Asymptotically Good Quantum Codes

Alexei Ashikhmin
Bell Laboratories, Lucent Technologies, 600 Mountain Avenue, Murray Hill, NJ 07974, USA, aea@research.bell-labs.com

Simon Litsyn
Department of Electrical Engineering–Systems, Tel Aviv University, Ramat Aviv 69978, Israel, litsyn@eng.tau.ac.il

Michael A. Tsfasman
Institute for Information Transmission Problems, Russian Academy of Sciences, 19 Bolshoi Karetny, 101447 Moscow GSP-4, Russia, tsfasman@iitp.ru

Using algebraic geometry codes we give a polynomial construction of quantum codes with asymptotically non-zero rate and relative distance.

I. INTRODUCTION

Let $\mathcal{B} = \mathbf{C}^2$, an element of $\mathcal{B}$ is called a *qubit*. The space $\mathcal{B}^n = \mathcal{B}^{\otimes n} = (\mathbf{C}^2)^{\otimes n}$ is the space of quantum words of length n. An $((n, K))$ *quantum code* Q is a K-dimensional linear subspace of $\mathcal{B}^n$. The parameters n and K are called the *length* and the *size* (or *cardinality*) of the code.

Let $\mathbf{L}(\mathcal{B}^n)$ be the space of linear operators on $\mathcal{B}^n$. A *quantum information message* is a vector $w \in Q$. The message w can be altered by a linear operator $E \in \mathbf{L}(\mathcal{B}^n)$, called an *error operator*.

Let us define the set $\mathrm{Supp}E \subseteq [1, n]$ in the following way. Consider the action of E on $\mathcal{B}^n$. If E can be written as $\mathrm{Id}_j \otimes E'$, where Id_j is the identity operator acting on the j-th tensor component and E' an operator on the tensor product of the other components, then $j \notin \mathrm{Supp}E$. The *weight* of E is defined as $\mathrm{wt}(E) = |\mathrm{Supp}E|$.

We say that E is *detectable* by Q if for any two $v, u \in Q$ if $v \perp u$ then $v \perp E(u)$. Let d_Q be the maximum integer such that Q can detect any error of weight $d_Q - 1$ or less; d_Q is called the *minimum distance* of Q. We say that Q is an $((n, K, d_Q))$-code. It can be proved that the code Q can correct any error of weight $\lfloor \frac{d_Q - 1}{2} \rfloor$ or less.

Remark One can find a more details discussion of the notions of quantum minimum distance, quantum detection, and quantum correction in [1–4].

Probably the most interesting and important class of quantum codes are quantum stabilizer codes. These codes can be viewed as natural analogues of classical linear codes. To define a quantum stabilizer code we first introduce another class of (non-quantum) codes.

Let $T = \mathbf{F}_4$. The non-trivial automorphism of $\mathbf{F}_4$ over $\mathbf{F}_2$ is called complex conjugation and denoted in the same way. We fix a (symplectic) form on T^n given by $\omega(x, y) = \mathrm{Tr}(x\bar{y})$. There is a usual $\mathbf{F}_4$ Hamming norm on T^n. A *small symplectic code* $F \subset T^n$ is an ω-isotropic $\mathbf{F}_2$-subspace in T^n, i.e., $\omega(x, y) = 0$ for any $x, y \in F$. Its *minimal distance* $d = d_F$ is defined as the minimum $\mathbf{F}_4$ Hamming norm of a non-trivial vector in F. Its dimension $k = k_F$ is its $\mathbf{F}_2$-dimension, in particular, $k \leq n$. The ω-dual F^ω of a small symplectic code F is called a *large symplectic code*, for a large symplectic code we have $n \leq k_{F^\omega} \leq 2n$. Of course, $F \subset F^\omega$.

