Des. Codes Cryptogr. (2008) 48:307–322
DOI 10.1007/s10623-008-9209-3

Distorting symmetric designs

Ulrich Dempwolff · William M. Kantor

Received: 17 April 2007 / Revised: 26 March 2008 / Accepted: 28 March 2008 /
Published online: 7 May 2008

Abstract A simple replacement approach is used to construct new symmetric and affine designs from projective or affine spaces. This is used to construct symmetric designs with a given automorphism group, to study GMW designs, and to construct new affine designs whose automorphism group fixes a point and has just two point- and block-orbits.

Keywords Symmetric and affine designs · Projective or affine spaces · GMW designs · Point- and block-orbits

AMS Classifications 05B05 · 05B25 · 51E05 · 05B10

1 Introduction

In this paper we present a very simple way to modify projective or affine spaces in order to produce many other symmetric or affine designs having the same parameters. This contains as very special cases constructions used in [8,9] (which are in turn based on a construction in [13]), and will be used here for several purposes. We will prove the following

Theorem 1.1 *For any finite group G and some $d < 35|G|$, for each prime power q there is a symmetric design* $\mathbf{D}$ *having the parameters of* $\mathrm{PG}(d, q)$ *such that* $\mathrm{Aut}\mathbf{D} \cong G$.

This result previously was proved in [9] under the more restrictive conditions $q \geq 3$ and (an arbitrary) $d \geq 50|G|^2$; and in [11] in greater generality when $q = 2$. The argument

Communicated by A. Pott.

U. Dempwolff
Universität Kaiserslautern, Kaiserslautern 6750, Germany
e-mail: dempwolff@mathematik.uni-kl.de

W. M. Kantor (✉)
Department of Mathematics, University of Oregon, Eugene, OR 97403, USA
e-mail: kantor@math.uoregon.edu

presented here is far simpler than in [9]. Our methods also provide information concerning GMW *designs*, an important class of difference set designs discovered and studied in [5]. Isomorphisms and automorphisms of those designs were completely dealt with in [10], using the classification of finite simple groups. Here we will provide an elementary proof of the most "natural" special case of those results:

Theorem 1.2 *Let* $K = \mathrm{GF}(q)$, F_1 *and* F_2 *be finite fields such that* $K \subset F_1, F_2 \subset \mathrm{GF}(q^d)$ *and* $[F_i : K] \geq 3$; *for* $i = 1, 2$, *let* $D_i \supset K$ *be a hyperplane of the* K*-space* F_i, *so that* D_i^*/K^* *is the standard Singer difference set in* F_i^*/K^*, *where* $D_i^* = D_i \backslash \{0\}$. *For* $i = 1, 2$, *let* $\mathbf{D}_i$ *be the GMW design having the parameters of* $\mathrm{PG}(d-1, q)$, *determined by the difference set* $D_i^{*r_i}/K^*$ *for integers* r_i *relatively prime to* $q|F_i^*|$ *such that* $1 \leq r_i < |F_i^*|$.

- (i) *If* $\mathbf{D}_1 \cong \mathbf{D}_2$ *then* $F_1 = F_2$ *and* $r_2 \equiv r_1 p^a w \,(\mathrm{mod}\, q^n - 1)$, *where* p *is the prime dividing* q *and* $w \equiv 1 (\mathrm{mod}\, (q^n - 1)/(q - 1))$.
- (ii) $\mathrm{Aut}\mathbf{D}_1 \cong \Gamma\mathrm{L}(N, F_1)/Z$, *where* $q^d = |F_1|^N$ *and* Z *consists of the scalar transformations* $v \to kv$ *with* $k \in K^*$.

The construction of these designs $\mathbf{D}_i$ is recalled in Sect. 4. The aforementioned result in [10] deals with difference sets more general than $D_i^{*r_i}/K^*$ (the design corresponding to the latter difference set is isomorphic to the projective space over K determined by F_i).

Much of this paper—and in particular, the proofs of the preceding theorems—uses *lines* of designs [3,4]. If x and y are distinct points of a design, the *line* xy is the intersection of all blocks containing x and y; two points are on exactly one line.

Throughout this paper, q will be a prime power, $K = \mathrm{GF}(q) \subset F = \mathrm{GF}(q^h)$ where $h \geq 3$, and d and N will be integers > 1. Also, D_0 is the kernel of the trace map $F \to K$, so that D_0^*/K^* is the standard Singer difference set in F^*/K^*. In Sect. 7 we prove the following

Theorem 1.3 *Let* $N > 1$ *be an integer, and let* $q > 2$ *be a prime power. If* r *is an integer such that* $1 < r < q^h - 1$ *and* $(r, q(q^h - 1)) = 1$, *then there is an affine design* $\mathbf{A}(r)$ *with the following properties*:

- (i) *Its parameters are those of the classical affine design* $\mathrm{AG}(hN, q)$ *but it is not isomorphic to that design.*
- (ii) *There is a point* 0 *such that all lines through* 0 *have size* q.
- (iii) *The incidence structure of lines and blocks containing* 0 *is isomorphic to the GMW design obtained using the difference set* $D_0^{*^r}/K^*$ *of* F^*/K^*.
- (iv) *There is a cyclic automorphism group* A *of order* $q^{hN} - 1$ *fixing* 0 *and acting regularly on the points* $\neq 0$ *of* $\mathbf{A}(r)$, *on the blocks containing* 0, *and on the blocks not containing* 0.
- (v) $\mathrm{Aut}\mathbf{A}(r) \cong \Gamma\mathrm{L}(N, q^h)$.
- (vi) $\mathbf{A}(r_1) \cong \mathbf{A}(r_2)$ *if and only if* $r_2 = cr_1$, *where* c *is a power of the prime dividing* q.

In view of (iv), $\mathbf{A}(r)$ can be described using a relative difference set in A with distinguished subgroup K^* (cf. Remark 7.6).

In Sect. 2 we present our perturbations of projective spaces, and study their lines in Sect. 3. This is used in Sect. 4 for our elementary proof of Theorem 1.2. Theorem 1.1 is proved in Sect. 5. The affine versions of these results are in Sects. 6, 7 and 8: Sect. 6 discusses perturbations of affine spaces, Sect. 7 contains the proof of Theorem 1.3, and Sect. 8 contains an affine design version of Theorem 1.1. We emphasize that all of the proofs in this paper are elementary. In particular, the proof we give for Theorem 1.2 is far easier to understand than the argument in [10].

2 Perturbations of projective spaces

Suppose that Σ is a partition of the point set of $\mathbf{P} = \mathrm{PG}(d, q)$ by subspaces. For each point or line $X \in \Sigma$ let α_X denote the identity map on X; for any other $X \in \Sigma$ let α_X be a bijection from the hyperplanes of X to the blocks of a symmetric design $\mathbf{D}_X$ having point set X and the same parameters as $\mathrm{PG}(X)$. Also write $X^{\alpha_X} = X$. Define an incidence structure $\mathbf{P}^\alpha$ by using

$$\begin{array}{ll} \textit{points}: & \text{the points of } \mathbf{P} \\ \textit{blocks}: & H^\alpha := \bigcup_{X \in \Sigma} (H \cap X)^{\alpha_X} \text{ for each hyperplane } H \text{ of } \mathbf{P}. \end{array} \tag{2.1}$$

Theorem 2.2 $\mathbf{P}^\alpha$ *is a symmetric design having the same parameters as* $\mathbf{P}$.

Proof For any hyperplanes H, H' of $\mathbf{P}$,

$$\begin{aligned} |H^\alpha \cap H'^\alpha| &= \sum_X |(H \cap X)^{\alpha_X} \cap (H' \cap X)^{\alpha_X}| \\ &= \sum_X |(H \cap X) \cap (H' \cap X)| = |H \cap H'|. \end{aligned} \tag{2.3}$$

(We have used the fact that $(H \cap X)^{\alpha_X}$ and $(H' \cap X)^{\alpha_X}$ are distinct blocks of $\mathbf{D}_X$ if and only if $H \cap X$ and $H' \cap X$ are distinct hyperplanes of X.) □

We will write $x \, \mathrm{I} \, H$ if $x \in H^\alpha$. Note that a special case of this construction was used in [8,9].

Remark 2.4 If $X \in \Sigma$ is not a point or line, then $\{H^\alpha \cap X \mid H^\alpha \not\supseteq X\}$ is the set of blocks of $\mathbf{D}_X$.

