Designs, Codes and Cryptography (2022) 90:2145–2157
https://doi.org/10.1007/s10623-021-00936-x

Automorphism subgroups for designs with $\lambda = 1$

William M. Kantor[1,2]

Received: 16 March 2021 / Accepted: 19 August 2021 / Published online: 31 October 2021

Abstract
Given an integer $k \geq 3$ and a group G of odd order, if there exists a 2-$(v, k, 1)$-design and if v is sufficiently large then there is such a design whose automorphism group has a subgroup isomorphic to G. Weaker results are obtained when $|G|$ is even.

Keywords Design · Automorphism group

Mathematics Subject Classification 05B99 · 05E18

1 Introduction

About 40 years ago Babai [1, p. 8] proposed the following "subgroup problem":

> PROBLEM 2.7. Prove for every $k \geq 3$, that, given a finite group G, there is a BIBD of block size k (a 2-$(v, k, 1)$-design) X such that $G \lesssim \mathrm{Aut}\, X$.

Wilson proved this when k is a multiple of $|G|$ [1, p. 8]; [10, Theorem 12.1] contains this when $k - 1$ is a multiple of $|G|$. (These results are also in [14, p. 311].)

In this note we will prove other special cases of Babai's problem:

Theorem 1.1 *Given an integer $k \geq 3$ and a group G of odd order, if v satisfies the divisibility conditions for a 2-$(v, k, 1)$-design and is sufficiently large then there is a 2-$(v, k, 1)$-design whose automorphism group has a subgroup isomorphic to G.*

When $k = 3$ stronger results appear in [3,5].

Theorem 1.2 *Given an odd integer $k \geq 3$ and a group G of even order such that $(k, |G|) = 1$, there are infinitely many v for which there is a 2-$(v, k, 1)$-design whose automorphism group has a subgroup isomorphic to G.*

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue: The Art of Combinatorics – A Volume in Honour of Aart Blokhuis".

✉ William M. Kantor
kantor@uoregon.edu

[1] University of Oregon, Eugene, OR 97403, USA

[2] Northeastern University, Boston, MA 02115, USA

Theorem 1.3 *Consider an even integer $k \geq 4$ and a group G of even order. Assume that every prime power dividing $|G|$ either divides k or is relatively prime to $k(k-1)$. Then there are infinitely many v for which there is a 2-$(v, k, 1)$-design whose automorphism group has a subgroup isomorphic to G.*

When k or $k-1$ is a prime power, see [1, p. 8] or [8] for a stronger type of result: there are infinitely many 2-$(v, k, 1)$-designs D for which $G \cong \mathrm{Aut}\, D$. Babai [1, Conjecture 2.8] asked for such a stronger result for arbitrary $k \geq 3$, but this presently seems out of reach: there appears to be no method for recovering the classical geometry underlying one of our designs as was done when k or $k-1$ is a prime power. See Remark 2.5 and Sect. 8 for further comments about proving this stronger result.

The single idea behind the above three theorems is to place copies of a 2-$(p, k, 1)$-design in the lines of an affine space $AG(d, p)$ in a G-invariant manner, for large d and a suitable prime p; this occurred in [9, Sect. III.C] for a very different purpose. The 2-$(p, k, 1)$-designs we use admit suitable automorphism groups (which are cyclic for Theorems 1.2 and 1.3), and are special cases of lovely results in [10,13,14].

Theorem 1.2 is proved in Sect. 3, while Theorem 1.3 is in Sect. 5. The remainder of this paper is devoted to Theorem 1.1: Sect. 2 contains a proof that there are infinitely many designs behaving as in Babai's problem when $|G|$ is odd, while Propositions 6.2 and 7.1 (based on Theorem 4.1) contain the background needed for the proof of Theorem 1.1 at the end of Sect. 7.

All of our proofs are the same for abelian and nonabelian groups. The fact that $|G|$ is odd in Theorem 1.1 is used for its combinatorial implications rather than its implications for group structure. In all of the results mentioned above $|G|$ is tiny relative to v. Our theorems do not deal with the case $|G| \equiv 0 \pmod 4$ and $k \equiv 2 \pmod 4$. The case $(|G|, k) \neq 1 \neq (|G|, k-1)$ seems especially difficult when $|G|$ is even.

Preliminaries If G is a group of permutations $x \mapsto x^g$ of a set X, and $L \subseteq X$, then $G_L := \{g \in G \mid L^g = L\}$ is the set-stabilizer of L in G, which induces the subgroup G_L^L of the symmetric group $\mathrm{Sym}(L)$.

A permutation group C on a set X is *semiregular* if $x^c \neq x$ whenever $x \in X$ and $1 \neq c \in C$; and C is *regular* if it is transitive and semiregular. If $\langle c \rangle$ and $\langle c' \rangle$ are semiregular cyclic groups of permutations of X having the same order then c and c' are conjugate in $\mathrm{Sym}(X)$.

We will use the same symbol to denote a design and its set of points.

2 Odd order

Theorem 2.1 (Wilson [13, pp. 22–26]) *Given $k \geq 3$, for all sufficiently large primes $p \equiv 1 \pmod{k(k-1)}$ there is a 2-$(p, k, 1)$-design E whose set of points is $F := \mathbb{F}_p$ and whose automorphism group contains $\{x \mapsto x + b \mid b \in F\}$.*

Moreover, if $p = 1 + k(k-1)t$ with t odd then E can be chosen so that $\{x \mapsto sx \mid s \in F,\ s^t = 1\}$ is also a group of automorphisms of E.

If $t = (p-1)/k(k-1)$ is odd, the subgroup of F^* of order $2t$ factors as $S \times \langle -1 \rangle$ for a subgroup S of order t. Then [13] obtains $A \subset F$ such that $\{sA + b \mid s \in S,\ b \in F\}$ is the set of blocks of E.

The preceding theorem lets us handle Babai's problem when $|G|$ is odd:

Theorem 2.2 *Given an integer $k \geq 3$ and a group G of odd order, there are infinitely many v for which there is a 2-$(v, k, 1)$-design whose automorphism group has a subgroup isomorphic to G.*

Proof By Dirichlet's Theorem there is a prime $p \equiv 1 + k(k-1)|G| \pmod{2k(k-1)|G|}$. If we write $p - 1 = k(k-1)t$, it follows that $(p-1)/\{k(k-1)\} = t$ is odd and divisible by $|G|$. As above, let $F = \mathbb{F}_p$ and let S be the subgroup of F^* of order t.

