := \{v \in H \mid v \equiv -v' \text{ mod}(q - 1)\mathbb{Z}^m \text{ for some } v' \in V\}.$$


For a generalized toric code $C_U$ defined by a subset $U \subseteq H$, we define its defining set to be $H \setminus U^\perp$. We denote this by $D(C_U)$.

(ii) Over $\mathbb{F}_{q^2}$, for a subset $V \subseteq H$, we let

$$V^{-q} := \{ v \in H \mid v \equiv -qv' \mod((q^2 - 1)\mathbb{Z})^m \text{ for some } v' \in V \}.$$ 

For a generalized toric code $C_U$ defined by a subset $U \subseteq H$, we define its defining set to be $H \setminus U^{-q}$. We denote this by $D_h(C_U)$.

Next we have the following lemma, which is quite useful in computing the defining set.

**Lemma 2.4.** Let $V \subseteq H$. Then $H \setminus V^\perp = (H \setminus V)^\perp$. In the Hermitian case, i.e. over $\mathbb{F}_{q^2}$, $H \setminus V^{-q} = (H \setminus V)^{-q}$.

**Proof.** We only discuss the first statement, since the proof in the Hermitian case is entirely similar. The proof is identical to the “only if” part of Proposition 2.2. We have $H = V^\perp \oplus (H \setminus V^\perp)$, and so $H^\perp = (V^\perp)^\perp \oplus (H \setminus V^\perp)^\perp$. Hence, noting that $H^\perp = H$, we have $H = V \oplus (H \setminus V^\perp)^\perp$, and thus $H \setminus V^\perp = (H \setminus V)^\perp$.

Next we make the following definitions.

**Definition 2.5.** For any subset $U \subseteq H$, recall that $C_U$ denotes the corresponding generalized toric code and $D(C_U)$ its defining set. Furthermore, we let $U^\perp := H \setminus U^\perp = (H \setminus U)^\perp$, and using the standard metric structure on $\mathbb{F}_q^n$, we define for any linear code $C \subseteq \mathbb{F}_q^n$, its dual

$$C^\perp := \{ v \in \mathbb{F}_q^n \mid \langle v, w \rangle = 0 \forall w \in C \}.$$ 

In the Hermitian case, (i.e. over $\mathbb{F}_{q^2}$ with the inner product $\langle \cdot, \cdot \rangle_h$ on $\mathbb{F}_{q^2}$), we let $U^\perp_h := H \setminus U^{-q} = (H \setminus U)^{-q}$ and for any linear code $C \subseteq \mathbb{F}_q^n$, its dual

$$C^\perp_h := \{ v \in \mathbb{F}_q^n \mid \langle v, w \rangle_h = 0 \forall w \in C \}.$$ 

**Remark.** For $U \subseteq H = \{0, \cdots, q - 2\}^m$, $C_{U^\perp} = C^\perp_U$ and for $U \subseteq H = \{0, \cdots, q^2 - 2\}^m$, $C_{U^\perp_h} = C^\perp_h$. (See [Rua] Theorem 6.)

Then we obtain the following lemma which relates generalized toric codes with their defining sets. (We skip its largely self-evident proof.)

**Lemma 2.6** (See also [AN], Lemma 4). With notation as above, we have the following.

(i) $C_{U_1} \cap C_{U_2} = C_{U_1 \cap U_2}$ and hence $D(C_{U_1} \cap C_{U_2}) = D(C_{U_1}) \cup D(C_{U_2})$.

(ii) If $C_{U_1} + C_{U_2}$ denotes the code generated by $C_{U_1}$ and $C_{U_2}$, then $D(C_{U_1} + C_{U_2}) = D(C_{U_1}) \cap D(C_{U_2})$.

(iii) $C_{U_1} \subseteq C_{U_2}$ if and only if $D(C_{U_1}) \subseteq D(C_{U_2})$. In particular, $C_{U_1} = C_{U_2}$ if and only if $U_1 = U_2$.

(iv) $D(C_{U_1}) = U_1 = H \setminus D(C_{U_1})^\perp$.

(v) The corresponding statements also hold in the Hermitian case.
3. Quantum stabilizer codes and subsystem codes

We will provide a quick review of quantum stabilizer codes from a non-binary point of view. The basic Hilbert spaces of interest to us will be $\mathbb{H} = \mathbb{C}^q$ or $\mathbb{H} = \mathbb{C}^q^\otimes n := \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$. We will denote by $|x>$ the vectors of a distinguished orthonormal basis of $\mathbb{C}^q$, where the labels $x$ range over the elements of the field $\mathbb{F}_q$, where $q = p^n$ for some prime $p$ and some integer $n > 0$. A quantum error-correcting code $Q$ is defined to be a subspace of $(\mathbb{C}^q)^\otimes n$.

A nice error basis for $\mathbb{H} = (\mathbb{C}^q)^\otimes n$ may be constructed as follows. If $a, b \in \mathbb{F}_q$, one defines unitary operators $X(a)$ and $Z(b)$ on $\mathbb{C}^q$ by

$$X(a)|x> = |x+a>, \quad Z(b)|x> = \omega^{tr(bx)}|x>$$

where $tr$ denotes the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $\omega = \exp(2\pi i/p)$ is a primitive $p$-th root of unity. Then it is shown in [KKKS, §2] that the set $E = \{X(a)Z(b) \mid a, b \in \mathbb{F}_q\}$ forms a nice error basis of $\mathbb{C}^q$, i.e. it has the following properties:

(a) it contains the identity matrix,
(b) the product of two matrices in $E$ is a scalar multiple of another matrix in $E$, and
(c) $Tr(A^TB) = 0$ for distinct elements $A, B$ of $E$.

Moreover $E$ forms a basis for the set of all $q \times q$ matrices with $\mathbb{C}$-entries. For any $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, we let

$$X(a) = X(a_1) \otimes \cdots \otimes X(a_n) \quad \text{and} \quad Z(a) = Z(a_1) \otimes \cdots \otimes Z(a_n).$$

Then $E_n = \{X(a)Z(b) \mid a, b \in \mathbb{F}_q^n\}$ forms a nice error basis for $(\mathbb{C}^q)^\otimes n$.

Now one defines stabilizer codes as follows. Let $G_n$ denote the group generated by the matrices of the nice error basis $E_n$. Then

$$G_n = \{\omega^cX(a)Z(b) \mid a, b \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}.$$}

It is known that $G_n$ is a finite group of order $pq^{2n}$. The stabilizer code $Q$ is a non-zero subspace of $(\mathbb{C}^q)^\otimes n$ so that

$$Q = \bigcap_{E \in S} \{v \in \mathbb{C}^q^\otimes n \mid Ev = v\}$$

for some subgroup $S$ of $G_n$.

3.0.1. Subsystem Codes from classical codes. There are three predominant approaches to quantum error-correction: stabilizer codes, noiseless systems, and decoherence free subspaces. Subsystem codes, often also referred to as operator quantum error-correcting codes, have emerged as an important new discovery in the area of quantum error-correcting codes, unifying the above three approaches. Subsystem codes provide a common platform for comparing the different types of quantum codes and make it possible to treat active and passive quantum error-correction within the same framework. This generalization is more than a theoretical construct: it has also important practical implications in the form of simpler error recovery schemes as shown in [Bac]. Other advantages for subsystem codes that have been claimed are that some of them are self-correcting, offer greater flexibility for fault-tolerant operations and that some subsystem codes that beat the quantum Hamming bound may exist. There is an extensive literature on
this subject, but it needs to be pointed out that some of this would be listed under operator quantum error correcting codes rather than subsystem codes and also may be spread out in various sources, with a significant number of publications in this area appearing in Physics journals as [Bac], [Pou], [KLP], [KLPL] for example.

