CONWAY GROUPOIDS, REGULAR TWO-GRAPHS AND SUPERSIMPLE DESIGNS

NICK GILL, NEIL I. GILLESPIE, CHERYL E. PRAEGER, AND JASON SEMERARO

ABSTRACT. A $2-(n,4,\lambda)$ design $(\Omega,\mathcal{B})$ is said to be supersimple if distinct lines intersect in at most two points. From such a design, one can construct a certain subset of $\mathrm{Sym}(\Omega)$ called a "Conway groupoid". The construction generalizes Conway's construction of the groupoid M_{13}. It turns out that several infinite families of groupoids arise in this way, some associated with 3-transposition groups, which have two additional properties. Firstly the set of collinear point-triples forms a regular two-graph, and secondly the symmetric difference of two intersecting lines is again a line. In this paper, we show each of these properties corresponds to a group-theoretic property on the groupoid and we classify the Conway groupoids and the supersimple designs for which both of these two additional properties hold.

1. INTRODUCTION

In his famous paper [Con97], John Conway used a "game" played on the projective plane $\mathbb{P}_3$ of order 3 to construct the sporadic Mathieu group M_{12}, as well as a special subset of $\mathrm{Sym}(13)$ which he called M_{13}, and which could be endowed with the structure of a groupoid.

In recent work ([GGNS, GGS]), Conway's construction has been generalized to geometries other than $\mathbb{P}_3$, namely to supersimple $2-(n,4,\lambda)$ designs. In this more general context, the analogue of M_{13} is a subset of $\mathrm{Sym}(n)$ that is known as a *Conway groupoid*. The aim of this paper is to classify an infinite family of Conway groupoids with the remarkable property that they are subgroups of $\mathrm{Sym}(n)$. They also have links to regular two-graphs and to 3-transposition groups.

In order to state our main results, we briefly review the definition of a Conway groupoid (full definitions and background can be found in §2): we start with a $2-(n,4,\lambda)$ design $\mathcal{D} := (\Omega,\mathcal{B})$ in which any two lines intersect in at most two points. We call such designs *supersimple*, and note that distinct points a, b of $\mathcal{D}$ lie in λ lines $\{a,b,a_i,b_i\}$ such that the points $a_1, \ldots, a_\lambda, b_1, \ldots, b_\lambda, \in \Omega$ are pairwise distinct. We associate with $\{a,b\}$ the permutation

$$(1.1) \qquad [a,b] = (a,b)\prod_{i=1}^{\lambda}(a_i,b_i),$$

of $\mathrm{Sym}(\Omega)$, which we call an *elementary move*; we also set $[a,a] = 1$, the identity permutation, for each $a \in \Omega$. For an arbitrary sequence of points $a_0, a_1, \ldots, a_k \in \Omega$, we extend this notation and define the permutation

$$[a_0, a_1, a_2, \ldots, a_k] := [a_0, a_1][a_1, a_2] \cdots [a_{k-1}, a_k],$$

called a *move sequence*. For a point $\infty \in \Omega$, the subset

$$(1.2) \qquad \mathcal{L}_\infty(\mathcal{D}) := \{[\infty, a_1, a_2, \ldots, a_k] \mid k \in \mathbb{Z}^+, \infty, a_1, \ldots, a_k \in \Omega\} \subset \mathrm{Sym}(\Omega)$$

is called the *Conway groupoid* associated with the point ∞, and the *hole-stabilizer* associated with ∞ is defined as

$$(1.3) \qquad \pi_\infty(\mathcal{D}) := \{[\infty, a_1, a_2, \ldots, a_{k-1}, \infty] \mid k \in \mathbb{Z}^+, \infty, a_1, \ldots, a_{k-1} \in \Omega\}.$$

It is an easy matter to check that the set $\pi_\infty(\mathcal{D})$ forms a subgroup of $\mathrm{Sym}(\Omega \setminus \{\infty\})$ and, moreover, its isomorphism class as a permutation group does not depend on the choice of the point ∞.

By way of example, if we consider, as Conway did, the design of points and lines of the projective plane $\mathbb{P}_3$, then we obtain $\mathcal{L}_\infty(\mathbb{P}_3) = M_{13}$ and $\pi_\infty(\mathbb{P}_3) = M_{12}$. In the search for other interesting Conway groupoids, two particularly interesting phenomena have arisen: firstly, it turns out that the Conway groupoid $\mathcal{L}_\infty(\mathcal{D})$ is sometimes not just a subset of $\mathrm{Sym}(\Omega)$, but a subgroup; secondly, by considering the set of collinear point-triples of $\mathcal{D}$, one can sometimes associate with $\mathcal{D}$ the structure of a *regular two-graph* (see Definition 2.2).[1] It turns out that these two properties, both separately and together, correspond to certain additional properties of the Conway groupoid, as our first main result makes clear:

---

[1]According to the first sentence of [Tay77], "regular two-graphs were introduced by G. Higman in his Oxford lectures as a means of studying Conway's sporadic simple group ·3 in its doubly transitive representation of degree 276."

Theorem A. *Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple $2 - (n, 4, \lambda)$ with $n > 2\lambda + 2$, and let $\mathcal{C}$ denote the set of all collinear triples of elements in Ω. Let $\infty \in \Omega$ and define $G := \mathcal{L}_\infty(\mathcal{D})$. Then the following hold.*

    (a) *If G is a group then G is primitive on Ω.*
    (b) *If $(\Omega, \mathcal{C})$ is a regular two-graph then $\pi_\infty(\mathcal{D})$ is transitive on $\Omega \setminus \{\infty\}$.*
    (c) *If $(\Omega, \mathcal{C})$ is a regular two-graph and G is a group then $\pi_\infty(\mathcal{D})$ is primitive on $\Omega \setminus \{\infty\}$.*

We remark that the condition $n > 2\lambda + 2$ is stated only for convenience. Any $2 - (n, 4, \lambda)$ design automatically satisfies $n \geqslant 2\lambda + 2$; furthermore full information concerning the Conway groupoids corresponding to supersimple $2 - (n, 4, \lambda)$ designs with $n = 2\lambda + 2$ is given by Proposition 5.3.

Our other main results concern Conway groupoids satisfying the conditions in part (c), together with the following additional property on the supersimple design $\mathcal{D} = (\Omega, \mathcal{B})$:

$$(\triangle) \qquad\qquad\qquad \text{if } B_1, B_2 \in \mathcal{B} \text{ such that } |B_1 \cap B_2| = 2, \text{ then } B_1 \triangle B_2 \in \mathcal{B}$$

where $B_1 \triangle B_2$ denotes the *symmetric difference* of the lines B_1 and B_2. (Observe that the condition $|B_1 \cap B_2| = 2$ implies that $|B_1 \triangle B_2| = 4$.) Our next result gives a classification of such groupoids. Its statement refers to elementary moves defined in (1.1), and also mentions 3-transposition groups, which are defined in Definition 2.10.

Theorem B. *Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple $2 - (n, 4, \lambda)$ design that satisfies $(\triangle)$, and let $\mathcal{E}$ be the set of elementary moves on $\mathcal{D}$. Let $\mathcal{C}$ be the set of collinear triples in $\mathcal{B}$ and suppose that $(\Omega, \mathcal{C})$ is a regular two-graph. Then, for $\infty \in \Omega$, $(\mathcal{L}_\infty(\mathcal{D}), \mathcal{E})$ is a 3-transposition group and, for some positive integer m, one of the following holds:*

    (a) $n = 2^m$ *and* $\mathcal{L}_\infty(\mathcal{D}) \cong (\mathbb{F}_2)^m$;
    (b) $n = 2^{m-1}(2^m \pm 1)$ *and* $\mathcal{L}_\infty(\mathcal{D}) \cong \mathrm{Sp}_{2m}(2)$;
    (c) $n = 2^{2m}$ *and* $\mathcal{L}_\infty(\mathcal{D}) \cong 2^{2m}.\mathrm{Sp}_{2m}(2)$.

Our proof of Theorem B is independent of the Classification of Finite Simple Groups (CFSG); let us briefly explain our approach: we remarked above that when $n = 2\lambda + 2$, Proposition 5.3 gives full information and, in particular, it implies that Theorem B, part (a) holds. In addition, one can prove fairly easily that the assumptions of Theorem B imply that $\mathcal{L}_\infty(\mathcal{D})$ is a group (Lemma 2.6). For the situation where $n > 2\lambda + 2$ we now apply Theorem A, part (c) to conclude that $\mathcal{L}_\infty(\mathcal{D})$ is 2-primitive on Ω.

At this point, if were we happy to use CFSG, we could invoke Taylor's classification [Tay92] of 2-transitive regular two-graphs. However we prefer to avoid reliance on the simple group classification, and instead we apply Fischer's classification of finite 3-transposition groups; this is done in §5.

It is natural to ask at this point whether all of the possibilities for $\mathcal{L}_\infty(\mathcal{D})$ that are listed in Theorem B can occur. The answer to this question is "yes" and we now present three families of designs that demostrate this. These families will also be of central importance in our final major result, Theorem C, below.

Example 1.1. The *Boolean quadruple system of order 2^m*, where $m \geqslant 2$, is the design $\mathcal{D}^b = (\Omega^b, \mathcal{B}^b)$ such that Ω^b is identified with the set of vectors in $\mathbb{F}_2^m$, and

$$\mathcal{B}^b := \{\{v_1, v_2, v_3, v_4\} \mid v_i \in \Omega^b \text{ and } \sum_{i=1}^4 v_i = \mathbf{0}\}.$$

Equivalently, we can define
$$\mathcal{B}^b = \{v + W \mid v \in \Omega^b, W \leqslant \mathbb{F}_2^m, \dim(W) = 2\};$$
that is, $\mathcal{B}^b$ is the set of all affine subplanes of Ω^b. It is easy to see that $\mathcal{D}$ is both a 3-$(2^m, 4, 1)$ Steiner quadruple system and a supersimple 2-$(2^m, 4, 2^{m-1} - 1)$ design. Moreover, $\mathcal{D}^b$ satisfies property $(\triangle)$ (see Lemma 2.8). In what follows, we will often make statements like "$\mathcal{D}$ is a Boolean system" to mean that $\mathcal{D}$ is a Boolean quadruple system of order 2^m for some integer $m \geqslant 2$.

To describe the other two families, we need the following set-up: Let $m \geqslant 2$ and $V := (\mathbb{F}_2)^{2m}$ be a vector space equipped with the standard basis. Define

$$(1.4) \qquad\qquad e := \begin{pmatrix} 0_m & I_m \\ 0_m & 0_m \end{pmatrix}, \qquad f := \begin{pmatrix} 0_m & I_m \\ I_m & 0_m \end{pmatrix} = e + e^T,$$

where I_m and 0_m represent the $m \times m$ identity and zero matrices respectively. Write elements of V as row vectors and define $\varphi(u, v)$ as the alternating bilinear form $\varphi(u, v) := ufv^T$. Also, write $\theta(u) := ueu^T \in \mathbb{F}_2$, so that

$$\theta(u + v) + \theta(u) + \theta(v) = \varphi(u, v).$$

(Note that the right hand side equals $uev^T + veu^T$ while the left hand side is $u(e + e^T)v^T$.) Finally, for each $v \in V$ define $\theta_v(u) := \theta(u) + \varphi(u, v)$, and note that $\theta_0 = \theta$.

Example 1.2. Let $\mathcal{D}^a = (\Omega^a, \mathcal{B}^a)$, where $\Omega^a := V$ and

$$\mathcal{B}^a := \{\{v_1, v_2, v_3, v_4\} \mid v_1, v_2, v_3, v_4 \in \Omega^a, \sum_{i=1}^4 v_i = \mathbf{0}, \sum_{i=1}^4 \theta(v_i) = 0\}.$$

By [GGS, Theorem B], $\mathcal{L}_\infty(\mathcal{D}^a) \cong 2^{2m} . \mathrm{Sp}_{2m}(2)$, while $\pi_\infty(\mathcal{D}^a) \cong \mathrm{Sp}_{2m}(2)$. Indeed, taking ∞ to be the zero vector in V, it turns out that $\pi_\infty(\mathcal{D}^a) = \mathrm{Isom}(V, \varphi)$, the isometry group of the formed space (V, φ).

Example 1.3. For $\varepsilon \in \mathbb{F}_2$, let $\mathcal{D}^\varepsilon = (\Omega^\varepsilon, \mathcal{B}^\varepsilon)$, where $\Omega^\varepsilon := \{\theta_v \mid v \in V, \theta(v) = \varepsilon\}$ and

$$\mathcal{B}^\varepsilon := \{\{\theta_{v_1}, \theta_{v_2}, \theta_{v_3}, \theta_{v_4}\} \mid \theta_{v_1}, \theta_{v_2}, \theta_{v_3}, \theta_{v_4} \in \Omega^\varepsilon, \sum_{i=1}^4 v_i = \mathbf{0}\}.$$

By [GGS, Theorem B], $\mathcal{L}_\infty(\mathcal{D}^\varepsilon) \cong \mathrm{Sp}_{2m}(2)$, the isometry group of φ, while $\pi_\infty(\mathcal{D}^\varepsilon) \cong \mathrm{O}_{2m}^{\varepsilon'}(2)$, where $\varepsilon' = \pm$ and $\varepsilon = (1 - \varepsilon'1)/2$ (as an integer in $\{0, 1\}$).

