Séminaire Lotharingien de Combinatoire **79** (2018), Article B79b

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}. One would like to classify all of the Conway groupoids constructed using supersimple designs. In this paper we classify a particular subclass, consisting of those groupoids which satisfy 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. The proof uses Hall's work on 3-transposition groups of symplectic type, and Seidel's work on graphs that satisfy the triangle property.

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 ([GGNS16, GGS17]), 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 design $\mathcal{D} = (\Omega, \mathcal{B})$ consisting of a set Ω of points and a set $\mathcal{B}$ of blocks, which are subsets of Ω of size 4. We call two points *collinear* if there is a block containing both of them. Assume moreover that distinct blocks intersect in at most 2 points. Then for each pair of collinear points $\{a, b\}$, we define a unique permutation $[a, b]$ of Ω as the product of the 2-cycle (a, b) with all 2-cycles (c, d) for which $\{a, b, c, d\} \in \mathcal{B}$. For any path $a_0, \dots, a_n$ in the collinearity graph of $\mathcal{D}$, we define the permutation

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

It is called a *move sequence* starting at a_0 and ending at a_n. Let $\infty \in \Omega$. Then the *Conway groupoid at* ∞ is the sub-groupoid of $\mathrm{Sym}(\Omega)$ generated by all move sequences starting at

2010 *Mathematics Subject Classification.* 20B15, 20B25, 05B05.

∞:[1]

$$\mathcal{L}_\infty(\mathcal{D}) := \{[\infty, a_1, a_2, \ldots, a_k] \mid k \in \mathbb{Z}^+,\ a_1, \ldots, a_k \in \Omega\} \subset \mathrm{Sym}(\Omega). \tag{1.1}$$

The *hole-stabilizer* at ∞ is the sub-groupoid generated by all move sequences starting and ending at ∞:

$$\pi_\infty(\mathcal{D}) := \{[\infty, a_1, a_2, \ldots, a_{k-1}, \infty] \mid k \in \mathbb{Z}^+,\ a_1, \ldots, a_{k-1} \in \Omega\}. \tag{1.2}$$

Notice that a hole-stabilizer is a subgroup of $\mathrm{Sym}(\Omega)$. Moreover, if the collinearity graph of $\mathcal{D}$ is connected, then all hole-stabilizers are conjugate subgroups of $\mathrm{Sym}(\Omega)$.

In this paper we consider the special case where the design $\mathcal{D}$ is a 2-$(n, 4, \lambda)$ design (as defined in §2); such designs with the property that two blocks meeting in at least 3 points are equal are called *supersimple*.

By way of example, if we consider, as Conway did, the (supersimple) 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).[2] 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.

Theorem A. *Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple 2-$(n, 4, \lambda)$ design 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 $n \geqslant 2\lambda + 2$ by an elementary counting argument; furthermore full information concerning the Conway groupoids corresponding to supersimple 2-$(n, 4, \lambda)$ designs with $n = 2\lambda + 2$ is given by Lemma 2.8.

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

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

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 (2.1), and also mentions 3-transposition groups, which are defined in Definition 2.10.

[1]In this paper we do not need to consider the groupoid structure of $\mathcal{L}_\infty(\mathcal{D})$ and will just think of that object as a subset of $\mathrm{Sym}(\Omega)$. For discussion of $\mathcal{L}_\infty(\mathcal{D})$ as a groupoid see, for instance, [GGS17, §2.2].

[2]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 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) *$n = 2^{2m}$ and $\mathcal{L}_\infty(\mathcal{D}) \cong 2^{2m}.\,\mathrm{Sp}_{2m}(2)$;*
(c) *$n = 2^{m-1}(2^m \pm 1)$ and $\mathcal{L}_\infty(\mathcal{D}) \cong \mathrm{Sp}_{2m}(2)$.*

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 $n = 2\lambda + 2$, Lemma 2.8 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, 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 CFSG, and instead we apply Hall's classification of finite 3-transposition groups of symplectic type [Hal89]; this is done in §4.

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 demonstrate 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 $\mathcal{D}^b$ is both a supersimple 2-$(2^m, 4, 2^{m-1} - 1)$ design and a 3-$(2^m, 4, 1)$ Steiner quadruple system; in particular the collinear triples of $\mathcal{D}^b$ form the lines of a regular two-graph. 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

$$e := \begin{pmatrix} 0_m & I_m \\ 0_m & 0_m \end{pmatrix}, \qquad f := \begin{pmatrix} 0_m & I_m \\ I_m & 0_m \end{pmatrix} = e + e^T, \tag{1.3}$$

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 $\varphi(u, v) := u f v^T$. Also, write $\theta(u) := ueu^T \in \mathbb{F}_2$, so that θ is a quadratic form that polarizes to give φ, i.e.,

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

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

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

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

It is straightforward to check that $\mathcal{D}^a$ is a supersimple 2-$(2^{2m}, 4, 2^{2m-2}-1)$ design; in addition, we prove in Lemma 2.9 that $\mathcal{D}^a$ satisfies property $(\triangle)$ and its collinear triples form the lines of a regular two-graph. Finally, by [GGS17, 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 $\pi_\infty(\mathcal{D}^a) = \mathrm{Isom}(\mathrm{V}, \varphi)$, the isometry group of the formed space (V, φ).

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

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

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

Now we define $\mathcal{D}^\varepsilon = (\Omega^\varepsilon, \mathcal{B}^\varepsilon)$. One can check that $\mathcal{D}^\varepsilon$ is a supersimple 2-$(f(m), 4, f(m-1)-1)$ design, where $f(m) = 2^{m-1}(2^m + \varepsilon'.1)$; in addition, we prove in Lemma 2.9 that $\mathcal{D}^a$ satisfies property $(\triangle)$ and its collinear triples form the lines of a regular two-graph. Finally, by [GGS17, Theorem B], $\mathcal{L}_\infty(\mathcal{D}^\varepsilon) \cong \mathrm{Sp}_{2m}(2)$, the isometry group of φ, while $\pi_\infty(\mathcal{D}^\varepsilon) \cong \mathrm{O}_{2m}^{\varepsilon'}(2)$.