The following is the standard definition of a quantum subsystem code. Let $Q$ denote a quantum code of dimension $k$ in $H = (C^n)^{\otimes n}$. Then a sub-system code with parameters $[[n, k, r, d]]_q$ is a decomposition of $Q$ into the tensor product of two subspaces $A$ and $B$, where $\dim(A) = q^k$ and $\dim(B) = q^r$. Moreover all errors of weight less than $d$ can be detected by $A$. $A$ is called the sub-system and $B$ is called the co-subsystem. Information is stored in system $A$ and system $B$ provides additional redundancy. Errors acting only on the subsystem $B$ can be ignored. Error recovery with subsystem codes, often require fewer syndrome measurements than a corresponding stabilizer code: see [KS].

The following constructions of sub-system codes given in [Aly, Lemmas 2 and 3] will play an important role in this paper.

**Proposition 3.1.** (i) Let $C$ denote a $k'$ dimensional $F_q$-linear code of length $n$ that has a $k''$-dimensional linear sub-code $D = C \cap C^\perp$ with $k' + k'' < n$. Then there exists an $[[n, n - (k' + k''), k' - k'', \text{wt}(D^\perp - C)]]_q$ sub-system code.

(ii) Let $C$ denote a $k'$ dimensional $F_{q^2}$-linear code of length $n$ that has a $k''$-dimensional linear sub-code $D = C \cap C^\perp$ with $k' + k'' < n$. Then there exists an $[[n, n - (k' + k''), k' - k'', \text{wt}(D^\perp - C)]]_q$ sub-system code.

4. Construction of sub-system codes from Generalized toric codes

In this section, we begin by providing a construction of sub-system codes from generalized toric codes. This will exploit the multi-cyclic nature of such generalized toric codes.

**4.1. Subsystem codes.** Making use of Lemma 2.6, we obtain the constructions of sub-system codes from generalized toric codes discussed in Theorems 1.1 and 1.2. Recall that we define a linear code $C$ over $F_q$ ($F_{q^2}$) to be self-orthogonal if $C \subseteq C^\perp$ ($C \subseteq C^{\perp_{-}}$ respectively).

**Proof of Theorems 1.1 and 1.2** The proof of Theorem 1.2 is nearly identical to the proof of Theorem 1.1 with $U^\perp$ ($T^-$) replaced by $U^\perp_{-0}$ ($T^{0}$, respectively). Therefore, we will discuss only the proof of Theorem 1.1. Since $C_U$ is assumed to be self-orthogonal, $C_U \subseteq C_U^\perp$ and therefore, $D(C_U^\perp) \subseteq D(C_U)$.

Making use of Lemma 2.6(iv), we have

$$D(C_U) \setminus D(C_U^\perp) = (H \setminus U^-) \setminus U = H \setminus (U^- \cup U).$$

Thus for any $T \subset H \setminus U \cup U^-$, we obtain:

$$T^- \subset (H \setminus U \cup U^-) = H \setminus (U \cup U^-) = H \setminus (U^- \cup U).$$

We observe that the set

$$D(C_U) \setminus (T \cup T^-) = (H \setminus U^-) \setminus (T \cup T^-) = H \setminus (U^- \cup T \cup T^-).$$
Set $\mathcal{F} := C_{U \cup T \cup T^-}$: then clearly its defining set $D(\mathcal{F}) = D(C_U) \setminus (T \cup T^-)$. Furthermore, using Lemma 2.6(iv), we obtain:

$$D(\mathcal{F}^\perp) = D(C_{U \cup T \cup T^-}^\perp) = (U \cup T \cup T^-)^\perp = D(C_U) \cup T \cup T^-.$$ 

Therefore,

$$D(\mathcal{F}) \cup D(\mathcal{F}^\perp) = (H \setminus (U^- \cup (T \cup T^-))) \cup (U \cup T \cup T^-) = (H \setminus U^-) \cup U = D(C_U) \cup D(C_U^\perp).$$

Since $D(C_U^\perp) \subseteq D(C_U)$, we observe that $D(\mathcal{F} \cap \mathcal{F}^\perp) = D(\mathcal{F}) \cup D(\mathcal{F}^\perp) = D(C_U)$. It follows, therefore, that $\mathcal{F} \cap \mathcal{F}^\perp = C_U$.

Now $|D(C_U)| = n - k$ by our assumption that $\dim_{F_q}(C_U) = k$. Since $|T \cup T^-| = r$, it follows that $\dim_{F_q}(\mathcal{F}) = n - |D(\mathcal{F})| = n - (n - k - r) = k + r$ since $D(\mathcal{F}) = D(C_U) - (T \cup T^-)$ and $|T \cup T^-| = r$.

Now we apply Proposition 3.1(i) with $\mathcal{C} = \mathcal{F}$. Then $\dim_{F_q}(\mathcal{C}) = \dim_{F_q}(\mathcal{F}) = k + r$ and $\dim_{F_q}(\mathcal{F} \cap \mathcal{F}^\perp) = \dim_{F_q}(C_U) = k$. Since $2k + r$ is assumed to be less than $n$, Proposition 3.1(i) applies to complete the proof. □

4.2. Estimation of parameters of the subsystem codes constructed from toric codes. We proceed to estimate the parameters of the subsystem codes constructed above. We begin with the following result that will show we can invoke the techniques of toric residue codes developed in [JA11].

**Proposition 4.1.** (i) Suppose the base field is $F_q$, $U \subseteq H = \{0, \ldots, q - 2\}^m \subseteq \mathbb{Z}^m$ and $v \in \mathbb{Z}^m$ so that the translate $U_1 = U + v \subseteq H$. Then both the codes $C_U^\perp$ and $C_{U_1}^\perp$ have the same code parameters.

(ii) Suppose the base field is $F_{q^2}$, $U \subseteq H = \{0, \ldots, q^2 - 2\}^m \subseteq \mathbb{Z}^m$ and $v \in \mathbb{Z}^r$ so that the translate $U_1 = U + v \subseteq H$. Then both the codes $C_{U_1}^{\perp h}$ and $C_{U_1}^{\perp h}$ have the same code parameters.

**Proof.** We will first discuss the proof of (i). Let $G$ denote the generator matrix for the code $C_U$ and $G_1$ denote the generator matrix for the code $C_{U_1}$. By [LS] Theorem 4], we have $G_1 = G \Delta \Pi$, where $\Delta$ is a diagonal $n \times n$ invertible matrix with entries in $F_q^*$ and $\Pi$ is an $n \times n$ permutation matrix. Multiplying by $\Delta$ corresponds to multiplying the columns of $G$ by the entries of $\Delta$ and multiplying by $\Pi$ corresponds to permuting the resulting columns.

Next observe that the $G$ (respectively $G_1$) is a parity check-matrix for the dual code $C_U^\perp$ (respectively $C_{U_1}^\perp$). Recall that the minimum distance of a code can determined from its parity check matrix as the largest integer $d$, so that any $d - 1$ columns of the parity check matrix are linearly independent, while there exist some $d$ columns in the parity check matrix which are linearly dependent. It follows therefore, that the minimum distances of the codes $C_U^\perp$ and $C_{U_1}^\perp$ are the same.

Since both $U$ and $U_1$ are contained in $H$, the dimension of $C_U = |U|$, while the dimension of $C_{U_1} = |U_1|$. Therefore, $\dim(C_U^\perp) = n - \dim(C_U) = n - \dim(C_{U_1}) = \dim(C_{U_1}^\perp)$.

To deduce (ii) from (i), one first considers the automorphism $\phi : F_{q^2}^n \to F_{q^2}^n$ defined by $u = (u_1, \ldots, u_n) \mapsto \bar{u} = (u_1^q, \ldots, u_n^q)$. The main observations then are the following:

If $V$ is an $F_{q^2}$-linear subspace of $F_{q^2}^n$, then $\phi(V)$ is also an $F_{q^2}$-linear subspace of the same dimension and that $V^{\perp h} = \phi(V)^\perp$, where $\phi(V)^\perp$ denotes the orthogonal complement defined using the standard
inner product on $\mathbb{F}_{q^2}$. Moreover, if $U_1 = U + v$, for some $v \in \mathbb{F}_{q^2}^n$, then $\phi(U_1) = \phi(U) + \phi(v) = \phi(U) + \nabla$. Therefore, one may readily deduce (ii) from (i) by applying (i) to $\phi(U)$ and $\phi(U_1)$.