Variations:

1. We could have used *any* symmetric design $\mathbf{P}$ having a partition into suitable subsets that inherit the structure of symmetric designs. The simplest example of this uses a good block of a symmetric design $\mathbf{P}$ along with the individual points in its complement, as in [8,9].
2. We did not quite need a partition Σ. Instead we could have used a family Σ of subspaces whose union is all points and such that $X \cap Y = W$ is the same subspace for all distinct $X, Y \in \Sigma$. If the α_X are required to send hyperplanes on x to blocks on x for each point x in W, then we obtain a symmetric design as before. While this seems a bit artificial, in Sect. 6 we will see that a similar idea produces Theorem 1.3.

3 Lines and colines

If X and Y are distinct blocks of a symmetric design, the *coline* $[X, Y]$ is the set of all blocks containing $X \cap Y$; two blocks are in exactly one coline. In $\mathrm{PG}(d, q)$, colines are just the duals of lines; all lines and colines have size $q + 1 = (v - \lambda)/(k - \lambda)$, which is the maximum possible size for any symmetric design [4].

We now study line sizes in the designs $\mathbf{P}^\alpha$ constructed in the preceding section.

Proposition 3.1 *Let* $X \in \Sigma$. *The line of* $\mathbf{P}^\alpha$ *determined by two points of* X *is contained in* X. *Moreover, if* $\mathbf{D}_X$ *is a projective space of dimension at least* 2, *then in* $\mathbf{P}^\alpha$ *each line containing two points of* X *has size* $q + 1$.

Proof For the first assertion, observe that X is the intersection of the hyperplanes of $\mathbf{P}$ that contain X, and hence also of some of the blocks of $\mathbf{P}^{\alpha}$. For the second assertion, observe that the blocks of $\mathbf{P}^{\alpha}$ induce on X the projective space $\mathbf{D}_X$ by Remark 2.4. □

Proposition 3.2 *Let $X, Y \in \Sigma$ be distinct, and $x \in X$, $y \in Y$. If there is a third point on the line xy of $\mathbf{P}^{\alpha}$, then the following condition holds in X and $\mathbf{D}_X$:*

$$\begin{array}{l}\text{For any distinct hyperplanes } A_1, A_2, A_3 \text{ in a coline of } X,\\ x \in A_1^{\alpha_X} \cap A_2^{\alpha_X} \Rightarrow x \in A_3^{\alpha_X}.\end{array} \tag{3.3}$$

Proof Let $z \neq x, y$ be a point of xy, and let $z \in Z \in \Sigma$. Then $Z \neq X, Y$ by Proposition 3.1.

Let H_1 be a hyperplane of $\mathbf{P}$ such that $H_1 \cap X = A_1$ and $H_1 \supseteq Y$. Let H_2 be a hyperplane of $\mathbf{P}$ such that $H_2 \cap X = A_2$ and $H_2 \supseteq Z$. Then $H_3 = \langle H_1 \cap H_2, A_3\rangle$ is a hyperplane of $\mathbf{P}$, since

$$(H_1 \cap H_2) \cap A_3 = (H_1 \cap X \cap A_3) \cap (H_2 \cap X \cap A_3) = (A_1 \cap A_3) \cap (A_2 \cap A_3) = A_1 \cap A_2$$

is a hyperplane of A_3. Note that $H_3 \cap X = A_3$ (as otherwise $H_3 \supseteq \langle X, H_1 \cap H_2\rangle \supseteq \langle A_1, H_1 \cap H_2, A_2, H_1 \cap H_2\rangle = \langle H_1, H_2\rangle$).

By hypothesis, $x \in (H_1 \cap X)^{\alpha_X}$, while $y \in (H_1 \cap Y)^{\alpha_Y}$ trivially, so that $x, y \mathrel{\mathrm{I}} H_1$. Then also $z \mathrel{\mathrm{I}} H_1$, and hence $z \in (H_1 \cap Z)^{\alpha_Z}$. Consequently, since $H_2 \supseteq Z$,

$$z \in (H_1 \cap Z)^{\alpha_Z} = (H_1 \cap (H_2 \cap Z))^{\alpha_Z} = (H_3 \cap (H_2 \cap Z))^{\alpha_Z} = (H_3 \cap Z)^{\alpha_Z}.$$

Hence, $z \mathrel{\mathrm{I}} H_3$. Similarly, $y \mathrel{\mathrm{I}} H_3$. Thus, $x \mathrel{\mathrm{I}} H_3$, so that $x \in (H_3 \cap X)^{\alpha_X} = A_3^{\alpha_X}$, as asserted. □

Remark Here (3.3) is a property of a *single* subspace X and a *single* bijection α_X. It can be viewed as a "local collinearity condition" on the dual space X°: for any three collinear points of X^*, if the images of two of them are on the "hyperplane" x then so is the image of the third. As in [9, Lemma 4.1], this suggests the

Corollary 3.4 *In the situation of the preceding proposition, the following condition holds:*

(*) α_X^{-1} *maps the set of blocks of $\mathbf{D}_X$ containing x to the set of hyperplanes of X containing a uniquely determined point of X.*

Proof Let S denote the set of α_X^{-1}-images in X of the blocks of $\mathbf{D}_X$ containing x. We claim that S is closed under colines: let A_1, A_2, A_3 be distinct members of a coline of X, where $A_1, A_2 \in S$. Then $x \in A_1^{\alpha_X} \cap A_2^{\alpha_X}$, and hence $x \in A_3^{\alpha_X}$ by the proposition, so that $A_3 \in S$, as required.

Thus, S is a subspace of the dual space of X, and in view of its size it is the set of hyperplanes on a point of X. □

The preceding results can be used to determine the isomorphisms among a large class of the designs $\mathbf{P}^{\alpha}$. Later we will use similar ideas. However, the total number of symmetric designs obtainable by this approach is far inferior to the number already known [8,9].

Remark 3.5 (1) Any permutation β_X of the points of X induces a permutation β_X of all subsets of X, and hence produces an isomorphism $\mathrm{PG}(X) \to \mathrm{PG}(X)^{\beta_X}$. In particular, (3.3) holds using β_X and $\mathbf{D}_X = \mathrm{PG}(X)^{\beta_X}$.

For example, view $X = Fv$ using a difference set: let $K = \mathrm{GF}(q)$, $F = \mathrm{GF}(q^h)$, $h \geq 3$; as usual, let D_0 be the kernel of the trace map $F \to K$, so that D_0^*/K^* is the usual Singer difference set in F^*/K^*. Let r be an integer such that $1 < r < |F^*|$ and $(r, q|F^*|) = 1$, so that $D_X = D_0^r$ projects onto another difference set in F^*/K^* *not equivalent to* D_0^*/K^*. Then $\beta_X : av \mapsto a^r v, a \in F$, sends $aD_0v \mapsto (aD_0)^r v = a^r D_X v$ and induces an isomorphism from $\mathrm{PG}(X)$ to another projective space $\mathbf{D}_X$. These projective spaces are isomorphic but are not equal, and 3.3 holds for the map β_X.

(2) In the next section we will use a variation on β_X in order to study GMW designs. Namely, if D_X and $\mathbf{D}_X$ are as above, consider the bijection $\alpha_X : aD_0v \mapsto aD_Xv, a \in F$, from the hyperplanes of $\mathrm{PG}(X)$ to those of $\mathbf{D}_X$.

Note that *this bijection does not arise from an isomorphism of projective spaces.* For otherwise, if $\{a_i^{-1}D_0v \mid a_i \in F^*, 1 \leq i \leq (q^{h-1} - 1)/(q - 1)\}$ be the set of hyperplanes of $X = Fv$ containing v, then $a_i \in D_0$ and $\cap_i (a_i^{-1}D_0v)^{\alpha_X}$ is a point Kav for some $a \in F^*$. Thus, for each $k \in K$ and each i we have $kav \in (a_i^{-1}D_0v)^{\alpha_X} = a_i^{-1}D_Xv$, and hence $ka_i \in a^{-1}D_X$. Then $D_0 \subseteq a^{-1}D_X$. This contradicts the fact that D_X^*/K^* and D_0^*/K^* are inequivalent difference sets.

This can be further clarified by observing that $\alpha_X\beta_X^{-1}$ maps $\mathrm{PG}(X)$ to itself sending $D_0a^r \mapsto D_0a$. In view of our choice of r, the latter map is not induced by a collineation of $\mathrm{PG}(X)$.

