ELSEVIER

Discrete Mathematics 208/209 (1999) 235–246

DISCRETE MATHEMATICS

Monomial embeddings of the Klein curve

Iwan M. Duursma

AT&T Labs-Research, Room 2D-147, 600 Mountain Avenue, Murray Hill, NJ 07974, USA

Received 5 March 1997; revised 25 November 1997; accepted 22 December 1997

Abstract

The Klein curve is defined by the smooth plane model $X^3Y + Y^3Z + Z^3X = 0$. We give all embeddings in higher dimension with a linear action of the automorphism group. The curve has 24 flexpoints, i.e. points where the tangent intersects with multiplicity three. For even characteristic, the embeddings yield interesting configurations of the flexpoints and good linear codes.

For the Klein curve in even characteristic, we give the essentially unique embedding of degree six in three dimensions with the property that no plane contains more than five flexpoints. The flexpoints are defined over the field of eight elements. In PG(3, 8), there exists a 'knot', a unique point not in any plane through five flexpoints. Section 1 gives the combinatorial properties of the configuration. Section 2 describes some of the special behaviour of the Klein curve in even characteristic. Section 3 gives the construction of a best possible, easily decodable code of type [24, 16, 7] over $\mathbf{F}_8$. Section 4 describes, for arbitrary characteristic, the invariant embeddings of the Klein curve.

1. Configuration in PG(3, 8)

We give a configuration of 25 planes in PG(3, 8) such that points are contained in one, three or five of the planes. The interpretation in terms of the Klein curve follows in the next section.

Theorem 1. *For a set of N points in* PG(3, 8), *such that no three are on a line, let n_i be the number of planes intersecting the set in precisely i points. If at most three n_i are nonzero, then either $N = 65$ with $n_1 = 65$, $n_9 = 520$, or $N = 25$* with $n_1 = 175$, $n_3 = 200$, $n_5 = 210$.

☆ Presented at Combinatorics'96, in honour of Giuseppe Tallini, Assisi, Italy, 8–14 September 1996.

E-mail address: duursma@research.att.com (I.M. Duursma)

0012-365X/99/$ - see front matter
PII: S0012-365X(99)00074-6

Table 1
Configuration in PG(2, 8) and its dual

	7	42	24		7	42	24
7	3	6	0	7	3	6	0
42	1	4	4	42	1	4	4
24	0	7	2	24	0	7	2

Proof. The result follows from numerical constraints. After solving

$$\begin{pmatrix} \binom{i}{1} & \binom{j}{1} & \binom{k}{1} \\ \binom{i}{2} & \binom{j}{2} & \binom{k}{2} \\ \binom{i}{3} & \binom{j}{3} & \binom{k}{3} \end{pmatrix} \begin{pmatrix} n_i \\ n_j \\ n_k \end{pmatrix} = \begin{pmatrix} 73\binom{N}{1} \\ 9\binom{N}{2} \\ \binom{N}{3} \end{pmatrix}$$

for n_i, n_j, n_k, for $\{i,j,k\} \subset \{1,2,\ldots,10\}$, the equation $n_i + n_j + n_k = 585$ for N has few solutions in integers, and only two feasible cases remain. □

The case $N = 65$ is realized by an ovoid, in particular by the rational points of an elliptic quadric [11]. For the case $N = 25$, we first consider a configuration in a plane $\mathscr{H}$ of PG(3, 8). Let $\mathscr{F}$ be a Fano plane in $\mathscr{H}$. Among the lines of $\mathscr{H}$ not in $\mathscr{F}$ there are 42 lines that pass through a point of $\mathscr{F}$ and 24 lines that do not. Among the points of $\mathscr{H}$ not in $\mathscr{F}$ there are 42 points that lie on a line of $\mathscr{F}$ and 24 points that do not. Table 1 gives the tactical decomposition. The classes in the decomposition are orbits under the action of the automorphism group SL(3,2) of $\mathscr{F}$. We choose as generators

$$S = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

The Frobenius collineation $(x : y : z) \mapsto (x^2 : y^2 : z^2)$ acts on the classes. It divides the class $\mathscr{P}$ of 24 points into eight triples (P, P^2, P^4). Through a point $P \in \mathscr{P}$ pass seven lines that intersect $\mathscr{P}$ in four points plus the two lines PP^2, PP^4. We turn this into a partial geometry pg($K = 4$, $R = 8$, $T = 4$) by considering P, P^2, P^4 to be collinear with the virtual point O. This gives a set $\mathscr{L}$ of $42 + 8 = 50$ lines, with each line intersecting $\mathscr{P} \cup O$ in $K = 4$ points, and with $R = 8$ lines through each $P \in \mathscr{P} \cup O$.