We will prove the theorem by using suitable powers $v = p^d$. Let $V = F^d$, where d is chosen so that G is (isomorphic to) a group of permutations of a basis of V and hence is in $\mathrm{GL}(V)$. (For example, any integer $d \geq |G|$ can be chosen.)

We will use the affine space $\mathbf{A} := \mathrm{AG}(d, p)$ whose set of points is V. Clearly $G < \mathrm{GL}(V) < \mathrm{AGL}(V)$. (Here $\mathrm{AGL}(V) = \{v \mapsto vM + c \mid M \in \mathrm{GL}(V),\ c \in V\}$ is $\mathrm{Aut}\,\mathbf{A}$ if $d > 1$.) Let $\mathcal{L}$ be a set of representatives of the orbits of G on the lines of $\mathbf{A}$.

Let $L \in \mathcal{L}$. View L as F, so the group $\mathrm{AGL}(1, p)$ of $p(p-1)$ affine transformations $x \mapsto ax + b$ for $a \in F^*$, $b \in F$, corresponds to the affine group $\mathrm{AGL}(L)$ on L obtained from $\mathrm{AGL}(V)$. Then $\{x \mapsto sx + b \mid s \in S, b \in F\}$ corresponds to a subgroup $S(L)$ of $\mathrm{AGL}(L)$ of order pt. Each subgroup of $\mathrm{AGL}(L)$ of order dividing $|S| = t$ lies in $S(L)$ (since the quotient group $\mathrm{AGL}(1, p)/\{x \mapsto x + b \mid b \in F\}$ is isomorphic to the cyclic group F^*).

The set-stabilizer G_L induces on L a subgroup G_L^L of $\mathrm{AGL}(L)$. Since $|G|$ divides $t = |S|$ so does $|G_L^L|$. Then $G_L^L \leq S(L)$ by the preceding paragraph. (In fact, G_L^L is even more restricted since $p > |G_L^L|$, but we will not need this fact.)

Use each $L \in \mathcal{L}$ as the set of points of a 2-$(p, k, 1)$-design D_L behaving as E does at the end of Theorem 2.1, so $G_L^L \leq S(L) \leq \mathrm{Aut}\, D_L$. (The end of Theorem 2.1 needed t to be odd. Since $|G| | t$, this is where we need $|G|$ to be odd.)

For each $L \in \mathcal{L}$ let $\mathcal{B}_L$ be the set of blocks of D_L. If $g \in G$ let ${D_L}^g$ denote the design $(D_L)^g$ whose set of points is L^g and whose set of blocks is $(\mathcal{B}_L)^g$.

This well-defined: if $L^g = L^{g'}$ for $g, g' \in G$ then $(D_L)^g = (D_L)^{g'}$. For, if $h = g'g^{-1}$ then $h \in G$ and $L^h = L$, so the permutation h^L induced by h on L lies in $G_L^L \leq \mathrm{Aut}\, D_L$. Then h^L sends D_L to itself, so $(D_L)^g = (D_L)^{g'}$, as required.

Define a design D as follows:

points are the points of $\mathbf{A}$

blocks are the elements of $\bigcup_{L \in \mathcal{L},\, g \in G} (\mathcal{B}_L)^g$.

It is elementary that D is a 2-$(p^d, k, 1)$-design: any two points lie in a unique line L^g for $L \in \mathcal{L}$ and $g \in G$, and then in a unique member of $(\mathcal{B}_L)^g$. Since G is in $\mathrm{AGL}(V)$ and permutes the sets $(D_L)^g$ it is a subgroup of $\mathrm{Aut}\, D$. □

Remark 2.3 By the last sentence of Theorem 2.1, the first paragraph of the above proof contains a solution to Babai's problem for the cyclic group of order $|G|$. The proofs of Theorems 1.2 and 1.3 involve something similar: a cyclic group case of Babai's problem is used to deal with much more general groups.

Remark 2.4 Placing designs on the blocks of another design is standard [13, p. 28]. Preserving the automorphism group is less standard. The above simple method was used in [9, Sect. III.C] to construct flag-transitive designs; preserving a group of automorphisms of the larger design was as essential there as it is here.

Remark 2.5 We used $\mathbf{A}$ with an arbitrary group G of odd order. Given the action of G on V, the groups G_L and G_L^L are known; since $p > |G|$, the group G_L^L is cyclic.

However, there is flexibility with the designs D_L. We only needed to have $G_L^L \le \mathrm{Aut}\, D_L$ (for each $L \in \mathcal{L}$) in order for the proof to work. Thus, each of the original designs D_L ($L \in \mathcal{L}$) can be replaced by $(D_L)^{h(L)}$ for any permutation $h(L)$ of the points of L that normalizes G_L^L.

Suitable changes of this sort might provide a way to obtain a 2-$(p^d, k, 1)$-design D' such that $G \cong \mathrm{Aut}\, D'$. For this purpose *it appears to be necessary to recover the affine space* $\mathbf{A}$ *from some such design* D'. However, we have been unable to do this (cf. Sect. 8).

Remark 2.6 On the other hand, *each design* D_L *admits the group* $S(L) < \mathrm{AGL}(L) = \mathrm{AGL}(V)_L^L$ *as a group of automorphisms that is regular on blocks*: $\{sA + b \mid s \in S,\ b \in F\}$ is the set of $|S|p = p(p-1)/k(k-1)$ blocks of each design constructed in [13, p. 22] starting from a suitable initial block $A \subset F$. Once again this uses the fact that t and $|G|$ are odd.

Remark 2.7 If B is a block of the design D constructed in the proof of Theorem 2.2 then $G_B^B = 1$. For, B is in a unique line L of $\mathbf{A}$, so L is fixed by G_B. Then $G_B^L \le S(L)$ as in the above proof. However, as already noted in the preceding remark, $S(L)$ is regular on the blocks of D_L, so $G_B^L \le S(L)_B = 1$ and hence $G_B^B = 1$.

This will be crucial in Sect. 7.

If d is large then G has many fixed points so there are many lines of $\mathbf{A}$ fixed pointwise by many elements of G.