4 GMW designs

GMW designs are symmetric designs that arise from cyclic difference sets and have the same parameters as projective spaces [5]. There are various constructions; we will use the one in [6,7,9], generalized somewhat.

Let $N \geq 2$, and let Σ denote the set of 1-dimensional subspaces of the F-space $V_F = F^N$.

Let K, F, and D_0 be as in the Introduction, so that D_0 is the kernel of the trace map $T : F \to K$. In each $X \in \Sigma$ choose a nonzero vector v_X; also choose a subset $D_X = KD_X$ of F such that D_X^*/K^* is a difference set in F^*/K^*, with corresponding difference set design $\mathbf{D}_X$. We will consider the symmetric design $\mathbf{P}^\alpha$, where

$$\alpha_X : aD_0v_X \mapsto aD_Xv_X \quad \text{for all } a \in F^* \tag{4.1}$$

for each $X \in \Sigma$. Note that this is well-defined since $KD_0 = D_0$ and $KD_X = D_X$.

We also define another incidence structure $\mathbf{D}$, whose points are the 1-spaces Kv when V_F is viewed as a K-space (i.e., these are the points of $\mathbf{P} = \mathrm{PG}(hN - 1, q)$), whose blocks are the 1-spaces $K\lambda$ with nonzero λ in the dual space V_F° of V_F, and with incidence given by

$$Kv\,\mathrm{I}'K\lambda \iff \lambda(v) \in D_{Fv}. \tag{4.2}$$

Proposition 4.3 $\mathbf{P}^\alpha \cong \mathbf{D}$.

Proof Our isomorphism will be the identity on points and send the block H^α of $\mathbf{P}^\alpha$ to the block $K\lambda$ of $\mathbf{D}$, where $H = \mathrm{Ker}(Tk\lambda)$ for all $k \in K^*$ (here $Tk\lambda(v) = T(k\lambda(v))$ for $v \in V_F$). It suffices to show that incidence is preserved.

Consider incidences involving the points of $X = Fv_X \in \Sigma$. If $\lambda(v_X) = 0$ then $X \subseteq \mathrm{Ker}(T\lambda)$, and all points of X are incident with $K\lambda$ in $\mathbf{P}^\alpha$ and with $H = \mathrm{Ker}(T\lambda)$ in $\mathbf{D}$.

Suppose that $\lambda(v_X) \neq 0$. Let $a \in F^*$. In $\mathbf{P}$ we have

$$Kav_X \subset \mathrm{Ker}(T\lambda) \iff T(\lambda(av_X)) = 0 \iff a \in \lambda(v_X)^{-1}D_0. \tag{4.4}$$

Hence, by (2.1), in $\mathbf{P}^\alpha$ we have $Kav_X \,\mathrm{I}\, H \iff Kav_X \subseteq (\lambda(v_X)^{-1}D_0v_X)^{\alpha_X} = \lambda(v_X)^{-1} D_Xv_X$. On the other hand, in $\mathbf{D}$ we have $Kav_X \,\mathrm{I}'K\lambda \iff T(\lambda(av_X)) \in D_{Fv_X} \iff a \in \lambda(v_X)^{-1}D_X$. □

Definition If all D_X are equal, then $\mathbf{D}$ is a GMW *design* [5], and the above description is the same as the one in [6,7,10]. In this case, (2.1) and (4.1) imply that every element of $\Gamma\mathrm{L}(V_F)$ acts as an automorphism of $\mathbf{D}$.

Proposition 4.5 *Assume that X and Y are distinct members of Σ, and that D_X^*/K^* is not equivalent to D_0^*/K^*. If $x \in X$ and $y \in Y$ then the line xy of $\mathbf{P}^\alpha$ has size 2.*

First proof Otherwise, according to Corollary 3.4, there is a point x' of X such that α_X maps the set of hyperplanes of X on x' to the set of blocks of $\mathbf{D}_X$ on x. Since α_X commutes with the action of F^* (by (4.1)), it follows that this holds for *all* $x' \in X$. Consequently, α_X arises from an isomorphism of projective spaces, which is not the case by Remark 3.5(2). □

Second, more direct proof We will use the description (4.2). Let $x = Kv$ and $y = Kw$, and suppose that xy contains a third point $z = Ku$. Let $z \in Z = Fu$. We first show that $Z \subset X + Y$. For if not, then $Z \cap (X + Y) = 0$ in view of the definition of Σ, so there is some $\lambda \in V^*$ that vanishes on $X + Y$ such that $\lambda(u) \notin D_Z$. By (4.2), x and y are on $K\lambda$ but z is not, which is a contradiction.

Thus, $u = av + bw$ for some $a, b \in F$. By Proposition 3.1, $a, b \neq 0$.

Pick $\lambda, \mu \in V_F^\circ$ such that $\lambda(v) = 1, \lambda(w) = 0$ and $\mu(v) = 0, \mu(w) = 1$. Let $c, d \in F$. By (4.2),

$$Kv, Kw \,\mathrm{I}'K(c\lambda + d\mu) \iff c = (c\lambda + d\mu)(v) \in D_X,\ d = (c\lambda + d\mu)(w) \in D_Y.$$

Hence, since $z = K(av + bw)$ is in the line xy, whenever $c \in D_X$ and $d \in D_Y$, we have $ac + bd = (c\lambda + d\mu)(av + bw) \in D_Z$ by (4.2), so that $aD_X + bD_Y \subseteq D_Z$.

Since $0 \in D_X, D_Y$, it follows that $aD_X \subseteq D_Z$ and $bD_Y \subseteq D_Z$ with $a, b \neq 0$, and hence $aD_X = D_Z = bD_Y$ as these all have the same size. Then $aD_X + aD_X \subseteq aD_X$. Since $KD_X = D_X$, this means that D_X is a K-subspace of X, and hence is a hyperplane in view of its size. This contradicts the fact that D_X^*/K^* is not equivalent to D_0^*/K^*. □

In the situation of Propositions 3.1 and 4.5, the set Σ is uniquely determined by the design $\mathbf{D}$: for two different points x and y, the line of $\mathbf{D}$ through them has size $q + 1$ if they lie in the same member Fv of Σ and has size 2 otherwise. In other words, Σ can be reconstructed from $\mathbf{D}$. We now show that the same is true for the underlying projective space $\mathbf{P}$, provided that we further restrict $\mathbf{D}$. Geometrically reconstructing $\mathbf{P}$ will easily yield Theorem 1.2.

Proposition 4.6 *Assume that all D_X are the same set $D = D_0^r$, where $1 < r < |F|$, $(r, |F|) = 1$ and D^*/K^* is not equivalent to D_0^*/K^*. Then the projective space $\mathbf{P}$ can be canonically reconstructed from the symmetric design $\mathbf{D}$.*

Proof We just saw that Σ is uniquely determined by $\mathbf{D}$. Since lines will not suffice for the proof, we introduce a technical variation of the notion of line. For any distinct points x and

y, let $x \in X \in \Sigma$ and $y \in Y \in \Sigma$, and define the *pseudoline* $((x, y))$ of $\mathbf{D}$ as follows, where H ranges over hyperplanes of $\mathbf{P}$:

$$((x, y)) = \{z \mid \ if\ x, y \mathrm{I} H = \mathrm{Ker}(\lambda),\ and\ either \\ X \subseteq \mathrm{Ker}(\lambda)\ or\ Y \subseteq \mathrm{Ker}(\lambda),\ then\ z \mathrm{I} H\}.$$

Claim *Each pseudoline $((x, y))$, with $x \in X$ and $y \in Y$ for different $X, Y \in \Sigma$, is just the set of points of the line $x + y$ of $\mathbf{P}$ determined by x and y.*

For, let $x = Ku$, $y = Kv$. Then all points of $((x, y))$ are contained in all $K\lambda$ such that $\lambda(u) = \lambda(v) = 0$, so that $((x, y)) \subseteq X + Y$. Let $z = K(au + bv)$ for some $a, b \in F^*$. Then $z \in ((x, y))$ if and only if the following holds: if $\lambda(u) \in D$, $\lambda(v) \in D$ and $\lambda(u)\lambda(v) = 0$, then $\lambda(au + bv) \in D$.

