Quantum twisted codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)
Yves Edel
Mathematisches Institut der Universität
Im Neuenheimer Feld 288
69120 Heidelberg (Germany)

January 18, 1999

1 Introduction

The translation from quantum error correcting codes to the language of error-correcting codes as given in [1] leads to quaternary codes, which are linear over $\mathbb{F}_2$. For background and motivation the reader is advised to consult [1] and its extensive bibliography. It is natural to consider a generalization from $\mathbb{F}_2$ to an arbitrary finite ground field $\mathbb{F}_q$. This motivates the following Definition:

Definition 1 *Let $E = V(2,q) = \mathbb{F}_q^2$ be the 2-dimensional vector space over $\mathbb{F}_q$. An $\mathbb{F}_q-$linear* **quantum code** *$[[n,k,d]]_q$ is an $\mathbb{F}_q-$subspace $\mathcal{C} \subset E^n$, which satisfies the following conditions:*

1. *$\mathcal{C}$ has $\mathbb{F}_q-$dimension $n-k$.*

2. *$\mathcal{C} \subseteq \mathcal{C}^\perp$. Here the dual is taken with respect to an $I\!F_q-$linear symplectic scalar product on E^n, where each copy of E is a hyperbolic plane.*

3. *The elements in $\mathcal{C}^\perp \setminus \mathcal{C}$ have weight $\geq d$.*

$\mathcal{C}$ is **pure** if $\mathcal{C}^\perp$ has minimum distance d. The highest value of k, which makes sense, is $k = n$. Then $\mathcal{C}$ is the 0-code, its dual is the whole space and we have a code $[[n, n, 1]]_q$. This is not very interesting. The opposite extreme is $k = 0$. In this case $\mathcal{C}$ is self-dual. The convention is to define d as the minimum nonzero weight of $\mathcal{C}$ in this case. We want to apply a variant of our theory of twisted BCH-codes as developed in [2].
As we are going to work in symplectic geometry let us fix notation: Let $V = V(2n, q)$ be a $2n$-dimensional vector space, endowed with a non-degenerate symplectic bilinear form $<,>$. A **hyperbolic plane** is a 2-dimensional subspace $H \subset V$, such that the restriction of $<,>$ to H is non-degenerate. A **symplectic basis** of V is a basis $\{v_j | j = 1, 2, \ldots, n\} \cup \{w_j | j = 1, 2, \ldots, n\}$, where $< v_j, v_k >=< w_j, w_k >= 0, < v_j, w_k >= \delta_{jk} = - < w_j, v_k >$. In particular V is the orthogonal sum of the hyperbolic planes $H_j = v_j I\!F_q + w_j I\!F_q$.

2 The contribution of linear codes

We use the terminology of the introduction. Let $F = I\!F_{q^2}$ and $\overline{x} = x^q$ the **conjugate** of $x \in F$. Let $\mathcal{C}$ be an F-linear code of length n, which is self-orthogonal ($\mathcal{C} \subseteq \mathcal{C}^\perp$) with respect to the hermitian form. This means that whenever $(x_1, x_2, \ldots, x_n) \in \mathcal{C}$ and $(y_1, y_2, \ldots, y_n) \in \mathcal{C}$ we have

$$\sum_{i=1}^{n} x_i \overline{y_i} = 0.$$

Let $\Phi : F \longrightarrow I\!F_q$ be a surjective $I\!F_q-$linear mapping. Choose a basis $\{\omega_1, \omega_2\}$ of $F \mid I\!F_q$, expand $x \in F$ in the form $x = \alpha_1(x)\omega_1 + \alpha_2(x)\omega_2$. This gives us an $I\!F_q$-isomorphism from $\mathcal{C}$ to the $I\!F_q$-linear code $\mathcal{C}'$ of length $2n$, where

$$(x_1, \ldots, x_n) \mapsto (\alpha_1(x_1), \alpha_2(x_1), \ldots, \alpha_1(x_n), \alpha_2(x_n)).$$

We claim that Φ, ω_1, ω_2 can be chosen such that $\mathcal{C}'$ is self-orthogonal with respect to the symplectic scalar product. This will prove the following generalization of [1], Theorem 3.

Theorem 1 *Let $\mathcal{C}$ be an $\mathbb{F}_{q^2}-$linear code of length n, dimension $n-k$ and dual distance d, which is self-orthogonal with respect to the Hermitian inner product. Then there is an $\mathbb{F}_q$-isomorphism from $\mathcal{C}$ to $\mathcal{C}'$ such that $\mathcal{C}'$ is an $\mathbb{F}_q-$ linear q^2-ary code, which is self-orthogonal with respect to the symplectic form and yields a pure quantum code $[[n, 2k-n, d]]_q$.*

Proof: Choose $0 \neq \gamma \in F$ such that $tr(\gamma) = 0$ and define Φ by $\Phi(x) = tr(\gamma x)$. Here $tr : F \longrightarrow \mathbb{F}_q$ is the **trace.** If $x \in \mathbb{F}_q$, then $\Phi(x) = tr(\gamma x) = xtr(\gamma) = 0$. As before consider $(x_1, x_2, \ldots, x_n) \in \mathcal{C}$ and $(y_1, y_2, \ldots, y_n) \in \mathcal{C}$. We have $\sum_{i=1}^n x_i\overline{y_i} = 0$. Using the basis $\{\omega_1, \omega_2\}$ we obtain

$$x_i\overline{y_i} = \alpha_1(x_i)\alpha_1(y_i)\omega_1\overline{\omega_1} + \alpha_2(x_i)\alpha_2(y_i)\omega_2\overline{\omega_2}+$$

$$+\alpha_1(x_i)\alpha_2(y_i)\omega_1\overline{\omega_2} + \alpha_1(y_i)\alpha_2(x_i)\omega_2\overline{\omega_1}$$

As $\omega_j\overline{\omega_j} \in \mathbb{F}_q$ we see that Φ vanishes on the first two summands. Comparison with the symplectic form shows that it suffices to choose the basis such that $\Phi(\omega_1\overline{\omega_2}) = 1$ and $\Phi(\omega_2\overline{\omega_1}) = -1$. Let $\alpha \in F$ such that $tr(\gamma\alpha) = 1$. Choose ω_1 as an arbitrary nonzero element of F, let ω_2 be determined by $\alpha = \omega_1\overline{\omega_2}$. ω_1, ω_2 do form a basis (if $\omega_2 = \lambda\omega_1$ for some $\lambda \in \mathbb{F}_q$, then $tr(\gamma\alpha) = 0$, contradiction). We have $\Phi(\omega_1\overline{\omega_2}) = tr(\gamma\alpha) = 1$. Further $tr(\gamma\alpha + \gamma\overline{\alpha}) = tr(\gamma tr(\alpha)) = tr(\alpha)tr(\gamma) = 0$. It follows $\Phi(\omega_2\overline{\omega_1}) = -1$.

