A family of 2-weight codes related to BCH-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)

Abstract

For every prime-power q and every pair of natural numbers $m \leq n'$ we construct a q-ary linear code of length $q^m(q^{n'}-1)(q^{n'}-q^{n'-m}+1)/(q-1)$ and dimension $3n'$, whose only nonzero weights are $q^{2n'+m-1}-q^{2n'-1}$ and $q^{2n'+m-1}-q^{2n'-1}+q^{n'+m-1}$. These code parameters and those of the corresponding family of strongly regular graphs are new in odd characteristic.

1 A family of extended twisted BCH-codes

We consider extended primitive q^m-ary q-linear BCH-codes of length q^n, where $n = 2n', n' \geq m$. The theory of this generalization of the concept of a BCH-code to additive nonlinear codes was developed in [8]. We recall the basic definitions as far as relevant for our purposes: Let $F = \mathbb{F}_{q^n}$, where $n = 2n', F_0 = \mathbb{F}_{q^{n'}}$. Let $m \leq n'$. Fix an m-dimensional subspace $U \subset F_0$ with basis $\Gamma = \{\gamma_1, \dots, \gamma_m\}$ (over $\mathbb{F}_q$). Denote by $tr = tr : F \longrightarrow \mathbb{F}_q$ and $Tr : F \longrightarrow F_0$ the corresponding traces. Let $E = \mathbb{F}_q^m$. The $\mathbb{F}_q$-linear surjective mapping $\Phi : F \longrightarrow E$ is defined by $\Phi(u) = (tr(\gamma_1 u), \dots, tr(\gamma_m u))$. For every $0 < t \leq q^n$ the array $\mathcal{A}(t)$ is defined in the following way: its columns are indexed by $u \in F$, its rows by the pairs $(p(X), z)$, where $z \in E$ and $p(X)$ is a polynomial with coefficients in F, of degree $< t$, satisfying $p(0) = 0$. The corresponding entries are $\Phi(p(u)) + z$. We have shown that $\mathcal{A}(t)$ is an orthogonal array of strength t, with parameters $OA_{q^{(t-1)(n-m)}}(t, q^n, q^m)$. Each row of $\mathcal{A}(t)$ occurs with multiplicity $q^{\rho_0(t)}$, where $\rho_0(t)$ is the $\mathbb{F}_q$-dimension of the space of polynomials $p(X)$ as above, which satisfy in addition $\Phi(p(F)) = 0$. It has been shown that we can define a dual code $\mathcal{A}(t)^\perp$. This is a q^m-ary $\mathbb{F}_q$-linear code of length q^n, minimum distance (equal to minimum weight) $\geq t + 1$ and dimension $q^n - \{n(t-1) + m\} + \rho_0(t)$. It was easy to see that $\mathcal{A}(q^n - 1)^\perp$ is the repetition code $\{(e, e, \dots, e) | e \in E\}$, with parameters $[q^n, m, q^m]$. Put $\mathcal{C}_1 = \mathcal{A}(q^n - 1)^\perp$. We want to study the low-dimensional members of the family $\mathcal{A}(t)^\perp$, corresponding to the highest values of t. Denote by $\Delta(t) = \rho_0(t + 1) - \rho_0(t)$ the increase of function ρ_0. Observe that the codimension of $\mathcal{A}(t + 1)^\perp$ in $\mathcal{A}(t)^\perp$ is $n - \Delta(t)$. In [8] we studied $\Delta(t)$. We will make frequent use of Theorems 3 and 2 of [8] in order to determine $\Delta(t)$ in the cases which are of interest to us. The notation of [8] will be used freely from now on.

Let $t = q^n - q^{n-m} - 1$, put $\mathcal{C}_2 = \mathcal{A}(q^n - q^{n-m} - 1)^\perp$. The cyclotomic coset $Z(t) = \{-1, -q, \dots, -q^{n-m}, \dots, -q^{n-1}\}$ has length n. Its smallest element is $z_1 = -q^{n-1}$. We have $t = z_m$ and in general $z_j = z_1 q^{-(j-1)}$, hence $\pi(j) = j - 1$. By Theorems 2 and 3 of [8] we have $H = \{1, 2, \dots, m\}$. In particular $m \in H$. [8],Theorem 3 yields $\Delta(t) = 0$. We conclude that $\mathcal{C}_2$ has dimension $\geq n + m$. Let $x \in \mathcal{C}_2 - \mathcal{C}_1$. Denote by χ_u the frequency of entry u in x. Then $x - (u, u, \dots, u)$ has weight $q^n - \chi_u$. As $\mathcal{C}_2$ has minimal weight $\geq q^n - q^{n-m}$, it follows $\chi_u \leq q^{n-m}$. We conclude that $\chi_u = q^{n-m}$ for every $u \in E$. In particular every word in $\mathcal{C}_2 - \mathcal{C}_1$ has weight $q^n - q^{n-m}$. It follows that $\mathcal{A}(t)^\perp = \mathcal{C}_1$ for all $q^n - q^{n-m} - 1 < t \leq q^n - 1$. In particular $dim(\mathcal{C}_2) = n + m$.