In fact, the result in [GGS17, Theorem B] uses a slightly different definition of Ω^ε. This definition requires that we view the integer ε, defined above as either 0 or 1, to be an element of $\mathbb{F}_2$. Now our alternative definition is that

$$\Omega^\varepsilon := \{\theta_v \mid v \in V, \quad \theta(v) = \varepsilon\}.$$

To see that these two definitions are equivalent, one must prove that the quadratic form θ_v is of type ε' if and only if $\theta(v) = \varepsilon$. This is an easy exercise.

The existence of these three families of designs confirms that the possibilities 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 $\mathcal{D}$ is isomorphic to one of the designs $\mathcal{D}^b, \mathcal{D}^a$ or $\mathcal{D}^\varepsilon$ given in Examples 1.1, 1.2 and 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 5.3 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].[3] We use the result of Seidel in §5 to give a fairly short proof of Theorem C; our presentation of Seidel's result in that section (Theorem 5.4) 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 [GGS17, 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 1.7 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 [GGNS16] 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 [GGS17]. 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 proofs of Theorems B and C rely on work of Hall (on 3-transposition groups of symplectic type) and Seidel (on graphs that satisfy the triangle property). Hall's result holds for infinite 3-transposition groups, and versions of Seidel's result hold in the infinite setting. In addition, the examples of groups and designs that appear in Theorems B and C all have infinite analogues and geometric descriptions [CJP93, CP93].

Question 1.5. *Can Theorems B and C be extended to include infinite balanced incomplete block designs?*

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

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

[GGS17, Theorem D] gives strong bounds on the possible parameters of a design $\mathcal{D}$ for which $\mathcal{L}_\infty(\mathcal{D})$ is exotic.

Question 1.6. *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 1.7. *Are there alternative combinatorial structures which can be used to define interesting groupoids?*

In [GGPS17], the authors address Question 1.7 via a concept we call a *pliable function*; full details can be found in §5.1 of that paper. It is possible of course that Question 1.7 may admit many different, interesting answers.

1.2. **Structure of the paper.** In §2 we present background definitions and results concerning block 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; in §4 we prove Theorem B, and in §5, we prove Theorem C. [4]

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.

Finally, all four authors would like to thank the three anonymous referees. Their tremendously insightful comments and suggestions have improved the paper enormously, and we are very grateful to them all.

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, λ) 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 set $\mathcal{B}$ 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.

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

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 $\mu(n-1)/2$ triples in $\mathcal{C}$. The following result is [Tay77, Proposition 3.1].

[4] We note that this structure is different from an earlier version [GGPS] of this paper. This earlier version is available on the math arXiv, and references to the current paper in the survey paper [GGPS17] use numbering from the earlier arXiv version.

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. □

2.2. **Moves and groupoids.** Let $\mathcal{D}$ be a supersimple 2-$(n, 4, \lambda)$ design. For distinct $a, b \in \Omega$, the pair $\{a, b\}$ lies in λ lines $\{a, b, a_i, b_i\}$ and we associate with $\{a, b\}$ the *elementary move*

$$[a, b] = (a, b) \prod_{i=1}^{\lambda} (a_i, b_i), \tag{2.1}$$

which is a permutation in $\mathrm{Sym}(\Omega)$; we also set $[a, a] = 1$, the identity permutation, for each $a \in \Omega$. Note that the right-hand side of (2.1) 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 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 $\mathrm{Sym}(\Omega)$:

(a) $\mathcal{L}(\mathcal{D})$, the set of all move sequences;
(b) $\mathcal{L}_\infty(\mathcal{D})$, the set of all move sequences starting at ∞, called the *Conway groupoid* of $\mathcal{D}$; and
(c) $\pi_\infty(\mathcal{D})$, 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 [GGS17, §2.2] for more discussion. Finally, for distinct $x, y \in \Omega$, we write

$$\overline{x, y} := \{z \in \Omega \mid \text{there exists } \ell \in \mathcal{B} \text{ such that } x, y, z \in \ell\} \tag{2.2}$$

and note in particular that $\overline{x, y}$ contains x and y. The next result is a simple observation and we omit the proof. Note that the union given in part (a) is in fact a *disjoint* union.

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

(a) $\mathcal{L}_\infty(\mathcal{D}) = \bigcup_{x \in \Omega} \pi_\infty(\mathcal{D}) \cdot [\infty, x]$ *(a disjoint union);*
(b) $\pi_\infty(\mathcal{D}) = \langle [\infty, x, y, \infty] \mid x, y \in \Omega \rangle$.

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:*

(a) *G is a group;*
(b) *$G = \mathcal{L}(\mathcal{D}) = \langle [a, b] \mid a, b \in \Omega \rangle$;*

(c) $\mathcal{L}(\mathcal{D}) = \mathcal{L}_x(\mathcal{D})$ *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 $G \subseteq \mathcal{L}(\mathcal{D}) \subseteq H$.

(a) *implies* (c): 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.

(b) *implies* (c): 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 (c) follows.

(c) *implies* (a): 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 (c) 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 (a), 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. □

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

(a) *for all* $a, b, c, d \in \Omega$, $[a,b]^{[c,d]} = [a^{[c,d]}, b^{[c,d]}]$;
(b) *for all* $a, b, c \in \Omega$, $[a,b]^{[b,c]} = [a^{[b,c]}, c]$;
(c) *for all* $a, b, c \in \Omega$, $[b,c] = [a, b, c, a^{[b,c]}]$;
(d) *for all* $\infty \in \Omega$, $\mathcal{L}_\infty(\mathcal{D})$ *is a group of automorphisms of* $\mathcal{D}$.

