QUANTUM STABILIZER AND SUBSYSTEM CODES FROM ALGEBRO-GEOMETRIC TORIC CODES

ROY JOSHUA AND G. V. RAVINDRA

Abstract. We show how to construct 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. We also show that the parameters of our quantum codes compare favorably with several of the existing quantum codes.

Contents

1. Introduction 1
2. Toric and Generalized Toric evaluation codes as multicyclic codes 6
3. Quantum stabilizer codes and subsystem codes 11
4. Construction of sub-system codes from Generalized toric codes 12
5. Quantum stabilizer codes from toric varieties over \( \mathbb{F}_q \) 14
6. Examples 15
7. Appendix: Toric residue theorems over finite fields 28
References 32

1. Introduction

Quantum information processing is a rapidly developing field which promises to speed up computations exponentially faster than often possible using classical computers: it exploits and utilizes fundamental rules of quantum mechanics. However, quantum states carrying quantum information are susceptible to noise and decoherence, so that quantum error-correction has to be incorporated into quantum information processing itself. This feature makes quantum error correction and fault tolerant computational techniques a key component of quantum information processing.

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, making use of the technique of Toric Residues on projective toric varieties over finite fields. The Toric residue theorems, [JA11] Theorems 4.1 and 4.3] prove a toric residue theorem for toric varieties of arbitrary dimensions over finite fields, as well as a partial converse. These enable one to adapt the methods of [SHan02] and [JHan02] making use of intersection theory, to determine

The first author was supported by a grant from the NSF and the second author was supported by a grant from the Simons Foundation.
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 [CCD], 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 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. Another equally important result in [JA11] was the following discovery. One needs to first restrict to toric evaluation codes on projective toric varieties defined by polytopes satisfying a small number of conditions as in [JA11, Theorem 3.4]. Here, toric varieties of arbitrary dimensions are allowed. A modified toric evaluation (residue) code is one where we evaluate (take residues) only at a proper subset of the set of all rational points on the dense torus. It is shown in [JA11, Corollary 4.11] that, associated to a given modified toric evaluation code from such a projective toric variety, one can construct a modified toric residue code, which, while not equal to the dual of the original modified toric evaluation code, maps surjectively onto this dual code, so that the minimum distance of the toric residue code provides a readily computable lower bound for the minimum distance of the dual of the original modified toric evaluation code.

Though Reed-Solomon codes are simple enough to define, and have been around since the early 1960s, the simple fact that they are MDS codes makes them quite superior, at least in certain respects, and may in fact account for the fact that Reed-Solomon codes are still widely used.

Toric codes, i.e. codes coming from convex polytopes, behave quite similar to Reed-Solomon codes, but with one major advantage: for the Reed-Solomon codes, the block size can never exceed the cardinality of the field, whereas toric codes can easily reach block-sizes that are several powers of the cardinality of the field, by taking higher dimensional toric varieties. In addition, for toric codes constructed from convex polytopes, the intersection theory methods enable one to produce lower bounds for the minimum distance as well as the dimension of the code that are directly proportional to the block length so that taking larger and larger field extensions often produce families of toric codes that behave very nicely. We show that these advantages carry over to the quantum codes that we construct in this paper. In addition, the method of toric residues and intersection theory are simple and transparent enough that one can compute the parameters of many quantum codes derived from toric surface codes, over fields of arbitrarily large size, by hand. The parameters of quantum codes derived from toric 3-folds and higher dimensional toric varieties can be computed with a little computer help in computing mixed volumes (i.e. intersection numbers) as shown in the last example in section 6 and also in [JTS].

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 $\mathbb{F}_{q^2}$, where $q$ is any prime power, where the presence of the involution $x \mapsto x^q$, $x \in \mathbb{F}_{q^2}$ (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 purpose of the present paper, is to address all of the above issues, and as we show in this paper, this method seems particularly suited for producing quantum codes with readily computable large minimum distances and dimensions that are directly proportional to the block-size. Varying the size of the field then produces nice families of codes where the ratio of the minimum distance to block-size remains bounded. The parameters of the codes produced compare favorably with the parameters of several existing quantum codes.

In order to state our main results, we need to introduce a few key technical terms. The vector space $\mathbb{F}_q^n$ will have the standard inner product defined by $\langle v, w \rangle = \sum_{i=1}^n v_i w_i$, where $v = (v_1, \ldots, v_n)$ and $w = (w_1, \ldots, w_n)$. As mentioned above, the field $\mathbb{F}_q$ comes equipped with the involution $x \mapsto x^q$. The vector space $\mathbb{F}_q^n$, therefore also has the inner product defined by $\langle v, w \rangle = \sum_{i=1}^n v_i^q w_i$. (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 $\mathbb{F}_q$ ($\mathbb{F}_2$), and $W$ is a subspace of $V$, we let $W^\perp = \{ v \in V | \langle v, w \rangle = 0, \text{ for all } w \in W \}$ ($W^\perp_h = \{ v \in V | \langle v, w \rangle_h = 0, \text{ for all } w \in W \}$, 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 in the box $H = \{0, \ldots, q - 2\}^r$ if we are considering codes over $\mathbb{F}_q$ and by polytopes in $H = \{0, \ldots, q^2 - 2\}^r$ if we are considering codes over $\mathbb{F}_q^2$, for some $r > 0$. If $U \subseteq H$, $C_U$ will denote the associated toric evaluation code. A linear code $C$ over $\mathbb{F}_q$ ($\mathbb{F}_2$) 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 $T \subseteq H = \{0, \ldots, q - 2\}^r$, $T^- := \{ v \in H | v \equiv -v' \text{mod}((q - 1)\mathbb{Z})^r \text{ for some } v' \in T \}$: 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 $H \setminus U^-$. 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) $T^- \subseteq D(C_U) \setminus D(C_U^\perp)$.

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

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

Over $\mathbb{F}_q^2$, for a subset $T \subseteq H = \{0, \ldots, q^2 - 2\}^r$, we let $T^-_q := \{ v \in H | v \equiv -v' \text{mod}((q^2 - 1)\mathbb{Z})^r \text{ for some } v' \in T \}$: 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 $H \setminus U^{-q}$. We denote this 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 $\mathbb{F}_q$. Let $T$ denote a subset of $D_h(C_U) \setminus D_h(C_U^{\perp h})$. Then

(i) $T^{-q} \subseteq D_h(C_U) \setminus D_h(C_U^{\perp h})$.

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

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

The proof of these theorems are discussed in section 4 and make intrinsic use of defining sets. Aly, Klappenecker and Sarvepalli (see [AKS]) and Aly (see [Aly]) had shown that Euclidean and Hermitian constructions may be applied to classical cyclic codes to produce subsystem codes. The above theorems extend these constructions, to produce subsystem codes starting with classical toric codes over finite fields. In fact Aly’s construction then becomes a very special case of our construction, by viewing classical cyclic codes as one-dimensional generalized toric codes.

The main results of [JA11] were stated only for fields of the form $\mathbb{F}_q$ and with the standard inner product $\langle , \rangle$ 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 $\langle , \rangle_h$. 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 $U_1 \subseteq U_1^\perp$. Assume further that $U_2 \subseteq U_1$ and let $D_i = C_{U_i}^\perp$, $i = 1, 2$ and 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, $k_1' = |U_1^\perp|$, $k_2' = |U_2^\perp|$ and $d_1 = \text{distance}(D_1)$, $d_2 = \text{distance}(D_2)$, then there exists a quantum stabilizer code with parameters $[[n, k_1'^\perp + k_2' - n, \min(d_1, d_2)]]_q$. Moreover, there exist toric residue codes $E_i$, $i = 1, 2$, so that $\text{distance}(E_i) \leq \text{distance}(D_i)$.

The above theorem makes intrinsic use of [KKKS] Lemma 20] which extends the well-known Calderbank-Shor-Steane construction to classical codes over finite fields of arbitrary characteristic. This theorem is discussed in section 5.

Here is an overview of the paper. We are aware that this paper would be of interest to two somewhat different groups: an important group would be mathematicians, especially pure mathematicians (for example, algebraic geometers) who are interested in applications to coding theory and cryptography: in fact we ourselves belong to this group. Another group would be scientists primarily interested in coding theory, especially from a point of view of quantum computing. It needs to be pointed out, the more
or less obvious fact, that since the perspectives of these two groups are widely different, so are their preferences and tastes. We have tried to organize the paper so that it would be of interest to both these groups. But while doing so, it is unavoidable that we need to present some material that may seem rather familiar to one of these groups. This may be particularly true of the introductory section 2, where 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, so that it becomes possible to define such objects for higher dimensional toric codes. In cyclic codes, i.e. involving only polynomials in one variable, the defining sets can simply be defined as the zero set of a generating polynomial. The extension of this to multicyclic codes is not automatic and in fact, the first step in being able to define subsystem toric and generalized toric codes was to provide an extension of this to higher dimensions and show that indeed our notion of defining sets for multicyclic codes specialize to the usual defining sets for cyclic codes.

Section 3 reviews quantum codes and subsystem codes and extends the construction of quantum stabilizer codes in [JA11] to finite fields of arbitrary characteristic. Following the suggestions from one of the referees, we have provided an expanded discussion on subsystem codes, especially since some of the literature on this important and rather recent development seems to be scattered among various Physics and EE journals.

Sections 4 and 5 discuss the main results 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 proceed to show that the techniques of [JA11] may be invoked to compute the distance of the dual of toric codes.

Section 6 is devoted to several examples as well as a comparison of the parameters of the codes considered in this paper with the parameters of several of the quantum codes available in the literature. The first example considers stabilizer and subsystem codes produced from the 2-dimensional projective space, while the second example considers similar codes produced from the 2-dimensional projective space with a single point blown-up. The third example considers stabilizer and subsystem codes produced from the projective toric variety corresponding to the Hirzebruch surface $F_2$. The fourth example considers similar codes produced from $\mathbb{P}^3$. As we increase the dimensions or consider varieties with points blown-up, the necessary computations become increasingly complicated so that it becomes necessary to make use of computer packages to perform the relevant calculations. One may see an example of this already in the last example, where it becomes advantageous to make use of calculations using the Macaulay2 package. Finally we also provide an elementary example where we use the ToricPackage in Sage to compute the minimum distance of the dual code.

We point out that the ability to start with higher dimensional toric varieties improves the good features of the quantum codes by comparing our codes, for example, with those quantum codes produced from classical Reed-Solomon codes. (One may observe that Reed-Solomon codes are in fact toric codes when the toric variety is one dimensional and hence $\mathbb{P}^1$.) We also provide a quick comparison with other quantum codes in the literature. The conclusions we seem to arrive are the following:
The quantum codes produced from toric varieties using the methods of this paper have high minimum distances in comparison with other code parameters. Since the minimum distances are computed using the methods of toric residue codes and using intersection theory, these distance computations are transparent and show that in fact, the minimum distance is directly proportional to the block-size, with the constant of proportionality being independent of the ground field. Consequently, as we vary over field extensions, we obtain particularly nice families of codes, with the ratios of minimum distance and dimension to the block size remaining bounded away from 0.