Consider now $t = q^n - q^{n-m} - 1 - j$, where $0 < j < q^{n'-m}$. We want to show that there is no increase of dimension in this range. In order to handle this situation let us visualize the action of $G = Gal(F|\mathbb{F}_q)$ in a more convenient way: consider the q-adic representation of the numbers $\leq q^n - 1$. Then the Frobenius automorphism simply operates as a cyclic change of the n coordinates. Denote the q-adic representation of i by $i_q = (\alpha_{n-1}, \dots, \alpha_0)$. In the q-adic representation of $q^n - q^{n-m} - q^{n'-m} - 1$ all but two of the $\alpha_j = q - 1$, the exceptions being $\alpha_{n-m} = \alpha_{n'-m} = q-2$. The q-adic representations of $t = q^n - q^{n-m} - 1 - j$ above will agree with this, except for the $\alpha_j, j = 0, \ldots, n'-m-1$. These values are arbitrary, but they are not all $q-1$. We see that $tq^i, i = 1, \ldots, m-1$ are smaller than t as is $tq^{n'}$. In the terminology of Theorem 3 of [8] we want to show that $j \notin H$, where $t = z_j$ is the j-smallest element of $Z(t)$. It suffices to show that there is a regular submatrix of M corresponding to columns, which are indexed by elements $< t$ in $Z(t)$. Consider the columns corresponding to $tq^i, i = 1, 2, \ldots, m-1$ and $tq^{n'}$. We have to show that a nontrivial linear combination of these columns is nonzero. Recall that $U \subset F_0$. Consider the corresponding automorphisms $x \longrightarrow x^{q^i}, i = 1, 2, \ldots, m-1$ and $x \longrightarrow x^{q^{n'}}$. We have to show that the kernel of a nonzero linearized polynomial $p(X) = \sum_{i=1}^{m-1} a_i X^{q^i} + aX^{q^{n'}}$ intersects F_0 in dimension $< m$. Let $L = ker(p(X)) \cap F_0$. Because of Theorem 2 of [8] we have without restriction $a = 1$. It was shown in [2] that the polynomial $p_L(X) = \prod_{u \in L}(X - u)$ is linearized of degree $q^{dim(L)}$. As $U \subseteq F_0$ we have that $p_L(X)$ divides $X^{q^{n'}} - X$. We are assuming that $P_L(X)$ divides $P(X)$. It must therefore also divide $p(X) - (X^{q^{n'}} - X)$, which is a nonzero linearized polynomial of degree $\leq q^{m-1}$. We conclude that $dim(L) < m$, hence $j \notin H$. It follows that $\mathcal{A}(q^n - q^{n-m} - q^{n'-m})^\perp = \mathcal{A}(q^n - q^{n-m} - 1)^\perp$. Finally let $t = q^n - q^{n-m} - q^{n'-m} - 1$, put $\mathcal{C}_3 = \mathcal{A}(t)^\perp$. We see that $|Z(t)| = n', t = z_m$ and $z_j = z_1 q^{-(j-1)}, j = 1, \ldots, m$. We conclude from Theorems 2 and 3 of [8] that $H = \{1, 2, \ldots, m\}$. From Proposition 3 of [8] we know that the total contribution of $Z(t)$ is $\sum_{z \in Z(t)} \Delta(z) = n'(n-m)$. The contribution of the $z_j, j \notin H$ is $(n'-m)n$. It follows that the average contribution of a $j \in H$ is n'. We claim that for every $j \in H$ we have $\Delta(z_j) = n'$. It suffices to prove $\Delta(z_j) \geq n'$ for every $j \in H$. As $K = ker(Tr : F \longrightarrow F_0)$ is F_0-linear it suffices to prove $\Delta(z_j) \neq 0, j = 1, 2, \ldots, m$. Theorem 3 of [8] expresses this quantity as $\Delta(z_j) = d_j - d_{j-1} = dim(S_j \cap \mathcal{D}) - dim(S_{j-1} \cap \mathcal{D})$. The entries of M are $m_{k,j} = \gamma_k^{q^{j-1}}$. The space S_j is generated by the first j columns. Choose a vector $(x_1, \ldots, x_j)$, where $x_a \in K$ and $x_j \neq 0$. We claim that the corresponding linear combination of the first j columns of M represents an element of $(S_j \cap \mathcal{D}) - (S_{j-1} \cap \mathcal{D})$. We have to prove that $Tr(\sum_{a=1}^{j} x_a \gamma_k^{q^{a-1}}) = 0$. As $\gamma_k \in F_0$ and $Tr(x_a) = 0$ this is clear. We have proved our claim. In particular $\Delta(t) = n'$. It follows that $\mathcal{C}_3$ has dimension $n' + (n+m) = 3n' + m$.

