Aequationes Mathematicae **25** (1982) 153–176
University of Waterloo

0001–9054/82/002153-24 $1.50 + 0.20/0

Variations on seven points: An introduction to the scope and methods of coding theory and finite geometries

THOMAS BETH AND DIETER JUNGNICKEL

To Professor Günter Pickert on the occasion of his 65th birthday

Abstract and Introduction. We use a simple example (the projective plane on seven points) to give an introductory survey on the problems and methods in finite geometries — an area of mathematics related to geometry, combinatorial theory, algebra, group theory and number theory as well as to applied mathematics (e.g., coding theory, information theory, statistical design of experiments, tomography, cryptography, etc.). As this list already indicates, finite geometries is — both from the point of view of pure mathematics and from that of applications related to computer science and communication engineering — one of the most interesting and active fields of mathematics. It is the aim of this paper to introduce the nonspecialist to some of these aspects.

Variation 1. Geometries

The following figure probably is the most famous one in all of finite geometries:

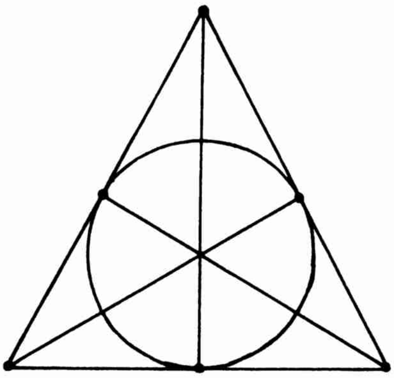


Figure 1

AMS (1980) subject classification: Primary 05B25, 20B25, 94B05. Secondary 05B10, 10L10.

Manuscript received April 7, 1982.

It graphically represents the projective plane of order 2: Dots are to be interpreted as points, and the straight lines as well as the circle are lines. Our example enjoys some remarkable features of uniformity: It has 3 points on each line, three lines through each point, two points determine a unique line and two lines intersect in a unique point. Also, there are as many points as lines. Structures enjoying such a uniform behavior are of particular interest and lead to the following definition.

DEFINITION. Let $\mathcal{P}$ be a set (of "points") and $\mathcal{B}$ a family of subsets of $\mathcal{P}$ (called "blocks"*). Then $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ is called a *t-design* with *parameters t, k, v* and λ or, more briefly, an $S_\lambda(t, k; v)$ provided that the following properties hold:

(S_1) Given any t-subset T of $\mathcal{P}$, there exist exactly λ blocks B with $T \subset B$.

(S_2) $|B| = k$ for any block B.

(S_3) $|\mathcal{P}| = v$.

In this terminology, our example is an $S_1(2,3;7)$. The reader may wonder why we did not include any assertions on the number of blocks through a point or the total number of blocks in our definition: These may be computed from the remaining parameters as we will show now.

LEMMA 1. *Let $\mathcal{S}$ be an $S_\lambda(t, k; v)$ and let s be an integer with $0 \le s \le t$. Then $\mathcal{S}$ is also an s-design with λ-value*

$$\lambda_s = \lambda \binom{v-s}{t-s} \Big/ \binom{k-s}{t-s}.$$

Proof. Let S be any s-set of points and count all pairs (X, B) where X is a $(t-s)$-set of points with $S \cap X = \varnothing$ and where B is a block with $S \cup X \subset B$ in two ways. By (S_1) we obtain $\lambda\binom{v-s}{t-s}$, as we may choose X in $\binom{v-s}{t-s}$ ways; on the other hand, any block B with $B \supset S$ contains exactly $\binom{k-s}{t-s}$ sets X with $S \cap X = \emptyset$, yielding $\lambda_s(S)\binom{k-s}{t-s}$ pairs of the desired type. This yields the desired formula and shows that $\lambda_s(S)$ is indeed independent of the choice of S. □

COROLLARY. *Let $\mathcal{S}$ be an $S_\lambda(t, k; v)$. Then any point of $\mathcal{S}$ is on precisely $r = \lambda_1$ blocks. In particular, for $t = 2$ one has*

$$r = \lambda(v-1)/(k-1)$$

and

$$b = |\mathcal{B}| = \lambda_0 = vr/k = \lambda v(v-1)/k(k-1).$$

* One generally uses the term "block" instead of "line" since one often has to consider structures where the term "line" would be awkward, e.g., the points and hyperplanes of a projective or affine space, or here the "line" formed by the circle.

Lemma 1 poses some numerical restrictions on the possible parameters for t-designs, as all the numbers λ_s have to be integers. These restrictions are usually called the "arithmetic conditions". If these conditions are fulfilled for a particular quadruple (t, k, v, λ) one may pose the following two fundamental questions:

PROBLEM 1. Does there exist any $S_\lambda(t, k; v)$?

PROBLEM 2. Is an $S_\lambda(t, k; v)$ already uniquely determined by its parameters?

Let us show that the answer to Problem 2 is "yes" in the case of an $S_1(2, 3; 7)$. Of course, by "unique" we only mean unique up to isomorphism — clearly we may rename points and blocks. To be precise we need a definition.

DEFINITION. Let $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ and $\mathcal{S}' = (\mathcal{P}', \mathcal{B}')$ be two *incidence structures* (i.e., $\mathcal{P}$ and $\mathcal{P}'$ are sets and $\mathcal{B}$ and $\mathcal{B}'$ families of subsets of $\mathcal{P}$, resp. $\mathcal{P}'$). Then any bijection $\alpha : \mathcal{P} \to \mathcal{P}'$ which induces a bijection $\mathcal{B} \to \mathcal{B}'$ is called an *isomorphism* and $\mathcal{S}$ and $\mathcal{S}'$ are called *isomorphic*. In the case $\mathcal{S} = \mathcal{S}'$, α is called an *automorphism*.

PROPOSITION 1. *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ be any $S_1(2, 3; 7)$. Then $\mathcal{S}$ is isomorphic to the example given above.*

Proof. Choose any ordered quadrangle in $\mathcal{S}$ (i.e., a set of 4 points no 3 of which are on a common block), say (a, b, c, d). Similarly, let (a', b', c', d') be any ordered quadrangle in our example and put* $a^\alpha = a'$, $b^\alpha = b'$, $c^\alpha = c'$, $d^\alpha = d'$. Then there is a unique way of extending α to an isomorphism: If e is the third point on the block of $\mathcal{S}$ containing $\{a, b\}$ and if e' is the third point on the block through a' and b', we have to put $e^\alpha = e'$ if α is to be an isomorphism. Similarly, $\{a, c\}$ and $\{a, d\}$ define two further points f and g which have to be mapped onto the corresponding points f' and g'. It is now possible to write down the list of blocks for both $\mathcal{S}$ as well as for our former example and to check that α is indeed an isomorphism. □

We will henceforth denote the unique $S_1(2, 3; 7)$ by $\mathcal{D}$.

Variation 2. Groups

Uniqueness assertions like that of Proposition 1 also give a lot of information on the automorphisms of the structure considered. Our proof of Proposition 1 in fact shows much more than originally claimed:

* a^α denotes the image of a under α.

PROPOSITION 2. *The full automorphism group* Aut $\mathscr{D}$ *of* $\mathscr{D}$ *(i.e., the group of all automorphisms of* $\mathscr{D}$*) acts regularly* on the set of ordered quadrangles of* $\mathscr{D}$*. Hence* Aut $\mathscr{D}$ *has order 168.*

Proof. The first assertion has already been proved. Counting ordered quadrangles, one obtains $168 = 7 \cdot 6 \cdot 4 \cdot 1$: The first point a may be chosen in 7 ways, the second one b in 6 ways, then the third one c in 4 ways (a, b, and the third point on the block through a and b are forbidden!); then the last point d is uniquely determined. □

As an example, let us label the seven points of $\mathscr{D}$ by the integers $0, \ldots, 6$,

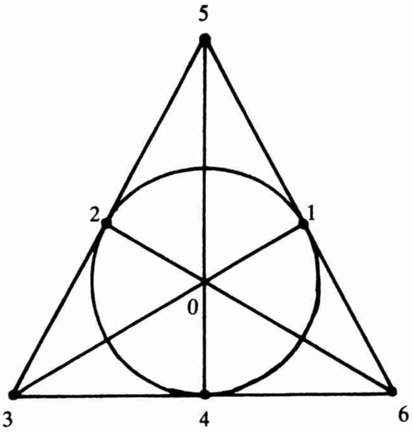


Figure 2

and then determine the isomorphism mapping the quadrangle $(0, 1, 2, 5)$ onto $(4, 2, 0, 3)$. This implies $3 \to 1$, $6 \to 5$ and $4 \to 6$.

In general one is interested in the following problem.

PROBLEM 3. Given an $S_\lambda(t, k; v)$, determine its full automorphism group.

Of course, we have not yet really determined Aut $\mathscr{D}$ up to now; we only know its order. To obtain further information, we need two basic results on permutation groups:

* Let G be a permutation group on a set X. Then G is said to act *regularly* on X provided that the following condition holds: Given any two elements x and x' of X, there is a unique $\gamma \in G$ with $x^\gamma = x'$.