Let $F \subset T^n$ be a small symplectic code with parameters $[n, k, d]$. We are going to define the stabilizer code $Q_F \subset \mathcal{B}^n$ corresponding to F. Let $\mathbf{F}_4 = \{0, 1, \varepsilon, \bar{\varepsilon}\}$. Set

$$\sigma(0) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \sigma(\varepsilon) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma(\bar{\varepsilon}) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$
$$\sigma(1) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

These are the usual *Pauli matrices*. Then, for $t = (t_1, \ldots, t_n) \in T^n$ we put

$$\sigma(t) = \sigma(t_1) \otimes \ldots \otimes \sigma(t_n). \tag{1}$$

We get a map (of sets) $\sigma : T^n \to \mathbf{L}(\mathcal{B}^n)$. Being restricted to a small symplectic code $F \subset T^n$, the map σ happens to be almost a group homomorphism, namely for $f_1, f_2 \in F$ we have

$$\sigma(f_1)\sigma(f_2) = \sigma(f_2)\sigma(f_1) = \pm\sigma(f_1 + f_2),$$

in particular $\sigma(f_1)$ and $\sigma(f_2)$ commute. This makes it possible to consider the subspace of $\mathcal{B}^n$ fixed by $\sigma(F)$ in the following way. Let $\mathcal{F} = \{f_1, \ldots, f_k\}$ be an $\mathbf{F}_2$-basis of F and let $\mu = \{\mu_1, \ldots, \mu_k\}$, $\mu_i \in \{\pm 1\}$.

Define $Q_{\mathcal{F},\mu}$ as follows

$$Q_{\mathcal{F},\mu} = \{x \in \mathcal{B}^n \mid \sigma(f_i)(x) = \mu_i x \text{ for any } i = 1, \ldots, k\}.$$

The quantum code $Q_{\mathcal{F},\mu}$ is called a *stabilizer code*. For any $f \in F$ the operator $\sigma(f)$ acts on $Q_{\mathcal{F},\mu}$ as ± 1.

The small symplectic code F being fixed, we get 2^k different codes $Q_{\mathcal{F},\mu}$. Their properties, we are interested in, do not depend on the choice of $\mathcal{F}$ and μ, and by abuse of notation we call each of them Q_F.

The main theorem on stabilizer codes says that the parameters of the obtained quantum codes are

$$K_{Q_F} = 2^{n-k_F} \quad , d_{Q_F} = \min_{f \in F^\omega \setminus F} \|f\| \geq d_{F^\omega} \ . \tag{2}$$

Remark Detailed descriptions of quantum stabilizer codes including the proof of the above statements on their parameters can be found in [5–8,3].

Let $k_Q = \log_2 K_Q$ and set

$$R_Q = \frac{k_Q}{n} \text{ and } \delta_Q = \frac{d_Q}{n}.$$

We are interested in

$$R(\delta) = \limsup_{n\to\infty} R_Q,$$

where the limit is taken over all codes with $\delta_Q \geq \delta$.

The best known *nonconstructive* lower bound on $R(\delta)$ was obtained in [10] via codes over $\mathbf{F}_4$:

$$R(\delta) \geq 1 - \delta \log_2 3 - H(\delta), \tag{3}$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. For upper bounds see [2].

Several methods were proposed to construct quantum codes, see, e.g. [9–12,5,4,7,8,13,14]. However, when n grows for a fixed $R > 0$, the relative minimum distance δ of all these codes tends to zero.

In this paper we give a (polynomial in n) construction of quantum codes from algebraic geometry codes, so that in a certain interval of rates R the relative minimum distance of these quantum codes is separated from zero, i.e., we construct a family of *asymptotically good quantum codes.*

The construction proceeds in four steps. Algebraic curves give us asymptotically good nonbinary algebraic geometry codes, and we provide that each of them contains its dual. Then we take a binary symbolwise expansion in a self-dual basis of the codewords of these algebraic geometry codes, so that the resulting binary codes also contain their duals. Then we plug these codes into Steane's construction [14] to construct good symplectic codes. The corresponding quantum codes are asymptotically good.

To make the exposition simpler, we follow this path backwards. We have already explained how quantum codes are related to symplectic codes. In Section II we recall Steane's construction of symplectic codes starting from triples $D' \supset D \supset D^\perp$ of binary codes. Section III explains how to construct binary codes containing their duals from codes over $\mathbf{F}_{2^m}$ with the same property. In Section IV we produce necessary algebraic geometry codes. Finally, in Section V we sum up to get the parameters. Here is the result (see Fig.1).