3 Twisted codes

In this section we develop the theory of twisted codes as far as it applies to the problem at hand. Our approach is somewhat different from the method used in [2]. Also, we specialize the theory of twisted codes in two respects: we consider only the quadratic case and we choose the underlying bilinear form to be symplectic.

Let $F = \mathbb{F}_{q^r}$ and E a 2-dimensional $\mathbb{F}_q-$vector space (the fact that $dim_{F_q}(E) = 2$ expresses the fact that we are in the quadratic case). Let $\Phi : F \longrightarrow E$ be a surjective $\mathbb{F}_q-$linear mapping. We fix a divisor $n|(q^r - 1)$ and a subset $A \subset \mathbb{Z}/n\mathbb{Z}$. Consider the array $\mathcal{B}(A) = \mathcal{B}(A, n, q)$. The columns of $\mathcal{B}(A)$ are indexed by the elements u of the subgroup W of order n of F^*. Let $\mathcal{P}(A) = \{\sum_{i\in A} a_i X^i | a_i \in F\}$. The rows of $\mathcal{B}(A)$ are indexed by the polynomials $p(X) \in \mathcal{P}(A)$. The entry in row $p(X)$ and column $u \in W$ is defined as $p(u)$.

Definition 2 *Identify E with $\mathbb{F}_q^2$. Then every row of $\Phi(\mathcal{B}(A, n, q))$ can be seen as a $2n-$tuple over $\mathbb{F}_q$. Fix a nondegenerate symplectic $\mathbb{F}_q$-bilinear form $<,>$ on $V = E^n = \mathbb{F}_q^{2n}$ with symplectic basis $\{v_u | u \in W\} \cup \{w_u | u \in W\}$. Then V is the orthogonal sum of the hyperbolic planes H_u generated by v_u and w_u. Define $\mathcal{C}(A) = \mathcal{C}(A, n, \Phi) = (\Phi(\mathcal{B}(A)))^\perp$, where the orthogonal is with respect to the symplectic form $<,>$ in V.*

Let $tr : F \longrightarrow \mathbb{F}_q$ be the **trace.** We can find $\gamma_1, \gamma_2 \in F$ such that $\Phi(x) = (tr(\gamma_1 x), tr(\gamma_2 x))$. If we replace γ_i by $\gamma\gamma_i$, this has the effect of a permutation of the rows of $\Phi(\mathcal{B}(A))$. It follows that we can assume without restriction

$$\Phi(x) = ((tr(x), tr(\gamma x)) \text{ for some } \gamma \in F \setminus \mathbb{F}_q.$$

Here the condition $\gamma \notin \mathbb{F}_q$ assures that Φ is onto. It follows that Φ is determined by the choice of γ. An important parameter is the degree $\kappa = [\mathbb{F}_q(\gamma) \mid \mathbb{F}_q]$. We note that $\kappa > 1$ can be chosen among the divisors of r.

Our first and most difficult aim is the determination of the $\mathbb{F}_q-$dimension of $\mathcal{C}(A)$.

4 The dimension of twisted codes

Definition 3 *Call a polynomial $p(X) \in F[X]$* **cyclotomic** *if all the exponents of its nonzero monomials belong to the same* **cyclotomic coset**. *Here* *a* **cyclotomic coset** *is an orbit of the Galois group* $G = Gal(F|\mathbb{F}_q)$ *in its operation on the integers mod* n*. Recall that the Frobenius automorphism operates as multiplication by* q *and that* G*, a cyclic group of order* r*, consists of the powers of the Frobenius automorphism.*

Clearly $dim(\mathcal{C}(A)) = 2n - dim(\Phi(\mathcal{B}(A)))$, where $dim(\Phi(\mathcal{B}(A)))$ denotes the dimension of the row space of $\Phi(\mathcal{B}(A))$. We make use of the following theorem, which is all but trivial but nevertheless of fundamental importance (see Lemma 1 of [4]):

Theorem 2 *Let* $\mathcal{C}$ *be linear code over* $F = \mathbb{F}_{q^r}$*. Let* $tr : F \longrightarrow \mathbb{F}_q$ *be the trace. Assume* $\mathcal{C} = \mathcal{C}^q$ *(*$\mathcal{C}$ *is* **Galois invariant***). Then the following hold:*

- $tr(\mathcal{C}) = \mathcal{C}|_{F_q}$*.*
- *The* $\mathbb{F}_q$*-dimension of* $tr(\mathcal{C})$ *equals the* F*-dimension of* $\mathcal{C}$*.*

Let $\mathcal{B} \subset F^n$ be an F-linear code. We define $(\mathcal{B}, \gamma\mathcal{B}) = \{(v \mid \gamma{\cdot}v) \mid v \in \mathcal{B}\}$, a code of length $2n$ and the same dimension as $\mathcal{B}$. By definition of Φ we have $\Phi(\mathcal{B}(A)) = tr((\mathcal{B}(A), \gamma \cdot \mathcal{B}(A)))$. Finally let $\mathcal{D}(A) = \mathcal{D}_\gamma(A)$ be the **Galois closure** of $(\mathcal{B}(A), \gamma \cdot \mathcal{B}(A))$, that is the smallest code containing $(\mathcal{B}(A), \gamma \cdot \mathcal{B}(A))$, which is Galois invariant. Theorem 2 yields the following:

Theorem 3 $dim_{F_q}(\mathcal{C}(A)) = 2n - dim_F(\mathcal{D}(A))$*, where* $\mathcal{D}(A)$ *is the Galois closure of* $(\mathcal{B}(A), \gamma \cdot \mathcal{B}(A))$*.*