LEMMA 2. *Let N be a normal subgroup of a permutation group G acting on X. If G is primitive* and $N \neq 1$, then N is transitive* on X.*

Proof. If N is not transitive, then the orbits $x^N = \{x^\nu : \nu \in N\}$ are sets of imprimitivity for G, since $(x^N)^\gamma = (x^\gamma)^N$. □

LEMMA 3. *Let N be a transitive normal subgroup of a permutation group G acting on X and let x be an element of X. Then the stabilizer $G_x = \{\gamma \in G : x^\gamma = x\}$ is isomorphic to a subgroup of* $\operatorname{Aut} N$.

Proof. For $\gamma \in G_x$, define $i(\gamma)$: $N \to N$ by $\nu^{i(\gamma)} = \gamma^{-1}\nu\gamma$; then $i(\gamma)$ is in $\operatorname{Aut} N$, as N is normal in G. Clearly i: $G \to \operatorname{Aut} N$ is a homomorphism. Furthermore, the kernel of i is trivial: If $\gamma \in \operatorname{Ker} i$, then $\gamma\nu = \nu\gamma$ for all $\nu \in N$. As N is transitive, any $y \in X$ may be written as $y = x^\nu$ for some $\nu \in N$, hence $y^\gamma = x^{\nu\gamma} = x^{\gamma\nu} = x^\nu = y$ and $\gamma = \mathrm{id}_X$. □

Quite generally, the theory of permutation groups is a very valuable tool in dealing with automorphism groups of t-designs. Excellent references for permutation groups are the books of Wielandt [51] and Huppert [22]. Using Lemmas 2 and 3, we may now prove:

PROPOSITION 3. $\operatorname{Aut} \mathcal{D}$ *is simple.*

Proof. We consider $G = \operatorname{Aut} \mathcal{D}$ in its action on $\mathcal{B}$ (the set of blocks of $\mathcal{D}$). As G is transitive on ordered quadrangles of $\mathcal{D}$, G is easily seen to be 2-transitive** on $\mathcal{B}$, hence primitive on $\mathcal{B}$. Thus any normal subgroup N of G acts transitively on $\mathcal{B}$. Choose a block B and consider its stabilizer G_B. As G is regular on ordered quadrangles one sees that G_B is isomorphic to S_4 (the symmetric group on 4 elements). Thus $M = G_B \cap N$ is a normal subgroup of S_4; hence M is one of 1, V_4 or A_4 (provided $N \neq G$). In case $M = 1$, N acts regularly on $\mathcal{B}$, i.e., $|N| = 7$ and therefore $N \cong \mathbb{Z}_7$. Thus $S_4 \cong G_B$ would be a subgroup of $\operatorname{Aut} \mathbb{Z}_7 \cong \mathbb{Z}_6$ by Lemma 3, a contradiction. In case $M \cong V_4$ or A_4, N has order $7 \cdot 4 = 28$, respectively, $7 \cdot 12 = 84$. We then consider a Sylow 7-subgroup S of N: As the number of such subgroups is $\equiv 1 \bmod 7$ and also divides 28, resp. 84, it is easily seen to be 1. Hence S is a

* Let G be a permutation group on a set X. Then G is said to act *transitively* on X provided that any $x \in X$ may be mapped onto any other element x' of X by some element of G. Now assume G to be transitive; then a subset K of X is called a *set of imprimitivity* iff $1 < |K| < |X|$ and if $K^\gamma = K$ or $K^\gamma \cap K = \emptyset$ for each $\gamma \in G$. G is called *primitive* provided it is transitive and does not admit any set of imprimitivity.

** G is called 2-*transitive* on B if it is transitive on the set of ordered 2-subsets of B.

characteristic subgroup of N and (using $N \lhd G$) S is a normal subgroup of G. But then S is a regular normal subgroup of G — a case already excluded. □

COROLLARY. $\mathrm{Aut}\,\mathscr{D} \cong \mathrm{PGL}(3,2)$.

Proof. The assertion may be seen as follows. Let $F = \mathrm{GF}(q)$. Then the 1-dimensional subspaces of F^3 (as points) and the 2-dimensional subspaces of F^3 (as blocks) form an $S_1(2, q+1; q^2+q+1)$ as the reader may prove as an exercise.* For $q = 2$, we obtain an $S_1(2,3;7)$ which is isomorphic to $\mathscr{D}$ by Proposition 1. Clearly each bijective linear mapping of F^3 induces an automorphism of $\mathscr{D}$ and in the case $q = 2$ only the identity on F^3 induces the identity of $\mathscr{D}$. Hence $\mathrm{Aut}\,\mathscr{D} \cong \mathrm{PGL}(3,2) = \mathrm{GL}(3,2) = \mathrm{SL}(3,2)$ in this case as both $\mathrm{Aut}\,\mathscr{D}$ and $\mathrm{PGL}(3,2)$ have order 168. □

To obtain even more information on the structure of $\mathrm{Aut}\,\mathscr{D}$, let us find its Sylow subgroups. The representation of $\mathscr{D}$ on $\{0,\dots,6\}$ given above shows that $\mathrm{Aut}\,\mathscr{D}$ contains $\mathbf{Z}_7$: Here $x \in \mathbf{Z}_7$ maps a point $p \in \{0,\dots,6\}$ onto $p+x$, and a block $\{b, b+1, b+3\}$ onto $\{b+x, b+x+1, b+x+3\}$ (mod 7). A Sylow 3-subgroup may be obtained from the graphical representation of $\mathscr{D}$ in Figure 2: the three rotations with 0 as fixed point with 0°, 120° and 240° yield automorphisms of $\mathscr{D}$. The Sylow 7- resp. Sylow 3-subgroup generates the semidirect product

$$\mathrm{ASL}(1,7) = \{x \to a^2x + b \mid a \in \mathrm{GF}(7)^*, b \in \mathrm{GF}(7)\}$$

which acts in its natural representation on 7 points. Finally, the Sylow 2-subgroups are dihedral groups of order 8. Choosing any block B (e.g., $\{3,4,6\}$) and any point p on B (e.g., 3) one obtains an automorphism of order 3 fixing all points of B and all lines through p (e.g., $0 \leftrightarrow 1$, $2 \leftrightarrow 5$). Now fixing a point p on B (say 4) and interchanging the remaining two points of B (in our example we may, e.g., reflect the triangle of Figure 1 at the line $\{0,4,5\}$) together with the elementary abelian group already obtained (which, by the way, acts in its natural representation on the quadrangle $\mathscr{P} \setminus B$) yields the desired dihedral group.

It is also easy to find the number of Sylow subgroups. For $p = 3$, each such group fixes a point and a block not containing this point; hence there are $7 \cdot 4 = 28$ Sylow 3-subgroups. Similarly, for $p = 2$, such a group fixes a point and a block through this point yielding $7 \cdot 3 = 21$ Sylow 2-subgroups. Finally, the number of Sylow 7-subgroups is $\neq 1$ ($\mathrm{Aut}\,\mathscr{D}$ is simple!), but $\equiv 1 \bmod 7$ and divides 168. Thus it is necessarily 8.

* I.e., a projective plane of order q. In general (where F may be infinite) one still obtains a projective plane; cf. Hughes and Piper [21] for projective planes.

Let us return to the representation of $\mathscr{D}$ on $\{0, \ldots, 6\} = \mathbf{Z}_7$. One sees that the "start block" $\{0, 1, 3\}$ yields each non-zero element of $\mathbf{Z}_7$ exactly once as a difference: $\pm 1 = \pm(1-0)$, $\pm 2 = \pm(3-1)$, $\pm 3 = \pm(3-0)$. This motivates the definition of a (v, k, λ)-*difference set* in a group G of order v: This is a k-subset whose set of differences contains each nonzero element of G exactly λ times; clearly this implies $\lambda(v-1) = k(k-1)$. Given such a difference set D, one obtains an $S_\lambda(2, k; v)$ with $b = v$ and G as regular (both on points and blocks) automorphism group by choosing G as point set and the sets $D + g$ $(g \in G)$ as blocks. The classical examples of difference sets are due to Singer [46]: The 2-design of points and hyperplanes of a finite projective space may be represented by a difference set in a cyclic group. This explains why an automorphism group of a 2-design with $b = v$ acting regularly on the points (and then by a result known as the "orbit theorem" also on blocks) is called a *Singer group*. Difference sets are the subject of a beautiful theory within finite geometries of which we would like to mention one further result. Given a projective plane admitting two distinct cyclic Singer groups, the plane is necessarily desarguesian (i.e., constructed from a field GF(q) as in the proof of the Corollary to Proposition 3). This result is due to Ott [38] and gives a partial converse to Singer's Theorem; a long standing conjecture says that the existence of just one Singer group (not even necessarily cyclic) would already imply the plane to be desarguesian. There is an extensive literature on difference sets; we mention the books of Baumert [2] and Hall [17].

Difference sets generalize naturally to *difference families*. Here one considers a family of k-subsets of a group G (of order v) whose differences altogether contain each nonzero element of G exactly λ times. Such a (v, k, λ)-difference family then yields an $S_\lambda(2, k; v)$ with $b > v$ (if the family contains more than one k-set). Although the theory of difference families is much weaker than that of difference sets, we mention one result due to Wilson [52]. If v is a prime power satisfying $\lambda(v-1) \equiv 1 \bmod k(k-1)$ (an obviously necessary condition for the existence of a $(v, k; \lambda)$-difference family) and if v is sufficiently large (e.g., $> \binom{k}{2}^{k(k-1)}$), then there exists a $(v, k; \lambda)$-difference family in the elementary abelian group of order v. This result and numerous direct constructions (introduced by Bose [8]) form the basis for the recursive existence theory of 2-designs. We mention two results: (i) the necessary existence conditions of the Corollary to Lemma 1 are sufficient for $t = 2$, $k = 3$, 4, 5 and arbitrary λ (with one exception), see Hanani [18]; (ii) they are always sufficient provided v is large enough (given k and λ), see Wilson [53].