Arbitrarily large finite fields of arbitrary characteristic are allowed and the distance computations do not get complicated by doing so, since the complexity of the intersection theory methods increases only with respect to the dimension of the toric variety.

We also provide a comparison with several quantum codes produced by alternate methods and show that indeed the parameters of our codes compare favorably. See Table 6 for such a comparison.

Acknowledgments. The first author thanks both Andreas Klappenecker and Pradeep Sarvepalli for helpful discussions and sharing their insights on the construction of quantum codes. 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.

2. Toric and Generalized Toric evaluation codes as multicyclic codes

Let $\mathbb{F}_q$ denote a fixed finite field, where $q = p^m$ for some prime $p$. We start with cyclic codes over $\mathbb{F}_q$, which are well-known in coding theory: see, for example, [HP, Chapter 4]. The importance of toric and generalized toric codes may be clear when one realizes that cyclic codes include many well-known families of classical codes (see [HP, Chapter 4]), and 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 $\mathbb{F}_q^*$ denote a split $r$-dimensional torus over $k = \mathbb{F}$. Then the correspondence between rational convex polytopes in $\mathbb{R}^r$ 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 $M_\mathbb{R} = M \otimes \mathbb{Z} \mathbb{R}$. Let $P$ denote such a lattice polytope in $M_\mathbb{R}$ and let $X_P$ denote the associated projective toric variety together with the choice of an ample Cartier divisor $D_P$. Let $\mathcal{L}(D_P) = H^0(X_P, \mathcal{O}(D_P))$ denote the space of global sections of the line bundle $\mathcal{O}(D_P)$. If $K(X_P)$ denotes the set of rational functions of $X_P$, then one has an identification

$$H^0(X_P, \mathcal{O}(D_P)) \cong \{ f \in K(X_P)| \text{div}(f) + D_P \geq 0 \}.$$

By subdividing the corresponding fan if necessary, we will always assume that the toric variety $X_P$ is in fact smooth.

Now recall that the toric evaluation code $C_P$ is defined to be the image of the $\mathbb{F}_q$-linear map

$$ev : H^0(X, \mathcal{O}(D_P)) \rightarrow \mathbb{F}_q^n, \quad f \mapsto (f(t))_{t \in T}$$
i.e. one sends sections of the line bundle $\mathcal{O}(D_P)$ to their evaluations at the rational points of the dense torus $T$. Therefore, the code $C_P$ has length $n = (q - 1)^r = |T|$. Let $H = \{0, \ldots, q - 2\}^r$. 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 $((q - 1)\mathbb{Z})^r$. 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 [JJS].

Any subset $U \subseteq H$ defines what is called a generalized toric evaluation code as follows: let $\mathbb{F}_q[U]$ denote the $\mathbb{F}_q$-vector space with basis vectors $\{Y^u = \prod_{i=1}^r Y_i^{u_i} \mid u \in U\}$. Then one has a natural injective map

$$\text{ev} : \mathbb{F}_q[U] \to \mathbb{F}_q^n, \quad f \mapsto (f(t))_{t \in T},$$

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 $\mathbb{F}_q$-rational points on $T$, $k$ denotes the dimension of the $\mathbb{F}_q$-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 $T$ are given by $\{\alpha^i = (\alpha^{i_1}, \ldots, \alpha^{i_r})\}$, and their cardinality is $n = (q - 1)^r$. We will order such multi-exponents $\{i = (i_1, \ldots, i_r)\}$ by $\{i_0, \ldots, i_{n-1}\}$. The box $H$ also has $n = (q - 1)^r$ elements which we will order and enumerate as $\{u_0, \ldots, u_{n-1}\}$. We denote by

$$\sum_{\alpha < u,i> \in U}(\alpha < u,i>)$$

where $Y^u = Y_1^{u_1} \cdots Y_r^{u_r}$ is the monomial associated to each point $u = (u_1, \ldots, u_r) \in H$.

We next consider the isomorphism

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

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

$$\sum_{\alpha < u,i> \in U}(\alpha < u,i>) x^i,$$

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

A code $C \subseteq \mathbb{F}_q^n$ 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 $\mathbb{F}_q[x_1, \ldots, x_r]/(x_1^{q-1} - 1, \ldots, x_r^{q-1} - 1)$, and hence a generalized toric evaluation code $C_U$ is a multi-cyclic
code. To summarize the discussion above, we have isomorphisms
\[
F_q[H] \rightarrow \mathbb{F}_q^n \rightarrow \frac{\mathbb{F}_q[x_1, \ldots, x_r]}{(x_1^{q-1} - 1, \ldots, x_r^{q-1} - 1)}
\]
(2.1.3)
\[
Y^u \leftrightarrow (\alpha^{-u,1}_{i \in \{0, 1, \ldots, q-2\}^r} \mapsto \sum_{i \in \{0, 1, \ldots, q-2\}^r} \alpha^{-u,1} x_i^i,
F_q[U] \mapsto C_U \mapsto \phi(C_U).
\]

In [JAT11], it is also shown that instead of evaluating sections of a line bundle \( \mathcal{O}(D_P) \) at the \( k \)-rational points of the (split) torus \( T \), one may start with \( H^0(\mathcal{X}_P, \omega(D_P)) \), 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 [ST]) 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 \( F_q \) 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
\[
\mathbb{F}_q^n \rightarrow \mathbb{F}_q[x]/(x^n - 1), (c_0, \cdots, c_{n-1}) \mapsto \sum_{i=0}^{n-1} c_i x^i,
\]
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 \( F_q \) is the splitting field for the polynomial \( x^q - x \) over \( F_p \), and hence \( F_q^* \) may be identified with the set of roots of the polynomial \( f(x) := x^q - 1 \). Let \( H := \{0, 1, \ldots, q-2\} \) and let \( \alpha \) be a primitive generator of the multiplicative subgroup \( F_q^* := F_q \setminus \{0\} \), so that \( F_q^* = \{\alpha^i \mid i \in H\} \). 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
\[
D^- := \{ d \in H \mid d \equiv -d' \mod(q - 1) \text{ for some } d' \in D \}.
\]

Moreover, in this case we have the standard inner product on \( \mathbb{F}_q^n \), i.e. given by \( \langle u, v \rangle = (u_1, \cdots, u_n), v = (v_1, \cdots, v_n) \rangle = \sum_{i=0}^{n-1} u_i v_i \). This is often called the Euclidean case, largely to distinguish this from what is often called the Hermitian case, which we proceed to consider next.

Next we consider the case where the field \( F_q \) is replaced by \( F_{q^2} \). In this case, \( x \mapsto x^q \) is an involution of \( F_{q^2} \), so that we may define a new inner product on \( \mathbb{F}_{q^2}^n \) by \( \langle u, v \rangle = (u_1, \cdots, u_{2n}), v = (v_1, \cdots, v_{2n}) \rangle_h = \sum_{i=0}^{2n-1} u_i v_i \). In this case, observe that \( H = \{0, 1, \cdots, q^2 - 2\} \). For a subset \( D \subseteq H \), we define
\[
D^{-q} := \{ d \in H \mid d \equiv -qd' \mod(q^2 - 1) \text{ for some } d' \in D \}
\]
There exists a bijective correspondence between (principal) ideals in $\mathbb{F}_q[x]/(x^{q-1} - 1)$ and the monic polynomial factors of $(x^{q-1} - 1)$. 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 result is probably well-known, but due to lack of references, we present the details here. An additional reason for doing so is to provide a motivation for the definition of defining sets in higher dimensions that we give in the next section.

**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 $\mathbb{F}_q^2$, $e_a(\alpha^{ab}) = 0$ if and only if $a + qb \neq q^2 - 1$.

**Proof.** For any $a \in H$, note that $e_a(\beta) = 0$ if and only if $e(\alpha^a \beta) = 0$. Hence $\mathbb{F}_q$ is the splitting field of $e_a(x)$. Since

$$e(x) = \prod_{i \in H \setminus \{0\}} (x - \alpha^i),$$

this means that the roots of $e_a(x)$ are precisely the elements of the set $S_a := \{\alpha^{a+i} | 0 < i < q - 1\}$ in the Euclidean case and $S_a = \{\alpha^{-a+i} | 0 < i < q^2 - 1\}$ in the Hermitian case. However, since the roots of $e_a(x)$ are elements of $\mathbb{F}_q^*$ ($\mathbb{F}_q^2$), by using the identification $H \cong \mathbb{Z}/(q - 1)\mathbb{Z}$, we may rewrite $S_a = \{\alpha^b | b + a \neq 0 \mod(q - 1)\}$ in the Euclidean case and $S_a = \{\alpha^b | qb + a \neq 0 \mod(q^2 - 1)\}$ in the Hermitian case.

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

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

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

**Proof.** Let $U$ be any subset of $H$. Then the image $\text{ev}(\mathbb{F}_q[U]) = \phi(C_U)$ (see (21.31) for notation) is generated by the polynomials $e_a(x) = \phi(Y^a)$ for $a \in U$. The greatest common divisor of the polynomials $e_a(x)$, $a \in U$ is the generator of the ideal $\phi(C_U)$. From the Lemma above, $\alpha^b$ is a root of this generator if and only if $b + a \neq 0 \mod(q - 1)$ for each $a \in U$ which is to say that $b \in H \setminus U^\perp$.

Conversely, let $g(x)$ be a polynomial with roots $\alpha^a$ for $a \in D$ for some subset $D \subseteq H$, and set $U := H \setminus D^\perp$. Then from what we have just proved, the defining polynomial of the ideal $\phi(C_U)$ has roots in the set $H \setminus U^\perp$. We claim that

$$H \setminus U^\perp = D.$$ 

To see this, using the identification $H \cong \mathbb{Z}/(q - 1)\mathbb{Z}$, we note that $H = H^\perp$. Next, $H = U^\perp \bigsqcup (H \setminus U^\perp)$, and hence $H^\perp = (U^\perp)^{-1} \bigsqcup (H \setminus U^\perp)^{-1}$. Since $(U^\perp)^{-1} = U$ for any set $U \subseteq H$, we have $H = U \bigsqcup (H \setminus U^\perp)^{-1}$, and so $(H \setminus U^\perp)^{-1} = H \setminus U$. This implies $H \setminus U^\perp = (H \setminus U)^{-1} = (D^\perp)^{-1} = D$. 
These prove the statements with the standard inner product. For the Hermitian case, observe that the condition \( a + qb \neq q^2 - 1 \) is equivalent to \( qb \in H \setminus U^- \) which is equivalent to \( b \in q(H \setminus U^-) = H \setminus U^{-q} \).

2.3. Defining sets for higher dimensional multi-cyclic codes. Over the field \( \mathbb{F}_q \), we let \( H = \{0, 1, \cdots, q - 2\}^r \) and over \( \mathbb{F}_{q^2} \), we let \( H = \{0, 1, \cdots, q^2 - 2\}^r \) 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
\[
V^- := \{ v \in H | v \equiv -v' \mod ((q - 1)\mathbb{Z})^r \text{ for some } v' \in V \}.
\]
For a generalized toric code \( C_U \) defined by a subset \( U \subseteq H \), we define its defining set to be \( H \setminus U^- \). We denote this by \( D(C_U) \).