Assume that $\lambda(u) \in D$, $\lambda(v) \in D$ and $\lambda(u)\lambda(v) = 0$. If $a, b \in K$ then $\lambda(au + bv) = a\lambda(u) + b\lambda(v) = b\lambda(u)$ or $a\lambda(v)$ is in D, so that $K(au + bv) \in ((x, y))$.

Now consider $z = K(au + bv) \in ((x, y))$ and suppose that $a \notin K$. Choose λ such that $\lambda(u) \neq 0 = \lambda(v)$. Then for each $c \in D$ we have $c\lambda(u) \in D$ and $c\lambda(v) = 0$, so that $a[c\lambda(u)] = [c\lambda](au + bv) \in D$ since $z \in ((x, y))$. Then $aD \subseteq D$. Since D^*/K^* is a difference set, this contradicts the fact that $a \notin K$ and proves our Claim.

Each subspace of $\mathbf{P}$ not contained in any member of Σ is the union of those of its lines not contained in any member of Σ, and hence is determined from $\mathbf{D}$ in view of the above Claim. Moreover, if x_1 and x_2 are distinct points of $X \in \Sigma$, and if $y \in Y \in \Sigma$ with $X \neq Y$, then the projective line $x_1 + x_2$ is just $[((x_1, y)), ((x_2, y))] \cap X$. Consequently, all subspaces of members of Σ are uniquely determined from $\mathbf{D}$. Hence, so is $\mathbf{P}$. □

Proof of Theorem 1.2 We have seen that $\mathbf{P}$ and Σ_i are uniquely determined by $\mathbf{D}_i$. Thus, $|F_1| = |F_2|$, and we may assume that $\Sigma = \Sigma_i$ is the same for both designs $\mathbf{D}_i$. In particular, $F_1 = F_2$. (N.B.—The fact that $|F_1| = |F_2|$ follows more directly by considering the parameters of the $\mathbf{D}_i$. However, this does not give us information useful for (i) and (ii).)

Let $\hat{\Sigma}$ denote the set of K-subspaces of V projecting onto members of Σ. Then the set-stabilizer of $\hat{\Sigma}$ in $\Gamma\mathrm{L}(V)$ is $\Gamma\mathrm{L}(N, F_1)$ (since $\{\hat{X} + v \mid \hat{X} \in \hat{\Sigma}, v \in V\}$ is the set of lines of $\mathrm{AG}(N, F_1)$). It follows that $\mathrm{Aut}\mathbf{D}_1 \leq \Gamma\mathrm{L}(N, F_1)/Z$, while we have already noted that $\Gamma\mathrm{L}(N, F_1)/Z$ acts on $\mathbf{D}_1$ (cf. [6,7,10]). This proves (ii).

For (i), since $\mathbf{D}_i$ uniquely determines $\mathbf{P}$ and Σ, any isomorphism $\varphi\colon \mathbf{D}_1 \to \mathbf{D}_2$ acts on both $\mathbf{P}$ and Σ.

Let A denote the cyclic subgroup of both $\mathrm{Aut}\mathbf{D}_1$ and $\mathrm{Aut}\mathbf{D}_2$ induced by $\mathrm{GF}(q^d)^*/K^*$. Then $A^\varphi = \varphi^{-1}A\varphi$ lies in $\mathrm{Aut}\mathbf{D}_2$, which has just one conjugacy class of cyclic subgroups of order $(q^N - 1)/(q - 1)$ (e.g., by Schur's Lemma). Thus, $A^{\varphi g} = A$ for some $g \in \mathrm{Aut}\mathbf{D}_2$.

Then φg normalizes the subgroup F^*/K^* of A. Since φg sends blocks of $\mathbf{D}_1$ to blocks fof $\mathbf{D}_2$ it sends D_1 to D_2, and hence induces an equivalence between the difference sets D_1 and D_2. Thus, (i) holds [10, Theorem 4; 12, pp. 77–78]. □

Remark When $N > 2$ we could have sidestepped Proposition 4.6 and proceeded as in [10]: There is a natural structure of projective space induced by $\mathbf{D}_i$ on Σ, and hence any isomorphism $\mathbf{D}_1 \to \mathbf{D}_2$ induces a collineation of that space. However, the proof of Proposition 4.6 is no more difficult than what is needed in this approach, and that proposition is slightly more general (the case $N = 2$ is dealt with group theoretically in [10, pp. 66–67]). Moreover, that proposition gives a rather strong form of an answer to a question appearing in [10, pp. 67–68], at least in the case of the GMW designs $\mathbf{D}$ it deals with: it provides *a purely geometric way to reconstruct the projective space* $\mathbf{P}$ *from* $\mathbf{D}$.

5 Proof of Theorem 1.1

Once again fix finite fields $F \supset K$ with $[F:K] \geq 5$; let D_0 be as before, and let ω denote a generator of F^*.

Fix an integer $n \geq 3$. Let G be a finite group and Γ a simple, undirected, connected graph on $\{1, \ldots, n\}$ such that $\mathrm{Aut}\Gamma$ is isomorphic to G and is not vertex-transitive, and moreover such that Γ has more than n edges.

Let V_F be an $(n+1)$-dimensional vector space over F, with basis $v_\sharp, v_1, \ldots, v_n$ and corresponding dual basis $\lambda_\sharp, \lambda_1, \ldots, \lambda_n \in V_F^\circ$. As in Sect. 4, we will need to consider the vector space $V = V_K$ as well.

We will use five subsets $D_\sharp, D_1, D_2, D_3, D_\infty$ of F, where, for each $m \in \{\sharp, 1, 2, 3, \infty\}$,

(a) $K \subseteq D_m \subseteq F$ and $K D_m = D_m$,
(b) D_m^*/K^* is a difference set in F^*/K^* with associated design isomorphic to $\mathrm{PG}(F_K)$,
(c) the five difference sets D_m^*/K^* are pairwise inequivalent, and
(d) no difference set D_m^*/K^* is equivalent D_0^*/K^*.

Example Let $\alpha_\sharp, \alpha_1, \alpha_2, \alpha_3, \alpha_\infty : F^* \to F^*$ represent five different, nontrivial cosets of $(\mathrm{Aut}\, F) \cdot \{\beta \in \mathrm{Aut}\, F^* \mid \beta = 1 \text{ on } F^*/K^*\}$ in $\mathrm{Aut}\, F^*$; extend these to F by sending $0 \mapsto 0$. Then the sets $D_m = D_0^{\alpha_m}$ satisfy (a-d).

Each point of $\mathrm{PG}(V_F)$ is a set of points of $\mathrm{PG}(V_K)$, called a *clump* in [10]; the set of clumps is precisely the set Σ used in Sect. 4. Dually, each point of $\mathrm{PG}(V_F^\circ)$ is a set of points of $\mathrm{PG}(V_K^\circ)$, called a *coclump*.

Let $\Lambda := \mathrm{PG}(V_F^\circ) \backslash \{F\lambda_\sharp\}$. For each $F\lambda \in \Lambda$, define $D_\lambda \subset F$ as follows (whenever $1 \leq i, j \leq n$):

(1) $D_{\lambda_\sharp+\lambda_i} = D_\sharp$ for each i in the shortest G-orbit on $\{1, \ldots, n\}$,
(2) $D_{\lambda_i} = D_1$,
(3) $D_{\lambda_i+\lambda_j} = D_2$ if ij is an edge of Γ,
(4) $D_{\omega\lambda_i+\lambda_j} = D_{\lambda_i+\omega\lambda_j} = D_3$ if ij is an edge of Γ, and
(5) $D_\lambda = D_\infty$ for all other $F\lambda \in \Lambda$.

For convenience we say that $F\lambda$ has *color* D_m iff $D_\lambda = D_m$.

We need one further design: let $\mathbf{D}_\sharp$ be a symmetric design having the same parameters as $\mathrm{PG}(F_K)$ but not admitting a nontrivial semiregular automorphism. Such a design $\mathbf{D}_\sharp$ is known to exist. (For example, this follows from [9, Corollary 3.5(i)]: since $[F:K] \geq 4$ there is such a design in which some block is fixed by all automorphisms. We note that the argument used in that Corollary is just an elementary and standard use of lines of the designs obtained in an elementary construction of Shrikhande [13].) We assume that the points of $\mathbf{D}_\sharp$ are the points of $\mathrm{PG}(F_K)$, and that incidence in $\mathbf{D}_\sharp$ is just inclusion.