Each of the designs in Examples 1.1–1.3 satisfies property ($\triangle$) and their collinear triples form the lines of a regular two-graph (see Lemmas 2.8 and 2.9), thereby proving that the three outcomes listed in Theorem B really occur. Our final main result asserts that, in fact, the examples just given are the only designs that satisfy the assumptions of Theorem B.

Theorem C. *Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple $2 - (n, 4, \lambda)$ design that satisfies ($\triangle$). Let $\mathcal{C}$ be the set of collinear triples in $\mathcal{B}$ and suppose that $(\Omega, \mathcal{C})$ is a regular two-graph. Then there is an integer m such that $\mathcal{D}$ is a $2 - (f(m), 4, f(m-1) - 1)$ design, where one of the following holds:*
  (a) *$f(m) = 2^m$ and $\mathcal{D} = \mathcal{D}^b$ as in Example 1.1;*
  (b) *$f(m) = 2^{2m}$ and $\mathcal{D} = \mathcal{D}^a$ as in Example 1.2;*
  (c) *$f(m) = 2^{m-1}(2^m + \varepsilon'.1)$ and $\mathcal{D} = \mathcal{D}^\varepsilon$ is isomorphic to one of the designs in Example 1.3.*

Our proof of Theorem C is entirely independent of Theorem B; indeed the whole approach to the proof is different from that for Theorem B because we use the theory of *polar spaces*. More precisely, we prove in Proposition 6.3 that, for any point $\infty \in \Omega$, the assumptions of Theorem B (along with the condition $n > 2\lambda + 2$) imply that $(\Omega \backslash \{\infty\}, \mathcal{C}_\infty)$ is a polar space in the sense of Buekenhout–Shult. (Here $\mathcal{C}_\infty$ is the set of all triples of points in $\Omega \backslash \{\infty\}$ which occur in a line with ∞.) In fact, the polar space $(\Omega \backslash \{\infty\}, \mathcal{C}_\infty)$ has the extra property that all lines in the space contain exactly three points. Such polar spaces were characterized in a special case by Shult [Shu72] and then later, in full generality, by Seidel [Sei73].[2] We use the result of Seidel in §6 to give a fairly short proof of Theorem C; our presentation of Seidel's result in that section (Theorem 6.4) is couched in graph-theoretic terminology.

It is natural to ask about the connection between Theorems B and C. Although the two proofs given in this paper are independent of one another, the two theorems are in fact equivalent. That Theorem C implies Theorem B is an easy consequence of [GGS, Theorem B]; the reverse implication is slightly more difficult and is not presented here.

We have chosen to give two proofs because we believe that the different approaches (one algebraic, one geometric) shed complementary light on the set-up being studied here. What is more, while a proof of Theorem B that goes via Theorem C appears somewhat shorter, an approach which goes via Theorem A (and hence a *group-theoretic* analysis of $\mathcal{L}_\infty(\mathcal{D})$) is likely to be applicable in more general contexts (see Question 1.6 below).

1.1. **Context and open problems.** As we mentioned above, the study of Conway groupoids was inspired by Conway's construction of M_{13} in [Con97]. This was generalized in [GGNS] to the context of supersimple $2 - (n, 4, \lambda)$ designs, and a classification programme for such groupoids was initiated in that paper and continued in [GGS]. Theorems B and C may be regarded as contributions to this programme. With this classification problem in mind, several questions arise.

Question 1.4. *Can Theorems B and C be extended to cover the situation where ($\triangle$) does not hold?*

Our current state of knowledge about Conway groupoids suggests that M_{13} is particularly special. To see this, we define a Conway groupoid $\mathcal{L}_\infty(\mathcal{D})$ associated to a supersimple design $\mathcal{D}$ to be *exotic* if $\mathcal{L}_\infty(\mathcal{D})$ is not a group and $\pi_\infty(\mathcal{D})$ is primitive. Thus M_{13} is exotic, and [GGS, Theorem D] gives strong bounds on the possible parameters of a design $\mathcal{D}$ for which $\mathcal{L}_\infty(\mathcal{D})$ is exotic.

---

[2]Note that [Sei73] is an internal university report; it can be accessed in the volume of Seidel's selected works [Sei91].

Question 1.5. *Is M_{13} the only exotic Conway groupoid?*

More broadly, we ask whether structures other than supersimple designs could be used to construct Conway groupoids.

Question 1.6. *Are there alternative combinatorial structures which can be used to define interesting groupoids?*

In unpublished work, the authors address Question 1.6 as follows: we consider a more general framework under which to define Conway groupoids by replacing the supersimple design $\mathcal{D}$ with an abstract function $f : \Omega^2 \to \mathrm{Sym}(\Omega)$ that sends an unordered pair of points $\{a, b\}$ to an involution $[a, b]$. Several interesting examples arise in this context, and under certain conditions on f one can show that the structure of the resulting groupoid is tightly controlled.

1.2. **Structure of the paper.** In §2 we present background definitions and results concerning blocks designs, two-graphs, Conway groupoids and 3-transposition groups. We also prove that the designs presented in Examples 1.1–1.3 satisfy the assumptions of Theorems B and C. In §3 we prove Theorem A. The main result of §4 is Theorem 4.2 which is a precursor to Theorem B; the proof of Theorem B is completed in §5. Finally, in §6, we prove Theorem C.

1.3. **Acknowledgments.** The authors would like to thank Dr Ben Fairbairn and Dr Justin McInroy for their helpful comments. The last author would especially like to thank the University of Western Australia for its hospitality and for helping to finance a three week visit in April 2015.

2. BACKGROUND

2.1. **Block designs and two-graphs.** For positive integers t, k, n, λ such that $t \leqslant k \leqslant n$, a $t - (n, k, \lambda)$ design $(\Omega, \mathcal{B})$ consists of a finite set Ω of size n, whose elements are called the points of the design, together with a finite multiset $\mathcal{B}$ of subsets of Ω each of size k (called *lines*), such that any subset of Ω of size t is contained in exactly λ lines. Recall:

Definition 2.1. A $2 - (n, 4, \lambda)$ design $(\Omega, \mathcal{B})$ is *supersimple* if any two lines intersect in at most two points.

Note that a supersimple design is *simple*, that is, distinct liens correspond to distinct subsets of Ω.

Definition 2.2. A $2 - (n, 3, \mu)$ design $(\Omega, \mathcal{C})$ is a *regular two-graph* if for any 4-subset X of Ω, either $0, 2$ or 4 of the 3-subsets of X lie in $\mathcal{C}$. A subset X of Ω is *coherent* if every 3-subset of X lies in $\mathcal{C}$.

We note that each point of a $2 - (n, 3, \mu)$ regular two-graph $(\Omega, \mathcal{C})$ is contained in $\mu(n-1)/6$ triples in $\mathcal{C}$, hence the name 'regular'. The following result is [Tay77, Proposition 3.1].

Lemma 2.3. *Let $(\Omega, \mathcal{C})$ be a $2 - (n, 3, \mu)$ regular two-graph. Then there is a constant s such that each element of $\mathcal{C}$ is contained in exactly s coherent 4-subsets of Ω. Moreover, $n = 3\mu - 2s$.*

Corollary 2.4. *Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple $2 - (n, 4, \lambda)$ design such that $(\Omega, \mathcal{C})$ is a regular two-graph, where $\mathcal{C}$ is the set of collinear triples of $\mathcal{D}$. Then $n = 6\lambda - 2s$ where s is the number of coherent 4-subsets of Ω containing a given element of $\mathcal{C}$. In particular, n is even.*

Proof. Observe that $(\Omega, \mathcal{C})$ is a $2 - (n, 3, 2\lambda)$ design, and hence the result follows from Lemma 2.3. $\qquad\square$

2.2. **Moves and groupoids.** Let $\mathcal{D}$ be a supersimple $2 - (n, 4, \lambda)$ design. For distinct $a, b \in \Omega$, recall the definition of the elementary move from a to b in (1.1). Note that the right hand side of (1.1) is independent of the ordering of the lines, since the 'supersimple' condition means that $\{a_i, b_i\}$ is disjoint from $\{a_j, b_j\}$ for $i \neq j$. Recall also the definition of a move sequence $[x_0, x_1, \ldots, x_k] := [x_0, x_1] \cdot [x_1, x_2] \cdots [x_{k-1}, x_k]$. For a point $\infty \in \mathcal{B}$, we are interested in the following three subsets of $\mathrm{Sym}(\Omega)$:

(1) $\mathcal{L}(\mathcal{D})$, the set of all move sequences;
(2) $\mathcal{L}_\infty(\mathcal{D})$, the set of all move sequences starting at ∞, called the *Conway groupoid* of $\mathcal{D}$; and
(3) $\pi_\infty(\mathcal{D})$, the set of all move sequences which start and end at ∞, called the *hole-stabilizer* of $\mathcal{D}$.

Similarly we define $\mathcal{L}_x(\mathcal{D})$ and $\pi_x(\mathcal{D})$ for arbitrary $x \in \Omega$. We remark that $\pi_\infty(\mathcal{D})$ is a subgroup of $\mathrm{Sym}(n-1)$, and is permutationally isomorphic to $\pi_x(\mathcal{D})$ for each x (so we may refer to it as *the* hole-stabilizer of $\mathcal{D}$). Similarly, the isomorphism type of $\mathcal{L}_\infty(\mathcal{D})$ as a groupoid does not depend on the choice of ∞. See [GGS, §2.2] for more discussion. Finally, for distinct $x, y \in \Omega$, we write

$$(2.1) \qquad\qquad \overline{x, y} := \{ z \in \Omega \,|\, \text{there exists } \ell \in \mathcal{B} \text{ such that } x, y, z \in \ell \}$$

and note in particular that $\overline{x, y}$ contains x and y. The next result is a simple observation and we omit the proof.

Lemma 2.5. *Let $\mathcal{D}$ be a supersimple $2 - (n, 4, \lambda)$ design. The following hold:*

(i)
$$\mathcal{L}_\infty(\mathcal{D}) = \bigcup_{x \in \Omega} \pi_\infty(\mathcal{D}) \cdot [\infty, x],$$

(ii) $\pi_\infty(\mathcal{D}) = \langle [\infty, x, y, \infty] \mid x, y \in \Omega \rangle$.

Lemma 2.6. *Let $\mathcal{D}$ be a supersimple $2 - (n, 4, \lambda)$ design. Fix $\infty \in \Omega$ and define $G := \mathcal{L}_\infty(\mathcal{D})$. The following are equivalent:*

    (i) *G is a group;*
    (ii) *$G = \mathcal{L}(\mathcal{D}) = \langle [a, b] \mid a, b \in \Omega \rangle$;*
    (iii) *$\mathcal{L}(\mathcal{D}) = \mathcal{L}_x(\mathcal{D})$ for all $x \in \Omega$.*

Furthermore, if one (and therefore all) of these conditions hold, then G is transitive on Ω and $\mathrm{stab}_G(\infty) = \pi_\infty(\mathcal{D})$.

Proof. Write $H := \langle [a, b] \mid a, b \in \Omega \rangle$ and note that $G \subseteq \mathcal{L}(\mathcal{D}) \subseteq H$.

(i) implies (ii): Note that $[a, b] = [\infty, a] \cdot [\infty, a, b]$, and so $[a, b] \in G$ since G is a group. Hence $H \subseteq G$ and so $H = \mathcal{L}(\mathcal{D}) = G$ as required.

(ii) implies (iii): Observe that, for each $x \in \Omega$, we have $\mathcal{L}_x(\mathcal{D}) \subseteq H = G$, and each move sequence $[x, x_2, \ldots, x_k] = [x, \infty][\infty, x, x_2, \ldots, x_k]$, so $|\mathcal{L}_x(\mathcal{D})| = |[x, \infty] \cdot G| = |G|$. Thus $\mathcal{L}_x(\mathcal{D}) = G = \mathcal{L}(\mathcal{D})$, and (iii) follows.

(iii) implies (i): Let $g, h \in G$ and recall that $G = \mathcal{L}(\mathcal{D})$; let x be the last element of Ω in a move sequence corresponding to g. Now by (iii) there exist $y_i \in \Omega$ such that $h = [x, y_1, y_2 \ldots, y_l]$. Hence $g \cdot h \in G$ and G is closed under composition. Since G is finite this implies that G is a group.

To prove the final statement, suppose that G is a group. Now $\pi_\infty(\mathcal{D})$ clearly fixes ∞ and so is a subgroup of $\mathrm{stab}_G(\infty)$. Thus the length of the G-orbit containing ∞, namely $|G : \mathrm{stab}_G(\infty)|$, divides the index $|G : \pi_\infty(\mathcal{D})|$. However, by Lemma 2.5 (i), the index of $\pi_\infty(\mathcal{D})$ in G is equal to $|\Omega|$. It follows that G is transitive and $\mathrm{stab}_G(\infty) = \pi_\infty(\mathcal{D})$, as required. $\square$

Lemma 2.7. *For a supersimple $2 - (n, 4, \lambda)$ design $\mathcal{D}$, the following are equivalent:*

    (i) *for all $a, b, c, d \in \Omega$, $[a, b]^{[c,d]} = [a^{[c,d]}, b^{[c,d]}]$;*
    (ii) *for all $a, b, c \in \Omega$, $[a, b]^{[b,c]} = [a^{[b,c]}, c]$;*
    (iii) *for all $a, b, c \in \Omega$, $[b, c] = [a, b, c, a^{[b,c]}]$.*

In addition, if these conditions hold, then $\mathcal{L}_\infty(\mathcal{D})$ (where $\infty \in \Omega$) is a group of automorphisms of $\mathcal{D}$.

