A family of highly symmetric codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

Stefano Marcugini and Fernanda Pambianco
Dipartimento di Matematica
Università degli Studi di Perugia
Perugia (Italy)

Abstract

We define a class of codes admitting a large automorphism group. This family contains the binary extended Hamming code, the hexacode, the Golay codes, the Pless symmetry codes as well as the $[16, 4, 12]_8$-codes constructed in [4]. A computer search resulted in the construction of codes with new parameters $[28, 7, 18]_8$, $[32, 8, 20]_8$ and $[39, 13, 17]_4$ belonging to this family.

1 Introduction

We define a class of linear codes in terms of the action of a group of symmetries. The group of symmetries is a direct product $G \times \langle\phi\rangle$, where G is a regular subgroup of the symmetric group S_k and ϕ is the Frobenius automorphism of the field extension $\mathbb{F}_{q^r}|\mathbb{F}_q$. The parameters of the codes in question are $[(r + 1)k, k, d]_{q^r}$. The group $G \times \langle\phi\rangle$ has two orbits, of lengths k and rk, respectively, on the coordinates of the code. In Section 2 we give a precise definition of the action of the group and prove that some of the most famous codes, the Golay codes, the hexacode, the binary extended Hamming code and the Pless symmetry codes, belong to the family. For the sake of illustration we use one of the $[16, 4, 12]_8$ NMDS-codes constructed in [4]. Section 3 reports the results of a computer search for codes with new parameters belonging to the family. The new code parameters are $[32, 8, 20]_8$, $[28, 7, 18]_8$ and $[39, 13, 17]_4$. The full automorphism groups of the new codes are described in Section 4. The presence of a large automorphism group tends to give a better understanding of the code. We demonstrate this in Section 5 by giving a synthetic construction of the more symmetric of the $[16, 4, 12]_8$-codes and determining its weight distribution.

2 A family of codes

Let a projective $[n, k, d]_q$-code $\mathcal{C}$ be described by a generator matrix A. The set of n points in projective $(k-1)$-dimensional geometry $PG(k-1, q)$ generated by the columns of A describes the code geometrically. Define the automorphism group $Aut(\mathcal{C})$ as the stabilizer of the point set under the action of $P\Gamma L(k, q)$. Matrices from $GL(k, q)$ act from the left on column vectors. Denote conjugation by $g^h = hgh^{-1}$. Consequently the image of matrix M under a field automorphism ϕ is denoted by M^ϕ. The reason is that M^ϕ acts like the conjugate of M under ϕ. Identify the permutation $\pi \in S_k$ with the permutation matrix, which has entry 1 in row i and column $\pi(i)$, for all i.

We describe a family of linear codes, as follows. Consider the field extension $\mathbb{F}_{q^r}|\mathbb{F}_q$. Let the Frobenius automorphism be defined by $\phi(x) = x^q$. It generates the Galois group $Gal(\mathbb{F}_{q^r}|\mathbb{F}_q) \cong Z_r$. Let $G \subset S_k$ be a regular permutation group on k symbols and P a point in $PG(k-1, q^r)$ generated by $s \in \mathbb{F}_{q^r}^k$ and $\mathcal{O}$ the orbit of P under the action of the direct product $G \times \langle\phi\rangle$, where G permutes the indices and ϕ acts coordinatewise. Here $\mathcal{O}$ should be chosen different from the orbit of length k consisting of the elementary (weight 1) vectors. Let A be the $(k, k + |\mathcal{O}|)$-matrix whose first k columns form the identity matrix, whose remaining columns are representatives of the elements of $\mathcal{O}$.

Let $\mathcal{C} = \mathcal{C}(q, r, G, P)$ be the code with A as generator matrix. Clearly $\mathcal{C}$ is a q^r-ary code of dimension k and length $k + |\mathcal{O}|$. The problem is to find $P \in PG(k-1, q^r)$ such that the minimum distance d is large. Observe that the first k columns of A (the identity matrix) form an orbit under the action of $G \times \langle\phi\rangle$. It follows that $G \times \langle\phi\rangle$ is a subgroup of the automorphism group of $\mathcal{C}$.