Theorem 1 *For any $\delta \in (0, \frac{1}{18})$ and R lying on the broken line given by the piecewise linear function*

$$R(\delta) = 1 - \frac{2}{2^m - 2} - \frac{10}{3} m\delta \text{ for } \delta \in [\delta_m, \delta_{m-1}],$$

where $m = 3, 4, 5, \ldots$; $\delta_2 = \frac{1}{18}$ and

$$\delta_m = \frac{3}{5}\frac{2^m}{(2^m-2)(2^{m+1}-2)} \text{ for } m = 3, 4, 5, \ldots,$$

there exist polynomially constructible families of quantum codes with $n \to \infty$ and asymptotic parameters greater than or equal to (δ, R).

II. FROM BINARY CODES TO SYMPLECTIC CODES

We follow Steane's construction [14] with improved estimates on the parameters given by by Cohen, Encheva and Litsyn [11].

We start with a triple $D' \supset D \supset D^\perp$ of binary codes, where D is an $[n, k, d]$-code containing its dual $D^\perp$, and D' a larger $[n, k']$-code with $k' \geq k + 2$. Let G be a generator matrix of D, and let G' be such a matrix that

$$\begin{pmatrix} G \\ G' \end{pmatrix}$$

is a generator matrix of D'. Denote by d_2' the second generalized weight of D', i.e., the minimum weight of the bitwise OR of two different nonzero codewords (see [15–18] for properties and known bounds). Form the code $C \subset \mathbf{F}_2^{2n}$ with the generator matrix

$$\begin{pmatrix} G & 0 \\ 0 & G \\ G' & G'' \end{pmatrix},$$

where the matrix G'' is obtained from G' by permuting its rows so that no row stays on its place.

Fix the following $\mathbf{F}_2$-linear isomorphism between $\mathbf{F}_2^{2n}$ and $\mathbf{F}_4^n$ first mapping $(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbf{F}_2^{2n}$ to $((x_1, y_1), \ldots, (x_n, y_n)) \in (\mathbf{F}_2^2)^n$ and then identifying $\mathbf{F}_2^2$ and $\mathbf{F}_4$ by $(0,0) = 0, (0,1) = \varepsilon, (1,0) = \bar{\varepsilon}, (1,1) = 1$. The image of C under this map is $F \subset \mathbf{F}_4^n$. Here is an estimate for its parameters [14,11]:

Theorem 2 *The code $F \subset \mathbf{F}_4^n$ is a large symplectic code, i.e., $F \supset F^\omega$. Its parameters are $k_F = k + k'$ and $d_F \geq \min(d, d_2')$.*

Proof Let $x = (a_1, \ldots, a_n, b_1, \ldots, b_n)$ and $x' = (a_1', \ldots, a_n', b_1', \ldots, b_n')$. We choose the above identification between $\mathbf{F}_4^n$ and $\mathbf{F}_2^{2n}$. In the basis of $\mathbf{F}_2^{2n}$ the form $\omega(x, x')$ is given by $\omega(x, x') = \sum_{j=1,\ldots,n} a_j b_j' + a_j' b_j$. Then suppose that $x \in F^\omega$. This means that $\omega(x, x') = 0$ for any $x' \in F$. In particular, this is true for $x' = (a_1', \ldots, a_n', 0, \ldots, 0)$ and $x' = (0, \ldots, 0, b_1', \ldots, b_n')$. We get $\sum_{j=1,\ldots,n} a_j b_j' = 0$ for any $(b_1', \ldots, b_n') \in D$, and therefore $(a_1, \ldots, a_n) \in D^\perp \subset D$. Analogously, $(b_1, \ldots, b_n) \in D^\perp \subset D$, and we see that $x \in F$.

The value of k_F is obvious. Then we have to estimate d_F. Let $x \in F$. Then

$$x = (a_1, \ldots, a_n, 0, \ldots, 0) + (0, \ldots, 0, b_1, \ldots, b_n) + (a_1', \ldots, a_n', b_1', \ldots, b_n'),$$

where $(a_1,\ldots,a_n) \in D$, $(b_1,\ldots,b_n) \in D$, and $(a'_1,\ldots,a'_n,b'_1,\ldots,b'_n) \in D'$. If the last summand is zero, the number of non-zero pairs (a_j,b_j) is at least d. If it is non-zero, then both $(a_1+a'_1,\ldots,a_n+a'_n)$ and $(b_1+b'_1,\ldots,b_n+b'_n)$ lie in D' and they are different since two generators of D' not lying in D cannot differ by an element of D. Hence, the $\mathbf{F}_4$-weight of the sum is at least d'_2. □

Corollary 1 *The parameters of the corresponding quantum stabilizer code Q_F satisfy*

$$k_{Q_F} = k + k' - n, \quad , d_{Q_F} \geq \min(d, d'_2) \geq \min\left(d, \frac{3}{2}d'\right).$$

Proof By Eq. (2) the dimension $k_{Q_F} = n - k_{F^\omega} = n - (2n - k_F) = k + k' - n$. The first inequality is also that of Eq. (2).

