Quantum Goppa Codes Exceeding the Quantum Gilbert-Varshamov Bound

Annika Niehage
Universität Mannheim
Lehrstuhl für Mathematik V, Seminargebäude A5
68131 Mannheim

No. 279 / 2006

NONBINARY QUANTUM GOPPA CODES EXCEEDING THE QUANTUM GILBERT-VARSHAMOV BOUND

by

Annika Niehage

Abstract. — An explicit construction for nonbinary quantum Goppa codes (often also called quantum AG codes) exceeding the quantum Gilbert-Varshamov bound is given. First a weighted symplectic inner product is introduced and a method how to transform weighted codes into quantum codes with respect to the standard symplectic inner product is given. Then families of quantum Goppa codes using a tower of function fields by Stichtenoth are constructed. Finally a proof that these codes lie above the quantum Gilbert-Varshamov bound is given.

1. Introduction

Quantum error-correcting codes (QECC) have been developed in several ways to protect quantum systems from decoherence and errors similarly to classical coding theory. The first ideas were to use direct constructions [**4**]. Later the theory of stabilizer codes was developed [**7**]. One method to construct classical codes and transform them into QECCs is called CSS and used most of the time in connection with algebraic geometric codes [**2**], [**3**], [**5**], [**6**]. A construction without using CSS can be found in [**10**]. In the last years, attention was mainly paid to binary codes, but in nature a lot of nonbinary quantum systems appear. Therefore it is natural to consider nonbinary QECCs. Nonbinary quantum codes already have been constructed in [**1**], [**8**], [**12**]. Nonbinary constructions using algebraic geometry have been considered in [**9**].

In this paper a direct and explicit construction of families of nonbinary QECCs using a tower of function fields of [**14**] is given. These families are asymptotically good and better than the quantum Gilbert-Varshamov bound. The structure of the paper is the following: Section 2 introduces nonbinary quantum codes. In Section 3

Key words and phrases. — Coding theory, Algebraic geometry, Quantum error-correcting codes.

we see Goppa codes and their transformation to quantum codes including an important result not published yet about an asymptotically good tower of function fields by H. Stichtenoth. Section 4 consists of the main construction of good families of quantum Goppa codes. The last section proves that the asymptotics of these constructed codes lie above the quantum Gilbert-Varshamov bound.

2. Nonbinary quantum codes

In this section some basic definitions and main theorems about nonbinary quantum stabilizer codes are given. A weighted symplectic inner product is introduced and a way how to transform codes with respect to this weighted symplectic inner product to quantum stabilizer codes with respect to the standard symplectic inner product. For a more detailed introduction to quantum codes and quantum stabilizer codes see [**11**].

Let K be a finite field of odd characteristic. The common way to define a *stabilizer code* is to take vectors of length $2n$, the first n entries stand for the X-errors, the second n entries for the Z-errors on the n qudits, where:

$$X^j|i\rangle = |i+j\rangle, \quad Z^j|i\rangle = e^{\frac{2\pi i}{p}\cdot \mathrm{tr}(i\cdot j)}|i\rangle$$

with $i, j \in K$, addition in K, and $\mathrm{tr} : K \to \mathbb{F}_p$ the trace map. A *generator matrix* of a code is of the form $(X|Z)$. This defines an $[[n,k,d]]$-code. Here n is the length of the codewords, $k = n - l$ is the dimension of the code, where l is the number of rows of the generator matrix, and d is the distance of the code. A stabilizer code satisfies a symplectic inner product, i. e. for all codewords x, y $\langle x, y\rangle_s = \sum_{i=1}^{n}(x_i\, y_{n+i} - x_{n+i}\, y_i) = 0$. We now introduce a weighted version of this symplectic inner product which gives more freedom in constructing stabilizer codes. This will be useful in particular in the nonbinary case.