(ii) Over \( \mathbb{F}_{q^2} \), for a subset \( V \subseteq H \), we let
\[
V^{-q} := \{ v \in H | v \equiv -qv' \mod ((q^2 - 1)\mathbb{Z})^r \text{ for some } v' \in V \}.
\]
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 \( H \setminus V^- = (H \setminus V)^- \). 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 \( H = V^- \perp (H \setminus V^-) \), and so \( H^- = (V^-)^- \perp (H \setminus V^-)^- \). Hence, noting that \( H^- = H \), we have \( H = V \perp (H \setminus V^-)^- \), and thus \( H \setminus V^- = (H \setminus V)^- \).

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 \( U^\perp := H \setminus U^- = (H \setminus U)^- \), 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
\[
C^\perp := \{ v \in \mathbb{F}_q^n | <v, w> = 0 \ \forall \ w \in C \}.
\]
In the Hermitian case, (i.e. over \( \mathbb{F}_{q^2} \) with the inner product \( <, >_H \) on \( \mathbb{F}_{q^2}^n \)), 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
\[
C^{\perp_h} := \{ v \in \mathbb{F}_q^n | <v, w>_H = 0 \ \forall \ w \in C \}.
\]

**Remark.** For \( U \subseteq H = \{0, \cdots, q - 2\}^r \), \( C_{U^\perp} = C_U^\perp \) and for \( U \subseteq H = \{0, \cdots, q^2 - 2\}^r \), \( C_{U^{\perp_h}} = C_{U^\perp}^{\perp_h} \). (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 [Aly], 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 $D(C_{U_2}) \subseteq D(C_{U_1})$. In particular, $C_{U_1} = C_{U_2}$ if and only if $U_1 = U_2$.
(iv) $D(C_{U_1}) = U_1 = H \setminus D(C_{U_1})^{-}$.
(v) The corresponding statements also hold in the Hermitian case.

3. Quantum Stabilizer Codes andSubsystem Codes

Though quantum codes were constructed from classical codes originally only in the binary case, i.e. over fields of characteristic 2, the work of Klappenecker and his collaborators have extended these methods to other finite fields as well: see [KKKS], for example.

In view of this 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 $\mathcal{H} = \mathbb{C}^q$ or $\mathcal{H} = \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$. 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 $\mathcal{H} = (\mathbb{C}^q)^\otimes n$ is constructed in [KKKS] section 2 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 $\mathcal{E} = \{X(a)Z(b) | a, b \in \mathbb{F}_q\}$ 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 $\mathcal{E}$ is a scalar multiple of another matrix in $\mathcal{E}$, and
(c) $Tr(A^T B) = 0$ for distinct elements $A, B$ of $\mathcal{E}$.

Moreover $\mathcal{E}$ forms a basis for the set of all $q \times q$ matrices with $\mathbb{C}$-entries. For any $a = (a_1, \cdots, a_n) \in \mathbb{F}_q^n$, 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 $\mathcal{E}_n = \{X(a)Z(b) | a, b \in \mathbb{F}_q^n\}$ 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 $\mathcal{E}_n$. Then

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

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

$$(3.0.1) \quad Q = \bigcap_{E \in S} \{v \in \mathbb{C}^q \otimes n | Ev = v\}$$

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], [Pon], [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 $\mathcal{H} = (\mathbb{C}^q)^\otimes n$. 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 [Alv] Lemmas 2 and 3] will play an important role in this paper.

**Proposition 3.1.** (i) Let $C$ denote a $k'$ dimensional $\mathbb{F}_q$-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 $\mathbb{F}_{q^2}$-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 $[[n,n-(k'+k''),k'-k'',\text{wt}(D^{\perp_{h}}-C)]]_q$ 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. The results of this section may be viewed as higher dimensional extension of the results of [Alv] section 3] where he constructs sub-system codes from cyclic 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 $\mathbb{F}_q (\mathbb{F}_{q^2})$ to be self-orthogonal if $C \subseteq C^\perp (C \subseteq C^{\perp_{h}}$ respectively).
Proof of Theorems 1.1 and 1.2 The proof of the second theorem is nearly identical to the proof of the first, with $U \perp (T^-)$ replaced by $U \perp (T^- q)$, respectively. Therefore, we will discuss only the proof of the first theorem. Since $C_U$ is assumed to be self-orthogonal, $C_U \subseteq C_U^{\perp}$ and therefore, $D(C_U^{\perp}) \subseteq D(C_U)$. Therefore, using Lemma 2.6, 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 have

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

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

$$D(F^{\perp}) = D(C_U^{1}_{UT UT^-}) = (U \cup T \cup T^-) = D(C_U^{1}) \cup T \cup T^-.$$

Therefore, we have

$$D(F) \cup D(F^{\perp}) = (H \setminus (U^- \cup (T \cup T^-))) \cup (U \cup T \cup T^-) = (H \setminus U^-) \cup U = D(C_U) \cup D(C_U^{1}).$$

Since $D(C_U^{1}) \subseteq D(C_U)$, we have $D(F \cap F^{\perp}) = D(F) \cup D(F^{\perp}) = D(C_U)$. It follows, therefore, that $F \cap F^{\perp} = C_U$.

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

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

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 [JAI1].

**Proposition 4.1.** (i) Suppose the base field is $F_q$, $U \subseteq H = \{0, \cdots, q - 2\}^r \subseteq \mathbb{Z}^r$ and $v \in \mathbb{Z}^r$ so that the translate $U_1 = U + v \subseteq H$. Then both the codes $C_U^{1}$ and $C_{U_1}$ have the same code parameters.

(ii) Suppose the base field is $F_q^2$, $U \subseteq H = \{0, \cdots, q^2 - 2\}^r \subseteq \mathbb{Z}^r$ and $v \in \mathbb{Z}^r$ so that the translate $U_1 = U + v \subseteq H$. Then both the codes $C_U^{1h}$ and $C_{U_1}^{1h}$ 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 $\phi : \mathbb{F}_{q^2}^n \to \mathbb{F}_{q^2}^n$ defined by $u = (u_1, \ldots, u_n) \mapsto \overline{u} = (u_1^q, \ldots, u_n^q)$. The main observations then are the following:

If $V$ is an $\mathbb{F}_{q^2}$-linear subspace of $\mathbb{F}_{q^2}^n$, then $\phi(V)$ is also an $\mathbb{F}_{q^2}$-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 $\mathbb{F}_{q^2}^n$. Moreover, if $U_1 = U + v$, for some $v \in \mathbb{F}_{q^2}^n$, then $\phi(U_1) = \phi(U) + \phi(v) = \phi(U) + v$. 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 $\mathbb{F}_q$

Though a significant number of results in [JA11] extended to arbitrary finite characteristics, the construction of quantum stabilizer codes from toric evaluation codes had to be restricted to characteristic 2. There were two reasons for this: one was that the well-known CSS-construction was originally worked out only for such fields. The second was that in order to construct codes $C \subseteq C^\perp$ from toric codes, we made use of the toric residue theorem (i.e. [JA11, Theorems 4.1 and 4.3] as well as [JA11, Theorem 4.14]. The latter needed the assumption that the characteristic was indeed 2. Fortunately, using the method of generalized toric codes, it is now possible to construct codes $C \subseteq C^\perp$ directly without making use of the above theorems on toric residues.

The well-known CSS-construction of quantum-stabilizer codes from classical codes over fields of characteristic 2 was extended to fields of arbitrary finite characteristic $p$ in [KKKS, Lemma 20]. Therefore it is now possible to extend all the main results in [JA11] to arbitrary characteristics as follows.

**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 $C_U^\perp$ follows from [JA11, Corollary 4.11] as well as Proposition 4.11 since the polytopes $U_1$ are supposed to be the translates of polytopes satisfying the assumptions in [JA11].
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 $U_1 \subseteq U_1^+$ and $U_2 \subseteq (U_2)^+$ 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 discuss several examples mostly of smooth projective toric surfaces. We will assume that the cardinality of $k^*$ is $c$. (Since $k = \mathbb{F}_q$, this means $c = q - 1$. In view of the discussion above, $\mathbb{F}_q$ can be of arbitrary positive characteristic.) The rational points where we evaluate the sections of a line bundle will be the $k$-rational points on the dense torus, which will be always assumed to be split.

Let $\mathcal{M}$ denote the lattice of characters of the split torus $T = \mathbb{G}_m^n$. The correspondence between lattice polytopes (i.e. polytopes whose vertices are lattice points) in $\mathcal{M}$ of dimension $n$ 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. $n = r$ 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 $\mathbb{R}^3$ so that all coordinates of all its vertices are multiples of 2 are normal.) We will use the symbol $U$ for the lattice polytope in $\mathcal{M}$ from which we construct toric codes.

Recall from [KS] p. 2892] that for a subsystem code with parameters $[[n_q, k_Q, r_Q, d_Q]]_q$, the quantum singleton bound is given by

$$n_q - (k_Q + r_Q) + 2 \geq 2d_Q. \tag{6.0.1}$$

For the quantum subsystem code provided by Theorem [1.1] recall that $k_Q = n - 2k - r$, $r_Q = r$, $n_Q = n$, and $d_Q$ may be replaced by the minimum distance of the dual code $d = d_{c_U}$ 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 obtained by applying the CSS-code construction to two generalized toric codes as in Theorem [1.3] the corresponding quantum singleton bound (see [KKKS] §13]) is given by

$$n - (k'_1 + k'_2 - n) + 2 = 2n - (k'_1 + k'_2) + 2 \geq 2d_Q. \tag{6.0.2}$$

Recall that for the quantum stabilizer code provided by Theorem [1.3] $k'_1 = n - k_1$, $k'_2 = n - k_2$, where $k_i = \text{dim}(C_i)$, $i = 1, 2$ and $n_Q = n$. Therefore, the Quantum Singleton Bound, in this case becomes, $n - (n - k_1 + n - k_2 - n) + 2 = k_1 + k_2 + 2 \geq 2d$. Here we may replace $d_Q$ by the minimum distance of the dual codes $C_{U_i}$. Observe also that clearly we will need $k_i < n$ so that $k'_i > 0$, $i = 1, 2$.

An assumption we make in all the examples is that if $x_i$, $i = 1, \ldots, r$ denotes one of the coordinates of $\mathcal{M}$, then there exists one $i$ so that the $x_i$ - coordinates of all the vertices of $U \leq \frac{q^2 - 2}{2}$. In fact, then 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). The above assumption on the coordinates above will ensure that $U \subseteq U^\perp$, which is part of the hypotheses of both the theorems.

Let $H = \{0, \cdots, q - 2\}^r$. 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.) In the Hermitian case, one still needs the above conditions, which will ensure that there exists an $i$ so that $q(\text{the } x_i - \text{coordinates of all the vertices}) \leq \frac{q^2 - 2}{2}$. This will ensure $U \subseteq U^\perp$.) Observe that the first three examples consider toric surfaces starting with $\mathbb{P}^2$ and the last example considers $\mathbb{P}^3$.

