Europ. J. Combinatorics (2001) **22**, 63–69
doi:10.1006/eujc.2000.0426
Available online at http://www.idealibrary.com on IDEAL®

Note on GMW Designs

WILLIAM M. KANTOR

Equivalence of GMW difference sets corresponds to isomorphism of the associated designs.

Let N and n be integers such that $n|N$ and $2 < n < N$. Let q be a prime power. The difference sets introduced by Gordon, Mills and Welch in [1] produce symmetric designs with the same parameters $v = (q^N - 1)/(q - 1)$, $k = (q^{N-1} - 1)/(q - 1)$, $\lambda = (q^{N-2} - 1)/(q - 1)$ as the point-hyperplane design of $\mathrm{PG}(N - 1, q)$. The purpose of this note is to prove that inequivalent difference sets of this sort produce nonisomorphic designs.

There are various ways to construct the GMW designs. Since we wish to study designs rather than difference sets, we will use the very nice alternative description in [4] rather than the more standard difference set point of view [1, 6].

Consider the fields $V = \mathbf{F}_{q^N} \supset \mathbf{F}_{q^n} \supset \mathbf{F}_q$; let V° denote the dual of the $\mathbf{F}_{q^n}$-space V, consisting of all linear functionals $f: V \to \mathbf{F}_{q^n}$. We will also view V and V° as $\mathbf{F}_q$-spaces, in which case we write $\langle v \rangle$ for the 1-space spanned by $v \in V - \{0\}$ and $\langle f \rangle$ for the 1-space spanned by $f \in V^\circ - \{0\}$. Fix a $((q^n - 1)/(q - 1), (q^{n-1} - 1)/(q - 1), (q^{n-2} - 1)/(q - 1))$ difference set D in $\mathbf{F}^*_{q^n}/\mathbf{F}^*_q$ (hence the assumption $n > 2$), let $\tilde{D}$ denote the union in $\mathbf{F}^*_{q^n}$ of the cosets comprising D, and define the incidence structure $\mathbf{D}(N, n, D)$ as follows: its points are the 1-spaces $\langle v \rangle$, its blocks are the 1-spaces $\langle f \rangle$, and $\langle v \rangle$ and $\langle f \rangle$ are incident if and only if $f(v) \in \tilde{D} \cup \{0\}$. As noted in [4], these are symmetric designs that include the "classical" ones in [1] (where D is taken to be equivalent to a difference set with corresponding symmetric design $\mathrm{PG}(n - 1, q)$).

Since the case in which $\mathbf{D}(N, n, D)$ is isomorphic to a projective space is fully handled in [1, 4], we will exclude this possibility. The statements of the following theorems deal with the fact that the same symmetric design can arise as $\mathbf{D}(N, n, D)$ for different values of n (which is why we have included n in the notation $\mathbf{D}(N, n, D)$).

THEOREM 1. *Assume that* $\mathbf{D}$ *is a symmetric design, not isomorphic to a projective space, such that* $\mathbf{D} \cong \mathbf{D}(N, n, D)$ *for some* N, n *and* D *and where* n *is chosen as small as possible. Then* $\mathrm{Aut}\mathbf{D} \cong \Gamma\mathrm{L}(N/n, q^n)/Z_{q-1}$, *where* Z_{q-1} *consists of the scalar transformations of* V *induced by* $\mathbf{F}^*_q$.

THEOREM 2. *Assume that* D *is a difference set in* $\mathbf{F}^*_{q^n}/\mathbf{F}^*_q$ *such that* $\mathbf{D}(N, n, D)$ *is not isomorphic to a projective space.*

(i) If D' *is a difference set in* $\mathbf{F}^*_{q^n}/\mathbf{F}^*_q$, *then* $\mathbf{D}(N, n, D) \cong \mathbf{D}(N, n, D')$ *if and only if* $D' = aD$ *for some* $a \in \mathbf{F}^*_{q^n}/\mathbf{F}^*_q$.