Proof. First we show that conditions (b) and (c) are equivalent. Writing $[a,b]^{[b,c]} = [b,c][a,b][b,c]$, we see that condition (b) 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 (c) for a, b, c is also equivalent to $[b,c] = [a,b][b,c][a^{[b,c]}, c]$. Thus conditions (b) and (c) are equivalent.

Next, if condition (a) 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 (b) for a, b, c. Thus condition (a) implies condition (b). Now assume that the equivalent conditions (b) and (c) 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 (b) yields

$$[a,b]^{[c,d]} = [a,b]^{[b,c][c,d][d,b^{[c,d]}]} = [a^{[c,d]}, b^{[c,d]}].$$

Next, we show that conditions (a), (b) and (c) imply condition (d). First, we show that $\mathcal{L}_\infty(\mathcal{D})$ is 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 (c) 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 $g = [x_1, x_2, \dots, x_k]$ and a given point x. By induction, there exist $y_1, y_2 \dots, y_l \in \Omega$ and $z_1, z_2 \dots, z_m \in \Omega$ such that

$$[x_1, x_2] = [x, y_1, y_2 \dots, y_l] \text{ and } [x_2, \dots, x_k] = [y_l, z_1, \dots, z_m].$$

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 (a) 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.

Finally we show that condition (d) implies condition (a). Note, first, that if $\mathcal{L}_\infty(\mathcal{D})$ is a group, then Lemma 2.6 implies that $[c, d] \in \mathcal{L}_\infty(\mathcal{D})$ for all $c, d \in \Omega$. Thus, by supposition, $[c, d]$ is an automorphism of $\mathcal{D}$. Let $a, b \in \Omega$ and write

$$[a, b] = (a, b)(x_1, y_1)(x_2, y_2) \cdots (x_\lambda, y_\lambda),$$

where $\{a, b, x_i, y_i\}$ are lines in $\mathcal{D}$ for $i = 1, \dots, \lambda$. Now write $a' = a^{[c,d]}$, $b' = b^{[c,d]}$, $x_i' = x_i^{[c,d]}$ and $y_i' = y_i^{[c,d]}$ for $i = 1, \dots, \lambda$. Now one obtains that $[a^{[c,d]}, b^{[c,d]}] = [a', b']$. Since $[c, d]$ is an automorphism of $\mathcal{D}$ one obtains that $\{a', b', x_i', y_i'\}$ is a line of $\mathcal{D}$ for $i = 1, \dots, \lambda$ and so

$$[a', b'] = (a', b')(x_1', y_1')(x_2', y_2') \cdots (x_\lambda', y_\lambda'),$$

which is clearly equal to $[a, b]^{[c,d]}$, as required. □

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 Theorems B and C.

Lemma 2.8. *Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple 2-$(n, 4, \lambda)$ design with $n = 2\lambda + 2$. The following conditions are equivalent:*

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

In addition, if any of the above conditions hold, then $(\Omega, \mathcal{C})$ is the complete regular two-graph, where $\mathcal{C}$ is the set of collinear triples of $\mathcal{D}$.

Proof. Let us prove that (b) implies (a): 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 $(\triangle)$.

To see that (b) implies (c), simply observe that, for $v \in V = \Omega^b$, the elementary move $[\mathbf{0}, v]$ is equal to the translation $t_v : V \to V, w \mapsto w + v$. This implies that for $\infty = \mathbf{0}$,

$$\mathcal{L}_\infty(\mathcal{D}) \cong \langle t_v \mid v \in V \rangle \cong (V, +),$$

an elementary-abelian group of order 2^m. Then, $\pi_\infty(\mathcal{D})$ is a subgroup of $\mathcal{L}_\infty(\mathcal{D})$ that fixes $\infty = \mathbf{0}$, and so is trivial.

That (c) implies (b) is a consequence of [GGNS16, Theorem B], thus we must prove that (a) implies (b). 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 non-collinear $a, b, c \in \Omega\backslash\{\infty\}$ 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

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

On the other hand, if $a, b, c \in \Omega \setminus \{\infty\}$ are collinear, then

$$a * (b * c) = a * a = \infty = c * c = (a * b) * c.$$

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 $m \geqslant 2$.

Now, observe that $a * b * c * d = \infty$ if and only if $a * b = c * d$ if and only if there exists $x \in \Omega$ such that $\{a, b, x, \infty\}$ and $\{c, d, x, \infty\}$ are lines. But now $(\triangle)$ implies that $\{a, b, c, d\}$ is a line; conversely $\{a, b, c, d\}$ a line implies that $a * b * c * d = \infty$, and we conclude that $\mathcal{D} = \mathcal{D}^b$ is a Boolean quadruple system, as required.

For the final statement note that an immediate consequence of the definition of a Boolean quadruple system is that it is a 3-$(2^k, 4, 1)$ design. Thus $\mathcal{C}$ contains all triples in Ω and $(\Omega, \mathcal{C})$ is the complete regular two-graph. □

The fact that $(\Omega^a, \mathcal{C}^a)$ and $(\Omega^\varepsilon, \mathcal{C}^\varepsilon)$ are also 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 $(\mathcal{L}_\infty(\mathcal{D}^\varepsilon), \pi_\infty(\mathcal{D}^\varepsilon)) = (\mathrm{Sp}_{2m}(2), O^{\varepsilon'}_{2m}(2))$.*

Proof. Recall that $\varphi : V \times V \to \mathbb{F}_2$ is a particular nondegenerate alternating form, and 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 hence $(\Omega, \mathcal{C})$ 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

$$v_1 + v_2 + v_3 + v_4 = v_1 + v_2 + v_5 + v_6 = \mathbf{0}, \tag{2.3}$$

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 $\{v_3, v_4, v_5, v_6\} \in \mathcal{B}$.