As an illustration we use the $[16,4,12]_8$ NMDS-codes constructed in [4]. It was shown in [4] that there are exactly two non-equivalent $[16,4,12]_8$-codes. The first of those codes, call it $\mathcal{A}_1$, can be described as $\mathcal{C}(2,3,E_4,A_1)$, where E_4 is the Klein group in its natural action on 4 points and $A_1 = (1:\epsilon^3:\epsilon^2:\epsilon)$. The second $[16,4,12]_8$-code $\mathcal{A}_2$ is $\mathcal{C}(2,3,Z_4,A_2)$, where Z_4 is the cyclic group of order 4 and $A_2 = (1:\epsilon:\epsilon^3:\epsilon^2)$. A generator matrix of $\mathcal{A}_1$ is

$$A = \left(\begin{array}{cccc|cccc|cccc|cccc} 1 & 0 & 0 & 0 & a_1 & a_2 & a_3 & a_4 & a_1^2 & a_2^2 & a_3^2 & a_4^2 & a_1^4 & a_2^4 & a_3^4 & a_4^4 \\ 0 & 1 & 0 & 0 & a_2 & a_1 & a_4 & a_3 & a_2^2 & a_1^2 & a_4^2 & a_3^2 & a_2^4 & a_1^4 & a_4^4 & a_3^4 \\ 0 & 0 & 1 & 0 & a_3 & a_4 & a_1 & a_2 & a_3^2 & a_4^2 & a_1^2 & a_2^2 & a_3^4 & a_4^4 & a_1^4 & a_2^4 \\ 0 & 0 & 0 & 1 & a_4 & a_3 & a_2 & a_1 & a_4^2 & a_3^2 & a_2^2 & a_1^2 & a_4^4 & a_3^4 & a_2^4 & a_1^4 \end{array}\right)$$

Here $a = (a_1,a_2,a_3,a_4) = (1,\epsilon^3,\epsilon^2,\epsilon)$. By construction the group $E_4 \times \langle\phi\rangle \cong E_4 \times Z_3$ of order 12 is a subgroup of $Aut(\mathcal{A}_1)$.

Let $C(a) = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \\ a_3 & a_4 & a_1 & a_2 \\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}$ where $a \in \mathbb{F}_8^4$. Matrices of this type may be considered as analogues of circulant matrices. Circulants are obtained when the underlying permutation group is cyclic. Choosing $a = (1,\epsilon^3,\epsilon^2,\epsilon)$ we obtain a Klein group $V = \langle C(a), C(\phi(a))\rangle = \{I, C(a), C(\phi(a)), C(\phi^2(a))\} \subset Aut(\mathcal{A}_1)$. The Klein group V commutes with E_4, and $V\langle\phi\rangle$ is an alternating group on 4 objects. We have in fact

$$Aut(\mathcal{A}_1) = E_4 \times V\langle\phi\rangle \cong E_4 \times A_4$$

of order 48, whereas $Aut(\mathcal{A}_2)$ is the group $Z_4 \times \langle\phi\rangle \cong Z_{12}$ used for its construction. Observe also that the $[16,4,12]_8$-codes can be used to construct good binary codes by concatenation. For instance, $[16,4,12]_8$ as outer code with $[7,3,4]_2$ as inner code produce an $[112,12,48]_2$-code, realizing the highest known value of d.