(ii) Assume that D' *is a difference set in* $\mathbf{F}^*_{q^{n'}}/\mathbf{F}^*_q$, *and that* n *and* n' *are both minimal in the sense of Theorem* 1. *Then* $\mathbf{D}(N, n, D) \cong \mathbf{D}(N, n', D')$ *if and only if* $n = n'$ *and* $D' = aD$ *for some* $a \in \mathbf{F}^*_{q^n}/\mathbf{F}^*_q$.

Some instances of Theorem 2 are already known. These are surveyed at length in [6, pp. 77–88]: the rank of the $\mathbf{F}_p$-code determined by an incidence matrix of $\mathbf{D}(N, n, D)$ has been computed when $q = 2$ and D is classical or in a few instances when $q \le 9$, and when these ranks are different the designs cannot be isomorphic. However, it should be noted that these

0195–6698/01/010063 + 07 $35.00/0

same rank results show that the ranks for $\mathbf{D}(N, n, D)$ and $\mathbf{D}(N, n, D')$ are often the same, in which case no nonisomorphism information can be obtained in this manner.

More generally, it appears that standard difference set methods are not strong enough to decide design isomorphism. Therefore, we need to use other techniques: our approach to Theorem 2 depends on Theorem 1, which in turn uses group theory and internal properties of these designs.

Let $h = N/n$. We define a *clump* of $\mathbf{D}(N, n, D)$ to be the set of points in $\mathbf{F}_{q^n}v$ for some $0 \neq v \in V$; of course, clumps correspond to the points of $\mathrm{PG}(h-1, q^n)$. Let $\mathcal{C}$ denote the set of all clumps. There is also the notion of a *dual clump* determined by a non-zero linear functional. We will need the following observations, where each block $\langle f \rangle$ is identified with the set of points incident with it.

(1) The set $\mathcal{C}_f$ of clumps in $\langle f \rangle$ has size $(q^{N-n}-1)/(q^n-1)$; these clumps arise from the hyperplane of $\mathrm{PG}(h-1, q^n)$ corresponding to $\mathrm{Ker}\, f$.

(2) If C_1 and C_2 are distinct clumps, then the intersection of the set of blocks containing both of them contains exactly q^n+1 clumps; by (1) these clumps arise from a line of $\mathrm{PG}(h-1, q^n)$.

The derived group of a group S is denoted S'.

(3) The construction shows that $\mathrm{Aut}\mathbf{D}(N, n, D)$ contains $G = \mathrm{GL}(h, q^n)/Z_{q-1}$; that it contains $\Gamma\mathrm{L}(h, q^n)/Z_{q-1}$ is noted in [4]. Moreover, G' is a homomorphic image of $\mathrm{SL}(h, q^n)$ [10, p. 23] that is transitive on points (and blocks), and clumps are blocks for this transitive action, as well as for that of G. (Note: We need two entirely different standard uses for the term "block", which can be easily distinguished from context. See [11] for the standard background concerning primitive and imprimitive permutation groups.)

Let p denote the prime dividing q. Before continuing we digress briefly by noting the following special case of a lemma of Tits [8, (1.6)] (the special case is easily proved using linear algebra):

($*$) If M is a subgroup of $\mathrm{GL}(h, q^n)$ that does not contain $\mathrm{SL}(h, q^n)$ but contains a Sylow p-subgroup of $\mathrm{GL}(h, q^n)$, then there is a set of subspaces such that M fixes each of them and contains every Sylow p-subgroup of $\mathrm{GL}(h, q^n)$ that fixes each of them.

(3′) Each nontrivial block of G on points is contained in a clump. (This states that any proper subgroup M of G containing the stabilizer G_x of a point x fixes the clump containing x; that is, fixes the point of $\mathrm{PG}(h-1, q^n)$ containing x. To see this, note that $|G{:}\,M|$ divides $(q^N-1)/(q-1)$ and hence is not divisible by p, so that M contains a Sylow p-subgroup of G. Since $G = \langle G', G_x \rangle$, M cannot contain G' and hence must be reducible by ($*$). Then the only proper subspace of V fixed by G_x must also be fixed by M.)