Let ρ be an arbitrary bijection from the hyperplanes of $\mathrm{PG}(F_K)$ to the blocks of $\mathbf{D}_\sharp$. This determines a map from the hyperplanes of the K-space F to the blocks of $\mathbf{D}_\sharp$; we also call this map ρ.

Define an incidence structure $\mathbf{D}$ by taking as points and blocks the points Kv and hyperplanes $K\lambda$ of $\mathrm{PG}(V_K)$, defining incidence $Kv \,\mathrm{I}\, K\lambda$ (or "Kv is on $K\lambda$") if and only if one of the following occurs (for some $c \in F^*$):

$$K\lambda \not\subseteq F\lambda_\sharp \text{ and } \lambda(v) \in D_\lambda \text{ or}$$
$$K\lambda = Kc\lambda_\sharp \text{ and } \lambda_\sharp(v) \in (D_0c^{-1})^\rho. \tag{5.1}$$

In particular, $Kc\lambda$ *is on all points in* $\ker\lambda$ *for each* λ.

In a series of lemmas we will prove that

Theorem 5.2 $\mathrm{Aut}\mathbf{D} \cong G$.

Lemma 5.3

(a) $\mathbf{D}$ *is a symmetric design.*
(b) *The coline determined by two blocks of* $F\lambda$ *lies in* $F\lambda$. *If* $F\lambda \neq F\lambda_\sharp$ *then each such coline has size* $q + 1$.

Proof

(a) For any $X = Fv$ and any hyperplane $H = K\lambda$ of V define $\alpha_X : X \to X$ by

$$(X \cap H)^{\alpha_X} = \{Kcv \subseteq X \mid c \in F^* \text{ and } Kcv \,\mathrm{I}\, K\lambda\}.$$

Then $\mathbf{D} \cong \mathbf{P}^\alpha$ as in the proof of Proposition 4.3.
(b) This is immediate by the dual of Proposition 3.1. □

Lemma 5.4 *Colines determined by blocks from different coclumps contain only two blocks.*

Proof This follows exactly as in (the dual of) the first proof of Proposition 4.5 (since each coline not inside $F\lambda_\sharp$ meets some coclump $\neq F\lambda_\sharp$). However, for completeness we will imitate the (dual of the) simpler second proof of that proposition.

Let $F\lambda \neq F\mu$, and consider a block $K\tau \neq K\lambda, K\mu$ in the coline $[K\lambda, K\mu]$. As in the aforementioned proof, $K\tau \subseteq F\lambda + F\mu$, and hence $\tau = a\lambda + b\mu$ for some $a, b \in F$.

Assume first that $\mu = c\lambda_\sharp$ with $c \in F^*$. Choose any $v, w \in V$ such that $\lambda(v) = \lambda_\sharp(w) = 1$ and $\lambda(w) = \lambda_\sharp(v) = 0$. If $x, y \in F$ then $K(xv+yw)\,\mathrm{I}\,K\lambda, K\mu$ iff $x = \lambda(xv+yw) \in D_\lambda$ and $Ky = K\lambda_\sharp(xv+yw) \subseteq (c^{-1}D_0)^\rho$. The latter conditions must imply that $K(xv+yw)\,\mathrm{I}\,K\tau$, and hence that $\tau(xv + yw) \in D_\tau$. Thus, $aD_\lambda + b(c^{-1}D_0)^\rho \subseteq D_\tau$. We have $ab \neq 0$ by Lemma 5.3(b), so that $aD_\lambda = b(c^{-1}D_0)^\rho = D_\tau$. This implies that $D_\tau + D_\tau \subseteq D_\tau$, which contradicts condition (d).

Assume next that $F\lambda_\sharp \neq F\lambda, F\mu$. The previous paragraph shows that $F\tau \neq F\lambda_\sharp$. This time choose $v, w \in V$ with $\lambda(v) = \mu(w) = 1$ and $\lambda(w) = \mu(v) = 0$. As above we obtain $K(xv + yw)\,\mathrm{I}\,K\lambda, K\mu$ iff $x = \lambda(xv + yw) \in D_\lambda$ and $y = \mu(xv + yw) \subseteq D_\mu$, in which case $\tau(xv + yw) \in D_\tau$ and hence $aD_\lambda + bD_\mu \subseteq D_\tau$. This produces the same contradiction as before. □

Lemma 5.5 *Every automorphism of* $\mathbf{D}$ *permutes the clumps, permutes the coclumps, sends* $F\lambda_\sharp$ *to itself, and induces a collineation of* $\mathrm{PG}(V_F)$.

Proof Lemmas 5.3 and 5.4 characterize all coclumps in Λ; hence also $F\lambda_\sharp$ is determined as the complement of their union. The clump Fv containing the point Kv is determined as the intersection of those coclumps all of whose members are on Kv. (Those are precisely the coclumps $F\lambda$ for which $\lambda(v) = 0$.) This determines all clumps, i.e., all points of $\mathrm{PG}(V_F)$. In particular, every automorphism of $\mathbf{D}$ induces a collineation of $\mathrm{PG}(V_F)$.

By Remark 2.4, $\mathbf{D}$ induces difference set designs on all $F\lambda \neq F\lambda_\sharp$, but not on $F\lambda_\sharp$ in view of the choice of $\mathbf{D}_\sharp$. □

Lemma 5.6 *Every automorphism of* **D** *preserves the colors of coclumps.*

Proof We call a triple $(K\lambda, K\mu, Fv)$ consisting of two blocks and a clump *admissible* if $F\lambda, F\mu, F\lambda_\sharp$ are distinct, $\lambda(v) \neq 0$, $\mu(v) \neq 0$, and $\{x \in Fv \mid x \, \mathrm{I} \, K\lambda\} = \{x \in Fv \mid x \, \mathrm{I} \, K\mu\}$. Note that

$$\textit{A triple } (K\lambda, K\mu, Fv) \textit{ is admissible iff } D_\lambda = D_\mu \textit{ and } K\lambda(v) = K\mu(v). \tag{5.7}$$

For, if $a = \lambda(v)$, $b = \mu(v)$ and $c \in F^*$, then admissibility states that $Kcv \, \mathrm{I} \, K\lambda \iff Kcv \, \mathrm{I} \, K\mu$; by (5.1) this occurs iff $ca \in D_\lambda \iff cb \in D_\mu$; and this occurs iff $D_\lambda = D_\mu$ and $ba^{-1} D_\lambda = D_\lambda$, in which case $ba^{-1} = d_1^{-1} d_2$ has $|D_\lambda| - 1$ solutions $d_1, d_2 \in D_\lambda$, and hence $ba^{-1} \in K$, as asserted.

Claim *If* $F\lambda$ *has color* D_m*, then* $K\lambda$ *is in precisely*

$$(c_m - 1) \cdot \frac{q^h - 1}{q - 1} \cdot (q - 1) \cdot (q^h)^{n-1} \tag{5.8}$$

admissible triples, where c_m *is the number of coclumps of color* D_m.

To prove this, we consider any block $K\mu$ with corresponding coclump $F\mu \neq F\lambda$ of color $D_\mu = D_\lambda$ (cf. (5.7)), and count the number of admissible triples $(K\lambda, K\mu, Fv)$. Choose $u, w \in V$ such that $\lambda(u) = \mu(w) = 1$ and $\lambda(w) = \mu(u) = 0$, so that $V = Fu \oplus Fw \oplus [\ker(\lambda) \cap \ker(\mu)]$. Write $v = au + bw + z$ for some $a, b \in F^*$ and $z \in \ker \lambda \cap \ker \mu$. Then $(K\lambda, K\mu, Fv)$ is admissible $\iff \lambda(au + bw + z)^{-1} \mu(au + bw + z) \in K \iff a^{-1} b \in K \iff Fv = F(u + kw + y)$ for uniquely determined $k \in K^*$, $y \in \ker(\lambda) \cap \ker(\mu)$. Since there are $c_m - 1$ choices for $F\mu$ and $(q^h - 1)/(q - 1)$ choices for $K\mu$ inside $F\mu$, and $\dim[\ker(\lambda) \cap \ker(\mu)] = n - 1$, this proves (5.8).

By conditions (1–5) in our construction of **D**, $c_\sharp < c_1 < c_2 < c_3 < c_\infty$. (For the first two inequalities recall that $\mathrm{Aut}\Gamma$ is not vertex-transitive and that Γ has more than n edges.) Thus, the numbers in (5.8) differ for different m.