$$\begin{aligned}
\rho(v_3, v_4, v_5) &= \varphi(v_3, v_4) + \varphi(v_3, v_5) + \varphi(v_4, v_5) && \text{(definition of } \rho) \\
&= \varphi(v_3, v_4) + \varphi(v_3, v_5) + \varphi(v_1 + v_2 + v_3, v_5) && \text{(by (2.3))} \\
&= \varphi(v_3, v_4) + \varphi(v_1, v_5) + \varphi(v_2, v_5) && \text{(bilinearity of } \varphi) \\
&= \varphi(v_3, v_4) + \varphi(v_1, v_2) && \text{(since } \rho(v_1, v_2, v_5) = 0) \\
&= \varphi(v_3, v_1 + v_2 + v_3) + \varphi(v_1, v_2) && \text{(by (2.3))} \\
&= \varphi(v_1, v_2) + \varphi(v_1, v_3) + \varphi(v_2, v_3) = 0, && \text{(since } \varphi(v_3, v_3) = \rho(v_1, v_2, v_3) = 0)
\end{aligned}$$

as needed. The last assertion is a consequence of [GGS17, 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:

(a) $G = \langle \mathcal{E} \rangle$; and
(b) $\mathcal{E}$ is a union of G-conjugacy classes of involutions;
(c) 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 following special kind of 3-transpositions were introduced and studied by J. I. Hall in [Hal89].

Definition 2.11. A class of 3-transpositions is said to be of *symplectic type* if the following condition holds for all $g_1, g_2, g_3 \in \mathcal{E}$:

$$\text{If } o(g_1g_2) = o(g_1g_3) = o(g_2g_3) = 3, \text{ then } \langle g_1, g_2, g_3 \rangle \cong \mathrm{Sym}(3) \text{ or } \mathrm{Sym}(4).$$

We need a result of Hall [Hal89, Theorem 1], which we state for finite groups (see Hall's comments about the finite case on [Hal89, Section 3, especially page 118]; note that in the case of $\mathrm{Sym}(m)$, the transvections are transpositions and the natural module is the deleted permutation module).

Theorem 2.12 (Hall). *Let $(G, \mathcal{E})$ be a finite group generated by a conjugacy class $\mathcal{E}$ of 3-transpositions of symplectic type. Then there is a split exact sequence*

$$1 \to Q \to G/Z(G) \to G^* \to 1.$$

Here G^* is isomorphic to a symmetric group $\mathrm{Sym}(m)$*, an orthogonal group* $\mathcal{O}_{2n}^{\varepsilon}(2)$ *(with* $\varepsilon = \pm$*), or a symplectic group* $\mathrm{Sp}_{2n}(2)$*. The elementary abelian 2-group Q is a direct sum of natural modules for G^*. The image of $\mathcal{E}$ in $G/Z(G)$ is uniquely determined as the class containing the transvections of any complement G^* except when G is isomorphic to* $\mathrm{Sym}(6)$*.*

3. Proof of Theorem A

Throughout the section we assume the hypotheses of Theorem A, namely:

(a) $(\Omega, \mathcal{B})$ is a supersimple 2-$(n, 4, \lambda)$ design with $n > 2\lambda + 2$;

(b) ∞ 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 $\Delta = \{\infty, a_2, \dots, a_k\}$ 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. $\square$

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

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

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 no 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. □

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 Proposition 3.2, $\pi_\infty(\mathcal{D})$ is transitive on $\Omega \setminus \{\infty\}$. Assume, for a contradiction, 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 claim 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 $c = b^g \in \Delta^g = \Delta$ proving the claim 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 the claim is proved, and hence 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 $(\Omega, \mathcal{C})$ is a regular two-graph. □

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

4. Proof of Theorem B

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

($\triangle$) 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.

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

The first main result of this section is the following.

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

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 $\{y, z\}$. □

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

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

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 there are two possibilities: first X itself may be a line. In this case both w and $[x, y]$ send a to z. Alternatively, we have distinct 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. □

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 $\mathcal{D}$.*
(d) *$[x,y]^g = [x^g,y^g]$ for all $g\in\langle\mathcal{E}\rangle$ and all $x,y\in\Omega$.*
(e) *If two elements $[x,y],[z,w]\in\mathcal{E}$ do not commute then at least one of x,y lies in $\overline{z,w}$.*
(f) *If $[x,y]=(x,y)(x_1,y_1)\cdots(x_\lambda,y_\lambda)$, then $[x,y]=[x_i,y_i]$ for all $i=1,\dots,\lambda$.*

Proof. For (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.

For (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.

To prove (c), we check that $\mathcal{D}$ satisfies the condition given in Lemma 2.7(c). 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 that $[x, y]$ and $[x, z]$ commute (Lemma 4.4). Thus the condition given in Lemma 2.7(c) is satisfied and we conclude that $\mathcal{L}_\infty(\mathcal{D})$ is a group of automorphisms of $\mathcal{D}$. In particular, $\mathcal{L}_\infty(\mathcal{D})$ is a group, and so $\mathcal{L}(\mathcal{D}) = \mathcal{L}_\infty(\mathcal{D})$ by Lemma 2.6.

Item (d) and (e) follow from (c) and Lemma 2.7 (especially statement (a) of Lemma 2.7). Finally, for item (f) observe that, by assumption, $\{x, y, x_i, y_i\}$ are lines for $i = 1, \ldots, \lambda$. But now, condition ($\triangle$) implies that $\{x_i, y_i, x_j, y_j\}$ for all $i, j = 1, \ldots, \lambda$ with $i \neq j$. Part (f) follows. $\square$

Proof of Theorem 4.2. It follows from Lemma 4.5(c) that $G = \mathcal{L}_\infty(\mathcal{D})$ is a subgroup of $\mathrm{Aut}(\mathcal{D})$. We first prove that $(G, \mathcal{E})$ is a 3-transposition group. To do this, we need only verify the three conditions (a),(b) and (c) of Definition 2.10: condition (a), that $G = \langle \mathcal{E} \rangle$, follows from Lemma 4.5(c); condition (b) follows from Lemma 4.5(d); condition (c) is proved in Lemma 4.5(a).