(4) If $\mathcal{F}$ is any dual clump of blocks not containing a clump C, then the induced incidence structure $(C, \mathcal{F})$ is isomorphic to the design determined by the difference set D (i.e., if $f \in V^\circ$ and $f(v) \neq 0$, then for $\alpha, \beta \in \mathbf{F}_{q^n}^*$ we have $(\alpha f)(\beta v) \in \tilde{D}$ if and only if $\beta \in (\alpha f(v))^{-1}\tilde{D}$).

(4′) If C is a clump then $\{C \cap X \mid X \text{ is a block} \not\supset C\}$ is the set of blocks of a symmetric design, with point set C, isomorphic to the design determined by the difference set D (proved as in (4); cf. [4, Lemmas 4 and 5]).

We begin with a slight extension of [4, Theorem 7].

PROPOSITION 3. *If* $\mathbf{D}$ *is a symmetric* $((q^N-1)/(q-1), (q^{N-1}-1)/(q-1), (q^{N-2}-1)/(q-1))$ *design, and if* $S = S' \leq \mathrm{Aut}\mathbf{D}$ *is point-transitive and* $S/Z(S) \cong \mathrm{PSL}(N/n, q^n)$ *for some* $n > 2$, *then* $\mathbf{D} \cong \mathbf{D}(N, n, D)$ *for some* D.

PROOF. S is a homomorphic image of $\mathrm{SL}(N/n, q^n)$ [9], and hence we may assume that $S = \mathrm{SL}(N/n, q^n)$, not necessarily acting faithfully (as in the case of the designs $\mathbf{D}(N, n, D)$ for suitable q). In view of the argument in the proof of [4, Theorem 7], it is only necessary to show that the action of S on points is completely determined (up to an automorphism of S).

If x is a point then its stabilizer S_x contains a Sylow p-subgroup of S. Since $S_x < S$, by $(*)$ it follows that S_x fixes some subspace of V. Then $(q^N-1)/(q-1) = |S\colon S_x|$ is divisible by the number of subspaces of the h-space V of some dimension. Consequently, that dimension must be 1 or $h-1$ (e.g., using [12]). Up to an outer automorphism of S, we may assume that S_x fixes a point $\mathbf{x}$ of $\mathrm{PG}(h-1, q^n)$ and acts irreducibly on $V/\mathbf{x}$.

If $h > 2$ then $(S_{\mathbf{x}})'$ induces at least $\mathrm{SL}(h-1, q^n)$ on $V/\mathbf{x}$ [10, p. 22] since $q^n > 3$; by $(*)$ and irreducibility we have $S_x \geq (S_{\mathbf{x}})'$. If $h = 2$ then $(S_{\mathbf{x}})'$ is an elementary abelian group consisting of q transvections, and again $S_x \geq (S_{\mathbf{x}})'$. More precisely, for any h, with respect to a suitable basis $S_{\mathbf{x}}$ consists of all $\mathbf{F}_{q^n}$-matrices $\left(\begin{smallmatrix} a & O \\ * & A \end{smallmatrix}\right)$ with A an $(h-1)\times(h-1)$ matrix and $a^{-1} = \det A$, while $(S_{\mathbf{x}})'$ consists of all $\left(\begin{smallmatrix} 1 & O \\ * & A \end{smallmatrix}\right)$ with $\det A = 1$.

We have $\{(q^N-1)/(q-1)\}|S_x\colon (S_{\mathbf{x}})'| = |S\colon (S_{\mathbf{x}})'| = q^N - 1$ since $(S_{\mathbf{x}})'$ is the stabilizer in S of a nonzero vector. Then $|S_x\colon (S_{\mathbf{x}})'| = q-1$, so that S_x consists of all $\left(\begin{smallmatrix} a & O \\ * & A \end{smallmatrix}\right)$ with $a^{-1} = \det A \in \mathbf{F}_q^*$ and hence is determined up to conjugacy, as required. □

REMARK. If we allowed $n = 1$ or 2 in the proposition then the same argument would show that $\mathbf{D}$ is a projective space.

