

# Recognizing the Commuting Graph of a Finite Group\*

V. Arvind<sup>†</sup>      Peter Cameron<sup>‡</sup>

## Abstract

In this paper we study the realizability question for commuting graphs of finite groups: Given an undirected graph  $X$  is it the commuting graph of a group  $G$ ? And if so, to determine such a group. We seek efficient algorithms for this problem. We make some general observations on this problem, and obtain a polynomial-time algorithm for the case of extraspecial groups.

## 1 Introduction

The commuting graph  $\Gamma(G)$  of a finite group  $G$  is a simple undirected graph with vertex set  $G$  and undirected edges  $(x, y)$  for each pair of commuting elements  $x \neq y \in G$ . There are variations of this definition in the literature. For example, often the center  $Z(G)$  is removed from the graph, because vertices in  $Z(G)$  are adjacent to every vertex.

The commuting graph of a group has been a topic of research for over sixty years with a variety of results about properties of the commuting graph. The earliest reference to commuting graphs, arguably, is the seminal paper of Brauer and Fowler on centralizers of involutions in simple groups [BF55], where it is used though not explicitly defined.

---

\*This work was initiated during the online series of Research Seminars on “Groups and Graphs”, March-August, 2021, run by Ambat Vijaykumar and Aparna Lakshmanan, Cochin Univ of Science and Technology. The second author acknowledges the Isaac Newton Institute for Mathematical Sciences, Cambridge, for support and hospitality during the programme *Groups, representations and applications: new perspectives* (supported by EPSRC grant no. EP/R014604/1), where he held a Simons Fellowship.

<sup>†</sup>The Institute of Mathematical Sciences (HBNI), Chennai, India. [arvind@imsc.res.in](mailto:arvind@imsc.res.in)

<sup>‡</sup>Mathematics Department, University of St. Andrews, UK. [pjc20@st-andrews.ac.uk](mailto:pjc20@st-andrews.ac.uk).

Our focus is on the recognition problem of commuting graphs. It is an algorithmic problem: given an undirected graph  $X = (V, E)$  as input, we want to check if there is a group  $G$  with  $|V|$  elements such that  $X$  is isomorphic to  $\Gamma(G)$ . Our main results are:

- A deterministic polynomial time algorithm for the case of extraspecial  $p$ -groups (which are a special case of  $p$ -groups of nilpotence class 2).
- A quasipolynomial time algorithm in the general case, based on short (i.e.,  $O(\log^3 n)$  size) presentations for finite groups of order  $n$  combined with Babai's quasipolynomial time algorithm for graph isomorphism.

A natural question in connection with our algorithm for recognizing the commuting graphs of extraspecial groups is whether groups with the same commuting graphs are isoclinic. This holds for extraspecial groups which is exploited by the algorithm, and it is natural to conjecture that this property holds for all groups of nilpotence class 2 (of which extraspecial groups are a subclass). We present counter-examples for class-3 nilpotent groups and conjecture that the property holds for class-2 nilpotent groups.

Additionally, we have some other observations: an efficient reduction of the problem to recognizing the commuting graphs of indecomposable groups, recognizing the commuting graph of dihedral groups along with a generalization to Frobenius groups.

**Some related work.** There is a result by Giudici and Kuzma [GK16] that shows the following: every  $n$ -vertex graph  $X$  with at least two vertices of degree  $n - 1$  is realizable as the commuting graph of a semigroup. It is easy to see that their construction actually gives a polynomial-time algorithm for finding a semigroup with  $n$  elements and a bijection from it to the vertex set of  $X$  such that the edges of  $X$  realize the commuting relation of the semigroup. It is a nearly complete answer to the question in the semigroups setting.

Solomon and Woldar [SW13] have shown that the commuting graph  $\Gamma(G)$  of a finite simple group  $G$  is uniquely determined by the group. That is,  $\Gamma(H) \simeq \Gamma(G)$  if and only if  $G \simeq H$ . We believe that checking if  $X$  is the commuting graph of a simple group should be possible in polynomial time.

## 2 Basic properties

We begin with some preliminary observations that are well-known in the literature (see, e.g., the survey [Ca21]).

Let  $G$  be a finite group. What are the cliques of  $\Gamma(G)$ ? If a vertex subset  $S$  induces a clique in  $\Gamma(G)$  then  $S$  is a commuting subset of elements of  $G$ . Conversely, every commuting subset of elements of  $G$  forms a clique in  $\Gamma(G)$ . Which cliques of  $\Gamma(G)$  correspond to subgroups of  $G$ ? Although we cannot directly infer the group multiplication from  $\Gamma(G)$ , we can observe that

**Lemma 1.** *A vertex subset  $S$  is a maximal clique of  $X$  iff  $S$  is a maximal abelian subgroup of  $G$ .*

*Proof.* Suppose  $H$  is a maximal abelian subgroup of  $G$ . Clearly,  $H$  is a clique in  $X$ . If  $x \notin H$  is adjacent to all of  $H$  then  $x$  commutes with all of  $H$  implying that  $\langle H \cup \{x\} \rangle$  is an abelian subgroup of  $G$  strictly larger than  $H$ . Hence the clique induced by  $H$  is maximal. Conversely, by a similar argument, if  $S$  is a maximal clique in  $X$  then  $S$  is a maximal abelian subgroup of  $G$ .  $\square$

### The vertex degrees of $\Gamma(G)$ and conjugacy classes of $G$

Let  $X = (G, E)$  be the commuting graph of a finite group  $G$ . Let  $x^G$  denote the *conjugacy class* of  $x \in G$ :

$$x^G = \{g^{-1}xg \mid g \in G\},$$

which is the orbit of  $x$  under the conjugation action of  $G$  on itself. Let  $\deg(x)$  denote the degree of a node  $x$  in the graph  $X$ . The closed neighborhood  $\bar{N}(v)$  of any vertex  $v$  of the commuting graph  $\Gamma(G)$  is defined as

$$\bar{N}(x) = \{u \in G \mid u = x \text{ or } (u, x) \in E\}.$$

The orbit-stabilizer lemma [Ca99] directly implies the following

**Proposition 2.** *For each  $x \in G$  its centralizer  $C_G(x)$  is the closed neighborhood  $\bar{N}(x)$  of  $x$  in  $\Gamma(G)$ , and*

$$|C_G(x)| = 1 + \deg(x) = \frac{|G|}{|x^G|}, \text{ for all } x \in G.$$

Let  $m$  denote the number of edges in the commuting graph  $\Gamma(G)$ , and let  $k$  denote the number of conjugacy classes. As  $\sum_{x \in G} \deg(x) = 2m$ , we have:

$$2m + n = \sum_{x \in G} \frac{|G|}{|x^G|} = |G| \cdot \sum_{x \in G} \frac{1}{|x^G|} = n \cdot k. \quad (1)$$

Thus the number of conjugacy classes of  $G$  is  $k = (2m + n)/n$ , which, by the above equation, can be inferred from the commuting graph. Thus, for example, the only regular commuting graphs are the complete graphs, which are the commuting graphs of abelian groups.