We will determine the dimension $d(A)$ of the F-linear code $\mathcal{D}(A)$ (see Theorem 3). It will be convenient to identify the row of $\mathcal{B}(A)$ indexed by polynomial $p(X)$ with that polynomial itself. In this notation the elements of $(\mathcal{B}(A), \gamma{\cdot}\mathcal{B}(A))$ are the pairs $(p(X), \gamma{\cdot}p(X))$, where $p(X) \in \mathcal{P}(A)$. We define a symplectic structure on the underlying space F^{2n}, which we can view as a tensor product $V \otimes_{F_q} F$. In our short notation $V \otimes_{F_q} F = \{(p(X), q(X)) \mid deg(p(X)), deg(q(X)) < n\}$. We use the same symplectic basis and the same symbol for the symplectic scalar product. This scalar product on $V \otimes_{F_q} F$ is then as follows:

$$< (p(X), q(X)), (p'(X), q'(X)) >= \sum_{u \in W} p(u)q'(u) - q(u)p'(u).$$

Lemma 1 *Let Z be a cyclotomic coset. Denote by $(V \otimes_{F_q} F)_Z$ the set of all $(p(X), q(X))$, where $p(X), q(X) \in \mathcal{P}(Z)$. Then $dim((V \otimes_{F_q} F)_Z) = 2 \mid Z \mid$,*

$$V \otimes_{F_q} F = \bigoplus_Z (V \otimes_{F_q} F)_Z$$

and $(V \otimes_{F_q} F)_Z^{\perp}$ is the sum of all $(V \otimes_{F_q} F)_{Z'}$, where $Z' \neq -Z$.

This is almost trivial. The last statement of the lemma follows from the fact that $\sum_{u \in W} u^i = 0$ unless i is a multiple of n. If $p(X) \in \mathcal{P}(Z)$, then the Galois closure of $(p(X), \gamma \cdot p(X))$ is contained in $(V \otimes_{F_q} F)_Z$. It follows that $\mathcal{D}(A)$ is the direct sum of its subspaces $\mathcal{D}_Z(A) = \mathcal{D}(A) \cap (V \otimes_{F_q} F)_Z$, where Z varies over the cyclotomic cosets. Let $d_Z(A)$ be the dimension of $\mathcal{D}_Z(A)$. We have seen $d(A) = \sum_Z d_Z(A)$ and $d_Z(A) \leq 2 \mid Z \mid$. Clearly $d_Z(A) = 0$ if $Z \cap A = \emptyset$.
Let now Z be such that $Z \cap A \neq \emptyset$. To fix notation put $Z = \{z_0, z_1, \ldots, z_{s-1}\}$ such that $z_i = z_0 q^i$ (calculation mod n). Let $z_i \in Z \cap A$. The Galois closure of $(X^{z_i}, \gamma \cdot X^{z_i})$ is

$$\mathcal{D}_{z_i}(A) = \{(\sum_{j=0}^{s-1} a_j X^{z_j}, \sum_{j=0}^{s-1} \gamma^{q^{i-j+\nu s}} a_j X^{z_j}) \mid a_j \in F, \nu = 0, \ldots, r/s - 1\}$$

Assume we have $\gamma^{q^{i-j+\nu s}} \neq \gamma^{q^{i-j}}$ for some choice of ν. This is equivalent with κ not dividing s and we have $dim(\mathcal{D}_{z_i}(A)) = 2s$ in this case, hence $\mathcal{D}_Z(A) = (V \otimes_{F_q} F)_Z$. So assume $\kappa \mid s$. We have $dim(\mathcal{D}_{z_i}(A)) = s$ whenever $z_i \in Z \cap A$, and $\mathcal{D}_Z(A)$ is the sum of the spaces $\mathcal{D}_z(A)$, where z varies over $Z \cap A$. Let now z_i and $z_{i'}$ be different elements in $Z \cap A$. Assume $\mathcal{D}_{z_i}(A) \neq \mathcal{D}_{z_{i'}}(A)$. The description of these spaces shows that they intersect in the 0-space then. It follows that $d_Z(A) = 2s$ in this case as well. We see that $\mathcal{D}_{z_i}(A) = \mathcal{D}_{z_{i'}}(A)$ is now equivalent with $\gamma^{q^{i-j}} = \gamma^{q^{i'-j}}$ for all j, which in turn is equivalent with $\gamma^{q^{i-i'}} = \gamma$. The definition of κ shows that it is equivalent with $i-i'$ being a multiple of κ. As the $\kappa-$th power of the Frobenius automorphism generates the subgroup H of order r/κ of the Galois group we are led to the following:

Definition 4 *Let $A \subset \mathbb{Z}/n\mathbb{Z}$ and let $Z \subset \mathbb{Z}/n\mathbb{Z}$ be a cyclotomic coset such that $Z \cap A \neq \emptyset$. We call $Z \cap A$* **unsaturated** *if $\kappa| \mid Z \mid$ and the subgroup H of order r/κ of the Galois group G is transitive on $Z \cap A$.*

In case $\kappa = r$ we have that $Z \cap A$ is unsaturated if and only if Z has full length r and $\mid Z \cap A \mid = 1$. We have seen the following:

Theorem 4 *The dimension $d(A)$ of the Galois closure $\mathcal{D}(A)$ of $(\mathcal{B}(A), \gamma \cdot \mathcal{B}(A))$ is $d(A) = \sum_Z d_Z(A)$, where the sum is over all cyclotomic cosets Z and*

$$d_Z(A) = \begin{cases} 0 & \textit{if } Z \cap A = \emptyset \\ s & \textit{if } Z \cap A \textit{ is unsaturated} \\ 2s & \textit{if } Z \cap A \textit{ is saturated} \end{cases}$$

It follows from Theorem 3 that we have determined the dimension of $\mathcal{C}(A)$:

Theorem 5 *The dimension $c(A)$ of $\mathcal{C}(A) = (\Phi(\mathcal{B}(A)))^{\perp}$ is $c(A) = \sum_Z c_Z(A)$, where the sum is over all cyclotomic cosets Z and*

$$c_Z(A) = \begin{cases} 2s & \textit{if } Z \cap A = \emptyset \\ s & \textit{if } Z \cap A \textit{ is unsaturated} \\ 0 & \textit{if } Z \cap A \textit{ is saturated} \end{cases}$$