Now starting with a polytope $U \subseteq H$ which is sufficiently small, we first translate it to $U_1$, so that $U_1^\perp \supseteq U_1$. (See for example, the worked out examples in section 6.) Then the minimum distance of the dual code $C_{U_1}^\perp$ provides a lower bound for the subsystem code provided by the above theorem from $U_1$. As shown in the worked out examples in section 5, we will invoke the method of toric residue codes to obtain a lower bound for the minimum distance of the dual code $C_{U_1}^\perp$, which by the above Proposition, will also be the minimum distance of $C_{U_1}^\perp$.

5. Quantum stabilizer codes from toric varieties over $\mathbb{F}_q$

First we would like to point out that well-known CSS-construction (see [CS] and [St]) was only worked out originally for fields of characteristic 2: this was later extended to other characteristics (see, for example, [KKKS, Lemma 20]). Secondly, using the method of generalized toric codes, it is now possible to construct codes $C \subseteq C_{U_1}^\perp$ directly without making use of the toric residue theorem (i.e. [JA11, Theorems 4.1 and 4.3] as well as [JA11, Theorem 4.14]: the latter approach needed the restriction to characteristic 2. In view of these advances, we are able to construct quantum stabilizer codes starting with toric varieties in all characteristics.

**Proof of Theorem 1.3** The first statement on the existence of the quantum stabilizer code with parameters given by $[[n, k'_1 + k'_2 - n, \min(d_1, d_2)]]_q$ follows from [KKKS, Lemma 20]. The last statement that there exist toric residue codes whose minimum distance provides a lower bound for the code $C_{U_1}^\perp$ follows from [JA11, Corollary 4.11] as well as Proposition 4.1, since the polytopes $U_i$ are supposed to be the translates of polytopes satisfying the assumptions in $7.1$. □

One way to choose the polytopes $U_1$ and $U_2$ are as follows: choose a projective toric variety of rank $n$ and let the polytope $U_1$ (resp. $U_2$) correspond to an ample divisor $E_1$ (resp. $E_2$) so that $E_2 \leq E_1$. The conditions $U_1 \subseteq U_1^\perp$ and $U_2 \subseteq (U_2)^\perp$ may be verified in many examples as we show in the last section by replacing the above polytopes by suitable translates. It remains to know what the minimum distances $d_1$ and $d_2$ are. It is here that we invoke [JA11, Theorems 4.1 and 4.3] to estimate both $d_1$ and $d_2$. See also [JA11, Proposition 4.9 and Corollary 4.11]: observe that [JA11, Theorems 4.1 and 4.3] hold in arbitrary positive characteristics.

6. Examples

In this section we briefly discuss various families of codes we construct, beginning with smooth projective toric varieties of various dimensions. We will always implicitly assume that the basic hypotheses in [JA11, 3.3, 3.4] hold. For the convenience of the reader, we will presently recall some of the more fundamental assumptions there.

1. The base field $k = \mathbb{F}_q$ will be any finite field of cardinality $q$, which is a prime power. We will let $c$ denote the cardinality of $k^*$, i.e. $c = q - 1$. 


(2) The rational points where we evaluate the sections of a line bundle will be the $k$-rational points on the dense torus, which will always be assumed to be split.

(3) Let $\mathcal{M}$ denote the lattice of characters of the split torus $T = G_m^m$. The correspondence between lattice polytopes (i.e. polytopes whose vertices are lattice points) in $\mathcal{M}$ of dimension $m$ and projective toric varieties of dimension $n$ together with the choice of an ample divisor is well-known. See [CLS, Chapters 1 through 4, especially Chapter 2] for further details. In particular, we will always assume that our lattice polytopes are full dimensional i.e. $n = m$ and normal in the sense of [CLS, Definition 2.2.9].

Recall from [CLS, Theorem 2.2.12] that all lattice polytopes in $\mathbb{R}^2$ are normal and lattice polytopes in $\mathbb{R}^m$ so that all coordinates of all its vertices are multiples of $m - 1$ are normal. We ensure this is the case in all the examples, by means of a function in Macaulay2 that automatically fine-tunes the coordinates to ensure this condition. We will use the symbol $U$ for the lattice polytope in $\mathcal{M}$ from which we construct toric codes.

The following are additional assumptions we put on the polytopes.

(4) An assumption we make in all the examples is that if $x_1, \cdots, x_m$ denote the coordinates of $\mathcal{M}$, then there exists one $i$ so that the $x_i$ - coordinates of all the vertices of $U \leq \frac{q-2}{2}$. This will ensure $U \subseteq U^\perp$: see below. (In the Hermitian case, we will instead require that there exists an $i$ so that for all vertices, $q(x_i - \text{coordinate}) \leq \frac{q^2-2}{2}$. This will ensure $U \subseteq U^{\perp_{\text{h}}}$.)

(5) Therefore, we will choose this $x_i$ to be rather small while all the other co-ordinates will be quite large in comparison, so that all our polytopes will be short in one direction and long in the other directions, with all the long-sides being of equal length. The length of the short-side (long-sides) of $U$ will be denoted $s$ ($t$, respectively). We will always assume that $s = s_1 \ast c$, with $s_1 \leq \frac{1}{3}$. In fact, by this choice, $s$ is sufficiently smaller than $(q-2)/2$ (for large enough $q$), and therefore, the difference $(H \setminus U^-) \setminus U$ has many lattice points.

(6) We begin each example with a polytope whose vertices are denoted $v'_i, i = 0, 1, \cdots,$ with the vertex $v'_0$ denoting the origin. We then replace these polytopes by the corresponding polytope obtained by translating the original polytope by adding 1 to all the coordinates of all the vertices. Denoting these polytopes by $U, -U$ will denote the polytope obtained by replacing all the coordinates of all the vertices by their negatives. Then the polytope denoted $U^-$ in Definition 2.3 will be the polytope obtained by adding $(q-1)$ to each of the vertices of the polytope $-U$.

(7) Moreover, as in [JAI1] sections 3.3 and 3.4], the first $m$-faces of the polytopes will be parallel to the coordinate planes. The variables corresponding to these faces in the homogeneous coordinate ring will be denoted $x_i, i = 1, \cdots m$, with the remaining variables denoted $x_{m+1}, x_{m+2},$ etc. The coordinates on the dense torus will be denoted $t_i, i = 1, \cdots, m$.

Let $H = \{0, \cdots q - 2\}^m = \{0, \cdots, q^2 - 2\}^m$ in the Hermitian case). For the purpose of estimating the minimum distance using the corresponding residue codes, it is often convenient and necessary to allow polytopes that do not quite lie in the box $H$: but then we can always replace them by polytopes that lie in the box $H$ and which define the same codes. (One may see this explicitly in the examples.)
Recall from [KS, p. 2892] that for a subsystem code with parameters \([n_Q, k_Q, r_Q, d_Q]\), the quantum singleton bound is given by
\[
(6.0.1) \quad n_Q - (k_Q + r_Q) + 2 \geq 2d_Q.
\]
For the quantum subsystem code provided by Theorems 1.1, recall that \(n_Q = n\), \(k_Q = n - 2k - r\), \(r_Q = r\), \(n_Q = n\), and \(d_Q\) may be replaced by the minimum distance of the dual code \(d = d_{C^\perp}^U\) so that the above Quantum Singleton Bound becomes \(2k + 2 \geq 2d\). Observe that since \(r > 0\), we will need \(0 < r < n - 2k\) as well.

For a quantum stabilizer code with parameters \([n_Q, k_Q, d_Q]\) obtained by applying the CSS-code construction to two generalized toric codes as in Theorem 1.3, again \(n_Q = n\) and \(k_Q = n - k_1 - k_2\), so that the corresponding quantum singleton bound (see [KKKS, §13]) is given by
\[
(6.0.2) \quad n - (k_1' + k_2' - n) + 2 = 2n - (k_1' + k_2') + 2 \geq 2d_Q.
\]
Recall that for the quantum stabilizer code provided by Theorem 1.3, \(k_1' = n - k_1\), \(k_2' = n - k_2\), where \(k_i = \text{dim}(C^U_i), i = 1, 2\) and \(n_Q = n\). Therefore, in this case the Quantum Singleton Bound becomes, \(n - (n - k_1 + n - k_2 - n) + 2 = k_1 + k_2 + 2 \geq 2d_Q\). Here we may again replace \(d_Q\) by the minimum distance of the dual codes \(C^\perp_{U_1}\), which is \(d\). Observe also that clearly we will need \(k_i < n\) so that \(k_i' > 0\), \(i = 1, 2\).