3 Theorem 1.2

When $|G|$ is even we use a consequence of a theorem of Lamken and Wilson [10]; but first we need a prime:

Lemma 3.1 *Let* $k \ge 3$, *and let* h *be a multiple of* 4 *such that* $(k, h) = 1$. *Then there are infinitely many primes* $p > h$ *satisfying the following conditions for some integer* n:

(i) $p = 1 + (k-1)n$,
(ii) $n(n-1) \equiv 0 \pmod k$,
(iii) $n(n-1) \equiv 0 \pmod{4k}$ *if* $k \equiv 3 \pmod 4$, *and*
(iv) $(p-1, h) = (k-1, h)$.

Proof Let w be a positive integer such that $kw \equiv 1 \pmod h$. Then $\big(1 + k(k-1)w, hk(k-1)\big) = \big(1 + k(k-1)w, h\big) = (1 + (k-1), h) = 1$. By Dirichlet's Theorem there are infinitely many integers y such that $p := 1 + k(k-1)w + \{hk(k-1)\}y = 1 + (k-1)n$ is prime, where $n := kw + hky \equiv 0 \pmod k$. Then (ii) is clear, and (iii) holds: $n - 1 = (kw - 1) + hky$ is a multiple of h and hence of 4. Finally, (iv) holds: $(p-1, h) = \big(k(k-1)w + \{hk(k-1)\}y, h\big) = \big(kw(k-1), h\big) = (k-1, h)$. □

Theorem 3.2 (Lamken and Wilson [10, Theorem 12.1]) *Given* k, *for all sufficiently large* p *satisfying the first three conditions of* Lemma 3.1 *there is a* 2-$(p, k, 1)$*-design* E *such that* Aut E *has a cyclic subgroup of order* $k - 1$ *having one fixed point and semiregular on the remaining points.*

Proof of Theorem 1.2 We imitate the proof of Theorem 2.2. In Lemma 3.1 let $h := |G|$, where we increase G if necessary in order to have h divisible by 4. (Admittedly this is annoying.) Choose a sufficiently large $p > |G|$ so that the lemma applies. Choose d sufficiently large so

that G is (isomorphic to) a subgroup of the symmetric group S_d and hence also of $\mathrm{AGL}(d, p)$. The points of our design D are the points of $\mathbf{A} = \mathrm{AG}(d, p)$.

Let $L \in \mathcal{L}$, where $\mathcal{L}$ is a set of representatives of the orbits of G on the lines of $\mathbf{A}$. Then $G_L^L \leq \mathrm{AGL}(L) \cong \mathrm{AGL}(1, p)$ and $p > |G| \geq |G_L^L|$, so G_L^L is a cyclic group of order dividing $(p-1, |G|) = (k-1, |G|)$ by Lemma 3.1(iv). This cyclic group fixes a point, and all remaining orbits have length $|G_L^L|$; all permutations of L having this cycle structure are conjugate in $\mathrm{Sym}(L)$. After identifying L with the set of points of the design in Theorem 3.2 and conjugating by an element of $\mathrm{Sym}(L)$, we may assume that G_L^L is contained in the cyclic group of order $k-1$ provided by Theorem 3.2. Thus, L is the set of points of a design D_L, isomorphic to the design E in that theorem, such that $G_L^L \leq \mathrm{Aut}\, D_L$.

Now repeat the last three paragraphs of the proof of Theorem 2.2. □

4 Moore and Ray-Chaudhuri

Wilson [13, p. 29] credits Ray-Chaudhuri for the following generalization of a standard, fundamental result due to Moore [11, p. 276]:

Theorem 4.1 *A 2-$(w, k, 1)$-design W, a transversal design $TD(k, y-x)$ and a 2-$(y, k, 1)$-design Y with an x-point subdesign X produce a 2-$(w(y-x)+x, k, 1)$-design.*

Here a *transversal design* $TD(k, n)$ consists of kn points, n^2 subsets of size k called "blocks", and a partition of the points into k "groups" of size n, such that each block meets each group in a single point and any two points in different groups are in a unique block.

The following proof is based on [13, pp. 29–30], and is included since we need properties of the constructed design.

Proof If $Z := Y - X$ as a set of points, then $X \cup (W \times Z)$ will be the set of points of our new design. Let A be a block of W, hence of size k. There is a transversal design $TD(k, y-x)$ on $A \times Z$ whose set of groups is $\{a \times Z \mid a \in A\}$ and whose set of blocks will be denoted $\mathcal{B}_{A\times Z}$; this transversal design, denoted $T_{A\times Z}$, has nothing to do with the design on Y.

Imitating Moore [11, p. 276] produces a new design as follows:

points: elements of $X \cup (W \times Z)$;

blocks are of four sorts:

- the blocks of X,
- for each $a \in W$ and each block B of Y not inside X,
  - $a \times B$ if $B \cap X = \emptyset$, or
  - $x \cup \big(a \times (B - x)\big)$ if $B \cap X = x$, and
- $\bigcup\{\mathcal{B}_{A\times Z} \mid A \text{ is a block of } W\}$.

There is no conflict between the blocks in $T_{A\times Z}$ for different choices of A: distinct intersecting sets $A \times Z$ and $A' \times Z$ intersect in a group.

The only other part the proof worth a comment concerns a pair $(a_1, z_1), (a_2, z_2) \in W \times Z$ with $a_1 \neq a_2$. Since $a_1 \neq a_2$ there is a unique block A of W containing them, and (a_1, z_1) and (a_2, z_2) belong to different groups $a_1 \times Z$ and $a_2 \times Z$ of $T_{A\times Z}$. Then there is a unique block in $\mathcal{B}_{A\times Z}$ containing them. □

Remark 4.2 The existence of a $TD(k, n)$ is equivalent to the existence of a set of $k-2$ mutually orthogonal Latin squares of order n [12, Lemma 2.1]. If $N(n)$ denotes the maximum number

of mutually orthogonal Latin squares of order n, then [4] proves that there is an integer n_0 such that $N(n) \geq \frac{1}{3}n^{1/91}$ if $n > n_0$ (and there are better bounds known [12]). Thus, if $n(k) := \max(n_0, (3k)^{91})$ then

$$\text{If } n > n(k) \quad \text{then there is a } TD(k, n). \tag{4.1}$$

5 Nets and even k

As in Sects. 2 and 3 the proof of Theorem 1.3 requires a suitable design on a prime number of points. Whereas Theorem 1.2 used a 2-$(p, k, 1)$-design having a cyclic automorphism group of order $k-1$ fixing one point and semiregular on the remaining points (Theorem 3.2), this time we need a 2-$(p, k, 1)$-design having a cyclic automorphism group of order k fixing one point and semiregular on the remaining points (Theorem 5.4). For this purpose we use Theorem 4.1 and transversal designs. However, it will be easier to start with nets.