PROOF OF THEOREM 1. The subgroup H of G inducing the identity on $\mathrm{Ker} f$ consists of all $\mathbf{F}_{q^n}$-matrices $\left(\begin{smallmatrix} * & * \\ O & I_{h-1} \end{smallmatrix}\right)$ (with respect to a suitable basis), and hence has order $(q^n)^{h-1}(q^n-1) = q^{N-n}(q^n-1)$ and is transitive on the vectors in $V - \mathrm{Ker} f$. Then H fixes $(q^{N-n}-1)/(q-1)$ points of $\mathbf{D}(N, n, D)$ and is transitive on the remaining $(q^N - q^{N-n})/(q-1)$ points.

Let Y denote a block of imprimitivity for the action of $A = \mathrm{Aut}\mathbf{D}$ on points such that A acts nontrivially and primitively on the corresponding block system $\Sigma = Y^A$. Then

(#) Every member of $\mathcal{C}$ is a union of members of Σ (by (3′) since Σ is a block system for G).

The group A^Σ induced by A on Σ is a primitive permutation group having a subgroup H^Σ fixing certain points and transitive on the remaining ones. All such primitive groups are known [5], and one of the following holds:

(I) H^Σ fixes exactly t members of Σ, and A^Σ is $(t+1)$-transitive;

(II) $|\Sigma| = 22, 23$ or 24, A^Σ is a Mathieu group and the members of Σ fixed by H^Σ arise from a block of the associated Steiner system;

(III) A^Σ has a normal affine subgroup $\mathrm{ASL}(m, r)$, acting in its natural 2-transitive action, for some m and some prime power r, and the members of Σ fixed by H arise from a subspace of the underlying affine space; or

(IV) $\mathrm{PSL}(m, r) \leq A^\Sigma \leq \mathrm{P\Gamma L}(m, r)$ for some m and some prime power r, where these groups act in one of their natural 2-transitive actions, and the members of Σ fixed by H arise from a subspace of the underlying projective space.

We first consider further properties of H before dealing with cases (I)–(IV) separately.

Let P denote the normal elementary abelian Sylow p-subgroup of H of order q^{N-n} (consisting of all transvections $\left(\begin{smallmatrix} 1 & * \\ O & I_{h-1} \end{smallmatrix}\right)$ with respect to a suitable basis). Then P fixes $(q^{N-n} - 1)/(q-1)$ points and acts semiregularly on the remaining ones. Moreover, P acts faithfully on Σ and P^{Σ} is semiregular on each of its nontrivial orbits. (Namely, if $g \in P - \{1\}$ fixes some $Y \in \Sigma$ then, since $p \nmid |Y|$ by (#), g fixes a point of Y, so that P also fixes that point and hence also fixes Y.)

Let S denote the subgroup of A generated by all of the conjugates of P. Let K denote the kernel of the action of A on Σ.

LEMMA 4. *(i) $S = S'$.*
(ii) If C is a clump then its pointwise stabilizer $K_{(C)}$ in K is 1.
(iii) $K \cap S \leq Z(S)$ and G centralizes K.

PROOF. (i) By (3) and [10, pp. 21–23], $S \geq G' = G''$ since $q^n > 3$ and G' is generated by the conjugates of P lying in G. Now (i) follows from the fact that S is generated by the conjugates of G'.

(ii) By (#), K is the identity on $\mathcal{C}$. If $\mathcal{F}$ is any dual clump then, by (1), each of its members contains exactly the same clumps, and no block outside $\mathcal{F}$ contains precisely these clumps. Hence, K fixes $\mathcal{F}$.

If each member of $\mathcal{F}$ does not contain C then, by (4), $(C, \mathcal{F})$ is a symmetric design, and $K_{(C)}$ acts on this design, fixing all points. Thus, $K_{(C)}$ is the identity on each dual clump none of whose blocks contain C. Dually, $K_{(C)}$ is the identity on each clump not contained in any member of any such $\mathcal{F}$. It follows that $K_{(C)} = 1$.

(iii) We claim that K normalizes H. For, if $k \in K$ then H and $H^k = k^{-1}Hk$ are the identity on any clump C in $\mathcal{C}_f$, while $H^{k\Sigma} = H^{\Sigma}$. If $H^k \neq H$ then $\langle H, H^k \rangle \cap K \neq 1$, which contradicts (ii). Thus, K normalizes H.