6.1. Determination of the parameters of the classical and quantum codes constructed. We outline here a few basic principles which apply to the whole class of examples we consider.

(i) The length: The length of all the classical and quantum codes we consider, denoted \(n\), will be almost \(c^m\), if the dimension of the toric variety is \(m\). (The reason it is not exactly \(c^m\) is because we have to remove a small number of points from the open orbit so that none of the global sections of the corresponding line bundles have poles in the open orbit. This will become clear in the specific examples considered below.) The lengths of the classical codes and the corresponding quantum codes will both be the same value \(n\).

(ii) The dimension: For a classical code defined by a projective smooth toric variety and the choice of an ample line bundle, the dimension of the code will be the volume of the part of the corresponding lattice polytope that lies in the box \(H\). The dimensions of the corresponding quantum subsystem and quantum stabilizer codes may be determined knowing the dimensions of the two classical codes that are used in their construction as discussed above.

(iii) The minimum distance. For a classical code produced from a projective smooth toric variety and an ample line bundle, we invoke the methods developed by the Hansens: see [JHan99], [SHan02] and amplified in [JHan02]. The main idea here is to subtract from the length of the code determined above, the largest number of possible zeros for any global section of the given line bundle when evaluated at the given rational points: see [SHan02, Theorem 5.9] and/or [JA11, theorem 2.3] for further details.

This involves the choice of certain curves written as an iterated intersection of divisors (each linearly equivalent to a toric divisor), so that all the \(\mathbb{F}_q\)-rational points in the open orbit will lie in the union
of these curves. For the case the toric variety is of dimension 2, these curves may be chosen to be all linearly equivalent to toric divisors as worked out in the examples below. (For higher dimensions, the choice of such curves and computing with them can become a bit involved. This is one of the reasons, we have chosen to restrict to projective spaces in higher dimensions.)

This will provide a lower bound for the minimum distance of the corresponding classical code. Such methods have been adapted in [JAI11, Theorem 1.2] to compute the minimum distances of (modified) toric residue codes, and also of the corresponding dual toric codes. These lower bounds, therefore, will also give a lower bound for the corresponding quantum codes as Theorems 1.1, 1.2 and [1.3] show.

6.2. Examples from Toric surfaces: 2 dimensional examples. In all these examples, the dimension of the codes are given by the areas of the part of the polytopes that lie within the box $H$. We make a careful determination of this parameter ($k$) so that it becomes possible to decide if a given quantum code is Quantum MDS or near Quantum MDS by finding a lower bound for the minimum distance ($d$) and seeing how close $2k$ is to $2d$. The lower bound for the minimum distance will be determined as follows.

Observe that in all these examples $n_Q = c^2$ (at least ignoring lower order terms). Let $\ell$ denote the number of curves of the form $Z(x_i - ax_0)$ (for $i = 1$ or $i = 2$) on which a section $f \in \Gamma(X, \mathcal{O}_X(D + K - E))$ vanishes identically. Since each of these curves has at most $c$-rational points, and there are $c - \ell$ remaining such curves, the maximum possible number of zeros of $f$ is given by $\ell \ast c + (c - \ell) \ast \text{ino}$, where $\text{ino}$ denotes the intersection number $(D + K - E) \ast Z(x_i)$. Therefore, we start with the lower bound $d$ given by

\[(6.2.1) \quad d \geq c^2 - \ell \ast c - (c - \ell) \ast (\text{ino}).\]

The sharpest lower bound for $d$ is obtained as follows. If a global section $f$ of the given line bundle $\mathcal{O}_X(D + K - E)$ vanishes identically on $\ell$ curves of the form $Z(x_i - ax_0)$, then $f$ is also a global section of $\mathcal{O}_X(D + K - E - \ell Z(x_i))$: see [JHan99, §2.3]. Now a similar calculation as above shows:

\[(6.2.2) \quad d \geq c^2 - \ell \ast c - (c - \ell) \ast (\text{ino} - m \ast \ell)\]

if the intersection number $Z(x_i) \ast Z(x_i) = m > 0$.

Then one may readily see that, viewing $d$ as a function of $\ell$, $\text{ino}/m \geq \ell \geq 0$, the critical values for $d$ are $\ell = 0$, $\ell = \text{ino}/m$ which are both local minima for $d$ and $\ell_0 = \frac{(m-1)c + \text{ino}}{2m}$ which is a local maximum. The absolute minimum occurs at $\ell = 0$, (and also at $\ell = \text{ino}$, when $m = 1$) with the absolute minimum value $c^2 - c \ast \text{ino}$. This method, gives us the best possible lower bound for $d$.

For a subset $J_i \subseteq k^*$, $i = 1, 2$, $D_{J_i} = \Sigma_{p \in J_i} Z(x_i - px_3)$ in the first example and $D_{J_i} = \Sigma_{p \in J_i} Z(x_i - px_4)$ in the second example. $f_i$, $i = 1, 2$ are chosen rational points on the 1-dimensional torus forming the 1-st (2-nd) factor of the 2-dimensional torus $G_m^2$ forming the open orbit.
The polytope $U_{11}$

<table>
<thead>
<tr>
<th>Toric variety</th>
<th>The polytope $U$ (Vertices)</th>
<th>The polytope $U^-$ (Vertices)</th>
<th>The Divisors $D_1, D_2$</th>
<th>The Divisor $E$</th>
</tr>
</thead>
</table>
| $\mathbb{P}^2$ | $v_0 = \left( \frac{1}{1} \right)$,  
$v_1 = \left( \frac{t+1}{1} \right)$,  
$v_2 = \left( \frac{1}{s+1} \right)$ | $v_0^- = \left( \frac{q-2}{q-2} \right)$,  
$v_1^- = \left( \frac{q-2-t}{q-2} \right)$,  
$v_2^- = \left( \frac{q-2}{q-2-s} \right)$ | $D_1 = D_{1}' + Z(x_2 - f_2 x_3)$,  
$J'_1 = k^* - \{ t_1 = f_1 \}$,  
$D_2 = D_{2}'$,  
$J'_2 = k^* - \{ t_2 = f_2 \}$ | $E = tZ(x_3 - x_1)$ |
| $Bl_2 \mathbb{P}^2$ | $v_0 = \left( \frac{1}{1} \right)$,  
$v_1 = \left( \frac{t+1}{1} \right)$,  
$v_2 = \left( \frac{t-s+1}{s+1} \right)$,  
$v_3 = \left( \frac{1}{s+1} \right)$ | $v_0^- = \left( \frac{q-2}{q-2} \right)$,  
$v_1^- = \left( \frac{q-2-t}{q-2} \right)$,  
$v_2^- = \left( \frac{q-2}{q-2-s} \right)$,  
$v_3^- = \left( \frac{q-2-t+s}{q-2-s} \right)$ | $D_1 = D_{1}' + D_{2}f_2$  
$J'_1 = k^* - \{ t_1 = f_1, 1 \}$  
$D_2 = Z(x_1 - f_1 x_4) + D_{12}$  
$J'_2 = k^* - \{ t_2 = f_2 \}$ | $E = tZ(x_3 - x_1)$  
$+ sZ(x_4)$ |
| $F_m$ | $v_0 = \left( \frac{1}{1} \right)$,  
$v_1 = \left( \frac{mt+1}{1} \right)$ and  
$v_2 = \left( \frac{mt-m s+1}{s+1} \right)$,  
$v_3 = \left( \frac{1}{s+1} \right)$ | $v_0^- = \left( \frac{q-2}{q-2} \right)$,  
$v_1^- = \left( \frac{q-2-m t}{q-2} \right)$,  
$v_2^- = \left( \frac{q-2-m t + m s}{q-2-s} \right)$,  
$v_3^- = \left( \frac{q-2}{q-2-s} \right)$ | $D_1 = D_{1}' + D_{2}f_2$  
$J'_1 = k^* - \{ t_1 = f_1, 1 \}$  
$D_2 = Z(x_1 - f_1 x_4) + D_{12}$  
$J'_2 = k^* - \{ t_2 = f_2 \}$ | $E = tZ(x_3 - x_1)$  
$+ sZ(x_4)$ |

Parameters for the Codes produced in the above Examples.