Proof. First we show that conditions (ii) and (iii) are equivalent. Writing $[a, b]^{[b,c]} = [b, c][a, b][b, c]$, we see that condition (ii) for a, b, c is equivalent to $[b, c] = [a, b][b, c][a^{[b,c]}, c]$. On the other hand, by the definition of a move sequence,
$$[a, b, c, a^{[b,c]}] = [a, b][b, c][c, a^{[b,c]}] = [a, b][b, c][a^{[b,c]}, c]$$
and hence condition (iii) for a, b, c is also equivalent to $[b, c] = [a, b][b, c][a^{[b,c]}, c]$. Thus conditions (ii) and (iii) are equivalent.

Next, if condition (i) holds, then taking (a, b, c, d) in this condition as (a, b, b, c) and noting that $b^{[b,c]} = c$, we obtain condition (ii) for a, b, c. Thus condition (i) implies condition (ii). Now assume that the equivalent conditions (ii) and (iii) hold, and let $a, b, c, d \in \Omega$. Note that $[c, d] = [b, c, d, b^{[c,d]}]$. Then using this and several applications of condition (ii) yields
$$[a, b]^{[c,d]} = [a, b]^{[b,c][c,d][d,b^{[c,d]}]} = [a^{[c,d]}, b^{[c,d]}].$$

We now prove the final statement. We first show that $G := \mathcal{L}_\infty(\mathcal{D})$ is a group. To achieve this, we prove by induction on k that each move sequence of length k can be written as a move sequence starting from any given point x of Ω and apply Lemma 2.6. The identity element is equal to $[x, x]$ by convention, and it follows from (iii) that each elementary move $[a_1, a_2]$ may be represented by a move sequence starting with x. Thus the assertion is true for $k \leqslant 2$. Suppose that $k > 2$ and the assertion holds for all move sequences of length less than k, and consider $g = [x_1, x_2, \ldots, x_k]$ and a given point x. By induction, there exist $y_1, y_2 \ldots, y_l \in \Omega$ and $z_1, z_2 \ldots, z_m \in \Omega$ such that:
$$[x_1, x_2] = [x, y_1, y_2 \ldots, y_l] \text{ and } [x_2, \ldots, x_k] = [y_l, z_1, \ldots, z_m].$$
Composing these two move sequences yields the required expression for g.

Lastly, suppose that $\{a, b, c, d\}$ is a line of $\mathcal{D}$, and let $g \in G$. Then g is a move sequence, and condition (i) applied several times implies that $[a, b]^g = [a^g, b^g]$. Then, since (c, d) is a 2-cycle in the elementary move $[a, b]$, it follows that (c^g, d^g) is a 2-cycle in the elementary move $[a^g, b^g]$. Therefore, $\{a^g, b^g, c^g, d^g\}$ is a line of $\mathcal{D}$. Thus $g \in \mathrm{Aut}(\mathcal{D})$, as needed. $\square$

2.3. **Examples.** In this section we prove that the three families of designs discussed in Examples 1.1, 1.2 and 1.3 satisfy the hypotheses of Theorem B and C.

Lemma 2.8. *Let $\mathcal{D}^b = (\Omega^b, \mathcal{B}^b)$ be a Boolean quadruple system of order 2^k, and let $\mathcal{C}^b$ be the set of collinear triples of $\mathcal{D}^b$. Then $(\Omega^b, \mathcal{C}^b)$ is a regular two-graph and $\mathcal{D}^b$ satisfies $(\triangle)$. Furthermore, $(\mathcal{L}_\infty(\mathcal{D}^b), \pi_\infty(\mathcal{D}^b)) = ((\mathbb{F}_2)^m, \mathrm{Id})$.*

Proof. An immediate consequence of the definition of a Boolean quadruple system is that it is a $3 - (2^k, 4, 1)$ design. Thus $\mathcal{C}^b$ contains all triples in Ω^b and (Ω^b, C^b) is the complete two-graph (hence, in particular, it is regular).

To see that $\mathcal{D}^b$ satisfies $(\triangle)$, consider intersecting lines $\{v_1, v_2, v_3, v_4\}$ and $\{v_1, v_2, v_5, v_6\}$ in $\mathcal{B}^b$. By definition

$$v_1 + v_2 + v_3 + v_4 = v_1 + v_2 + v_5 + v_6 = \mathbf{0}.$$

This implies that

$$v_1 + v_2 = v_3 + v_4 = v_5 + v_6$$

and we conclude immediately that $v_3 + v_4 + v_5 + v_6 = \mathbf{0}$. In other words $\{v_3, v_4, v_5, v_6\} \in \mathcal{B}^b$, so $\mathcal{D}^b$ satisfies $(\triangle)$. The last assertion is an immediate consequence of the definition of a Boolean quadruple system.

□

The fact that $(\Omega^a, \mathcal{C}^a)$ and $(\Omega^\varepsilon, \mathcal{C}^\varepsilon)$ are regular two-graphs goes back to Taylor [Tay92]. We give a self-contained proof here for the convenience of the reader:

Lemma 2.9. *Each design $\mathcal{D}$ in Example 1.2 or 1.3 satisfies $(\triangle)$ and the set $\mathcal{C}$ of collinear triples in $\mathcal{D}$ forms a regular two-graph. Furthermore, $(\mathcal{L}_\infty(\mathcal{D}^a), \pi_\infty(\mathcal{D}^a)) = (2^{2m}.\mathrm{Sp}_{2m}(2), \mathrm{Sp}_{2m}(2))$ and $(\mathcal{L}_\infty(\mathcal{D}^\varepsilon), \pi_\infty(\mathcal{D}^\varepsilon)) = (\mathrm{Sp}_{2m}(2), O_{2m}^{\varepsilon'}(2))$.*

The final sentence in the lemma requires the identification of Ω^a with a vector space V over the field $\mathbb{F}_2$, as described in Example 1.2. Recall that $\varphi : V \times V \to \mathbb{F}_2$ is a particular alternating form.

Proof. Define $\rho : V \times V \times V \to \mathbb{F}_2$ by $(a, b, c) \mapsto \varphi(a, b) + \varphi(a, c) + \varphi(b, c)$. Observe that the lines $\{v_1, v_2, v_3, v_4\}$ in $\mathcal{D}^a$ are precisely those 4-subsets of Ω for which $\sum_{i=1}^4 v_i = \mathbf{0}$ and $\rho(a, b, c) = 0$ for one (and hence any) 3-subset $\{a, b, c\}$ of $\{v_1, v_2, v_3, v_4\}$. Observe further that the lines in $\mathcal{D}^\varepsilon$ are precisely the lines $\{v_1, v_2, v_3, v_4\}$ in $\mathcal{D}^a$ with the property that $\theta_0(v_i) = \varepsilon$ for $1 \leqslant i \leqslant 4$. Since

$$\rho(a, b, c) + \rho(a, b, d) + \rho(a, c, d) + \rho(b, c, d) = 0$$

for any four points $a, b, c, d \in \Omega$, we conclude immediately that an even number of the 3-subsets of $\{a, b, c, d\}$ lies in $\mathcal{C}$ and Ω is a regular two-graph.

To prove $(\triangle)$, consider intersecting lines $\{v_1, v_2, v_3, v_4\}$ and $\{v_1, v_2, v_5, v_6\}$ in $\mathcal{B}$. By definition

$$(2.2) \qquad\qquad v_1 + v_2 + v_3 + v_4 = v_1 + v_2 + v_5 + v_6 = \mathbf{0},$$

so that

$$v_3 + v_4 + v_5 + v_6 + = \mathbf{0}.$$

We check that $\rho(v_3, v_4, v_5) = 0$ from which it follows that $\{v_3, v_4, v_5, v_6\} \in \mathcal{B}$.

$$
\begin{aligned}
\rho(v_3, v_4, v_5) &= \varphi(v_3, v_4) + \varphi(v_3, v_5) + \varphi(v_4, v_5) && \text{(definition of } \rho) \\
&= \varphi(v_3, v_4) + \varphi(v_3, v_5) + \varphi(v_1 + v_2 + v_3, v_5) && \text{(by (2.2))} \\
&= \varphi(v_3, v_4) + \varphi(v_1, v_5) + \varphi(v_2, v_5) && \text{(bilinearity of } \varphi) \\
&= \varphi(v_3, v_4) + \varphi(v_1, v_2) && \text{(since } \rho(v_1, v_2, v_5) = 0) \\
&= \varphi(v_3, v_1 + v_2 + v_3) + \varphi(v_1, v_2) && \text{(by (2.2))} \\
&= \varphi(v_1, v_2) + \varphi(v_1, v_3) + \varphi(v_2, v_3) = 0, && \text{(since } \varphi(v_3, v_3) = \rho(v_1, v_2, v_3) = 0)
\end{aligned}
$$

as needed. The last assertion is a consequence of [GGS, Theorem B]

□

2.4. **3-transposition groups.** We will need a number of results concerning 3-transposition groups; we gather these together below.

Definition 2.10. A *3-transposition group* is a pair $(G, \mathcal{E})$, where G is a group, $\mathcal{E}$ is a set of involutions in G and the following conditions hold:

  (i) $G = \langle \mathcal{E} \rangle$; and
  (ii) $\mathcal{E}$ is a union of G-conjugacy classes of involutions;
  (iii) for all $g, h \in \mathcal{E}$, gh has order $1, 2$ or 3.

Elements of the set $\mathcal{E}$ are called 3-*transpositions*. The pair $(G, \mathcal{E})$ is called a *finite 3-transposition group* if the group G is finite.

The first result is virtually immediate; a proof is given at [Fis71, 1.1.2].

Lemma 2.11. *Let* $(G, \mathcal{E})$ *be a 3-transposition group. If* N *is a normal subgroup of* G, *then either* $N = G$, *or* $(G/N, \mathcal{E}N/N)$ *is a 3-transposition group.*

Recall that $O_p(G)$ denotes the largest normal p-subgroup of a finite group G. The following result is an immediate consequence of [Asc97, Theorem 9.3] and [CH92, Theorem 2.2].

Proposition 2.12. *Let* $(G, \mathcal{E})$ *be a finite 3-transposition group and suppose that* $\mathcal{E}$ *is a conjugacy class in* G *and that* $Z(G) = 1$. *Then* $O_p(G) = 1$ *for all primes* $p > 3$, *and exactly one of the following holds:*

(i) $O_2(G) \neq 1$;
(ii) $O_3(G) \neq 1$; *or*
(iii) $Q(G) := \langle gh \, | \, g, h \in \mathcal{E}, |gh| = 2 \rangle$ *is a nonabelian simple group.*

Finally we will require the celebrated classification of finite 3-transposition groups due to Fischer [Fis71]. Note that this classification is not dependent on the classification of finite simple groups (indeed the reverse is true). There are several versions of this theorem, and we prefer to use a slightly simplified version covering the case with trivial soluble radical.

Theorem 2.13. *Let* $(G, \mathcal{E})$ *be a finite 3-transposition group. Suppose that* $\mathcal{E}$ *is a conjugacy class in* G, *and that* G *contains no non-trivial solvable normal subgroups. Then, up to conjugation in* $\mathrm{Aut}(G)$, *one of the following holds:*

(1) $m \geqslant 5$, $G \cong \mathrm{Sym}(m)$ *and* $\mathcal{E}$ *is the class of transpositions;*
(2) $m \geqslant 2$, $G \cong \mathrm{O}_{2m}^{\pm}(2)$ *and* $\mathcal{E}$ *is the class of transvections;*
(3) $m \geqslant 2$, $G \cong \mathrm{Sp}_{2m}(2)$ *and* $\mathcal{E}$ *is the class of transvections;*
(4) $m \geqslant 4$, $G \cong \mathrm{PSU}_{\mathrm{m}}(2)$ *and* $\mathcal{E}$ *is the class of (projective images of) transvections;*
(5) $m \geqslant 2$, G *is a subgroup of* $\mathrm{PO}_{2m}^{\pm}(3)$ *containing* $\mathrm{P\Omega}_{2m}^{\pm}(3)$ *and* $\mathcal{E}$ *is a class of (projective images of) reflections;*
(6) G *is one of* Fi_{22}, Fi_{23}, Fi_{24}, $\Omega_8^+(2) : \mathrm{Sym}(3)$, *or* $\mathrm{P\Omega}_8^+(3) : \mathrm{Sym}(3)$, *and in each case* $\mathcal{E}$ *is a unique class of involutions in* G.

Proof. The assumptions of [CH92, Theorem (1.1)] hold. Since $G = \langle \mathcal{E} \rangle$, and G contains no non-trivial solvable normal subgroups (so in particular $Z(G) = 1$), it follows that G is an almost simple group containing $\mathcal{E}$ (in fact generated by $\mathcal{E}$), and so G is one of the groups given in (1) – (6). (Information about the groups generated by $\mathcal{E}$ may be found, for example, in [Asc97, §11]). $\qquad\square$

3. PROPERTIES OF CONWAY GROUPOIDS

In this section we prove Theorem A. Throughout the section we assume the hypotheses of Theorem A, namely:

- $(\Omega, \mathcal{B})$ is a supersimple $2 - (n, 4, \lambda)$ design with $n > 2\lambda + 2$;
- ∞ is an element of Ω, and $G := \mathcal{L}_\infty(\mathcal{D})$.