Theorem 1 *With notation as above the lowest-dimensional extended primi-*

tive twisted BCH-codes of length q^n, where $n = 2n'$, form a chain $\mathcal{C}_1 \subset \mathcal{C}_2 \subset \mathcal{C}_3$ with parameters

$$[q^n, m, q^n] \subset [q^n, n+m, q^n - q^{n-m}] \subset [q^n, 3n'+m, q^n - q^{n-m} - q^{n'-m}].$$

Here $\mathcal{C}_1$ is the repetition-code. The dimensions are over $\mathbb{F}_q$.

Next we wish to study the weight-distribution of these codes. $\mathcal{C}_2$ has been dealt with already. As a preparation we note that we can make use of a rather large automorphism group:

Theorem 2 *Let $A = AGL_1(q^n)$ be the affine group of order $q^n(q^n-1)$ in its operation on the elements of F (the columns of $\mathcal{A}(t)$). Then A is a group of automorphisms of $\mathcal{A}(t)$ (and of $\mathcal{A}(t)^\perp$.*

Proof: Let $0 \neq \lambda \in F$. We claim that the permutation $u \longrightarrow \lambda \cdot u$ on the columns of the array is an automorphism. In fact, the entry in row $(p(X), z)$ and column u of the permuted array is $\Phi(p(\lambda \cdot u)) + z$. This shows that our permutation maps row $(p(X), z)$ to row $(p(\lambda X), z)$.
Consider a permutation $u \longrightarrow u + \alpha$. The entry in row $(p(X), z)$ and column u of the permuted array is $\Phi(p(u+\alpha)) + z$. However, we cannot use the polynomial $p(X+\alpha)$, as its constant term may not vanish. Put $q(X) = p(X+\alpha) - p(\alpha)$. Then write our entry in the form $\Phi(q(u)) + \Phi(p(\alpha)) + z$. It remains to be shown that the mapping $(p(X), z) \longrightarrow (p(X+\alpha) - p(\alpha), \Phi(p(\alpha)) + z)$ is a permutation of the rows of our array. This is immediately clear.■

We start by exhibiting an element of $\mathcal{C}_3 - \mathcal{C}_2$. Observe at first that we could have started from arrays $\mathcal{A}'(t)$ instead of $\mathcal{A}(t)$, whose rows are given by the polynomials $p(X)$ if degree $< t$ and with entry $\Phi(p(u))$ in column u. Then $\mathcal{A}'(t)$ differs from $\mathcal{A}(t)$ only in the multiplicities of rows. In particular $\mathcal{A}'(t)^\perp = \mathcal{A}(t)^\perp$. We have mentioned earlier that the information used about Φ is its kernel. We take the liberty to redefine Φ by setting $\Phi(x) = \sum_{i=1}^m tr(\gamma_i x)\gamma_i$. In this way we identify E with U. Fix the scalar product $\cdot$ on U with Γ as orthonormal basis. Let $p_V(X) = \prod_{v \in V}(X - v)$, where the subspace $V \subset F_0$ is chosen such that $p_V(F_0) = U$. It was shown in [2] that V is uniquely defined and has dimension $n' - m$. In particular the linearized polynomial $p_V(X)$ has degree $q^{n'-m}$. Put $q(X) = p_V(Y)$, where $Y = X^{q^{n'}+1}$. We see that $q(F) \subseteq U$ and $q(X)$ is a polynomial of degree $q^{n-m} + q^{n'-m}$. Put