Clearly H normalizes K, so that $h^{-1}k^{-1}hk \in H \cap K = 1$ whenever $h \in H, k \in K$. Then H centralizes K, and hence so does each conjugate of H in A. The conjugates of H in G generate G. □

We now return to the proof of Theorem 1. Let $y = |Y|$ and let C be a clump. Then $(q^N - 1)/(q-1) = |\Sigma| y$, and y divides $|C| = (q^n - 1)/(q-1)$ by (#).

Case (I). First suppose that $h > 2$. Since H fixes exactly $(q^{N-n} - 1)/(q^n - 1)$ clumps, by (#) we have $t \geq (q^{N-n} - 1)/(q^n - 1) \geq q^n + 1 > 5$ and hence A^{Σ} contains the alternating group. Again by (#), the subgroup B of A sending $\mathcal{C}$ to itself also induces at least the alternating group on $\mathcal{C}$. If C_1 and C_2 are distinct clumps then it follows that their stabilizer in B is transitive on the remaining clumps, but this contradicts (2).

The case $N/n = h = 2$ is harder since (2) is then vaccuous and this case can actually occur. First we will consider the possibility that A^{Σ} contains the alternating group. By Lemma 4(iii), S is a central extension of that alternating group. If B denotes the subgroup of S sending $\mathcal{C}$ to itself, then $B'^{\mathcal{C}}$ is the alternating group by (#). Then B'_C acts on $\mathcal{C} - \{C\}$ as the alternating group $A_{|\mathcal{C}|-1}$ of degree $|\mathcal{C}| - 1 = q^n > |C|$. On the other hand, $B'_C/(B' \cap K)$ acts on the set of $B' \cap K$-orbits within C. Since $A_{|\mathcal{C}|-1}$ is simple it has no proper subgroup of index $< |\mathcal{C}| - 1$, so that B'_C induces on C a subgroup of $B' \cap K$. Then $|B'_C| \leq |B' \cap K| \leq |S \cap K| \leq 2$ by [7]. However, B' contains G', and G'_C induces on C a cyclic group of order $(q^n - 1)/(q-1)$. This contradiction shows that A^{Σ} does not contain the alternating group.

Nevertheless, A^{Σ} is $(t+1)$-transitive, where t is the number of members of Σ fixed by H, which in turn are determined by fixed points of H. By (#) we have $t = \{(q^{N-n} - 1)/(q-1)\}/y$, where $y = |Y|$ divides $|C| = (q^n - 1)/(q - 1)$. Moreover, $|\Sigma| = \{(q^N - 1)/(q - 1)\}/y = (q^n + 1)t$.

We will compare this information with a list of all 2-transitive groups (excluding alternating and symmetric groups) found, for example, in [5]. First of all, $t + 1 \leq 5$ in view of $(t + 1)$-transitivity, and hence $|\Sigma| = (q^n + 1)t$ cannot be of any of the following forms: 11, 12, 22, 23, 24, 176, 276, $2^{s-1}(2^s \pm 1)$ with $s \geq 3$, or a prime power. Now the aforementioned list shows that only $t = 1$ is possible. Since A^Σ is a 2-transitive group of degree $q^n + 1$, other than the alternating or symmetric group, having an abelian subgroup P^Σ of order q^n with an orbit of length q^n, the list yields $\mathrm{PSL}(2, q^n) \leq A^\Sigma \leq \mathrm{P\Gamma L}(2, q^n)$. Moreover, $y = (q^n - 1)/(q - 1)$ and $\Sigma = \mathcal{C}$.

If $\Gamma = \Gamma\mathrm{L}(2, q^n)/Z_{q-1}$ denotes the subgroup of A in (3), it follows that $A^\mathcal{C} = \Gamma^\mathcal{C} = \mathrm{P\Gamma L}(2, q^n)$. Thus, the only place A and Γ might differ is in the kernel K of the action of A on $\mathcal{C}$, so it suffices to show that $K \leq G$. Suppose that $k \in K - G$. By Lemma 4(iii), $\langle G \cap K, k\rangle$ is an abelian group acting on C, where $G \cap K$ is transitive on C. Thus, there is some $g \in G \cap K$ such that kg fixes a point of C, commutes with the transitive group $G \cap K$, and hence fixes all points of C. This contradicts Lemma 4(ii). Thus, $A = \Gamma$, as required.