It remains to prove that $\mathcal{E}$ is a union of conjugacy classes of 3-transpositions of symplectic type. Suppose then that $a_1, a_2, a_3 \in \mathcal{E}$ such that $o(a_1a_2) = o(a_1a_3) = o(a_2a_3) = 3$ and let $H = \langle a_1, a_2, a_3 \rangle$. Let X be a non-trivial H-orbit in Ω and let H^X denote the permutation group induced by H on X. We claim that $H^X \cong \mathrm{Sym}(4)$ or $\mathrm{Sym}(3)$.

Without loss of generality we may assume that $\mathrm{supp}(a_1) \cap X \neq \emptyset$, so by Lemma 4.5(f), there exist $x, y \in X$ such that $a_1 = [x, y]$. Suppose $a_2 = [z, w]$ and $a_3 = [s, t]$. Then by Lemma 4.5(e), at least one of $x, y \in \overline{z, w}$, and at least one of $x, y \in \overline{s, t}$, so $\mathrm{supp}(a_i) \cap X \neq \emptyset$ for $i = 1, 2, 3$.

Suppose first that $x \in \mathrm{supp}(a_i) \cap X$, for each $i = 1, 2, 3$. Then by Lemma 4.5(f) there exist $y, z, w \in X \backslash \{x\}$ such that $a_1 = [x, y], a_2 = [x, z], a_3 = [x, w]$, and since $o(a_ia_j) = 3$ for all $i \neq j$, the elements x, y, z, w are pairwise distinct so $|X| \geqslant 4$. Moreover, Lemma 4.5(a) implies that

$$z, w \notin \overline{x, y}, \ \ y, w \notin \overline{x, z}, \ \ y, z \notin \overline{x, w}.$$

These non-inclusions imply that each of the a_i fixes $\{x, y, z, w\}$ setwise, and since X is an H-orbit it follows that $X = \{x, y, z, w\}$ and $H^X \cong \mathrm{Sym}(4)$.

Now suppose that

$$\bigcap_{i=1}^{3}(\mathrm{supp}(a_i)\cap X)=\emptyset. \tag{4.1}$$

Then by Lemma 4.5(a and f), and since $\mathrm{supp}(a_i)\cap X\neq\emptyset$ for all i, we can assume that $a_1=[x,y], a_2=[x,z], a_3=[y,w]$ where $x,y,z,w\in X$ and $z,w\notin\{x,y\}$. We claim that the following all hold.

$$z\notin\overline{x,y},\ \ w\notin\overline{x,y},\ \ w\in\overline{x,z},\ \ z\in\overline{y,w}.$$

The two non-inclusions follow from Lemma 4.5(a), as do the non-inclusions $y\notin\overline{x,z}$ and $x\notin\overline{y,w}$. The final two inclusions follow from this observation together with Lemma 4.5(e). If $w=z$, then these conditions imply that each of the a_i fixes $\{x,y,z\}$ setwise, and as in the previous case we deduce that $X=\{x,y,z\}$ and $H^X\cong\mathrm{Sym}(3)$.

Assume now that $w\neq z$, so that x,y,z,w are pairwise distinct elements of X. The displayed conditions imply that $w^{a_2},z^{a_3}\notin\{x,y,w,z\}$. Let $w'=w^{a_2}$ and $z'=z^{a_3}$. Then by the definition of $\mathcal{E}$, the 4-subsets $\{x,z,w,w'\}$ and $\{y,w,z,z'\}$ are both lines of $\mathcal{D}$, and so by condition ($\triangle$), $\{x,y,w',z'\}$ is also a line of $\mathcal{D}$. Thus $X':=\{x,y,z,w,z',w'\}$ is a 6-element subset of X. Moreover, $a_1=[x,y]=[w',z']$ by Lemma 4.5(f) since $\{x,y,w',z'\}$ is a line of $\mathcal{D}$, and a_1 fixes z and w since these points do not lie in $\overline{x,y}$. We claim that $z'^{a_2}=z'$: this holds if and only if $z^{a_3a_2a_3}=z$. Since $o(a_2a_3)=3$ we have $a_3a_2a_3=a_2a_3a_2$, so $z^{a_3a_2a_3}=z^{a_2a_3a_2}=x^{a_3a_2}=x^{a_2}=z$. A similar argument shows that $w'^{a_3}=w'$. Thus each of the a_i fixes X' setwise, and hence $X=X'$. By making the assignments $(1,2)\mapsto a_1$, $(1,3)\mapsto a_2$ and $(1,4)\mapsto a_3$ we see that H^X is isomorphic to the action of $\mathrm{Sym}(4)$ on unordered pairs from $\{1,2,3,4\}$:

α	α^{a_1}	α^{a_2}	α^{a_3}	Label of α
w	w	w'	y	$\{3,4\}$
w'	z'	w	w'	$\{1,4\}$
x	y	z	x	$\{2,3\}$
y	x	y	w	$\{1,3\}$
z	z	x	z'	$\{1,2\}$
z'	w'	z'	z	$\{2,4\}$

Thus we have $H^X\cong\mathrm{Sym}(4)$ or $\mathrm{Sym}(3)$ proving the claim.