We also write $\mathcal{C}$ for the set of all collinear triples in $(\Omega, \mathcal{B})$.

Proposition 3.1. *Part (a) of Theorem A holds: if* G *is a group then* G *is a primitive subgroup of* $\mathrm{Sym}(\Omega)$.

Proof. Suppose that G is a group. Then, by Lemma 2.6, G is a transitive subgroup of $\mathrm{Sym}(\Omega)$. Suppose for a contradiction that G preserves a system of imprimitivity with m blocks of size k, where $m \geqslant 2, k \geqslant 2$, and let $\Delta = \{\infty, a_2, \ldots, a_k\}$ be the block of imprimitivity that contains ∞.

Since $n > 2\lambda + 2$ there exists $y \notin \overline{\infty, a_2}$. Then $g := [\infty, y]$ fixes a_2, so g must fix Δ setwise, and hence $y = \infty^g \in \Delta$. It follows that every element in $(\Omega \setminus \overline{\infty, a_2}) \cup \{\infty, a_2\}$ lies in Δ, which implies that $k \geqslant n - 2\lambda$. In particular the number of fixed points of g is $n - 2\lambda - 2 < k$.

Now let $b \in \Omega \setminus \Delta$, so that the block of imprimitivity Δ_2 containing b is distinct from Δ, and consider $h := [\infty, b]$. Note that h interchanges Δ and Δ_2. On the other hand, since $n > 2\lambda + 2 = |\mathrm{supp}(h)|$, h has a fixed point in Ω, say c, and the block of imprimitivity Δ_3 containing c is fixed setwise by h and hence is distinct from Δ and Δ_2. Since $k = |\Delta_3|$ is larger than the number of fixed points of h, it follows that $\mathrm{supp}(h) \cap \Delta_3$ contains a point, say c', and since $\mathrm{supp}(h) = \overline{\infty, b}$, the set $\ell := \{\infty, b, c', b'\}$ is a line, where $b' := c'^{[\infty,b]}$. Note that b' lies in the block $\Delta_3^{[\infty,b]}$ which is equal to Δ_3. Now consider the elementary move $h' := [\infty, b']$. Since (∞, b') is a 2-cycle of h' the element h' interchanges Δ and Δ_3. However since also (b, c') is a 2-cycle of h' (since ℓ is a line containing ∞, b') h' should interchange Δ_2 and Δ_3. This contradiction completes the proof. $\qquad\square$

Proposition 3.2. *Part (b) of Theorem A holds: if $(\Omega, \mathcal{C})$ is a regular two-graph then $\pi_\infty(\mathcal{D})$ is transitive on $\Omega \setminus \{\infty\}$.*

Proof. Suppose that $(\Omega, \mathcal{C})$ is a regular two-graph, and let $a \in \Omega \setminus \{\infty\}$. We claim that

$$(3.1) \qquad\qquad\qquad 2\lambda + 2 \leqslant |a^{\pi_\infty(\mathcal{D})}|.$$

Since $n > 2\lambda + 2$, there exists $b \notin \overline{\infty, a}$. Then $a^{[\infty, a, b, \infty]} = b \in a^{\pi_\infty(\mathcal{D})}$. It is sufficient to prove that $\overline{a, b} \subseteq a^{\pi_\infty(\mathcal{D})}$, for then (3.1) follows from $|\overline{a, b}| = 2\lambda + 2$. To see this, let $c \in \overline{a, b} \setminus \{a, b\}$. Then, since $(\Omega, \mathcal{C})$ is a regular two-graph, either $\infty \notin \overline{a, c}$ or $\infty \notin \overline{b, c}$ (but not both). Hence, either $[\infty, a, c, \infty]$ or $[\infty, b, c, \infty]$ fixes ∞ and maps a to c, or b to c, respectively, whence $c \in a^{\pi_\infty(\mathcal{D})}$. Thus (3.1) is proved.

By (3.1), each orbit of $\pi_\infty(\mathcal{D})$ in $\Omega \setminus \{\infty\}$ has length at least $2\lambda + 2$. Thus if $n \leqslant 4\lambda + 4$, there is not space for two orbits and so $\pi_\infty(\mathcal{D})$ is transitive on $\Omega \setminus \{\infty\}$. We may therefore assume that $n > 4\lambda + 4$. Let $a, b \in \Omega$ and observe that

$$|\overline{a, \infty} \cup \overline{b, \infty}| \leqslant 2(2\lambda + 2) - 1 = 4\lambda + 3$$

so there exists $w \notin \overline{a, \infty} \cup \overline{b, \infty}$. Then $[\infty, a, w, \infty, w, b, \infty] \in \pi_\infty(\mathcal{D})$ and sends a to b. Thus $\pi_\infty(\mathcal{D})$ is transitive on $\Omega \setminus \{\infty\}$ in this case also. $\qquad \square$

Proposition 3.3. *Part (c) of Theorem A holds: if $\mathcal{C}$ is a regular two-graph and G is a group then $\pi_\infty(\mathcal{D})$ is primitive on $\Omega \setminus \{\infty\}$.*

Proof. Suppose that $(\Omega, \mathcal{C})$ is a regular two-graph and that G is a group. By Propositions 3.1 and 3.2, G is 2-transitive on Ω, and it is sufficient to prove that $\pi_\infty(\mathcal{D})$ is primitive on $\Omega \setminus \{\infty\}$. Suppose to the contrary that $\pi_\infty(\mathcal{D})$ acts imprimitively on $\Omega \setminus \{\infty\}$ with m blocks of size k, where $m \geqslant 2, k \geqslant 2$, and $n - 1 = mk$. Let $a, b \in \Omega \setminus \{\infty\}$ lie in the same block of imprimitivity, say Δ.

Suppose first that $\infty \notin \overline{a, b}$. Choose $c \in \overline{a, b}$ so that there exists a line $\{a, b, c, d\} \in \mathcal{B}$ for some $d \in \Omega \setminus \{\infty\}$. We show first that $c \in \Delta$. Consider the set of points $\{\infty, a, b, d\}$. Since $(\Omega, \mathcal{C})$ is a regular two-graph, exactly one of a, b lies in $\overline{\infty, d}$. By interchanging the roles of a and b if necessary, we may assume that $a \in \overline{\infty, d}$ and $b \notin \overline{\infty, d}$. Then, considering the set of points $\{\infty, b, c, d\}$ we see that exactly one of b, d lies in $\overline{\infty, c}$. If $d \notin \overline{\infty, c}$ then the permutation $g := [\infty, a, d, \infty]$ fixes a and sends b to c. Thus $c = b^g \in \Delta^g = \Delta$ in this case. Assume now that $b \notin \overline{\infty, c}$. Then considering $\{\infty, a, b, c\}$ we see that $\infty \in \overline{a, c}$. Hence the permutation $h := [\infty, b, c, a, \infty]$ sends a to b (and hence fixes Δ), and sends b to c, so $c = b^h \in \Delta^h = \Delta$ in this case also. Thus in either case Δ contains each point of $\overline{a, b}$, and so $k = |\Delta| \geqslant 2\lambda + 2$. Now, by Corollary 2.4, n is even so that $m = \frac{n-1}{k}$ is odd. Hence $m \geqslant 3$ so that by Corollary 2.4 again,

$$6\lambda < (2\lambda + 2)m \leqslant km < n \leqslant 6\lambda,$$

a contradiction.

Thus, $\infty \in \overline{a, b}$, and we note that this holds whenever a, b lie in the same block of imprimitivity of $\pi_\infty(\mathcal{D})$. Since $n > 2\lambda + 2$, there exists $c \notin \overline{a, b}$. In particular $c \neq \infty$. If $\infty \notin \overline{a, c}$ then by Lemma 2.6, $[a, c]$ lies in $\pi_\infty(\mathcal{D})$, fixes b and sends a to c. Thus c lies in the same block of imprimitivity Δ containing a, b. In particular a, c lie in the same block of imprimitivity so $\infty \in \overline{a, c}$, which is a contradiction. Hence $\infty \in \overline{a, c}$ and an identical argument (with the roles of a and b interchanged) shows that $\infty \in \overline{b, c}$. This proves that exactly three 3-subsets of $\{\infty, a, b, c\}$ lie in $\mathcal{C}$, contradicting the fact that $\mathcal{C}$ is a regular two-graph. $\qquad \square$

Theorem A now follows from Propositions 3.1, 3.2, and 3.3.

4. Towards a proof of Theorem B

Recall condition $(\triangle)$ defined in Section §1 for a design $\mathcal{D} = (\Omega, \mathcal{B})$:

$(\triangle) \qquad\qquad$ If $B_1, B_2 \in \mathcal{B}$ such that $|B_1 \cap B_2| = 2$, then $B_1 \triangle B_2 \in \mathcal{B}$.

Throughout this section we assume the following hypotheses and notation.

Hypotheses 4.1.
- $\mathcal{D} = (\Omega, \mathcal{B})$ *is a supersimple* $2 - (n, 4, \lambda)$ *design that satisfies* $(\triangle)$*;*
- $(\Omega, \mathcal{C})$ *is a regular two-graph, where* $\mathcal{C}$ *is the set of collinear triples of* $\mathcal{D}$*;*
- $\infty \in \Omega$*, and* $G := \mathcal{L}_\infty(\mathcal{D})$*;*
- $\mathcal{E} := \{[a, b] \mid a, b \in \Omega\}$ *is the set of elementary moves on* $\mathcal{D}$*.*

The main result of the section is Theorem 4.2. One of its conclusions is that G is a group.

Theorem 4.2. *If Hypotheses* 4.1 *hold, then G is a subgroup of* $\mathrm{Aut}(\mathcal{D})$*, and $(G, \mathcal{E})$ is a 3-transposition group.*

Lemma 4.3. *If $\{w, x, y, z\} \in \mathcal{B}$ is a line then $[w, x] = [y, z]$.*

Proof. This follows from the fact (using ($\triangle$)) that $\{w, x, a, b\}$ is a line containing $\{w, x\}$ if and only if $\{y, z, a, b\}$ is a line containing $\{y, z\}$. $\square$

Lemma 4.4. *For pairwise distinct $x, y, z \in \Omega$,*

$$[y, z] \cdot [x, y] \cdot [y, z] = \begin{cases} [x, y], & \text{if } x \in \overline{y, z}; \\ [x, z], & \text{otherwise.} \end{cases}$$

Proof. Let $w = [y, z] \cdot [x, y] \cdot [y, z]$. Note first that w is conjugate to $[x, y]$, and hence is an involution. Thus it suffices to show directly that the image under w of each point $a \in \Omega$ is the same as its image under $[x, y]$ or $[x, z]$, according to whether $x \in \overline{y, z}$ or $x \notin \overline{y, z}$, respectively. It is straightforward to check that this is true if $a \in \{x, y, z\}$, so let $a \in \Omega \setminus \{x, y, z\}$. We consider three cases, according to whether zero, two or four of the 3-subsets of $X := \{x, y, z, a\}$ are collinear.

If no 3-subsets of X are collinear then $x \notin \overline{y, z}$ and since a is fixed by all of $[x, y]$, $[y, z]$, $[x, z]$, it is also fixed by w. If all 3-subsets of X are collinear then $x \in \overline{y, z}$, and we have lines $\{x, y, a, b\}$, $\{x, z, a, c\}$, $\{y, z, a, d\} \in \mathcal{B}$, for some $b, c, d \in \Omega$. Moreover, by ($\triangle$), the following 4-subsets are also lines:

$$\{x, y, a, b\} \triangle \{x, z, a, c\} = \{y, z, b, c\};$$
$$\{x, y, a, b\} \triangle \{y, z, a, d\} = \{x, z, b, d\};$$
$$\{x, z, a, c\} \triangle \{y, z, a, d\} = \{x, y, c, d\}.$$

It can now be checked that w and $[x, y]$ both send a to b.

Lastly suppose that exactly two of the 3-subsets of X are collinear. There are six possibilities for the collinear pairs, corresponding to the six rows of Table 1. Suppose first that $\{x, y, z\}$ is collinear. If $\{a, x, y\}$ is also collinear then $\{x, y, a, b\}$ is a line, for some $b \in \Omega$. In this case, if $\{b, y, z\}$ is collinear then for some $c \in \Omega$, $\{y, z, b, c\}$ is a line and hence $\{x, y, a, b\} \triangle \{y, z, b, c\} = \{x, z, a, c\}$ is a line, whence $\{a, x, z\}$ is collinear, which is a contradiction. Thus $\{b, y, z\}$ is not collinear, and hence $a^w = a^{[x,y]} = b$ proving the assertions of row 1. Next, if $\{a, y, z\}$ is collinear, then $\{y, z, a, b\}$ is a line, for some $b \in \Omega$, and a similar argument to the previous case shows that $\{b, x, y\}$ is not collinear. Thus $a^w = a^{[x,y]} = a$ and the assertions of row 2 hold. If $\{a, x, z\}$ is collinear, then a is fixed by both $[y, z]$ and $[x, y]$, and hence $a^w = a^{[x,y]} = a$ and the assertions of row 3 hold. This completes the proof that $w = [x, y]$ if $x \in \overline{y, z}$.