The problem of the minimum number  $f(n)$  of conjugacy classes in a group of order  $n$  has a long history. Landau [La03] showed that  $f(n) \rightarrow \infty$  as  $n \rightarrow \infty$ . The first lower bound was by Brauer [Br63] and Erdős and Turán [ET68], who showed that  $f(n) \geq \log \log n$  (logarithms to base 2). This was improved to  $\epsilon \log n / (\log \log n)^8$  by Laci Pyber [Py92]. The exponent 8 was reduced to 7 by Thomas Keller [Ke11], and to  $3 + \epsilon$  by Barbara Baumeister, Attila Maróti and Hung Tong-Viet [B<sup>+</sup>17]. It is conjectured that a bound of the form  $f(n) \geq C \log n$  holds for some constant  $C$ . In the other direction,  $f(n) \leq (\log n)^3$ .

This is relevant to us because an  $n$ -vertex graph  $X$  with  $o(f(n))$  edges cannot be the commuting graph of an  $n$  element group.

At the other extreme, we can rule out very dense incomplete graphs by the 5/8-theorem [Gu73] for finite groups: any graph  $X$  that is not complete and has more than  $5/8 \cdot n^2$  edges cannot be the commuting graph of an  $n$ -element group.

## The commuting graph and maximal abelian subgroups

For a finite group  $G$ , let  $\mathcal{M} \subseteq 2^G$  denote the set of all *maximal abelian subgroups* of  $G$ . Associated with  $G$  is the natural *hypergraph*  $(G, \mathcal{M})$ , where the hyperedges are precisely the maximal abelian subgroups of  $G$ .

**Proposition 3.** *The commuting graph of a finite group determines the hypergraph of its maximal abelian subgroups, and, conversely the maximal abelian subgroups hypergraph of the group determines its commuting graph.*

*Proof.* Let  $G$  be a finite group. Clearly, from the commuting graph  $\Gamma(G)$  we can determine all the maximal cliques which corresponds to all maximal abelian subgroups of  $G$  which implies that the hypergraph of maximal abelian subgroups is determined by  $\Gamma(G)$ . Conversely, given the hypergraph  $(G, \mathcal{M})$  we define the edge set  $E = \{\{u, v\} \mid u, v \in A \text{ for some } A \in \mathcal{M}\}$ . Clearly,  $E$  is the edge set of the commuting graph  $\Gamma(G)$ .  $\square$

**Remark 4.** Since the commuting graph  $\Gamma(G)$  of a finite simple group  $G$  is uniquely determined [SW13], by Proposition 3 it follows that the set of maximal abelian groups of a finite simple group  $G$  uniquely determines  $G$ .

For a finite group  $G$ , the number of maximal abelian subgroups is bounded by  $\binom{|G|}{\log |G|}$  because every subgroup of  $G$  has a generating set of size bounded by  $\log |G|$ . Thus, the hypergraph of maximal abelian subgroups has size at most  $n^{\log n}$  for  $n$  element groups.

This simple bound is tight apart from a constant in the exponent. To see this, consider the extraspecial group  $G$  of order  $p^{2n+1}$  and exponent  $p$ , where  $p$  is an odd prime. The centre has order  $p$ , and  $G/Z(G)$  is isomorphic to a  $2n$ -dimensional vector space  $V$  over the field  $F$  of  $p$  elements, with the bilinear form from  $V \times V$  to  $F$  corresponding to the commutation map from  $G/Z(G) \times G/Z(G)$  to  $Z(G)$ . Maximal abelian subgroups contain the centre, and correspond to maximal totally isotropic subspaces of  $V$ . It is known that the number of such subspaces is  $\prod_{i=1}^n (p^i + 1)$  (see [Tay92]), which is greater than  $p^{n(n+1)}/2$ , roughly  $|G|^{n/4}$ .

### 3 Commuting graphs of product groups

Let  $G$  and  $H$  be finite groups. We now consider the commuting graph  $\Gamma(G \times H)$  of their direct product.

Let  $X = (V, E)$  and  $X' = (V', E')$  be simple undirected graphs. Recall [IK08] that the *strong product* of the graphs  $X$  and  $X'$ , denoted  $X \boxtimes X'$  is a simple undirected graph with the cartesian product  $V \times V'$  as its vertex set and edges defined as follows: distinct pairs  $(u, u')$  and  $(v, v')$  are adjacent if and only if one of the following holds:

- $u = u'$  and  $(v, v') \in E'$ ,
- $v = v'$  and  $(u, u') \in E$ ,
- $(u, u') \in E$  and  $(v, v') \in E'$ .

The following proposition is immediate from the definition.

**Proposition 5.** *For finite groups  $G$  and  $H$*

$$\Gamma(G \times H) = \Gamma(G) \boxtimes \Gamma(H).$$

Since simple undirected graphs can be uniquely factorized into strong products of prime graphs [IK08], which can be computed in polynomial time [FS92], we can derive the following reduction. Recall that a group  $G$  is said to be *indecomposable* if it is not the direct product of two non-trivial groups.

**Theorem 6.** *The problem of recognizing the commuting graphs of groups is polynomial-time reducible to the problem of recognizing the commuting graphs of indecomposable groups.*

*Proof.* Suppose we have an algorithm  $\mathcal{A}$  for recognizing the commuting graphs of indecomposable groups. Using  $\mathcal{A}$  as subroutine, we present a polynomial-time algorithm for recognizing the commuting graphs of all finite groups.

Let  $X = (V, E)$  be an undirected graph on  $n$  vertices which is a purported commuting graph.

First, using the polynomial-time algorithm of Feigenbaum and Schäffer we can factorize  $X$  as

$$X = X_1 \boxtimes X_2 \boxtimes \cdots \boxtimes X_k,$$

where each  $X_i$  is a prime graph on at least two vertices. It follows that  $k \leq \log n$ . Now, for each subset  $S \subseteq [k]$  of the prime graphs we combine them by taking the strong direct product to define the graph

$$X_S = \boxtimes_{i \in S} X_i.$$

Notice that any order in which the strong product of these graphs  $X_i$  is computed yields the same graph, up to isomorphism.

Thus, we have computed graphs  $X_S$  for each subset  $S$  of  $[k]$ . Now, we invoke the subroutine  $\mathcal{A}$  that check if  $X_S$  is the commuting graph of an indecomposable group  $G_S$ , and if so, finds a labeling of the vertices of  $X_S$  with elements of  $G_S$  consistent with the commuting relations.

We can now check if the input graph  $X$  is the commuting graph of a group with a straightforward dynamic programming strategy based on the following easy claim.

**Claim 7.** *For any two disjoint subsets  $S, S'$  of  $[k]$  such that  $X_S$  and  $X_{S'}$  are the commuting graphs of groups  $G_S$  and  $G_{S'}$  the graph  $X_S \boxtimes X_{S'}$  is the commuting graph of the direct product group  $G_S \times G_{S'}$ .*

Now, the algorithm works in stages, computing subsets  $S$  of  $[k]$  along with the graph  $X_S$  and group  $G_S$  such that  $X_S = \Gamma(G_S)$ .