Variation 3. Extensions

Next, we consider another combinatorial problem. Let $\mathscr{S}$ be any $S_\lambda(t, k; v)$ and choose a point p of $\mathscr{S}$. Then the set of points $\neq p$ together with all blocks containing p form an $S_\lambda(t-1, k-1; v-1)$; this design $\mathcal{S}_p$ is called the *derived design* of $\mathcal{S}$ at p. Conversely, $\mathcal{S}$ is called an *extension* of $\mathcal{S}_p$. This leads to another important question:

PROBLEM 4. Given an $S_\lambda(t, k; v)$, is it extendable to an $S_\lambda(t+1,\ k+1; v+1)$? And is the extension unique?

Lemma 1 shows that $b(v+1) \equiv 0 \bmod k+1$ if an $S_\lambda(t, k; v)$ is extendable. This simple remark, e.g., suffices to show that no projective plane of order n (i.e., no $S_1(2, n+1; n^2+n+1)$) is extendable unless possibly $n = 2$, 4, or 10. We leave the proof of this assertion (due to Hughes [20]) to the reader and mention that Cameron [10] has studied the more general problem of extending symmetric designs, cf., Variation 4. Regarding $\mathcal{D}$, we now prove the following proposition.

PROPOSITION 4. *$\mathcal{D}$ admits a unique extension to an $S_1(3, 4; 8)$.*

Proof. Let $\mathcal{S}$ be any $S_1(3, 4; 8)$. We claim that any two blocks of $\mathcal{S}$ which have nonempty intersection in fact have precisely 2 points in common. Thus let p be a point in $B \cap B'$; then $\mathcal{S}_p$ is an $S_1(2, 3; 7)$ and thus $B \setminus \{p\}$ and $B' \setminus \{p\}$ intersect in a unique point. Using this and the fact that any two points of $\mathcal{S}$ are on exactly 3 common blocks (this follows from Lemma 1) we see that exactly $12 = 2 \cdot \binom{4}{2}$ blocks intersect a given block B. But $\mathcal{S}$ has 14 blocks altogether, and so there is a unique block $\bar{B}$ not intersecting B; as both B and $\bar{B}$ have 4 points, this block $\bar{B}$ is necessarily the complement of B. Thus the only possibility of extending $\mathcal{D}$ to an $S_1(3, 4; 8)$ $\bar{\mathcal{D}}$ is to proceed as follows: one adds a new point ∞ and takes as blocks all sets $B \cup \{\infty\}$ and all sets $\bar{B} = \mathcal{P} \setminus B$ (where B is any block of $\mathcal{D}$). This already yields all blocks of $\bar{\mathcal{D}}$. We leave it to the reader to check that $\bar{\mathcal{D}}$ is indeed an $S_1(3, 4; 8)$. □

COROLLARY 1. *There is a unique $S_1(3, 4; 8)$ $\bar{\mathcal{D}}$ and its full automorphism group is isomorphic to* AGL(3, 2).

Proof. The first part of the assertion has already been shown. Now it is easily seen that points and planes of the affine space of dimension 3 over GF(2) (i.e., the vectors and the cosets of 2-dimensional subspaces of the vector space of dimension 3 over GF(2)) form an $S_1(3, 4; 8)$; the automorphism group of this design clearly contains AGL(3, 2). But $|\mathrm{AGL}(3, 2)| = 8|\mathrm{Aut}\,\mathcal{D}|$ and $\mathrm{Aut}\,\bar{\mathcal{D}}$ clearly has order $8|\mathrm{Aut}\,\mathcal{D}|$ (the stabilizer of ∞ has order 168 and the uniqueness of $S_1(3, 4; 8)$ implies that $\mathrm{Aut}\,\bar{\mathcal{D}}$ is transitive on points) proving the assertion. □

$\bar{\mathcal{D}}$ has no further extension, as $k+1 = 5$ does not divide $b(v+1) = 14 \cdot 9$. We remark that Proposition 4 is just the special case $\lambda = 1$ of a much more general result: Any $S_\lambda(2, 2\lambda + 1; 4\lambda + 3)$ has a unique extension (by complementation — as explained above) to an $S_\lambda(3, 2\lambda + 2; 4\lambda + 4)$ and any $S_\lambda(3, 2\lambda + 2; 4\lambda + 4)$ is obtained in this way (Norman [37]). Such designs are called Hadamard 2-, resp., Hadamard 3-designs; their existence is conjectured for every value of λ and is a famous open problem. As an exercise the reader may show that the set of nonzero squares in GF(q) (with $q \equiv 3 \bmod 4$) is a difference set for an Hadamard 2-design with $\lambda = (q-3)/4$. There is an extensive literature on Hadamard designs; we mention the surveys by Wallis, Street and Wallis [50] and Hedayat and Wallis [19].

Proposition and Corollary 1 yield another remarkable result:

COROLLARY 2. Aut $\bar{\mathscr{D}}$ *contains* PSL(2, 7) *in its natural representation on* 8 *points.*

Proof. From the previous section we recall that ASL(1, 7) acts on $\mathscr{D}$ in its standard representation

$$\left\{\begin{matrix} \mathrm{GF}(7) \to \mathrm{GF}(7) \\ x \mapsto a^2x + b \end{matrix}\right\},$$

hence also on GF(7) ∪ {∞} by fixing the new point ∞. As PSL(2, 7) in its action on GF(7) ∪ {∞} is generated by ASL(1, 7) and the involution $i : x \mapsto -1/x$ we just have to show that $i \in \operatorname{Aut} \bar{\mathscr{D}}$. Take any block $B = \{\infty, 0 + b, 1 + b, 3 + b\}$ and verify that its image B^i is again a block of $\bar{\mathscr{D}}$. □

As an example take $B_1 = \{\infty, 0, 1, 3\}$ and compute

$$B_1^i = \{0, \infty, 6, 2\} = B_1 + 6,$$

or $B_2 = B_1 + 1 = \{\infty, 1, 2, 4\}$, and compute $B_2^i = \{0, 6, 3, 5\} = \bar{B}_2$.

This property generally is not true for all Hadamard designs generated in this manner, i.e., by quadratic residues. While ASL(1, q) always is a group of automorphisms of these designs, PSL(2, q) in its canonical representation is *not* (cf. Beth [3]) *but* PSL(2, q) acts on the so-called Quadratic Residue Code generated by this design, cf. Variation 6.

It is well-known that there exists — up to isomorphism — exactly one simple group of order 168, see, e.g., Huppert [22]. In particular, this implies PGL(3, 2) ≅ PSL(2, 7); we will now use Corollary 2 and the proof of Corollary 1 to give a purely geometric proof of this last assertion:

COROLLARY 3. PSL(2, 7) ≅ PGL(3, 2).

Proof. Consider the unique $S_1(3,4;8)$ $\bar{\mathscr{D}}$ which is isomorphic to AG(3,2) with planes as blocks, and identify the points of $GF(2)^3$ with the points $\{0,\ldots,7,\infty\}$ by observing that the Singer cycle of length 7 may be considered as the cyclic group of nonzero elements of $GF(2^3)$ generated by the primitive polynomial x^3+x+1 over GF(2) (cf. Variation 7). Thus let ω be a root of this polynomial; then

$$\begin{aligned}
(0\ 0\ 0) &\triangleq \infty\\
\omega^0 = (1\ 0\ 0) &\triangleq 0\\
\omega^1 = (0\ 1\ 0) &\triangleq 1\\
\omega^2 = (0\ 0\ 1) &\triangleq 2\\
\omega^3 = (1\ 1\ 0) &\triangleq 3\\
\omega^4 = (0\ 1\ 1) &\triangleq 4\\
\omega^5 = (1\ 1\ 1) &\triangleq 5\\
\omega^6 = (1\ 0\ 1) &\triangleq 6.
\end{aligned}$$

Thus the blocks of $\bar{\mathscr{D}}$ passing through ∞ (e.g., $\{\infty,0,1,3\}$) are the 2-dimensional subspaces of AG(3,2) and hence the derived $S_1(2,3;7)$ $\bar{\mathscr{D}}_\infty$ is $\mathscr{D}$ with the Singer group $G=\langle x\to x+1 \bmod 7\rangle$. But as $\operatorname{Aut}\bar{\mathscr{D}}\cong AGL(3,2)$, $\operatorname{Aut}\bar{\mathscr{D}}$ also contains the (elementary abelian) translation group of order 8. Denote by $\boldsymbol{a}$ the unique vector in $GF(2^3)$ corresponding to a $(\in\{0,\ldots,7\}\cup\{\infty\})$ and by $t(\boldsymbol{a})$ the translation of $\bar{\mathscr{D}}$ induced by $\boldsymbol{a}$. Thus $t(\boldsymbol{a})$ maps a to ∞ and therefore $\alpha t(\infty^\alpha)\in(\operatorname{Aut}\bar{\mathscr{D}})_\infty=\operatorname{Aut}\mathscr{D}$ for all $\alpha\in\operatorname{Aut}\bar{\mathscr{D}}$. But $\operatorname{Aut}\bar{\mathscr{D}}$ contains PSL(2,7) in its natural representation on $\{0,\ldots,7\}\cup\{\infty\}$; using the fact that the translation group is normal in AGL(3,2) and acts regularly on $\{0,\ldots,7\}\cup\{\infty\}$, it is now not difficult to see that $\alpha\to\alpha t(\infty^\alpha)$ is the required isomorphism of PSL(2,7) onto $\operatorname{Aut}\mathscr{D}\cong PGL(3,2)$. □