5.1 Nets

The dual of a transversal design $TD(k, n)$ is a (k, n)-*net*: a set of n^2 points and kn subsets of size n called "lines" such that distinct lines meet at most once and the points are partitioned into k "parallel classes" each consisting of n lines. (Parallel classes correspond to groups.) The examples we need arise from unions of k parallel classes of lines of a desarguesian affine plane AG$(2, n)$; the translation group of the plane acts as a group of automorphisms of the net. Clearly these examples exist whenever n is a prime power and $k \leq n + 1$.

Lemma 5.1 *Let q and m be powers > 1 of a prime p, and $E = \mathbb{F}_{q^m} \supset F = \mathbb{F}_q$. Let $\sigma : x \mapsto x^q$ and let $T : E \to F$ be the trace map. If $a \in E - \operatorname{Ker} T$ and $h : x \mapsto x\sigma + a$, then $\langle h \rangle$ has order pm and is semiregular on E.*

Proof By induction, $h^i : x \mapsto x\sigma^i + \sum_{j=0}^{i-1} a\sigma^j$ for all $i \geq 1$, so $h^m : x \mapsto x\sigma^m + T(a) = x + T(a)$ and h has order pm.

If $x \in E$ then $T(x) = \sum_{j=0}^{m-1} x\sigma^j$ and $T(x(\sigma - 1)) = T(x)\sigma - T(x) = 0$, so $\operatorname{Im}(\sigma - 1) \subseteq \operatorname{Ker} T$. If $i \geq 1$, $d := (m, i) < m$ and $x\sigma^i = x$, then $T(x) = (m/d) \sum_{j=0}^{d-1} x\sigma^j = 0$ since m/d is a multiple of p, so $\operatorname{Im}(\sigma - 1) + \operatorname{Ker}(\sigma^i - 1) \subseteq \operatorname{Ker} T$.

For semiregularity, let $0 < i < pm$ and suppose that h^i fixes x. Then $x(1 - \sigma^i) = \sum_{j=0}^{i-1} a\sigma^i$, so $x(1 - \sigma^i)(\sigma - 1) = a(\sigma^i - 1)$ and $x(\sigma - 1) + a \in \operatorname{Ker}(\sigma^i - 1)$. If $i \neq m$ then $(m, i) < m$; we have seen that this implies that $\operatorname{Ker} T$ contains $\operatorname{Im}(\sigma - 1) + \operatorname{Ker}(\sigma^i - 1)$ and hence also a, which is not the case. If $i = m$ then we obtain the same contradiction: $0 = x(1 - \sigma^m) = \sum_{j=0}^{m-1} a\sigma^j = T(a)$. □

Lemma 5.2 *Let q and m be powers > 1 of a prime p. Let $3 \leq k < q$. Then there is a (k, q^m)-net having a cyclic automorphism group of order m that is semiregular on both the points and lines and leaves invariant each parallel class.*

Proof We use the notation of the preceding lemma. Consider the affine plane AG$(2, q^m)$ defined using E. Our net will consist of the points of this plane and any union of k parallel classes of lines of the form $y = tx + b$ with $1 \neq t \in F$ (so $t\sigma = t$).

Let $g : (x, y) \mapsto (x^h, y^h)$. By the preceding lemma, $\langle g \rangle$ has order pm and is semiregular on points. Moreover, if $i \geq 1$ then g^i sends the line $\{(x, tx + b) \mid x \in F\}$ to the parallel line

$\{(x\sigma^i + a_i, t(x\sigma^i) + b\sigma^i + a_i) \mid x \in F\}$, where $a_i := \sum_{j=0}^{i-1} a\sigma^j$. As above, $a_i(\sigma - 1) = a(\sigma^i - 1)$.

We still need semiregularity on lines. If $0 < i < pm$ and g^i fixes a line $y = tx + b$ of the net, then $t(x\sigma^i) + b\sigma^i + a_i = t(x\sigma^i + a_i) + b$, so $b(\sigma^i - 1) = a_i(t - 1)$. Then $b(\sigma - 1)(\sigma^i - 1) = a(\sigma^i - 1)(t - 1)$, so $b(\sigma - 1) - a(t - 1) \in \mathrm{Ker}(\sigma^i - 1)$. If $i \neq m$ then $a(t - 1) \in \mathrm{Im}(\sigma - 1) + \mathrm{Ker}(\sigma^i - 1) \subseteq \mathrm{Ker}\, T$ (as seen above), which is impossible since $0 \neq t - 1 \in F$ and a is not in the F-space $\mathrm{Ker}\, T$. Thus, $i = m$ and $0 = b(\sigma^m - 1) = a_m(t - 1) = T(a)(t - 1)$, which is again impossible since $t \neq 1$.

This proves that $\langle g^p \rangle$ behaves as required. □

Lemma 5.3 *Let $k \geq 3$ be an integer and let $p_1, \ldots, p_r$ be its distinct prime factors. For each i let $m_i > k$ be a power of p_i, so $k|\pi := \prod_i m_i$.*

Then for each integer $s > n(k)$ there is a $(k, s\prod_i m_i^{m_i})$-net having a cyclic automorphism group of order π that is semiregular on both points and lines while leaving invariant each parallel class. □

Remark 4.2 contains the definition of $n(k)$. We emphasize that s and the m_i are not related.

Proof For each i, by using Lemma 5.2 with $q = m = m_i$ we obtain a $(k, m_i^{m_i})$-net N_i having a cyclic automorphism group C_i of order m_i that is semiregular on both points and lines and leaves invariant each parallel class.

By Remark 4.2, if $s > n(k)$ then there is a (k, s)-net N_∞. The net required in the lemma is a product $N = N_1 \cdots N_r N_\infty$, which we now define.

Let X_i be the set of points of N_i and $\mathcal{L}_{i1}, \ldots, \mathcal{L}_{ik}$ the parallel classes of N_i, so $\bigcup_j \mathcal{L}_{ij}$ is the set of lines of N_i. Then N is defined as follows: $X := X_1 \times \cdots \times X_r \times X_\infty$ is its set of points, while its parallel classes are $\mathcal{L}_j := \mathcal{L}_{1j} \times \cdots \times \mathcal{L}_{rj} \times \mathcal{L}_{\infty j}$, $1 \leq j \leq k$, and $\bigcup_j \mathcal{L}_j$ is its set of lines.