We proceed to show that some of the most famous codes belong to the family. If Z_k is the cyclic group in its natural action, then $\mathcal{C}(q,r,Z_k,P)$ is a quasi-cyclic code. Codes $\mathcal{C}(q,r,G,P)$ are interesting even in the case $r=1$ when the contribution of the Galois group vanishes. Consider $\mathcal{C}(2,1,S_4,P)$, where $P = (0:1:1:1)$. As P is in an orbit of length 4 we obtain the generator matrix

$$\left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

Clearly the code is the extended binary Hamming code $[8,4,4]_2$. Likewise $\mathcal{C}(4,1,S_3,(1:1:\omega))$ has generator matrix

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & \omega \\ 0 & 1 & 0 & 1 & \omega & 1 \\ 0 & 0 & 1 & \omega & 1 & 1 \end{array}\right)$$

This describes the hexacode $[6,3,4]_4$, geometrically the hyperoval in $PG(2,4)$.

The fact that the Pless symmetry codes belong to the family follows directly from the basic theory, see [8, 3].

The binary Golay code is $\mathcal{C}(2,1,Z_{12},P)$, where Z_{12} is generated by $(1,2,8,4,10,11,5,9,6,12,3,7)$ and $P=(1:0:1:0:0:1:0:0:1:1:1:1)$. The corresponding generator matrix is $(I|M)$, where

$$M=\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

It is a natural generalization to admit subgroups G of order k not in the symmetric group S_k but in the monomial group $Z_{q-1} \wr S_k$ of order $(q-1)^k k!$ The ternary Golay code is a member of this family. It is $\mathcal{C}(3,1,Z_6,P)$, where Z_6 is generated by $s=(1,2,3,4,5,6)m(2,5,6)$ (at first apply the permutation, then multiply by -1 in coordinates $2,5,6$), and $P=(0:1:1:1:1:1)$. In fact, we obtain the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 & 1 & 1 & 0 \end{pmatrix}$$

of the ternary Golay code.

3 New codes

We used a computer search to find codes belonging to the family with record-breaking parameters. The following table summarizes the results.

name	parameters	description
$\mathcal{B}_1$	$[32,8,20]_8$	$\mathcal{C}(2,3,D_8,B_1),\ B_1=(0:1:\epsilon^3:\epsilon^5:\epsilon^2:\epsilon^4:\epsilon^6:1)$
$\mathcal{B}_2$	$[32,8,20]_8$	$\mathcal{C}(2,3,D_8,B_2),\ B_2=(0:1:\epsilon^3:\epsilon^6:\epsilon^5:\epsilon^2:\epsilon^4:1)$
$\mathcal{B}_3$	$[32,8,20]_8$	$\mathcal{C}(2,3,D_8,B_3),\ B_3=(0:1:\epsilon^5:1:\epsilon^2:\epsilon:\epsilon^6:\epsilon^3)$
$\mathcal{B}_4$	$[32,8,20]_8$	$\mathcal{C}(2,3,D_8,B_4),\ B_4=(0:1:\epsilon^5:1,\epsilon^4:\epsilon^2:\epsilon^3:\epsilon^6)$
$\mathcal{B}_5$	$[32,8,20]_8$	$\mathcal{C}(2,3,D_8,B_5),\ B_5=(0:1:\epsilon^5:1:\epsilon^6:\epsilon^3:\epsilon^2:\epsilon)$
$\mathcal{B}_6$	$[32,8,20]_8$	$\mathcal{C}(2,3,D_8,B_6),\ B_6=(0:1:\epsilon^5:1:\epsilon^3:\epsilon^2:\epsilon:\epsilon^6)$
$\mathcal{B}_7$	$[32,8,20]_8$	$\mathcal{C}(2,3,D_8,B_7),\ B_7=(0:1:\epsilon^5:1:\epsilon^3:\epsilon^6:\epsilon:\epsilon^2)$
$\mathcal{C}_1$	$[28,7,18]_8$	$\mathcal{C}(2,3,Z_7,C_1),\ C_1=(0:1:\epsilon^5:1:\epsilon^6:\epsilon:\epsilon^2)$
$\mathcal{C}_2$	$[28,7,18]_8$	$\mathcal{C}(2,3,Z_7,C_2),\ C_2=(1:\epsilon:\epsilon^5:\epsilon^4:\epsilon^4:\epsilon^5:\epsilon)$
$\mathcal{C}_3$	$[28,7,18]_8$	$\mathcal{C}(2,3,Z_7,C_3)=\mathcal{C}(2,3,M,C_3),$
		$C_3=(1:\epsilon^6:\epsilon^3:\epsilon^5:\epsilon^5:\epsilon^3:\epsilon^6)$
$\mathcal{C}_4$	$[28,7,18]_8$	$\mathcal{C}(2,3,M,C_4),\ C_4=(1:1:1:\epsilon^4:\epsilon^4:\epsilon^3:\epsilon^3)$
$\mathcal{D}$	$[39,13,17]_4$	$\mathcal{C}(2,2,Z_{13},D),$
		$D=(0:\omega:1:\omega:\overline{\omega}:1:1:1:1:\omega:\overline{\omega}:1:\overline{\omega})$