Another aspect that is common to all the examples is the following. We will 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 will 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 $-U$. For the purposes of obtaining a code $C_U$ so that $C_U \subseteq C_U^\perp$ we will replace $U$ by its image in $H$. (Observe, as a result that $U^\perp$ is not a polytope.) For computing the minimum distance of the dual code, we will still work with the original polytope $C_U$.

Moreover, following the terminology and conventions adopted in [JA11, sections 3.3 and 3.4], the first $d$-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 $x_i$, $i = 1, \cdots, d$, with the remaining variables denoted $x_{d+1}, x_{d+2}, \text{etc.}$ The coordinates on the dense torus will be denoted $t_i$, $i = 1, \cdots, d$.

**Example 6.1.** $\mathbb{P}^2$ with a narrow polytope.

<table>
<thead>
<tr>
<th>Toric variety</th>
<th>Original Polytope (Vertices)</th>
<th>The polytope $U$ (Vertices)</th>
<th>The polytope $U^-$ (Vertices)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{P}^2$</td>
<td>$v'_0 = \begin{pmatrix} 0 \ 0 \end{pmatrix}$, $v'_1 = \begin{pmatrix} t \ 0 \end{pmatrix}$, $v'_2 = \begin{pmatrix} 0 \ s \end{pmatrix}$</td>
<td>$v_0 = \begin{pmatrix} 1 \ 1 \end{pmatrix}$, $v_1 = \begin{pmatrix} t + 1 \ 1 \end{pmatrix}$, $v_2 = \begin{pmatrix} 1 \ s + 1 \end{pmatrix}$</td>
<td>$v^-_0 = \begin{pmatrix} q - 2 \ q - 2 \end{pmatrix}$, $v^-_1 = \begin{pmatrix} q - 2 - t \ q - 2 \end{pmatrix}$, $v^-_2 = \begin{pmatrix} q - 2 \ q - 2 - s \end{pmatrix}$</td>
</tr>
</tbody>
</table>

We will let $t = \frac{5}{4}c$ and $s = \frac{1}{4}c$ so that $t = 5s$. In fact, by this choice of $s$, it is sufficiently smaller than $(q - 3)/2$ (for large enough $q$), and therefore, the difference $(H \setminus U^-) \setminus U$ has many lattice points. The image of $U$ in $H$ is a smaller trapezoid with two parallel sides orthogonal to the $x_1$-axis and positioned
with the vertices \( \mathbf{v}_i, i = 1, 3 \) as before, but where the long-side of the triangle along the x-axis has been chopped off a bit. Then we make use of Proposition 4.3. This shows that the hypotheses of Theorem 1.1 are indeed satisfied, with the above choice of \( U, s \) and \( t \). Observe that the corresponding divisor is:

\[
E' = tZ(x_3).
\]

The divisors \( D_i, D = D_1 + D_2, \) and the polytope corresponding to \( D + K - E \). In [JA1] Example 5.3, we chose the subsets \( J'_1 = k^* - \{ f_1 \} \) and \( J'_2 = k^* - \{ f_2 \} \). i.e. we removed the point \( t_1 = f_1 \) from the \( x_1 \)-axis and removed the single point \( t_2 = f_2 \) from the \( x_2 \)-axis. We will continue to do that here. Therefore we will let \( J'_i, i = 1, 2 \) be chosen as follows: \( J'_1 = k^* - \{ t_1 = f_1 \} \) and \( J'_2 = k^* - \{ t_2 = f_2 \} \),

\[
D_{J'_i} = \Sigma_{c \in J'_i} Z(x_1 - cx_3) \quad \text{and} \quad D_{J'_2} = \Sigma_{d \in J'_2} Z(x_2 - dx_3).
\]

We then let

\[
D_1 = D_{J'_1} + Z(x_2 - f_2 x_3) \quad \text{and} \quad D_2 = D_{J'_2}.
\]

We replace the divisor \( E' \) by the linearly equivalent divisor \( E = tZ(x_3 - x_1) \). Now as in op. cit. we see that the divisor \( D_1 + D_2 + K - E \) is then linearly equivalent to \( (c - 1)Z(x_1) + cZ(x_2) - Z(x_1) - Z(x_2) - Z(x_3) = (c - 2)Z(x_1) + (c - 1)Z(x_2) - (t + 1)Z(x_3) \).

Next we proceed to compute the support function associated to the divisor \( D_1 + D_2 + K - E = (c - 2)Z(x_1) + (c - 1)Z(x_2) - (t + 1)Z(x_3) \). This support function \( h \) (see [Oda, p. 72]) is given by \( h(\mathbf{u}_1) = -c + 2 \), \( h(\mathbf{u}_2) = -c + 1 \) and \( h(\mathbf{u}_3) = t + 1 \). It follows that the corresponding polytope is bounded by the faces which are the lines \( x_1 = -c + 2 \), \( x_2 = -c + 1 \) and \( -x_1 - tx_2 = t + 1 \); see figure below.

![Diagram](https://via.placeholder.com/150)

Minimum distance estimate for the dual code.

We first compute the intersection numbers \( Z(x_1) \bullet Z(x_1) = 1 \), \( Z(x_2) \bullet Z(x_2) = 1 \), \( Z(x_3) \bullet Z(x_3) = 1 \), \( Z(x_2) \bullet Z(x_1) = 1 \), \( Z(x_1) \bullet Z(x_3) = 1 \) and \( Z(x_2) \bullet Z(x_3) = 1 \). It follows that the conditions in \([7.1, 7.2, 7.22]\) are satisfied. Moreover, the intersection number \( (D_1 + D_2 + K - E) \bullet Z(x_2) = 2c - t - 4 = \frac{8}{4}c - 4 = \frac{3}{4}c - 4 \) by our choice of \( t = \frac{3}{4}c \). Therefore, we may apply Corollary \([7.22]\) to estimate the minimum distance of \( C_U^\perp \).

Next suppose that the residue function in Definition 7.3 vanished identically on \( \ell \) curves of the form \( Z(x_2 - a(j)x_3) \), for \( j = 1, \cdots, \ell \), then the polytope corresponding to \( D_1 + D_2 + K - E - \ell Z(x_2) \) has its bottom face moved from \( x_2 = -c + 1 \) to \( x_2 = -c + 1 + \ell \). Since the global sections of this line bundle is
non-empty, it follows that \(-c + 1 + \ell \leq \frac{c-3}{5}\), and hence that

\[(6.0.5)\]

\[\ell \leq c + \frac{c-t}{5} - \frac{3}{5} - 1 = c(1 - \frac{1}{4*5}) - \frac{3}{5} - 1.\]

Observe that we may now determine the following parameters of the code as follows. First \(n = (c - 1)(c - 1) = c^2 - 2c + 1\) since we removed one point each from the \(x_1\)-axis and 1 point from the \(x_2\)-axis. Observing that each of the \(\ell\) curves above have at most \(c\) \(k\)-rational points where the residue is computed, and \(t = \frac{4}{5}c\), we obtain the estimate:

\[(6.0.6)\]

\[\text{dist}(C_U^\perp) \geq (c^2 - 2c + 1) - (\ell * c) - (\frac{3}{4}c - 4)(c - \ell)\]

\[= (c^2 - 2c + 1) - \ell * c - \frac{3}{4}c^2 + \frac{3}{4}\ell * c - 4 * \ell = \frac{1}{4}c^2 - \frac{1}{4}(c * \ell) - 2c + 1 - 4 * \ell\]

\[\geq \frac{1}{4}c^2 + \frac{1}{4}c * (-c(1 - \frac{1}{4*5}) + \frac{3}{5} + 1) - 2c + 1 - 4 * \ell\]

\[= \frac{1}{4}c^2 - \frac{1}{4}c^2 + \frac{1}{16*5}c^3 + \frac{3c}{4*5} + \frac{c}{4} - 2c + 1 - 4 * \ell\]

\[\geq \frac{1}{16*5}c^2 + c(-2 + \frac{3}{4*5} + \frac{4}{5} - \frac{16}{5} - 4 + 1) = \frac{1}{16*5}c^2 + c(-\frac{23}{4} + \frac{7}{4*5}) - \frac{16}{5} - 3.\]

Clearly we may approximate this by \(\frac{1}{16*5}c^2\) ignoring lower order terms in \(c\).

**Dimension of the code.** Next, one may compute the dimension of the code \(C_U\) to be given by the area of the corresponding polytope which lies in the box \(H\). Once may observe that the rectangular box of height \(x_2 = (t - c + 1)/r\) and length \(c - 1\) lies in the given triangle and also in \(H\), so that we use the area of this box as a lower bound for the dimension of the code \(C_U\): this works out, therefore to be \((\frac{4}{5}c + 1)/5 * (c - 1)\) which is approximated by \(\frac{1}{5}c^2\) (ignoring the lower order terms). Thus

\[(6.0.7)\]

\[k \geq \frac{1}{4*5}c^2.\]

**Parameters of the corresponding subsystem code provided by Theorem** \(1.1\)

\[(6.0.8)\]

\[n_Q = n = c^2, \quad \text{dim}(C_U) = k \geq \frac{1}{4*5}c^2, \quad r < c^2 - 2(\frac{1}{4*5}c^2) = \frac{2*5 - 1}{2*5}c^2\] and \(d \geq \text{distance}(C_U^\perp) \geq \frac{1}{16*5}c^2\).

We will choose \(r \leq \frac{1}{4*5}c^2\), so that \(kQ \geq c^2 - \frac{2}{4*5}c^2 - \frac{1}{4*5}c^2 = c^2(1 - \frac{3}{4*5})\). Now to check the Quantum Singleton Bound, it suffices to check if \(k \geq d\). But \(k = \frac{1}{4*5}c^2\) and \(d = \frac{1}{16*5}c^2\) (ignoring lower order terms in \(c\)) so that, \(k > d\).

**Parameters of the corresponding quantum stabilizer code provided by Theorem** \(1.1\) Next we consider the quantum stabilizer code provided by the CSS-construction in Theorem \(1.3\). For this we will let \(E = tZ(x_3 - x_1), \quad F = t'Z(x_3 - x_1)\), with \(0 < t' \leq t\). Therefore, \(F < E\). We will translate the original polytope corresponding to \(F\) and \(E\) so that the origin is shifted to \(v_1\). Let \(U_2\) (\(U_1\)) denote the polytopes corresponding to \(F\) (\(E\), respectively). Clearly \(U_2 \subseteq U_1\) and therefore if \(D_1 = C_U^\perp, \quad D_2 = C_{U_2}^\perp\), then \(D_2 \supseteq D_1 \supseteq D_1^\perp\). Taking \(t' = t\),
We consider a projective space of dimension 2 with a point blown up as follows.