Let $K(X)$ be the kernel of the action of H on X. Suppose (for a contradiction) that $K(X)$ contains a non-identity element g, so $K(X)\neq 1$. Since $\mathrm{supp}(a_i)\cap X\neq\emptyset$, $a_i=[x_i,y_i]$ for some $x_i,y_i\in X$ for $i=1,2,3$. Thus, by Lemma 4.5(d), we deduce that $a_i^g=[x_i,y_i]^g=[x_i^g,y_i^g]=[x_i,y_i]=a_i$. This implies that $K(X)\leqslant Z(H)$. Let Y be an H-orbit that contains a non-trivial $K(X)$-orbit. Then $1\neq K(X)^Y\leqslant Z(H^Y)$. However $Z(H^Y)=1$ since, as we have just proved, $H^Y\cong\mathrm{Sym}(4)$ or $\mathrm{Sym}(3)$, and this is a contradiction. Thus $K(X)=1$, and hence $H\cong\mathrm{Sym}(4)$ or $\mathrm{Sym}(3)$ as required. □

4.1. **Completing the proof of Theorem B.** Note that Lemma 2.8 yields that part (a) of Theorem B holds if $n=2\lambda+2$. If $n>2\lambda+2$ then we deduce three additional properties.

Lemma 4.6. *If Hypotheses* 4.1 *hold and, in addition, $n > 2\lambda + 2$, then the following hold:*

(a) *G is 2-primitive on Ω;*
(b) *$\mathcal{E}$ is a conjugacy class in G;*
(c) *$Z(G) = 1$.*

Proof. By Theorem 4.2, G is a group, and so by Theorem A (c), G is a 2-primitive subgroup of $\mathrm{Sym}(\Omega)$, so part (a) is true. 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 2.7(a), $[a, b]^g = [a^g, b^g] = [c, d]$ and (b) 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]. □

Now, we combine Lemma 4.6 and Theorem 2.12 to obtain the following.

Proposition 4.7. *If Hypotheses* 4.1 *hold and $n > 2\lambda+2$, then there is a split exact sequence*

$$1 \to Q \to G \to G^* \to 1,$$

where $G^* \cong \mathrm{Sym}(m)$ and Q is either trivial, or elementary-abelian and regular on Ω of order $2^{m-(m,2)}$; or $G^* \cong \mathrm{O}^{\pm}_{2m}(2)$ or $\mathrm{Sp}_{2m}(2)$ for some integer m, and the group Q is either trivial, or elementary-abelian and regular on Ω of order 2^m. Furthermore, if Q is non-trivial, then Q is equal to the natural module for G^* over $\mathbb{F}_2$.

Proof. The statement is almost immediate, although we should justify why Q (if nontrivial) is regular on Ω and equal to the natural module for G^* over $\mathbb{F}_2$ (rather than a direct sum of more than one copy of the natural module) — both facts follow from the fact that G acts primitively on Ω. □

Proposition 4.7 is a weaker version of Theorem B — it allows for more possibilities; thus to complete the proof of Theorem B we must show that G^* must be a symplectic group — the next four lemmas do this; the first is a simple counting result. We first show that $G^* \cong \mathrm{Sym}(m)$ cannot occur unless $m = 6$, and $G \cong \mathrm{Sp}_4(2)$.

Lemma 4.8. *If Hypotheses* 4.1 *hold and $n > 2\lambda+2$, then $|\mathcal{E}| = \frac{n(n-1)}{2(\lambda+1)}$. In particular, $|\mathcal{E}| \geq n$.*

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 disjoint 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 disjoint 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. □

Lemma 4.9. *If Hypotheses* 4.1 *hold and $n > 2\lambda + 2$, and if $G \cong \mathrm{Sym}(m)$ with $m \geqslant 5$, then $m = 6$, $G \cong \mathrm{Sp}_4(2)$, and $n = 10$.*

Proof. By Lemma 4.6, we know, first, that $G \cong \mathrm{Sym}(m)$ acts 2-primitively on the elements of Ω; we know, second, that $\mathcal{E}$ is a conjugacy class of G, and, by Theorem 2.12, $\mathcal{E}$ is the class of transpositions (or, possibly, the class of triple-transpositions if $m = 6$). Hence $|\mathcal{E}| = \binom{m}{2}$.

If the action of G on Ω is isomorphic to the action of G on k-subsets of $\{1, \dots, m\}$, then (for instance, by considering the possible intersections of k-subsets) we conclude that 2-primitivity implies that $k = 1$ or $m-1$. Thus $m = n$ and Lemma 4.8 implies that $\lambda = 0$, a contradiction.

Similarly if the action of G on Ω is isomorphic to the action of G on some set of partitions of $\{1, \dots, m\}$, then (for instance, by considering the possible common refinements of two partitions) we conclude that 2-primitivity implies that $m = 6$, and $n = 10$, as required.

Let M be the stabilizer of a point in the action of G on Ω; the actions that remain correspond to M being a primitive subgroup of $\mathrm{Sym}(m)$. Now a classical theorem of Bochert (see, for instance [Wie64, Theorem 14.2]) implies that

$$n = |G : M| \geqslant \left\lfloor \frac{m+1}{2} \right\rfloor! \; .$$

On the other hand, $n > 2\lambda + 2$ and so Lemma 4.8 implies that

$$\frac{m(m-1)}{2} = \frac{n(n-1)}{2(\lambda+1)} > n - 1,$$

and we conclude that

$$\left\lfloor \frac{m+1}{2} \right\rfloor! \leqslant n < \frac{m(m-1)}{2} + 1, \tag{4.2}$$

which implies, immediately, that $m = 5, 6$ or 8. Checking these remaining cases, we use (4.2), the fact that $n(n-1)$ must divide $m!$, and the fact that Lemma 4.8 holds for some positive integer λ, to conclude that $m = 6$ and $n = 10$, as required. □

Lemma 4.10. *Suppose that Hypotheses 4.1 hold, $n > 2\lambda+2$, $G \cong Q \rtimes G^*$, $G^* \cong \mathrm{Sym}(m)$ for some $m \geqslant 5$, and Q is elementary-abelian and regular on Ω and equal to the natural module for G^* over $\mathbb{F}_2$. Then $m = 6$, $G \cong Q \rtimes \mathrm{Sp}_4(2)$, and $|Q| = 2^4$.*