Extending designs and simultaneously "extending" their groups is sometimes a way of constructing interesting permutation groups, i.e., t-transitive groups (this means groups transitive on ordered t-subsets of a given set) for large values of t. Starting with an $S_1(2,3;9)$ (which is unique and may be obtained as the affine plane over GF(3): points are vectors and blocks are cosets of 1-dimensional subspaces of the 2-dimensional vector space over GF(3)) one obtains successively an $S_1(3,4;10)$, an $S_1(4,5;11)$ and $S_1(5,6;12)$; similarly, the (unique) projective plane of order 4 (i.e., the unique $S_1(2,5;21)$) may be extended until one reaches an $S_1(5,8;24)$. All these designs are unique and their automorphism groups are the famous sporadic simple groups due to Mathieu. The construction of these designs and their relation to the Mathieu groups have been discovered by Witt [54], [55]. A detailed treatment of the step-by-step extension sketched above, using the geometry of the underlying $S_1(2,3;9)$, resp., $S_1(2,5;21)$, is given by Lüneburg [28]. An alternative more combinatorial treatment simultaneously dealing with both classes of "Witt" designs is given by Beth and Jungnickel [4]. We remark in passing that the classification of finite simple groups implies that the only nontrivial (i.e., neither symmetric nor alternating) finite 4-transitive groups are the Mathieu groups on 11, 12, 23 and 24 elements with those on 12 and 24 elements in fact even being 5-transitive. Indeed, using the classification of simple groups, even all 2-transitive groups are known (see Cameron [11]).

Variation 4. Some linear algebra

We now introduce a representation for designs which allows the application of linear algebra to combinatorial questions on designs. If $\mathcal{S} = (\mathcal{P}, \mathcal{B})$ is any incidence structure, we may define a $0-1$-matrix indexed by points and blocks of $\mathcal{S}$ as follows: The matrix A has $a_{p,B} = 1$ iff $p \in B$ and $= 0$ otherwise. Then A is called an *incidence matrix* for $\mathcal{S}$. Of course, A depends on the ordering of points, resp., blocks one chooses. The following result is an immediate consequence of the definitions.

LEMMA 4. *Let A be an incidence matrix for an incidence structure $\mathcal{S}$. Then* $\mathcal{S}$ is an $S_\lambda(2,k;v)$ iff one has $AA^T = \lambda J + (r-\lambda)I$, where $r = \lambda(v-1)/(k-1)$ and $v = |\mathcal{S}|$.*

THEOREM 1 (Fisher's inequality). *Let $\mathcal{S}$ be an $S_\lambda(2,k;v)$ with $v > k$. Then $b \geq v$.*

Proof. Using Lemma 4, one has (where A is an incidence matrix for $\mathcal{S}$)

$$\det AA^T = \det(\lambda J + (r-\lambda)I) = (r-\lambda)^{v-1}((v-1)\lambda + r);$$

but $r > \lambda$ (otherwise we would have $k = v$) and thus $\det AA^T \neq 0$ (e.g., over the reals), hence $\operatorname{rank} A = v$ and therefore $b \geq v$. □

Theorem 1 is the starting point for a long sequence of further investigations. E.g., it may be strengthened for t-designs with $t > 2$ as follows: If $\mathcal{S}$ is an $S_\lambda(2s,k;v)$ with $v \geq k+s$, then $b \geq \binom{v}{s}$, and if $\mathcal{S}$ is an $S_\lambda(2s+1,k;v)$ with

* A^T denotes the transpose of A, J a matrix with all entries 1, and I the identity matrix.

$v \geq k+s+1$, then $b \geq 2\binom{v-1}{s}$. These results are due to Petrenyuk [42] and Ray-Chaudhuri and Wilson [44]. There are many similar inequalities for various other types of incidence structures which we shall not discuss here.

By Theorem 1 it is also interesting to study those 2-designs which satisfy Fisher's inequality with equality, i.e., $v = b$; such 2-designs are called *symmetric*. For example, the symmetric 2-designs with $\lambda = 1$ are just the projective planes, i.e., the designs $S_1(2, n+1; n^2+n+1)$. Again, the incidence matrix will yield some strong results. For this, it will be convenient to introduce a further concept: Let $\mathcal{S}$ be an incidence structure $\mathcal{S} = (\mathcal{P}, \mathcal{B})$; then the *dual* of $\mathcal{S}$ is the structure $\mathcal{S}^{\mathrm{d}}$ which has as its point set the set $\mathcal{B}$ of blocks of $\mathcal{S}$ and as its block set the set $\mathcal{P}$ of points of $\mathcal{S}$. Here a point p of $\mathcal{S}$ is — when considered as a block of $\mathcal{S}^{\mathrm{d}}$ — the set of all those blocks in $\mathcal{B}$ which contain p (in $\mathcal{S}$). If A is an incidence matrix for $\mathcal{S}$, then A^{T} is an incidence matrix for $\mathcal{S}^{\mathrm{d}}$. E.g., $\mathcal{D}^{\mathrm{d}}$ has as point set the elements $D+x$ (where $D = \{0, 1, 3\}$ and $x \in \mathbb{Z}_7$) and as block set $\mathbb{Z}_7$ (where $i \in \mathbb{Z}_7$ is considered as the set of those $D+x$ with $i \in D+x$). One now has

THEOREM 2. *Let $\mathcal{S}$ be an $S_\lambda(2, k; v)$ with $v > k$. Then the following assertions are equivalent*:

(i) *$\mathcal{S}$ is symmetric (i.e., $b = v$)*;

(ii) $r = k$;

(iii) *any two blocks of S intersect in precisely λ points*;

(iv) *$\mathcal{S}^d$ is also an $S_\lambda(2, k; v)$*;

(v) *both $\mathcal{S}$ and $\mathcal{S}^d$ are 2-designs.*

Proof. (i) and (ii) are equivalent by the Corollary to Lemma 1. Now let $r = k$ and let A be an incidence matrix for $\mathcal{S}$; then A is invertible by the proof of Theorem 1. Thus

$$A^{\mathrm{T}}A = A^{-1}AA^{\mathrm{T}}A = A^{-1}((r-\lambda)I + \lambda J)A = (r-\lambda)I + \lambda J,$$

where one uses $AJ = JA = kJ$. But this matrix equation is easily seen to imply (iii). Assuming (iii), we at once obtain (v). Assuming (v), we have (because of Theorem 1) both $b \geq v$ and $v \geq b$ (which is Fisher's inequality for $\mathcal{S}^{\mathrm{d}}$), hence (i). Finally, (iv) is equivalent to (i) and (iii) together. □

Our arguments show that the symmetric 2-designs are precisely those which admit a *normal* incidence matrix: $AA^{\mathrm{T}} = A^{\mathrm{T}}A$. In spite of the terminology generally used, such a design does not necessarily admit a *symmetric* incidence matrix; this will be the case iff $\mathcal{S}$ is *self-dual*, i.e., iff $\mathcal{S}$ is isomorphic to $\mathcal{S}^{\mathrm{d}}$. Any isomorphism of $\mathcal{S}$ onto $\mathcal{S}^{\mathrm{d}}$ is called a *correlation*. As an example, we mention:

PROPOSITION 5. *$\mathcal{D}$ is self-dual.*

Proof. We will show more generally that any symmetric design $\mathcal{S}$ with an abelian Singer group is self-dual. Thus, let D be a difference set in G (for $\mathcal{D}$, e.g., $D = \{0, 1, 3\} \subseteq \mathbb{Z}_7$); hence $\mathcal{S}$ has point set G and block set $\mathcal{B} = \{G + g : g \in G\}$. Map the point x onto the block $D - x$; this clearly defines a bijection $\zeta : \mathcal{P} \leftrightarrow \mathcal{B}$ and it will suffice to show that ζ preserves incidence in both directions. But one has $x \in D - y$ iff $x = d - y$ for some $d \in D$ iff $y = d - x$ for some $d \in D$ iff $y \in D - x$ iff $(D - y)^{\zeta} \in x^{\zeta}$. □

If a design is self-dual, then the group $\operatorname{Cor} \mathcal{S}$ generated by all automorphisms and all correlations clearly contains $\operatorname{Aut} \mathcal{S}$ as a normal subgroup of index 2; e.g., $\operatorname{Cor} \mathcal{D}$ has order $2 \cdot 168 = 336$. It may be mentioned that there are examples of projective planes which are not self-dual; see, e.g., Hughes and Piper [21].