Example 6.2. We consider a projective space of dimension 2 with a point blown up as follows.

\[ \text{Example 6.2} \]

We consider a projective space of dimension 2 with a point blown up as follows. We had chosen the subsets \( J'_1 = k^* - \{ f_1, 1 \} \) and \( J'_2 = k^* - \{ t_2, f_2 \} \). i.e. we had removed two points \( t_1 = f_1 \) and \( t_1 = 1 \) from the \( t_1 \)-axis and removed the single point \( t_2 = f_2 \) from the \( t_2 \)-axis. We will continue to do that here. Therefore we will let \( J'_i, i = 1, 2 \) be chosen as follows: \( J'_1 = k^* - \{ t_1 = f_1, 1 \} \) and \( J'_2 = k^* - \{ t_2 = f_2 \} \), so that \( D_1 = D_{J'_1} + D_{2,f_2} \) and \( D_2 = D_{1,f_1} + D_{J'_2} \). We choose the divisor \( E = tZ(x_3 - x_1) + sZ(x_4) \). Now as in [JAA1-5.3], we see that the divisor \( D_1 + D_2 + K - E \) is then linearly equivalent to \((c - 2)Z(x_1) + (c - 1)Z(x_2) - Z(x_1) - Z(x_2) - Z(x_3) - Z(x_4) - tZ(x_3) - sZ(x_4)\).

Next we proceed to compute the support function associated to the divisor \( D_1 + D_2 + K - E = (c - 3)Z(x_1) + (c - 2)Z(x_2) - (t + 1)Z(x_3) - (s + 1).Z(x_4) \). This support function \( h \) (see [Oda p. 72]) is given by \( h(u_1) = -c + 3, h(u_2) = -c + 2, h(u_3) = t + 1 \), and \( h(u_4) = s + 1 \). It follows that the corresponding polytope is bounded by the faces which are the lines \( x_1 = -c+3, x_2 = -c+2, x_2 = -s-1, \) and \( -x_1 - x_2 = t + 1 \): see figure below.
Minimum distance estimate for the dual code. Now one may compute the intersection numbers
\(Z(x_1) \cdot Z(x_1) = 0, Z(x_2) \cdot Z(x_1) = 1, Z(x_1) \cdot Z(x_4) = 1, Z(x_1) \cdot Z(x_3) = 0, Z(x_2) \cdot Z(x_2) = 1, Z(x_3) \cdot Z(x_2) = 1, Z(x_4) \cdot Z(x_3) = 0, Z(x_4) \cdot Z(x_3) = 1\) and \(Z(x_4) \cdot Z(x_4) = -1\).

It follows that the conditions in 7.1, 7.2 and (7.2.2) are satisfied. Moreover, the intersection number
\((6.0.12)\)

Next suppose that the residue function in Definition 7.4 vanished identically on \(\ell\) curves of the form
\(Z(x_1 - a(x_3))\), for \(j = 1, \cdots, \ell\), then the polytope corresponding to the line bundle corresponding to
\(D_1 + D_2 + K - E\) \(\cdot Z(x_1) = c - 1 - s = \frac{3}{4}c - 1\) by our choice of \(s = \frac{1}{4}c\). Therefore, we may apply Corollary 7.7 to estimate the minimum distance of \(C_U^\perp\).

Observe that we may now determine the following parameters of the code as follows. First \(n = (c - 2)(c - 1) = c^2 - 3c + 2\) since we removed two points from the \(x_1\)-axis and 1 point from the \(x_2\)-axis. Observing that each of the \(\ell\) curves above have at most \(c\) \(k\)-rational points where the residue is computed, and \(t = \frac{12}{10}c\), we obtain the estimate
\((6.0.10)\)

\[\text{dist}(C_U^\perp) \geq (c^2 - 3c + 2) - (\ell * c) - \left(\frac{3}{4}c - 1\right) * (c - \ell)\]

\[= (c^2 - 3c + 2) - \ell * c - \frac{3}{4}c^2 + \frac{3}{4}\ell * c + (c - \ell)\]

\[= \frac{1}{4}c^2 + \frac{1}{4}c * (-\ell) - 2c - \ell + 2 \geq \frac{1}{4}c^2 + \frac{1}{4}c * (-2c + t + 6) - 2c - \ell + 2\]

\[\geq \frac{1}{4}c^2 + \frac{1}{4}c * (-\frac{8}{10}c + 6) - 2c - 2c + t + 6 + 2 = \frac{1}{4}c^2 - \frac{2}{10}c^2 + \frac{6}{4}c - 4c + \frac{12}{10}c + 6 + 2\]

\[= \frac{1}{20}c^2 - \frac{26}{20}c + 6 + 2.\]

Dimension of the code \(C_U\). Next, one may compute the dimension of the code \(C_U\) to be given by the area of the corresponding polytope which lies in the box \(H\). One may observe that \(t - s = \frac{12}{10}c - \frac{1}{4}c = \frac{19}{20}c\), so that the part of the polytope \(U\) that lies in \(H\) contains a rectangle of sides \(\frac{19}{20}c\) and \(\frac{1}{4}c\). Thus
\((6.0.12)\)

\[k \geq \frac{19}{80}c^2.\]
Parameters of the subsystem code provided by Theorem 1.1 as:

\[ n_Q = n = c^2, \ dim(C_U) = k \geq \frac{19}{80} c^2, \ r < c^2 - 2\left(\frac{19}{80} c^2\right) = \frac{42}{80} c^2 \text{ and } d \geq \text{distance}(C_U^⊥) \geq \frac{1}{20} c^2 - \frac{52}{40} c + 8. \]

We will choose \( r \leq \frac{19}{80} c^2 \), so that \( k_Q \geq c^2 - \frac{38}{80} c^2 - \frac{19}{80} c^2 = \frac{33}{80} c^2 \). Since \( k = \frac{19}{80} c^2 \) and \( d = \frac{1}{20} c^2 \) (ignoring lower order terms in \( c \)), \( k > d \) which proves the quantum singleton bound.

Parameters of the quantum stabilizer code provided by the CSS-construction in Theorem 1.3. For this we will let \( E = tZ(x_3 - x_1) + sZ(x_4), \ F = t'Z(x_3 - x_1) + s'Z(x_4) \), with \( 0 < t' \leq t \) and \( 0 < s' \leq s \). Therefore, \( F < E \). We will translate the original polytope corresponding to \( E \) and \( E' \) so that the origin is shifted to \( v_1 \). Let \( U_2 (U_1) \) denote the polytopes corresponding to \( E \) (\( E' \), respectively). Clearly \( U_2 \subseteq U_1 \) and therefore if \( D_1 = C_{U_1}^⊥, \ D_2 = C_{U_2}^⊥ \), then \( D_2 \supseteq D_1 \supseteq D_1^⊥ \). Taking \( s' = s \) and \( t' = t \),

\[ n_Q = n = c^2, \ k_1 = dim(C_{U_1}) = \frac{19}{80} c^2, \ k_2 = dim(C_{U_2}) = \frac{19}{80} c^2. \]

Therefore for the parameters of the quantum stabilizer code provided by Theorem 1.3, observe that \( n = c^2, \ k_Q = (n - k_1) + (n - k_2) = n - k_1 - k_2 \) and we need this to be positive. This is clear since, by our choice, \( k_1 = k_2 \) and we already verified that \( 2dim(C_U) < n \). Therefore in this case \( k_Q = c^2 - \frac{38}{80} c^2 = \frac{42}{80} c^2 \). Moreover the Quantum Singleton Bound, in this case becomes \( k_1 + k_2 + 2 = 2k + 2 \geq 2d \), which we already verified in the case of the corresponding subsystem code.

**Example 6.3.** Next we begin with \( \mathbb{P}_2(1,1,2) \), a weighted projective space of dimension 2 where the weights are \((1,1,2)\). This is a toric variety with one singular point; its fan is given by \( e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \) and \( e_3 = -e_1 - 2e_2 \). On resolving the singularity by blowing up the singular point, the resulting non-singular variety is precisely the Hirzebruch surface \( F_2 \), that is, the total space of the \( \mathcal{O}_{\mathbb{P}^1}(-2) \)-bundle over \( \mathbb{P}^1 \). This is the variety we consider in this example.

**Table 3.** Details on the Toric Variety and the Polytope

<table>
<thead>
<tr>
<th>Toric variety</th>
<th>Original Polytope (Vertices)</th>
<th>The polytope ( U ) (Vertices)</th>
<th>The polytope ( U^− ) (Vertices)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( F_2 )</td>
<td>( v_0 = \begin{pmatrix} 0 \ 0 \end{pmatrix}, \ v_1 = \begin{pmatrix} 2t \ 0 \end{pmatrix}, \ v_2 = \begin{pmatrix} 2t - 2s \ s \end{pmatrix}, \ v_3 = \begin{pmatrix} 0 \ s \end{pmatrix} )</td>
<td>( v_0 = \begin{pmatrix} 1 \ 1 \end{pmatrix}, \ v_1 = \begin{pmatrix} 2t + 1 \ 1 \end{pmatrix}, \ v_2 = \begin{pmatrix} 2t - 2s + 1 \ s + 1 \end{pmatrix}, \ v_3 = \begin{pmatrix} 1 \ s + 1 \end{pmatrix} )</td>
<td>( v_0 = \begin{pmatrix} q - 2 \ q - 2 \end{pmatrix}, \ v_1 = \begin{pmatrix} q - 2 - 2t \end{pmatrix}, \ v_2 = \begin{pmatrix} q - 2 \end{pmatrix}, \ v_3 = \begin{pmatrix} q - 2 - 2t + 2s \ q - 2 - s \end{pmatrix} )</td>
</tr>
</tbody>
</table>

Here we will let \( t = \frac{11}{10} c \) and \( s = \frac{1}{5} c \). In fact, by this choice of \( s \), it is sufficiently smaller than \((q - 3)/2 \) (for large enough \( q \)), and therefore, the difference \((H \setminus U^-) \setminus U \) has many lattice points. As in the last
example, we will replace U by its image in H: this may be taken to be a rectangle of sides $\frac{1}{4}c$ and $c - 1$ positioned with the vertices $v_i$, $i = 1, 3, 4$ as before. Then we make use of Proposition 4.1. This shows that the hypotheses of Theorem 4.1 are indeed satisfied, with the above choice of U, s and t. Observe that the polytope above corresponds to the divisor $E' = 2tZ(x3) + sZ(x4)$.

The divisor $D_i$, $D$, $D + K - E$ and the minimum distance of the dual code. We choose the divisors $D_1$ and $D_2$ as in the last example. Now as in [4.11 Example 5.3], we see that the divisor $D_1 + D_2 + K - E$ is then linearly equivalent to $(c - 2)Z(x_1) + (c - 1)Z(x_2) - Z(x_1) - Z(x_2) - Z(x_3) - Z(x_4) - (2t + 1)Z(x_3) - (s + 1)Z(x_4)$.

Now one may compute the intersection numbers $Z(x_1) \cdot Z(x_1) = 0$, $Z(x_2) \cdot Z(x_1) = 1$, $Z(x_1) \cdot Z(x_4) = 1$, $Z(x_1) \cdot Z(x_3) = 0$, $Z(x_2) \cdot Z(x_2) = 2$, $Z(x_3) \cdot Z(x_2) = 1$, $Z(x_4) \cdot Z(x_2) = 0$, $Z(x_3) \cdot Z(x_3) = 0$, $Z(x_4) \cdot Z(x_3) = 1$, and $Z(x_4) \cdot Z(x_4) = -2$. One may show using these computations that the hypotheses in [4.11, 4.2] and [4.2.2] are satisfied. Moreover the intersection number $(D_1 + D_2 + K - E) \cdot Z(x_1) = c - 1 - (s + 1) = c - s - 2 = \frac{3}{4}c - 2$ by our choice of $s = \frac{1}{4}c$. Therefore, we may again apply Corollary 4.7 to estimate the minimum distance of $C^\perp_U$.