Let us call $\langle x, y\rangle_s^a = \sum_{i=1}^{n} a_i(x_i\, y_{n+i} - x_{n+i}\, y_i)$ a *weighted symplectic inner product* where the coefficients $a_i \neq 0$ are elements of the alphabet (i.e. elements of the finite field). If we construct a code C that satisfies $\langle x, y\rangle_s^a = \sum_{i=1}^{n} a_i(x_i\, y_{n+i} - x_{n+i}\, y_i) = 0$, we can change the codewords of C by multiplying each component x_i of every codeword by the corresponding a_i, for $1 \leq i \leq n$. Hence we change the codewords $(x_1, \ldots, x_n|z_1, \ldots, z_n)$ to $(a_1x_1, \ldots, a_nx_n|z_1, \ldots, z_n)$ and we get a stabilizer code that is self-orthogonal with respect to the standard symplectic inner product and has a generator matrix

$$\left(\begin{array}{ccc|ccc} a_1 \cdot c_{1,1} & \cdots & a_n \cdot c_{1,n} & c_{1,n+1} & \cdots & c_{1,2n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_1 \cdot c_{l,1} & \cdots & a_n \cdot c_{l,n} & c_{l,n+1} & \cdots & c_{l,2n} \end{array}\right).$$

This code satisfies $\langle x', y'\rangle_s = \sum_{i=1}^{n}(a_i\, x_i\, y_{n+i} - x_{n+i}\, a_i\, y_i) = \langle x, y\rangle_s^a = 0$ for all new codewords x', y'. The code properties do not change by this transformation:

Lemma 2.1. — *Let C be a linear code over $\mathbb{F}_{p^m}$ which is self-orthogonal with respect to the weighted symplectic inner product $\langle\ ,\ \rangle_s^a$ and has a corresponding quantum code with parameters $[[n, k, d]]$ and generator matrix*

$$\mathcal{G} = \left(\begin{array}{ccc|ccc} c_{1,1} & \cdots & c_{1,n} & c_{1,n+1} & \cdots & c_{1,2n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ c_{l,1} & \cdots & c_{l,n} & c_{l,n+1} & \cdots & c_{l,2n} \end{array}\right).$$

Then the code C' with generator matrix

$$\mathcal{G}' = \left(\begin{array}{ccc|ccc} a_1 \cdot c_{1,1} & \cdots & a_n \cdot c_{1,n} & c_{1,n+1} & \cdots & c_{1,2n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_1 \cdot c_{l,1} & \cdots & a_n \cdot c_{l,n} & c_{l,n+1} & \cdots & c_{l,2n} \end{array}\right)$$

where the $c_{i,j}$ are the elements of $\mathcal{G}$, defines a stabilizer code with respect to the standard symplectic inner product $\langle\ ,\ \rangle_s$ with the same parameters $[[n, k, d]]$.

Proof. — It is easy to show that $\mathcal{G}'$ defines a stabilizer code with respect to the standard symplectic inner product:

Let $x = (a_1x_1, \ldots, a_nx_n, x_{n+1}, \ldots, x_{2n}), y = (a_1y_1, \ldots, a_ny_n, y_{n+1}, \ldots, y_{2n}) \in C'$, then

$$\langle x, y\rangle_s \quad = \quad \sum_{i=1}^{n} (a_ix_i) \cdot y_{n+i} - x_{n+i} \cdot (a_iy_i) \quad = \quad 0$$

because $(x_1, \ldots, x_{2n}), (y_1, \ldots, y_{2n}) \in C$ and C is a stabilizer code with respect to $\langle\ ,\ \rangle_s^a$. Therefore C' is a stabilizer code.

The reason why the parameters $[[n, k, d]]$ do not change when going to $\mathcal{G}'$ is the following:

- The code length n stays the same, because all codewords still have the length $2n$.
- The number of encoded qudits also does not change, because $\mathcal{G}' = \mathcal{G} \cdot D$ where $D = \mathrm{diag}(a_1, \ldots, a_n, 1, \ldots, 1)$. Since $D \in \mathrm{GL}(2n, \mathbb{F}_{p^m})$, we have that $\mathcal{G}$ and $\mathcal{G}'$ have the same rank.
- The distance d of the code could only change, if the weights of the normalizer elements change. This is not possible, because all coefficients $a_i \neq 0$ and $\mathbb{F}_{p^m}$ is a field and has no zero divisors. Therefore the weights stay the same and the distance of the code, too, because

  $$d \quad = \quad \min\{wt(x) \mid x \in N(S) \backslash S\}.$$

  Detailed descriptions about the distance of a quantum code can be found in [**11**].