Variation 5. Quadratic forms

Incidence matrices may also be used to exclude the existence of certain symmetric 2-designs:

THEOREM 3 (Schützenberger [45]). *Let $\mathcal{S}$ be a symmetric $S_\lambda(2, k; v)$, where $k < v$ and v is even. Then $n := k - \lambda$ is a perfect square.*

Proof. As $\mathcal{S}$ is symmetric, one has $(v-1)\lambda + r = (v-1)\lambda + k = k^2$ (by the Corollary to Lemma 1). Using the proof of Theorem 2, we thus obtain $(\det A)^2 = \det AA^T = (k-\lambda)^{v-1}k^2$. But this term is a square iff $n = k - \lambda$ is a square. □

E.g., there is no $S_2(2, 7; 22)$: Such a design would be symmetric but $5 = k - \lambda$ is not a square. Theorem 3 does not yield any information for projective planes, as $v = n^2 + n + 1$ is always odd. For odd v there is another theorem due to Bruck and Ryser [9] (for $\lambda = 1$) and to Chowla and Ryser [13] (in the general case). An elementary but lengthy proof (using a result from number theory, namely Lagrange's Four Square Theorem) is available, see, e.g., Hall [17]. We will just state the result:

THEOREM 4 (The Bruck–Ryser–Chowla Theorem). *Let $\mathcal{S}$ be an $S_\lambda(2, k; v)$ with $k > v$ where v is odd. Then the Diophantine equation*

$$x^2 = (k - \lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2$$

has a nontrivial solution (i.e., a solution in integers x, y, z not all of which are $= 0$).

This equation at once yields the following non-existence criterion: Let p be an odd prime dividing the square-free part of $n = k - \lambda$ but not dividing the square-free part λ' of λ; then $(-1)^{(v-1/2)}\lambda'$ is a square mod p. As an example, consider an $S_1(2, n+1; n^2+n+1)$ (a projective plane of order n) where $n \equiv 1$ or 2 mod 4. Then $(-1)^{(v-1/2)} = -1$ is a non-square mod p whenever $p \equiv 3$ mod 4. Thus there is no such plane whenever $n \equiv 1$ or 2 mod 4 has a prime $p \equiv 3$ mod 4 dividing its square free part n', e.g., no projective plane with $n \equiv 6$ mod 8. Thus the first values of n ruled out are $n = 6, 14, 21, 22, 30, 33, 38, \dots$.

It must be emphasized that our knowledge on the existence of symmetric designs is far from being satisfactory. There is no set of parameters (v, k, λ) for which the nonexistence of an $S_\lambda(2, k; v)$ is known, although the arithmetic conditions for a symmetric design are fulfilled and the parameters are not rejected by Theorems 3 and 4. For $\lambda = 1$, the smallest open cases are the projective planes of order $n = 10$ or 12. In spite of extensive research these cases are still not settled although one knows by now that a plane of order 10 admits no automorphisms (cf. Anstee, Hall and Thompson [1]). The remaining case of a possible collineation of order 3 has been excluded by Z. Janko in the meantime, a clear indication that it will be next to impossible to construct if it should exist. Our lack of knowledge is even more evident for $\lambda > 1$: Here only a finite number of symmetric 2-designs are known for each given value of λ. The situation is somewhat nicer for the case of 2-designs in general: Here the result of Wilson [53] already cited above leaves only a finite number of values for v undecided (given k and λ). But even for small values of k the bound given by Wilson is so large that his result is of no value whatsoever for practical applications.

Finally, we have to make one further remark on the existence problem for symmetric 2-designs: The conditions of Theorems 3 and 4 are sufficient for the existence of a *rational* $(v \times v)$-matrix satisfying the incidence equation $AA^T = (k-\lambda)I + \lambda J$. In case $n = k - \lambda$ is a square, one may take $A = n^{1/2}I + (k - n^{1/2})J/v$ and in the case of Theorem 4 the assertion may be proved using the Hasse–Minkowski Theory of rational quadratic forms, cf., e.g., Hall [17]. But already the existence question for *integral* solutions to the incidence equation is not settled; examples may be found in Hall [17] and in Johnsen [25] who in fact constructs integral solutions to the incidence equation for a projective plane of order n in cases where such a plane is not known to exist (including $n = 10$).

Variation 6. Codes — The bridge to applicable mathematics

Up to now we considered the incidence matrix of a symmetric design over the reals. Here the matrix is nonsingular, leading to the results discussed above; but the cases where the matrix is singular are quite interesting too. Thus we consider A over the fields GF(p), where p in general divides det A, i.e., where p divides k or n. The techniques used in these cases are slightly more complicated than those of usual linear algebra, because here we will be interested in the rank of A as well as in the so-called *weight* (i.e., the number of nonzero coordinates) of the vectors of the so-called *code* generated by the columns of A.

The concept of a code is conceived from communications engineering, where a *message* vector m of k entries from a field $\mathsf{F} = \mathrm{GF}(p)$ has to be transmitted over a channel which in general is noisy and thus disturbs the transmission seriously. In order to prevent these effects the transmitter usually lengthens the message vector m by adjoining another r *control* entries which are functions $(f_1(\boldsymbol{m}), \ldots, f_r(\boldsymbol{m})) = f(\boldsymbol{m})$ and sends the thus *encoded* message through the channel:

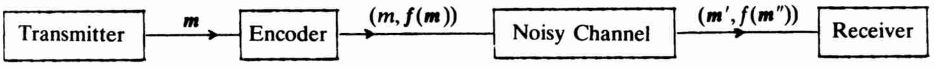

Transmitter
$\boldsymbol{m}$
Encoder
$(m, \boldsymbol{f}(\boldsymbol{m}))$
Noisy Channel
$(\boldsymbol{m}', \boldsymbol{f}(\boldsymbol{m}''))$
Receiver

Figure 3

The receiver at the other end reads the distorted message sequence $(\boldsymbol{m}', \boldsymbol{f}(\boldsymbol{m}''))$ which he now has to *decode* into the original message $\boldsymbol{m}$ by performing a maximum-likelihood decision based on $\boldsymbol{m}$ and the redundant r control entries $f(\boldsymbol{m}'')$. If the mapping $\boldsymbol{m} \rightarrow \boldsymbol{f}(\boldsymbol{m})$ is linear, the range $\mathscr{C} = G(\mathsf{F}^k)$ in F^{k+r} of the encoder $\boldsymbol{m} \rightarrow \boldsymbol{m} \cdot G = (\boldsymbol{m}, \boldsymbol{f}(\boldsymbol{m}))$ with generating matrix G is called a *linear* code. Its characteristic parameters are its *rate* $k/(k+r)$ and its *minimum weight* d. While the rate gives the rank of G, the minimum weight d guarantees two distinct *codewords* (i.e., vectors in $\mathscr{C}$) to differ in at least d coordinates, such that the receiver can retrieve the original message provided no more than $[(d-1)/2]$ coordinates of $\boldsymbol{m} \cdot G$ have been in error. By this short outline it has become obvious that coding theory differs from usual linear algebra in the aspect of being *base dependent.* In order to find linear codes which fulfil the requirements of a high rate and a large minimum weight, incidence matrices of geometries S play an important role as we will explain in using our "model" geometry $\mathscr{D}$:

PROBLEM 5. a) Determine the p-dimension of $\mathscr{C}(\mathscr{S})$, the code generated by the blocks of $\mathscr{S}$. b) Determine the weights of the codewords in $\mathscr{C}(\mathscr{S})$.

To give a taste of the manifold methods used in treating these problems we give

PROPOSITION 6. *$\mathscr{C}(\mathscr{D})$ has dimension* 4 *over* GF(2).

Proof. Extend the incidence matrix A of $\mathscr{D}$ by adjoining a row of entries $+1$ and call the new matrix $\bar{A}$. Then $\bar{A}^{\mathrm{T}}\bar{A} = 0$ over GF(2) as both $k+1=4$ and

$\lambda + 1 = 2$ are $\equiv 0 \bmod 2$; hence $\bar{\mathscr{C}}$ is contained in its dual $\bar{\mathscr{C}}^{\perp}$ (with respect to the standard inner product). Thus $\dim \bar{\mathscr{C}} \leq 4$ and hence $\dim \bar{\mathscr{C}} = 4$ as $\dim \bar{\mathscr{C}} \geq 4$ is obvious from the following arrangement of A which uses the representation of $\mathscr{D}$ over $\mathbb{Z}_7$:

$$A = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

But then also $\dim \mathscr{C} = 4$. □

We remark that the code $\mathscr{C}(\mathscr{D})$ is a special example of a *Hamming code*: Let m be a positive integer and $n = 2^m - 1$ and let H_m be an $(m \times n)$-matrix over GF(2) containing each vector in $\mathrm{GF}(2)^m$ which is distinct from 0 exactly once as a column. Then the set $\mathscr{C}_m = \{u \in \mathrm{GF}(2)^n : H_m \cdot u = 0\}$ is called the Hamming code of length $n = 2^m - 1$. The reader is asked to check that indeed $\mathscr{C}(\mathscr{D}) = \mathscr{C}_3$.