Case (II). Here $q^{N-n} = |P^\Sigma| = 2^4$, the size of the complement of a block of the associated Steiner system, whereas $n|N$ and $n \geq 3$.

Case (III). We first claim that r is a power of p. For suppose not. Certainly P^Σ acts on $W = \mathbf{F}_r^m$, and its set of fixed points is a subspace U. Recall that P^Σ acts semiregularly on each of its nontrivial point-orbits, and hence on $W - U$. Since p does not divide r, P^Σ acts fixed-point-freely on W/U according to [2, p. 187], but that is impossible for a noncyclic abelian group according to [2, p. 69].

Thus, r is a power of p, which contradicts the fact that $(q^N - 1)/(q - 1) = y|\Sigma| = yr^m$.

Case (IV). Precisely as in (III) we find that r is a power of p.

We have $(q^N - 1)/(q - 1) = y(r^m - 1)/(r - 1)$, where $y|(q^n - 1)/(q - 1)$. By [12] it follows that $q^N = r^m$, so that $y = (r - 1)/(q - 1)$ and hence $r = q^j$ for some integer j. Then $j \leq n$ since $(q^j - 1)/(q - 1) = y \leq (q^n - 1)/(q - 1)$.

Now $S^\Sigma = S'^\Sigma = \mathrm{PSL}(m, q^j)$ with $N = mj$. Since $S^\Sigma \cong S/Z(S)$ by Lemma 4(iii), in view of Proposition 3 and the remark following it we have $j > 2$ and $\mathbf{D} \cong \mathbf{D}(N, j, D')$ for some difference set D' in $\mathbf{F}_{q^j}^*/\mathbf{F}_q^*$. Then $j = n$ by the hypothesized minimality of n.

Thus, $y = (q^n - 1)/(q - 1)$, $\Sigma = \mathcal{C}$, and $\mathrm{PSL}(h, q^n) \leq A^\mathcal{C} \leq \mathrm{P\Gamma L}(h, q^n)$. Now we can complete the proof exactly as in (I). □

PROOF OF THEOREM 2. (i) If $\varphi\colon \mathbf{D}(N, n, D') \to \mathbf{D}(N, n, D)$ is an isomorphism then it sends $\mathrm{Aut}\mathbf{D}(N, n, D')$ to $\mathrm{Aut}\mathbf{D}(N, n, D)$. Let Z denote the cyclic subgroup of both $\mathrm{Aut}\mathbf{D}(N, n, D)$ and $\mathrm{Aut}\mathbf{D}(N, n, D')$ induced by $\mathbf{F}_{q^N}^*/\mathbf{F}_q^*$. Then $Z^\varphi = \varphi^{-1}Z\varphi$ lies in the group $\mathrm{Aut}\mathbf{D}(N, n, D)$, described in Theorem 1, which has just one conjugacy class of cyclic subgroups of order $(q^N - 1)/(q - 1)$ (e.g., by Schur's Lemma). Thus, for some $g \in \mathrm{Aut}\mathbf{D}(N, n, D)$ we have $Z^{\varphi g} = Z$, so that φg induces an automorphism of the cyclic group Z.

If Δ and Δ' are the difference sets in Z determined by blocks X and X' of $\mathbf{D}(N, n, D)$ and $\mathbf{D}(N, n, D')$, respectively, then $\Delta'^{\varphi g}$ is the difference set in Z determined by the block $X^{\varphi g}$ of $\mathbf{D}(N, n, D)$ and hence is a translate of Δ. This means that Δ and Δ' are equivalent difference sets, so that D' is a translate of D by [1, Theorem 4] or [6, pp. 77–78]. The easy converse is also in [1, Theorem 4].