1. **for** stages 0 **to**  $k$  **do**
2. **Stage 0** we have subsets  $S$  such that  $G_S$  is an indecomposable group. We mark all such subsets  $S$  as true. We mark the remaining subsets as false.

3. **Stage  $i + 1$**  For each pair of disjoint subsets  $S$  and  $S'$  marked true in Stages  $1, 2, \dots, i$ , such that  $S \cup S'$  is marked false, we mark  $S \cup S'$  true and compute  $X_{S \cup S'} = X_S \boxtimes X_{S'}$  and  $G_{S \cup S'} = G_S \times G_{S'}$ .
4. **end-for**
5. If  $[k]$  is marked true then the input  $X$  is the commuting graph of the group  $G_{[k]}$  computed above.

The above description checks if  $X$  is the commuting graph of a group with at most  $2^k \leq n$  calls to the subroutine  $\mathcal{A}$  and the running time of the remaining computation is clearly polynomially bounded in  $n$ .  $\square$

**Remark 8.** From Theorem 6 we can easily deduce that the Solomon Woldar theorem [SW13] implies that the direct product of simple groups too have uniquely determined commuting graphs. In fact, the algorithm can be simplified in this case; the following result shows that we only need to consider the indecomposable factors, not arbitrary sums of them.

**Proposition 9.** *The commuting graph of a finite simple group is a prime graph under the strong product.*

*Proof.* We use the fact that, if  $G$  is a non-abelian simple group and  $g \in G \setminus \{1\}$ , then there exists  $h \in G$  such that  $\langle g, h \rangle = G$  [GK00]. Now if  $\langle g, h \rangle = G$ , then

- $g$  and  $h$  are nonadjacent in the commuting graph (since  $G$  is non-abelian);
- $g$  and  $h$  have no non-identity common neighbour in the commuting graph (since a common neighbour would belong to  $Z(G)$ , but  $Z(G) = \{1\}$ ).

Now suppose for a contradiction that  $\Gamma(G)$  is the strong product of two nontrivial graphs with vertex sets  $A$  and  $B$  (i.e., with  $|A| > 1$  and  $|B| > 1$ ). Then we can identify  $G$  with the Cartesian product  $A \times B$ . Suppose that  $(a, b)$  is the identity of  $G$ . Then  $(a, b)$  is joined to all other vertices in the commuting graph.

It follows that  $a$  is joined to every other vertex in  $A$ , and  $b$  to every other vertex in  $B$ ; therefore, for all  $x \in A \setminus \{a\}$ ,  $y \in B \setminus \{b\}$ , the three vertices  $(a, y)$ ,  $(x, b)$  and  $(x, y)$  are adjacent to each other in the commuting graph  $\Gamma(G)$ .

Choose  $y \in B \setminus \{b\}$ , and suppose that  $\langle (a, y), (u, v) \rangle = G$ . Now

- if  $u = a$  then  $(a, y)$  and  $(a, v)$  are both joined to  $(x, b)$  for any  $x \in A \setminus \{a\}$ ;
- if  $v = b$  then  $(a, y)$  and  $(u, b)$  are joined;
- if neither of the above, then  $(a, y)$  and  $(u, v)$  are both joined to  $(u, b)$ .

Each case is contradictory; so our assumption that  $\Gamma(G)$  is the strong product of two nontrivial graphs is false, and the theorem is proved.  $\square$

The proof only requires that  $Z(G) = 1$  and that any non-identity element is contained in a 2-element generating set. These assumptions are valid in any almost simple group  $G$  with simple normal subgroup  $S$  such that  $G/S$  is cyclic [BGH21].

## 4 Commuting graphs of semidirect products

In this section we explore whether we can recognize the commuting graph of semidirect products  $G = H \rtimes K$  if  $H$  and  $K$  are both from group classes whose commuting graphs are easily recognizable.

For example, consider the commuting graph of the dihedral group  $D_n$ . Let  $D_n = \langle a, b \rangle$  where  $a^2 = 1, b^n = 1$  and  $aba^{-1} = b^{-1}$ . For  $n$  odd, 1 is the only dominant vertex, there is an  $n$ -clique corresponding to  $\langle b \rangle$  and the  $ab^i$  are pendant vertices. For  $n$  even, it is a bit different with  $b^{n/2}$  being the other dominant vertex.

Seeking a generalization of this example we first consider Frobenius groups.

### Commuting graphs of Frobenius groups

In this subsection we demonstrate that we can recognise from its commuting graph that a group  $G$  is a Frobenius group.

A finite group  $G$  is a *Frobenius group* if it contains a non-trivial proper subgroup  $H$ , the *Frobenius complement*, with the property that  $H \cap H^g = \{1\}$  for all  $g \notin H$ . The theorem of Frobenius asserts that a Frobenius group has a normal subgroup  $N$ , the *Frobenius kernel*, such that  $NH = G$  and  $N \cap H = \{1\}$ ; every non-identity element of  $G$  is in either the Frobenius kernel or a conjugate of the Frobenius complement. Thompson proved that a Frobenius kernel is nilpotent, and Zassenhaus worked out the detailed structure of a Frobenius complement.



An alternative definition is that  $G$  is a Frobenius group if it is isomorphic to a transitive permutation group which is not regular but in which the stabilizer of any two points is the identity.

Everything we need about Frobenius groups is contained in Passman's book [P68].

In the commuting graph of a group  $G$ , the identity is a *dominant* vertex (that is, joined to all others); indeed, any vertex in the centre is dominant, so if  $Z(G)$  is non-trivial then the commuting graph is 2-connected.

**Lemma 10.** *A Frobenius kernel has non-trivial centre.*

*Proof.* By Thompson's theorem, a Frobenius kernel is nilpotent. □

**Lemma 11.** *A Frobenius complement has non-trivial centre.*

*Proof.* Suppose that  $H$  is a Frobenius complement.

If  $H$  has even order, then it contains a unique involution (which acts on the Frobenius kernel as inversion – so in this case the Frobenius kernel is abelian). This involution is joined to all other vertices.

If  $H$  has odd order, then we use the fact that any subgroup whose order is the product of two primes is cyclic. So all the Sylow subgroups of  $G$  are cyclic. Suppose that the prime divisors of  $|H|$  are  $p_1, p_2, \dots, p_r$  in order.

Now  $H$  is metacyclic; its Fitting subgroup  $F$  is cyclic and contains its centralizer. If  $F$  contains a subgroup  $P$  of order  $p_1$ , then this subgroup is normal in  $G$ ; and conversely, a normal subgroup of prime order is contained in  $F$ . Let  $P$  be a subgroup of order  $p_1$  and suppose that  $P \not\leq F$ . Then  $P$  normalizes but does not centralize  $F$ , so  $P$  must act non-trivially on a cyclic  $p$ -subgroup of  $F$ , and hence on a cyclic subgroup of order  $p \neq p_1$ ; then  $G$  has a non-abelian subgroup of order  $pp_1$ , a contradiction. So  $F$  contains a cyclic subgroup of  $P$  order  $p_1$ .