In general, the groups $\mathrm{Aut}\, N_i$ are not involved in $\mathrm{Aut}\, N$ since we used an arbitrary ordering of the parallel classes of each N_i. However, for our purposes this is not a problem since C_i leaves invariant each parallel class of N_i and we will use the identity on N_∞: there is a cyclic automorphism group $C \cong \prod_i C_i$ of N of order $\pi = \prod_i m_i$, consisting of all $(x_1, \ldots, x_r, x_\infty) \mapsto (x_1^{c_1}, \ldots, x_r^{c_r}, x_\infty)$ for $c_i \in C_i$. (This is an automorphism of N: c_i permutes the lines in each $\mathcal{L}_{ij}$, so if $(x_1, \ldots, x_r, x_\infty) \in (L_{1j}, \ldots, L_{rj}, L_{\infty j}) \in \mathcal{L}_j$ then $(x_1^{c_1}, \ldots, x_r^{c_r}, x_\infty) \in (L_{1j}^{c_1}, \ldots, L_{rj}^{c_r}, L_{\infty j}) \in \mathcal{L}_j$.)

The only way a point (or line) of N can be fixed by the above element of C is for a point (or line) of every component to be fixed, and then each $c_i = 1$ by the semiregularity of each C_i. □

5.2 Theorem 1.3

Following the models in Sects. 2 and 3 we need a prime p and a 2-$(p, k, 1)$-design admitting a suitable automorphism group.

Proposition 5.4 *Given integers $k \geq 3$ and $h \geq 1$ such that $(k - 1, h) = 1$, there are infinitely many primes p such that $(p - 1, h)$ divides some power of k and there is a 2-$(p, k, 1)$-design having a cyclic automorphism group of order k fixing one point and semiregular on the remaining points.*

Proof We will use a design in Theorem 4.1 whose set of points is $U := X \cup (W \times Z)$, $Z := Y - X$, where X is a subset of size 1 of the design Y (as in [2, Corollary 2C.1]). For

this we need three ingredients involving one choice of a suitable prime $q > h$, a suitable choice in Lemma 5.3 of the m_i such that $\pi = \prod_i m_i$ is divisible by k, and infinitely many s (chosen below in (I)):

(1) a 2-$(qk, k, 1)$-design W having a cyclic automorphism group C of order k that is semiregular on points and whose q point-orbits are blocks of W [14, Theorem 1.2 and pp. 308–309],
(2) a transversal design $T = TD(k, (k-1)h\pi s)$ having a cyclic automorphism group of order k that is semiregular on both points and lines (T exists for all sufficiently large s by Lemma 5.3), and
(3) a 2-$(y, k, 1)$-design Y with $y := 1 + k(k-1)(\pi/k)s$, and an arbitrary point X of Y (Y exists for all sufficiently large s [13, Theorem 1.1]). (Note that we do not have any information concerning automorphisms of Y.)

Moreover, we require that

(4) $p := 1 + qk \cdot (k-1)\pi s = 1 + |W|(y-1)$ is prime, and
(5) $(p-1, h)$ divides some power of k (a condition in the proposition).

We will proceed in four steps.

(I) *Number Theory*: π, *p and s*. Write $h = h_0 h'$, where $(k, h') = 1$ and all primes dividing h_0 also divide k. Then $(k(k-1), h') = 1$ since $(k-1, h) = 1$, so h' is odd. We may assume that h_0 divides the product π of the m_i used in Lemma 5.3.

We have a prime $q > h$ in (1), so $(qk(k-1)\pi, h') = 1$ since $(k, h') = 1 = (k-1, h)$. Let t be a positive integer such that $qk(k-1)\pi t \equiv 1 \pmod{h'}$. Then $(t, h') = 1$ and $\big(1 + qk(k-1)\pi t, qk(k-1)\pi h'\big) = \big(1 + qk(k-1)\pi t, h'\big) = (1+1, h') = 1$ since h' is odd. By Dirichlet's Theorem there are infinitely many integers f such that

$$p := 1 + qk(k-1)\pi t + qk(k-1)\pi h' f$$

is a prime.

Choose $s := t + h' f$ with f so large that the designs in (2) and (3) exist. Clearly (4) holds.

Moreover, $(p-1, h)$ divides $\big(q(k-1)(t + h' f), h'\big)k\pi h_0 = \big((k-1)t, h'\big)k\pi h_0 = k\pi h_0$, which divides some power of k, as required in (5).

Now that we have W, T and Y we need to turn the set $U = X \cup \big(W \times Z\big)$ of size p into a design.

(II) *The cyclic group* $\bar{C}$. We need *a group* $\bar{C} \cong C$ *of permutations of* U. Extend each $c \in C$ (cf. (1)) to a permutation $\bar{c}$ of U that fixes the point in X and sends $(a, z) \mapsto (a^c, z)$ for $a \in W$, $z \in Z$. Then $\bar{C} = \{\bar{c} \mid c \in C\}$ is a group of k permutations of U *fixing* X *and semiregular on the remaining points.* This is not yet a group of automorphisms of anything.

We will construct the design in Theorem 4.1 by placing (in (III)) copies of the transversal design T in the sets $B \times Z$ of size $k(y-1)$ arising from blocks B of W, and (in (IV)) copies of Y in the sets $Y_a := X \cup \big(a \times Z\big)$ of size y for $a \in W$.

(III) *Copies of* T. We will use copies of the transversal design T in (2) as the transversal designs occurring in the proof of Theorem 4.1.

In view of the point-orbits in (1), the stabilizer in C of a block of W is either 1 or C.

Let $\mathcal{B}$ be a set of orbit representatives of C on the blocks of W. *If* $B \in \mathcal{B}$ *let* $T_{B\times Z} \cong T$ *have* $B \times Z$ *as its set of points and* $\{b \times Z \mid b \in B\}$ *as its set of groups.* If the stabilizer of B in C is 1, $T_{B\times Z}$ is placed in $B \times Z$ arbitrarily. If B is a C-orbit we have to be more careful. Initially, place $T_{B\times Z}$ arbitrarily. We then have two semiregular cyclic permutation groups of order k on $B \times Z$: one is the restriction $\bar{C}^{B\times Z}$ of $\bar{C}$ to $B \times Z$, and the other is the cyclic automorphism group of $T_{B\times Z}$ provided by (2). These cyclic groups of order k are

conjugate by an element of $\mathrm{Sym}\big(B \times Z\big)$; conjugate by such an element in order to assume that $T_{B\times Z}$ has been placed in $B \times Z$ so that the cyclic groups coincide, and hence so that $\bar{C}^{B\times Z} \leq \mathrm{Aut}\, T_{B\times Z}$.