Proposition 1. *The pair* $(\mathscr{P} \cup O, \mathscr{L})$ *defines a partial geometry* pg(4, 8, 4), *or a quasi-symmetric* $2 - (25, 4, 1)$ *design. It has automorphism group* (Frob) $\times$ SL(3, 2). *The dual partial geometry* pg(8, 4, 4), *or the block graph of the design, is a strongly regular graph* srg(50, 28, 15, 16). *Its adjacency matrix* A *has eigenvalues* $(-4, 3, 28)$ *and satisfies* $A^2 + A = 16J + 12I$.

Table 2
Configuration in PG(3, 8)

	7	24	42	8	168	168	168
1	7	24	42	0	0	0	0
14	3	0	6	4	36	12	12
42	3	0	6	0	16	24	24
24	0	2	7	1	21	7	35
168	0	2	7	1	21	23	19
168	1	4	4	2	18	22	22
168	1	4	4	0	24	20	20

Table 3
Dual configuration in PG(3, 8)

	1	14	42	24	168	168	168
7	1	6	18	0	0	24	24
24	1	0	0	2	14	28	28
42	1	2	6	4	28	16	16
8	0	7	0	3	21	42	0
168	0	3	4	3	21	18	24
168	0	1	6	1	23	22	20
168	0	1	6	5	19	22	20

Proof. See [12,19] for definitions and general properties. The $2-(25,4,1)$ design was first found by [5,23]. The design has 504 automorphisms. The other nonisomorphic designs with the same parameters all have less automorphisms [17]. □

The group $\mathrm{SL}(3,2)$ acts on points from the left, and on lines from the right. Since it is closed under transposition, the orbits of points and lines are similar. For the action of SL(3,2) on PG(3, 8) this is no longer the case. A faithful four-dimensional representation of SL(3,2) fixes either a point or a plane. For a representation that fixes the plane at infinity, let

$$S = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The action on the points in the plane at infinity is the one we have seen above. But the action on the planes is different from that on the points. Tables 2 and 3 give the sizes of the orbits and the tactical decomposition. Actually there are nine orbits. Three orbits of 56 points each are essentially the same. They differ by the action of the Frobenius collineation and are represented by their union. Similarly for three orbits of 14 planes each. The planes in the fourth and first column of the dual configuration yield a set $\mathscr{P}' \cup O'$ of 25 planes with only a few distinct small intersection numbers. This gives the following result.

Theorem 2. *The plane of* $P' \cup O'$ *realize the case* $N = 25$ *in Theorem* 1. *A point of* PG(3, 8) *is contained in either one* (175), *three* (200), *or five* (210) *of the* 25 *planes.*

2. The Klein curve

We will interpret the configuration of 25 planes $\mathscr{P}' \cup O'$ in PG(3, 8) in terms of the Klein curve and its dual curve. The Klein curve

$$K\colon X^3Y + Y^3Z + Z^3X = 0$$

is the essentially unique plane curve of degree four with 168 automorphisms. The curve has good reduction for $p \neq 7$. Other models are also used [6,7,2,10]. The Hessian of the Klein curve has equation

$$H\colon X^5Z + Y^5X + Z^5Y - 5X^2Y^2Z^2 = 0.$$

It has good reduction only for $p \neq 2, 7$. For $p \neq 2, 3$, the dual curve of the Klein curve has equation

$$K^*\colon 4K^3 - 27H^2 = 0.$$

For $p = 2$ and $p = 3$, respectively, the dual curve K^* is isomorphic to the Hessian H and to the curve K, respectively. In both cases, the natural map $K \to K^*$ is purely inseparable. The case $p = 3$ is dealt with in [14, Exercise 2.4, Chapter IV]. For $p = 2$, we have morphisms

$$K \xrightarrow{(K_X : K_Y : K_Z)} H^{(2)} \xrightarrow{(H_X : H_Y : H_Z)} K^{(8)},$$

with factorization

$$K \xrightarrow{(y^2z : z^2x : x^2y)} H \xrightarrow{(x^2 : y^2 : z^2)} H^{(2)},$$

$$H^{(2)} \xrightarrow{(y^3+z^2x : z^3+x^2y : x^3+y^2z)} K^{(2)} \xrightarrow{(x^4 : y^4 : z^4)} K^{(8)}.$$