5 The structure of twisted codes

The results of the preceding section lead to an almost canonical representation for the code words of $\Phi(\mathcal{B}(A))$ and its dual $\mathcal{C}(A)$. In the case of $\Phi(\mathcal{B}(A))$ we have

$$\Phi(\mathcal{B}(A)) = \bigoplus_{Z \cap A \neq \emptyset} tr(\mathcal{D}_Z(A)).$$

Here $dim_{F_q}(tr(\mathcal{D}_Z(A))) = dim_F(\mathcal{D}_Z(A)) = d_Z(A)$ (see Theorem 2). Put $\mid Z \mid = s$, fix $z \in Z$. Let $\alpha_i, i = 1, \ldots, s$ be a basis of a complement of $\mathbb{F}_{q^s}^{\perp}$ in F. Here $\perp$ is with respect to the trace form. If $Z \cap A$ is saturated, then $\mathcal{D}_Z(A) = (V \otimes_{F_q} F)_Z$. A basis of the $2s-$dimensional space $(V \otimes_{F_q} F)_Z$ is given by the words with entry $(tr(\alpha_i u^z), 0)$ in the hyperbolic plane H_u and by the words with entry $(0, tr(\alpha_i u^z))$ in H_u (see Definition 2). The fact that these words are indeed linearly independent follows from the following lemma:

Lemma 2 *With the established terminology the following holds:*

If the cyclotomic coset Z containing z has s elements, then the $\mathbb{F}_q-$subspace $< u^z \mid u \in W >$ generated by the u^z is the subfield $\mathbb{F}_{q^s}$.

Proof: We have $(u^z)^{q^s} = u^s$, hence $u^z \in \mathbb{F}_{q^s}$. On the other hand it is obvious that $< u^z \mid u \in W >$ is closed under multiplication, hence a subfield. This subfield cannot be smaller that $\mathbb{F}_{q^s}$ as otherwise $\mid Z \mid < s$.$\blacksquare$

Let now $Z \cap A$ be unsaturated. We know that $dim(tr(\mathcal{D}_Z(A))) = s$ in this case. The words with entry $(tr(\alpha_i u^z), tr(\gamma\alpha_i u^z))$ in H_u form a basis of $tr(\mathcal{D}_Z(A))$ $(i = 1, \ldots, s)$.
An analogous procedure may be used in the case of $\mathcal{C}(A)$. We have

$$\mathcal{C}(A) = \bigoplus_Z tr(\mathcal{C}_Z(A)),$$

where $\mathcal{C}_Z(A) \subseteq (V \otimes_{F_q} F)_{-Z}$ and the sum is over all Z such that $Z \cap A$ is not saturated. If $Z \cap A = \emptyset$, then $\mathcal{C}_Z(A) = (V \otimes_{F_q} F)_{-Z}$ and we have seen above how to obtain a basis of $tr((V \otimes_{F_q} F)_{-Z})$.
Let $Z \cap A$ be unsaturated. We have $dim(tr(\mathcal{C}_Z(A))) = s$. The words with entry $(tr(\alpha_i u^{-z}), tr(\gamma\alpha_i u^{-z}))$ in H_u form a basis of $tr(\mathcal{C}_Z(A))$ $(i = 1, \ldots, s)$.
This discussion also shows that duals of twisted codes are twisted codes and how the defining intervals may be obtained:

Lemma 3 *The maximum defining set $\tilde{A} \supseteq A$ such that $\mathcal{C}(\tilde{A}) = \mathcal{C}(A)$ is*

$$\tilde{A} = \bigcup_{Z \cap A \ sat} Z \cup \bigcup_{Z \cap A \ unsat} (Z \cap A)^H,$$

where $(Z \cap A)^H$ *denotes the* H*-orbit containing* $Z \cap A$.

$\Phi(\mathcal{B}(A)) = \mathcal{C}(A)^\perp = \mathcal{C}(B)$, *where*

$$B = \tilde{B} = \bigcup_{Z \cap A = \emptyset} -Z \cup \bigcup_{Z \cap A \ unsat} -(Z \cap A)^H.$$

Our bound on the minimum distance of $\mathcal{C}(A)$ is a generalization of the famous BCH-bound for cyclic codes.

Proposition 1 *If* A *contains an interval* $[l, l+t-2] = \{l, l+1, \dots, l+t-2\}$ *of* $t-1$ *consecutive numbers (mod* n*), then* $\Phi(\mathcal{B}(A))$ *is an orthogonal array of strength* $t-1$*. The minimum distance of* $\mathcal{C}(A)$ *is* $\geq t$.

In order to prove Proposition 1 we can clearly assume $A = [l, l+t-2]$. The proof that $\Phi(\mathcal{B}(A)$ has strength $t-1$ is identical to the proof of Proposition 1 in [2]. It is an easy consequence of Lagrange interpolation. The proof that $\mathcal{C}(A)$ has minimum distance $\geq t$ follows just as in the case of Theorem 1 of [2]. The only property of the bilinear form that is used is its nondegeneracy. In order to decide when $\Phi(\mathcal{B}(A))$ is a quantum code we have to determine when it is self-orthogonal

Theorem 6 *We use the notation established earlier (*$q, n \mid (q^r-1), \gamma, \Phi, \kappa, A, G$*). Moreover let* $H \subset G$ *be the subgroup of order* r/κ *of the Galois group* $G = Gal(F \mid \mathbb{F}_q)$.
Then $\Phi(\mathcal{B}(A)) \subseteq \Phi(\mathcal{B}(A)^\perp = \mathcal{C}(A)$ *if and only if the following are satisfied for all cyclotomic cosets* Z :

1. *If* $Z \cap A$ *is saturated, then* $(-Z) \cap A = \emptyset$.
2. *If* $Z \cap A$ *is unsaturated, then* H *is transitive on* $(Z \cap A) \cup -((-Z) \cap A)$ *(equivalently:* $(Z \cap A)^H = -((-Z) \cap A)^H$*).*

Proof: By our earlier discussion we see that the only critical case is when $Z \cap A$ is unsaturated. Clearly a necessary condition is that $(-Z) \cap A$ be unsaturated. The exact condition follows from Lemma 3.■

6 The parameters of quantum twisted codes

We use the terminology introduced earlier. As defining set we choose an interval $A = [l, l + t - 2]$. The mapping Φ is determined by the choice of $\gamma \in F \setminus \mathbb{F}_q$. $\Phi(\mathcal{B}(A))$ and $\mathcal{C}(A)$ are $q^2 - ary$ and $\mathbb{F}_q$-linear. They are duals of each other with respect to the symplectic scalar product. The following describes the output of our method what quantum codes are concerned.