□

3. Some results about Goppa codes

This section summarises some results about towers of function fields, Goppa codes (also called AG codes), and their transformation to quantum codes in order to provide a method to construct asymptotically good quantum Goppa codes (or quantum AG codes). The following theorems and propositions provide all preliminaries for the proof of the main result, Theorem 4.1, of this paper.

The following theorem is a short version of Theorem 1.7 and Proposition 4.4 of [**14**] by H. Stichtenoth.

Theorem 3.1. — *Let $q = p^{2r}$ be a square, $p > 2$ a prime, $r \geq 1$. Then there exists a tower of function fields (F_i) over $\mathbb{F}_q$ of transcendental degree one such that:*

1. *The number of rational places of F_i is given by $N(F_i) = 2n_i + k_i$ where $k_i/g(F_i) \longrightarrow 0$ and*
$$\frac{n_i}{g(F_i)} \longrightarrow \frac{\sqrt{q}-1}{2}.$$
2. *There exists an automorphism σ_i of F_i of order 2, a differential η_i of F_i, and rational places $P_1, \ldots, P_{n_i}$ such that the $2n_i$ rational places are given by $P_1^{(i)}, \sigma_i P_1^{(i)}, \ldots, P_{n_i}^{(i)}, \sigma_i P_{n_i}^{(i)}$, pairwise different. Furthermore we have:*
   (a) *All differentials η_i satisfy*
   $$\sigma_i(\eta_i) \;=\; -\eta_i.$$
   (b) *$(\eta_i) = -D_i + A_i$ with $D_i = P_1 + \sigma_i P_1 + \cdots + P_{n_i} + \sigma_i P_{n_i}$, $(\deg D_i = 2n_i)$, $A_i \geq 0$, and $\operatorname{supp}(A_i) \cap \operatorname{supp}(D_i) = \emptyset$.*

Proof. —

1. Theorem 1.7 (j) in [**14**] states that $N(F_i)/g(F_i) \to \sqrt{q} - 1$ and that the place P_1 corresponding to $(1 - z)$ in the rational function field $\mathbb{F}_q(z)$ is completely splitting in all extensions. We define $N(F_i) = 2\,n_i + k_i$ and $2\,n_i$ is the number of places over P_1 in the extension F_i. We get from [**14**, Thm. 1.7]:
$$\begin{aligned} \frac{n_i}{g(F_i)} &\to \frac{\sqrt{q}-1}{2} \\ \frac{k_i}{g(F_i)} &\to 0. \end{aligned}$$
2. (a) The differential is given in [**14**] by $\eta = dw/(1 - z)$ with $w^{\sqrt{q}-1} = z$ and $\mathbb{F}_q(z)$ is the rational function field. Take an automorphism σ of order two. An automorphism like that exists because of Sylow's Theorem: The order of the group of automorphisms of F_i over the rational function field is $2n_i$, because $\deg(F_i/\mathbb{F}_q(z)) = 2n_i$ and $F_i/\mathbb{F}_q(z)$ is Galois. Therefore it is divisible by two, a prime number, and by Sylow's Theorem there exists an automorphism of order two. This automorphism can be chosen to map

w to $-w$ and to permute the support of A_i, because A_i is the pole and zero divisor of w. So we have for z:

$$\sigma(z) = \sigma(w^{\sqrt{q}-1}) = (-w)^{\sqrt{q}-1} = z,$$

and therefore for the differential η

$$\sigma(\eta) = \sigma(\frac{dw}{1-z}) = \frac{d\,\sigma(w)}{\sigma(1)-\sigma(z)}$$
$$= \frac{-dw}{1-z} = -\eta.$$

(b) The last statement is exactly [**14**, Prop. 4.4 (i)].