Next we proceed to compute the support function associated with the divisor $D_1 + D_2 + K - E = (c - 3)Z(x_1) + (c - 2)Z(x_2) - (2t + 1)Z(x_3) - (s + 1).Z(x_4)$. This support function $h$ (see [Oda, p. 72]) is given by $h(u_1) = -c + 3$, $h(u_2) = -c + 2$, $h(u_3) = 2t + 1$, and $h(u_4) = s + 1$. Therefore, the corresponding polytope has as faces, the lines $x_1 = -c + 3$, $x_2 = -c + 2$, $x_2 = -s - 1$, and $-x_1 - 2x_2 = 2t + 1$.

Next suppose there are $\ell$ ($0 \leq \ell \leq c$) curves $Z(x_1 - a_1(j)x_3)$, $j = 1, \ldots, \ell$ (with $a_i(j) \in k$) so that a nonzero rational function $f \in \Gamma(X, O_X(D + K' - E))$ vanishes identically on these curves. i.e.

$$\text{div}(f)_0 - Z(x_1 - a_1(j)x_3) \geq 0$$

for all $j = 1, \ldots, \ell$. An argument as in the last example will show that $-c + \ell + 3 \leq 2c - 2t + 5$, and hence that

$$\ell \leq 3c - 2t - 8.$$ 

Therefore, the number of zeroes of $f$ is bounded above by $\ell \ast c \leq 3c^2 - 2tc = 3c^2 - (\frac{22}{10})c^2$. Therefore, we may compute the parameters of the code $C = C(X, \mathcal{L}, \mathcal{P})^\perp$ as follows. First $n = c^2$ and

$$\text{dist}(\mathcal{C}_U^\perp) \geq (c^2 - 3c + 2) - \ell \ast c - \frac{3}{4}(c - \ell) = c^2 - 3c + 2 - \ell \ast c - \frac{3}{4}c^2 + \frac{3}{4} \ell \ast c + 2(c - \ell)$$

$$= \frac{1}{4}c^2 + \frac{1}{4}c \ast (-\ell) - 3c + 2 + 2 \ast \left(\frac{2}{10}c + 8\right) \geq \frac{1}{4}c^2 + \frac{1}{4}c \ast (-\frac{8}{10}c + 8) - 3c + \frac{4}{10}c + 18$$

$$= \frac{1}{4}c^2 - \frac{2}{10}c^2 - c + \frac{4}{10}c + 18 = \frac{1}{20}c^2 - c + \frac{4}{10}c + 8 = \frac{1}{20}c^2 - \frac{6}{10}c + 8.$$ 

Dimension of the code $C_U$. Next, one may compute the dimension of the code $C_U$ to be given by the area of the part of polytope $U$ that lies in the box $H$. Since $2t - 2s = \frac{22}{10}c - \frac{1}{2}c = \frac{17}{10}c > c$, it follows that this area is the area of a rectangle with sides $c$ and $\frac{1}{4}c$. Therefore,

$$k = \frac{1}{4}c^2.$$
The parameters of the subsystem code provided by Theorem 1.1 are:

\[(6.0.19)\]

\[n_Q = n = c^2, \quad \text{dim}(C_U) = k = \frac{1}{4}c^2, \quad r < c^2 - 2\left(\frac{1}{4}\right)c^2 = \frac{1}{2}c^2 \text{ and } d \geq \text{distance}(C_U^1) \geq \frac{1}{20}c^2 - \frac{6}{10}c + 18.\]

We will let \(r \leq \frac{1}{4}c^2\), so that \(k_Q \geq c^2 - \frac{1}{2}c^2 - \frac{1}{4}c^2 = \frac{1}{4}c^2\). Since \(k = \frac{1}{4}c^2\) and \(d = \frac{1}{20}c^2\) (ignoring lower order terms in \(c\)), \(k > d\) proving the Quantum Singleton Bound.

**Example 6.4.** Here we consider the 3-dimensional example of \(\mathbb{P}^3\) already verified in the case of the corresponding subsystem code.

We will let \(k_1 = k_2\) and \(d = \frac{1}{20}c^2\) so that \(\text{dim}(C_U) \geq k_1 + k_2 + 2 = 2k + 2 \geq 2d\), which we already verified in the case of the corresponding subsystem code.

Therefore for the parameters of the quantum stabilizer code provided by Theorem 1.3 observe that \(\text{dim}(C_U) < n\). Therefore in this case \(k_Q = c^2 - \frac{1}{2}c^2 = \frac{1}{4}c^2\).

Moreover the Quantum Singleton Bound, in this case becomes \(k_1 + k_2 + 2 = 2k + 2 \geq 2d\), which we already verified in the case of the corresponding subsystem code.

**Example 6.4.** Here we consider the 3-dimensional example of \(\mathbb{P}^3\) provided by the following polytope.

**Table 4.** Details on the Toric Variety and the Polytope

<table>
<thead>
<tr>
<th>Toric variety</th>
<th>Original Polytope (Vertices)</th>
<th>The polytope (\mathbb{P}^3) (Vertices)</th>
<th>The polytope (\mathbb{P}^3) (Vertices)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\mathbb{P}^3)</td>
<td>(v'_0 = \begin{pmatrix} 0 \ 0 \ 0 \end{pmatrix})</td>
<td>(v_0 = \begin{pmatrix} 1 \ 1 \ 0 \end{pmatrix})</td>
<td>(v_0^- = \begin{pmatrix} q - 2 \ q - 2 \ q - 2 \end{pmatrix})</td>
</tr>
<tr>
<td>(v'_1 = \begin{pmatrix} t \ 0 \ 0 \end{pmatrix})</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></td>
</tr>
<tr>
<td>(v'_2 = \begin{pmatrix} 0 \ t \ 0 \end{pmatrix}) and</td>
<td>(v_2 = \begin{pmatrix} 1 \ t + 1 \ 1 \end{pmatrix}) and</td>
<td>(v_2^- = \begin{pmatrix} q - 2 \ q - 2 \ q - 2 \end{pmatrix}) and</td>
<td></td>
</tr>
<tr>
<td>(v'_3 = \begin{pmatrix} 0 \ 0 \ s \end{pmatrix})</td>
<td>(v_3 = \begin{pmatrix} 1 \ 1 \ s + 1 \end{pmatrix})</td>
<td>(v_3^- = \begin{pmatrix} q - 2 \ q - 2 \ q - 2 - s \end{pmatrix})</td>
<td></td>
</tr>
</tbody>
</table>

Here we will let \(t = \frac{10}{q}c\) and \(s = \frac{1}{c}c\) so that \(t = 10s\). In fact, by this choice of \(s\), it is sufficiently smaller than \((q - 3)/2\) (for large enough \(q\)), and therefore, the difference \((H \setminus U^-) \setminus U\) has many lattice points. For the purposes of obtaining a code \(C_U\) so that \(C_U \subseteq C_U^1\) we will replace \(U\) by its image in \(H\): see
the discussion in 6.1. below. Then we make use of Proposition 4.1. This shows that the hypotheses of Theorem 1.1 are indeed satisfied, with the above choice of $U$, $s$ and $t$.

The variables $x_i$ provide the homogeneous coordinates for $\mathbb{P}^3$ and generate the Cox-ring. Let $T = G_m^3$ 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

$$E' = tZ(x_4)$$

(6.0.21)

denotes the divisor on $\mathbb{P}^3$ corresponding to the given polytope, where $Z(x_i)$ denotes the toric divisor where the homogeneous coordinate $x_i = 0$. We will replace $E'$ by the linearly equivalent divisor $E = tZ(x_4 - x_1)$.

Now we choose the divisors as follows. Let $f_i, i = 0, 1, 2$ denote a chosen element in $\mathbb{F}_q^*$. Let $J'_i = \mathbb{F}_{q^*} - \{f_i\}$, for each $i = 1, 2, 3$.

$$D_1 = \sum_{e \in J'_1} Z(x_1 - ex_4) + Z(x_2 - f_2x_4) + Z(x_3 - f_3x_4),$$
$$D_2 = \sum_{d \in J'_2} Z(x_2 - dx_4)$$
$$D_3 = \sum_{e \in J'_3} Z(x_3 - ex_4).$$

Lemma 6.5. (i) $\cap_{i=0}^2 |D_i| - \{[1 : 0 : 0 : 0], [0 : x_2 : x_3 : x_4], \text{each } x_i \neq 0\} \subseteq \text{the dense torus } G_m^3$. (ii) $\cap_{i=0}^2 |D_i| \cap |E|$ 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 $E = Z(x_4 - x_1)$.

6.1. Dimension of the code $C_U$. Observe that inclined face of the polytope has the equation $x_1 + x_2 + 10x_3 = t$. Therefore, the cylinder whose base is a right triangle of sides each $c - 1$ along the $x_1$ and $x_2$ axes and of height $x_3 = \frac{t-(c-1)}{10}$ lies entirely inside the above polytope and also in the box $H$. Therefore a lower bound for the dimension of the code $C_U$ is given by the volume of the above cylinder, which is $\frac{(c-1)^2}{2} \times \frac{t-(c-1)}{10}$. Since $t = \frac{10}{4}$, therefore a lower bound for the dimension of the code $C_U$ is given by

$$k = \text{dim}(C_U) \geq \frac{(c-1)^2}{2} \times \frac{6}{4 \times 10} c.$$ 

(6.1.1)

Ignoring the lower order terms, this becomes $\frac{3}{40} c^3$. We will let

$$P = \cap_{i=0}^2 |D_i|$$

denote the set of rational points where we evaluate sections of line bundles or take residues of differential forms.
6.2. Let $s_0 = \frac{(x_3 - f_3 x_2)}{(x_4 - x_1)}$; 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 $\cap_{i=0}^3 D_i$.

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 $(X, O_X(E))$, except that the bottom face is at $x_3 = -c + 1$, with the two bottom vertices will be $\begin{pmatrix} (10 + 1)c - t - 10 - 2 \\ -c + 1 \\ -c + 1 \end{pmatrix}$ 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 $x_1 + x_2 + 10x_3 = -t - 1$. 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 $x_1 + x_2 + 10x_3 = -t - 1$, shows that the top vertex of the polytope $U$ is given by $(-c + 2, -c + 1, \frac{2c - t - 4}{10})$.