By (5.1), $\lambda(v) = 0$ iff all members of the coclump $F\lambda$ are incident with all members of the clump Fv. Consequently, Lemma 5.5 implies that automorphisms of **D** permute the admissible triples and hence, by (5.8), preserve the colors of coclumps. □

Lemma 5.9

(a) *G is isomorphic to a subgroup of* Aut**D**.
(b) Aut**D** *induces a subgroup of* $\mathrm{Aut}\Gamma$ *and hence of* G.
(c) *If* $\gamma \in$ Aut**D** *induces the trivial automorphism of* Γ, *then* $\gamma = 1$.

Proof

(a) Each element of G naturally acts (dually) on our basis $v_\sharp, v_1, \ldots, v_n$ and dual basis $\lambda_\sharp, \lambda_1, \ldots, \lambda_n$, fixing $v_\sharp$ and $\lambda_\sharp$. By (1–5) and (5.1), the resulting linear transformation induces an automorphism of **D**.
(b) By Lemma 5.6, each element of Aut**D** induces permutations on the sets of coclumps of colors D_1 and D_2, and hence induces permutations of the vertices and edges of Γ, respectively. Condition (3) guarantees that this produces an automorphism of Γ.
(c) By Lemma 5.5, γ induces a collineation of V_F. Since $n \geq 3$, this collineation is also produced by a semilinear transformation T of V_F.

We first show that T *induces a scalar transformation of* V_F. By the hypothesis, $(F\lambda_i)^\gamma = F\lambda_i$ and hence $\lambda_i T = a_i\lambda_i$ for some $a_i \in F^*$ and all i (including $i = \sharp$). If ij is an edge of Γ, then $(F(\lambda_i + \lambda_j))^\gamma = F(a_i\lambda_i + a_j\lambda_j)$ has color D_3 by Lemma 5.6, and hence $a_i = a_j$. Since Γ is connected, $\lambda_i T = a\lambda_i$ for some $a \in F$ whenever $1 \le i \le n$. Also $(F(\lambda_\sharp + \lambda_i))^\gamma = F(a_\sharp\lambda_\sharp + a\lambda_i)$ has color $D_\sharp$ by Lemma 5.6, and hence $a_\sharp = a$. Consequently, $T(c\lambda_i) = ac^\sigma\lambda_i$ for all i, all $c \in F$, and some $\sigma \in \mathrm{Aut}F$.

Let ij be an edge. Since γ fixes $F\lambda_i$ and $F\lambda_j$, by Lemma 5.6 it permutes the colors of the coclumps in $F\lambda_i + F\lambda_j$ and hence permutes the pair $\{F(\omega\lambda_i + \lambda_j), F(\lambda_i + \omega\lambda_j)\}$ of coclumps of color D_4. Then $F(a\omega^\sigma\lambda_i + a\lambda_j) = (F(\omega\lambda_i + \lambda_j))^\gamma = F(\omega\lambda_i + \lambda_j)$ or $F(\omega^{-1}\lambda_i + \lambda_j)$. Consequently, $\omega^\sigma = \omega$ or ω^{-1}, and hence $\sigma = 1$ since ω generates F^*. Thus, T is precisely multiplication by the scalar $a \in F$, as asserted.

In particular, T acts on $F\lambda_\sharp$ as multiplication by a, so that γ acts fixed-point-freely on the points of $F\lambda_\sharp$. By Remark 2.4, γ induces a fixed-point-free automorphism of $\mathbf{D}_\sharp$. In view of our choice of $\mathbf{D}_\sharp$, it follows that γ acts trivially on $F\lambda_\sharp$. Thus, $a \in K^*$, so that $\gamma = 1$. □

Proof of Theorem 5.2 The theorem is an immediate consequence of Lemma 5.9. □

Proof of Theorem 1.1 By [1] and its proof, there is a graph Γ behaving as required and having $n \le 6|G|$ vertices (some care is needed here for small G). Also, we choose $[F\colon K] = 5$ in order to guarantee both the existence of a design $\mathbf{D}_\sharp$ having the desired properties and the requirement that there are five different, nontrivial cosets of $(\mathrm{Aut}\,F)\cdot\{\beta \in \mathrm{Aut}\,F^* \mid \beta = 1$ on $F^*/K^*\}$ in $\mathrm{Aut}\,F^*$. Then the design $\mathbf{D}$ in Theorem 5.2 has the parameters of $\mathrm{PG}(d, q)$ with $d + 1 = 5(n + 1) \le 35|G|$. □

We also note the following variation on this theorem:

Theorem 5.10 *Let G be any finite group. Then there are infinitely many integers $d \ge 35|G|$ such that, for each prime power q, there is a symmetric design* $\mathbf{D}$ *having the parameters of* $\mathrm{PG}(d, q)$ *such that* $\mathrm{Aut}\mathbf{D} \cong G$.

Proof First observe that, for every integer $m \ge 6$, there is a connected graph Γ_1 on m vertices whose full automorphism group is trivial. For example, start with an $(m-3)$-cycle, pick two of its vertices v, w, and add an additional edge containing v, and an additional path of length 2 containing w. Then the automorphism group of the resulting graph Γ_1 is the trivial group.

Therefore, if $G = 1$ and $d + 1 = 5(m + 1) \ge 35 = 35|G|$, then our construction (with $[F : K] = 5$ and $\Gamma = \Gamma_1$) produces the desired design.

Suppose that $|G| > 1$. By [1] there is a connected graph Γ' on $n' \le 3|G|$ vertices such that $\mathrm{Aut}\,\Gamma' \cong G$. Choose $d \ge 30|G|$ such that 5 divides $d+1$, and write $d+1 = 5(n'+m+1)$. Since $5m = d+1-5n'-5 \ge 15|G|-4 \ge 26$, there is a graph Γ_1 as above. Then the graph Γ with connected components Γ_1 and Γ' has G as full automorphism group. Once again our construction produces the desired design. □

6 Perturbations of affine spaces

Temporarily let Σ be a partition of the point set of $\mathbf{A} = \mathrm{AG}(d, q) = \mathrm{AG}(V)$ by affine subspaces (as in Sect. 2). For each point or line $X \in \Sigma$ let $\alpha_X = 1$; for any other $X \in \Sigma$ let α_X be a *parallelism-preserving* bijection from the hyperplanes of X to the blocks of an affine design $\mathbf{A}_X$ having point set X and the same parameters as $\mathrm{AG}(X)$. Also write $X^{\alpha_X} = X$. Define an incidence structure $\mathbf{A}^\alpha$ by using

$$\begin{aligned} &\textit{points}: && \textit{the points of } \mathbf{A}, \textit{ i.e., the vectors in } V \\ &\textit{blocks}: && H^{\alpha} := \bigcup_{X\in\Sigma} (H\cap X)^{\alpha_X} \textit{ for each hyperplane } H \textit{ of } \mathbf{A}. \end{aligned} \tag{6.1}$$

As in the proof of Theorem 2.2, it is straightforward to check that $\mathbf{A}^{\alpha}$ *is an affine design having the same parameters as* $\mathbf{A}$. However, we do not know interesting partitions Σ other than families of parallel subspaces. The following variation on this idea appears to be more useful.

Consider a family Σ of nonzero subspaces of V such that

$$\begin{aligned} &\bigcup_{X\in\Sigma} X = V \quad \text{and} \\ &X\cap Y = 0 \quad \text{for any distinct} X, Y \in \Sigma. \end{aligned} \tag{6.2}$$

Let α_X again be a parallelism-preserving bijection from the hyperplanes of X to the blocks of an affine design $\mathbf{A}_X$ having point set X and the same parameters as $\mathrm{AG}(X)$, but with the additional requirement that

$$\alpha_X \textit{ sends hyperplanes of } X \textit{ containing } 0 \textit{ to blocks of } \mathbf{A}_X \textit{ containing } 0. \tag{6.3}$$

Finally, define H^{α} and $\mathbf{A}^{\alpha}$ using (6.1).

Theorem 6.4 $\mathbf{A}^{\alpha}$ *is an affine design having the same parameters as* $\mathbf{A}$.

Proof In (2.3) we have $|(H\cap X)^{\alpha_X}\cap(H'\cap X)^{\alpha_X}| = |(H\cap X)\cap(H'\cap X)|$. (By (6.3), $(H\cap X)^{\alpha_X}\cap(H'\cap X)^{\alpha_X}$ can contain 0 only if $(H\cap X)\cap(H'\cap X)$ does). In particular, if H and H' are disjoint then so are H^{α} and H'^{α}.