$t=q^n-q^{n-m}-q^{n'-m}-1$. As the polynomials defining the rows of $\mathcal{A}'(t)$ have degrees $<t$ we see that $\sum_{u\in F}p(u)q(u)=0$ for all those $p(X)$. We claim that $x=(q(u))_u\in\mathcal{A}(t)^\perp$. Put $q(u)=\sum_{i=1}^m q(u)_i\gamma_i$. Then $\sum_u\Phi(p(u))\cdot q(u)=\sum_u\sum_{i=1}^m tr(\gamma_i p(u))q(u)_i=tr(\sum_u p(u)\sum_i q(u)_i\gamma_i)=tr(\sum_u p(u)q(u))=0$.
We have found an element $x\in\mathcal{C}_3-\mathcal{C}_2$. Let χ_e be the frequency of entry $e\in U$ in x. We have $\chi_0=1+(q^{n'-m}-1)(q^{n'}+1)=q^{n-m}+q^{n'-m}-q^{n'}$. Thus $wt(x)=q^n-q^{n-m}-q^{n'-m}+q^{n'}$. If $e\neq 0$, then $\chi_e=q^{n'-m}(q^{n'}+1)=q^{n-m}+q^{n'-m}$, hence $wt(x-(e,e,\dots,e))=q^n-q^{n-m}-q^{n'-m}$. It follows that there are only $q-1$ words of weight $wt(x)$ in the space generated by x and $\mathcal{C}_1$. Consider the stabilizer of x under the action of the affine group A. The element $u\longrightarrow\alpha u+\beta$ stabilizes x if and only if $p_V((\alpha u+\beta)^{q^{n'}+1})=p_V(u^{q^{n'}+1})$ for every $u\in F$. As the degrees of the polynomials involved are $<q^n$ this is a polynomial equation in u. Comparing coefficients we see $\beta=0,\alpha^{q^{n'}+1}=1$. It follows that the stabilizer of x under the action of A is cyclic of order $q^{n'}+1$. The length of the orbit is therefore $q^n(q^{n'}-1)$.
The number of $(m+1)-$dimensional subspaces containing $\mathcal{C}_1$ and not contained in $\mathcal{C}_2$ clearly is $(q^{3n'+m}-q^{n+m})/(q^{m+1}-q^m)=\frac{1}{q-1}q^n(q^{n'}-1)$. It follows that A is transitive on these subspaces. In particular we know the weight distribution of our codes.

Theorem 3 *Every word in $\mathcal{C}_2-\mathcal{C}_1$ has weight $a_1=q^n-q^{n-m}$. Put $a_2=q^n-q^{n-m}+q^{n'}$. The only weights occuring in $\mathcal{C}_3-\mathcal{C}_2$ are $a_1-q^{n'-m}$ and $a_2-q^{n'-m}$. The words of weight $a_2-q^{n'-m}$ form a single orbit under the affine group of order $q^n(q^n-1)$. The length of this orbit is $q^n(q^{n'}-1)$.*

2 A family of 2-weight codes and strongly regular graphs

We use the codes constructed in the previous section. At first consider the subcodes $\mathcal{C}'_i\subset\mathcal{C}_i$ consisting of the words with entry $e=0$ in the coordinate $u=0$. Naturally we omit this entry 0 then. We obtain q^m-ary codes of length q^n-1. The dimensions of $\mathcal{C}_2,\mathcal{C}_3$ are n and $3n'$, respectively. Only weights $a_1,a_1-q^{n'-m}$ and $a_2-q^{n'-m}$ survive. Next we use concatentation with the q-ary simplex code $[(q^m-1)/(q-1),m,q^{m-1}]$. Observe that this is a constant-weight code. The result is a pair of linear q-ary codes $\mathcal{D}_2\subset\mathcal{D}_3$ of length $(q^n-1)(q^m-1)/(q-1)$. The dimensions remain unchanged. The weights pick up a factor of q^{m-1}. Finally apply construction X [10, 4] to the pair $\mathcal{D}_3 \supset \mathcal{D}_2$ of q^m-ary codes. As auxiliary code use the simplex code $[(q^{n'}-1)/(q-1), n', q^{n'-1}]$. In the resulting code $\tilde{\mathcal{D}_3}$ the only weights occuring are $w_1 = a_1 q^{m-1}$ and $w_2 = a_2 q^{m-1}$. This is so because the weights of the words in $\mathcal{D}_2$ remain unchanged, whereas the weight of every word in $\mathcal{D}_3 - \mathcal{D}_2$ increases by $q^{n'-1}$.