The morphism $K \to H$ is the reduction of the morphism

$$K \xrightarrow{(y^2z : z^2x : x^2y)} S_6\colon X^5Z + Y^5X + Z^5Y - 3X^2Y^2Z^2 = 0.$$

The curve S_6 has seven double points. In even characteristic, they are the singularities of the Hessian H. And they correspond to the seven bitangents of the Klein curve. It is straightforward to give a smooth model $\bar{S}_6$ of S_6 in three dimensions.

Klein uses the traingle $XYZ=0$ as Ref. [16]. Its three vertices O_0, O_1, O_2 are flexpoints of the Klein curve. The triangle shares 21 automorphisms with the curve. For ζ a fixed primitive seventh root of unity, they are generated by

$$\rho : (x : y : z) \mapsto (y : z : x), \quad \tau : (x : y : z) \mapsto (\zeta x : \zeta^4 y : \zeta^2 z).$$

The curve S_6 is invariant under ρ, τ. The double points are in a single orbit that is represented by $(1 : 1 : 1)$.

Lemma 1. *The functions y^2z, z^2x, x^2y intersect the Klein curve with multiplicity at least two in O_0, O_1, O_2.* So does the function xyz. The embedding $(X:Y:Z:T) = (y^2z : z^2x : x^2y : xyz)$ gives a desingularization $\bar{S}_6$ of S_6, with ideal

$$I = \langle T^2X + TY^2 + YZ^2, T^2Y + TZ^2 + ZX^2, T^2Z + TX^2 + XY^2, T^3 - XYZ \rangle.$$

Proof. The embedding is defined with the divisor $3L - 2(O_0 + O_1 + O_2)$, which is very ample. Which means by [14, Proposition 3.1, Chapter IV] applied to this particular case, that no conic exists that passes through $2(O_0 + O_1 + O_2)$. The four given relations generate the kernel of the map

$$k[X,Y,Z,T] \to k[x,y,z]/(x^3y + y^3z + z^3x),$$
$$X \mapsto y^2z, \quad Y \mapsto z^2x, \quad Z \mapsto x^2y, \quad T \mapsto xyz. \qquad \square$$

Above a regular point $(X:Y:Z)$ of S_6 lies a unique point $(X:Y:Z:T)$ of $\bar{S}_6$. For a singular point, there are two choices for T; for example, the roots of $T^2 + T + 1$ for $(X:Y:Z) = (1:1:1)$. In even characteristic, the variable T separates the points on the seven bitangents.

The divisor $\Delta = O_0 + O_1 + O_2$ is invariant under the subgroup of index 8 generated by ρ, τ. It has eight images under the automorphism group. Among them there is the sum $\Delta' = O_0' + O_1' + O_2'$ of the other three real flexpoints. Consider

$$X^3Y + Y^3Z + Z^3X = (X + Y + Z)(X^2Y + Y^2Z + Z^2X + XYZ) - (XY + YZ + ZX)^2.$$

The line $X + Y + Z$ is one of the 28 bitangents of the Klein curve. The conic $XY + YZ + ZX$ intersects the curve in the two points of the bitangent and in the six real flexpoints. It follows that the form of degree three intersects the Klein curve in $2\Delta + 2\Delta'$. The symmetry among the six real flexpoints is more obvious for the isomorphic model with equation

$$7s_1(s_1^3 + s_3) - (2s_1^2 + s_2)^2 = 0$$

for s_1, s_2, s_3 the elementary symmetric functions of X, Y, Z [10].

Theorem 3. *The automorphism group of the Klein curve acts linearly on the models K and $\bar{S}_6$; that is, the automorphisms for the two embeddings are restrictions of projective transformations of the ambient space.*

Proof. We need to prove that the divisor classes of L and $3L - 2(O_0 + O_1 + O_2)$, respectively, are invariant under the automorphism group. For L this is obvious, since the divisor class is the canonical class. On the other hand, $3L \sim 4\Delta$. And for any pair (Δ, Δ') of distinct images of Δ, we have as above that $3L \sim 2\Delta + 2\Delta'$. $\square$

We can now interpret the sets $\mathscr{P}$ of 24 points and $\mathscr{P}'$ of 24 planes which were defined in the previous section.