Consequently, $\mathbf{A}^{\alpha}$ has constant block size, has a parallellism, has a constant number of points common to any two nonparallel blocks, and has the same parameters as an affine space. Hence, an elementary counting argument (see [2, Lemma 8.2 and Theorem 8.8]) completes the proof. □

Variations:

1. We could have used *any* affine design having a partition into suitable subsets that inherit the structure of affine designs.
2. We could have used a family Σ of subspaces whose union is all points and such that $X\cap Y = W$ is the same subspace for all distinct $X, Y \in \Sigma$. We would also require that the maps α_X send hyperplanes on x to blocks on x for each point x in W. This produces an affine design as before.

7 Affine versions of GMW designs

Let $K = \mathrm{GF}(q)$, $F = \mathrm{GF}(q^h)$, V_F of dimension N, Σ, $X = Fv_X$, D_0 and D_X be as in Sect. 4. In particular, $D_0 = T^{-1}(0)$ where $T\colon F\to K$ is the trace map; we also need the set $\Delta_0 := T^{-1}(1)$.

Let $\alpha\colon \{F\lambda \mid 0\neq\lambda\in V^{\circ}\}\to \mathrm{Aut}(F^*)$ be an arbitrary map, and extend each $\alpha_\lambda = \alpha_{F\lambda}$ to F by $0^{\alpha_\lambda} = 0$. Define an incidence structure $\mathbf{A}^{\alpha}$ by using

$$\begin{aligned} &\textit{points}: && \text{the vectors in} V \\ &\textit{blocks}: && (K\lambda)_{\alpha} := \lambda^{-1}(D_0^{\alpha_\lambda}) \text{ and} \\ & && [\lambda]_{\alpha} := \lambda^{-1}(\Delta_0^{\alpha_\lambda}) \text{ whenever } 0\neq\lambda\in V^{\circ}. \end{aligned} \tag{7.1}$$

Note that $(K\lambda)_\alpha = (K\lambda')_\alpha$ iff $\lambda' = c\lambda$ for some $0 \neq c \in K$, while $[\lambda]_\alpha = [\lambda']_\alpha$ iff $\lambda' = \lambda$. Moreover, if $\lambda \neq 0$ then $\{K\lambda, [k\lambda]_\alpha \mid k \in K^*\}$ is a parallel class: a partition of the points into pairwise disjoint blocks.

Proposition 7.2 $\mathbf{A}^\alpha$ *is an affine design having the same parameters as* $\mathrm{AG}(hN, q)$.

Proof We will use Theorem 6.4. Clearly $\Sigma = \{Fv \mid 0 \neq v \in V\}$ satisfies (6.2). We need to verify (6.3). Take $X = Fv_X \in \Sigma$ and $0 \neq \lambda \in V^\circ$ and set $c = \lambda(v)$. Then it is easy to check that

$$Fv_X \cap (K\lambda)_\alpha = \begin{cases} Fv_X & \text{if } c = 0 \\ c^{-1} D_0^{\alpha_\lambda} v_X & \text{if } c \neq 0 \end{cases}$$

$$Fv_X \cap [\lambda]_\alpha = \begin{cases} \emptyset & \text{if } c = 0 \\ c^{-1} \Delta_0^{\alpha_\lambda} v_X & \text{if } c \neq 0. \end{cases}$$

The sets $c^{-1}D_0^{\alpha_\lambda}$ and $c^{-1}\Delta_0^{\alpha_\lambda}$ are obtained from the hyperplanes of the affine space $\mathrm{AG}(F) = \mathrm{AG}(h, q)$ by applying the permutation α_λ of the points. It follows that the map sending $X \cap K\lambda \mapsto X \cap (K\lambda)_\alpha$ and $X \cap [\lambda] \mapsto X \cap [\lambda]_\alpha$ preserves parallelism and satisfies (6.3). □

Remark 7.3 Each Hadamard design produces an affine Hadamard 3-design by adjoining one further point. In particular, any GMW design obtained as in Sect. 4 with $q = 2$ produces an affine design with one more point. Therefore, in this case we do not need to use the above construction to "extend" such designs, and hence *we will assume that* $q > 2$.

Lemma 7.4 *Let x and y be distinct points of* $\mathbf{A}^\alpha$, *where* $0 \neq x \in X \in \Sigma$ *and* $y \in Y \in \Sigma$.

(i) *If $X = Y$ then the line xy has size q and lies in X. In particular, this holds for every line through* 0 : *each such line has the form Kx' for some $x' \in X$.*
(ii) *If $X \neq Y$, $y \neq 0$ and $|xy| > 2$, then* (3.3) *and Corollary 3.4 hold.*
(iii) *If $X \neq Y$, $y \neq 0$ and D_X^*/K^* is not equivalent to D_0^*/K^*, then $|xy| = 2$.*

Proof These are proved exactly as in Sect. 3 and Proposition 4.5. □

Proof of Theorem 1.3 Assume that all α_λ arise from the same automorphism $\beta \colon x \mapsto x^r$, where $(r, q(q^h - 1)) = 1$. Then the design $\mathbf{A}(r)$ in the theorem is just $\mathbf{A}^\alpha$.

(i) The parameters are clear, while the isomorphism assertion will follow once we prove (v).
(ii) By Lemma 7.4(i), lines contained in members of Σ have size q.
(iii) By Lemma 7.4(i), the stated lines all have the form Kv for $0 \neq v \in V$. Hence, the indicated incidence structure is exactly the one in Sect. 4, using the difference set $D = D_0^r$.
(iv) We already observed this.
(v) Recall that $q \geq 3$. By Lemma 7.4(i, iii), the q-point lines of $\mathbf{A}(r)$ are the lines in members of Σ. Consequently, every automorphism fixes 0, since this is the intersection of the members of Σ.
By (iii) and Sect. 4, we have $\mathrm{Aut}\mathbf{A}(r) \leq \Gamma\mathrm{L}(V_F)$. In order to prove the reverse inclusion, let $g \in \Gamma\mathrm{L}(V_F)$ and let $\sigma = \sigma_g$ be the associated field automorphism. Then $\sigma\lambda g^{-1}$ is a linear functional $V \to K$. We claim that g sends $[\lambda]_\alpha$ to $[\sigma\lambda g^{-1}]_\alpha$:

$$\begin{aligned} \lambda(v) \in \Delta_0^\beta &\iff \sigma\lambda g^{-1}(gv) = \lambda(v)^\sigma \in \Delta_0^{\beta\sigma} \\ &\iff \sigma\lambda g^{-1}(gv) \in (\Delta_0^\sigma)^\beta = \Delta_0^\beta \\ &\iff gv \in [\sigma\lambda g^{-1}]_\alpha \end{aligned} \tag{7.5}$$

(since σ commutes with β, is additive, and sends $\Delta_0 = T^{-1}(1)$ to itself). Similarly, g sends $(K\lambda)_\alpha$ to $(K\sigma\lambda g^{-1})_\alpha$. Therefore, $g \in \mathrm{Aut}\mathbf{A}(r)$, and hence $\mathrm{Aut}\mathbf{A}(r) = \Gamma\mathrm{L}(V_F)$.

(vi) One direction is clear. By (v), any isomorphism $\mathbf{A}(r_1) \to \mathbf{A}(r_2)$ must send 0 to 0 and hence induces an isomorphism of the GMW-designs in (iii). Now apply Theorem 1.2.

□

Remark 7.6 Relationship with relative difference set designs and their automorphism groups. Let Δ be a *relative difference set* of size q^{h-1} in F^* relative to K^*. This means that $|\Delta c \cap \Delta|$ is 0 if $1 \neq c \in K^*$ and q^{h-1} if $c \in F - K$. This produces an incidence structure $\mathbf{A}'_\Delta$ whose point set is the nonzero elements of $V = F^N$ and whose blocks are the sets $\lambda^{-1}(\Delta)$, $0 \neq \lambda \in V_F^\circ$. It is straightforward to check that any two distinct blocks meet in $q^{h(N-2)}$ points unless the corresponding linear functionals are linearly dependent over K, in which case the intersection is empty.

Identify V with $\mathrm{GF}(q^{Nh})$. Then it is easy to check that $\mathbf{A}'_\Delta$ admits the automorphisms $v \mapsto cv$, $v \in V^*$ (compare (7.7) below). It follows that each block of $\mathbf{A}'_\Delta$ is a relative difference set in V^* with respect to K^*.