We represent the field $\mathbb{F}_8$ in the form $\mathbb{F}_8=\mathbb{F}_2(\epsilon)$, where $\epsilon^3=\epsilon^2+1$. The group Z_7 is the cyclic group in its natural operation on 7 objects, D_8 is the dihedral group of order 8 generated by the permutations $(1,2,3,4)(5,6,7,8),(1,5)(2,6)(3,7)(4,8)$, and M is generated by the diagonal matrix $diag(1,\epsilon,\epsilon^2,\epsilon^3,\epsilon^4,\epsilon^5,\epsilon^6)$. The codes $\mathcal{B}_i$ have dual distance $d'=6$, the $\mathcal{C}_j$ have $d'=5$ with the exception of $\mathcal{C}_3$ which has $d'=4$. The quaternary code $\mathcal{D}$ has $d'=7$.

The best $[32,8]_8$-codes hitherto known have $d = 19$, see [2, 11]. We searched for 8-dimensional codes $\mathcal{C}(2,3,G,P)$, where $G \subset S_8$ is a permutation group of order 8 in its regular action on 8 symbols. Only in case $G = D_8$ a minimum distance of $d = 20$ was obtained.

We also performed an exhaustive search for octal codes $\mathcal{C}(2,3,G,P)$, where G is a regular permutation group on $k < 8$ objects. Only the $[28,7,18]_8$-codes $\mathcal{C}_j,\ j = 1,2,3$ have new parameters.

4 Symmetries

$Aut(\mathcal{C}_1)$ is the cyclic group of order 21 used for the construction. $Aut(\mathcal{C}_2)$ has order 42. It is the direct product of the Galois group $\langle\phi\rangle$ and the dihedral group of order 14 generated by Z_7 and the involutory permutation $(2,7)(3,6)(4,5)$.

Code $\mathcal{C}_3$ is particularly interesting. $Aut(\mathcal{C}_3)$ contains $Aut(\mathcal{C}_2)$ as a subgroup and has the unusually large order $3528 = 8 \times 9 \times 49$. Let $\pi = (1,2,3,4,5,6,7),\ m = diag(1,\epsilon,\epsilon^2,\epsilon^3,\epsilon^4,\epsilon^5,\epsilon^6)$. The elementary abelian subgroup $S = \langle\pi, m\rangle$ of order 7^2 is a normal subgroup of $Aut(\mathcal{C}_3)$. Let $\sigma = (2,4,3,7,5,6) \in Aut(\mathcal{C}_3)$. Then σ maps $\pi \mapsto \pi^3,\ m \mapsto m^3$ under conjugation, whereas $\phi : \pi \mapsto \pi,\ m \mapsto m^3$.