Theorem 4. *Up to a projective transformation of the ambient space, the set* $\mathscr{P}$ of 24 *points in* PG(2,8) *and the set* $\mathscr{P}'$ *of* 24 *planes in* PG(3,8) *are the flexpoints* $P=(x:y:z)$ *of the Klein curve* K *and their images* $P'=(y^4z^2:z^4x^2:x^4y^2:x^2y^2z^2)$ *on the desingularized dual curve* $\bar{K}^*$, *respectively.*

Proof. By the previous theorem, the set of 24 flexpoints and the set of 24 images are orbits under the linear action of SL(3,2) on PG(2,8) and PG(3,8), respectively. The orbits under the action are given in the previous section. In particular, the orbits $\mathscr{P}$ and $\mathscr{P}'$ are unique of size 24. □

There are two natural correspondences between $\mathscr{P}$ and $\mathscr{P}'$. The 24 points $P\in\mathscr{P}$ lie in the plane O' at infinity. The plane $P'=(y^4z^2:z^4x^2:x^4y^2:x^2y^2z^2)$ intersects the plane O' in the tangent at $P=(x:y:z)$. The plane $P'=(x^2y:y^2z:z^2x:xyz)$ intersects the plane O' in a tangent through $P=(x:y:z)$.

3. Linear codes

For a pair of embeddings in $\mathbf{P}^2$ and in $\mathbf{P}^3$ we define a three-error-locating code. In general, the code is two-error-correcting. Using results of the previous sections, we obtain a code over $\mathbf{F}_8$ that is actually three-error-correcting. Consider the embedding

$$(X:Y:Z:T)=(x^2y:y^2z:z^2x:xyz)$$

for points $(x:y:z)$ on the Klein curve. Over $\mathbf{F}_8$, the image of the 24 flexpoints together with the point $(0:0:0:1)$ realizes the case $N=25$ in Theorem 1. The embedding

$$(X:Y:Z:T)=(xw:yw:zw:xy+yz+zx)$$

for $w=x+y+z$, maps the projective plane onto the elliptic quadric

$$XY+YZ+ZX-(X+Y+Z)T=0.$$

Again over $\mathbf{F}_8$, the image of the 64 points $(x:y:z)$ not on the line $x+y+z=0$ together with the point $(0:0:0:1)$ realizes the case $N=65$ in Theorem 1.

In general, let $\mathscr{P}$ be a set of n points in $\mathbf{P}^2$ together with an embedding in $\mathbf{P}^3$. We will assume that no three points of $\mathscr{P}$ are collinear in $\mathbf{P}^3$. Let each point $P\in\mathscr{P}$ have a fixed affine representative (x,y,z) with image (X,Y,Z,T). Through three distinct points $P_1,P_2,P_3\in\mathscr{P}$, we can find a line (if it exists) or a plane by solving for the null space of

$$U=\begin{bmatrix}x_1 & y_1 & z_1\\ x_2 & y_2 & z_2\\ x_3 & y_3 & z_3\end{bmatrix},\qquad V=\begin{bmatrix}X_1 & Y_1 & Z_1 & T_1\\ X_2 & Y_2 & Z_2 & T_2\\ X_3 & Y_3 & Z_3 & T_3\end{bmatrix},$$

respectively. A simple observation shows that a single matrix suffices to find either a line or a plane through P_1,P_2,P_3.

Lemma 2. *A line through P_1, P_2, P_3 can be found in the null space of $V^t U$. If the null space is empty, a plane through P_1, P_2, P_3 can be found in the null space of $U^t V$.*

Definition 1. The code $C(\mathscr{P}) \in \mathbf{F}^n$ is the set of solutions $c = (c_P)$ to the system of linear equations

$$\sum_{P\in\mathscr{P}} x_P X_P c_P = \sum_{P\in\mathscr{P}} x_P Y_P c_P = \cdots = \sum_{P\in\mathscr{P}} z_P T_P c_P = 0.$$

For a codeword $c \in C(\mathscr{P})$, up to three errors can be located.