Theorem 7 *Let $A = [l, l + t - 2]$. If $\Phi(\mathcal{B}(A)) \subseteq \mathcal{C}(A)$ and $dim(\mathcal{C}(A)) = K$, then $\Phi(\mathcal{B}(A))$ is a pure $\mathbb{F}_q$-linear quantum code $[[n, K - n, t]]_q$*

Here the dimension K of $\mathcal{C}(A)$ is determined by Theorem 5. The self-orthogonality of $\Phi(\mathcal{B}(A))$ is decided by using Theorem 6.

As a first example we construct a quantum code $[[21, 6, 5]]_2$. The cyclotomic cosets mod 21 are as follows:

cyclotomic cosets
0
1,2,4,8,16,11
3,6,12
5,10,20,19,17,13
7,14
9,15,18

As $21 \mid 2^6 - 1$ we have $r = 6$ (this is the maximum length of the cyclotomic cosets). As we aim at a code with minimum distance 5 we choose as defining set an interval of length 4. Let $A = \{1, 2, 3, 4\}$. The mapping Φ is determined by the choice of γ. We use $\gamma \in \mathbb{F}_8$, hence $\kappa = 3$. The binary dimension K of the twisted BCH-code $\mathcal{C}(A)$ is obtained from Theorem 5. The cyclotomic cosets intersecting A trivially yield a contribution of 24. $Z(3)$ intersects A only in 3. This gives another contribution of 3 to the dimension. We conclude that the additive quaternary code $\mathcal{C}(A)$ of minimum distance ≥ 5 has binary dimension 27. The conditions of Theorem 6 are trivially satisfied as for every $i \in A$ we have $Z(-i) \cap A = \emptyset$. We conclude that we have a pure quantum code $[[21, 6, 5]]_2$.

7 Standard lengthening

Theorem 8 *Consider the twisted code $\Phi(\mathcal{B}(A))$, where $A = [1, t-1]$. If $\Phi(\mathcal{B}(A))$ is a (pure) quantum code $[[n,k,t]]_q$, then its standard lengthening is a pure quantum code $[[n+1, k-1, t+1]]_q$.*

Proof: Put $A_0 = \{0\} \cup A$ and let H be a generator matrix of $\Phi(\mathcal{B}(A_0))$. As $dim(\Phi(\mathcal{B}(A_0)) = 2 + dim(\Phi(\mathcal{B}(A)))$ we have that H has $n-k+2$ rows and n columns. As $\Phi(\mathcal{B}(\{0\}))$ is a complement of $\Phi(\mathcal{B}(A))$ in $\Phi(\mathcal{B}(A_0))$ we can choose notation such that the $n-k$ first rows of H are a generator matrix of $\Phi(\mathcal{B}(A))$ and the two remaining rows are e_1^n and e_2^n, where $e_1 = (1,0), e_2 = (0,1)$. We append a $(n+1)-$st coordinate ∞. The new ambient space is $V(2(n+1),q)$, with a symplectic scalar product such that coordinate ∞ corresponds to a hyperbolic plane. A generator matrix H' of an $(n-k+2)-$dimensional code $\mathcal{D}$ is obtained by lengthening the rows of H as follows: the $n-k$ first rows of H are lengthened by $(0,0)$, the two last rows are lengthened by $(1,0) = e_1$ and $(0,-n) = -ne_2$, respectively. These last rows are then orthogonal to each other. It is now easy to see that $\mathcal{D}$ is self-orthogonal. The main points are that $\Phi(\mathcal{B}(A))$ is self-orthogonal and is orthogonal to $\Phi(\mathcal{B}(\{0\}))$ (see Theorem 6). Remains to prove that $\mathcal{D}^\perp$ has minimum distance $\geq t+1$. Assume $(v_1, v_2, \ldots, v_n, v_\infty)$ is a nonzero codeword in $\mathcal{D}^\perp$ of weight $\leq t$. If $v_\infty = (0,0)$, then we obtain a nonzero relation between t columns of H. This is impossible as $\mathcal{C}(A_0)$ has minimum distance $\geq t$ by the BCH-bound Proposition 1. If $v_\infty \neq 0$, then restriction to the first $n-k$ rows shows that we have a nontrivial linear combination involving $t-1$ columns of a generator matrix of $\Phi(\mathcal{B}(A))$. This is another contradiction.■

Continuing with our example we see that we can lengthen our quantum code $[[21,6,5]]_2$ and obtain a pure code $[[22,5,6]]_2$.

An explicit example

It follows from Section 5 that our theory yields an efficient construction for our quantum codes. The generator matrices and check matrices are essentially canonical. We illustrate by working out the construction of the quantum code $[[22,5,6]]_2$ explicitly. We are in case $q=2, n=21, r=6, \kappa=3, A=[1,4]$. We need to start from an explicit representation of the field $F=\mathbb{F}_{64}$. Choose a primitive element ϵ such that $\epsilon^6=\epsilon+1$. It is easy to see that X^6+X+1 is indeed an irreducible polynomial and that ϵ is a primitive element. As we need the trace $tr: F \longrightarrow \mathbb{F}_2$ and as the trace is constant on cyclotomic cosets mod 63 it will be handy to have a table of cyclotomic cosets mod 63 and the value of tr on each such coset

cosets mod 63	value of trace
0	0
1,2,4,8,16,32	0
3,6,12,24,48,33	0
5,10,20,40,17,34	1
7,14,28,56,49,35	0
9,18,36	0
11,22,44,25,50,37	1
13,26,52,41,19,38	0
15,30,60,57,51,39	1
21,42	1
23,46,29,58,53,43	1
27,54,45	0
31,62,61,59,55,47	1

Observe that the values on the left hand side of the table are the exponents of ϵ. The first row says $tr(\epsilon^0)=tr(1)=0$, the second rows says that $tr(\epsilon^1)=tr(\epsilon^2)=\ldots=0$.