**Estimating the minimum distance of the code.** Next let $s \in \mathbb{F}_q^*$ be fixed element, and suppose a global section $f \in \Gamma(X, O_X(D + K - E))$ vanishes identically on $\ell_s$ lines of the form $L_j : Z(x_3 - a(j)x_4) \cap Z(x_2 - s x_1)$, $j = 1 \cdots, \ell_s$. Observe that the equation $Z(x_2 - s x_1)$ defines a hyperplane $\mathcal{H}_s \subseteq \mathbb{P}^3$, i.e. a closed subvariety isomorphic to a $\mathbb{P}^2$. The polytope that corresponds to this hyperplane $\mathcal{H}_s$ and the restriction of the line bundle $O_{\mathbb{P}^3}(D_1 + D_2 + D_3 + K - E)$ to $\mathcal{H}_s$ is the triangle obtained by intersecting the polytope $U$ in the plane defined by $x_2 = s x_1$. (In fact, if $M_{\mathcal{H}_s}$ denotes the character lattice for the maximal torus in $\mathcal{H}_s$, the above triangle lives in the vector space $M_{\mathcal{H}_s} \otimes \mathbb{R}$.) One may verify readily that each of these triangles satisfies the hypotheses on the triangle used in the very first example of $\mathbb{P}^2$. Therefore, one obtains the equation

\begin{equation}
-c + 1 + \ell_s \leq \frac{2c - t - 4}{10} \text{ or equivalently } \ell_s \leq c(1 + \frac{2}{10}) - 1 - \frac{t}{10} - \frac{4}{10}.
\end{equation}

Now varying the $s \in \mathbb{F}_q^*$, we see that

\begin{equation}
\ell = \sum_{s \in \mathbb{F}_q^*} \ell_s \leq c^2(1 + \frac{2}{10}) - c(1 + \frac{t}{10} + \frac{4}{10})
\end{equation}

\begin{equation}
= c^2(1 + \frac{2}{10} - \frac{t_1}{10}) - c(1 + \frac{4}{10}), \text{ with } t = t_1 c.
\end{equation}

Since $D_1 + D_2 + K - E$ is linearly equivalent to $(c - 2)Z(x_1) + (c - 1)Z(x_2) + (c - 1)Z(x_3) - (t + 1)Z(x_4)$, and $Z(x_2 - sx_1)$ is linearly equivalent to $Z(x_2)$ while $Z(x_3 - a(j)x_4)$ is linearly equivalent to $Z(x_3)$, one may compute the intersection number:

\begin{equation}
(D_1 + D_2 + D_3 + K - E) \cap Z(x_2 - s x_1) \cap Z(x_3 - a(j)x_0) = 3c - t - 5
\end{equation}

Here we are using the observation that all the intersection numbers between the toric divisors for $\mathbb{P}^3$ are all 1, which may be verified readily using a calculation using our functions (see [JTS] supplementing those in [Mac2] NormalToricVarieties].
Therefore, with \( t = t_1c \) and \( t_1 = \frac{5}{2} \), the minimum distance of the code \( C_U^1 \) is given by

\[
\text{dist}(C_U^1) \geq (c - 1)^2(c - 2) - \ell * c - (\Sigma_j(D + K - E)).(Z(x_3 - a(j)x_0) \cap Z(x_1 - b(j)x_3))
\]

\[
= c^3 - 4c^2 + 5c - 2 - \ell * c - (3c - t - 5) * (c^2 - \ell)
\]

\[
= c^3 - 4c^2 + 5c - 2 - \ell * c - (c(3 - t_1) - 5) * (c^2 - \ell)
\]

\[
= c^3 - \ell * c - (3 - t_1)c^3 + (3 - t_1)\ell * c - 4c^2 + 5c - 2 + 5 * (c^2 - \ell)
\]

\[
= c^3 - \ell * c - 3c^3 + t_1c^3 + 3\ell * c - t_1\ell * c - 4c^2 + 5c - 2 + 5c^2 - 5\ell
\]

\[
= c^3 - 3c^3 + \frac{5}{2}c^3 + 3\ell * c - \ell * c + \frac{5}{2}\ell * c - 4c^2 + 5c - 2 + 5c^2 - 5\ell
\]

\[
= \frac{1}{2}c^3 - \frac{1}{2}\ell * c \geq \frac{1}{2}c^3 - \frac{1}{2}(1 - \frac{1}{2*10})c^3 = \frac{1}{4*10}c^3, \text{ ignoring lower order terms.}
\]

Now we proceed to compute the parameters of the subsystem code provided by Theorem 1.1 (ignoring the lower order terms).

\[
n_Q = n = c^3, \quad \dim(C_U) = k = \frac{3}{4 * 10}c^3, \quad r < c^3 - 2(\frac{3}{4 * 10})c^3 = (1 - \frac{3}{2 * 10})c^3 \quad \text{and} \quad d_Q \geq \text{distance}(C_U^1) \geq \frac{1}{4 * 10}c^3.
\]

We will choose \( r = \frac{1}{2}(1 - \frac{3}{2*10})c^3 \), so that \( k_Q = n - 2k - r = \frac{1}{2}c^3 - \frac{3}{4*10}c^3 \).

To obtain the parameters of the quantum code provided by the CSS construction, we take the divisor \( E = F = tZ(x_4 - x_1) \). Then the corresponding polytopes will be denoted \( U_i, i = 1, 2 \) so that \( \dim(C_{U_i}) = \frac{3}{4*10}c^3 \). Therefore, the parameters of the corresponding quantum code (ignoring the lower order terms) are given by

\[
n_Q = n = c^3, \quad \dim(C_{U_1}) = k_i = \frac{3}{4 * 10}c^3, \quad k_Q = n - k_1 - k_2 = c^3 - \frac{3}{2 * 10}c^3 = (1 - \frac{3}{2 * 10})c^3, \quad \text{and} \quad d_Q \geq \text{distance}(C_U^1) \geq \frac{1}{4 * 10}c^3.
\]

**Remark.** In case the field \( k = \mathbb{F}_{q^2} \) for some prime power \( q \), making use of Theorem 1.2, we obtain very similar results, with \( c = q^2 - 1 \) and with the code \( C_U^1 \) replaced by \( C_U^{1,h} \).

**Proposition 6.6.** The codes constructed in the above examples have the following property where \([n_Q, k_Q, d_Q]\) denote the corresponding quantum code parameters: On letting \( m \to \infty \) (where \( c = q^m - 1 \), \( q \) being a power of the characteristic) the ratio \( d_Q/n_Q \) remains bounded below by a positive number in the resulting families of quantum codes.

**Proof.** The statement is clear since \( d_Q \) is bounded below by \( \frac{1}{80}c^2 \) in example 1, by \( \frac{c^2}{20} \) in examples 2 and 3 and by \( \frac{1}{50}c^3 \) in example 4, (ignoring the low order terms).
Table 5. Parameters for the Codes produced in the Examples

| Type of code | Variety | Polytope | $c = |\mathbb{P}^{n}_q|$ | $n_Q$ | $k$ | $k_Q$ | $d_Q$ |
|--------------|---------|----------|----------------|------|-----|-------|-----|
| Subsystem code | $\mathbb{P}^2$ | See Eg 5.1 | $c = q^m - 1$ | $c^2$ | $\frac{1}{36} c^2$ | $\frac{1}{6} (1 - \frac{1}{36}) c^2$ | $\frac{1}{20} c^2$ |
| Stabilizer code | $\mathbb{P}^2$ | See Eg 5.1 | $c = q^m - 1$ | $c^2$ | $\frac{1}{20} c^2$ | $\frac{1}{10} (1 - \frac{1}{20}) c^2$ | $\frac{1}{50} c^2$ |
| Subsystem code | $Bl^1 \times \mathbb{P}^2$ | See Eg 5.2 | $c = q^m - 1$ | $c^2$ | $\frac{11}{80} c^2$ | $\frac{23}{80} c^2$ | $\frac{1}{20} c^2 - \frac{6}{50} c + 8$ |
| Stabilizer code | $Bl^1 \times \mathbb{P}^2$ | See Eg 5.2 | $c = q^m - 1$ | $c^2$ | $\frac{11}{80} c^2$ | $\frac{23}{80} c^2$ | $\frac{1}{20} c^2 - \frac{6}{50} c + 8$ |
| Subsystem code | $F_2$ | See Eg 5.3 | $c = q^m - 1$ | $c^2$ | $\frac{1}{4} c^2$ | $\frac{1}{4} c^2$ | $\frac{1}{20} c^2 - \frac{6}{10} c + 18$ |
| Stabilizer code | $F_2$ | See Eg 5.3 | $c = q^m - 1$ | $c^2$ | $\frac{1}{4} c^2$ | $\frac{1}{4} c^2$ | $\frac{1}{20} c^2 - \frac{6}{10} c + 18$ |
| Subsystem code | $\mathbb{P}^3$ | See Eg 5.3 | $c = q^m - 1$ | $c^3$ | $\frac{3}{40} c^3$ | $\frac{3}{40} c^3$ | $\frac{1}{10} c^3$ |
| Stabilizer code | $\mathbb{P}^3$ | See Eg 5.4 | $c = q^m - 1$ | $c^3$ | $\frac{3}{40} c^3$ | $\frac{3}{40} c^3$ | $\frac{1}{10} c^3$ |

Further examples computed using Sage. In addition to the above examples, we also consider the following elementary example and compute the minimum distances using the Toric Package in Sage. However, this method is rather limited in scope, because the above package allows computations only with relatively small fields in a reasonable amount of time. Nevertheless, we provide the following example to illustrate what is possible this way.

Example 6.7. Here we consider a field of characteristic 5 and consider the planar polytope with vertices given by $U = \{[1,1],[1,2],[2,1],[2,2]\}$. In this case, the code $C_U$, has length $16 = 4^2$ and dimension $= 4$. The minimum distance of the dual code was determined to be 3 in this case. Therefore, one may estimate the parameters of the subsystem code provided by Theorem [JA11] as:

$$n = 16, \quad dim(C_U) = 4, \quad r < 16 - 8 = 8 \quad \text{and} \quad d \geq \text{distance}(C_U^\perp) \geq 3.$$  

6.3. Comparison of the code parameters. We proceed to compare the parameters of the quantum codes constructed above with the parameters of several codes in the literature.