Theorem 5. *For $c \in C(\mathscr{P})$ and for a vector e with zero coordinates except for coordinates e_1, e_2, e_3 at positions P_1, P_2, P_3, let $r = c + e$. The matrix $U^t \operatorname{diag}(e_1, e_2, e_3) V$ has the same null spaces as the matrix $U^t V$. Its entries are given by*

$$\sum_{P\in\mathscr{P}} x_P X_P r_P, \quad \sum_{P\in\mathscr{P}} x_P Y_P r_P, \quad \ldots, \quad \sum_{P\in\mathscr{P}} z_P T_P r_P.$$

In particular, given r, we can determine either a line or a plane through P_1, P_2, P_3.

Proof. The matrix $U^t \operatorname{diag}(e_1, e_2, e_3) V$ has entries

$$\sum_{i=1}^{3} x_i X_i e_i, \quad \sum_{i=1}^{3} x_i Y_i e_i, \quad \ldots, \quad \sum_{i=1}^{3} z_i T_i e_i.$$

Since e_P is zero outside $P = P_1, P_2, P_3$, we may extend the summation from $i = 1, 2, 3$ to $P \in \mathscr{P}$. And by definition of $C(\mathscr{P})$, we may then replace e_p with r_p. □

The fact that three errors can be located yields the following restrictions on words in $C(\mathscr{P})$ with at most six nonzero coordinates.

Corollary 1. *A word $c \in C(\mathscr{P})$ with six nonzero coordinates has support on a line or in a plane. A word with five nonzero coordinates has support on a line. No nontrivial codeword exists with support of size less than five.*

Proof. We can write $c = e - e'$ with both e and e' supported in at most three points. Applying the theorem with $r = 0 + e = (e - e') + e'$ yields that the lines and planes through the support of e coincide with those through the support of e'. The claims easily follow. □

A partial converse is given by the following result.

Lemma 3. *Let the code $C(\mathscr{P})$ have codimension r in $\mathbf{F}^n$.*

(i) *If $r - 3$ points of $\mathscr{P}$ are collinear in $\mathbf{P}^2$ then a codeword exists in $C(\mathscr{P})$ with support in the $r - 3$ points.*
(ii) *If $r - 2$ points of $\mathscr{P}$ are coplanar in $\mathbf{P}^3$ then a codeword exists in $C(\mathscr{P})$ with support in the $r - 2$ points.*

Proof. For each set of r points that contains the $r-3$ points of the line, we can find a nontrivial function in the span $xX,\ldots,zT$ that vanishes at the r points. By duality, each $n-r$ columns of the generator matrix of $C(\mathscr{P})$ outside the $r-3$ points are dependent. But then the $n-r+3$ columns outside the $r-3$ points have rank at most $n-r-1$ and a nonzero word exists in $C(\mathscr{P})$ that cancels at the $n-r+3$ points. Part (ii) follows similarly. □

We return to the two special cases.

Lemma 4. *For both the Klein curve* (*with* $n=24$) *and the elliptic quadric* (*with* $n=64$), *the code* $C(\mathscr{P})\in\mathbf{F}^n$ *is of codimension* $r=8$.

Proof. Consider the 12 functions $xX,xY,\ldots,zT$. For the Klein curve, there are four obvious relations. For the elliptic quadric, all functions are of degree three in x,y,z and pass through the intersection of $x+y+z=0$ and $xy+yz+zx=0$. □

From Corollary 1 and Lemma 3 we see that a code of redundancy eight is three-error-correcting if and only if no line in $\mathbf{P}^2$ contains five points and no plane in $\mathbf{P}^3$ contains six points. The bounds are met sharply by the embeddings of the Klein curve.

Theorem 6. *For the Klein curve, the code* $C(\mathscr{P})$ *is of type* $[24,16,7]$. *For the elliptic quadric, the code* $C(\mathscr{P})$ *is of type* $[64,56,5]$.

4. Monomial embeddings

So far we have dealt with the embeddings $(x:y:z)$ and $(x^2y:y^2z:z^2x:xyz)$ of the Klein curve. We show that they are the building blocks for invariant embeddings. Every embedding with a linear action of the automorphism group is obtained from these two by suitable Segre embeddings. More generally, we consider monomial embeddings of arbitrary degree and we explicitly give the codewords of the previously defined code $C(\mathscr{P})$.

Definition 2. The monomial embedding of degree d of the Klein curve is defined, up to a projective transformation, by the complete linear series of the divisor $d(L-O_0-O_1-O_2)$.