Proof. By Lemma 4.6, G acts 2-primitively on Ω, and so G^* acts primitively on the set of non-trivial elements of Q. Now, since Q is the deleted permutation module for $G^* \cong \mathrm{Sym}(m)$, the elements of Q can be identified with pairs $\{\Lambda, \{1, \dots, m\} \setminus \Lambda\}$ where Λ ranges over the set of even order subsets of $\{1, \dots, m\}$. Then G^* acts in the obvious way on the set of all such pairs and we note that the action preserves the pair of cardinalities: $\{|\Lambda|, m - |\Lambda|\}$. We conclude immediately that, provided $m \neq 6$, G^* has more than one orbit on the set of non-trivial elements of Q, which is a contradiction. If $m = 6$, then we observe that the deleted permutation module for $\mathrm{Sym}(6)$ over $_{\mathbf{2}}$ has dimension $m - (m, 2) = 4$. □

To complete the proof of Theorem B we must show that G^* cannot be an orthogonal group.

Lemma 4.11. *If Hypotheses 4.1 hold and $n > 2\lambda + 2$, then the group G is not isomorphic to $\mathrm{O}^{\pm}_{2m}(2)$ for any $m \geqslant 2$.*

Proof. Suppose that $G \cong \mathrm{O}^{\varepsilon}_{2m}(2)$. If $m < 4$ then one of the following holds:

(a) $G \cong \mathrm{O}_4^+(2) \cong (S_3 \times S_3) : 2$;
(b) $G \cong \mathrm{O}_4^-(2) \cong \mathrm{Sym}(5)$ with $n = 5$ or 6;
(c) $G \cong \mathrm{O}_6^+(2) \cong \mathrm{Sym}(8)$ with $n = 8$ or 15;
(d) $G \cong \mathrm{O}_6^-(2) \cong \mathrm{PSU}_4(2)$.

In cases (a) and (d) the groups in question have no 2-transitive representations while in cases (b) and (c) G is a symmetric group and Lemma 4.9 immediately excludes them. Thus we may assume that $m \geq 4$. By Lemma 4.8, $(2^m - \varepsilon 1)(2^{m-1} + \varepsilon 1) = |\mathcal{E}| \geq n$. On the other hand, [Coo78, Table 1] implies that

$$n \geq \begin{cases} (2^m + 1)(2^{m-1} - 1), & \text{if } \varepsilon = -; \\ 2^{m-1}(2^m - 1), & \text{if } \varepsilon = +. \end{cases} \tag{4.3}$$

Thus if $\varepsilon = -$ we deduce that $n = |\mathcal{E}|$ is odd, which contradicts Corollary 2.4. If $\varepsilon = +$ then [Kan79, Theorem 3] implies that either $m \leq 15$ or else G is acting on non-degenerate or totally isotropic 1-spaces and n is either $2^{m-1}(2^m - 1)$ or $(2^m - 1)(2^{m-1} + 1)$. In the latter case, n is odd, contradicting Corollary 2.4 again. In the former case, $n(n-1) = 2^{m-1}(2^{2m}-1)(2^{m-1}-1)$ and the 2-transitivity of G implies that

$$n(n-1) \mid |G| = 2^{m(m-1)}(2^m - 1) \prod_{i=1}^{m-1} (2^{2i} - 1). \tag{4.4}$$

Now by Zsigmondy's theorem there exists a prime divisor of $2^{2m} - 1$ which does not divide $2^k - 1$ for each $k < 2m$ (since $m \geq 4$) which contradicts (4.4).

In the remaining cases we have that n is even, (4.4) holds and

$$2^{m-1}(2^m - 1) < n < (2^m - 1)(2^{m-1} + 1) \tag{4.5}$$

by (4.3). One quickly deduces that these conditions cannot simultaneously be satisfied for $4 \leq m \leq 15$, completing the proof. $\square$

Lemma 4.12. *If Hypotheses 4.1 hold and $n > 2\lambda + 2$, then the group G is not isomorphic to $Q \rtimes \mathrm{O}_{2m}^{\pm}(2)$ for any $m \geqslant 2$, with Q elementary-abelian and regular on Ω of order 2^{2m}.*

Proof. Suppose that $G \cong Q \rtimes \mathrm{O}_{2m}^{\pm}(2)$ for some $m > 2$. By Lemma 4.6, G acts 2-primitively on Ω. However, as Q acts regularly on Ω, the action of $\mathrm{O}_{2m}^{\pm}(2)$ is isomorphic to its action on the natural module. Since the sets of singular vectors and non-singular 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. $\square$

It follows from Lemmas 4.9–4.12 that, if Hypotheses 4.1 hold and $n > 2\lambda + 2$, then n and the group G satisfy part (b) or (c) of Theorem B. This completes the proof of Theorem B.

5. Proof of Theorem C

Suppose that the the assumptions of Theorem C hold, and let $\mathcal{E}$ denote the set of elementary moves on $\mathcal{D}$, let $\infty \in \Omega$, and $G = \mathcal{L}_\infty(\mathcal{D})$. Then Hypotheses 4.1 hold, and we assume that this is so throughout this section. As explained earlier, the number n of points is at least $2\lambda + 2$. If $n = 2\lambda + 2$, then, by Lemma 2.8, $\mathcal{D}$ is the design $\mathcal{D}^b$ of Example 1.1, so Theorem C holds. From now on we assume that $n > 2\lambda + 2$.