Theorem 4 *For every prime-power q and natural numbers $m \leq n'$ there is a q-ary 2-weight code $\mathcal{C}_{q,m,n'}$ of length $n_{q,m,n'} = q^m(q^{n'}-1)(q^{n'}-q^{n'-m}+1)/(q-1)$ and dimension $3n'$, with weights $w_1 = q^{2n'+m-1} - q^{2n'-1}$ and $w_2 = q^{2n'+m-1} - q^{2n'-1} + q^{n'+m-1}$*

The weight-distribution is given by

$$A(w_1) = (q^{2n'}-1)(q^{n'}-q^{n'-m}+1),\ A(w_2) = q^{n'-m}(q^{n'}-1)(q^{n'}-q^m+1).$$

Consider the strongly regular graph $\Gamma_{q,m,n'}$, whose vertices are the code words and with adjacency defined in the following way: the coordinates of $\mathcal{C}_{q,m,n'}$ form a family of linear functionals $\phi_i : \mathcal{C}_{q,m,n'} \longrightarrow \mathbb{F}_q$. Put $P_i = ker(\phi_i)^\perp, i = 1, 2, \ldots, n_{q,m,n'}$. Informally the one-dimensional subspaces P_i may be described as generated by the columns of a generator matrix of $\mathcal{C}_{q,m,n'}$. Two code words x, y are adjacent in $\Gamma_{q,m,n'}$ if $x - y$ is contained in one of the P_i. The parameters of the strongly regular graph $\Gamma_{q,m,n'}$ are easily determined: The number of vertices is $q^{3n'}$, the valency is $K = q^m(q^{n'}-1)(q^{n'}-q^{n'-m}+1)$. The number of common neighbours of a pair of nonadjacent vertices is $\mu = q^m(q^m-1)(q^{n'}-q^{n'-m}+1)$. As the formula for λ looks rather ugly it may be wiser to work with the intersection numbers. In fact, we have $K - 1 - \lambda = (q^{n'}+1)(q^m-1)(q^{n'}-q^m+1)$. We remark that the smallest odd-characteristic member of our family is not new. Gulliver [9] has constructed a ternary 2-weight code $[84, 6, 54]$ (with the same parameters as $\mathcal{C}_{3,1,2}$) by different means.

3 Motivation from maximal arcs

Consider the classical projective plane $\Pi = \mathcal{P}_2(q)$ of order q. A point-set $\mathcal{K}$ is a $\{v; k\}$-**arc** if $|\mathcal{K}| = v$ and no line contains more than k points of $\mathcal{K}$. Denote by $m_2(k, q)$ the largest cardinality v of a $\{v; k\}$-arc in Π. Fix a point $P \in \mathcal{K}$.

There are $q+1$ lines through P. Each line contains at most $k-1$ points from $\mathcal{K}$, aside of P itself. It follows $v \leq (q+1)(k-1)+1$. In the case of equality we call $\mathcal{K}$ a **maximal $\{v;k\}$-arc.** Assume $\mathcal{K}$ is a maximal $\{v;k\}$-arc. Call $\mathcal{K}$ nontrivial if $1 < k < q$. The same type of counting argument shows that k divides q. Denniston [7] has given an elegant construction of maximal arcs in characteristic two. Thus in characteristic 2 all conceivable maximal arcs do exist. In a forthcoming paper by Ball, Blokhuis and Mazzocca [1] the question of existence of maximal arcs is completely settled. These authors show the nonexistence of nontrivial maximal $\{v;k\}$-arcs in desarguesian projective planes of odd order.
A fundamental relationship between linear codes and sets of points in projective spaces (see [6], for example), shows that a maximal $\{v;k\}$-arc in the projective plane $\mathcal{P}_2(q)$ is equivalent with a q-ary projective code $[kq+k-q, 3, kq-q]$, which has only two weights: $kq-q$ and $kq+k-q$. Consider now $\mathbb{F}_{q^{n'}}$ as the ground field and assume for the moment that a maximal $\{v;k\}$-arc exists in the classical projective plane of order $q^{n'}$, where $k = q^m$. This means that we have a $q^{n'}$-ary 2-weight code $[q^{n'+m} - q^{n'} + q^m, 3, q^{n'+m} - q^{n'}]$ with $q^{n'+m} - q^{n'}$ and $q^{n'+m} - q^{n'} + q^m$ as nonzero weights. Use concatenation with the q-ary Simplex code $[(q^{n'}-1)/(q-1), n', q^{n'-1}]$. This would yield a large family of q-ary two-weight codes. The parameters are precisely those of our family of codes $\mathcal{C}_{q,m,n'}$. We conclude that these codes exist although the corresponding maximal $\{v;k\}$-arcs do not exist in odd characteristic.