Now  $P$  is normal in  $G$ , and so  $P \leq Z(G)$  as required, since its automorphism group is divisible only by primes smaller than  $P$ . □

**Theorem 12.** *Let  $G$  be a group of order  $nk$ , where  $n, k > 1$  and  $\gcd(n, k) = 1$ , and let  $\Gamma$  be the commuting graph of  $G$ . Then  $G$  is a Frobenius group with Frobenius complement of order  $k$  if and only if  $\Gamma$  satisfies the following conditions:*

- (a) *there is a dominant vertex  $v$ ;*

(b)  $\Gamma \setminus \{v\}$  has a component of size  $n - 1$  and  $n$  components of size  $k - 1$ , and each component has a dominant vertex.

*Proof.* Suppose that  $G$  is a Frobenius group with kernel  $N$  of order  $n$  and complement  $H$  of order  $k$ . The identity is a dominant vertex. Also non-identity vertices in the kernel do not commute with non-identity vertices in a complement, and non-identity vertices in different complements do not commute with each other. So the components of  $\Gamma \setminus \{1\}$  are as stated, and the lemmas above show that they have dominant vertices.

Conversely, suppose that the commuting graph  $\Gamma$  of  $G$  has properties (a) and (b). If  $C$  is a component with a dominant vertex  $c$ , then the centralizer  $C_G(c)$  is equal to  $C \cup \{1\}$ , which is thus a subgroup of  $G$ . Let  $N$  be the subgroup containing the component of size  $n - 1$ , and let  $H_1, \dots, H_n$  be the subgroups containing the other components.

Since  $\Gamma$  is invariant under automorphisms of  $G$ , we have an action of  $G$  on the set  $\Omega$  of components of  $\Gamma \setminus \{v\}$  of size  $k - 1$  by conjugation. We show that this action satisfies the conditions for a Frobenius group given above.

Choose a prime  $p$  dividing  $k$ . Since  $p$  does not divide  $n$ , the subgroup  $N$  cannot contain a Sylow  $p$ -subgroup; but each of  $H_1, \dots, H_n$  contains such a subgroup. By the conjugacy part of Sylow's theorem,  $G$  acts transitively on  $\Omega$ .

A non-identity element of  $G$ , acting by conjugation, fixes itself, and so fixes the component containing it. We must show that it fixes no other component. Count fixed point of elements of  $G$ . The identity fixes  $n$ ; non-identity elements of  $N$  fix  $\geq 0$ ; and the remaining elements fix  $\geq 1$ . So the sum of the fixed point numbers is at least  $n + n(k - 1) = nk$ . But, by the Orbit-counting Lemma, this sum is equal to  $|G| = nk$ , since  $G$  is transitive. So equality holds; non-identity elements of  $N$  fix no point, and the remaining non-identity elements fix exactly one point each. So  $G$  is a Frobenius group.  $\square$

Can we go further and identify an individual Frobenius group from its commuting graph? The above analysis gives us the commuting graphs of the Frobenius kernel and complement, so we would need to be able to recognise these (albeit from rather restricted classes of groups). But we would also need to identify the fixed-point-free action of  $H$  on  $N$ , and it is not clear how to do this from the graph. Given  $H$  and  $N$ , we could simply compute all fixed-point-free actions of  $H$  on  $N$ , and conclude that  $G$  was the semidirect product given by one of these actions.

## 5 Commuting graphs of $p$ -groups of order $p^3$

Let  $G$  be a nonabelian  $p$ -group of order  $p^3$ . As it is nonabelian, its center  $Z(G)$  is  $C_p$  (cyclic of order  $p$ ). Furthermore, as  $G/Z(G)$  is abelian, being order  $p^2$ , and it cannot be cyclic for otherwise  $G$  would be abelian,  $G/Z(G) = C_p \times C_p$ .

It follows that the  $G$ -homomorphism  $\phi : x \mapsto x^p$  has image contained in  $Z(G) = C_p$ . Therefore,  $\ker(\phi)$  is a subgroup of order  $p^2$  or  $p^3$ .

**Case 1:  $\ker(\phi)$  is order  $p^3$**  Then every nontrivial element in  $G$  has order  $p$ .

For any  $x \notin Z$ , we have  $\langle x, Z \rangle = \{x^i z^j \mid 0 \leq i, j \leq p-1\}$  is a  $G$ -subgroup of order  $p^2$  (which is always abelian).

Given the graph  $X$ , we can first identify  $Z$  (the degree  $n-1$  vertices). Take any vertex  $x \notin Z$ . Then  $\{x\} \cup Z$  is a clique which we can keep growing as follows: if  $S$  is the current clique pick any vertex  $y$  not in  $S$  such that  $y$  is adjacent to all of  $S$  and include it. Since  $\langle Z, x \rangle$  is an abelian subgroup of  $G$  and is of order  $p^2$ , we will be able to grow the clique to precisely  $\langle Z, x \rangle$  and no further (because  $G$  is not abelian).

We can repeat the above process of building a  $p^2$ -size clique starting with a fresh vertex  $x'$  each time to obtain  $p+1$  cliques corresponding to the subgroups of size  $p^2$ . These cliques all intersect pairwise at  $Z$  and are otherwise mutually disjoint. There will be no edges in the graph between a  $z^i x^j$  and a  $z^\ell y^m$  if  $x \neq y$  and  $0 < j, m \leq p-1$ .

Thus, we can recognize precisely the commuting graphs of such groups of order  $p^3$ .

**Case 2:  $\ker(\phi)$  is order  $p^2$ :** In this case there are elements in  $G$  of order  $p^2$  (not  $p^3$  because  $G$  is nonabelian). Indeed, each element in  $G \setminus \ker(\phi)$  is order  $p^2$ . Clearly, the cyclic groups  $\langle x \rangle$ ,  $x \in G \setminus \ker(\phi)$ , all intersect precisely at the group's center  $Z$  (like a sunflower's center). That would account for

$$\frac{(p^3 - p^2)}{(p^2 - p)} = p$$

such cyclic groups of order  $p^2$ . These  $p^3 - p^2$  vertices in the graph  $X$  would form a "sunflower" of  $p$  cliques, each of size  $p^2$  and all intersecting at the center  $Z$ .

The remaining  $p^2$  elements are in  $\ker(\phi)$  which will also form a clique of

size  $p^2$ . Thus, we again have a sunflower of  $p + 1$  cliques of size  $p^2$  each that pairwise intersect precisely at the center  $Z$  and no other element is repeated.

This commuting graph structure is exactly as in the first case and can be easily detected.

## 6 Recognizing commuting graphs of extraspecial groups

Let  $p$  be an odd prime. Let  $G$  be an extraspecial group of order  $p^{2n+1}$ ,  $n \geq 2$ , and let  $X = (V, E)$  be an undirected graph with  $p^{2n+1}$ .

Our goal is to design a polynomial-time algorithm that takes a simple undirected graph  $X = (V, E)$ , with  $p^{2n+1}$  vertices, as input and determines if  $X$  is the commuting graph of an extraspecial group  $G$  of order  $p^{2n+1}$ . Moreover, the algorithm is required to find a bijection  $v \mapsto g_v$  labeling each vertex  $v \in V$  by a unique group element  $g_v \in G$ .