Now suppose that $\{x, y, z\}$ is not collinear. Then one of rows 4,5 or 6 holds. For row 4, there exist $b, c \in \Omega$ such that $\{x, y, a, b\}$ and $\{x, z, a, c\}$ are lines. Property ($\triangle$) implies that $\{x, y, a, b\} \triangle \{x, z, a, c\} = \{y, z, b, c\}$ is a line, from which it follows that w and $[x, z]$ both send a to c. Similarly, for row 5, there exist $b, c \in \Omega$ such that $\{x, y, a, b\}$ and $\{y, z, a, c\}$ are lines. Property ($\triangle$) implies that $\{x, y, a, b\} \triangle \{y, z, a, c\} = \{x, z, b, c\}$ is a line. If we also had a line $\{x, y, c, d\}$ for some $d \in \Omega$, then $\{y, z, a, c\} \triangle \{x, y, c, d\} = \{x, z, a, d\}$ is a line, which is a contradiction since $\{x, z, a\}$ is not collinear. Hence $\{x, y, c\}$ is not collinear, and so w and $[x, z]$ both fix a. Finally for row 6, there exist $b, c \in \Omega$ such that $\{y, z, a, b\}$ and $\{x, z, a, c\}$ are lines. Property ($\triangle$) implies that $\{y, z, a, b\} \triangle \{x, z, a, c\} = \{x, y, b, c\}$ is a line. If we also had a line $\{y, z, c, d\}$ for some $d \in \Omega$, then $\{x, z, a, c\} \triangle \{y, z, c, d\} = \{x, y, a, d\}$ is a line, which is a contradiction since $\{x, y, a\}$ is not collinear. Hence $\{y, z, c\}$ is not collinear, and so w and $[x, z]$ both send a to c. This completes the proof. $\square$

Collinear triples in X	a^w	$a^{[x,y]}$	$a^{[x,z]}$
$\{x, y, z\}$, $\{a, x, y\}$	$a^{[x,y]}$	$a^{[x,y]}$	$-$
$\{x, y, z\}$, $\{a, y, z\}$	a	a	$-$
$\{x, y, z\}$, $\{a, x, z\}$	a	a	$-$
$\{a, x, y\}$, $\{a, x, z\}$	$a^{[x,z]}$	$-$	$a^{[x,z]}$
$\{a, x, y\}$, $\{a, y, z\}$	a	$-$	a
$\{a, y, z\}$, $\{a, x, z\}$	$a^{[x,z]}$	$-$	$a^{[x,z]}$

TABLE 1. Comparing images for the Proof of Lemma 4.4: here $w = [y, z] \cdot [x, y] \cdot [y, z]$.

Now we derive three more facts about the moves on $\mathcal{D}$.

Lemma 4.5. *Let $x, y, z \in \Omega$ be pairwise distinct.*

(a) *Then,*

$$o([x,y] \cdot [y,z]) = \begin{cases} 2, & \text{if } x \in \overline{y,z}; \\ 3, & \text{if } x \notin \overline{y,z}. \end{cases}$$

(b) *if $x \notin \overline{y,z}$ then $[z,x,y,z] = [x,y]$.*
(c) *$\mathcal{L}(\mathcal{D}) = \mathcal{L}_\infty(\mathcal{D})$ is a group of automorphisms of $\mathcal{D}$.*

Proof. (a) Let $X := [x,y]$ and $Y := [y,z]$. Note that, since x,y,z are distinct, $X \neq Y$ and so the product XY is not the identity. By Lemma 4.4, either $XY = YX$ (if $x \in \overline{y,z}$) and XY has order 2, or X and Y satisfy the braid relation $XYX = YXY$, and XY has order 3.

(b) Two applications of Lemma 4.4 yield

$$[z,x,y,z] = [z,x][x,y][y,z] = [z,x][x,y][z,x][z,x][y,z]$$
$$= [z,y][z,x][y,z] = [x,y],$$

as required.

(c) We check that $\mathcal{D}$ satisfies the hypotheses of Lemma 2.7(iii). Let $x,y,z \in \Omega$. If $x \notin \overline{y,z}$ then $[x,y] = [z,x,y,z] = [z,x,y,z^{[x,y]}]$ by part (b). If $x \in \overline{y,z}$, so that $\{x,y,z,w\}$ is a line say, then

$$[z,x,y,z^{[x,y]}] = [z,x] \cdot [x,y] \cdot [y,w] = [x,y] \cdot [z,x] \cdot [y,w] = [x,y] \cdot [z,x] \cdot [z,x] = [x,y],$$

where we use both the facts that $[z,x] = [y,w]$ (Lemma 4.3) and $[x,y]$ and $[x,z]$ commute (Lemma 4.4). Thus the hypotheses of Lemma 2.7(iii) are satisfied and we conclude that $\mathcal{L}(\mathcal{D})$ is a group of automorphisms of $\mathcal{D}$. In particular, $\mathcal{L}(\mathcal{D})$ is a group, and so $\mathcal{L}(\mathcal{D}) = \mathcal{L}_\infty(\mathcal{D})$ by Lemma 2.6. □

The previous two lemmas allow us to prove that the set $\mathcal{E}$ of elementary moves is closeD under conjugation by elements of $\langle \mathcal{E} \rangle$.

Lemma 4.6. *If Hypotheses 4.1 hold, then $[x,y]^g = [x^g, y^g]$ for all $g \in \langle \mathcal{E} \rangle$ and all $x,y \in \Omega$.*

Proof. This is trivially true if $x = y$ since $[x,x] = 1$ for all x, so we may assume that $x \neq y$. Moreover, it is sufficient to prove that $[x,y]^g = [x^g, y^g]$ for all $g \in \mathcal{E}$, so we may assume that $g = [z,w]$ for distinct $z,w \in \Omega$. Furthermore, by Lemma 2.7 (the equivalence of conditions (i) and (ii)) we may assume that $x = w$. If also $y = z$ the condition is easy to check, so assume that $y \neq z$, that is, x, y and z are pairwise distinct. Then Lemma 4.4 applies. If $y \in \overline{x,z}$ then there is a line $\{x,y,z,c\}$ of $\mathcal{D}$; Lemma 4.4 gives $[x,y]^g = [x,y]$, while $[x^g, y^g] = [z,c]$, which is equal to $[x,y]$ by Lemma 4.3. Thus $[x,y]^g = [x^g, y^g]$ holds in this case. Suppose now that $y \notin \overline{x,z}$. Then by Lemma 4.4, $[x,y]^g = [z,y]$, while $[x^g, y^g] = [z,y]$, so again the condition holds. □

Proof of Theorem 4.2. It follows from Lemma 4.5(c) that $G = \mathcal{L}_\infty(\mathcal{D})$ is a subgroup of $\mathrm{Aut}(\mathcal{D})$. It thus remains to prove that $(G, \mathcal{E})$ is a 3-transposition group. To do this, we verify the three conditions (i),(ii) and (iii) of Definition 2.10. Condition (i), that $G = \langle \mathcal{E} \rangle$, follows from Lemma 4.5(c), and condition (ii) is proved in Lemma 4.6. To prove (iii), let $x,y,z \in \Omega$. If these points are not pairwise distinct then $[x,y] \cdot [y,z]$ has order 1 or 2, so suppose they are pairwise distinct. We claim that

$$o([x,y] \cdot [y,z]) = \begin{cases} 2, & \text{if } x \in \overline{y,z}; \\ 3, & \text{if } x \notin \overline{y,z}. \end{cases}$$

To see this, let $X := [x,y]$ and $Y := [y,z]$. Note that, since x,y,z are distinct, $X \neq Y$ and so the product XY is not the identity. By Lemma 4.4, either $XY = YX$ (if $x \in \overline{y,z}$) and XY has order 2, or X and Y satisfy the braid relation $XYX = YXY$, and XY has order 3. □

If $n > 2\lambda + 2$ then we can strengthen Theorem 4.2 using Theorem A as follows.

Corollary 4.7. *If Hypotheses 4.1 hold and, in addition, $n > 2\lambda + 2$, then the following hold:*
(a) *$(G, \mathcal{E})$ is a 3-transposition group;*
(b) *G is a 2-primitive subgroup of $\mathrm{Sym}(\Omega)$;*
(c) *$Z(G) = 1$;*
(d) *$\mathcal{E}$ is a conjugacy class in G.*

Proof. Part (a) is given by Theorem 4.2, and (b) follows from Theorem A (c). Hence for any $a,b,c,d \in \Omega$ there exists $g \in G$ such that $a^g = c$ and $b^g = d$. Thus, by Lemma 4.6, $[a,b]^g = [a^g, b^g] = [c,d]$ and (d) is proved. To prove (c), note that, since $n > 2\lambda + 2$, for each $a \in \Omega$ there exists $b \in \Omega \setminus \overline{\infty, a}$. By Lemma 4.4, the permutations $[\infty, a]$ and $[a,b]$ do not commute, so G is nonabelian. Now $Z(G) \leqslant C_{\mathrm{Sym}(\Omega)}(G) = 1$ by [DM96, Theorem 4.2A]. □

5. Proof of Theorem B

Before proceeding with the proof of Theorem B, we record two background results from number theory.

Let x and n be positive integers. A *primitive prime divisor* (sometimes called a *Zsigmondy prime*) of $x^n - 1$ is a prime divisor s which does not divide $x^k - 1$ for any $k < n$. A special case of Zsigmondy's theorem [Zsi92], due to Bang [Ban86], tells us when primitive prime divisors exist with $x = 2$.

Lemma 5.1. *For positive integers n, $2^n - 1$ has a primitive prime divisor, unless $n = 6$.*

The other result that we need is elementary and can be found, for instance, as [GGS, Lemma 6.3].

Lemma 5.2. *Suppose that a, b, p are positive integers, and that $p^a \pm 1 = 2^b$. Then either $a = 1$ or $p = 1$ or $(p, a) = (3, 2)$.*

5.1. **The case $n = 2\lambda + 2$.** Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple $2 - (n, 4, \lambda)$ design. Since $\overline{a, b}$ contains $2\lambda + 2$ distinct points, for any $a, b \in \Omega$, the number of points $n \geqslant 2\lambda + 2$. The following result yields Theorems B and C in the case where equality holds. Recall that Boolean quadruple systems were defined in Example 1.1.

Proposition 5.3. *Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple $2 - (n, 4, \lambda)$ design with $n = 2\lambda + 2$. The following conditions are equivalent.*

    (1) *$\mathcal{D}$ satisfies $(\triangle)$;*
    (2) *$\mathcal{D} = \mathcal{D}^b$, a Boolean quadruple system of order 2^m for some integer $m \geqslant 2$;*
    (3) *$\pi_\infty(\mathcal{D}) = \{1\}$ and $\mathcal{L}_\infty(\mathcal{D})$ is elementary-abelian of order 2^m for some integer $m \geqslant 2$.*

Proof. That (3) implies (2) is a consequence of [GGNS, Theorem B], and that (2) implies (3) follows from Lemma 2.8. Next assume that condition (2) holds. Then condition $(\triangle)$ is equivalent to the assertion that, if two affine subplanes of $\mathbb{F}_2^m$ intersect in a line, then their symmetric difference is an affine subplane. This is clearly true, so (1) holds.

Finally we must prove that (1) implies (2). Since $n = 2\lambda + 2$ and $\mathcal{D}$ is supersimple, $\mathcal{D}$ is a $3 - (n, 4, 1)$ design. Define a commutative binary operation $*$ on Ω by setting $a * a := \infty$ and $a * \infty = \infty * a = a$, for all $a \in \Omega$, and, for distinct $a, b \in \Omega \setminus \{\infty\}$,

$$a * b := c \quad \text{where } c \text{ is the unique point such that } \{\infty, a, b, c\} \in \mathcal{B}.$$

Now if for distinct $a, b, c \in \Omega \setminus \{\infty\}$ we have $\{\infty, a, b, d\}, \{\infty, b, c, e\}, \{\infty, a, e, x\} \in \mathcal{B}$, then

$$(\{\infty, a, b, d\} \triangle \{\infty, b, c, e\}) \triangle \{\infty, a, e, x\} = \{\infty, c, d, x\} \in \mathcal{B}$$

and hence

$$a * (b * c) = a * e = x = d * c = (a * b) * c.$$

It is easy to verify that $a * (b * c) = (a * b) * c$ also holds if a, b, c are not pairwise distinct or if $\infty \in \{a, b, c\}$. Thus $*$ is associative, and it follows that $(\Omega, *)$ is an abelian group of exponent 2, and hence is isomorphic to $(\mathbb{F}_2^m, +)$ for some integer $m \geqslant 2$. Furthermore, an identical argument to the one given above shows that $\{a, b, c, d\}$ is a line if and only if $a * b * c * d = \infty$. Hence $\mathcal{D} = \mathcal{D}^b$ is a Boolean quadruple system, and (2) holds. $\square$

It is worth noting that, since the Boolean quadruple system of order 2^m is a $3 - (2^m, 4, 2^{m-1} - 1)$, every 3-subset of Ω is collinear. Thus, if $\mathcal{C}$ is the set of all collinear 3-subsets of Ω, then $(\Omega, \mathcal{C})$ is a complete 3-uniform hypergraph, and in particular is trivially a regular two-graph.

5.2. **Almost simple case.** In this subsection we assume that Hypotheses 4.1 hold, and in addition that $n > 2\lambda + 2$ and that G contains no non-trivial solvable normal subgroup. (These are the hypotheses of Theorem B, plus $n \neq 2\lambda + 2$, and an extra restriction on G.)

