Asymptotically Good Quantum Codes

M. A. Tsfasman *

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

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.

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

Independent University of Moscow, Institute for Information Transmission Problems, and Institut de Mathématiques de Luminy. E-mail: tsfasman@iitp.ru. Partly supported by RBRF 99-01-01204. This lecture is based on my joint work with A.Ashikhmin and S.Litsyn [1].

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 $\sigma(t) = \sigma(t_1) \otimes \ldots \otimes \sigma(t_n)$. 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 $Q_{\mathcal{F},\mu} = \{x \in \mathcal{B}^n \mid \sigma(f_i)(x) = \mu_i x \text{ for any } i = 1, \ldots, k\}$. The quantum code $Q_{\mathcal{F},\mu}$ is called a *stabilizer code*. By abuse of notation we denote it Q_F. The main result on stabilizer codes says that the parameters of the obtained quantum code are $K_{Q_F} = 2^{n-k_F}, d_{Q_F} = \min_{f \in F^\omega \setminus F} \|f\| \geq d_{F^\omega}$. Let $k_Q = \log_2 K_Q$ and set $R_Q = \frac{k_Q}{n}, \delta_Q = \frac{d_Q}{n}$, and $R(\delta) = \limsup_{n\to\infty} R_Q$, where the limit is taken over all codes with $\delta_Q \geq \delta$.

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 use these codes to construct good symplectic codes. The corresponding quantum codes are asymptotically good. Here is the result.

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

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

where $m = 3, 4, 5, \ldots$; $\delta_2 = \frac{1}{18}$, $\delta_3 = \frac{3}{56}$, and

$$\delta_m = \frac{3}{5} \frac{2^{m-2}}{(2^m - 1)(2^{m-1} - 1)} \quad \text{for } m = 4, 5, 6, \ldots,$$

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

Reference

[1] A. Ashikhmin, S. Litsyn, M. Tsfasman "Asymptotically Good Quantum Codes", Phys. Rev. A, vol.63, 032311 (2001)