To prove that $d'_2 \geq \frac{3}{2}d'$ write two different vectors one below the other. Let the number of columns $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ equal, respectively, a_1, a_2, a_3, a_4. Then $d'_2 = a_2 + a_3 + a_4$. The weight of the first vector is $a_3 + a_4 \geq d'$, of the second $a_2 + a_4 \geq d'$, and of their sum $a_2 + a_3 \geq d'$. Summing up we get the result. □

To apply this construction one needs good binary codes with $D^\perp \subset D$.

III. FROM NON-BINARY TO BINARY CODES

The following theorem is due to T.Kasami an S.Lin [19].

Theorem 3 *Let C be a code over $\mathbf{F}_{2^m}$ and $C^\perp \subset C$. Let $\alpha_i, i = 1,\ldots,m$ be a self-dual basis of $\mathbf{F}_{2^m}$ over $\mathbf{F}_2$, i.e.,*

$$Tr(\alpha_i\alpha_j) = \delta_{ij}.$$

Let D and $D^\perp$ be codes obtained by the symbolwise binary expansion of codes C and $C^\perp$ in the basis α_i. Then $D^\perp \subset D$ and $D^\perp$ is the binary dual of D.

Proof The first statement is obvious.

Let us prove the second one. Let $x = (x_1, x_2, \ldots, x_n) \in C$ and $y = (y_1, y_2, \ldots, y_n) \in C^\perp$. Let

$$x_j = \sum_{i=1}^{m} x_i^{(j)}\alpha_i\,,$$

$$y_j = \sum_{i=1}^{m} y_i^{(j)}\alpha_i\,.$$

Then

$$\sum_{j=1}^{n} x_j y_j = \mathbf{xy} = 0$$

Hence

$$\begin{aligned} 0 &= \mathrm{Tr}\left(\sum_{j=1}^{n} x_j y_j\right) \\ &= \mathrm{Tr}\left(\sum_{j=1}^{n}\sum_{i=1}^{m}\sum_{t=1}^{m} x_i^{(j)} y_t^{(j)}\alpha_i\alpha_t\right) \\ &= \sum_{j=1}^{n}\sum_{i=1}^{m}\sum_{t=1}^{m} x_i^{(j)} y_t^{(j)}\mathrm{Tr}(\alpha_i\alpha_t) \\ &= \sum_{j=1}^{n}\sum_{i=1}^{m} x_i^{(j)} y_i^{(j)}. \end{aligned}$$

So we have proved that $(D)^\perp \supseteq D^\perp$. It rests to remark that the dimensions of D and $D^\perp$ are complimentary. □

Of course, if we start from a triple $C' \supset C \supset C^\perp$ of codes over $\mathbf{F}_{2^m}$ the same descent gives us a triple $D' \supset D \supset D^\perp$ of binary codes.

IV. FROM ALGEBRAIC CURVES TO CODES

In this section we follow standard algebraic geometry constructions presented in [20], proving that they satisfy some extra properties needed to use them in above constructions. Namely, we want a triple $C' \supset C \supset C^\perp$ of codes over $\mathbf{F}_{2^m}$ with good parameters. Let us start from looking for algebraic codes containing their duals.

Let $w \in (\mathbf{F}_q^*)^n$. For a code $C \subset \mathbf{F}_q^n$ we define

$$C_w^\perp = \left\{x \in \mathbf{F}_q^n : \sum w_i x_i y_i = 0 \text{ for any } y \in C\right\}.$$

Let X be a (smooth projective geometrically irreducible algebraic) curve of genus g defined over $\mathbf{F}_q$, let $\mathcal{D}$ be an effective divisor of degree a and $\mathcal{P}' = \{P_1,\ldots,P_{n'}\} \subseteq X(\mathbf{F}_q)$ a set of $\mathbf{F}_q$-points such that $\mathrm{Supp}\mathcal{D} \cap \mathcal{P}' = \emptyset$; we set $\mathbf{P}' = P_1 + \ldots + P_{n'}$. As usual,

$$L(\mathcal{D}) = \{f \in \mathbf{F}_q(X) : (f) + \mathcal{D} \geq 0\} \cup \{0\}$$

is the space of functions associated to the divisor, and

$$\Omega(\mathcal{D}) = \{\omega \in \Omega(X) : (\omega) + \mathcal{D} \geq 0\} \cup \{0\}$$

that of differential forms.