Let $N = \begin{pmatrix} 1 & \epsilon & \epsilon^4 & \epsilon^2 & \epsilon^2 & \epsilon^4 & \epsilon \\ \epsilon^6 & \epsilon^4 & \epsilon^4 & \epsilon^6 & \epsilon^3 & \epsilon^2 & \epsilon^3 \\ \epsilon^3 & \epsilon^5 & \epsilon^2 & \epsilon & \epsilon^2 & \epsilon^5 & \epsilon^3 \\ \epsilon^5 & \epsilon^4 & \epsilon^5 & \epsilon & \epsilon^6 & \epsilon^6 & \epsilon \\ \epsilon^5 & \epsilon & \epsilon^6 & \epsilon^6 & \epsilon & \epsilon^5 & \epsilon^4 \\ \epsilon^3 & \epsilon^3 & \epsilon^5 & \epsilon^2 & \epsilon & \epsilon^2 & \epsilon^5 \\ \epsilon^6 & \epsilon^3 & \epsilon^2 & \epsilon^3 & \epsilon^6 & \epsilon^4 & \epsilon^4 \end{pmatrix}$

The columns of N are scalar multiples of the images of P under $\langle\pi\rangle$. We have $N^2 = \sigma^3 = (2,7)(3,6)(4,5)$. In particular N represents an element ν of order 4 in $PGL(7,8)$. A direct calculation shows

$$NN^\phi = N^{\phi^2},\ N^\phi N = \sigma^3 N^{\phi^2} = (N^{\phi^2})^{-1}.$$

It follows that $Q = \langle N, N^\phi\rangle$ is a quaternion group of order 8 and a Sylow-2-subgroup of $Aut(\mathcal{C}_3)$. The semidirect product $Q\langle\phi\rangle$ of Q with a group of order 3 is isomorphic to $SL(2,3)$. Another direct calculation shows $N\sigma^2 = (\sigma^2 N)^\phi$. It follows $N\sigma^2 = \sigma^2 N^\phi$ and $N = \sigma^2 N^\phi \sigma^{-2}$. We see that $\sigma^2\phi$ commutes with

ν, and therefore with all elements of $SL(2,3)$. This clarifies the structure of the automorphism group:

$$Aut(\mathcal{C}_3) = S(Z \times Q\langle\phi\rangle) \cong (Z_7 \times Z_7)(Z_3 \times SL(2,3)).$$

There is a striking similarity with the structure of $Aut(\mathcal{A}_1)$, but $Aut(\mathcal{C}_3)$ is richer, involving additional types of symmetries. The presence of the diagonal matrices in $Aut(\mathcal{C}_3)$ shows that $\mathcal{C}_3$ can also be described as $\mathcal{C}(2,3,\langle m\rangle,P)$ with the same P as above, where $\langle m\rangle \subset PGL(7,8)$ affords the diagonal action just described. This motivated the search for codes $\mathcal{C}(2,3,\langle m\rangle,P)$ in general, which resulted in $\mathcal{C}_4$. $Aut(\mathcal{C}_4)$ is the direct product of the Galois group and a Frobenius group of order 21.

$Aut(\mathcal{D})$ contains $F \times \langle\phi\rangle$, where

$$F = \langle(1,2,3,4,5,6,7,8,9,10,11,12,13),(2,5,4,13,10,11)(3,9,7,12,6,8)\rangle$$

is a Frobenius group of order 13×6.

5 A synthetic construction

We have not been able to obtain general bounds on the minimum distance of the codes in our family. In some individual cases the presence of a large symmetry group enables us to determine the parameters in a theoretic fashion and thus obtain a better understanding of the code. We illustrate with the $[16,4,12]_8$-code $\mathcal{A}_1$ whose automorphism group $H = E_4 \times V\langle\phi\rangle \cong E_4 \times A_4$ and generator matrix A have been described in Section 2.

Denote by $\mathcal{K}$ the family of 16 points in $PG(3,8)$ generated by the columns of A. The fact that $\mathcal{A}_1$ has minimum distance 12 is equivalent to the following:

Theorem 1. *Each plane of $PG(3,8)$ intersects $\mathcal{K}$ in at most 4 points. No 3 points of $\mathcal{K}$ are collinear ($\mathcal{K}$ is a cap).*

The first claim of Theorem 1 states that $\mathcal{A}_1$ has minimum distance 12. The second claim is that the dual code is a $[16,12,4]_8$-code.