□

To use such a tower of function fields, we need the following proposition and corollaries. They provide the necessary machinery to use classical coding theory for the construction of quantum stabilizer codes. Proposition 3.2 is a generalisation of [**10**, Prop. 1].

Proposition 3.2. — *Let $F/\mathbb{F}_q$ be an algebraic function field, σ an automorphism of F of order two not moving elements in $\mathbb{F}_q$, and $P_1, \ldots, P_n$ pairwise distinct places of degree one such that $\sigma P_i \neq P_j$ for all $i, j = 1, \ldots, n$, $D = P_1 + \cdots + P_n + \sigma P_1 + \cdots + \sigma P_n$. Let η be a differential with the properties*

$$\begin{cases} v_{P_i}(\eta) = v_{\sigma P_i}(\eta) = -1, \\ \mathrm{res}_{P_i}(\eta) = -\mathrm{res}_{\sigma P_i}(\eta). \end{cases}$$

Further assume that we have a divisor G such that $\sigma G = G$, $v_{P_i}(G) = v_{\sigma P_i}(G) = 0$. Define

$$C(D,G) = \{(f(P_1), \ldots, f(P_n), f(\sigma P_1), \ldots, f(\sigma P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^{2n}.$$

Let $H = D - G + (\eta)$, then we have $C(D,G)^{\perp_s^a} = C(D,H)$ where

$$a = (a_1, \ldots, a_n) = (\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta))$$

and the elements a_i are the weights of the symplectic inner product $\langle x, y\rangle_s^a = \sum_{i=1}^n a_i\,(x_i\,y_{n+i} - x_{n+i}\,y_i)$.

Proof. — The proof is similar to the one of [**10**, Prop. 1]. The only difference is the more general assumption that $\mathrm{res}_{P_i}(\eta) = -\mathrm{res}_{\sigma P_i}(\eta)$, instead of 1 and -1. □

Corollary 3.3. — *For $G \leq H$, G and H as in Proposition 3.2, we have $C(D,G) \subseteq C(D,H)$. If we multiply*

$$C'(D,G) = C(D,G) \cdot \mathrm{diag}(\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta), 1, \ldots, 1)$$

then C' is a linear self-orthogonal code with respect to the standard symplectic inner product. This code modification does not change the code properties and defines a quantum stabilizer code, called a quantum Goppa code.

Proof. — Proposition 3.2 yields $C(D,G)^{\perp_s^a} = C(D,H)$ and as $H \geq G$, it follows $C(D,G) \subseteq C(D,H) = C(D,G)^{\perp_s^a}$. Hence we can apply Lemma 2.1 and the corollary is proven. □

Corollary 3.4 ([**10**, Cor. 3]). — *We use the same notations as in Proposition 3.2. Furthermore, we assume that $G \leq H$. Then we can construct an $[[n, k, d]]$ quantum code Q, where*

$$k = \dim H - \dim(H - D) - n.$$

For the minimum distance d of Q, we have

$$d \geq n - \left\lfloor \frac{\deg H}{2} \right\rfloor.$$

4. Construction of asymptotically good quantum codes

In the following section we will construct families of quantum Goppa codes over nonbinary finite fields. The main idea of this construction goes back to the construction of good binary quantum codes [**10**] and of quantum Goppa codes over hyperelliptic curves [**11**].

Theorem 4.1. — *Let $q = p^m$, $p > 2$ prime, m even. Furthermore let (F_i) be the tower of function fields over $\mathbb{F}_q$ constructed in Theorem 3.1. Then this tower yields the construction of a family of $([[n_i, k_i, d_i]])_{i\in\mathbb{N}}$ quantum Goppa codes with limits*

$$\begin{aligned} \lim_{i\to\infty} n_i &= +\infty, \\ \liminf_{i\to\infty} \frac{k_i}{n_i} &\geq R, \\ \liminf_{i\to\infty} \frac{d_i}{n_i} &\geq \frac{1-R}{2} - \frac{1}{\sqrt{q}-1}, \end{aligned}$$

where R can be chosen with $0 \leq R \leq 1 - 2/(\sqrt{q}-1)$.