Suppose that $a \leq \frac{n'}{2} + \frac{g}{2} - 1$, then for any effective divisor $\mathcal{E}$ of degree $\deg\mathcal{E} = n' + g - 2 - 2a$ we have $\deg(K + \mathbf{P}' - 2\mathcal{D} - \mathcal{E}) = g$ and by the Riemann–Roch theorem there exists an $\omega \in \Omega(\mathbf{P}' - 2\mathcal{D} - \mathcal{E})$. Unfortunately, working over a finite field, we cannot guarantee that ω actually has poles at all points of $\mathcal{P}'$. However, the set of poles $\mathcal{P} = \{P_1,\ldots,P_n\} \subseteq \mathcal{P}'$ consists of $n \geq n' - g$ points. Put $\mathbf{P} = P_1 + \ldots + P_n$. Of course, $\omega \in \Omega(\mathbf{P} - 2\mathcal{D} - \mathcal{E})$. Let $w = (\mathrm{Res}_{P_1}(\omega),\ldots,\mathrm{Res}_{P_n}(\omega))$.

The algebraic geometry code $C_L(X,\mathcal{D},\mathcal{P})$ is defined as the image of the evaluation map

$$\begin{array}{ccc} L(\mathcal{D}) & \longrightarrow & \mathbf{F}_q^n, \\ f & \longmapsto & (f(P_1),\ldots,f(P_n)). \end{array}$$

Put $C = C_L(X, \mathcal{D}, \mathcal{P})_w^{\perp}$. For any two functions $f, g \in L(\mathcal{D})$ we have $fg\omega \in \Omega(\mathbf{P})$. Therefore $fg\omega$ has no poles except in $\mathbf{P}$ and, by the residue formula, $\sum w_i f(P_i) g(P_i) = \sum \mathrm{Res}_{P_i}(\omega) = 0$. We have proved that $C \supseteq C_w^{\perp}$.

If $q = 2^m$, any element of $\mathbf{F}_q$ is a square, in particular, $w_i = v_i^2$. Let g_v be coordinatewise multiplication by $v = (v_1, \ldots, v_n)$. Then the code $C' = g_v(C)$ has the property $C' \supseteq C'^{\perp}$.

Recall that if $a \geq 2g - 1$, the parameters of C and C' are

$$\begin{aligned} k &= n - a + g - 1, \\ d &\geq a - 2g + 2. \end{aligned}$$

Summing up, we have proved

Theorem 4 *If there exists a curve over $\mathbf{F}_q$ of genus g with at least $n' \geq 4g$ $\mathbf{F}_q$-points, then for any $n \leq n' - g$ and any $a = 2g-1, \ldots, \frac{n}{2}+g-1$ there is an $[n, k, d]_q$-code C with*

$$k = n - a + g - 1, \tag{4}$$

$$d \geq a - 2g + 2, \tag{5}$$

such that $C \supseteq C_w^{\perp}$ for some $w \in (\mathbf{F}_q^*)^n$.

Moreover, if q is a power of 2, there is such a code with $C \supseteq C^{\perp}$.

Applying, as usual, this theorem to asymptotically good families of curves over $\mathbf{F}_q$, q being a square, such that

$$\frac{|X(\mathbf{F}_q)|}{g(X)} \to \sqrt{q} - 1,$$

we get

Corollary 2 *Let q be an even power of a prime. Then for any*

$$\alpha \in \left(\frac{2}{\sqrt{q} - 2} \ , \ \frac{1}{2} + \frac{1}{\sqrt{q} - 2} \right) \tag{6}$$

there exist families of codes with asymptotic parameters

$$R = 1 - \alpha + \frac{1}{\sqrt{q} - 2}, \tag{7}$$

$$\delta \geq \alpha - \frac{2}{\sqrt{q} - 2}, \tag{8}$$

with the auxiliary property $C \supseteq C_w^{\perp}$ for some $w \in (\mathbf{F}_q^*)^n$.