It is also easy to check that there is an affine design $\mathbf{A}_\Delta$ underlying $\mathbf{A}'_\Delta$ having the same parameters as $\mathrm{AG}(hN, q)$: include the zero vector as a new point and use the point sets $V - \bigcup_{c \in K^*}(c\lambda)^{-1}(\Delta)$, $0 \neq \lambda \in V_F^\circ$, as new blocks. There is an affine design determined in the same manner by D, with point set F and blocks Δc and $(F - K^*\Delta)c$, $c \in F^*$. Then the larger affine design $\mathbf{A}_\Delta$ can also be described as follows, using a specific linear functional, namely the trace map $\hat{T}\colon V \to F$: the blocks of $\mathbf{A}_\Delta$ are the sets $\big(\hat{T}^{-1}(\Delta)\big)c$ and $\big(\hat{T}^{-1}(F - K^*\Delta)\big)c$, $c \in V^*$.

However, this description focuses only on one cyclic automorphism group and hence loses some of the rich structure of these affine designs.

Namely, $\mathrm{GL}(V_F) \leq \mathrm{Aut}\mathbf{A}'_\Delta \leq \mathrm{Aut}\mathbf{A}_\Delta$. The second inclusion is obvious, so consider any $g \in \mathrm{GL}(V_F)$, sending $v \mapsto gv$. Then g sends $\lambda^{-1}(\Delta)$ to $(\lambda g^{-1})^{-1}(\Delta)$:

$$\lambda(v) \in \Delta \iff (\lambda g^{-1})(gv) \in \Delta \iff gv \in (\lambda g^{-1})^{-1}(\Delta). \tag{7.7}$$

(This is essentially the same calculation as in (7.5).) In particular, *these designs admit many cyclic automorphism groups acting regularly on both the points* $\neq 0$ *and the blocks not on* 0; in fact, analogues of Theorem 1.3(i)–(iv) hold for $\mathbf{A}_\Delta$. Moreover, $\Gamma\mathrm{L}(V) \leq \mathrm{Aut}\mathbf{A}'_\Delta$ if Δ is invariant under all automorphisms of F; this is the case when $\Delta = T^{-1}(1)$ for the trace map $T\colon F \to K$; and this produces affine versions of GMW designs.

The above examples appear implicitly in [12, p. 77]. However, no mention is made there of affine designs (or larger automorphism groups).

8 Automorphism groups of affine designs

We can use the ideas in Sect. 5 to give a simpler proof of a version of another result in [9]:

Theorem 8.1 *Let G be any finite group. Then for some integer $d < 35|G|$, and for infinitely many integers $d \geq 35|G|$, for each prime power $q > 2$ there is an affine design* $\mathbf{A}$ *having the parameters of* $\mathrm{AG}(d, q)$ *such that* $\mathrm{Aut}\mathbf{A} \cong G$.

Proof Let $G, F, K, D_0, V, \{v_\sharp, v_1, \dots, v_n\}, \{\lambda_\sharp, \lambda_1, \dots, \lambda_n\}, \alpha_m$ and $D_m = D_0^{\alpha_m}$ (for $m \in \{\sharp, 1, 2, 3, \infty\}$), and $D\colon \{F\lambda \mid 0 \neq \lambda \in V^\circ\} \to \{D_\sharp, D_1, D_2, D_3, D_\infty\}$ be as in Sect. 5. The integer d we use will be the one already used in the proofs of Theorems 1.1 and 5.10. Write $\Delta'_m = \Delta_0^{\alpha_m}$.

The hyperplanes of $AG(F_K)$ can be taken to be of the form $D_0 a$ and $\Delta_0 a$, $a \in F^*$. Let $\mathbf{A}_\sharp$ be an affine design with the parameters of $AG(F_K)$ and point set F such that no automorphism has precisely one fixed point. The existence of such a design again follows from [9]. Let ρ denote a parallelism-preserving bijection from the blocks of $AG(F_K)$ to the blocks of $\mathbf{A}_\sharp$ such that (6.3) holds.

Define an incidence structure $\mathbf{A}$ by using

$$\begin{array}{ll} \textit{points}: & \text{the vectors in } V \\ \textit{blocks}: & (K\lambda) \text{ and } [\lambda] \text{ whenever } 0 \neq \lambda \in V^\circ, \end{array}$$

with incidence defined by

$$v\,\mathrm{I}\,(K\lambda) \iff \begin{cases} \lambda(v) \in D_\lambda & \text{if } K\lambda \not\subseteq F\lambda_\sharp \\ \lambda(v) \in (D_0 c^{-1})^\rho & \text{if } K\lambda = Kc\lambda_\sharp \end{cases}$$

$$v\,\mathrm{I}\,[\lambda] \iff \begin{cases} \lambda(v) \in D'_\lambda & \text{if } F\lambda \neq F\lambda_\sharp \\ \lambda(v) \in (\Delta_0 c^{-1})^\rho & \text{if } \lambda = c\lambda_\sharp. \end{cases}$$

The argument in Sect. 6 shows that $\mathbf{A}$ is an affine design with the parameters of $AG(V_K)$. As in Sect. 7, whenever $0 \neq v \in V$ the line $0v$ is Kv, and there is some $w \in V$ such that $vw = \{v, w\}$. Since $q > 2$, this characterizes 0 as the only point such that all lines through it have size q. The 1-dimensional K-subspaces of V are precisely the lines through 0, and the blocks through 0 are precisely those of the form $(K\lambda)$. Consequently, starting with $\mathbf{A}$ we can geometrically reconstruct the design $\mathbf{D}$ of Sect. 5. On the other hand, the faithful, linear representation of G on V used in Sect. 5 maps into Aut$\mathbf{A}$.

Thus, $G \leq \mathrm{Aut}\mathbf{A}$. Assume that $G < \mathrm{Aut}\mathbf{A}$. Then by Sect. 5, some $1 \neq g \in \mathrm{Aut}\mathbf{A}$ fixes 0 as well as all lines and all blocks through 0. This shows that g induces on each clump $F\lambda$ multiplication by a scalar from K^*. The same argument as in Sect. 5 shows that then g acts on V as multiplication by a scalar.

Since g fixes the blocks $(Ka\lambda_\sharp)$, the blocks $[a\lambda_\sharp]$ parallel to these are permuted among themselves by g. The intersections $(Ka\lambda_\sharp) \cap Fv_\sharp$ and $[a\lambda_\sharp] \cap Fv_\sharp$ form a design isomorphic to $\mathbf{A}_\sharp$ and invariant under g. This contradicts the choice of $\mathbf{A}_\sharp$. □

Acknowledgement This research was supported in part by NSF grant DMS 0242983.

References

1. Babai L.: On the minimum order of graphs with given group. Can. Math. Bull. **17**, 467–470 (1974).
2. Beth T., Jungnickel D., Lenz H.: Design Theory, vol. 1. Cambridge University Press, Cambridge (1999).
3. Dembowski P.: Finite Geometries. Springer, Berlin (1968).
4. Dembowski P., Wagner A.: Some characterizations of finite projective spaces. Arch. Math. **11**, 465–469 (1960).
5. Gordon B., Mills W.H., Welch L.R.: Some new difference sets. Can. J. Math. **14**, 614–625 (1962).
6. Jackson W.-A.: A characterization of Hadamard designs with SL$(2, q)$ acting transitively. Geometriae Dedicate **46**, 197–206 (1993).
7. Jackson W.-A., Wild P.R.: On GMW designs and cyclic Hadamard designs. Des. Codes Cryptogr. **10**, 185–191 (1997).
8. Jungnickel D.: The number of designs with classical parameters grows exponentially. Geometriae Dedicate **16**, 167–178 (1984).

9. Kantor W.M.: Automorphisms and isomorphisms of symmetric and affine designs. J. Algebr. Comb. **3**, 307–338 (1994).
10. Kantor W.M.: Note on GMW designs. Eur. J. Comb. **22**, 63–69 (2001).
11. Merchant E.: Exponentially many Hadamard designs. Des. Codes Cryptogr. **38**, 297–308 (2006).
12. Pott A.: Finite Geometry and Character Theory. Springer, Berlin (1995).
13. Shrikhande S.S.: On the nonexistence of affine resolvable balanced incomplete block designs. Sankhyā **11**, 185–186 (1951).