Toric variety: $\mathbb{P}^2$

<table>
<thead>
<tr>
<th>Code type</th>
<th>$c$</th>
<th>$t_1$</th>
<th>$s_1$</th>
<th>$nQ$</th>
<th>$k$</th>
<th>$kQ$</th>
<th>$dQ$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsystem</td>
<td>c</td>
<td>41/40</td>
<td>28/100</td>
<td>$c^2$</td>
<td>$\frac{147}{1025}c^2 - \frac{97}{1025}c - \frac{25}{205}$</td>
<td>$575$</td>
<td>$120$</td>
</tr>
<tr>
<td>Stabilizer</td>
<td>c</td>
<td>41/40</td>
<td>28/100</td>
<td>$c^2$</td>
<td>$\frac{147}{1025}c^2 - \frac{97}{1025}c - \frac{25}{205}$</td>
<td>$575$</td>
<td>$120$</td>
</tr>
<tr>
<td>Subsystem $^1$</td>
<td>31</td>
<td>41/40</td>
<td>28/100</td>
<td>961</td>
<td>121</td>
<td>$575$</td>
<td>$120$</td>
</tr>
<tr>
<td>Stabilizer $^1$</td>
<td>31</td>
<td>41/40</td>
<td>28/100</td>
<td>961</td>
<td>121</td>
<td>$575$</td>
<td>$120$</td>
</tr>
<tr>
<td>Subsystem $^2$</td>
<td>31</td>
<td>41/40</td>
<td>29/100</td>
<td>961</td>
<td>125</td>
<td>$569$</td>
<td>$120$</td>
</tr>
<tr>
<td>Stabilizer $^2$</td>
<td>31</td>
<td>41/40</td>
<td>29/100</td>
<td>961</td>
<td>125</td>
<td>$569$</td>
<td>$120$</td>
</tr>
<tr>
<td>Subsystem</td>
<td>c</td>
<td>11/10</td>
<td>1/3</td>
<td>$c^2$</td>
<td>$\frac{2}{11}c^2 - \frac{7}{11}c - \frac{5}{3}$</td>
<td>$\frac{2}{11}c^2 + \frac{2}{11}c - \frac{3}{33}$</td>
<td>$\geq \frac{1}{10}c^2 + \frac{7}{10}c - \frac{3}{3}$</td>
</tr>
<tr>
<td>Stabilizer</td>
<td>c</td>
<td>11/10</td>
<td>1/3</td>
<td>$c^2$</td>
<td>$\frac{2}{11}c^2 - \frac{7}{11}c - \frac{5}{3}$</td>
<td>$\frac{7}{11}c^2 + \frac{14}{11}c + \frac{10}{3}$</td>
<td>$\geq \frac{1}{10}c^2 + \frac{29}{10}c - \frac{3}{3}$</td>
</tr>
<tr>
<td>Subsystem</td>
<td>120</td>
<td>11/10</td>
<td>1/3</td>
<td>14400</td>
<td>2540</td>
<td>7460</td>
<td>1780</td>
</tr>
<tr>
<td>Stabilizer</td>
<td>120</td>
<td>11/10</td>
<td>1/3</td>
<td>14400</td>
<td>2540</td>
<td>9310</td>
<td>1780</td>
</tr>
</tbody>
</table>

In the table appearing above and below, 1 (2) denotes a Quantum MDS code (a Near Quantum MDS code).
6.3. Examples from higher dimensional toric varieties. Next we consider the higher-dimensional examples of $\mathbb{P}^n$, beginning with $\mathbb{P}^3$. Though our methods apply for all $n > 2$, we only discuss explicitly the case $n = 3$ and $n = 4$.

The variables $x_i$ provide the homogeneous coordinates for $\mathbb{P}^3$ and generate the Cox-ring. Let $T = G_3^m$ denote the dense open torus in $\mathbb{P}^3$. Therefore the coordinates $(t_1, t_2, t_3)$ on the dense torus $G_m^3$ are given by $t_i = \frac{x_i}{x_4}$, $i = 1, 2, 3$.

Since $CH^1(\mathbb{P}^3) = \mathbb{Z}$, each variable $x_i$ has weight 1. Clearly

\[(6.3.1)\]

\[E' = t\mathbb{Z}(x_4)\]

denotes the divisor on $\mathbb{P}^3$ corresponding to the given polytope, where $\mathbb{Z}(x_i)$ denotes the toric divisor where the homogeneous coordinate $x_i = 0$. We will replace $E'$ by the linearly equivalent divisor $E = t\mathbb{Z}(x_4 - x_1)$.
The polytope $U$ is the image of the variety $T$ under the projection $\pi_1$. The polytope $U$ is the image of the variety $T$ under the projection $\pi_2$. The polytope $U$ is the image of the variety $T$ under the projection $\pi_3$. The polytope $U$ is the image of the variety $T$ under the projection $\pi_4$. The polytope $U$ is the image of the variety $T$ under the projection $\pi_5$. The polytope $U$ is the image of the variety $T$ under the projection $\pi_6$. The polytope $U$ is the image of the variety $T$ under the projection $\pi_7$. The polytope $U$ is the image of the variety $T$ under the projection $\pi_8$. The polytope $U$ is the image of the variety $T$ under the projection $\pi_9$.

Lemma 6.1. (i) $\cap_{i=0}^2 D_i - \{[1 : 0 : 0 : 0], [0 : x_2 : x_3 : x_4], \text{each } x_i \neq 0\} \subseteq \text{the dense torus } \mathbb{G}_m^3$. (ii) $\cap_{i=0}^2 D_i \cap |E| \text{ is empty}.$

Proof. Let $p = [x_1 : x_2 : x_3 : x_4]$ denote a point in $\cap_{i=0}^2 D_i$. Then one may observe that if $x_4 = 0$, then $x_2 = x_3 = 0$ as well, since the point lies in $\cap_{i=0}^2 D_i$; therefore, the only such point is $[1 : 0 : 0 : 0]$. But if $x_4 \neq 0$, then $x_2 \neq 0$ and $x_3 \neq 0$, so that the only possibility is with either $x_1 \neq 0$ also or $x_1 = 0$. Clearly if all the $x_i \neq 0, i = 1, 2, 3, 4$, then this point lies in the open dense torus. This proves (i). Now (ii) follows from the observation that neither the point $[1 : 0 : 0 : 0]$ nor the points $[0 : x_2 : x_3 : x_4]$, with all $x_i \neq 0, i = 2, 3, 4$ belong to $|E|$, since $E = Z(x_4 - x_1)$. The polytope and the divisors for $\mathbb{P}^3$ will be given as follows.