By Corollary 4.7, $(G, \mathcal{E})$ is a 3-transposition group, $\mathcal{E}$ is a G-conjugacy class, $Z(G) = 1$, and G is 2-primitive on Ω. In particular the assumptions of Theorem 2.13 are satisfied, so G is an almost simple group and lies in one of the classes (1)-(6) listed there. Our job, then, is to prove that only class (3) can occur. We carefully avoid appeal to the finite simple group classification by using properties of the known almost simple 3-transposition groups.

Lemma 5.4. $|\mathcal{E}| = \frac{n(n-1)}{2(\lambda+1)}$.

Proof. Let a and b be distinct elements of Ω. We are interested in those elements $[x, y] \in \mathcal{E}$ that contain the transposition (a, b) in their cycle decomposition. The definition of an elementary move implies immediately that this will be the case if and only if $\{x, y\} = \{a, b\}$ or $\{a, b, x, y\} \in \mathcal{B}$. Thus there are $\lambda + 1$ choices of $\{x, y\}$ for which $[x, y]$ contains (a, b) in its cycle decomposition.

Now Lemma 4.3 implies that, for all of these choices, the resulting elementary moves are equal. The result follows by observing that there are $n(n-1)/2$ choices for the set $\{x, y\}$ in Ω. $\square$

We now consider case (1) of Theorem 2.13. Note that, since $\mathrm{Sym}(6) \cong \mathrm{Sp}_4(2)$, the following lemma yields Theorem B in this case.

Lemma 5.5. *If $G \cong \mathrm{Sym}(m)$ with $m \geqslant 5$, then $m = 6$ and $n = 10$.*

Proof. By Corollary 2.4, we have $2(\lambda+1) < n < 6(\lambda+1)$, or equivalently, $2 < \frac{n}{\lambda+1} < 6$. By Theorem 2.13, $\mathcal{E}$ is the class of transpositions, so $|\mathcal{E}| = \binom{m}{2}$, and hence $m(m-1) = \frac{n(n-1)}{\lambda+1}$ by Lemma 5.4. Combining these two facts, we obtain $2(n-1) < m(m-1) < 6(n-1)$, or equivalently,

$$\frac{m(m-1)}{6} < n - 1 < \frac{m(m-1)}{2}.$$

In particular if $m = n$, then $m = 5$, a contradiction. More generally, since G is 2-transitive on Ω, we apply [Ban69, Theorem 1] and conclude that $(m,n) \in \{(5,5),(5,6),(6,10)\}$. However if $m, n \in \{5,6\}$, the equation in Lemma 5.4 implies that $\lambda \in \{0, \frac{1}{2}\}$, which is a contradiction. $\square$

Lemma 5.6. *If G is isomorphic to a group in one of the classes (2) – (6) of Theorem 2.13, then one of the following holds:*

(1) $G \cong \mathrm{Sp}_{2m}(2)$ and $n = 2^{m-1} \cdot (2^m \pm 1)$, for some $m \geqslant 2$, and the stabilizer of a point is isomorphic to $\mathrm{O}_{2m}^{\pm}(2)$;
(2) $G \cong \mathrm{Fi}_{22}, \mathrm{Fi}_{23}$ or Fi_{24}.

Proof. Observe first that, if G is isomorphic to a group in one of the classes (2) – (6) of Theorem 2.13, then G is either a Fischer group (and is listed at part (2) above), or is an almost simple Chevalley group of normal or twisted type. Thus we assume that we are in this second case and we derive part (1).

We use the fact that, by assumption, G admits a 2-transitive action. We apply [CKS76, Main Theorem], which lists all almost simple Chevalley groups of normal or twisted type admitting a 2-transitive action. We obtain immediately that either part (1) above holds, or (possibly) one of the following occurs:

(i) $G \cong \mathrm{O}_4^-(2) \cong \mathrm{Sym}(5)$ with $n = 5$ or 6;
(ii) $G \cong \mathrm{O}_6^+(2) \cong \mathrm{Sym}(8)$ with $n = 8$ or 15;
(iii) $\mathrm{Alt}(6) \cong \mathrm{P\Omega}_4^-(3) \leqslant \mathrm{G} \leqslant \mathrm{PO}_4^-(3)$ with $n = 6$ or 10;
(iv) $\mathrm{PSL}_4(3) \cong \mathrm{PSO}_6^+(3) \leqslant \mathrm{G} \leqslant \mathrm{PO}_6^+(3)$ with $n = 40$.

In cases (i) and (ii), G is a symmetric group and Lemma 5.5 immediately excludes them. In case (iii), [Asc97, p. 46] implies that $G \cong \mathrm{Sym}(6) \cong \mathrm{Sp}_4(2)$. Now Lemma 5.5 implies that part (1) holds.

In case (iv), G has a socle isomorphic to $\mathrm{PSL}_4(3)$ and [CKS76] implies that G has a 2-transitive action if and only if $G \cong \mathrm{PSL}_4(3)$ or $\mathrm{PGL}_4(3)$. However, [CCN+85] implies that $\mathrm{PO}_6^+(3)$ is a degree 2 extension of $\mathrm{PSL}_4(3)$ that is not isomorphic to $\mathrm{PGL}_4(3)$, and we conclude that G has a 2-transitive action if and only if $G \cong \mathrm{PSO}_6^+(3)$. Now, by definition, G is generated by (the projective image of) reflections which, in particular, have determinant equal to -1; thus G is not a quotient of $\mathrm{SO}_6^+(3)$ and so cannot be isomorphic to $\mathrm{PSO}_6^+(3)$. $\square$

Finally, we exclude the Fischer groups, by appealing to information about the minimal indices of their proper subgroups (we do not use the fact that these groups have no 2-transitive actions).

Lemma 5.7. *G is not isomorphic to one of the groups $\mathrm{Fi}_{22}, \mathrm{Fi}_{23}$ or Fi_{24}.*

Proof. Referring to [CCN+85, LW91] and [Asc97, (37.5) and (37.6)] we see that, for each of the groups $\mathrm{Fi}_{22}, \mathrm{Fi}_{23}$ and Fi_{24}, the minimum degree of a primitive permutation representation is equal to $|\mathcal{E}|$. Thus Lemma 5.4 implies that

$$\frac{n(n-1)}{2(\lambda+1)} \leqslant n,$$

and so $n - 1 \leqslant 2(\lambda+1)$. On the other hand, by assumption, $2(\lambda+1) < n$ and we conclude that $n = 2\lambda + 3$. This contradicts the fact that n is even (Corollary 2.4). $\square$

The following corollary draws together the results of this subsection (it also relies on Proposition 5.3).

Corollary 5.8. *If Hypotheses 4.1 hold, $n > 2\lambda+2$, and G does not contain a non-trivial normal solvable subgroup, then for some $m \geqslant 2$, $G \cong \mathrm{Sp}_{2m}(2)$, $n = 2^{m-1} \cdot (2^m \mp 1)$, and $\pi_\infty(\mathcal{D}) \cong \mathrm{O}_{2m}^{\pm}(2)$.*

5.3. **Affine case.** In this subsection we assume that Hypotheses 4.1 hold, that $n > 2\lambda + 2$, and that G contains a non-trivial solvable normal subgroup N. (Here also, these are the hypotheses of Theorem B, plus $n \neq 2\lambda + 2$, and an extra restriction on G.)

Again, by Corollary 4.7, $(G, \mathcal{E})$ is a 3-transposition group, $\mathcal{E}$ is a G-conjugacy class, $Z(G) = 1$, and G is 2-primitive on Ω. Hence by [DM96, Theorem 4.3B], N is an elementary abelian p-group that acts regularly on Ω. Moreover Lemma 2.6 implies that, for $\infty \in \Omega$, $\pi_\infty(\mathcal{D})$ is the stabilizer of ∞ in the action of G on Ω. Hence we write $G_\infty := \pi_\infty(\mathcal{D})$ and observe that $G = N \rtimes G_\infty$. Observing that N can be viewed as a vector space over a finite field of order p, we note that G_∞ acts linearly on N and so is isomorphic to a subgroup of $\mathrm{GL}_d(p)$ where $|N| = p^d$. Furthermore, since G is 2-transitive, G_∞ acts transitively on the set of non-zero vectors in N.

Lemma 5.9. $p = 2$ and $n = 2^d$ for some $d > 0$.

Proof. This follows immediately from the fact that n is even (Lemma 2.3), or the fact that G_∞ is primitive on $\Omega \setminus \{\infty\}$. □

Proposition 5.10. *There is a conjugacy class $\mathcal{E}_\infty$ of G_∞ such that $(G_\infty, \mathcal{E}_\infty)$ is a 3-transposition group. Furthermore, $Z(G_\infty) = 1$.*

Proof. We know that G_∞ is a primitive subgroup of $\mathrm{Sym}(\Omega \setminus \{\infty\})$. Furthermore, since $n > 2\lambda + 2$ and G is transitive, there exist $a, b \in \Omega$ such that $\infty \notin \overline{a, b}$. Suppose first that G_∞ is abelian, so $\langle [a, b] \rangle \trianglelefteq G_\infty$. Then the primitivity of G_∞ implies that $\langle [a, b] \rangle$ acts transitively (and therefore regularly) on $\Omega \setminus \{\infty\}$. But, since $\langle [a, b] \rangle$ has even order, this contradicts the fact that $n - 1$ is odd (Lemma 5.9). Thus G_∞ is nonabelian and primitive, and so, by [DM96, Theorem 4.2A], $Z(G_\infty) \leqslant C_{\mathrm{Sym}(\Omega \setminus \{\infty\})}(G_\infty) = 1$.

Since N is a proper subgroup of G, $G/N \cong G_\infty$ is a 3-transposition group with respect to $\mathcal{E}N/N$ by Lemma 2.11. Let $\mathcal{E}_\infty$ be the set of 3-transpositions for G_∞ obtained as the image of $\mathcal{E}N/N$ under an isomorphism from G/N to G_∞. Then $(G_\infty, \mathcal{E}_\infty)$ is a 3-transposition group. Moreover, since $\mathcal{E}$ is a G-conjugacy class (by Corollary 4.7), it follows that $\mathcal{E}N/N$ is a (G/N)-conjugacy class, and hence $\mathcal{E}_\infty$ is a G_∞-conjugacy class. □

Proposition 5.11. *G_∞ is almost simple, and lies in one of the classes (1)-(6) of Theorem 2.13.*

Proof. By Proposition 5.10, G_∞ satisfies the hypotheses of Proposition 2.12 and one of the conclusions (i), (ii) or (iii) holds. Suppose that (i) or (ii) holds. Since G_∞ is primitive on $\Omega \setminus \{\infty\}$, any nontrivial normal subgroup acts transitively, and so $|\Omega \setminus \{\infty\}| = n - 1 \in \{2^b, 3^b\}$ for some $b > 0$. However $n = 2^d$ (Lemma 5.9), and hence $2^d - 1 = 3^b$. This implies that $(d, b) = (2, 1)$ by Lemma 5.2, contradicting the fact that $n > 2\lambda + 2 \geqslant 4$. Thus Proposition 2.12 (iii) holds so $Q(G_\infty) = \langle gh \mid g, h \in \mathcal{E}, |gh| = 2 \rangle$ is a nonabelian simple normal subgroup of G_∞. Moreover since $|Q(G_\infty)|$ is even and $n - 1$ is odd (by Lemma 5.9), $Q(G_\infty)$ is not regular on $\Omega \setminus \{\infty\}$. Thus by [DM96, Theorem 4.3B], G_∞ is almost simple, and finally, by Theorem 2.13, G_∞ lies in one of the classes (1)-(6) of that result. □

To complete the proof of Theorem B, it remains to consider the possibilities for G_∞. We use the fact that G_∞ acts transitively on N^*, the set of non-zero vectors of a d-dimensional vector space over $\mathbb{F}_2$. All transitive linear groups were classified by Hering – with the key results appearing in [Her74], and a complete list given in Liebeck [Lie87, Appendix]. We avoid using the classification from [Lie87] since it depends on the finite simple group classification. Instead we use the fact that G_∞ is in one of the six classes of Theorem 2.13, together with some of the results in Hering's paper [Her85] (which do not depend on the simple group classification). First we consider the groups from cases (1) and (3) of Theorem 2.13 to identify the examples in Theorem B (c).

Lemma 5.12. *If $G_\infty \cong \mathrm{Sym}(m)$ for some $m \geqslant 5$ then $m = 6$ and $d = 4$, and Theorem B (c) holds with $m = 2$.*

Proof. We apply [Her74, Theorem 5.12] which (amongst other things) asserts that if a finite symmetric group acts transitively on the set of non-zero vectors of a d-dimensional vector space over $\mathbb{F}_2$, then $d = 4$. Now the fact that $m = 6$ follows by direct calculation, and since $\mathrm{Sym}(6) \cong \mathrm{Sp}_4(2)$, Theorem B (c) holds. □

Lemma 5.13. *If $G_\infty \cong \mathrm{Sp}_{2m}(2)$ for some $m \geqslant 2$ then $d = 2m$, and Theorem B (c) holds.*

Proof. Since G_∞ is transitive on N^*, we must have $(2^d - 1) \big| |G_\infty|$. If $d \neq 6$, let r be a primitive prime divisor of $2^d - 1$ (as in Lemma 5.1) and if $d = 6$ let $r := 7$. In particular, note that r divides

$$|G_\infty| = 2^{m^2} \cdot \prod_{i=1}^{m} (2^{2i} - 1).$$

If $d > 2m$ then $r \nmid 2^{2i} - 1$ for each $1 \leqslant i \leqslant m$, contradicting the fact that r divides $|G_\infty|$. Hence $d \leqslant 2m$.