The proof we present in this case began 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 sub-design of $\mathcal{D}^a$. A similar property was seen to hold in $\mathcal{D}^\varepsilon$ with $\varepsilon = 0$, 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 $V = \Omega \backslash \{\infty\}$, 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 $\mathcal{D}$.[5]

Definition 5.1. 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 $x \in V \backslash \{u, v, w\}$ 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. 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 5.2 ([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.[6]

Proposition 5.3. *Suppose that Hypotheses* 4.1 *hold and* $n > 2\lambda + 2$. *Let* $\infty \in \Omega$. *Then*

(a) *each vertex of $\mathcal{G}_{\mathcal{D},\infty}$ is incident with exactly* 2λ *edges;*
(b) *$\mathcal{G}_{\mathcal{D},\infty}$ has the strong triangle property; and*
(c) *every line of $\mathcal{D}$ containing ∞ is of the form $\{\infty, a, b, f(a, b)\}$.*

Proof. Since, for each $a \in V$, the pair $\{\infty, a\}$ lies in λ lines of $\mathcal{D}$, and hence in 2λ triples in $\mathcal{C}$, the edge set E of $\mathcal{G}_{\mathcal{D},\infty}$ is non-empty, and each vertex is incident with exactly 2λ edges, proving part (a).

Now we prove the triangle property for $\mathcal{G}_{\mathcal{D},\infty}$. 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

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

[5] 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.

[6] We asserted above that the totally isotropic subspaces of $\Omega^a = V \cup \{\infty\}$ coincide with (the set of points of) a maximal Boolean sub-design of $\mathcal{D}^a$. This observation easily implies that Proposition 5.3 holds for the designs $\mathcal{D}^a$; thus Proposition 5.3 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 $\mathcal{G}_{\mathcal{D},\infty}$ which is not adjacent to v. Therefore, by Lemma 5.2, $\mathcal{G}_{\mathcal{D},\infty}$ has the strong triangle property, and part (b) is proved.

For part (c), 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 5.1 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 $c = f(a, b)$. □

We are now ready to state Seidel's classification result [Sei73, Theorem 4.15]. 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 5.4 (Seidel's Classification Theorem). *Suppose that a graph* $\mathcal{G} = (V, E)$ *satisfies the triangle property. Then one of the following holds:*

(a) $\mathcal{G}$ *contains a vertex that is incident with all other vertices of* $\mathcal{G}$*;*
(b) $\mathcal{G}$ *is isomorphic to* $\mathcal{G}_{\mathcal{D}^a,\mathbf{0}}$*, the derived graph of a design* $\mathcal{D}^a$ *at the vertex* $\mathbf{0}$*;*
(c) $\mathcal{G}$ *is isomorphic to* $\mathcal{G}_{\mathcal{D}^\varepsilon,\mathbf{0}}$*, 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.

Note that, in Definition 5.1, the definition of the triangle property, we explicitly excluded the edgeless graphs from consideration — they vacuously satisfy the remaining conditions of the definition, but we prefer not to consider them in what follows. This explains their omission in the list above.

We are almost ready to derive Theorem C from Seidel's classification. Note that $\mathcal{G}_{\mathcal{D},\infty}$ has $n - 1$ vertices and valency 2λ (by Proposition 5.3), so the derived graph determines the parameters of the design. The following lemma shows that in fact $\mathcal{G}_{\mathcal{D},\infty}$ determines the design $\mathcal{D}$ up to isomorphism.

Lemma 5.5. *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 5.3, 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. □

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 a complete graph and so satisfies the triangle property. On the other hand, if $n > 2\lambda + 2$, then, by Proposition 5.3, $\mathcal{G}_{\mathcal{D},\infty}$ satisfies the triangle property. Thus in all cases $\mathcal{G}_{\mathcal{D},\infty}$ satisfies the triangle property.

We now apply Seidel's Classification Theorem 5.4 which lists three possible situations. In situation (a), $\mathcal{G}_{\mathcal{D},\infty}$ contains a vertex that is incident to all other vertices of the graph. By Proposition 5.3, each vertex is incident with exactly 2λ edges. Thus $n = 2\lambda + 2$, and hence, by Lemma 2.8, $\mathcal{D} = \mathcal{D}^b$, a Boolean quadruple system. On the other hand, in situations (b) and (c), Lemma 5.5 together with Theorem 5.4 imply that $\mathcal{D}$ is either $\mathcal{D}^a$ or $\mathcal{D}^\varepsilon$, and the proof is complete. □

References

[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.

[Coo78] B. N. Cooperstein, *Minimal degree for a permutation representation of a classical group*, Israel J. Math. **30** (1978), no. 3, 213–235.

[CJP93] H. Cuypers, P. Johnson, and A. Pasini, *On the classification of polar spaces*, J. Geom. **48** (1993), 56–62.

[CP93] H. Cuypers and A. Pasini, *Locally polar geometries with affine planes*, Europ. J. Combin. **13** (1993), no. 1, 39–57.

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

[GGNS16] N. Gill, N. I. Gillespie, A. Nixon, and J. Semeraro, *Generating groups using hypergraphs.*, Quart. J. Math. **67** (2016), no. 1, 29–52.

[GGPS] N. Gill, N. I. Gillespie, C. E. Praeger, and J. Semeraro, *Conway groupoids, regular two-graphs and supersimple designs*, 2015, `http://arxiv.org/abs/1510.06680`.

[GGPS17] ______, *Conway's groupoid and its relatives*, Contemp. Math. **694** (2017), 91–109.

[GGS17] N. Gill, N. I. Gillespie, and J. Semeraro, *Conway groupoids and completely transitive codes*, Combinatorica **38** (2017), no. 2, 1–44.

[Hal89] J. I. Hall, *Some* 3*-transposition groups with normal* 2*-subgroups.*, Proc. Lond. Math. Soc. (3) **58** (1989), no. 1, 112–136.

[Kan79] W. M. Kantor, *Permutation representations of the finite classical groups of small degree or rank*, J. Algebra **60** (1979), no. 1, 158–168.

[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, 1973, 25 pp.

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

[Shu72] E. Shult, *Characterizations of certain classes of graphs*, J. Combin. 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.

[Wie64] H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.

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`