Table 2. Details on the Toric Variety and the Polytope

<table>
<thead>
<tr>
<th>Toric Variety</th>
<th>The Polytope $U$ (Vertices)</th>
<th>The Polytope $U^-$ (Vertices)</th>
<th>The Divisors $D_i$ (Vertices)</th>
<th>The Divisor $E$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{P}^3$</td>
<td>$v_0 = \begin{pmatrix} 1 \ 1 \ 1 \end{pmatrix}$,</td>
<td>$v_0^- = \begin{pmatrix} q-2 \ q-2 \ q-2 \end{pmatrix}$,</td>
<td>$D_1 = D_{f_1} + Z(x_2 - f_2 x_4)$,</td>
<td>$E = tZ(x_4 - x_1)$</td>
</tr>
<tr>
<td></td>
<td>$v_1 = \begin{pmatrix} t+1 \ 1 \ 1 \end{pmatrix}$,</td>
<td>$v_1^- = \begin{pmatrix} q-2-t \ q-2 \ q-2 \end{pmatrix}$,</td>
<td>$D_2 = D_{f_2}$,</td>
<td>$D_3 = D_{f_3}$</td>
</tr>
<tr>
<td></td>
<td>$v_2 = \begin{pmatrix} t+1 \ 1 \ 1 \end{pmatrix}$,</td>
<td>$v_2^- = \begin{pmatrix} q-2-t \ q-2 \ q-2 \end{pmatrix}$,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$v_3 = \begin{pmatrix} 1 \ 1 \ s+1 \end{pmatrix}$,</td>
<td>$v_3^- = \begin{pmatrix} q-2 \ q-2 \ q-2 \end{pmatrix}$,</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6.4. Let $s_0 = \frac{(x_3 - f_2 x_4)}{(x_4 - x_1)}$; see, for example [JA11 4.2]. Then the weight of the numerator and denominator are both the same. By choosing $f_3$ suitably, we can make sure that $s_0$ does not vanish at any points in the intersection $\cap_{i=0}^2 D_i$.

The above observations verify all the hypotheses in [JA11 3.3 and 3.4]. Next observe that the divisor $D_1 + D_2 + D_3 + K - E$ is linearly equivalent to $(c-2)Z(x_1) + (c-1)Z(x_2) + (c-1)Z(x_3) - (t+1)Z(x_4)$. The latter divisor corresponds to the polytope similar to the polytope for $(X, \mathcal{O}_X(E))$, except that the
bottom face is at \( x_3 = -c + 1 \), with the two bottom vertices will be \( (r_1 + 1)c - t - r_1 - 3 \) and 
\[
\begin{pmatrix}
(r_1 + 1)c - t - r_1 - 2 \\
-c + 1 \\
-c + 1
\end{pmatrix}
\]
and the \( x_3 \)-axis will move to the line \( x_1 = -c + 2, x_2 = -c + 1 \), with the inclined face given by the equation \( x_1 + x_2 + r_1x_3 = -t - 1 \). One may also observe that, by putting \( x_1 = -c + 2, x_2 = -c + 1 \) and solving for \( x_3 \) in the equation of the inclined face \( x_1 + x_2 + r_1x_3 = -t - 1 \), shows that the top vertex of the polytope \( U \) is given by \( (-c + 2, -c + 1, \frac{2c-t-4}{r_1}) \).

**Estimating the minimum distance of the code.** Next let \( s \in \mathbb{F}_q^* \) be fixed element, and suppose a global section \( f \in \Gamma(X, \mathcal{O}_X(D + K - E)) \) vanishes identically on \( \ell_s \) lines of the form \( L_j : Z(x_3 - a(j)x_4) \cap Z(x_2 - sx_1), j = 1 \cdots, \ell_s \). Observe that the equation \( Z(x_2 - sx_1) \) defines a hyperplane

Essentially the same description applies to all the higher dimensional projective space. The parameters of the resulting quantum codes are listed below for both \( \mathbb{P}^3 \) and \( \mathbb{P}^4 \) for certain choice of the parameters \( t_1 \) and \( s_1 \).

<table>
<thead>
<tr>
<th>Code type</th>
<th>( c )</th>
<th>( t_1 )</th>
<th>( s_1 )</th>
<th>( n_Q )</th>
<th>( k )</th>
<th>( k_Q )</th>
<th>( d_Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsystem</td>
<td>( c )</td>
<td>412/200</td>
<td>.295</td>
<td>( c^3 )</td>
<td>( 5431/61800c^3 - \frac{177}{10300}c^2 )</td>
<td>( 5431c^3/61800 + \frac{177}{10300}c^2 )</td>
<td>( \geq \frac{3}{50}c^3 + \frac{72}{25}c^2 )</td>
</tr>
<tr>
<td>Stabilizer</td>
<td>( c )</td>
<td>412/200</td>
<td>.295</td>
<td>( c^3 )</td>
<td>( 6431/61800c^3 - \frac{177}{10300}c^2 )</td>
<td>( 6431c^3/61800 + \frac{177}{10300}c^2 )</td>
<td>( \geq \frac{3}{50}c^3 + \frac{72}{25}c^2 )</td>
</tr>
<tr>
<td>Subsystem</td>
<td>63</td>
<td>412/200</td>
<td>295/1000</td>
<td>123039</td>
<td>28000</td>
<td>194000</td>
<td>26908</td>
</tr>
<tr>
<td>Stabilizer</td>
<td>63</td>
<td>412/200</td>
<td>295/1000</td>
<td>123039</td>
<td>28000</td>
<td>194000</td>
<td>26908</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code type</th>
<th>( c )</th>
<th>( t_1 )</th>
<th>( s_1 )</th>
<th>( n_Q )</th>
<th>( k )</th>
<th>( k_Q )</th>
<th>( d_Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsystem</td>
<td>( c )</td>
<td>1203/400</td>
<td>.287</td>
<td>( c^4 )</td>
<td>( 28987c^4 + \frac{861}{401000}c^3 + \frac{34413}{401000}c^2 )</td>
<td>( 28987c^4 + \frac{861}{401000}c^3 + \frac{34413}{401000}c^2 )</td>
<td>( \geq \frac{3}{400}c^4 + \frac{1591}{400}c^3 )</td>
</tr>
<tr>
<td>Stabilizer</td>
<td>( c )</td>
<td>1203/400</td>
<td>.287</td>
<td>( c^4 )</td>
<td>( 17133c^4 + \frac{861}{401000}c^3 + \frac{34413}{401000}c^2 )</td>
<td>( 17133c^4 + \frac{861}{401000}c^3 + \frac{34413}{401000}c^2 )</td>
<td>( \geq \frac{3}{400}c^4 + \frac{1591}{400}c^3 )</td>
</tr>
<tr>
<td>Subsystem</td>
<td>63</td>
<td>1203/400</td>
<td>.287</td>
<td>15752961</td>
<td>1120000</td>
<td>10800000</td>
<td>953312</td>
</tr>
<tr>
<td>Stabilizer</td>
<td>63</td>
<td>1203/400</td>
<td>.287</td>
<td>15752961</td>
<td>1120000</td>
<td>13500000</td>
<td>953312</td>
</tr>
</tbody>
</table>
7. Appendix: Toric residue theorems over finite fields

In this section we first recall the toric residue theorems over finite fields first proved in [JA11, Theorems 4.1 and 4.3] which extends the intersection theory methods for evaluation codes discussed in [SHan02] and [JHan02] to compute the distance of the dual of toric evaluation codes. This is discussed for toric varieties of arbitrary dimensions satisfying the following basic assumptions (see [JA11, §3.4]). See also [JHan13] for a discussion of a residue theorem for toric surfaces that is established along similar lines.

7.1. Hypotheses on the toric varieties. In [JA11, §3.4] we made a number of hypotheses on the polytopes and the resulting projective toric varieties that we consider. We summarize most of them here, and the reader may consult [JA11, §3.4] for the remaining details. The first two are merely observations or notational conventions, the conditions (2), (3) and (7) are basic hypotheses on the toric variety and on the shape of the corresponding polytope, while (4) is a condition on the Euler form and (5), (6) are conditions on the line bundle $L$. As usual $\mathbb{M}$ will denote the lattice of characters of the dense torus and $\mathbb{N}$ its dual lattice.

(0) Given an $n$-dimensional toric variety defined over a field $k$, we will assume that for all toric varieties that we consider, all the orbits are in fact split tori. The divisor of zeros of a homogeneous polynomial $f$ (i.e. an element of the homogeneous coordinate ring of the toric variety: see [CLS]) will be denoted $Z(f)$.

(1) The cardinality of $k^*$ is denoted $c$. (Observe that, if $k = \mathbb{F}_{p^s}$ for some prime $p$ and $s \geq 1$, then $c = p^s - 1$.)