We will describe the twisted quantum code $[[21,6,5]]_2$ by a generator matrix G of $\Phi(\mathcal{B}(A))$. The dimension of this code is $d_{Z(1)}(A)+d_{Z(3)}(A)=2\cdot 6+1\cdot 3=15$, as $Z(1)\cap A$ is saturated and $Z(3)\cap A$ is unsaturated. These cyclotomic cosets are of course mod 21. The generator matrix will have size $(15,21)$, where $Z(1)$ contributes 12 rows and $Z(3)$ gives us 3 rows. The entries of G will be written with the usual notation inherited from $\mathbb{F}_4$:

$$0 \longleftrightarrow (0,0), 1 \longleftrightarrow (1,1), \omega \longleftrightarrow (1,0), \overline{\omega} \longleftrightarrow (0,1)$$

The generator of W is ϵ^3. Index the columns by $j=0,1,\ldots,20$. The element $u \in W$ corresponding to column j is ϵ^{3j}.

Start with the rows determined by $Z(1)$. We need a basis $\alpha_1, \dots, \alpha_6$ of $F \mid \mathbb{F}_2$. A natural choice is $\alpha_1 = 1, \alpha_2 = \epsilon, \dots, \alpha_6 = \epsilon^5$. The 6 first rows $z_i, i = 1, \dots, 6$ are determined by α_i. The entry in row z_i and column j is $(tr(\epsilon^{i-1+3j}), 0)$. Observe that 0 and ω are the only entries occuring in the first six rows. The second block of six rows $z_i, i = 7, \dots, 12$ is obtained from the first block by the substitution $\omega \longleftrightarrow \overline{\omega}$.

We turn to the remaining 3 rows determined by $Z(3)$. It is clear that the trace vanishes on $\mathbb{F}_8$, hence $\mathbb{F}_8^\perp = \mathbb{F}_8$. The elements $\alpha_1, \alpha_2, \alpha_3$ have to be chosen as basis of a complement of $\mathbb{F}_8$ in F. We use $\alpha_1 = \epsilon, \alpha_2 = \epsilon^2, \alpha_3 = \epsilon^5$. Further $\gamma = \epsilon^9 \in \mathbb{F}_8 \setminus \mathbb{F}_2$. The entries in row $12 + i$ and column j are then $(tr(\alpha_i \epsilon^{9j}), tr(\alpha_i \epsilon^{9(j+1)}))$, where $i = 1, 2, 3$. This describes matrix G. The effect of standard lengthening is as follows: There is a new column ∞. The rows of G obtain entry 0 in the new column. Two new rows, constant ω and constant $\overline{\omega}$ are added. Here is the generator matrix of $[[22, 5, 6]]_2$:

$i\backslash j$	0 to 6							7 to 13							14 to 20							∞
1	0	0	0	0	0	ω	0	ω	0	0	ω	0	0	ω	ω	0	0	ω	0	ω	ω	0
2	0	0	0	ω	0	0	0	ω	ω	0	ω	ω	ω	ω	ω	ω	0	0	ω	ω	ω	0
3	0	ω	0	ω	0	ω	ω	ω	0	ω	0	0	0	0	ω	ω	ω	ω	0	ω	ω	0
4	0	0	0	0	ω	0	ω	0	0	ω	0	0	ω	ω	0	0	ω	0	ω	ω	0	0
5	0	0	ω	0	0	0	ω	ω	0	ω	ω	ω	ω	ω	ω	0	0	ω	ω	ω	0	0
6	ω	0	ω	0	ω	ω	ω	0	ω	0	0	0	0	ω	ω	ω	ω	0	ω	ω	0	0
7	0	0	0	0	0	$\overline{\omega}$	0	$\overline{\omega}$	0	0	$\overline{\omega}$	0	0	$\overline{\omega}$	$\overline{\omega}$	0	0	$\overline{\omega}$	0	$\overline{\omega}$	$\overline{\omega}$	0
8	0	0	0	$\overline{\omega}$	0	0	0	$\overline{\omega}$	$\overline{\omega}$	0	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0	0	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0
9	0	$\overline{\omega}$	0	$\overline{\omega}$	0	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0	$\overline{\omega}$	0	0	0	0	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0	$\overline{\omega}$	$\overline{\omega}$	0
10	0	0	0	0	$\overline{\omega}$	0	$\overline{\omega}$	0	0	$\overline{\omega}$	0	0	$\overline{\omega}$	$\overline{\omega}$	0	0	$\overline{\omega}$	0	$\overline{\omega}$	$\overline{\omega}$	0	0
11	0	0	$\overline{\omega}$	0	0	0	$\overline{\omega}$	$\overline{\omega}$	0	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0	0	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0	0
12	$\overline{\omega}$	0	$\overline{\omega}$	0	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0	$\overline{\omega}$	0	0	0	0	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	0	$\overline{\omega}$	$\overline{\omega}$	0	0
13	$\overline{\omega}$	ω	0	$\overline{\omega}$	1	1	ω	$\overline{\omega}$	ω	0	$\overline{\omega}$	1	1	ω	$\overline{\omega}$	ω	0	$\overline{\omega}$	1	1	ω	0
14	$\overline{\omega}$	1	1	ω	$\overline{\omega}$	ω	0	$\overline{\omega}$	1	1	ω	$\overline{\omega}$	ω	0	$\overline{\omega}$	1	1	ω	$\overline{\omega}$	ω	0	0
15	ω	$\overline{\omega}$	ω	0	$\overline{\omega}$	1	1	ω	$\overline{\omega}$	ω	0	$\overline{\omega}$	1	1	ω	$\overline{\omega}$	ω	0	$\overline{\omega}$	1	1	0
16	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω	ω
17	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$	$\overline{\omega}$

We have mentioned how the second block of rows is obtained from the first block. Also, rows 4,5,6 are obtained from rows 1,2,3 by shifting. Rows 13,14,15 are periodic with a period of 7. In these rows, symbols 0 and ω are always followed by 0 or $\overline{\omega}$, symbols 1 and $\overline{\omega}$ are followed by 1 or ω.