Observe that $E_4 \times V$ acts transitively on $\mathcal{K}$. Denote the columns of A by $c_{ij}, i = 0,1,2,3; j = 1,2,3,4$, in lexicographic order. Let us call **blocks** the E_4-orbits contained in $\mathcal{K}$. The vectors c_{ij} form block B_i, where $i = 0,1,2,3$. Observe that the matrix with the c_{1j} as columns is $C(a)$. Similarly the columns from B_2 form $C(\phi(a))$ and the columns from B_3 form $C(\phi^2(a)) =$

$C(a)C(\phi(a))$. Denote by Q_{ij} the projective point generated by c_{ij}. We wish to prove that no plane in $PG(3,8)$ contains more than 4 of the points Q_{ij}.

An **ordered design** $OD_\lambda(t,n,v)$ is an $(\lambda\frac{v!}{(v-t)!},n)$-array with entries from a v-set such that the entries in each row are different and in the projection onto any set of t columns, each tuple of t distinct entries occurs precisely λ times (see [5]). As the ordering of the rows is irrelevant we may see an OD as a multiset of rows, and each row may be interpreted as an injective mapping from an n-set into a v-set. This makes it evident that the notion of an OD is a generalization of the notion of a t-transitive group of permutations (generalization from groups to multisets, from permutations to injective mappings), see also the introduction of [1]. Ordered designs are also known as **orthogonal arrays of type I**, see [6, 9].

Assume an $OD_\lambda(t,n,v)$ admits a group of order v in its action on the entries as a group of automorphisms. It is the difference set idea to represent the OD by a set of representatives for the orbits on the rows. This leads to the following definition in the special case when the group is cyclic and $t=2$.

Definition 1. *A* **D-matrix** $D_\lambda(2,n,v)$ *is a* $(\lambda(v-1),n)$*-array with entries from the cyclic group* Z_v *satisfying:*
for columns i,j*, where* $i\neq j$*, among the quotients of the entries in column* i *and the entries in column* j *in the same row each element* $\neq 1$ *of* Z_v *occurs precisely* λ *times.*

It is clear that a matrix $D_\lambda(2,n,v)$ exists if and only if $OD_\lambda(2,n,v)$ exists admitting the corresponding cyclic group as a group of automorphisms.

We start from a construction of $D_2(2,4,7)$, where we represent the group of entries as the multiplicative group of $\mathbb{F}_8$.

Lemma 1. *Let* $a=(a_1,a_2,a_3,a_4)\in\mathbb{F}_8^4$*, where the entries are nonzero and pairwise distinct. Then the orbit of* a *under* $E_4\times\langle\phi\rangle$ *forms the rows of an* $D_2(2,4,7)$.

Lemma 1 is implied by the following fact, which is obviously true:

Lemma 2. *Let* $a\in\mathbb{F}_8\setminus\mathbb{F}_2$*. Then* $\{a,a^2,a^4,1/a,1/a^2,1/a^4\}=\mathbb{F}_8\setminus\mathbb{F}_2$.

We conclude that in our present situation the columns of blocks B_1,B_2 and B_3 together form a $D_2(2,4,7)$, written in transposed form.

Let E be a plane in $PG(3,8)$ containing three points from one block. Because of the action of H we can assume the block is B_0 and the points are

Q_{01}, Q_{02}, Q_{03}. These points generate the plane with equation $X_4 = 0$, which meets $\mathcal{K}$ only in these three points.