(ii) Minimality implies that $n = n'$. □

REMARKS. (1) In view of the theorems, D and the way $\mathbf{D}(N, n, D)$ was constructed from $\mathrm{PG}(h - 1, q^n)$ can be recovered from the design $\mathbf{D}(N, n, D)$. Our proof does not, however, provide a purely *geometric* means of recovery, which would be far preferable. Instead, we have used [5], which depends on very difficult group theory, and hence its use is uncomfortably reminiscent of using a cannon to kill an ant. However, we hope that knowing that these theorems are true will make it more likely that much nicer proofs can be found.

In this direction, we conjecture that, under the minimality assumption of Theorem 1, clumps are the only sets C of points of $\mathbf{D}(N, n, D)$ such that $\{C \cap X \mid X \text{ is a block} \not\supset C\}$ is the set of blocks of a symmetric design, with point set C, having the same parameters as $\mathrm{PG}(n-1, q)$. If true, this would produce a simpler proof of both theorems. (Note that the minimality assumption is needed, as otherwise $\mathrm{Aut}\mathbf{D}(N, n, D)$ would not send $\mathcal{C}$ to itself.) Is there a coding theoretic interpretation of this conjecture? Is the conjecture more approachable in the case of the classical GMW designs, where minimality is automatic and the design is built up from two projective spaces?

(2) The case $h = q = 2$ of Theorem 2 appears in [3, Theorem 3.4]. However, the proof given there assumes that any design isomorphism must send the subgroup $\mathrm{SL}(2, 2^n)$ in (3) of the automorphism group of one of the designs to the corresponding automorphism group in (3) of the other design. We have seen that this is not the case unless n is minimal in the sense of Theorem 1. It was exactly the need to make this assertion correct up to conjugacy that originally led to Theorem 1.

(3) Proposition 3 requires a comment in view of the interesting Mathematical Review (#97m:51005) of [4], which states the following: “It is shown that any design with the parameters of $P_{N-1,q}$ can be constructed by their procedure [i.e., the one in [1]] if and only if the design admits $\mathrm{GL}(m, q^n)$ for some m and n such that $N = mn$.” The review does not mention transitivity, hence also not that [4] assumes the precise action of $\mathrm{GL}(h, q^n)$. It is not at all clear whether the proposition holds as stated without the transitivity assumption: it is plausible that $\mathrm{SL}(h, q^n)$ could act on a design having these parameters (possibly not faithfully, just as in the case of $\mathbf{D}(N, n, D)$ for suitable q) and yet have many orbits, even including some fixed points. Of course, the nature of some orbits would be severely restricted by $(*)$, perhaps so much so that the proposition could be generalized to the statement in the review.

Acknowledgement

This research was supported in part by the NSF and by the Israel Institute for Advanced Studies.

References

1. B. Gordon, W. H. Mills and L. R. Welch, Some new difference sets, *Can. J. Math.*, **14** (1962), 614–625.
2. D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.
3. W.-A. Jackson, A characterization of Hadamard designs with $\mathrm{SL}(2, q)$ acting transitively, *Geom. Ded.*, **46** (1993), 197–206.
4. W.-A. Jackson and P. R. Wild, On GMW designs and cyclic Hadamard designs, *Des. Codes Cryptogr.*, **10** (1997), 185–191.
5. W. M. Kantor, Homogeneous designs and geometric lattices, *J. Comb. Theory A*, **38** (1985), 66–74.
6. A. Pott, *Finite Geometry and Character Theory*, Springer LNM 1601, 1995.
7. I. Schur, Über die Darstellung der symmetrischen und alternierenden Gruppen durch gebrochene lineare Substitutionen, *J. reine ang. Math.*, **139** (1911), 155–250.
8. G. M. Seitz, Flag–transitive subgroups of Chevalley groups, *Ann. Math.*, **97** (1973), 27–56.

9. R. Steinberg, Generators, relations and coverings of algebraic groups, II, *J. Algebra*, **71** (1981), 527–543.
10. D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann, Berlin, 1992.
11. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.
12. K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.*, **3** (1892), 265–284.

Received 20 January 2000 and accepted 15 June 2000

WILLIAM M. KANTOR
Department of Mathematics,
University of Oregon,
Eugene, OR 97403,
U.S.A.
E-mail: kantor@math.uoregon.edu