PROPOSITION 7. *The minimum weight of $\mathscr{C}(\mathscr{D})$ is $d = 3$.*

Proof. The $2^4 = 16$ codewords are formed by the zero vector, the all-one-vector, the 7 blocks (of weight $= 3$) and their 7 complements (of weight $= 4$). □

Note that $\mathscr{C}(\bar{\mathscr{D}})$ thus is a self-dual code all of whose weights are divisible by 4.

Self-dual codes (as the code $\bar{\mathscr{C}}$ considered above) are particularly important both in "pure" coding theory as well as in applications. As examples, we mention the work of Lander [26] who used self-dual codes to study automorphisms of symmetric designs and that of McWilliams, Sloane and Thompson [32] who used self-dual codes to study the properties of a putative projective plane of order 10. In Variation 7 we will show that self-dual codes with weights $\equiv 0 \bmod 4$ can be classified by methods of invariant theory.

In Proposition 6 we only considered the code generated by $\mathscr{D}$ over GF(2); but $\det A = 0$ holds over GF(3), too. The following more general result shows that this situation is not too interesting as it just yields a hyperplane in the vector space under consideration.

PROPOSITION 8. *Let $\mathscr{C}$ be the code generated by the blocks of a symmetric 2-design $S_\lambda(2, k; v)$ over* GF(p), *where p divides k but does not divide n. Then* $\dim \mathscr{C} = v - 1$.

Proof. By Lemma 4, $AA^{\mathrm{T}} = \lambda K + nI$ and this matrix is equivalent to the matrix (using $(v-1)\lambda + k = k^2$)

$$\begin{bmatrix} n & 0 & 0 & & \cdots\cdots & & 0 \\ 0 & n & 0 & & \cdots\cdots & & 0 \\ & & \cdots\cdots & & & & \\ 0 & 0 & \cdots & 0 & & n & 0 \\ \lambda & \lambda & \cdots & & & \lambda & k^2 \end{bmatrix}$$

which clearly has rank $v-1$ over GF(p). But this implies that A itself has rank $v-1$, too. □

Variation 7. Representation theory and some applications

In our proof of Proposition 6 we used the fact that $\mathcal{D}$ admits a cyclic incidence matrix A in a rather ad hoc fashion; we will now make more systematic use of this fact to give an alternative proof of Propositions 6 and 7. We will require a definition: Let $\mathcal{C}$ be a subspace of the vector space GF$(q)^n$. Then $\mathcal{C}$ is called a *cyclic code* iff $(c_0, \ldots, c_{n-1})^{\mathrm{T}} \in \mathcal{C}$ always implies $(c_{n-1}, c_0, \ldots, c_{n-2})^{\mathrm{T}} \in \mathcal{C}$. Clearly the code $\mathcal{C}(\mathcal{D})$ is cyclic, as $\mathcal{D}$ admits $\mathbf{Z}_7$ as an automorphism group. The following result is obvious, noting that a cyclic shift of $(c_0, \ldots, c_{n-1})^{\mathrm{T}}$ as above corresponds to multiplying $c(x)$ by x modulo $x^n - 1$:

LEMMA 5. *The mapping*

$(c_0, \ldots, c_{n-1}) \rightarrow c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$

defines a vector space isomorphism from GF$(q)^n$ *onto the ring* $R =$ GF$(q)[x]/(x^n - 1)$. *A linear subspace* $\mathcal{C}$ *of* GF$(q)^n$ *is a cyclic code iff* $I := \{c(x) : c \in \mathcal{C}\}$ *is an ideal in* R.

An alternative proof of Proposition 6 may now be given as follows: By Lemma 5, $\mathcal{C} = \mathcal{C}(\mathcal{D})$ is an ideal in $R = \mathrm{GF}(2)[x]/(x^7 - 1)$. Since $x^7 - 1$ factors into the irreducible polynomials $x - 1$, $x^3 + x + 1$ and $x^3 + x^2 + 1$ over GF(2), using the Chinese remainder theorem we have $R \cong \mathrm{GF}(2) \oplus \mathrm{GF}(8) \oplus \mathrm{GF}(8)$ (as a ring). Now $\mathcal{C}$ is the ideal generated by $1 + x + x^3$ (as $\{0, 1, 3\}$ is a difference set for $\mathcal{D}$). As R is semi-simple, $\mathcal{C}$ is in fact the direct sum of the ideals generated by this polynomial in each of the three direct summands of R. This gives dimension 1 modulo $x - 1$, dimension 0 modulo $x^3 + x + 1$ and dimension 3 modulo $x^3 + x^2 + 2$ and thus $\dim \mathcal{C} = 3 + 1 = 4$ (where of course every ideal is considered as a vector space over GF(2)). □

The observations used in the alternative proof of Proposition 6 lead to an algebraic algorithm for a maximum likelihood decoding procedure for this Hamming code $\mathscr{H}_3$ which can correct one error (as $d = 3$): Suppose the receiver has read the sequence $\boldsymbol{u} = \boldsymbol{c} + \boldsymbol{e}$, where $\boldsymbol{e}$ is a weight-one-error pattern (say $\boldsymbol{e} = (0, 0, \ldots, 1, \ldots, 0, 0)$ with the entry 1 in position C), distorting $\boldsymbol{c}$ into $\boldsymbol{u}$. As $\mathscr{H}$ can correct such an error, we have to compute the location C of this error entry. This can be done as follows. Take the vector $\boldsymbol{u} = (u_0, \ldots, u_6)$, form the polynomial $u(x) = \sum_{i=0}^{6} u_i x^i$ and reduce it modulo $x^3 + x + 1$. Since $u(x) = c(x) + x^e$ we obtain $u(x) \equiv x^e \bmod x^3 + x + 1$ as $c(x) \equiv 0 \bmod x^3 + x + 1$ (see above). Since $x^3 + x + 1$ is a primitive polynomial for the field extension GF(2^3): GF(2), the powers x^e correspond to the seven nonzero elements of GF(2^3).

This algorithm can be beautifully implemented by elementary electronic units:

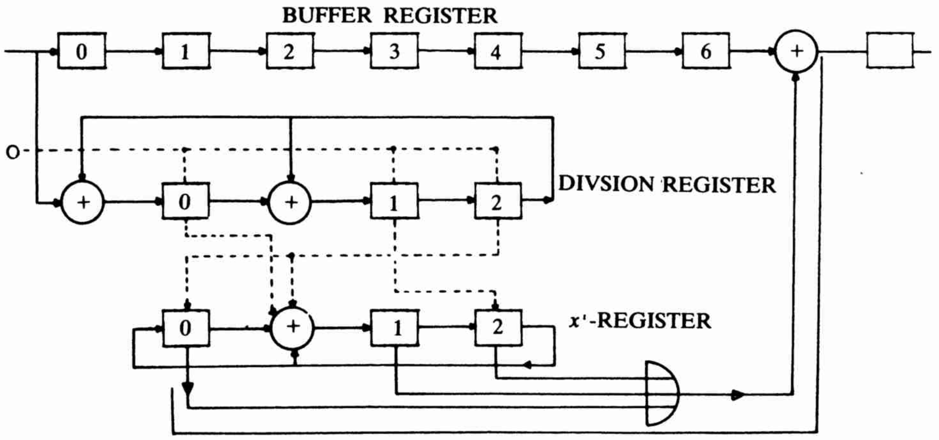
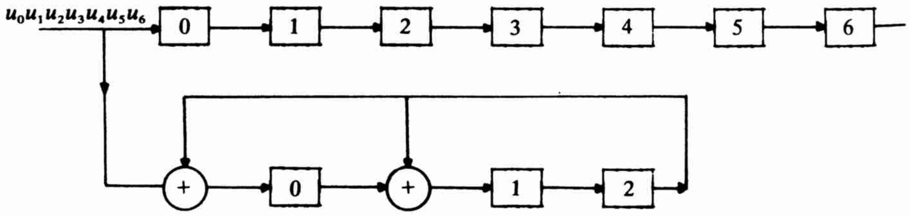


Figure 4

The upper part is just a storage buffer, while the lower part D is a *division register* performing Euclid's algorithm to compute $u(x) \bmod x^3 + x + 1$:



The register divides $u(x) = u_0 + u_1x + u_2x^2 + u_3x^3 + u_4x^4 + u_5x^5 + u_6x^6$

by

$g(x) = 1 \quad + \quad x \qquad\quad + x^3$

with remainder

$r(x) = r_0 + r_1x + r_2x^2.$

Figure 5

D contains the remainder of this computation after the last entry u_0 of $\boldsymbol{u}$ has entered. Then D is running autonomically, i.e., without input. If its content is zero it remains 0, 0, 0, and if its content is nonzero it cyclically passes through the 7 nonzero elements of GF(8)

$$\begin{array}{l}
1\ 0\ 0 \triangleq x^0 \\
0\ 1\ 0 \triangleq x^1 \\
0\ 0\ 1 \triangleq x^2 \\
1\ 1\ 0 \triangleq x^3 \\
0\ 1\ 1 \triangleq x^4 \\
1\ 1\ 1 \triangleq x^5 \\
1\ 0\ 1 \triangleq x^6 \\
1\ 0\ 0 \triangleq x^0 \\
\quad\ \vdots
\end{array}$$

Thus, if the remainder has been computed to be x^e, then D needs $6-e$ time units to reach the state $(1,0,1)$ in which case the gate will put out a "1" which then is added to the erroneous entry u_e of y which by then has also reached the 6th position of the buffer. □

This short trip to mathematical design of electronic units is one aspect of applications. The other aspect is that of applying these methods to again obtain theoretical results.