Consider case $q=2, n=31$. Clearly $r=\kappa=5$. Here are the cyclotomic cosets in this case:

cyclotomic cosets
0
1,2,4,8,16
3,6,12,24,17
5,10,20,9,18
7,14,28,25,19
11,22,13,26,21
15,30,29,27,23

Let $A=[1,5]$. We obtain $dim(\mathcal{C}(A))=2\cdot 16+10=42$. The orthogonality condition is trivially satisfied. We obtain codes $[[31,11,6]]_2$ and $[[32,10,7]]_2$.

Here is our first infinite series of (lengthened) twisted quantum codes.

Theorem 9 *For every q and every $r\geq 2$ an application of Theorem 8 yields a pure quantum code*

$$[[q^r, q^r-(r+2), 3]]_q$$

There is a twisted quantum code

$$[[q^2+1, q^2-3, 3]]_q.$$

Proof: Consider case $n=q^r-1, A=\{1\}$. The dimension of $\mathcal{C}(A)$ is $K=2(n-r)+r=2n-r$, hence $k=K-n=q^r-(r+1)$. As $Z(1)\neq Z(-1)$ clearly we have a self-orthogonal code. An application of Theorem 8 yields the first part of the Theorem. Let $r=4, n=q^2+1, \kappa=2, A=\{1\}$. We get a code of dimension $K=2(n-4)+4=2n-4$ and quantum dimension 4. It is self-orthogonal by Theorem 6.$\blacksquare$

This generalizes [1],Theorem 10.

In [3] a lengthening technique is applied to the classical Reed-Muller codes to derive a family of quantum codes with parameters

$$[[2^r, 2^r-\binom{r}{t}-2\sum_{i=0}^{t-1}\binom{r}{i}, 2^t+2^{t-1}]]_2.$$

We observe that these parameters are not good at all in general. Application of Theorem 8 in case $n = 2^r - 1, \kappa = r, A = [1, 2^t + 2^{t-1} - 2]$ yields better results in almost all cases. The generic choice $\kappa = r$ is always possible. If r is prime, then it is the only possible choice. We mention that choices $\kappa < r$ tend to give better parameters than $\kappa = r$. This is another source of possible improvements.

Choose $A = [1, 4]$. We have $\{1, 2, 4\} \subset Z(1), Z(3) \neq Z(1)$. Assume $r > 3$. Then $Z(1)$ and $Z(3)$ have maximum length r, and $Z(1) \cup Z(3)$ is disjoint from its negative. Self-orthogonality follows. We have $K = 2(n - 2r) + r = 2n - 3r, k = K - n = n - 3r$ and obtain

$$[[2^r - 1, 2^r - 3r - 1, 5]]_2 \text{ and } [[2^r, 2^r - 3r - 2, 6]]_2.$$

This is much better than the values from [3]. For larger t the gap widens.

Theorem 10 *Let $q = 2, n \mid 2^r - 1$. Then $[[n+1, n-r-1, 3]]_2$ exists. Assume that either r odd or that n does not divide $2^{r/2} + 1$. Then*

$$[[n, n - 2r, 3]]_2 \text{ and } [[n + 1, n - 2r - 1, 4]]_2 \text{ exist.}$$

Assume moreover that $n > 3$ and neither 3 nor -3 are in $Z(1)$. Then

$$[[n, n - 2r- \mid Z(3) \mid, 5]]_2 \text{ and } [[n + 1, n - 2r- \mid Z(3) \mid -1, 6]]_2 \text{ exist.}$$

Proof: The first cases correspond to $\kappa = r$ and $A = \{1\}$ or $A = \{1, 2\}$, the last family is given by $A = [1, 4], \kappa =\mid Z(3) \mid$. ∎

As examples for the last series in Theorem 10 we mention

$$[[46, 16, 6]]_2, [[51, 27, 5]]_2, [[52, 26, 6]]_2, [[73, 46, 5]]_2, [[74, 45, 6]]_2, [[85, 61, 5]]_2,$$

$$[[86, 60, 6]]_2, [[93, 68, 5]]_2, \text{ and } [[94, 67, 6]]_2.$$

8 A general lengthening method

Theorem 11 *Let $\mathcal{C}_i, i = 1, 2, \ldots, a$ be q-linear q^2-ary quantum codes of length n_i and dimension K_i. Let $\mathcal{C}_i, i < a$ have dual distance $\geq d$ and $\mathcal{C}_a$ have dual distance $\geq min(d, n_a)$. For $i < a$ let $\mathcal{D}_i \subset \mathcal{C}_i$ be a subcode of dual distance $\geq d-1$ such that $K_{i+1} \leq K_i - dim(\mathcal{D}_i), i = 1, 2, \ldots, a$.*
We can construct a quantum code of length $\sum_i n_i$, dimension K_1 and dual distance $\geq d$, in other words

$$[[\sum_i n_i, \sum_i n_i - K_1, d]]_q.$$

Proof: By assumption we can find matrices G_i with entries in $E = V(2, q)$ such that G_i has K_i rows and n_i columns and any $d-1$ columns of G_i are linearly independent. For $i < a$ we have a submatrix E_i of G_i with $dim(\mathcal{D}_i)$ rows, such that any $d-2$ columns of E_i are linearly independent. We define matrix G as concatenation of the G_i, where G_i is complemented by $K_1 - K_i$ final 0-rows and submatrix E_i consists of the last nonzero rows. Clearly G describes a self-orthogonal code of length $\sum_i n_i$ and dimension K_1. Assume some $d-1$ columns are linearly dependent. Let $i < a$ be minimal such that section i of G contains one of the columns. Not all of these columns are in this section. Consider the rows corresponding to matrix E_i. As E_i has strength $d-2$ and all columns of G belonging to segments $j > i$ have entries 0 there, we obtain that the coefficients of the linear relation of the columns in segment i all vanish. It follows that all of our columns with a nonzero coefficient are in section a. If $d-1 \geq a$ we obtain the usual contradiction. If $d-1 < a$, then the columns of the last section are linearly independent, another contradiction.∎

Theorem 11 of [1] can be described as an application of our Theorem 11 in case $q = 2, d = 3$. In fact we can use as ingrediences the codes $[[2^r, 2^r - r - 2, 3]]_2$ described in Section 7. Let us generalize this to the q-ary case. Our codes $[[q^r, q^r - (r+2), 3]]_q$ have dimension $r+2$ and they contain by construction the 2-dimensional repetition code (of dual distance 2). Let