(2) $X$ is a smooth projective toric variety defined over $k$ by the complete fan $\Sigma \subseteq \mathbb{N}$ or equivalently by the rational polytope $P \subseteq \mathbb{M}_\mathbb{R}$. Let $\Sigma(1) = \{\rho_i \mid i = 1, \ldots, N\}$ denote the 1-dimensional cones in the fan, and let $\{x_i \mid i = 1, \ldots, N\}$ denote the corresponding variables in the associated homogeneous coordinate ring of $X$. We will often denote the divisor $Z(x_i)$ by $B_i$.

(3) We will assume that $d = \dim_k X = \dim_\mathbb{R}(\mathbb{M}_\mathbb{R})$. We will also assume that $d$ faces of the polytope $P$ lie on the coordinate planes in $\mathbb{R}^d \cong \mathbb{M}_\mathbb{R}$: we may assume without loss of generality these faces correspond to the variables $x_1, i = 1, \ldots, d$.

(6) In addition, we require that there exist a section $s_0 \in \Gamma(X, L)$ of the following form:

$$\frac{(x_1 - f_1 \phi_1)^{g_1} \cdots (x_d - f_d \phi_d)^{g_d}}{(x_{d+1} - h_{d+1} \psi_{d+1})^{e_{d+1}} \cdots (x_N - h_N \psi_N)^{e_N}}.$$

where the $f_i$ are chosen as in (7.2.1) and the $g_i$ are non-negative integers. Observe that $s_0(P_i) \neq 0$ for any of the chosen points above. This follows from the observation that the points $P_i$ have all coordinates different from $f_i$, $i = 1, \ldots, d$.

(7) A generic point on the 1-dimensional rays $\rho_i$, for $i = d+1, \ldots, N$ belongs to the region of $\mathbb{N}_\mathbb{R} \cong \mathbb{R}^d$ with all the coordinates $x_1, \ldots, x_d$, non-positive.

The missing hypotheses (4) and (5) are assumptions on the Euler form as well as on the choice of the divisors associated to the polytopes.

7.2. Choice of the rational points and the divisors. One obvious choice of the set of $k$-rational points are all the $k$-rational points belonging to the open dense orbit: assuming the tori are all split,
this corresponds to picking these points to be all the \( k \)-rational points in \( \mathbb{G}^d_m \) if \( \dim_k(X) = d \). This is the common choice made in the construction of classical codes from toric varieties - see [JHan02]. For the purposes of our constructions below, and especially for the applications to residue codes, it seems nevertheless preferable to consider a slightly smaller subset of \( k \)-rational points chosen as follows. Let
\[ k[\mathbb{G}^d_m] = k[t_1, t_1^{-1}, t_2, t_2^{-1}, \ldots, t_d, t_d^{-1}] \]
The variable \( t_i \) will also denote the \( i \)-th coordinate of a point in \( \mathbb{G}^d_m \). For each rational point \( a \in k^* \) and \( i = 1, \ldots, d \), we let \( D_{i,a} \) denote the divisor which is the closure of \( \text{div}(t_i - a) \) in the given toric variety \( X \). We will often denote this by \( Z(t_i - a) \) as well. For a subset \( S_i \) of the \( k \)-rational points forming the \( i \)-th factor of \( \mathbb{G}^d_m \), we let \( D_{S_i} = \sum_{a \in S_i} D_{i,a} \).

We choose the divisors as follows. We let \( J_i = \mathbb{G}^* \), for \( i = 1, \ldots, d \). For each \( i = 1, \ldots, d \), we let \( f_i \in k^* \) denote a single chosen rational point. Then we let \( J_i' \subseteq J_i - \{ f_i \} \) be such that there exists a fixed integer \( n \) so that \( |J_i'| \geq |k^*|/n \), for all \( i \). We let
\begin{equation}
J_i = D_{J_i'} + \sum_{j \neq i} D_{j,f_j}, i = 1, \ldots, d.
\end{equation}
We let \( |J_i'| = n_i \) and also let \( D_i' = D_{J_i'} \). For each divisor \( F \), we let \( |F| \) denote its support. In this case, observe that the intersection \( \bigcap_{i=1}^d |D_i'| \) has at least \((c/n)^d\) \( k \)-rational points \textit{in the dense orbit} with \( c = |k^*| \), whereas the intersection \( \bigcap_{i=1}^d |D_i| \) has more points. This intersection always contains the point \( f = (f_1, \ldots, f_d) \) when \( D_i \) is defined by (7.2.1).

The basic hypotheses we impose then is the following:
\begin{equation}
D_{i,a} \cdot V(\rho) \geq 0, i = 1, \ldots, d, \quad (\sum_{i=1}^d D_{i,a}) \cdot V(\rho) > 0 \quad \text{and} \quad \bigcap_{i=1}^d |D_i| \text{ is finite}
\end{equation}
where \( V(\rho) \) denotes any of the \( d - 1 \)-dimensional cones in the given fan and \( a \in k^* \).

**Remark.** These hypotheses need to be verified on a case by case basis: we show these are satisfied in all the two dimensional examples we considered. These ensure that the next Proposition is true, which together with the last condition enables one to apply Theorem 7.2 as well as Theorem 7.3.

**Proposition 7.1.** (See [JA11], Proposition 3.7.] Under the hypothesis (7.2.2), each of the divisors \( D_i \) defined above is ample.

**Theorem 7.2.** (See [JA11], Theorem 4.1.) Let \( X \) denote a projective smooth toric variety defined over the finite field \( \mathbb{F}_q \). Let \( d = \dim_{\mathbb{F}_q}(X) \) and let \( D_1, \ldots, D_d \) denote \( d \) effective ample Cartier divisors on \( X \), so that their intersection is a finite number of \( \mathbb{F}_q \)-rational points. Then
\[ \sum_{x \in \cap_{i=1}^d |D_i|} \text{Res}_x(\omega) = 0 \]
for any differential form \( \omega \in \Gamma(X, \omega_X(D_1 + \cdots + D_d)) \) and where \( \text{Res}_x(\omega) \) denotes the local residue of the differential form \( \omega \) at \( x \).

**Theorem 7.3.** (See [JA11], Theorem 4.3.) Assume that \( X \) is a projective smooth toric variety of dimension \( d \) defined over \( k \) by a polytope \( \mathcal{P} \) satisfying the basic hypotheses as \( D_i, i = 1, \ldots, d \) is a set of effective ample divisors on \( X \) and \( \cap_{i=1}^d |D_i| = \{ R_\ell \mid \ell = 1, \ldots, M \} \) where each \( R_\ell \) is a \( k \)-rational
point of \( X \). Assume that for each point \( R_ℓ \), one is given \( vℓ(Rℓ) ∈ k^* \) so that the sum \( Σℓvℓ(Rℓ) = 0 \). Then
there exists a differential form \( η ∈ Γ(X, ω_X(Σ_iD_i)) \) so that \( \text{Res}_Rℓ(η) = vℓ(Rℓ) \).

The modified evaluation and residue codes associated to an effective divisor \( E \). Let \( P' = \{ P_1, \ldots, P_M \} \) denote a set of \( k \)-rational points in the dense orbits in \( X \). Let \( L \) denote an ample line bundle on \( X \) associated to an effective divisor \( E \). Now \( L = O(E) \). Let \( s \) denote a section of \( L \). We send any such section \( s \) to \( (s(P_0), s(P_1), \ldots, s(P_m), s(P_{m+1}), \ldots, s(P_M)) ∈ k^M \). Letting \( P = \{ P_1, \ldots, P_m \} \), we define the code \( C(X, E, P) \) to be the image in \( k^M \) by the evaluation map \( s ↦ (s(P_1), \ldots, s(P_m), \ldots, s(P_M)) \), of the \( k \)-subspace \( \{ s ∈ Γ(X, L)| s(P_i) = 0, i = m + 1, \ldots, M \} \). Since the last \( M - m \) coordinates are zero, one may view the code \( C(X, E, P) \) as a subspace of \( k^m \).