We prove the reverse inequality. First suppose that $m \neq 3$, and let r be a primitive prime divisor of $2^{2m} - 1$, which exists by Lemma 5.1. Then r divides $|G_\infty|$. Since $|G_\infty|$ divides

$$|\mathrm{GL}_d(2)| = 2^{\binom{d}{2}} \cdot \prod_{i=1}^{d} (2^i - 1)$$

an analogous argument shows that $2m \leqslant d$ and we conclude that $d = 2m$, as required. If $m = 3$, we simply check that $|\mathrm{Sp}_6(2)|$ does not divide the order of $|\mathrm{GL}_d(2)|$ for $d < 6$ and so $d = 6 = 2m$. Thus Theorem B (c) holds for $m \geqslant 3$. If $m = 2$ then $G \cong \mathrm{Sym}(6)$ and Theorem B(c) holds by Lemma 5.12. $\qquad\square$

Next we eliminate the groups in case (2) and a related group from case (6).

Lemma 5.14. *The group G_∞ is not isomorphic to $\mathrm{O}_{2m}^{\pm}(2)$ for any $m \geqslant 2$, and $G_\infty \neq \Omega_8^+(2) : \mathrm{Sym}(3)$.*

Proof. Suppose that $G_\infty \cong \mathrm{O}_{2m}^{\pm}(2)$ for some $m \geqslant 2$ and note that

$$|\mathrm{O}_{2m}^{\pm}(2)| = 2 \cdot 2^{m(m-1)}(2^m \mp 1) \prod_{i=1}^{m-1} (2^{2i} - 1).$$

Exactly as for Lemma 5.13, we use the fact that $2^d - 1$ divides $|G_\infty|$ to conclude that $d \leqslant 2m$. Now [KL90, Proposition 5.4.13] asserts that the smallest module for $\mathrm{O}_{2m}^{\pm}(2)$ over a field of characteristic 2 has dimension $2m$ and, moreover, it is the natural module. Since the sets of isotropic vectors and non-isotropic vectors are each invariant under the action of $\mathrm{O}_{2m}^{\pm}(2)$ on its natural module, and since each of these sets is non-empty, we conclude that $\mathrm{O}_{2m}^{\pm}(2)$ is not transitive on the set of non-zero vectors, which is a contradiction.

Now suppose that $G_\infty = \Omega_8^{\pm}(2) : \mathrm{Sym}(3)$. The arguments of the previous paragraph imply that $d = 8$, so there are $|\Omega \setminus \{\infty\}| = 2^d - 1 = 255$ non-zero vectors. Also G_∞ is transitive on $\Omega \setminus \{\infty\}$, and so its normal subgroup $\Omega_8^{\pm}(2)$ must have equal length orbits permuted transitively by $\mathrm{Sym}(3)$. However one of the $\Omega_8^{\pm}(2)$-orbits is the set of non-zero singular vectors, of size 119, so this is not possible. $\qquad\square$

Now we consider case (4) of Theorem 2.13.

Lemma 5.15. *G_∞ is not isomorphic to $\mathrm{PSU}_m(2)$ for any $m \geqslant 4$.*

Proof. Suppose that $G_\infty \cong \mathrm{PSU}_m(2)$ for some $m \geqslant 4$, and note that

$$|G_\infty| = \frac{2^{\binom{m}{2}}}{\delta} \cdot \prod_{i=2}^{m} (2^i - (-1)^i)$$

where $\delta = \gcd(m, 3)$. First we determine the value of d for m odd, and even, separately.

Claim: If m is odd then $d = 2m$. Suppose that m is odd and let r be a primitive prime divisor of $2^{2m} - 1$ (which exists, by Lemma 5.1 since $m \geqslant 4$). Observe that, since $2^{2m} - 1 = (2^m - 1)(2^m + 1)$, r divides $2^m + 1$ and hence r divides $|G_\infty|$. Then, as in the proof of Lemma 5.13, the fact that $|G_\infty|$ divides $|\mathrm{GL}_d(2)|$ implies that $2m \leqslant d$. Conversely, if $d > 2m$ and r is now a primitive prime divisor of $2^d - 1$, then, as in the proof of Lemma 5.13, we have $r \nmid 2^{2i} - 1$ for each $i \leqslant 2m$ and hence r does not divide $|G_\infty|$, contradicting the fact that $2^d - 1 \mid |G_\infty|$. Hence $d = 2m$.

Claim: If m is even then $d = 2m - 2$. Suppose first that m is even and $m > 4$. Then $|G_\infty|$ is divisible by a primitive prime divisor of $2^{2m-2} - 1$ and we conclude (as in the previous paragraph) that $2m - 2 \leqslant d$. For the reverse inequality, observe that a primitive prime divisor r of $2^d - 1$ (exists and) divides $|G_\infty|$ and hence $d \leqslant 2m - 2$. So $d = 2m - 2$ in this case. If $m = 4$, then we one can check directly that $|\mathrm{PSU}_4(2)|$ does not divide $|\mathrm{GL}_d(2)|$ for $d \leqslant 5$ and hence $d \geqslant 6$. If $d > 6$, then a primitive prime divisor of $2^d - 1$ exists and divides $|G_\infty|$ which in turn forces $d \leqslant 6$, which is a contradiction. Thus $d = 2m - 2 = 6$ in this case also.

Now we consult the list of small dimensional characteristic 2 representations of G_∞ in [KL90, Proposition 5.4.11]. When m is even, the only $(2m-2)$-dimensional characteristic 2 representation occurs when $m = 4$. Similarly, when m is odd, the only $2m$-dimensional characteristic 2 representation occurs when $m = 5$. In both cases, one can check directly that $2^d - 1$ does not divide the order of G_∞, completing the proof. $\qquad\square$

We next eliminate, with a single exception, the last infinite family, namely case (5), together with one further group from case (6).

Lemma 5.16. *Suppose that $\varepsilon \in \{+, -\}$ and $m \geqslant 2$, and that either $\mathrm{P\Omega}_{2m}^\varepsilon(3) \leqslant G_\infty \leqslant \mathrm{PO}_{2m}^\varepsilon(3)$, or $G_\infty = \mathrm{P\Omega}_8^+(3) : \mathrm{Sym}(3)$. Then $m = 2, \varepsilon = -, d = 4$ and $G_\infty \cong \mathrm{Sym}(6) \cong \mathrm{Sp}_4(2)$, as in Theorem B(c).*

Proof. If $G_\infty = \mathrm{P\Omega}_8^+(3) : \mathrm{Sym}(3)$, then set $m = 4$. First we use the results of [LS74] as found, for instance, in [KL90, Table 5.3.A] to prove that $m < 4$. Suppose to the contrary that $m \geqslant 4$, and note that (for example, by [PSY15, Table 1 and Lemma 2.2]) $|\mathrm{O}_{2m}^\varepsilon(3)| < 3^{2m^2-1}$. This is an upper bound for $|G_\infty|$ if $m > 4$, while if $m = 4$ then $G_\infty \leqslant \mathrm{P\Omega}_8^+(3) : \mathrm{Sym}(3)$ has order less than $3^{2m^2+1} = 3^{33}$. On the other hand $2^d - 1$ divides $|G_\infty|$ and so $|G_\infty| > 2^{d-1}$. Moreover since $\mathrm{P\Omega}_{2m}^\varepsilon(3)$ is contained in $\mathrm{GL}_d(2)$, we conclude from [KL90, Table 5.3.A] that $d = \dim(N) \geqslant 3^{2m-4}$. From this we deduce that 2^{d-1} is greater than the upper bound for $|G_\infty|$, which is a contradiction.

Thus $m \leqslant 3$. Indeed, by using the bounds in [KL90, Table 5.3.A] more carefully, we deduce that $m = 2$. Since G_∞ is an almost simple group, by Proposition 5.11, we must have $\varepsilon = -$, and so $\mathrm{P\Omega}_4^-(3) \leqslant G_\infty \leqslant \mathrm{PO}_4^-(3)$. Examining the list in [Asc97, P. 46] we see that $G_\infty \cong \mathrm{Sym}(6)$ and the fact that $d = 4$ follows from Lemma 5.12.   □

Finally we show that the remaining groups in case (6) do not arise.

Lemma 5.17. *G_∞ is not $\mathrm{Fi}_{22}, \mathrm{Fi}_{23}$ or Fi_{24}.*

Proof. Suppose that G_∞ is one of these groups. The dimensions d of minimal $\mathbb{F}_2$-representations for $\mathrm{Fi}_{22}, \mathrm{Fi}_{23}$ and Fi_{24} are 78, 782 and 3774 respectively [Jan05]. In each case, $2^d - 1 > |G_\infty|$, a contradiction.   □

Now, on combining Proposition 5.11 with Lemmas 5.12 – 5.17 we obtain:

Corollary 5.18. *If Hypotheses 4.1 hold, $n > 2\lambda + 2$, and G contains a non-trivial solvable normal subgroup, then $G \cong 2^{2m}.\mathrm{Sp}_{2m}(2)$, $n = 2^{2m}$, and the stabilizer of a point is isomorphic to $\mathrm{Sp}_{2m}(2)$, for some $m \geqslant 2$.*

Proof of Theorem B.   The proof follows immediately from Proposition 5.3, and Corollaries 5.8 and 5.18.

6. Proof of Theorem C

Throughout this section we assume that Hypotheses 4.1 hold. In particular, the assumptions of Theorem C hold.

The proof we present in this case originated with the simple observation that, for the design $\mathcal{D}^a$ described in Example 1.2, each maximal totally isotropic subspace of $\Omega^a = V$ coincides with (the set of points of) a maximal Boolean subdesign of $\mathcal{D}^a$. A similar property was seen to hold in $\mathcal{D}^+$ and this suggested that the theory of polar spaces may shed light on the geometry of designs satisfying Hypotheses 4.1. This turned out to be the case and led, eventually, to the proof that we now present.

In what follows we only need to consider polar spaces in which all lines are incident with exactly 3 points. Such spaces were classified by Seidel [Sei73] (available on-line as a preprint, and also published in his 'Selected works' [Sei91]). We describe his result below using graph-theoretic language. In that direction, we begin with some definitions: for $\infty \in \Omega$, we define $\mathcal{G}_{\mathcal{D},\infty} = (V, E)$ as the graph with vertex set $V = \Omega \setminus \{\infty\}$, and edge set E such that $\{a, b\} \in E$ if and only if $\{\infty, a, b\} \in \mathcal{C}$. This graph is called the *derived graph* of the design $\mathcal{D}$.[3]

Definition 6.1. A graph $\mathcal{G} := (V, E)$ satisfies the *triangle property* if its edge set $E \neq \emptyset$ and, for each pair of adjacent vertices $u, v \in V$, there exists a vertex $w \in V$, adjacent to both u and v, such that every vertex $x \in V\setminus\{u, v, w\}$ is adjacent to exactly one or exactly three vertices in the set $\{u, v, w\}$. We denote by $\mathcal{F}(u, v)$ the set of all vertices w with this property, and if $|\mathcal{F}(u, v)| = 1$, for all $u, v \in V$, then we say that $\mathcal{G}$ has the *strong triangle property*. In this case we denote the unique vertex in $\mathcal{F}(u, v)$ by $f(u, v)$.

Lemma 6.2 ([Sei73, Lemma 4.2]). *If a graph $\mathcal{G}$ has the triangle property and, further, if no vertex of $\mathcal{G}$ is adjacent to every other vertex, then $\mathcal{G}$ has the strong triangle property.*

Our next result shows the relevance of the strong triangle property for us.[4]

Proposition 6.3. *Suppose that Hypotheses 4.1 hold and $n > 2\lambda + 2$. Let $\infty \in \Omega$. Then*
 (i) *$\mathcal{G}_{\mathcal{D},\infty}$ has the strong triangle property; and*
 (ii) *every line of $\mathcal{D}$ containing ∞ is of the form $\{\infty, a, b, f(a, b)\}$.*

Proof. First we prove the triangle property for $\mathcal{G}_{\mathcal{D},\infty}$. Since ∞ lies in 2λ triples in $\mathcal{C}$, the edge set E of $\mathcal{G}_{\mathcal{D},\infty}$ is non-empty. Consider an edge $\{a, b\} \in E$, or equivalently $\{\infty, a, b\} \in \mathcal{C}$. Then there exists $c \in \Omega$ such that $\{\infty, a, b, c\} \in \mathcal{B}$, and therefore also

$$\{\infty, a, c\}, \{\infty, b, c\}, \{a, b, c\} \in \mathcal{C}.$$

---

[3]We refer to $\mathcal{G}_{\mathcal{D},\infty}$ as the derived graph *of the design* $\mathcal{D}$, but note that the definition of this graph refers to $\mathcal{C}$, rather than $\mathcal{B}$. Thus the definition could be extended to a more general setting including, in particular, all regular two graphs.

[4]We asserted above that the totally isotropic subspaces of $\Omega^a = V$ coincide with (the set of points of) a maximal Boolean subdesign of $\mathcal{D}^a$. This observation easily implies that Proposition 6.3 holds for the designs $\mathcal{D}^a$; thus Proposition 6.3 can be thought of as a generalization of this observation.

Thus c is adjacent to both a and b in $\mathcal{G}_{\mathcal{D},\infty}$. Let $x \in \Omega \setminus \{\infty, a, b, c\} = V \setminus \{a, b, c\}$, and consider $\{a, b, c, x\}$. Since $(\Omega, \mathcal{C})$ is a regular two-graph and $\{a, b, c\} \in \mathcal{C}$, there are exactly one or three pairs $\{r, s\} \subset \{a, b, c\}$ such that $\{r, s, x\} \in \mathcal{C}$.