The limits of the quantum code projected onto the base field are given by

$$\begin{aligned} \lim_{i\to\infty} n_i &= +\infty, \\ \liminf_{i\to\infty} \frac{k_i}{n_i} &\geq R, \\ \liminf_{i\to\infty} \frac{d_i}{n_i} &\geq \frac{1-R}{2m} - \frac{1}{m(\sqrt{q}-1)}. \end{aligned}$$

Proof. — We use the notation of Theorem 3.1.

Let A_i be given by Theorem 3.1 and denoted by $A_i = \sum_{j\in I_i} t_j T_j$ and σ_i as in Theorem 3.1. Let G_i be chosen $G_i = \sum_{j\in I_i} l_j T_j$ with $0 \leq l_j \leq 1/2\, t_j$ for all j, $l_j \in \mathbb{Z}$

such that $\sigma_i G_i = G_i$. The elements l_j will be fixed later on, we think of them as variables. Then H_i satisfies

$$\begin{aligned} H_i &= D_i - G_i + (\eta_i) = D_i - G_i - D_i + A_i \\ &= -\sum_{j \in I_i} l_j T_j + \sum_{j \in I_i} t_j T_j = \sum_{j \in I_i} (t_j - l_j) T_j \\ &\geq G_i. \end{aligned}$$

The last equation follows because $l_j \leq 1/2\, t_j$ and therefore $l_j \leq (t_j - l_j)$ for all j.

Let the coefficients l_j be chosen such that $n_i + g_i - 1 \leq \deg H_i < 2n_i$ where g_i is the genus of F_i. Furthermore let $r_i = \deg H_i - (n_i + g_i - 1)$.

We use the pairs of rational places $(P_j, \sigma_i P_j)$ with the automorphism σ_i of order two that satisfies $\sigma_i G_i = G_i$ and the differential η_i with $(\eta_i) = -D_i + A_i$ given by Theorem 3.1.

The properties of η_i and σ_i imply that

$$\operatorname{res}_{\sigma_i P_j}(\eta_i) = \operatorname{res}_{P_j}(\sigma_i \eta_i) = -\operatorname{res}_{P_j}(\eta_i).$$

With Proposition 3.2, and Corollary 3.3 we can construct an $[[n_i, k_i, d_i]]$ quantum Goppa code C_i. Its code properties can be calculated by Corollary 3.4:

$$\begin{aligned} d_i &\geq n_i - \left\lfloor \frac{\deg H_i}{2} \right\rfloor \\ &\geq n_i - \frac{n_i + g_i - 1 + r_i}{2} = \frac{n_i - g_i + 1 - r_i}{2}. \end{aligned}$$

And for k_i we have to consider that

$$\begin{aligned} \deg(H_i - D_i) &= \deg H_i - \deg D_i \\ &= \deg H_i - 2n_i < 0. \end{aligned}$$

Therefore we know that $\dim(H_i - D_i) = 0$ [**13**, I.4.12]. So we get for k_i:

$$\begin{aligned} k_i &= \dim H_i - \dim(H_i - D_i) - n_i \\ &\geq \deg H_i + 1 - g_i - n_i \\ &= n_i + g_i - 1 + r_i + 1 - g_i - n_i = r_i. \end{aligned}$$