If q is an even power of 2, there exist such codes with a stronger property $C \supseteq C^{\perp}$.

To construct quantum codes we need a somewhat stronger statement. Recall that we need a triple $C' \supset C \supset C^{\perp}$.

If we take two divisors $\mathcal{D}' \leq \mathcal{D}$ then $C_L(X, \mathcal{D}', \mathcal{P}) \subseteq C_L(X, \mathcal{D}, \mathcal{P})$ and we have the opposite inclusion for duals. The differential form ω with the above properties, good for $\mathcal{D}$ is also good for $\mathcal{D}'$. Taking $\mathcal{D} = aP_0$ and $\mathcal{D}' = a'P_0$ with $a' < a$ we prove the following

Corollary 3 *Let $q = 2^{2m}$. Then for any pair of real numbers (α', α) such that $\frac{2}{2^m - 2} \leq \alpha' \leq \alpha \leq \frac{1}{2} + \frac{1}{2^m - 2}$ there exist families of triples of 2^{2m}-ary codes $C' \supset C \supseteq C^{\perp}$ with asymptotic parameters*

$$R' = 1 - \alpha' + \frac{1}{2^m - 2}, \tag{9}$$

$$\delta' \geq \alpha' - \frac{2}{2^m - 2}, \tag{10}$$

$$R = 1 - \alpha + \frac{1}{2^m - 2}, \tag{11}$$

$$\delta \geq \alpha - \frac{2}{2^m - 2}. \tag{12}$$

Here R' signifies the asymptotic rate of codes C', and R and δ are asymptotic parameters of codes C.

Remark Choosing an $\mathbf{F}_q$-point P_∞ and taking $\mathrm{Supp}\mathcal{E} = \mathrm{Supp}\mathcal{D} = \mathrm{Supp}\mathcal{D}' = P_0$ and $\mathcal{P}' = X(\mathbf{F}_q) \setminus P_0$ we see that the above codes are polynomially constructible. This uses, of course, a difficult theorem of Vlăduţ, see [21,20].

V. SUMMING UP: QUANTUM CODES

We say that a quantum code can be constructed in polynomial time if there exists a polynomial time algorithm constructing explicitly an encoder of the code and this encoder has polynomially many elementary quantum gates.

In [22] it is in fact shown that knowledge of the generator matrix of the symplectic code F (also called generating operators of the stabilizer group of Q_F) suffices to construct a polynomial complexity encoder. Moreover this encoder construction is, roughly speaking, a sequence of Gaussian eliminations of $k \times n$ matrices and hence it has polynomial complexity. Any generator matrix of the code $C^{\perp}$ could be used to construct a set of generator operators of $\mathcal{S}$ polynomially. Finally, it is shown in [21,20] that generator matrices of algebraic geometry codes described in Section IV can be constructed in polynomial time. Thus the associated quantum stabilizer codes are also constructible in polynomial time.

To construct an asymptotically good quantum code Q we start with a family of curves X over $\mathbf{F}_{2^{2m}}$ with $\frac{|X(\mathbf{F}_q)|}{g(X)} \to 2^m - 1$. Each curve gives us a triple $C' \supset C \supset C^{\perp}$ of algebraic geometry codes C over $\mathbf{F}_{2^{2m}}$ as described in Section IV. Let C be an $[n, k, d]$-code and C' an $[n, k', d']$-code. Binary expansions of C and C' with respect to a self-orthogonal basis give us a triple $D' \supset D \supset D^{\perp}$ of binary codes with $n_{D'} = n_D = 2mn, k_{D'} = 2mk', k_D = 2mk, d_{D'} \geq d', d_D \geq d$, cf. Section III. These codes give us symplectic codes F, their parameters being $[2mn, 2m(k+k'), \geq \min\{d, \frac{3}{2}d'\}]$. In their turn these give us quantum stabilizer $[[2mn, 2m(k+k'-n), \geq \min\{d, \frac{3}{2}d'\}]]$-codes Q. The corresponding asymptotic parameters are

$$R_Q = R + R' - 1 \tag{13}$$

$$\delta_Q \geq \min\{\delta, \frac{3}{2}\delta'\} \tag{14}$$

where R, R', δ and δ' are the parameters of algebraic geometry $\mathbf{F}_{2^{2m}}$-ary codes.