We recall that for an extraspecial group  $G$  its centre  $Z(G)$  is of order  $p$  and coincides with its derived subgroup  $G'$  and the Frattini subgroup  $\Phi(G)$ . Furthermore, it is known that there are exactly two non-isomorphic extraspecial groups of order  $p^{2n+1}$ , for each prime  $p$ . They are given by the following generator-relator presentations:

- $G_1 = \langle z, x_i, y_i, 1 \leq i \leq n \rangle$  such that  $[x_i, x_j] = 1$ ,  $[y_i, y_j] = 1$  for all  $i, j$ , and  $[x_i, y_j] = 1$  for all  $i \neq j$ .  $[x_i, y_i] = z$  for all  $i$ , and  $x_i^p = y_i^p = z^p = 1$  for all  $i$ . The center  $Z(G_1) = \langle z \rangle$ .
- $G_2 = \langle z, x_i, y_i, 1 \leq i \leq n \rangle$  such that  $[x_i, x_j] = 1$ ,  $[y_i, y_j] = 1$  for all  $i, j$ , and  $[x_i, y_j] = 1$  for all  $i \neq j$ . And  $[x_i, y_i] = z$  for all  $i$ , and  $x_i^p = 1 = z^p$ ,  $y_i^p = z$  for all  $i$ . The center  $Z(G_2) = \langle z \rangle$ .

It is clear from the above that  $G_1$  and  $G_2$  have isomorphic commuting graphs. Thus, our aim is to design an algorithm that identifies the vertices of the input graph  $X$  with, say  $G = G_1$ , such that all commuting pairs are realized by the edges of  $X$ .

First, notice that the vertices of  $X$  corresponding to the centre  $Z = Z(G)$  of  $G$  are easily detected as precisely the  $p$  vertices in  $X$  of degree  $p^{2n+1} - 1$  each.

In either case ( $G \in \{G_1, G_2\}$ ), we note that its centre  $Z(G)$  can be identified with the additive group of  $\mathbb{F}_p$ , and the quotient  $G/Z(G)$  with a

$2n$ -dimensional vector space  $V(2n, p)$  over  $\mathbb{F}_p$ . Moreover, the commutation map

$$(xZ(G), yZ(G)) \mapsto [x, y]$$

from  $G/Z(G) \times G/Z(G)$  to  $Z(G)$  defines a *symplectic form* on  $V(2n, p)$ , that is, a non-degenerate alternating bilinear form  $\langle, \rangle$  on  $V(2n, p)$  with values in  $\mathbb{F}_p$ . More precisely, we recall the following.

Let  $V(2n, p)$  be the  $2n$ -dimensional vector space over  $\mathbb{F}_p$  which is isomorphic to  $G/Z(G)$ , where  $G$  is an extraspecial group of order  $p^{2n+1}$ . Let  $\langle, \rangle$  be a *symplectic form* on  $V(2n, p)$ . I.e.,

$$\langle, \rangle : V(2n, p) \times V(2n, p) \rightarrow \mathbb{F}$$

is a bilinear form that is *antisymmetric* and  $\langle u, u \rangle = 0$  for all vectors  $u$ .

We additionally know that  $\langle, \rangle$  is *non-degenerate*: there is no nonzero  $u$  such that  $\langle u, v \rangle = 0$  for all  $v \in V(2n, p)$ . For a subset  $S \subset V(2n, p)$  let

$$S^\perp = \{u \in V(2n, p) \mid \langle u, v \rangle = 0 \text{ for all } v \in S\}$$

denote the subspace of  $V(2n, p)$  consisting of vectors *orthogonal* to each vector in  $S$ :  $u$  is orthogonal to  $v$  if  $\langle u, v \rangle = 0$ .

The following is immediate.

**Lemma 13.** *From the extraspecial group  $G$  given by its multiplication table as input, we can construct its corresponding symplectic form  $\langle, \rangle$ , as an explicit bilinear map from  $\mathbb{F}_p^{2n} \times \mathbb{F}_p^{2n} \rightarrow \mathbb{F}_p$ , in polynomial time.*

**Definition 14.** The *orthogonality graph* of  $V(2n, p)$  is an undirected simple graph with  $V(2n, p)$  as vertex set such that for each pair of distinct vectors  $u, v \in V(2n, p)$ ,  $(u, v)$  is an undirected edge in the graph iff  $\langle u, v \rangle = 0$ .

For the actual input  $X$ , which is the purported commuting graph of  $G$ , we now show that the orthogonality graph of the underlying symplectic form can be efficiently computed.

**Lemma 15.** *Given as input a candidate commuting graph  $X = (V, E)$ , of the extraspecial group  $G$  of order  $p^{2n+1}$ , we can compute in polynomial time an undirected graph  $X_o = (V_o, E_o)$  with  $|V_o| = p^{2n}$  such that  $X_o$  is the orthogonality graph of the symplectic form  $\langle, \rangle$  if and only if  $X$  is the commuting graph of  $G$ .*

*Proof.* If  $X$  is the commuting graph of  $G$  then the subset of all *dominating vertices* of  $X$  (i.e., vertices of degree  $|V| - 1$  in  $X$ ) corresponds precisely

to the elements of the centre  $Z(G)$ . Hence, there are exactly  $p$  of them in  $X$ . Let  $Z$  denote this subset of vertices. If that number is different from  $p$  then we can reject  $X$  as being the commuting graph of an order  $p^{2n+1}$  extraspecial group.

Next, recall that the *closed neighborhood*  $\bar{N}(v)$  of a vertex  $v \in V$  is defined as

$$\bar{N}(v) = \{u \in V \mid (u, v) \in E\} \cup \{v\}.$$

Vertices  $v_1, v_2, \in V$  are called *closed twins* if  $\bar{N}(v_1) = \bar{N}(v_2)$ . We can identify all the subgroups of  $G$  of order  $p^2$  by defining the following equivalence relation on  $V \setminus Z$ . This clearly defines an equivalence relation on vertices in  $V \setminus Z$ .

For each order  $p^2$  subgroup  $H \leq G$  such that  $Z(G) \leq H \leq G$ , it is easy to see that for all  $h, h' \in H \setminus Z(G)$  their centralizers in  $G$  coincide:  $C_G(h) = C_G(h')$ . Hence, if  $X$  is the commuting graph of  $G$ , then  $\bar{N}(u) = \bar{N}(v)$  for all  $u, v \in U \setminus Z$ , where  $U$  corresponds to  $H$ . On other hand, if  $u \in H \setminus Z$  and  $v \notin H$  then we can use the symplectic form  $\langle \cdot, \cdot \rangle$  to see that for any two linearly independent vectors  $v_1, v_2 \in V(2n, p)$  we can find a vector orthogonal to exactly one of them (by expressing  $v_1, v_2$  using the basis  $\{e_i, f_i, 1 \leq i \leq n\}$ ). Thus, the equivalence classes defined by the closed-twins equivalence relation identifies all  $p^2 - p$  size vertex subsets of  $V \setminus Z$  that corresponds to  $H \setminus Z(G)$  for each subgroup  $H$  of order  $p^2$  such that  $Z(G) \leq H \leq G$ . The number of such equivalence classes is

$$\frac{p^{2n+1} - p}{p^2 - p} = 1 + p + p^2 + \dots + p^{2n-1}.$$

To obtain the corresponding orthogonality graph  $X_o = (V_o, E_o)$  we apply the following three steps to  $X$ .