Assume next that the divisors \( D_i, i = 1, \ldots, d, \) are chosen as in (7.2.1). Let \( σ \) denote a permutation of \( 1, \ldots, n \) so that \( σ(i) \neq i \) for all \( i \). Now let \( \bar{D}_i = D_i + D_{σ(i)}, f_{σ(i)} \), \( i = 1, \ldots, d \). Therefore, \( \bar{D}_i = \bar{D}_i + d_i, f_i \), and \( |D_i| = |D_i|, \) for each \( i \) so that \( \bigcap_i |D_i| = \bigcap_i |D_i|, \). In this case we let
\[
C(X, \omega_X, E, P) = \{ α ∈ Γ(X, K(X) ⊗ ω_X) | (α) + D + \sum_i D_i, f_i - E ≥ 0 \},
\]
where \( \omega_X \) denotes, as before, the sheaf of top-degree differential forms on \( X \). We call this the \( \text{modified residue code} \) in this case.

**Definition 7.4.** (i) If \( k = F_q \), we define \( \text{Res} : C(X, \omega_X, E, P) → F_q^m \subseteq F_q^M \) by sending \( α ∈ C(X, \omega_X, E, P) \mapsto (\text{Res}_{P_1}(α), \ldots, \text{Res}_{P_m}(α), 0, \ldots, 0) \).

(ii) If \( k = F_{q^2} \), we define \( \overline{\text{Res}} : C(X, \omega_X, E, P) → F_q^m \subseteq F_q^M \) by sending \( α ∈ C(X, \omega_X, E, P) \mapsto (\text{Res}_{P_1}^q(α), \ldots, \text{Res}_{P_m}^q(α), 0, \ldots, 0) \).

**Definition 7.5.** (i) For a code \( C ⊆ F_q^m \), we define
\[
C^⊥ = \{ x ∈ F_q^m | Σ_i x_i y_i = 0 \text{ for any } y ∈ C \}.
\]

(ii) For a code \( C ⊆ F_{q^2}^m \), we define
\[
C^⊥^h = \{ x ∈ F_{q^2}^m | Σ_i x_i^2 y_i = 0 \text{ for any } y ∈ C \}.
\]

**Proposition 7.6.** Assume the above situation. Then Theorem 7.2 implies the following:

(i) Assume that the base field is \( F_q \). Then the image of the code \( C(X, \omega_X, E, P) \) (defined above) under the residue map \( \text{Res} \) above is contained in \( C(X, E, P)^⊥ \).

(ii) Assume that the base field is \( F_{q^2} \). Then the image of the code \( C(X, \omega_X, E, P) \) (defined above) under the residue map \( \overline{\text{Res}} \) above is contained in \( C(X, E, P)^⊥^h \).

**Proof.** Statement (i) is already proved in [JA11, Proposition 4.9]. Therefore, we will consider (ii). Recall that the divisors are defined as in (7.2.1). Now a key observation is that \( |D_i| = |D_i|, \) for all \( i = 1, \ldots, d \). Let \( f ∈ C(X, E, P) \). Recall from above that \( f(P_i) = 0, \) for all \( i = m + 1, \ldots, M \). If \( α ∈ C(X, \omega_X, E, P) \), then
the product $f_\alpha$ has poles contained in $\bigcup_{i=1}^{d} |\tilde{D}_i| = \bigcup_{i=1}^{d} |D_i|$, so that Theorem 7.2 and the observation above show that the sum

$$\sum_{p \in \bigcap_{i=1}^{d} |\tilde{D}_i|} \text{Res}_p(f_\alpha) = \sum_{p \in \bigcap_{i=1}^{d} |D_i|} \text{Res}_p(f_\alpha) = \sum_{p \in \bigcap_{i=1}^{d} |D_i|} f(p) \text{Res}_p(\alpha) = 0. \tag{7.2.5}$$

In particular, we may replace $\text{Res}_{P_i}(\alpha)$ by 0 for all $i = m+1, \ldots, M$.

Now taking the $q$-th powers, we see that

$$\sum_{p} f(p)^q \text{Res}_p(\alpha) = \sum_{p} f(p)^q \text{Res}_p(\alpha)^q = \sum_{p} \text{Res}_p(f_\alpha)^q = \left(\sum_{p} f(P) \text{Res}_P(\alpha)\right)^q = 0.$$ 

Under the above hypotheses we obtain the following corollary to the last Proposition.

**Corollary 7.7.** (i) Assume the above situation and that the base field is $\mathbb{F}_q$. Given any sequence 
$$\{r_j \in k \mid j = 1, \ldots, m\}$$ 
with the property that

$$\sum_{j} f(p_j)r_j = 0$$ 

for any global section $f \in C(X, E, \mathcal{P})$, 

there exists a differential form $\omega' \in C(X, \omega_X, E, \mathcal{P})$ so that $\text{Res}_{P_i}(\omega') = r_i$, $i = 1, \ldots, m$. (The divisor $D_{i, f_i}$ is defined as in 7.2.1.) Therefore, the residue map of Definition 7.4 sends $C(X, \omega_X, E, \mathcal{P})$ onto $C(X, E, \mathcal{P})$.

(ii) Assume the base field is $\mathbb{F}_{q^2}$. Given any sequence 
$$\{r_j \in k \mid j = 1, \ldots, m\}$$ 
with the property that

$$\sum_{j} f(p_j)r_j = 0$$ 

for any global section $f \in C(X, E, \mathcal{P})$, 

there exists a differential form $\omega' \in C(X, \omega_X, E, \mathcal{P})$ so that $\text{Res}_{P_i}(\omega') = r_i^q$, (i.e. $\text{Res}_{P_i}(\omega') = r_i$), $i = 1, \ldots, m$. (The divisor $D_{i, f_i}$ is defined as in 7.2.1.) Therefore, the residue map of Definition 7.4 sends $C(X, \omega_X, E, \mathcal{P})$ onto $C(X, E, \mathcal{P})$.

**Proof.** The first statement is already proved in [JAI11, Corollary 4.11], so that we will only consider statement (ii). Consider the sequence $\{r_i s_0(P_i) \mid i = 1, \ldots, m\}$, where $s_0$ is the chosen section in $\Gamma(X, \mathcal{L})$, chosen so that $s_0(P_i) \neq 0$ for all $i = 1, \ldots, m$. (The existence of such a section is our hypothesis in 7.1.6.)

Define $r_j = 0$ for all $j = m+1, \ldots, M$. Next recall $s_0 \in K(X)$ so that $\text{div}(s_0) + E \geq 0$, where $\mathcal{L} = \mathcal{O}_X(E)$. Since $r_j = 0$ for all $j = m + 1, \ldots, M$, clearly the sum $\sum_j r_j s_0(P_j) = (\sum_j r_j s_0(P_j))^q = 0$, where the sum is taken over all the $k$-rational points in the intersection $\bigcap_{i=1}^{d} |D_i|$, so that by Theorem 7.3, there exists a differential form $\omega' \in \Gamma(X, \omega_X(\sum_{i=1}^{d} D_i))$ with $\text{Res}_{P_i}(\omega') = r_i^q s_0(P_i)$, $i = 1, \ldots, M$. Now consider the differential form $\omega' = \frac{\omega}{s_0}$; since $s_0$ is regular and does not vanish at each point $P_i$, $i = 1, \ldots, m$, it follows that $\text{Res}_{P_i}(\omega') = \text{Res}_{P_i}(\frac{\omega}{s_0}) = \frac{\text{Res}_{P_i}(\omega)}{s_0(P_i)} = r_i^q$, $i = 1, \ldots, m$. The hypotheses on $\omega$ and $s_0$ show that $\omega' \in \Gamma(X, \omega_X(\sum_{i=1}^{d} D_i + \sum_{i=1}^{d} D_{i, f_i} - E)) = C(X, \omega_X, E, \mathcal{P})$ in case the divisors $D_i$ are defined as in 7.2.1. These prove (ii).

**References**


[Mac2] Macaulay2:Package for Algebra and Algebraic Geometry, See: https://faculty.math.illinois.edu/Macaulay2/


**Department of Mathematics, Ohio State University, Columbus, Ohio, 43210, USA.**

*E-mail address*: joshua.10@math.osu.edu

**Department of Mathematics and Computer Science, University of Missouri, St. Louis, Missouri, USA.**

*E-mail address*: girivarur@umsl.edu