It is time to use Corollary 3. Put $\alpha' = \frac{2}{3}(\alpha + \gamma)$, where $\gamma = \frac{1}{2^m - 2}$ (this choice of α' is optimal here). The restrictions $2\gamma \leq \alpha' < \alpha \leq \frac{1}{2} + \gamma$ are equal to $2\gamma \leq \alpha \leq \frac{1}{2} + \gamma$. The asymptotic parameters of the algebraic geometry codes are

$$R = 1 - \alpha + \gamma, \tag{15}$$

$$\delta \geq \alpha - 2\gamma, \tag{16}$$

$$R' = 1 - \frac{2}{3}\alpha + \frac{1}{3}\gamma, \tag{17}$$

$$\delta' \geq \frac{2}{3}\alpha - \frac{4}{3}\gamma. \tag{18}$$

Their binary expansions have the same R and R', and the estimates for their δ and δ' are divided by $2m$. By Corollary 1 the parameters of the quantum codes obtained are

$$R_Q = R + R' - 1 = 1 + \frac{4}{3}\gamma - \frac{5}{3}\alpha, \tag{19}$$

$$\delta_Q \geq \frac{1}{2m}(\alpha - 2\gamma). \tag{20}$$

Therefore, for any $m \geq 3$ we get a polynomial bound

$$R_Q = 1 - \frac{2}{2^m - 2} - \frac{10}{3} m \delta_Q \tag{21}$$

with the restriction

$$\delta_Q \leq \frac{1}{2m}\left(\frac{1}{2} - \frac{1}{2^m - 2}\right), \tag{22}$$

i.e.,

$$1 - \frac{2}{2^m - 2} \geq R_Q \geq \frac{1}{6} - \frac{1}{3}\frac{1}{2^m - 2}. \tag{23}$$

Theorem 1 now follows from Eq. (21) and Eq. (23) by direct computation.

On Fig.1 we present the Gilbert–Varshamov type bound Eq. (3) and the polynomial bound of Theorem 1 based on Eq. (21) and Eq. (23).

Acknowledgements

The authors would like to thank M.Vyalyi for many fruitful discussions, and S.Lvovski for finding an important gap in the preliminary version of this paper.

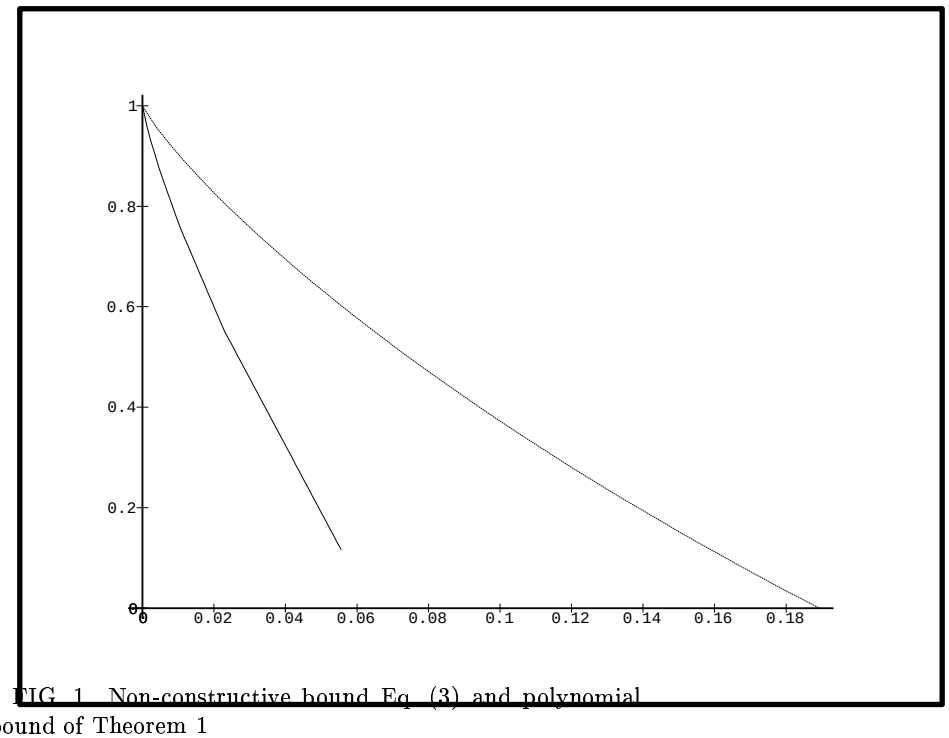


FIG. 1. Non-constructive bound Eq. (3) and polynomial bound of Theorem 1

[1] A.Ashikhmin, A.Barg, E.Knill, and S.Litsyn, "Quantum error detection I: Statement of the problem", *IEEE Transactions on Information Theory*, submitted.