- (a) Collapse each equivalence class in  $V \setminus Z$  into a single vertex. This gives rise to a set  $V_c$  of  $\sum_{i=0}^{2n-1} p^i$  many vertices. The edges between vertices in  $V_c$  are naturally inherited from  $X$ .
- (b) Include a new vertex  $v_0$  corresponding to the 0 element of  $V(2n, p)$ ; this corresponds to  $p$  dominant vertices of  $X$ .
- (c) The process of collapsing the closed-twin equivalence classes identifies vectors  $v \in V(2n, p)$  with all the  $p-1$  nonzero scalar multiples  $\alpha v$ ,  $\alpha \in \mathbb{F}_p^*$ . We restore the  $p-1$  copies by replacing each  $v \in V_c$  by  $p-1$  copies. The edges between these vertices are naturally inherited.

By construction,  $X_o$  is the orthogonality graph of the symplectic form on  $V(2n, p)$  defined by the commutation map of  $G$  if and only if  $X$  is the commuting graph of  $G$ .  $\square$

## 6.1 Recognizing the orthogonality graph of the symplectic form

We now show that the orthogonality graph of a non-degenerate symplectic form on  $V(2n, p)$  can be recognized in polynomial time.

**Theorem 16.** *Given a simple undirected graph  $X = (V, E)$  on a vertex set  $V$  of size  $p^{2n}$  vertices, in time polynomial in the size of  $X$  we can recognize if  $X$  is the orthogonality graph of some symplectic form on  $V(2n, p)$  and, if so, in polynomial time we can also compute a bijection from  $V$  to  $V(2n, p)$  and determine a symplectic form  $\langle, \rangle$  that is consistent with  $X$ .*

*Proof.* Let  $X = (V, E)$  be a graph with  $p^{2n}$  vertices,  $p$  prime. Our algorithm is based on an inductive argument. We know that  $V(2n, p)$  has a *symplectic basis* of  $2n$  vectors of the form  $e_i, f_i, 1 \leq i \leq n$  such that

- $\langle e_i, f_i \rangle = 1$  for all  $i$ .
- $\langle e_i, f_j \rangle = 0$  for all  $i \neq j$ .
- $\langle e_i, e_j \rangle = 0$  for all  $i, j$ .
- $\langle f_i, f_j \rangle = 0$  for all  $i, j$ .

Moreover, we can construct such a basis for  $V(2n, p)$  by the following greedy process. Pick  $e_1 \neq 0$  in  $V(2n, p)$  arbitrarily. Then pick any vector  $f_1 \neq 0$ , suitably scaled, such that  $\langle e_1, f_1 \rangle = 1$ . Notice that  $f_1$  must exist as the symplectic form is non-degenerate. Then notice that the subspace  $\{e_1, f_1\}^\perp$  is a  $2n - 2$  dimensional symplectic space  $V'$  (w.r.t. the same symplectic form). We can continue with the basis construction by induction applied to  $V'$ .

The problem we will solve is to efficiently simulate the above construction process given only the purported commuting graph  $X = (V, E)$  as input. First of all, the zero vector  $0$  is the only vertex in  $X$  adjacent to all others and is easily identified. Let  $e_1$  be any other vertex. We will choose  $f_1$  as any vertex not adjacent to  $e_1$ . The scaling factor does not matter since a

vector  $v$  and  $\alpha v, \alpha \in \mathbb{F}_p^*$  have identical neighborhoods in the orthogonality graph of the symplectic space  $V(2n, p)$ . Let

$$V' = \{v \in V \mid (v, e_1) \in E \text{ and } (v, f_1) \in E\}.$$

That is,  $V'$  is the common neighborhood of  $e_1$  and  $f_1$ . Let  $X'$  be the subgraph of  $X$  induced by the vertex subset  $V'$ . We have the following easy observation.

**Claim 17.** *If  $X$  is the orthogonality graph of a  $2n$ -dimensional symplectic space over  $\mathbb{F}_p$  then the graph  $X'$  is the orthogonality graph of a symplectic space of dimension  $2n - 2$  over  $\mathbb{F}_p$ .*

Inductively, therefore, we assume that we have checked that  $X'$  is indeed the orthogonality graph of a  $2n - 2$ -dimensional symplectic space over  $\mathbb{F}_p$  and we have a labeling of the vertices of  $V'$  by linear combinations  $\sum_{i=2}^n (\alpha_i e_i + \beta_i f_i), \alpha_i, \beta_i \in \mathbb{F}_p$  that is consistent with the orthogonality relation of a symplectic form  $\langle, \rangle$ .

The remaining task for the algorithm is to find a consistent labeling of the vertices in  $V \setminus V'$ .

**Claim 18.** *A vertex  $v \in V \setminus V'$  can be labeled by a nonzero vector  $\alpha e_1 + \beta f_1$  in  $V(2n, p)$ ,  $\alpha, \beta \in \mathbb{F}_p$ , if and only if  $(v, u) \in E$  for all  $u \in V'$ .*

*Proof of Claim.* Consider the orthogonality graph of  $V(2n, p)$ . Let  $V(2n - 2, p)$  denote the subspace spanned by  $e_i, f_i, 2 \leq i \leq n$ . Clearly, every vector of the form  $\alpha e_1 + \beta f_1, \alpha, \beta \in \mathbb{F}_p$  is orthogonal to each vector in  $V(2n - 2, p)$ . Conversely, consider a vector  $\alpha e_1 + \beta f_1 + v \in V(2n, p)$ , where  $v \in V(2n - 2, p)$  is nonzero. Since  $V(2n - 2, p)$  is non-degenerate, there is a  $u \in V(2n - 2, p)$  such that  $\langle v, u \rangle \neq 0$  which implies  $\langle \alpha e_1 + \beta f_1 + v, u \rangle = \langle v, u \rangle \neq 0$ .

Thus, we will find precisely  $p^2 - 1$  many such vertices in  $V$  that are adjacent to all of  $V'$ , of which we have already labeled two vertices as  $e_1$  and  $f_1$ .

The next claim is also clear from the construction of the  $e_i, f_i$  basis.

**Claim 19.** *If  $X = (V, E)$  is the orthogonality graph of the symplectic space  $V(2n, p)$  and  $V'$  corresponds to the subspace  $V(2n - 2, p)$  spanned by  $\{e_i, f_i \mid 2 \leq i \leq n\}$  then the subset*

$$V[e_1] = \{v \in V \setminus V' \mid (v, e_1) \in E \text{ and } (v, f_1) \notin E\}$$

*consists precisely of those vertices in  $V \setminus V'$  that correspond to the subset of vectors  $\{\alpha e_1 + V' \mid \alpha \neq 0\}$  of  $V(2n, p)$ .*



Furthermore, the vertices that correspond to  $\alpha e_1, \alpha \neq 0$  are precisely those vertices in  $V[e_1]$  whose neighborhood in  $X$  is identical to the neighborhood of the vertex labeled  $e_1$ .