Now we define R to be given by $r_i = \lfloor R n_i \rfloor$, $0 \leq R \leq 1 - 2/(\sqrt{q} - 1)$. The choice of R fixes our elements l_j. Therefore we can calculate the following limits

$$\begin{aligned} \liminf_{i \to \infty} \frac{k_i}{n_i} &\geq \liminf_{i \to \infty} \frac{r_i}{n_i} \geq R, \\ \liminf_{i \to \infty} \frac{d_i}{n_i} &\geq \liminf_{i \to \infty} \frac{n_i - g_i + 1 - r_i}{2n_i} \\ &\geq \frac{1 - R}{2} - \liminf_{i \to \infty} \frac{g_i}{2n_i} \\ &= \frac{1 - R}{2} - \frac{1}{\sqrt{q} - 1}. \end{aligned}$$

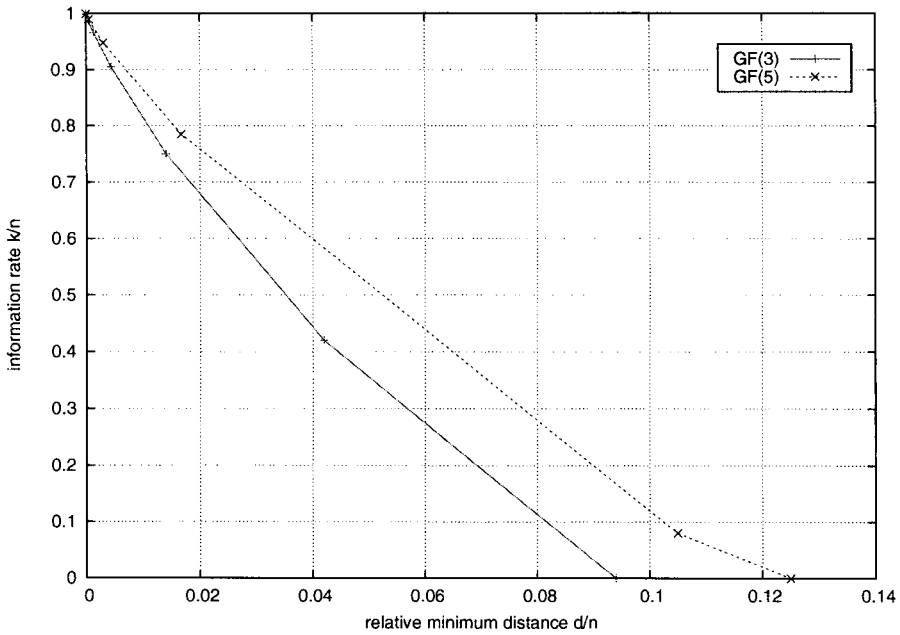

FIGURE 1. Asymptotically good family of quantum codes constructed in Section 4 over $\mathbb{F}_3$ and $\mathbb{F}_5$.

The projected code $[[n_i^p, k_i^p, d_i^p]]$ leads to

$$\begin{aligned} \liminf_{i\to\infty} \frac{k_i^p}{n_i^p} &\geq \liminf_{i\to\infty} \frac{m\,k_i}{m\,n_i} \geq R, \\ \liminf_{i\to\infty} \frac{d_i^p}{n_i^p} &\geq \liminf_{i\to\infty} \frac{d_i}{m\,n_i} \\ &\geq \frac{1-R}{2m} - \frac{1}{m(\sqrt{q}-1)}. \end{aligned}$$

For a detailed describtion of how to project quantum codes see [**11**]. □

If we calculate the properties of the constructed quantum codes projected onto $\mathbb{F}_3$ and $\mathbb{F}_5$ over $\mathbb{F}_{3^m}$ and $\mathbb{F}_{5^m}$, we get the limits shown in Figure 1.