[2] A.Ashikhmin and S.Litsyn, "Upper bounds on the size of quantum codes", *IEEE Trans. Info. Theory*, vol.45, 4, 1999, pp.1206–1215.

[3] A.Kitaev, A.Shen, M.Vyalyi, *Classical and Quantum Calculations*, MCCME-CheRho, 1999 (in Russian).

[4] E.Knill and R.Laflamme, "A theory of quantum error-correcting codes", *Phys. Rev. A*, vol.55, pp. 900-911, 1997.

[5] A.R.Calderbank and P.W.Shor, "Good quantum error-correcting codes exist", *Phys. Rev. A*, vol.54, pp.1098-1105, 1996.

[6] D.Gottesman, "Stabilizer Codes and Quantum Error Correction", Ph.D. Thesis, California Institute of Technology, 1997.

[7] P.W.Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, vol.52, pp. 2493-2496, Oct. 1995.

[8] A.M.Steane, "Multiple particle interference and quantum error correction", *Proc. Roy. Soc. Lond. A*, vol. 452, pp. 2551-2577, 1996.

[9] A.R.Calderbank, E.M.Rains, N.J.A.Sloane, and P.W.Shor, "Quantum error correction and orthogonal geometry", *Phys. Rev. Lett.*, vol.78, pp. 405-409, 1997.

[10] A.R.Calderbank, E.M.Rains, N.J.A.Sloane and P.W.Shor, "Quantum error correction via codes over GF(4)", *IEEE Trans. Info. Theory*, vol.44, pp.1369 – 1387, 1998.

[11] G.Cohen, S.Encheva and S.Litsyn, "On binary constructions of quantum codes", *IEEE Trans. Inform. Theory*, vol.45, pp.2495-2498, 1999.

[12] D.Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound", *Phys. Rev. A*, vol.54, pp. 1862-1868, 1996.

[13] A.M.Steane, "Simple quantum error correcting codes", *Phys. Rev. Lett.*, vol. 77, pp. 793-797, 1996.

[14] A.M.Steane, "Enlargement of Calderbank – Shor – Steane quantum codes", *IEEE Trans. Inform. Theory*, vol.45, pp.2492–2495. 1998.

[15] A.Ashikhmin, A.Barg, and S.Litsyn, "New upper bounds on generalized weights", *IEEE Transactions on Information Theory*, vol.45, 4, 1999, pp.1258–1263.

[16] G.Cohen, S.Litsyn and G.Zémor, "Upper bounds on generalized distances", *IEEE Trans. Info. Theory*, vol.40, pp.2090-2092, 1994.

[17] M.A.Tsfasman and S.G.Vlăduţ, "Geometric approach to higher weights" *IEEE Trans. Info. Theory*, vol.41, pp.1564–1588, 1995.

[18] V.Wei, "Generalized Hamming weights for linear codes", *IEEE Trans. Info. Theory*, vol.37, pp.1412–1418, 1991.

[19] T.Kasami and S.Lin, "The binary weight distribution of the extended $(2^m, 2^m - 4)$ code of the Reed-Solomon code over $GF(2^m)$ with generator polynomial $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$", *Linear Algebra and its Applications*, vol. 98, pp.331–346, 1988.

[20] M.A.Tsfasman and S.G.Vlăduţ, *Algebraic-Geometric Codes*, Kluwer Acad. Publ., 1991

[21] G.L.Katsman, M.A.Tsfasman, and S.G.Vlăduţ, "Modular curves and codes with a polynomial construction", *IEEE Trans. Info. Theory*, vol.41, pp.353–355, 1984.

[22] R.Cleve and D.Gottesman, "Efficient computations of encodings for quantum error correction", *LANL preprint quant-ph/9607030*, 1996.