The monomial embeddings are a refinement of the embeddings that are defined with divisors $eL\sim 4e(L-O_0-O_1-O_2)$ of degree a multiple of four. A monomial $X^aY^bZ^c$ of degree d intersects the Klein curve at the vertices O_0,O_1,O_2) of the triangle $XYZ=0$ with multiplicities $(3a+b,\ 3b+c,\ 3c+a)$. The condition that the monomial intersects each of the vertices at least d times means

$$2a\geqslant c,\quad 2b\geqslant a,\quad 2c\geqslant b. \tag{1}$$

Different monomials may be linearly dependent in $k[X,Y,Z]/(X^3Y+Y^3Z+Z^3X)$. For $d=4e$, a basis of the linear series can be chosen among the monomials with

$$2e \geqslant a,b,c \geqslant e. \tag{2}$$

After dividing out $(XYZ)^e$, the monomials span the linear series of the divisor eL. We show that the embeddings of the Klein curve with a linear action of the automorphism group are precisely the monomial embeddings of even degree.

Lemma 5. *Each automorphism of order seven fixes a unique triple of flexpoints. Conversely, the flexpoints in a given triple have a common stabilizer of order seven. Let the real flexpoints O_0,O_1,O_2 and O_0',O_1',O_2', be the fixed oints of the automorphisms τ and τ', respectively.*

Theorem 7. *The only invariant divisor classes of the Klein curve are those containing an even multiple of $L-O_0-O_1-O_2$.*

Proof. The proof of Theorem 3 shows that the given classes are invariant. We show that invariant classes of odd degree do not exist and that invariant classes of given even degree are unique. It sufficies to prove the former for degree three and the latter for degree six. A divisor class of degree three either is of the form $L-P$, for a point P, or it contains a single effective divisor. Both situations contradict that the automorphisms τ,τ' of order seven have no common fixed point. Let D be an invariant class of degree six. The class $D-O_0-O_1-O_2$ is of degree three and is invariant under ρ,τ. It cannot be of the form $L-P$, for the point P would be invariant under ρ,τ. Thus, the class contains a unique effective divisor, which is invariant under ρ,τ. The only fixed points of τ are O_0,O_1,O_2, and the action of ρ is transitive on O_0,O_1,O_2. Hence $D\sim 2(O_0+O_1+O_2)$, or $D\sim 6(L-O_0-O_1-O_2)$. □

The invariant class $2(L-O_0-O_1-O_2)$ is a theta characteristic. Except for even characteristic, the action of the automorphism group on the theta characteristics has orbits of size $1,7,7,21,28$. For even characteristic, the sizes are $1,7$.

The theorem gives the case $p=7$ of a more general result: The group of $\mathrm{PSL}(2,p)$-invariant line bundles on $X(p)$ is an infinite cyclic group generated by a line bundle of degree $(p^2-1)/24$ [1, Theorem 24.1].

Definition 3. Let $\mathscr{P}=\{P_1,P_2,\ldots,P_{24}\}$ be the set of flexpoints of the Klein curve. The code $C(d)$, for $d=0,1,\ldots,28$, is defined as the subspace of $\mathbf{F}_8^{24}$ generated by the vectors

$$(f(P_1),\ldots,f(P_{24})), \quad f=x^ay^bz^c$$

for $a+b+c=d$ such that (1) holds.

At the vertices O_0,O_1,O_2 of $xyz=0$, a monomial takes the value 1 in case of equality ($2a=c$, $2b=a$, or $2c=b$, respectively) and 0 otherwise. The codes are

geometric Goppa codes and general results for such codes apply. Code constructions with the Klein curve appear in [3,4,13,18,20]. The 24 flexpoints lie in the intersection of the Klein curve and its Hessian. And the codes can be studied in the context of zero-dimensional complete intersections [9,22].