5. Comparison of constructed code and quantum Gilbert-Varshamov bound

If we do not project the codes onto the base field, most of them will have asymptotics that lie above the quantum Gilbert-Varshamov bound. One example is given

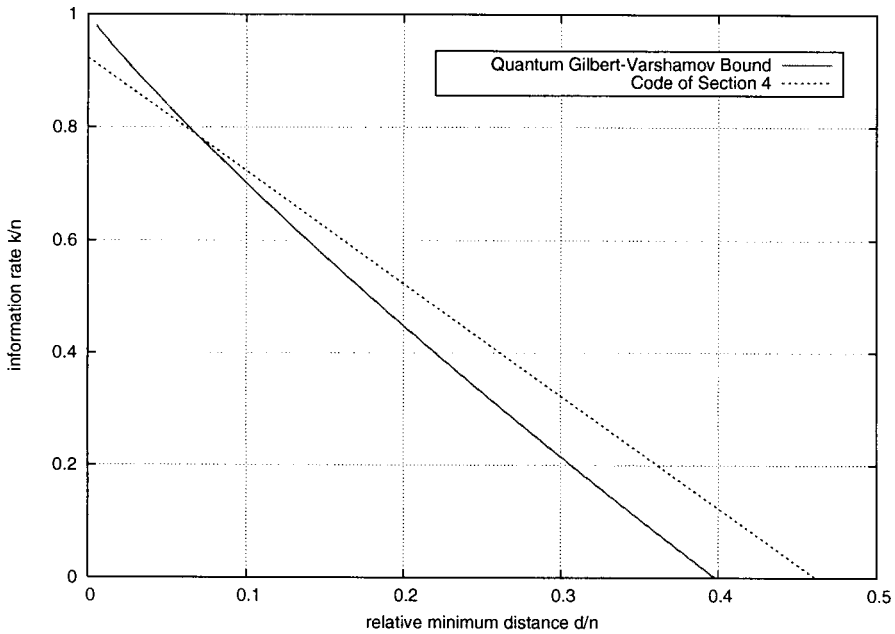

FIGURE 2. This figure shows that the asymptotics of the constructed code lie partly above the quantum Gilbert-Varshamov bound over the field $\mathbb{F}_{36}$

in Figure 2. The quantum Gilbert-Varshamov bound over $\mathbb{F}_{q^2}$ is given by

$$\frac{q^{n-k+2}-1}{q^2-1} \geq \sum_{i=1}^{d-1}(q^2-1)^{i-1}\binom{n}{i}$$

or in logarithmic notation by

$$\frac{k}{n} \geq 1 - 2H_{q^2}\left(\frac{d}{n}\right)$$

where we define the r-ary entropy function as usal by

$$H_r(\delta) = -\delta\log_r(\delta) - (1-\delta)\log_r(1-\delta) + \delta\log_r(r-1).$$

In general, all codes construced in Section 4 over a finite field with at least 81 elements are partly better than the quantum Gilbert-Varshamov bound. This is proven in the following theorem:

Theorem 5.1. — *Let $q = p^r$ be a prime power with $q \geq 9$. Then the family of quantum Goppa codes over $\mathbb{F}_{q^2}$ constructed in Section 4 exceeds the quantum Gilbert-Varshamov bound in its asymptotics.*

Proof. — Let us denote the asymptotics k/n by κ and d/n by δ. For the constructed code of Section 4 we have

$$\kappa_c = 1 - 2\delta - \frac{2}{q-1},$$

which is a linear monotone decreasing function in d.

The quantum Gilbert-Varshamov bound is given by

$$\begin{aligned} \kappa_{gv} &= 1 - 2H_{q^2}(\delta) \\ &= 1 - 2(-\delta \log_{q^2} \delta - (1-\delta)\log_{q^2}(1-\delta) + \delta \log_{q^2}(q^2-1)). \end{aligned}$$

This function is convex in δ as the second derivative is strictly greater than zero. It has a minimum in $\delta = (q^2-1)/q^2 > 1/2$ for $q > \sqrt{2}$. We are only interested in those values of δ where $\kappa_c \geq 0$, therefore $0 \leq \delta \leq 1/2$. The field size is by definition $q \geq 3$. Therefore the Gilbert-Varshamov bound is strictly decreasing in the considered part.