For $B \in \mathcal{B}$ and $c \in C$ let $T_{B^c\times Z}$ denote the transversal design $(T_{B\times Z})^{\bar{c}}$ having $(B \times Z)^{\bar{c}} = B^c \times Z$ as its set of points. This is well-defined: if $B^c = B^{c'}$ then $\bar{c}'\bar{c}^{-1}$ induces the permutation $(\bar{c}'\bar{c}^{-1})^{B\times Z}$ of $B \times Z$, which is an automorphism of $T_{B\times Z}$ by the preceding paragraph, so $(T_{B\times Z})^{\bar{c}} = (T_{B\times Z})^{\bar{c}'}$.

(IV) *Copies of* Y. Next we place *copies of the design* Y *into the sets* $Y_a = X \cup \big(a \times Z\big)$, $a \in W$, in the same manner. Namely, let $\mathcal{W}$ be a set of orbit representatives of C on the points of W. For $a \in \mathcal{W}$ place a copy of the design Y in Y_a using the bijection $X \mapsto X$, $z \mapsto (a, z)$ with $z \in Z$; then let $Y_{a^c} := (Y_a)^{\bar{c}}$ for $c \in C$. As usual, this is well-defined since $a^c = a^{c'}$ implies that $c = c'$ by semiregularity (cf. (1)).

Using the construction in the proof of Theorem 4.1 we obtain a 2-$(p, k, 1)$-design U having $\bar{C}$ as a group of k automorphisms that fixes the point X and is semiregular on the remaining points. □

Proof of Theorem 1.3 Let $h = |G|$ and $p > h$ be as in the preceding proposition. We imitate the proof of Theorem 2.2, regarding G as a group of automorphisms of $\mathbf{A} = \mathrm{AG}(d, p)$ for any sufficiently large d. Let $L \in \mathcal{L}$, where $\mathcal{L}$ is a set of representatives of the orbits of G on the lines of $\mathbf{A}$. Then G_L^L has order dividing $\big(p(p-1), |G|\big) = (p-1, |G|)$; by the proposition, this divides some power of k, and hence divides k by an hypothesis of the theorem.

The cyclic group G_L^L fixes a point and is semiregular on the remaining points. After identifying L with the set of points of the design U in Proposition 5.4 and conjugating by an element of $\mathrm{Sym}(L)$, we may assume that G_L^L is contained in the cyclic group of order k provided by the proposition. Thus, L is the set of points of a design D_L, isomorphic to U, such that $G_L^L \leq \mathrm{Aut}\, D_L$.

Now complete the proof by repeating the last three paragraphs of the proof of Theorem 2.2. □

6 Large designs

The Doyen-Wilson Theorem [6] states that, whenever $y \geq 2x+1$ and there are Steiner triple systems on y and x points, there is a Steiner triple system on y points having a subsystem on x points. The following is a significant generalization of that result [7]:

Theorem 6.1 *If* $k \geq 3$ *then there is an integer* $x_0(k) > k$ *such that, if* $x > x_0(k)$, $y > xk$, $x - 1 \equiv y - 1 \equiv 0 \pmod{k-1}$ *and* $x(x-1) \equiv y(y-1) \equiv 0 \pmod{k(k-1)}$, *then there is a* 2-$(y, k, 1)$*-design having an* x*-point subdesign.*

We use this for a result concerning large designs ($n(k)$ appears in Remark 4.2):

Proposition 6.2 *Let* $\mathcal{S}$ *be a set of* 2-$(u, k, 1)$*-designs, let* $\bar{\mathcal{S}}$ *be the set of all such* u *that occur for* $\mathcal{S}$, *and let* $w \in \bar{\mathcal{S}}$. *Assume that, if* x *and* y *are as in* Theorem 6.1 *with* $y - x > n(k)$, *then* $x + w(y - x) \in \bar{\mathcal{S}}$.

Then $\bar{\mathcal{S}}$ *contains all sufficiently large* u *satisfying the divisibility conditions for a* 2-$(u, k, 1)$*-design.*

Our argument imitates [3]. Note that the hypothesis involves only the initial existence of one $w \in \bar{\mathcal{S}}$.

Proof For $x_0(k)$ in Theorem 6.1, let $x_1 > x_0(k) > k$ be any representative for a congruence class (mod $k(k-1)$) of integers such that there exists a 2-$(x_1, k, 1)$-design. Consider any integer $a \geq wx_1n(k) \geq wx_1$ (cf. (4.1)). Choose $y - x = x_1k(k-1)a$, so $y - x > a > n(k)$, and then choose $x = x_1 + k(k-1)t$ with $0 \leq t < a$, so $x \geq x_1 > x_0(k)$. Then x and $y = x_1 + x_1k(k-1)a + k(k-1)t$ satisfy $y > kx$. (For, since $t < a$ and $x_1 > k$, we have $y - kx = (k-1)\big(-x_1 + x_1ka - k(k-1)t\big)$, where $x_1(ka-1) - k(k-1)t > k(ka-1) - k(k-1)a > 0$.)

Since x and y satisfy the divisibility conditions and the requirements $x > x_0(k)$ and $y > kx$ in Theorem 6.1, there is a 2-$(y, k, 1)$-design having an x-point subdesign. Theorem 4.1 also needs a $TD(k, y-x)$, which exists since $y-x > n(k)$. By hypothesis, Theorem 4.1 produces a 2-$(u, k, 1)$-design such that

$$u := x + w(y-x) \in \bar{\mathcal{S}}, \text{ with } u = x_1 + wx_1k(k-1)a + k(k-1)t. \tag{6.1}$$

Here $u - 1 \equiv x_1 - 1 \equiv 0 \pmod{k-1}$ and $u(u-1) \equiv 0 \pmod{k(k-1)}$. We will show that *the set of all u obtained in (6.1) contains the set of all sufficiently large $u \equiv x_1 \pmod{k(k-1)}$ satisfying these divisibility conditions.*

Given a, we have $y-x = x_1k(k-1)a$ and $x = x_1+k(k-1)t$. By choosing $t = 0, \ldots, a-1$ in (6.1), we realize

$$u = x_1 + wx_1k(k-1)a, \ldots, x_1 + wx_1k(k-1)a + k(k-1)(a-1).$$

For $y - x = x_1k(k-1)(a+1)$, we realize

$$u = x_1 + wx_1k(k-1)(a+1), \ldots, x_1 + wx_1k(k-1)(a+1) + k(k-1)a.$$

In order not to leave any gaps, we require that these intervals abut or overlap. This occurs as long as $x_1 + wx_1k(k-1)a + k(k-1)a \geq x_1 + wx_1k(k-1)(a+1)$, that is, $a \geq wx_1$, which is a condition already satisfied by a. So we can achieve all sufficiently large $x \equiv x_1 \pmod{k(k-1)}$.