Let E be a plane, which meets some block in precisely two points. Because of H we can assume these points are Q_{0a}, Q_{0b}. Let $\{1, 2, 3, 4\} = \{a, b, c, d\}$ and assume $Y = (y_1 : y_2 : y_3 : y_4)$ is a third point from $\mathcal{K}$ on E. Then E has equation $y_c X_d = y_d X_c$, equivalently $\frac{X_c}{X_d} = \frac{y_c}{y_d}$. It follows from Lemma 1 that $|E \cap \mathcal{K}| = 4$ in this case. As all remaining planes contain at most one point from each of the blocks, the main claim of Theorem 1 is proved.

Finally assume some three points of $\mathcal{K}$ are on a line l. As there are 9 planes incident with l and as each plane contains at most 4 points from $\mathcal{K}$ this yields the contradiction $16 = |\mathcal{K}| \leq 3 + 9 = 12$.

This concludes the proof of Theorem 1. We note that the minimum distance of $\mathcal{C}_3$ can be determined in a similar fashion. In the case of $\mathcal{A}_1$ we can do more.

The weight distribution of $\mathcal{A}_1$.

The weight distribution of $\mathcal{A}_1$ is equivalent to the determination of the numbers $n_i, i = 0, \ldots, 4$ where n_i is the number of planes intersecting $\mathcal{K}$ in precisely i points. As $\mathcal{A}_1$ is NMDS it suffices to determine n_4. The remaining n_i are then uniquely determined. This will also become clear in the sequel. As $\mathcal{K}$ is a cap we have $n_3 + 3n_4 = \binom{16}{3} = 560$.

Let us call E an i-plane if $|E \cap \mathcal{K}| = i$. The **type** of a plane E describes the distribution of $E \cap \mathcal{K}$ on the blocks. For example, a plane of type $(2, 2)$ is a 4-plane with 2 points from one block and two points from some other block. All 4-planes have one of the types $(2, 2)$, $(2, 1, 1)$ or $(1, 1, 1, 1)$ (transversal).

Observe the action of E_4 and V on the points Q_{ij}. Both are Klein groups, E_4 acts naturally on the second index, fixing the first (it acts on each block), V does the opposite (it permutes blocks). Define a **half-block** to be a pair of points from a block, with second indices $1, 2$ or $3, 4$. Each half-block is on 6 four-planes of type $(2, 1, 1)$, on two 3-planes (with all points from a block) and on one 2-plane. All other pairs of second indices yield 6 four-planes of type $(2, 2)$. Each pair of points from a block not forming a half-block is on 6 four-planes of type $(2, 2)$, on two 3-planes (with all points from a block) and on one 2-plane. The total number of 4-planes of type $(2, 2)$ is therefore

$16 \cdot 6/2 = 48$, the number of 4-planes of type $(2, 1, 1)$ is $8 \cdot 6 = 48$.

All remaining 4-planes are of transversal type. One orbit of transversal 4-planes contains

$$\{Q_{01}, Q_{14}, Q_{24}, Q_{34}\}.$$

It has length 16 (the block above is stabilized by ϕ). A second orbit of transversal 4-planes contains

$$\{Q_{01}, Q_{12}, Q_{23}, Q_{34}\}.$$

It has length 12, the stabilizer of the block above being the Klein group $\langle C(a)Z((12)(34)), C(\phi(a))Z((13)(24))\rangle$. These are all the 4-planes. We have $n_4 = 48 + 48 + 16 + 12 = 124$, hence $n_3 = 64$. One orbit of 3-planes is described by the sets of 3 points contained in a block. The second orbit, of full length 48, contains the plane generated by

$$\{Q_{01}, Q_{11}, Q_{22}\}.$$

Observe that the three images of $\{Q_{01}, Q_{11}, Q_{22}\}$ under the action of $E_4 \times V$ containing Q_{01} are $\{Q_{01}, Q_{11}, Q_{22}\}, \{Q_{01}, Q_{11}, Q_{32}\}, \{Q_{01}, Q_{22}, Q_{32}\}$. They are all subsets of $\{Q_{01}, Q_{11}, Q_{22}, Q_{32}\}$, and also $\{Q_{11}, Q_{22}, Q_{32}\}$ is an image under $E_4 \times V$. This shows that our orbit of 3-planes is defined by all 3-subsets of the orbit of $\{Q_{01}, Q_{11}, Q_{22}, Q_{32}\}$ (that orbit has length 12, leading indeed to 48 such 3-subsets and 48 such 3-planes). Denote these 4-subsets of $\mathcal{K}$ as **special quadruples.**