From the above claim it follows that we can identify the vertex subset  $V[e_1]$ , corresponding to  $\alpha e_1 + V', \alpha \neq 0$ . Similarly, we can identify  $V[f_1]$ , corresponding to  $\beta f_1 + V', \beta \neq 0$ .

### Labeling vertices in $V[e_1]$ and $V[f_1]$

Consider the vertex subset  $V[e_1]$ . For each  $u' \in V(2n-2, p)$  and  $u \in V(2n-2, p)$ , notice that

$$\langle u', u \rangle = 0 \text{ if and only if } \langle u', \alpha e_1 + u \rangle = 0, \alpha \in \mathbb{F}_p^*,$$

because  $\langle u', e_1 \rangle = 0$  for all  $u' \in V(2n-2, p)$ .

Let  $N(u, V')$  denote the neighborhood of  $u$  in  $V'$ . The above statement is equivalent to saying that for each vertex  $u \in V'$  there are exactly  $p-1$  vertices  $u'' \in V[e_1]$  such that

$$N(u'', V') = N(u, V').$$

We can label these  $p-1$  vertices arbitrarily as  $\alpha e_1 + u$ , for  $\alpha \in \mathbb{F}_p^*$ . Thus, in polynomial time, we can obtain the correct labeling of all vertices in  $V[e_1]$  by the vectors in  $\alpha e_1 + V(2n-2, p), \alpha \neq 0$ .

Similarly, we can obtain the correct labeling of  $V[f_1]$  by the vectors in  $\beta f_1 + V(2n-2, p)$ .

### Labeling vertices in $V[e_1 + \beta f_1], \beta \neq 0$

For  $\beta \neq \beta' \in \mathbb{F}_p$ , we have

$$\langle e_1 + \beta f_1, e_1 + \beta' f_1 \rangle = \beta' - \beta \neq 0.$$

Hence, the vertices to be labeled  $e_1 + \beta f_1$  and  $e_1 + \beta' f_1$  are not adjacent in  $X$ . Since  $\langle e_1 + \beta f_1, v \rangle = 0 = \langle e_1 + \beta' f_1, v \rangle$  for all  $v \in V'$ , these two vertices are adjacent to each vertex in  $V'$ .

Notice that these two vertices could have been picked instead of  $e_1$  and  $f_1$  in the first place and we would have still obtained the same subset  $V'$  as the subspace  $V(2n-2, p)$ . Thus, we can repeat the previous argument (for

labeling vertices of  $V[e_1]$  to label each of the vertex subsets  $V[e_1 + \beta f_1]$  for  $\beta \in \mathbb{F}_p^*$ .

Putting it together, clearly if  $X$  is the orthogonality graph of some non-degenerate symplectic form on  $V(2n, p)$  the above algorithm verifies that by constructing a (possibly different) symplectic form on  $V(2n, p)$ , consistent with the orthogonality graph.

**Running time analysis** Let  $T(n)$  denote the running time for constructing a symplectic form  $\langle, \rangle$  for  $V(2n, p)$  consistent with  $X$  as the orthogonality graph. The inductive construction and the rest of the computation implies the recurrence  $T(n) = O(|V|^2) + T(n - 1)$ , which gives an overall cubic bound  $T(n) = O(|V|^3) = O(p^{6n+3})$  on the running time.

Putting it together, we have a polynomial-time algorithm that checks if  $X$  is the orthogonality graph for the symplectic space by finding out a labeling of vertices by the vectors along with a consistent symplectic form.  $\square$

Putting everything together, we have the following.

**Theorem 20.** *Given  $X = (V, E)$  with  $p^{2n+1}$  vertices we can determine in polynomial time if it is the commuting graph of an extraspecial group of order  $p^{2n+1}$  and, if so, label vertices by unique group elements satisfying the commuting relation.*

*Proof.* By Lemma 15 we can obtain the graph  $X_o = (V_o, E_o)$  from  $X$  in polynomial time. By Theorem 16 we can check if  $X_o$  is the orthogonality graph of a symplectic form  $\langle, \rangle$  on  $V(2n, p)$  and also find the symplectic form.

From the proof of Lemma 15, we have the following observations:

- The vertex of degree  $|V_o| - 1$  in  $X_o$  is the 0 element of  $V(2n, p)$ , and corresponds to  $Z$  in  $G$ .
- For each vertex  $x \in V_o$  there is a closed-twins equivalence class of size  $p - 1$  containing  $x$ . There is a corresponding subset of vertices  $H_x \setminus Z$  in  $X$  of size  $p^2 - p$ , where  $H_x$ , in turn, corresponds to an order- $p^2$  subgroup of  $G$  that contains  $Z$ . We have a labeling of the vertex  $x$  by a linear combination  $\sum_{i=1}^n (\alpha_i e_i + \beta_i f_i)$ , and the remaining  $p - 2$  vertices in the equivalence class are labeled by nonzero scalar multiples of this linear combination.

Now, using the description of the extraspecial group  $G_1$  we can label the vertices of the clique  $H_x \setminus Z$  with the group elements

$$z^j \cdot \left( \prod_{i=1}^n x_i^{\alpha_i} \cdot y_i^{\beta_i} \right)^k, 0 \leq j \leq p-1, 1 \leq k \leq p-1.$$

This will give us the labeling of  $X$  with the elements of the extraspecial group  $G_1$  of order  $p^{2n+1}$ , consistent with the commuting graph  $X$ . This completes the proof.  $\square$

## 7 A quasipolynomial time algorithm in the general case

We now describe a  $2^{O(\log^3 n)}$  time algorithm for checking if a given  $n$ -vertex graph is the commuting graph of some  $n$ -element group and, if so, labeling the vertices of the graph by the group elements consistent with all the commuting pairs.

This algorithm is based on a result of McIver and Neumann [MN87] that bounds the number of  $n$  element groups by  $2^{O(\log^3 n)}$ . The theorem is sharpened by subsequent work of Babai et al [BGK<sup>+</sup>97] on short presentations for finite groups. They show that groups of order  $n$  (that do not have a specific finite simple group type, called the Ree groups, as section) have short generator-relator presentations  $\langle Y|R \rangle$  of size  $O(\log^3 n)$ . The crux of their proof is that all simple groups of  $n$  elements (except the Ree groups) have generator-relator presentations of size  $O(\log^2 n)$ . Combined with the fact that  $n$  element groups have composition series of  $\log n$  length gives the  $O(\log^3 n)$  bound.