Now let $x_1 > x_0(k)$ run through a set of representatives for the congruence classes mod $k(k-1)$ that satisfy the divisibility conditions for a 2-$(x_1, k, 1)$-design. □

7 Theorem 1.1

We call an automorphism group of a design 1-*blocked* if the set-stabilizer of any block is the identity on the block; our basic example was in Remark 2.7. This notion is preserved by the construction in Sect. 4:

Proposition 7.1 *Let $k \geq 3$ and let G be a 1-blocked automorphism group of a 2-$(w, k, 1)$-design W. Then a 2-$(y, k, 1)$-design Y with a subdesign X on x points, together with a transversal design $TD(k, y-x)$, produce a 2-$(w(y-x)+x, k, 1)$-design U such that G is isomorphic to a 1-blocked subgroup of* Aut U.

Proof We use the construction and notation in the proof of Theorem 4.1. Each $g \in G$ induces on U the permutation $\bar{g}$ sending $b \mapsto b$ and $(a, z) \mapsto (a^g, z)$ for $b \in X$, $a \in W$, $z \in Z$. Clearly $G \cong \bar{G} := \{\bar{g} \mid g \in G\}$.

For each orbit-representative A of G on the blocks of W we have a transversal design $TD_{A\times Z}$ whose set of points is $A \times Z$ and whose set of groups is $\{a \times Z \mid a \in A\}$. If $g \in G$ then $(A \times Z)^{\bar{g}} = A^g \times Z$ for a block A^g of W; let $TD_{A^g\times Z} := (TD_{A\times Z})^{\bar{g}}$. As in the proof of Theorem 2.2 this is well-defined: if $A^g \times Z = A^{g'} \times Z$ with $g, g' \in G$ then

$A^g = A^{g'}$, so $g'g^{-1} = 1$ on A since G is 1-blocked, and hence $(TD_{A\times Z})^{\bar g} = (TD_{A\times Z})^{\bar g'}$ since $\bar g'\bar g^{-1} = 1$ on $A \times Z$.

By the construction in Sect. 4, each $\bar g$ permutes the designs $TD_{A'\times Z}$ with A' a block of W, and is the identity on any other block of U (i. e., a block of X, or else $a \times B$ if $a \in W$ or $x \cup \big(a \times (B - x)\big)$ if $B \cap X = x$). Thus, $\bar G \le \mathrm{Aut}\, U$.

We need to verify that $\bar G$ is 1-blocked. Consider a block E of U fixed by $\bar g \in \bar G$. By Sect. 4, either E is contained in $X \cup (a \times B)$ for $a \in W$ and a block B of Y, or E is a block of some $TD_{A\times Z}$. In the former case it is clear that $\bar g = 1$ on E, so we are left with E in $TD_{A\times Z}$. In view of the construction in Sect. 4, A is uniquely determined by E and hence is fixed by g. Since G is 1-blocked on W, it follows that $g = 1$ on A. Then $\bar g = 1$ on $A \times Z$ and hence on E. Thus, $\bar G$ is a 1-blocked subgroup of $\mathrm{Aut}\, U$. □

Remark 7.2 An automorphism group of even order cannot be 1-blocked. For, an involution interchanges two points, hence fixes the block containing them and acts nontrivially on that block.

Proof of Theorem 1.1 Apply Proposition 6.2 to the set $\mathcal{S}$ of 2-$(v, k, 1)$-designs whose automorphism group has a 1-blocked subgroup isomorphic to G. By Theorem 2.2 and Remark 2.7, $\mathcal{S}$ contains some 2-$(v, k, 1)$-design.

We defined $n(k)$ in Remark 4.2 and $x_0(k)$ in Theorem 6.1. Let $x > \max(n(k), x_0(k))$ and $y > kx$ be integers such that $x - 1 \equiv y - 1 \equiv 0 \pmod{k-1}$ and $x(x-1) \equiv y(y-1) \equiv 0 \pmod{k(k-1)}$. By Theorem 6.1 there is a 2-$(y, k, 1)$-design having an x-point subdesign. Since $y - x > kx - x > n(k)$ there is a $TD(k, y - x)$ by (4.1). Then $x + v(y - x) \in \bar{\mathcal{S}}$ by Proposition 7.1. Now use Proposition 6.2. □

8 Conjectures

Our theorems are significantly weaker than the corresponding results in [1,5,8], where G is isomorphic to the *full* automorphism group of the constructed design. We conclude with a conjecture concerning affine spaces that would produce designs with this stronger property.

Conjectur 8.1 Given: *an integer* $s \ge 14$, *a prime* $p \equiv 1\,(mod\ s)$, *and an affine space* $\mathbf{A}'$ *having the same set of points as the original affine space* $\mathbf{A} = \mathrm{AG}(d, p)$, *such that*
for any subspaces X *of* $\mathbf{A}$ *and* Y' *of* $\mathbf{A}'$,
either $X \cap Y' = \emptyset$ *or* $|X \cap Y'| \equiv 1\ (mod\ s)$.

Conjecture: $\mathbf{A} = \mathbf{A}'$ if d is sufficiently large.

Note that it is essential here that p is prime. For suppose that $p = p_0^e > p_0$ for a prime $p_0 \equiv 1 \pmod s$. Let $\mathbf{A}_0 = \mathrm{AG}(ed, p_0)$, let $\mathbf{A}$ be the set of affine $\mathbb{F}_p$-subspaces of $\mathbf{A}_0$. If $g \in \mathrm{AGL}(dn, p_0) - \mathrm{AGL}(d, p)$ then $\mathbf{A}' := \mathbf{A}^g$ provides a counterexample to the conclusion in the conjecture.