$r = 2u$ be even. As 4-dimensional member ($\mathcal{C}_a$ in the language of Theorem 11) we can use the code $[[q^2+1, q^2-3, 3]]_q$ from Theorem 9. Applying Theorem 11 in this case $r = 2u$ yields a quantum code of length $q^r + q^{r-2} + \ldots + q^2 + 1 = (q^{r+2}-1)/(q^2-1)$. In case $r = 2u+1$ odd we proceed in the same way, using members of our family all the way. The smallest member is $[[q^3, q^3-5, 3]]_q$. The length is $q^r + q^{r-2} + \ldots + q^3 = q^3(q^{r-1}-1)/(q^2-1)$. We have seen the following:

Theorem 12 *There exist pure quantum codes*

$$[[(q^{r+2}-1)/(q^2-1), (q^{r+2}-1)/(q^2-1)-(r+2), 3]]_q \textit{ (r even) and}$$

$$[[q^3(q^{r-1}-1)/(q^2-1), q^3(q^{r-1}-1)/(q^2-1)-(r+2), 3]]_q \textit{ (r odd)}$$

The first series in Theorem 12 (for r even) corresponds to the quantum codes obtained from the $\mathbb{F}_{q^2}-$ary Simplex/Hamming codes (see Theorem 1).

9 Conclusion

We have developed the theory of twisted codes in the quadratic case. These codes turned out to be a source for good quantum codes. We conclude with a table of additional parameters of additive quaternary quantum codes, which may be constructed from twisted codes, eventually via standard lengthening. More material is to be found on our homepages [5].

code parameters	interval A	κ
$[[13, 1, 4]]$	[6,8]	2
$[[21, 12, 3]]$	[2,3]	3
$[[31, 6, 7]]$	[1,6]	5
$[[32, 5, 8]]$	[1,6]	5
$[[41, 21, 4]]$	[11,13]	2
$[[43, 29, 4]]$	[13,15]	2
$[[46, 6, 8]]$	[1,6]	3
$[[45, 19, 5]]$	[3,6]	3
$[[51, 19, 6]]$	[1,5]	2
$[[52, 18, 7]]$	[1,5]	2
$[[63, 39, 6]]$	[1,5]	2
$[[64, 38, 7]]$	[1,5]	2
$[[63, 33, 7]]$	[1,6]	2
$[[64, 32, 8]]$	[1,6]	2
$[[63, 27, 9]]$	[1,8]	3
$[[64, 26, 10]]$	[1,8]	3
$[[63, 24, 10]]$	[1,9]	3
$[[64, 23, 11]]$	[1,9]	3
$[[63, 18, 11]]$	[1,10]	3
$[[64, 17, 12]]$	[1,10]	3
$[[63, 12, 13]]$	[1,12]	3
$[[64, 11, 14]]$	[1,12]	3
$[[63, 48, 4]]$	[7,9]	3
$[[63, 54, 3]]$	[8,9]	3
$[[73, 55, 4]]$	[20,22]	3
$[[86, 36, 10]]$	[1,8]	2
$[[86, 28, 11]]$	[1,9]	2
$[[85, 53, 7]]$	[23,28]	2

code parameters	interval A	κ
$[[85,69,4]]$	[26,28]	2
$[[85,33,10]]$	[48,56]	2
$[[85,41,9]]$	[49,56]	2
$[[85,49,8]]$	[50,56]	2
$[[92,18,12]]$	[1,10]	2
$[[94,52,8]]$	[1,6]	2
$[[93,43,9]]$	[1,8]	2
$[[94,42,10]]$	[1,8]	2
$[[94,57,7]]$	[1,5]	5
$[[93,38,10]]$	[1,9]	5
$[[94,37,11]]$	[1,9]	5
$[[94,27,12]]$	[1,10]	5
$[[106,68,6]]$	[1,4]	2
$[[106,62,7]]$	[1,5]	2
$[[105,47,9]]$	[1,8]	2
$[[106,46,10]]$	[1,8]	2
$[[105,71,5]]$	[4,7]	2
$[[105,83,4]]$	[5,7]	2
$[[105,95,3]]$	[14,15]	2
$[[113,85,4]]$	[73,75]	2
$[[118,80,6]]$	[1,4]	2
$[[118,68,7]]$	[1,5]	2
$[[118,56,8]]$	[1,6]	2
$[[117,63,7]]$	[11,16]	3
$[[117,93,4]]$	[48,50]	3
$[[117,105,3]]$	[49,50]	3
$[[117,75,6]]$	[64,68]	3
$[[117,87,5]]$	[65,68]	3
$[[127,99,6]]$	[1,5]	7
$[[128,98,7]]$	[1,5]	7
$[[127,92,7]]$	[1,6]	7
$[[128,91,8]]$	[1,6]	7
$[[127,85,9]]$	[1,8]	7
$[[128,84,10]]$	[1,8]	7
$[[127,78,10]]$	[1,9]	7
$[[128,77,11]]$	[1,9]	7

code parameters	interval A	κ
$[[127, 71, 11]]$	[1,10]	7
$[[128, 70, 12]]$	[1,10]	7
$[[127, 64, 13]]$	[1,12]	7
$[[128, 63, 14]]$	[1,12]	7
$[[127, 57, 14]]$	[1,13]	7
$[[128, 56, 15]]$	[1,13]	7
$[[127, 50, 15]]$	[1,14]	7
$[[128, 49, 16]]$	[1,14]	7

References

[1] A.R.Calderbank,E.M.Rains,P.W.Shor and N.J.A.Sloane: *Quantum error correction via codes over GF(4), IEEE Transactions on Information Theory,* to appear

[2] Y.Edel and J.Bierbrauer: *Twisted BCH-codes, Journal of Combinatorial Designs* **5** (1997),377-389.

[3] A.M.Steane: *Quantum Reed-Muller codes,* LANL e-print quant-ph/9608026.

[4] H.Stichtenoth: *On the dimension of subfield subcodes, IEEE Transactions on Information Theory* **36** (1990),90-93.

[5] Our homepages are http://www.mathi.uni-heidelberg.de/∼yves/ and http://www.math.mtu.edu/∼jbierbra/Home.html