Because κ_{gv} is convex, the two graphs will have at most two intersection points. For $\delta = 0$ the Gilbert-Varshamov bound is equal to one and therefore greater than the constructed code value κ_c for a fixed field $\mathbb{F}_{q^2}$. So it suffices to show that for $\kappa_c = 0$ it holds that $\kappa_c > \kappa_{gv}$ for all $q \geq 9$, because then the two graphs must have an intersection point and the graph of the code constructed in Section 4 lies partly above the Gilbert-Varshamov bound. For $1 - 2\delta - 2/(q-1) = 0$ we have:

$$\kappa_{gv}(\kappa_c = 0) = 1 - 2(-\delta \log_{q^2} \delta - (1-\delta)\log_{q^2}(1-\delta) + \delta \log_{q^2}(q^2-1))$$

Easy calculations show that this expression is smaller than zero for $q \geq 9$:

$$k_{gv}(k_c = 0) \leq 1 - 2\left(\frac{3}{8}\log_{81}\frac{8}{3} + \frac{1}{2}\log_{81} 2 + \frac{3}{8}\log_{81} 80\right) < 0.$$

Therefore for all $q \geq 9$ the constructed code exceeds the quantum Gilbert-Varshamov bound. □

Acknowledgements

The author would like to thank H. Stichtenoth for the useful discussions and to provide his result Theorem 3.1 prior to publication and M. Rötteler for the supervision during the diploma thesis. Also thank you to C. Hertling and J. Potthoff for the helpful discussions.

References

[1] A. Ashikhmin & E. Knill – "Nonbinary quantum stabilizer codes", *Transactions on Information Theory* **47** (2001), no. 7, p. 3065–3072.

[2] A. Ashikhmin, S. Litsyn & M. A. Tsfasman – "Asymptotically good quantum codes", *Phys. Rev. A* **63** (2001), no. 3, p. 032311.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor & N. J. A. Sloane – "Quantum error correction via codes over GF(4)", *IEEE Transactions on Information Theory* **44** (1998), no. 4, p. 1369–1387, see also LANL preprint quant-ph/9608006.

[4] A. R. CALDERBANK & P. W. SHOR – "Good quantum error-correcting codes exist", *Physical Review A* **54** (1996), no. 2, p. 1098–1105, see also LANL preprint quant-ph/9512032.

[5] H. CHEN – "Some good quantum error-correcting codes from algebraic geometry codes", *IEEE Transactions on Information Theory* **47** (2001), no. 5, p. 2059–2061.

[6] H. CHEN, S. LING & C. XING – "Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound", *IEEE Transactions on Information Theory* **47** (2001), no. 5, p. 2055–2058.

[7] D. GOTTESMAN – "Class of quantum error-correcting codes saturating the quantum hamming bound", *Phys. Rev. A* **54** (1996), no. 3, p. 1862–1868.

[8] M. GRASSL, T. BETH & M. RÖTTELER – "Efficient quantum circuits for non-qubit quantum error-correcting codes", *International Journal of Foundation of Computer Science* **47** (2003), no. 5, p. 757–775.

[9] J.-L. KIM & J. WALKER – "Nonbinary quantum error-correcting codes from algebraic curves", submitted for publication, 2004.

[10] R. MATSUMOTO – "Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes", *IEEE Transactions on Information Theory* **48** (2002), no. 7, p. 2122–2124.

[11] A. NIEHAGE – *Quantum Goppa codes over hyperelliptic curves*, Master's Thesis, University of Mannheim, Germany, 2004, see also LANL preprint quant-ph/0501074.

[12] E. M. RAINS – "Nonbinary quantum codes", *IEEE Transactions on Information Theory* **45** (1999), no. 6, p. 1827–1832, see also LANL preprint quant-ph/9703048.

[13] H. STICHENOTH – *Algebraic function fields and codes*, Springer, 1993.

[14] H. STICHTENOTH – "Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound", publication in preparation, 2005.

September 2005

ANNIKA NIEHAGE, Universität Mannheim, Fakultät für Mathematik und Informatik, 68131 Mannheim, Germany • *E-mail :* aniehage@math.uni-mannheim.de
Url : http://ls5.math.uni-mannheim.de