Theorem 8. *For $d = 0, 1, \ldots, 28$, the code $C(d)$ has dual code $C(28-d)$. For $a+b+c = 28$ such that (1) holds,*

$$\sum_{i=1}^{24} (x_i)^a (y_i)^b (z_i)^c = 0.$$

Proof. The dimensions of $C(d)$ and $C(28-d)$ add up to 24. We prove that the two codes are orthogonal. The summation is well-defined and does not depend on the affine representation (x_i, y_i, z_i) of P_i. We may assume as in (2) that $a, b, c \geqslant 7$. The only contribution from O_0, O_1, O_2 occurs when (a, b, c) equals $(14, 7, 7)$ up to a permutation. In that case the contribution is one. The 21 remaining points divide over three orbits under τ. Therefore, their contribution is nonzero only if $a + 4b + 2c \equiv 0 \pmod 7$. Or, since also $a + b + c \equiv 0 \pmod 7$, only if (a, b, c) equals $(14, 7, 7)$ or $(8, 11, 9)$ up to a cyclic permutation. In the first case the contribution is one and compensates the contribution by O_0, O_1, O_2. In the second case, the contribution by each of the seven orbits under ρ is zero since $x^8 y^{11} z^9 + x^9 y^8 z^{11} + x^{11} y^9 z^8 = 0$. □

Lemma 6. *The monomial embedding of degree d has a hyperplane passing through d flexpoints if and only if the monomial embedding of degree $d' = 24 - d$ has a hyperplane passing through the remaining d' points.*

Proof. The 24 flexpoints $P_1, P_2, \ldots, P_{24}$ are in the intersection with the Hessian and $P_1 + P_2 + \cdots + P_{24} \sim 6L \sim (d + d')(L - O_0 - O_1 - O_2)$. □

The result can be obtained in a different manner, in terms of linear algebra, by using the arguments that are used in Lemma 3. The embedding of degree five is given by

$$K \overset{(xy:yz:zx)}{\to} S_5 : \; X^3Z^2 + Y^3X^2 + Z^3Y^2 = 0.$$

Theorem 9. *For $d = 5, 6, 18, 19$, the monomial embedding of degree d has fewer than d flexpoints in each hyperplane.*

Proof. By Lemma 6, we only need to consider $d = 5, 6$. For even characteristic, the case $d = 6$ is given by Theorem 4 and Table 1. It follows that also in characteristic zero no hyperplane contains six flexpoints. We give a direct proof for arbitrary characteristic. The lines joining O_0, O_2, O_1 are tangents. More generally, each flexpoint is a member of a unique triple in which points are joined by tangents. Through two distinct triples a unique conic passes, whose other two points of intersection are the points of a bitangent.

It follows that a divisor class of degree six containing the sum of two distinct triples is not invariant.

Let the sum $P_1 + P_2 + \cdots + P_6$ of six distinct flexpoints be in an invariant divisor class. Assume that with O_0 also O_2, the other point on its tangent, is among them. Then $P_1+P_2+P_3+P_4 \sim O_0+2O_1+O_2 \sim L+O_2-O_1$. The latter divisor has basepoint O_2 which contradicts that $P_1, P_2, P_3, P_4 \neq O_2$. Hence, no two of the six flexpoints lie on a tangent. If the sum of the six points is in an invariant class, then so is the sum of the six distinct triples that contain them. This contradicts that the sum of the two excluded triples is not in an invariant class.

Let the sum of five distinct flexpoints be in the class $2L - O_0 - O_1 - O_2$, i.e. let five distinct flexpoints be on a conic through O_0, O_1, O_2. If say O_0 is among them, then $P_1 + P_2 + P_3 + P_4 \sim 2L - 2O_0 - O_1 - O_2 \sim L + O_0 - O_1$. As before, this contradicts that $P_1, P_2, P_3, P_4 \neq O_0$. If among the five points two are on a tangent, then the conic passes through two distinct triples and two points of a bitangent. If the points are different from O_0, O_1, O_2 and no two points are on a tangent, then addition of relations gives a sum of six distinct triples in an invariant divisor class. And we have a contradiction. □

Corollary 2. *For* $d = 4, 5, 6, 18, 19$, *the code* $C(d)$ *is of type* $[24, 3, 20]$, $[24, 3, 20]$, $[24, 4, 19]$, $[24, 16, 7]$, $[24, 17, 6]$, *respectively, over the field of eight elements.*

Over the cyclotomic field $Q(\zeta_7)$, the torsion of the divisor class group of the Klein curve is generated by the flexpoints and is of type $(Z/7Z)^3 \times (Z/2Z)^6$ [20], [8]. In even characteristic, the flexpoints generate a group $(Z/7Z)^3 \times (Z/2Z)^3$.