The condition $s \ge 14$ reflects the fact that 14 is the smallest integer $s = k - 1 \ge 2$ such that neither s nor $s + 1$ is a prime power, so that [1,8] do not apply.

Theorem 8.2 *Assume that the preceding conjecture is correct. Under the hypotheses in any of* Theorems 1.1–1.3, *for infinitely many* v *there is a* 2-$(v, k, 1)$*-design* D *such that* $G \cong \mathrm{Aut}\, D$.

Proof We may assume that $p > s := k - 1 \ge 14$. Each theorem in Sect. 1 uses 2-$(p, k, 1)$-designs appearing in Theorems 2.1 or 3.2, or Proposition 5.4. In the situation of any of

the theorems in Sect. 1, there are 2-$(p, k, 1)$-designs E_1, E_2, E_3 with AG$(1, p)$ as their set of points such that there is no isomorphism between any two of these designs that lies in AGL$(1, p)$. (Namely, start with a design E_1, and for $i = 2, 3$ apply an i-cycle of the points to the blocks of E_1 in order to obtain the blocks of E_i.)

Let $d > 4$ be as in the proofs, so we are using $\mathbf{A} = \mathrm{AG}(d, p)$ based on a d-space V. Let $\{v_1, \ldots, v_d\}$ be a basis of V. There is a connected graph Γ with vertex set $\{v_1, \ldots, v_d\}$ such that $G \cong \mathrm{Aut}\,\Gamma$.

Let $c := \sum_1^d v_t$. Place E_1 in each affine 1-space $\langle v_i \rangle$, place E_2 in each affine 1-space $\langle v_i + v_j \rangle + c$ such that $\{v_i, v_j\}$ is an edge of Γ, and place E_3 in every other affine 1-space of $\mathbf{A}$. (Note that, since $d > 4$, if $\langle v_i + v_j \rangle + c = \langle v_{i'} + v_{j'} \rangle + c$ then $\{i, j\} = \{i', j'\}$.)

This produces a 2-$(p^d, k, 1)$-design D with G (isomorphic to) a subgroup of $\mathrm{Aut}\,D$. (Compare the construction in [8].)

Let $h \in \mathrm{Aut}\,D$ and consider the affine space $\mathbf{A}' = \mathbf{A}^h$. If X and Y' are subspaces of $\mathbf{A}$ and $\mathbf{A}'$, respectively, and if $X \cap Y' \neq \emptyset$, then $X \cap Y'$ is the intersection of subdesigns and so is a subdesign of D. Then $|X \cap Y'| \equiv 1 \pmod{s}$. Thus, $\mathbf{A}^h = \mathbf{A}$ by our hypothesis concerning Conjecture 8.1, so h is an automorphism of $\mathbf{A}$, and hence permutes the lines of $\mathbf{A}$. Then h also permutes the designs we have placed inside these lines, so h permutes the lines $\langle v_i \rangle$. The intersection of these lines is 0, so h is a linear transformation. By construction, h also permutes the lines $\langle v_i + v_j \rangle + c$, so it induces an automorphism of Γ, and hence agrees with some $g \in G = \mathrm{Aut}\,\Gamma$ in its action on the lines $\langle v_i \rangle$. Now $h' := hg^{-1}$ fixes each line $\langle v_i \rangle$, and hence is a diagonal transformation: $v_t^{h'} = a_t v_t$ for some $a_i \in K^*$ and all t. Also h' fixes each edge of Γ: $\langle v_i + v_j \rangle + c = (\langle v_i + v_j \rangle + c)^{h'} = \langle a_i v_i + a_j v_j \rangle + \sum_1^d a_t v_t$. It follows that all $a_t = 1$ for $t \neq i, j$, so $h' = 1$ since Γ is connected, and then $h \in G$. □

Remark 8.3 The fact that $X \cap Y'$ is a subdesign imposes arithmetic and structural conditions that can be included in the hypotheses of the above conjecture.

Acknowledgements I am grateful to Peter Dukes for assistance with [7], and to Jean Doyen for many helpful comments. This research was supported in part by funding from the Simons Foundation.

References

1. Babai L.: On the abstract group of automorphisms. In: Combinatorics (Swansea, 1981). LMS Lecture Notes 52, Cambridge University Press, Cambridge-New York, pp. 1–40 (1981).
2. Bose R.C., Shrikhande S.S.: On the composition of balanced incomplete block designs. Can. J. Math. **12**, 177–188 (1960).
3. Cameron P.J.: Embedding partial Steiner triple systems so that their automorphisms extend. J. Comb. Des. **13**, 466–470 (2005).
4. Chowla S., Erdös P., Straus E.G.: On the maximal number of pairwise orthogonal Latin squares of a given order. Can. J. Math. **12**, 204–208 (1960).
5. Doyen, J., Kantor, W.M.: Automorphism groups of Steiner triple systems (submitted).
6. Doyen J., Wilson R.M.: Embeddings of Steiner triple systems. Disc. Math. **5**, 229–239 (1973).
7. Dukes P., Lamken E.R., Ling A.C.H.: An existence theory for incomplete designs. Can. Math. Bull. **59**, 287–302 (2016).
8. Kantor W.M.: Automorphism groups of designs with $\lambda = 1$. Disc. Math. **342**, 2886–2892 (2019).
9. Kantor W.M.: 2-Transitive and flag-transitive designs. In: Arasu K.T., et al. (eds.) Coding Theory, Design Theory, Group Theory: Proc Marshall Hall Conf, pp. 13–30. Wiley, New York (1993).
10. Lamken E.R., Wilson R.M.: Decompositions of edge-colored complete graphs. JCT(A) **89**, 149–200 (2000).
11. Moore E.H.: Concerning triple systems. Math. Ann. **43**, 271–285 (1893).
12. Wilson R.M.: Concerning the number of mutually orthogonal Latin squares. Disc. Math. **9**, 181–198 (1974).

13. Wilson R.M.: Constructions and uses of pairwise balanced designs. In: Hall M. Jr., van Lint J.H. (eds.) Combinatorics, pp. 18–41. Math. Centrum, Amsterdam (1974).
14. Wilson R.M.: Existence of Steiner systems that admit automorphisms with large cycles. In: Arasu K.T., Seress A. (eds.) Codes and Designs, pp. 305–312. Ohio State University Math. Res. Inst. Publ. 10, (2002).