A key advantage of our methods is that \textit{Toric residue theorems} of [JA11] and extended to cover the Hermitian case in the appendix below, seems to provide, one of the sharpest and the most readily computable estimates for the minimum distances of the quantum codes. This is because the minimum distances of the quantum codes are very often expressed in the minimum distances of the dual of a classical code. A key discovery in [JA11] was that, though the dual of a toric evaluation code is often not isomorphic to any toric residue code, a suitable toric residue code can be shown to contain the dual of a given toric evaluation code: see [JA11] Proposition 4.9 and Corollary 4.11]. This means that to estimate the minimum distance of the dual of a toric evaluation code, one can apply intersection theory methods to the corresponding toric residue code to estimate its minimum distance. These methods apply to compute the minimum distance, over fields of any size, for codes arising from toric surfaces, even by hand as we have shown in the above examples and the techniques are transparent and simple. We have also extended these techniques to higher dimensional toric varieties as shown in the last example above, where we construct quantum codes from a $\mathbb{P}^3$ provided with a certain special line bundle.
Table 6. Comparison of code Parameters

<table>
<thead>
<tr>
<th>Type of code</th>
<th>Prime p</th>
<th>c = ( p^s - 1 )</th>
<th>( n_Q )</th>
<th>( d_Q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes in Eg. 1</td>
<td>2</td>
<td>63</td>
<td>3969</td>
<td>50</td>
</tr>
<tr>
<td>Codes in Eg. 2</td>
<td>2</td>
<td>63</td>
<td>3969</td>
<td>124</td>
</tr>
<tr>
<td>Codes in Eg. 3</td>
<td>2</td>
<td>127</td>
<td>16129</td>
<td>649</td>
</tr>
<tr>
<td>Codes in Eg. 4</td>
<td>5</td>
<td>124</td>
<td>15376</td>
<td>713</td>
</tr>
<tr>
<td>Subsystem code: [LM]</td>
<td>p</td>
<td>( q^m - 1 )</td>
<td>( q^2 - 1 = 624 )</td>
<td>3</td>
</tr>
<tr>
<td>Subsystem code: [CLLH]</td>
<td>5</td>
<td>( q^2 + 1 ), with ( q = p^s )</td>
<td>( q - 1 )</td>
<td></td>
</tr>
<tr>
<td>Subsystem code: [CLLH]</td>
<td>7</td>
<td>2402, with ( q = 7^2 )</td>
<td>48</td>
<td></td>
</tr>
</tbody>
</table>

One may see from the above table, that, in all our examples, the ratios \( d_Q/n_Q \) and \( k_Q/n_Q \) remain bounded away from zero as the field size increases, since both \( d_Q \) and \( n_Q \) can be chosen to be proportional to \( n_Q \) independent of the field size: this is a major advantage of the quantum codes produced using our techniques. For both the subsystem codes considered in [LM] and [CLLH], one can see that the minimum distance is only of the same order as \( q \), i.e. of order \( n_Q^{1/m} \), \( m \geq 2 \), in the case of [LM], and of order \( n_Q^{1/2} \) in the case of [CLLH], whereas the minimum distances provided by our codes are of the order of \( n_Q \). For the remaining codes, comparison with our codes can be achieved readily by dividing \( d_Q \) by \( n_Q \). Then one may see that the (relative) minimum distances (i.e. the ratio \( d_Q/n_Q \)) in our examples are most of the time at least as large, and often better than the minimum distances provided by the remaining codes in the above 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 \( \mathcal{L} \). 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 $k = \mathbb{F}_p^*$ 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 $d = \dim_kX = \dim_\mathbb{R}(\mathbb{M}_\mathbb{R})$. 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 $x_i$, $i = 1, \ldots, d$.

(6) In addition, we require that there exist a section $s_0 \in \Gamma(X, \mathcal{L})$ 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 (a) 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 $\mathbb{G}_m^d$ 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 nonetheless preferable to consider a slightly smaller subset of $k$-rational points chosen as follows. Let $k[\mathbb{G}_m^d] = k[t_1, t_1^{-1}, t_2, t_2^{-1}, \ldots, t_d, t_d^{-1}]$. The variable $t_i$ will also denote the $i$-th coordinate of a point in $\mathbb{G}_m^d$. 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 $\mathbb{G}_m^d$, we let $D_{S_i} = \Sigma_{a \in S_i} D_{i,a}$.

We choose the divisors as follows. We let $J_i = k^*$, 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

$$
(7.2.1) \quad D_i = D_{J_i'} + \Sigma_{j \neq i} D_{J_j, f_j}, i = 1, \ldots, d.
$$
We let $|J_i'| = n_i$ and also let $D_i' = D_iP_i'$. For each divisor $F_i$, we let $|F_i|$ 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 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 (7.2.2).

The basic hypotheses we impose then is the following:

\[ (7.2.2) \quad D_{i,a} \cdot V(p) \geq 0, i = 1, \ldots, d, \quad (\sum_{i=1}^{d} D_{i,a}) \cdot V(p) > 0 \quad \text{and} \quad \bigcap_{i=1}^{d} D_i \quad \text{is finite} \]

where $V(p)$ 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 $d = \text{dim}_{\mathbb{F}_q}(X)$ 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

\[ \Sigma_{x \in \bigcap_{i=1}^{d} D_i} \text{Res}_x(w) = 0 \]

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 $P$ satisfying the basic hypotheses as 7.1. $D_i, i = 1, \ldots, d$, is a set of effective ample divisors on $X$ and $\bigcap_{i=1}^{d} D_i = \{ R_\ell \mid \ell = 1, \ldots, M \}$ where each $R_\ell$ is a $k$-rational point of $X$. Assume that for each point $R_\ell$, one is given $v_\ell(R_\ell) \in k^*$ so that the sum $\Sigma_{\ell} v_\ell(R_\ell) = 0$. Then there exists a differential form $\eta \in \Gamma(X, \omega_X(\Sigma D_i))$ so that $\text{Res}_{R_\ell}(\eta) = v_\ell(R_\ell)$.

The modified evaluation and residue codes associated to an effective divisor $E$. Let $\mathcal{P}' = \{ P_1, \ldots, P_M \}$ denote a set of $k$-rational points in the dense orbits in $X$. Let $\mathcal{L}$ denote an ample line bundle on $X$ associated to an effective divisor $E$. Now $\mathcal{L} = \mathcal{O}(E)$. Let $s$ denote a section of $\mathcal{L}$. We send any such section $s$ to $(s(P_0), s(P_1), \ldots, s(P_M)) \in k^M$. Letting $\mathcal{P} = \{ P_1, \ldots, P_m \}$, we define the code $C(X, E, \mathcal{P})$ to be the image in $k^M$ by the evaluation map $s \mapsto (s(P_1), \ldots, s(P_m), \ldots, s(P_M))$, of the $k$-subspace $\{ s \in \Gamma(X, \mathcal{L}) | s(P_i) = 0, i = m + 1, \ldots, M \}$. Since the last $M - m$ coordinates are zero, one may view the code $C(X, E, \mathcal{P})$ 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 $\sigma$ denote a permutation of $1, \ldots, n$ so that $\sigma(i) \neq i$ for all $i$. Now let $\tilde{D}_i = D_i + D_{\sigma(i)}f_{\sigma(i)}$, $i = 1, \ldots, d$. Therefore, $\Sigma_{i=1}^{d} \tilde{D}_i = \Sigma_{i=1}^{d} D_i + \Sigma_{i=1}^{d} D_{i,f_i}$ and $|\tilde{D}_i| = |D_i|$, for each $i$ so that $\bigcap_{i=1}^{d} |\tilde{D}_i| = \bigcap_{i=1}^{d} |D_i|$. In this case we let

\[ C(X, \omega_X, E, \mathcal{P}) = \{ \alpha \in \Gamma(X, K(X) \otimes \omega_X) \mid (\alpha) + D + \Sigma_{i=1}^{d} D_{i,f_i} - E \geq 0 \} \]
where $\omega_X$ denotes, as before, the sheaf of top-degree differential forms on $X$. We call this the modified residue code in this case.

**Definition 7.4.** (i) If $k = \mathbb{F}_q$, we define $\text{Res} : C(X, \omega_X, E, \mathcal{P}) \to \mathbb{F}_q^m \subseteq \mathbb{F}_q^M$ by sending

$$\alpha \in C(X, \omega_X, E, \mathcal{P}) \mapsto (\text{Res}_{P_1}(\alpha), \ldots, \text{Res}_{P_m}(\alpha), 0, \ldots, 0).$$

(ii) If $k = \mathbb{F}_{q^2}$, we define $\overline{\text{Res}} : C(X, \omega_X, E, \mathcal{P}) \to \mathbb{F}_q^m \subseteq \mathbb{F}_q^M$ by sending

$$\alpha \in C(X, \omega_X, E, \mathcal{P}) \mapsto (\text{Res}_{P_1}^q(\alpha), \ldots, \text{Res}_{P_m}^q(\alpha), 0, \ldots, 0).$$

**Definition 7.5.** (i) For a code $C \subseteq \mathbb{F}_q^m$, we define

$$(7.2.3) \quad C^\perp = \{ x \in \mathbb{F}_q^m \mid \sum_i x_i y_i = 0 \quad \text{for any} \ y \in C \}.$$

(ii) For a code $C \subseteq \mathbb{F}_{q^2}^m$, we define

$$(7.2.4) \quad C^\perp^h = \{ x \in \mathbb{F}_q^m \mid \sum_i x_i^q y_i = 0 \quad \text{for any} \ y \in C \}.$$

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

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

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

**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 $|\tilde{D}_i| = |D_i|$ for all $i = 1, \ldots, d$. Let $f \in C(X, E, \mathcal{P})$. Recall from above that $f(P_i) = 0$, for all $i = m+1, \ldots, M$. If $\alpha \in C(X, \omega_X, E, \mathcal{P})$, 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 the sum

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

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

$$\sum_{p \in \bigcap_{i=1}^d |D_i|} (\text{Res}_p(\alpha))^q = \sum_{p \in \bigcap_{i=1}^d |D_i|} (f(p) \text{Res}_p(\alpha))^q = (\sum_{p \in \bigcap_{i=1}^d |D_i|} f(p) \text{Res}_p(\alpha))^q = 0.$$

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

$$\sum_{j} f(p_j) r_j = 0 \quad \text{for any} \ f \in C(X, E, \mathcal{P}),$$

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 $C(X, E, \mathcal{P})^\perp$. 
(ii) Assume the base field is \( \mathbb{F}_q \). Given any sequence \( \{r_j \in k \mid j = 1, \ldots, m\} \) with the property that
\[
\sum_j f(p_j)^\varepsilon r_j = 0 \quad \text{for any global section} \quad f \in C(X, E, \mathcal{P}),
\]
there exists a differential form \( \omega' \in C(X, \omega_X, E, \mathcal{P}) \) so that \( \mathcal{R} \mathcal{S} \mathcal{P}_i(\omega) = r_i^q \), \( \omega \in C(X, \omega_X, E, \mathcal{P}) \) chosen so that \( \mathcal{R} \mathcal{S} \mathcal{P}_i(\omega) = r_i \), \( i = 1, \ldots, m \). (The divisor \( D_{i,f_i} \) is defined as in [7.2.1]) Therefore, the residue map of Definition [7.4](ii) sends \( C(X, \omega_X, E, \mathcal{P}) \) onto \( C(X, E, \mathcal{P})_{\perp h} \).

**Proof.** The first statement is already proved in [JA11 Corollary 4.11], so 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 [7.4](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 \( j = m+1, \ldots, M \), the sum \( \sum_j f(p_j)^\varepsilon r_j s_0(P_j) = (\sum_j f(p_j)^\varepsilon r_j s_0(P_j)^q)^q = 0 \), 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 \( \omega' \in \Gamma(X, \omega_X(\sum_i^d D_i)) \) with \( \mathcal{R} \mathcal{S} \mathcal{P}_i(\omega') = r_i^q s_0(P_i), \ i = 1, \ldots, M \). Now consider the differential form \( \omega' \in \mathcal{R} \mathcal{S} \mathcal{P}_i(\omega) = \mathcal{R} \mathcal{S} \mathcal{P}_i(\omega)_{s_0(P_i)} = r_i^q, \ i = 1, \ldots, m \). The hypotheses on \( \omega \) and \( s_0 \) show that \( \omega' \in \Gamma(X, \omega_X(\sum_i^d D_i + \sum_i^d D_i f_i - E)) = C(X, \omega_X, E, \mathcal{P}) \) 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.1@math.osu.edu

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

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