Corollary 3. *The* 24 *flexpoints plus the zero element define a subset of* 25 *elements in the group* $(Z/7Z)^3 \times (Z/2Z)^3$ *such that no six distinct elements in the subset have zero sum.*

An explicit description of the subset is given in [8]. The elements of $(Z/7Z)^3$ can be identified with the quadratic forms $aX^2 + bXY + cY^2$ over $Z/7Z$. The group $(Z/2Z)^3$ can be identified with the field $\mathbf{F}_8$. Let $\mathbf{F}_8^* = \langle \zeta \rangle$. The 24 flexpoints can be represented by $(Y^2, 0), (2Y^2, 0), (4Y^2, 0)$ and

$$((bX - aY)^2, \zeta^{(a/b)}) \quad \text{for } a \in Z/7Z,\ b \in (Z/7Z)^*.$$

We have presented several properties of the monomial embedding of degree six in even characteristic. It yields an interesting configuration in $\mathrm{PG}(3, 8)$ and a best possible three-error-correcting code of type $[24, 16, 7]$ over $\mathbf{F}_8$. It has an interpretation as the desingularization of the dual curve and it is the unique embedding of degree six with a linear action of the automorphism group. The corollary expresses a curious property of the embedding.

5. For further reading

The following references are also of interest to the reader [15] and [21].

References

[1] A. Adler, S. Ramanan, Moduli of abelian varieties, Lecture Notes in Mathematics, vol. 1644, Springer, New York, 1997.
[2] J.J. van Beelen, Models and modularity questions concerning Fermat and Klein curves, Ph.D. Thesis, University of Leiden, 1994.
[3] R.E. Blahut, Algebraic geometry codes without algebraic geometry, IEEE Information Theory Workshop, Salvator, Bahia, Brazil, June, 21–26, 1992.
[4] R.E. Blahut, Lectures in algebraic coding theory, Manuscript, 1996.
[5] A.E. Brouwer, Unpublished, 1980.
[6] E. Ciani, I. varii tipi possibili di quartiche piane più volte omologico-armoniche, Rend. Circ. Mat. Palermo 13 (1899) 347–373.
[7] M.J. de Resmini, On quartics in a plane over a field of characteristic 2, Atti del convegno di geometria combinatoria e sue applicazioni, Perugia, 1971.
[8] I.M. Duursma, The geometry of the flexpoints of the Klein curve, Preprint, 1993.
[9] I.M. Duursma, Reed–Muller codes on complete intersections, Preprint, 1995.
[10] I.M. Duursma, Twisted Klein curves in even characteristic, Preprint, 1996.
[11] O. Ferri, Caps with two characters with respect to the planes in a Galois space $S_{3,q}$, Riv. Mat. Univ. Parma 6 (1980) 55–63.
[12] J.-M. Goethals, J.J. Seidel, Strongly regular graphs derived from combinatorial designs, Canad. J. Math. 22 (1970) 597–614.
[13] J.P. Hansen, Codes from the Klein quartic, ideals and decoding, IEEE Trans. Inform. Theory 33 (1987) 923–925.
[14] R. Hartshorne, Algebraic Geometry, Springer, Berlin, 1977.
[15] R.H. Jeurissen, C.H. van Os, J.H.M. Steenbrink, The configuration of bitangents of the Klein curve, Discrete Math. 132 (1994) 83–96.
[16] F. Klein, Über die Transformàtionen siebenter Ordnung der elliptischen Funktionen, Math. Ann. 14 (1879) 428–471 (Gesammelte mathematische Abhandlungen Teil, vol. 3, Springer, Berlin, 1923, pp. 90–136.
[17] E.S. Kramer, S.S. Magliveras, R. Mathon, The Steiner systems $S(2,4,25)$ with nontrivial automorphism group, Discrete Math. 77 (1989) 137–157.
[18] J.H. van Lint, G. van der Geer, Introduction to Coding Theory and Algebraic Geometry, Birkhäuser, Basel, 1988.
[19] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, Cambridge University Press, Cambridge, England, 1992.
[20] C.J. Moreno, Algebraic Curves over Finite Fields, Cambridge University Press, Cambridge, England, 1991.
[21] D.T. Prapavessi, On the jacobian of the Klein curve, Proc. Amer. Math. Soc. 122 (4) (1994) 971–978.
[22] C. Renteria, H. Tapia-Recillas, Reed-Muller codes: an ideal theory approach, Comm. Algebra 25 (2) (1997) 401–413.
[23] V.D. Tonchev, Unpublished, 1980.