Proposition 1. *Consider $\mathcal{K}$ as ground set and the following family of 140 quadruples (4-subsets):*

- *The 124 intersections of 4-planes with $\mathcal{K}$,*
- *the four blocks,*
- *12* **special** *quadruples arising from the 48 intersections with transversal 3-planes as described above (if $T = \{a, b, c\}$ is the intersection with a transversal 3-plane, then the quadruple $\{a, b, c, d\}$ is the union of all four images of T under $E_4 \times V$, which contain a, b or c).*

Then the quadruples define a Steiner quadruple system $S(3, 4, 16)$.

Proof. Let T be a 3-set. If T is contained in a block then this block is the only quadruple containing T. If T intersects a block in 2 points, then the plane generated by T is a 4-plane and this yields the only quadruple containing T. Let T be transversal and E the plane generated by T. If E is a 4-plane then $E \cap \mathcal{K}$ is the only quadruple containing T, if E is a 3-plane then T is contained in precisely one special quadruple. $\square$

We know n_4, n_3. The standard equations yield the weight distribution.

Proposition 2. *The numbers n_i of planes intersecting $\mathcal{K}$ in precisely i points are the following:*

$$n_4 = 124,\ n_3 = 64,\ n_2 = 144,\ n_1 = 192,\ n_0 = 61.$$

The weight distribution of $\mathcal{A}_1$ is

$$A_0 = 1,\ A_{12} = 868,\ A_{13} = 448,\ A_{14} = 1008,\ A_{15} = 1344,\ A_{16} = 427.$$

References

[1] J.Bierbrauer and Y.Edel: *Theory of perpendicular arrays,* *Journal of Combinatorial Designs* **6** (1994),375-406.

[2] A.E. Brouwer: Data base of bounds for the minimum distance for binary, ternary and quaternary codes,
URL http://www.win.tue.nl/win/math/dw/voorlincod.html or
URL http://www.cwi.nl/htbin/aeb/lincodbd/2/136/114 or
URL ftp://ftp.win.tue.nl/pub/math/codes/table[234].gz.

[3] P. J. Cameron and J. H. van Lint: *Designs, graphs, codes and their links,* Cambridge University Press 1991.

[4] S.Marcugini, A.Milani and F.Pambianco: *NMDS-codes of maximal length over $GF(q)$, $8 \leq q \leq 11$*
IEEE Transactions on Information Theory **48** (2002), 963-966 .

[5] The CRC Handbook of Combinatorial Designs,
C.J. Colbourn and J.H.Dinitz (eds.), CRC Press 1996.

[6] Hedayat, N.J.A.Sloane and J.Stufken:
Orthogonal Arrays: Theory and Applications, Springer 1999.

[7] V. Pless: *Symmetry codes over $GF(3)$ and new 5-designs,*
Journal of Combinatorial Theory A **12** (1972), 119-142.

[8] V. Pless: *Symmetry codes and their invariant subcodes,*
Journal of Combinatorial Theory A **18** (1975), 116-125.

[9] C.R. Rao: *Combinatorial arrangements analogous to orthogonal arrays,* *Sankhya A* **23**(1961),283-286.

[10] R.C.Singleton: *Maximum distance q-ary codes,*
IEEE Transactions on Information Theory **10** (1964), 116-118.

[11] C. Xing and S.Ling: *A class of linear codes with good parameters,*
IEEE Transactions on Information Theory **46** (2000), 2184-2188.