Claim. $\{r, s, x\} \in \mathcal{C}$ if and only if $\{t, x\} \in E$, where $\{r, s, t\} = \{a, b, c\}$. We prove this for the pair $\{a, b\}$, the proofs for the other pairs being identical. The triple $\{a, b, x\} \in \mathcal{C}$ if and only if there exists d such that $\{a, b, x, d\} \in \mathcal{B}$. Using property $((\triangle))$ and the fact that $\{\infty, a, b, c\} \in \mathcal{B}$, we see that this holds if and only if there exists d such that $\{\infty, c, x, d\} \in \mathcal{B}$. The latter property is equivalent to the condition $\{\infty, c, x\} \in \mathcal{C}$, which in turn holds if and only if $\{c, x\} \in E$. This proves the claim.

Since there are exactly one or three pairs $\{r, s\} \subset \{a, b, c\}$ such that $\{r, s, x\} \in \mathcal{C}$, it follows from the claim that x is adjacent in $\mathcal{G}_{\mathcal{D},\infty}$ to exactly one or three vertices in $\{a, b, c\}$. Thus $\mathcal{G}_{\mathcal{D},\infty}$ has the triangle property. Now since $n > 2\lambda + 2$, for each vertex v of $\mathcal{G}_{\mathcal{D},\infty}$, there exists a vertex $u \notin \overline{\infty, v}$, that is, a vertex u of C_∞ which is not adjacent to v. Therefore, by Lemma 6.2, $\mathcal{G}_{\mathcal{D},\infty}$ has the strong triangle property, and part (i) is proved.

For part (ii), consider a line $B = \{\infty, a, b, c\} \in \mathcal{B}$ containing ∞. The arguments above show that the vertex c has the property of Definition 6.1 relative to $\{a, b\}$ and so $c \in \mathcal{F}(a, b)$. Since $\mathcal{G}_{\mathcal{D},\infty}$ has the strong triangle property, this means that $c = f(a, b)$. $\qquad\square$

For the next part we need an alternative definition of the designs $\mathcal{D}^\varepsilon$ from Example 1.3: let V be a $2m$-dimensional vector space over $\mathbf{F}_2$ and let $Q^{\varepsilon'} : V \to \mathbf{F}_2$ be a non-degenerate quadratic form of type ε' (for $\varepsilon' = \pm$) which polarizes to the non-degenerate alternating form φ on V. Write $\varepsilon = (1 - \varepsilon'1)/2$ and define

$$\Omega^\varepsilon = \{v \in V \mid Q^{\varepsilon'}(v) = 0\};$$

$$\mathcal{B}^\varepsilon = \{\{v_1, v_2, v_3, v_4\} \mid v_1, v_2, v_3, v_4 \in \Omega^\varepsilon, \sum_{i=1}^{4} v_i = \mathbf{0}\}.$$

Now we define $\mathcal{D}^\varepsilon = (\Omega^\varepsilon, \mathcal{B}^\varepsilon)$. The fact that this definition is consistent with the definition given in Example 1.3 is (almost) immediate for $\varepsilon' = +$; for $\varepsilon' = -$ it is an exercise.

We are now ready to state Seidel's classification result. We discussed it above in terms of polar spaces, although the statement we use concerns regular two-graphs whose derived graphs have the strong triangle property.

Theorem 6.4 (Seidel's Classification Theorem)**.** *Suppose that a graph $\mathcal{G} = (V, E)$ satisfies the triangle property. Then $\mathcal{G}$ is one of the following:*

    (1) *an edgeless graph, i.e. $E = \emptyset$;*
    (2) *a complete graph;*
    (3) $\mathcal{G}_{\mathcal{D}^a, \mathbf{0}}$, *the derived graph of a design $\mathcal{D}^a$ at the vertex $\mathbf{0}$;*
    (4) $\mathcal{G}_{\mathcal{D}^\varepsilon, \mathbf{0}}$, *the derived graph of a design $\mathcal{D}^\varepsilon$ at the vertex $\mathbf{0}$, for some $\varepsilon \in \mathbb{F}_2$.*

Conversely, all of the listed graphs satisfy the triangle property.

We are almost ready to derive Theorem C from Seidel's classification; we need one lemma first.

Lemma 6.5. *Suppose that $\mathcal{D}_1$ and $\mathcal{D}_2$ are two designs satisfying Hypotheses 4.1 with $n > 2\lambda + 2$. Let ∞_1 (resp. ∞_2) be a point in $\mathcal{D}_1$ (resp. $\mathcal{D}_2$). If $\mathcal{G}_{\mathcal{D}_1, \infty_1}$ and $\mathcal{G}_{\mathcal{D}_2, \infty_2}$ are isomorphic as graphs, then $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic as designs.*

Proof. Let $\mathcal{D}_i = (\Omega_i, \mathcal{B}_i)$, and $\mathcal{G}_i := \mathcal{G}_{\mathcal{D}_i, \infty_i}$, for $i = 1, 2$. Let $\phi : \mathcal{G}_1 \to \mathcal{G}_2$ be a graph isomorphism, and extend ϕ to a bijection $\Omega_1 \to \Omega_2$ by defining $\phi : \infty_1 \mapsto \infty_2$. It is sufficient to show that the image under ϕ of each line in $\mathcal{B}_1$ is a line in $\mathcal{B}_2$. We begin by considering the lines containing ∞_i. By Proposition 6.3, the graphs $\mathcal{G}_i$ have the strong triangle property, and every line of $\mathcal{D}_i$ containing ∞_i is of the form $\{\infty_i, a, b, f_i(a, b)\}$ for a, b vertices of $\mathcal{G}_i$ (where we write f_i for the function f on $\mathcal{G}_i$). Let $\ell = \{\infty_1, a, b, f_1(a, b)\} \in \mathcal{B}_1$ and let $a' = \phi(a), b' = \phi(b)$. By the definition of $f_1(a, b)$, it follows that $\phi(f_1(a, b)) = f_2(a', b')$, and hence $\phi(\ell) = \{\infty_2, a', b', f_2(a', b')\}$ is a line of $\mathcal{D}_2$.

Now consider a line $\ell := \{a, b, c, d\} \in \mathcal{B}_1$ which does not contain ∞_1. Then $\{a, b, c\}$ is a collinear triple from $\mathcal{D}_1$, and applying the two-graph property to the 4-subset $\{\infty_1, a, b, c\}$, we see that ∞_1 is collinear with at least one of $\{a.b\}, \{b, c\}, \{a, c\}$. Without loss of generality we may assume that $\{\infty_1, a, b\}$ is collinear so we have a second line $\ell_1 := \{\infty_1, a, b, f_1(a, b)\} \in \mathcal{B}_1$. Moreover, by the symmetric difference property $(\triangle)$, $\ell'_1 := \{\infty_1, f_1(a, b), c, d\}$ is also a line in $\mathcal{B}_1$, and so by the argument of the previous paragraph, we have $d = f_1(f_1(a, b), c)$. Let $a' = \phi(a), b' = \phi(b), c' = \phi(c)$ and $d' = \phi(d)$. Applying the argument of the previous paragraph again, we see that the images under ϕ of ℓ_1 and ℓ'_1 are lines of $\mathcal{B}_2$ and are $\{\infty_2, a', b', f_2(a', b')\}$ and $\{\infty_2, f_2(a', b'), c', d'\}$ respectively, with $d' = f_2(f_2(a', b'), c')$. Then, by the symmetric difference property $(\triangle)$ for $\mathcal{D}_2$, the 4-subset $\{a', b', c', d'\} = \phi(\ell)$ is also a line of $\mathcal{D}_2$. This completes the proof. $\qquad\square$

Proof of Theorem C. We assume that Hypotheses 4.1 hold. If $n = 2\lambda + 2$, then, since $\mathcal{D}$ is supersimple, we conclude that $\mathcal{D}$ is a $3 - (n, 4, 1)$ design. Thus $\mathcal{G}_{\mathcal{D},\infty}$ is the complete graph and so satisfies the triangle property. On the other hand, if $n > 2\lambda + 2$, then, by Proposition 6.3, $\mathcal{G}_{\mathcal{D},\infty}$ satisfies the triangle property. Thus this conclusion holds in all cases.

We now apply Seidel's Classification Theorem 6.4 to conclude that $\mathcal{G}_{\mathcal{D},\infty}$ is of one of the five listed types. Case (1) can be discarded immediately as it would imply that $\mathcal{D}$ contained no lines.

Case (2), on the other hand, implies that $\mathcal{D}$ is a $3 - (n, 4, 1)$ design and, by counting as before, we conclude that $n = 2\lambda + 2$. Now Proposition 5.3 implies that $\mathcal{D} = \mathcal{D}^b$, a Boolean quadruple system.

Finally, for cases (3), (4) and (5), Lemma 6.5 implies that $\mathcal{D}$ is either $\mathcal{D}^a$ or $\mathcal{D}^\varepsilon$.

$\square$

References

[Asc97]   M. Aschbacher, *3-transposition groups.*, Cambridge: Cambridge University Press, 1997.

[Ban86]   A. S. Bang, *Talteoretiske undersølgelser*, Tidskrifft Math. **5** (1886), no. 4, 130–137.

[Ban69]   E. Bannai, *Multiply transitive permutation representations of finite symmetric groups*, J. Fac. Sci., Univ. Tokyo, Sect. I **16** (1969), 287–296.

[CCN$^+$85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, 1985.

[CH92]   H. Cuypers and J. I. Hall, *The classification of 3-transposition groups with trivial center*, Groups, combinatorics and geometry. Proceedings of the L.M.S. Durham symposium, held July 5-15, 1990 in Durham, UK, Cambridge: Cambridge University Press, 1992, pp. 121–138.

[CKS76]   C. W. Curtis, W. M. Kantor, and G. M. Seitz, *The 2-transitive permutation representations of the finite Chevalley groups*, Trans. Am. Math. Soc. **218** (1976), 1–59.

[Con97]   J. H. Conway, M_{13}, Surveys in combinatorics, 1997 (London), London Math. Soc. Lecture Note Ser., vol. 241, Cambridge Univ. Press, Cambridge, 1997, pp. 1–11.

[DM96]   J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, 1996.

[Fis71]   Bernd Fischer, *Finite groups generated by 3-transpositions. I*, Invent. Math. **13** (1971), 232–246.

[GGNS]   N. Gill, N. I. Gillespie, A. Nixon, and J. Semeraro, *Conway groupoids*, 2015, `http://arxiv.org/abs/1405.1701`.

[GGS]   N. Gill, N. I. Gillespie, and J. Semeraro, *Conway groupoids and completely transitive codes*, 2015, `http://arxiv.org/abs/1410.4785`.

[Her74]   C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, Geom. Dedicata **2** (1974), 425–460.

[Her85]   ——, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II*, J. Algebra **93** (1985), 151–164.

[Jan05]   C. Jansen, *The minimal degrees of faithful representations of the sporadic simple groups and their covering groups*, LMS J. Comput. Math. **8** (2005), 122–144.

[KL90]   P. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.

[Lie87]   M. W. Liebeck, *The affine permutation groups of rank three*, Proc. Lond. Math. Soc. (3) **54** (1987), 477–516.

[LS74]   V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.

[LW91]   S. A. Linton and R. A. Wilson, *The maximal subgroups of the Fischer groups Fi_{24} and Fi'_{24}*, Proc. Lond. Math. Soc. (3) **63** (1991), no. 1, 113–164.

[PSY15]   C. E. Praeger, Á. Seress, and Ş. Yalçınkaya, *Generation of finite classical groups by pairs of elements with large fixed point spaces*, J. Algebra **421** (2015), 56–101.

[Sei73]   J. J. Seidel, *On two-graphs and Shult's characterization of symplectic and orthogonal geometries over GF (2)*, T.H.-Report 73-WSK-02. Eindhoven, Netherlands: Technological University, Dept. of Mathematics. 25 p. (1973)., 1973.

[Sei91]   ——, *Geometry and combinatorics*, Academic Press, Inc., Boston, MA, 1991, Selected works of J. J. Seidel, Edited and with a preface by D. G. Corneil and R. Mathon.

[Shu72]   E. Shult, *Characterizations of certain classes of graphs*, J. Combinatorial Theory Ser. B **13** (1972), 142–167.

[Tay77]   D. E. Taylor, *Regular 2-graphs*, Proc. Lond. Math. Soc. (3) **35** (1977), 257–274.

[Tay92]   ——, *Two-graphs and doubly transitive groups*, J. Combin. Theory Ser. A **61** (1992), no. 1, 113–122.

[Zsi92]   K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), no. 1, 265–284.

Department of Mathematics, University of South Wales, Treforest, CF37 1DL, U.K.
E-mail address: `nicholas.gill@southwales.ac.uk`

Heilbronn Institute for Mathematical Research, Department of Mathematics, University of Bristol, U.K.
E-mail address: `neil.gillespie@bristol.ac.uk`

Centre for the Mathematics of Symmetry and Computation, University of Western Australia, Australia
E-mail address: `cheryl.praeger@uwa.edu.au`

Heilbronn Institute for Mathematical Research, Department of Mathematics, University of Bristol, U.K.
E-mail address: `js13525@bristol.ac.uk`