4 Partial geometries

The parameters of the strongly regular graphs corresponding to our two-weight codes are pseudogeometric. This means that partial geometries $pg(q^{n'}, q^m(q^{n'} - q^{n'-m} + 1), q^m - 1)$ may exist.

Problem 1 *Let q be a prime-power and m, n' natural numbers, $0 < m < n'$. Does there exist a partial geometry with parameters $pg(q^{n'}, q^m(q^{n'} - q^{n'-m} + 1), q^m - 1)$?*

In characteristic two they can be constructed using the Denniston arcs (see [5]):

Theorem 5 *Let $q = 2^f, k = 2^i, i < f$. Then there exists a $pg(q, kq-q+k, k-1)$.*

Proof: As set of points we choose $\mathbb{F}_q^3$. Let $\mathcal{K} \subset \mathcal{P}_2(q)$ be a maximal $\{v; k\}$-arc (for example a Denniston arc), seen as a collection of $qk - q + k$ one-dimensional subspaces. As lines choose these one-dimensional subspaces and their cosets. The axioms are easily verified.■

In case $k = 2$ this yields a well-known family of generalized quadrangles $GQ(q-1, q+1)$. The substitution $q \longrightarrow q^{n'}, k \longrightarrow q^m$ shows that our family of partial geometries certainly exists in characteristic two. To the best of our knowledge the question of existence is open in all remaining cases.
The dual of $pg(k, r, t)$ is a $pg(r, k, t)$. In the case of our parameters this leads to the following problem:

Problem 2 *Let q be a prime-power and m, n' natural numbers, $0 < m < n'$. Does there exist a strongly regular graph on $q^{2n'+m}(q^{n'} - q^{n'-m} + 1)$ vertices, with valency $K = q^{n'}(q^m - 1)(q^{n'} + 1)$ and $\mu = q^{n'}(q^m - 1), K - 1 - \lambda = (q^{n'} - 1)(q^{n'+m} - q^{n'} + 1)$?*

It is clear by now that all these structures exist in characteristic two. In odd characteristic the question is wide open.

Acknowledgements

We wish to thank Marijn van Eupen and René Struik for helpful discussions.

References

[1] S.Ball, A.Blokhuis, F.Mazzocca: *Maximal arcs in desarguesian planes of odd order do not exist,* submitted for publication in *Combinatorica.*

[2] J.Bierbrauer: *Construction of orthogonal arrays,* to appear in *Journal of Statistical Planning and Inference.*

[3] J.Bierbrauer, Y.Edel: *New code-parameters from Reed-Solomon subfield codes,* to appear in *IEEE Transactions on Information Theory.*

[4] J.Bierbrauer, Y.Edel: *Extending and lengthening BCH-codes,* submitted for publication in *Finite Fields and Their Applications.*

[5] A.E.Brouwer, J. van Lint: *Strongly regular graphs and partial geometries, Enumeration and Design - Proc. Silver Jubilee Conference on Combinatorics Waterloo 1982 (D.M. Jackson and S.A.Vanstone, eds),* Academic Press, Toronto 1984, pp. 85-122.

[6] R. Calderbank, W.M. Kantor: *The geometry of two weight-codes, Bull.London Math.Soc* (1986),97-122.

[7] R.H.F.Denniston: *Some maximal arcs in finite projective planes,* *Journal of Combinatorial Theory* **6** (1969),317-319.

[8] Y.Edel, J.Bierbrauer: *Twisted BCH-codes,* to appear in *Journal of Combinatorial Designs.*

[9] A. Gulliver: *Two New Optimal Ternary Two-Weight Codes and Strongly Regular Graphs,Discrete Mathematics* **149**(1996),83-92.

[10] F.J.McWilliams, N.J.Sloane: *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam 1977.