Note that the ring $R = \mathrm{GF}(q)[x]/(x^n - 1)$ is isomorphic to the group ring $\mathrm{GF}(q)[\mathbb{Z}_n]$. Group rings play a fundamental role both in coding theory (as suggested by our example) and in the study of Singer groups of symmetric 2-designs. We will mention just two examples. First, consider a desarguesian projective plane (i.e., a projective plane constructed from a field GF(q) as indicated in the proof of the Corollary to Proposition 3). By the theorem of Singer [46], any such plane admits a cyclic Singer group (and thus may be represented using a difference set). This may be used to determine the dimension of its code (the alternative proof of Proposition 6 is an example). It turns out that the plane over $\mathrm{GF}(p^a)$ (p prime) yields a code of dimension $\binom{p+1}{2}^a + 1$ over GF(p). This result is due to McWilliams and Mann [30].

Our second example generalizes the following observation:

PROPOSITION 9. *Consider $\mathscr{D}$ represented within $\mathbb{Z}_7$ as above. Then the group automorphism $x \rightarrow 2x$ of $\mathbb{Z}_7$ induces an automorphism of $\mathscr{D}$.*

Proof. The block set of $\mathscr{D}$ may be written as $\{\{1,2,4\}+x: x \in \mathbf{Z}_7\}$. Observe that $\{1,2,4\}+x$ is mapped onto the block $\{1,2,4\}+2x$. □

This phenomenon has more generally been treated within the beautiful theory of abelian difference sets. Let $\mathscr{S}$ be a symmetric 2-design $S_\lambda(2,k;v)$ with an abelian Singer group G (so that $\mathscr{S}$ may be represented by a difference set over G). If t is a positive integer prime to v, then $x \to tx$ is a group automorphism of G; if this automorphism induces an automorphism of $\mathscr{S}$, then t is called a (*numerical*) *multiplier.* The following basic theorem of Hall [16] started the study of multipliers:

If G is cyclic, t a prime not dividing v, but dividing $n = k - \lambda$, and if $t > \lambda$, then t is a numerical multipler.

The present version of this result is much stronger but quite technical; the interested reader is referred to Mann [33]. But already the first result of Hall leads to quite interesting techniques which we will illustrate by some examples. We shall also need the fact that each multiplier fixes at least one block of $\mathscr{S}$. (This is not too difficult: Counting arguments show that each automorphism of $\mathscr{S}$ fixes an equal number of points and blocks, cf., also Parker [40]; and clearly a multiplier t fixes the neutral element 0 of G.)

Now consider a projective plane of order n (i.e., an $S_1(2, n+1; n^2+n+1)$). Clearly, each prime p dividing n satisfies the theorem stated above and thus each divisor of n is a multiplier of $\mathscr{S}$, provided $\mathscr{S}$ admits a cyclic Singer group (the same result in fact still holds for abelian groups). If $\mathscr{S}$ is the desarguesian plane of order $n = p^a$, this assumption is satisfied, and p is a multiplier. As p fixes one block of $\mathscr{S}$, we may choose this block as a difference set for $\mathscr{S}$. E.g., for $n = 2$, 2 is a multiplier; as it fixes the difference set D, D is of the form $\{x, 2x, 4x\}$ and as 7 is a prime we may w.l.o.g. assume $x = 1$ (by multiplying D by $1/x$ (mod 7) if necessary). Thus the knowledge that $\mathscr{S}$ is representable by a difference set suffices in this case to construct the difference set! Similarly, if $n = 3$, then D has to contain w.l.o.g. 1, 3, 9; but, as $v = 13$ is a prime in this case and as D contains 4 elements altogether, the only possible choice for the missing element is 0 (choosing $x \neq 0$, D would have to contain $3x$ and $9x$ too). Thus $\{0,1,3,9\} \subset \mathbf{Z}_{13}$ yields the projective plane of order 3. The case $n = 4$ is slightly more involved: Here, $v = 21$ is not prime. If $x \in D$, then also $2x, 4x, \ldots$ are in D; if x is prime to 21, this yields more than 5 elements (which is the size of D). Thus D must be a union of suitable sets from $\{3,6,12\}$, $\{7,14\}$ and $\{9,18,15\}$; indeed, both $\{3,6,12,7,14\}$ and $\{9,18,15,7,14\}$ work. The amount of computation becomes larger when n grows but the use of multiplier results in any case simplifies the task of finding a desired difference set.

Moreover, this method may even be used to show the nonexistence of certain difference sets. A $(31,10,3)$-difference set would be necessarily in a cyclic group and would admit 7 as a multiplier. Thus D would contain w.l.o.g. all elements 7^a mod 31; but this yields more than 10 elements and thus no such difference set exists. Similarly, no projective plane of order n divisible by 6 can admit a cyclic difference set: Here 2 and 3 would be multipliers and it can be shown that all the multipliers of a cyclic group fix a common block (this even holds for all numerical multipliers of an abelian group, cf. McFarland and Rice [34]). Hence D contains $2x$ and $3x$ if it contains x; but $3x - 2x = 2x - x = x$ are 2 distinct difference representations of x, contradicting $\lambda = 1$. As an exercise, the reader may find $(37, 9, 2)$- and $(23, 11, 5)$-difference sets and show the nonexistence of cyclic difference sets for a projective plane of order n divisible by 10. A detailed study of cyclic difference sets is given by Baumert [2]. A new proof method for multiplier theorems and some interesting applications have been given by Lander [26].

Finally we want to show that under a much more general aspect our model geometry plays a fundamental role. Let $\mathscr{C} \subset \mathrm{GF}(q)^n$ be a k-dimensional linear code. Let A_i denote the number of codewords of weight i in $\mathscr{C}$. The *weight enumerator* of $\mathscr{C}$ is the polynomial $\sum_{i=0}^{n} A_i x^i y^{n-i} = A_{\mathscr{C}}(x, y) \in \mathbb{C}[x, y]$. Let $\mathscr{C}^{\perp} \subset \mathrm{GF}(q)^n$ denote the orthogonal complement (the dual) of $\mathscr{C}$ with respect to the standard inner product.

Then the following theorem, due to McWilliams [29], gives the weight enumerator of $\mathscr{C}^{\perp}$.

THEOREM 5. $A_{\mathscr{C}^{\perp}}(x, y) = 1/q^k \cdot A_{\mathscr{C}}(y - x, y + (q-1)x)$.

For self-dual codes over GF(2) we thus have the following corollary.

COROLLARY. $A_{\mathscr{C}}(x, y) = A_{\mathscr{C}}((y - x)/\sqrt{2}, (y + x)/\sqrt{2}))$.

EXAMPLE. Let $\bar{\mathscr{H}}_3$ be the extended Hamming code of length 8. As already mentioned before, its weight enumerator is

$$A_{\bar{\mathscr{H}}_3}(x, y) = x^8 + 14x^4y^4 + y^8.$$

It is an easy exercise to verify that $A_{\bar{\mathscr{H}}_3}$ fulfils the equation of the corollary, i.e., $A_{\bar{\mathscr{H}}_3}(x, y)$ remains invariant under the transformation

$$(x, y) \to (x, y) \begin{bmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

After this example we can readily formulate a theorem by Gleason [15]:

THEOREM 6. *Let $\mathscr{C}$ be a self-dual linear code over* GF(2) *such that all codewords have weight divisible by* 4. *Then $A_{\mathscr{C}}(x, y)$ is an invariant of the group G generated by*

$$S = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad R = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$$

in GL(2, $\mathbb{C}$).

Using a theorem of Noether [36] we want to determine an integrity base of the ring of invariants of G. The theorem of Molien [35] tells us (see Sloane [47] or Beth and Stehl [6]) that such a base is formed by the weight enumerators of two codes: The extended Hamming Code $\bar{\mathscr{H}}_3$,

$$A_{\bar{\mathscr{H}}_3}(x, y) = x^8 + 14x^4y^4 + y^8,$$

and the extended Golay code $\overline{\mathscr{G}_{23}}$ which has also implicitly been mentioned in the context of this survey: It is the code generated by the incidence matrix of the Witt design $S_1(5, 8; 24)$ associated with the Mathieu group M_{24}, cf., e.g., Beth and Jungnickel [4]. Its weights enumerator is

$$A_{\bar{\mathscr{G}}_{23}}(x, y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}.$$

Coda

Concluding this excursion through 7 aspect of mathematics we see that our choice of the "model geometry" on 7 points has indeed revealed some of the remarkable features and developments that the area of finite geometries has created in the last three decades.

We close by mentioning some books which the interested reader might consult for further study. The fundamental notions and problems of finite geometries are studied in detail in our forthcoming joint book with Prof. Lenz [5]. Other general references are the books of Hall [17] and its updating given by van Lint [49]. For permutation groups, Wielandt [51] and Passman [41] are standard references, for groups in general see Huppert [22] and Huppert and Blackburn [23], [24]. Coding theory is treated extensively in McWilliams and Sloane [31] and the earlier book by van Lint [48]. A nice introductory monograph on the relations between groups and designs is Biggs and White [7]. Much more difficult, but fundamental, is the book of Cameron and van Lint [12] which explores the relations between graphs, codes and designs. An interesting collection of papers on t-designs has been edited by Lindner and Rosa [27]. Among others, it also contains the bibliography on t-designs with $\lambda = 1$ by Doyen and Rosa [14]. Finally, the standard references for projective planes are Pickert [43] and Hughes and Piper [21].

REFERENCES

[1] ANSTEE, R. P., HALL, M. and THOMPSON, J. G., *Planes of order 10 do not have collineation of order 5.* J. Comb. Theory, Ser. A *29* (1980), 39–58.

[2] BAUMERT, L. D., *Cyclic difference sets.* Lecture Notes in Math. Vol. 182, Springer, Berlin–Heidelberg–New York, 1971.

[3] BETH, TH., *Some remarks on D. R. Hughes' construction of M_{12} and its associated designs.* In *Finite geometries and designs* (Proc. 2nd. Isle of Thorns Conf., 1980), London Math. Soc. Lecture Notes, Vol. 49, Cambridge Univ. Press, 1981, pp. 22–30.

[4] BETH, TH. and JUNGNICKEL, D., *Mathieu groups, Witt designs and Golay codes.* In *Geometries and groups.* Springer Lecture Notes in Math. Vol. 893, Berlin–Heidelberg–New York, 1981, pp. 157–179.

[5] BETH, TH., JUNGNICKEL, D. and LENZ, H., *Design theory.* B. I. Wissenschaftsverlag, Mannheim, to appear in 1984.

[6] BETH, TH. and STREHL, V., *Materialien zur Colierungstheorie.* Arbeitsber. des Inst. Math. Masch. Datenverarb. (Inform.) *11* (1978), 14.

[7] BIGGS, N. L. and WHITE, A. T., *Permutation groups and combinatorial structures.* London Math. Soc. Lecture Notes *33,* Cambridge University Press, 1979.

[8] BOSE, R. E. *On the construction of balanced incomplete block designs.* Ann. Eugenics *9* (1939), 353–399.

[9] BRUCK, R. H. and RYSER, H. J., *The nonexistence of certain finite projective planes.* Canad. J. Math. *1* (1949), 88–93.

[10] CAMERON, P. J., *Extending symmetric designs.* J. Comb. Theory, Ser. A *14* (1973), 215–220.

[11] CAMERON, P. J., *Finite permutation groups and finite simple groups.* Bull. London Math. Soc. *13* (1981), 1–22.

[12] CAMERON, P. J. and VAN LINT, J. H., *Graphs, codes and designs.* London Math. Soc. Lecture Notes 43, Cambridge University Press, Cambridge, 1980.

[13] CHOWLA, S. and RYSER, H. J., *Combinatorial problems.* Canad. J. Math. *2* (1950), 93–99.

[14] DOYEN, J. and ROSA, A., *An updated bibliography and survey of Steiner systems.* Ann. Discrete Math. *7* (1980), 317–349.

[15] GLEASON, A. M., *Weight polynomials of self-dual codes and the McWilliams identities.* Actes du Congrès International des Mathématiciens (Nice 1970) Tóme 3, Gauthier-Villars, Paris, 1971, pp. 211–215.

[16] HALL, M. JR., *Cyclic projective planes.* Duke Math. J. *14* (1947), 1079–1090.

[17] HALL, M. JR., *Combinatorial theory.* Blaisdell, Waltham, Mass., 1967.

[18] HANANI, H., *Balanced incomplete block designs and related designs.* Discrete Math. *11* (1975), 255–369.

[19] HEDAYAT, A. and WALLIS, W. D., *Hadamard matrices and their applications.* Ann. Stat. *6* (1978), 1184–1238.

[20] HUGHES, D. R., *On t-designs and groups.* Amer. J. Math. *87* (1965), 761–778.

[21] HUGHES, D. R. and PIPER, F. C., *Projective planes.* Springer, Berlin–Heidelberg–New York, 1973.

[22] HUPPERT, B., *Endliche Gruppen I.* Springer, Berlin–Heidelberg–New York, 1967, 2nd ed., 1979.

[23] HUPPERT, B. and BLACKBURN, N., *Finite groups II.* Springer, Berlin–Heidelberg–New York, 1982.

[24] HUPPERT, B. and BLACKBURN, N., *Finite groups III.* Springer, Berlin–Heidelberg–New York, 1982.

[25] JOHNSEN, E. C., *The inverse multiplier for abelian group difference sets.* Canad. J. Math. *16* (1964), 787–796.

[26] LANDER, E. S., *Topics in algebraic coding theory.* Ph.D. Thesis, Oxford, 1980.

[27] LINDNER, C. C. and ROSA, A., (Eds.) *Topics on Steiner systems.* Ann. Discrete Math. *7* (1980).

[28] LÜNEBURG, H., *Transitive Erweiterungen endlicher Permutationsgruppen.* Lecture Notes 84, Springer, Berlin–Heidelberg–New York, 1969.

[29] MACWILLIAMS, F. J., *A theorem on the distribution of weights in a systematic code.* Bell System Tech. J. *42* (1963), 79–94.

[30] MACWILLIAMS, F. J. and MANN, H. B., *On the p-rank of the design matrix of a difference set.* Inform. and Control *12* (1968), 474–488.

[31] MACWILLIAMS, F. J. and SLOANE, N. J. A., *The theory of error-correcting codes.* North-Holland, Amsterdam, 1978.

[32] MACWILLIAMS, F. J., SLOANE, N. J. A. and THOMPSON, J. G., *On the existence of a projective plane of order 10.* J. Comb. Theory, Ser. A *14* (1973), 66–78.

[33] MANN, H. B., *Addition theorems.* Wiley Interscience, New York, 1965.

[34] MCFARLAND, R. L. and RICE, B. F., *Translates and multipliers of abelian difference sets.* Proc. Amer. Math. Soc. *68* (1978), 375–379.

[35] MOLIEN, T., *Über die Invarianten der linearen Substitutionsgruppen.* Sitzungsber. Kgl. Preuss. Akad. Wiss. (1897), 1152–1156.

[36] NOETHER, E., *Der Endlichkeitssatz der Invarianten endlicher Gruppen.* Math. Ann. *77* (1916), 89–92.

[37] NORMAN, C. W., *A characterization of the Mathieu group M_{11}.* Math. Z. *106* (1968), 162–166.

[38] OTT, U., *Endliche zyklische Ebenen.* Math. Z. *144* (1975), 195–215.

[39] PALEY, R. E. A. C., *On orthogonal matrices.* J. Math. Phys. Inst. Tech. *12* (1933), 311–320.

[40] PARKER, E. T., *On collineations of symmetric designs.* Proc. Amer. Math. Soc. *8* (1957), 350–351.

[41] PASSMAN, D., *Permutation groups.* Benjamin, New York, 1968.

[42] PETRENJUK, A. JA., *On Fisher's inequality for tactical configurations* (Russian). Math. Zametki *4* (1968), 417–424.

[43] PICKERT, G., *Projektive Ebenen.* Springer, Berlin–Heidelberg–New York, 2nd ed. 1975.

[44] RAY-CHAUDHURI, D. K. and WILSON, R. M., *On t-designs.* Osaka J. Math. *12* (1975), 737–744.

[45] SCHÜTZENBERGER, M. P., *A non-existence theorem for an infinite family of symmetric block designs.* Ann. Eugenics *14* (1949), 286–287.

[46] SINGER, J., *A theorem in finite projective geometry and some applications to number theory.* Trans. Amer. Math. Soc. *43* (1938), 377–385.

[47] SLOANE, N. J., *Error-correcting codes and invariant theory: New applications of a nineteenth century technique.* Amer. Math. Monthly *84* (1977), 82–107.

[48] VAN LINT, J. H., *Coding theory.* Lecture Notes in Math. *201*, Springer, Berlin–Heidelberg–New York, 1971.

[49] VAN LINT, J. H., *Combinatorial theory seminar Eindhoven Univ. of Technology.* Lecture Notes Vol. 382, Springer, Berlin–Heidelberg–New York, 1974.

[50] WALLIS, W. D., STREET, A. P. and WALLIS, J. S., *Combinatorics: Room squares, sum-free sets, Hadamard matrices.* Lecture Notes in Math. Vol. 292, Springer, Berlin–Heidelberg–New York, 1972.

[51] WIELANDT, H., *Finite permutation groups.* Academic Press, New York–San Francisco–London, 1964.

[52] WILSON, R. M., *Cyclotomy and difference families in elementary abelian groups.* J. Number Theory *4* (1972), 17–47.

[53] WILSON, R. M., *An existence theory for pairwise balanced designs III: Proof of the existence conjectures.* J. Comb. Theory, Ser. A *18* (1975), 71–79.

[54] WITT, E., *Die 5-fach transitiven Gruppen von Mathieu.* Abh. Math. Sem. Hamburg *12* (1938), 256–264.

[55] WITT, E., *Über Steinersche Systeme.* Abh. Math. Sem. Hamburg *12* (1938), 265–275.

Institut für Mathematische Maschinen
und Datenverarbeitung I,
Universität Erlangen,
Martenstr. 3,
D-8520 Erlangen,
F.R. Germany.

Mathematisches Institut
der Universität Giessen,
Arndtstr. 2,
D-6300 Giessen,
F.R. Germany.