**Theorem 21.** *There is a  $2^{O(\log^3 n)}$  time algorithm that recognizes if a given  $n$ -vertex graph is the commuting graph of a group of order  $n$  that does not have the Ree groups as section.*

*Proof.* Given such a generator-relator presentation  $\langle Y|R \rangle$  we first find the multiplication table of the group in polynomial time. More precisely, let  $G$  be a group of order  $n$  with composition series:

$$1 = N_0 \triangleright N_1 \triangleright \cdots \triangleright N_r = G,$$

where  $r \leq \log n$ . For each  $i \geq 1$ , the quotient group  $N_i/N_{i-1}$  is simple of some order  $n_i$ , where  $\prod_{i=1}^r n_i = n$ . By the above mentioned theorem

of [BGK<sup>+</sup>97], each  $N_i/N_{i-1}$  has an  $O(\log^2 n_i)$  size generator-relator presentation  $\langle Y_i | R_i \rangle$ . Inductively assume that we have computed the group multiplication table for  $N_{i-1}$ . The generating set  $Y_i$  for  $N_i/N_{i-1}$  is a collection of cosets  $yN_{i-1}$ . Combined with the multiplication table for  $N_{i-1}$ , and using the relations in  $R_i$ , we can compute the multiplication table for  $N_i$  in polynomial time.

Continuing thus, we will have the multiplication table for the entire group  $G$  from which we can find its commuting graph  $\Gamma(G)$ . Now, we can test if  $\Gamma(G)$  is isomorphic to the input graph  $X$  using Babai's  $2^{O(\log^3 n)}$  time algorithm.

Since each presentation  $\langle Y | R \rangle$  is of size  $O(\log^3 n)$ , we can go through all of them in time  $O(\log^3 n)$ , finding the commuting graph  $\Gamma(G)$  for the corresponding group  $G$  and then running Babai's isomorphism test to check if  $\Gamma(G) \simeq X$ .

Thus, the overall computation takes  $2^{O(\log^3 n)}$  time. □

## 8 Isoclinism of groups and commuting graphs

As extraspecial groups are a special case of nilpotent groups of class 2, a natural question is whether the algorithm of Section 6 can be extended to efficiently recognize the commuting graphs of nilpotent groups of class 2.

The property of extraspecial groups that we exploited in the algorithm is that extraspecial groups are *isoclinic*. We briefly recall the definition and its connection to commuting graphs [Ca21]:

Clearly, two isomorphic groups have the same commuting graph (meaning isomorphic commuting graphs). We can define an equivalence relation among finite groups of order  $n$ : two groups are equivalent if they have the same commuting graph.

The *commutator map* of  $G$  is the map

$$\kappa : (Za, Zb) \mapsto aba^{-1}b^{-1}$$

from the product  $G/Z(G) \times G/Z(G)$  to the commutator subgroup  $G'$ .

Two groups  $G_1$  and  $G_2$  are *isoclinic* if  $G_1/Z_1$  and  $G_2/Z_2$  are isomorphic, and their derived subgroups  $G'_1$  and  $G'_2$  are isomorphic via isomorphisms that commute with the  $\kappa$  map.

Suppose  $G_1$  and  $G_2$  are isoclinic groups such that their centers  $Z_1$  and  $Z_2$  are of the same order. Then, first of all, the commuting graphs of  $G_1/Z_1$  and

$G_2/Z_2$  are isomorphic because the groups are isomorphic. The commuting graph of  $G_i$  can be obtained from the commuting graph of  $G_i/Z_i$  by correctly blowing up each coset vertex to a coset of vertices (and including the edges as required: two vertex cosets are either fully connected with each other or not connected at all). The isoclinism property ensures that the commuting graphs of  $G_1$  and  $G_2$  remain isomorphic.

What about the converse? That is, if two groups have isomorphic commuting graphs, must they be isoclinic? This holds for various classes of groups, such as abelian groups, nonabelian simple groups, and extraspecial groups (as we have seen).

For extraspecial groups the converse property was exploited in obtaining the efficient recognition algorithm for their commuting graphs.

However, it is not true in general; we recycle an example taken from [CK20] to show this. Let  $G$  be the group of order 64 which is `SmallGroup(64,182)` in the SmallGroups library in GAP [GAP19]. The Schur multiplier of  $G$  has order 2, so a Schur cover (a group  $H$  of maximal order subject to having a subgroup  $Z \leq H' \cap Z(H)$  such that  $H/Z \cong G$ ) has order 128. Moreover, the Bogomolov multiplier of  $G$  is equal to the Schur multiplier, which implies that the Schur covers  $H$  are *commutation-preserving*: that is, two elements  $a, b \in H$  commute if and only if their projections  $Za, Zb \in G$  commute. This implies that the commuting graph of a Schur cover is obtained from the commuting graph of  $G$  by replacing each vertex with a clique of size 2, with all edges between cliques corresponding to adjacent vertices. This procedure also describes the commuting graph of  $G \times C_2$ . On the other hand, it is easy to verify computationally that the derived groups of  $H$  and  $G \times C_2$  are not isomorphic, so these groups cannot be isoclinic.

We note that the group  $G$  has nilpotency class 3, as do all of its Schur covers (these are `SmallGroup(128, i)` for  $i \in \{789, 790, 791, 815, 816, 817\}$  in the GAP library. So the following question is still open:

**Conjecture** Is it true that a nilpotent group of class 2 is determined up to isoclinism by its commuting graph?

## References

[BGK<sup>+</sup>97] L. Babai, A. J. Goodman, W. M. Kantor, E. M. Luks, and P. P. Pálffy. Short presentations for finite groups. *Journal of Algebra*,

- 194:79–112, 1997.
- [B<sup>+</sup>17] B. Baumeister, A. Maróti and H. P. Tong-Viet, Finite groups have more conjugacy classes, *Forum Mathematicum* **29** (2017), 259–275.
  - [Br63] R. Brauer, Representations of finite groups, *Lectures on modern mathematics*, Vol. I (ed. T. L. Saaty), Wiley, New York, 1963.
  - [BF55] Richard Brauer and K. A. Fowler. On groups of even order. *Ann. Math.* 62 (1955), 565–583.
  - [BGH21] T. C. Burness, R. M. Guralnick and S. Harper, The spread of a finite group, *Ann. Math.* **193** (2021), 619–687.
  - [Ca21] P.J. Cameron. Graphs defined on groups. *Int. Journal Group Theory*, to appear. Arxiv version available at <https://arxiv.org/abs/2102.11177>.
  - [Ca99] P.J. Cameron. *Permutation Groups*. London Mathematical Society Student Texts (45), Cambridge University Press, 1999.
  - [CK20] Peter J. Cameron and Bojan Kuzma. Between the enhanced power graph and the commuting graph, arXiv 2012.03789.
  - [ET68] P. Erdős and P. Turán, On some problems of a statistical group-theory, IV, *Acta Math. Acad. Sci. Hungar.* **19** (1968), 413–435.
  - [FS92] J. Feigenbaum and A. A. Schäffer. Finding the prime factors of strong direct product graphs in polynomial time. *Discret. Math.* 109(1-3): 77-102 (1992).
  - [GAP19] *GAP – Groups, Algorithms and Programming*, Version 4.10.2, the GAP group (2019), <https://www.gap-system.org>
  - [GK16] M. Giudici and B. Kuzma. Realizability problem for commuting graphs. *Journal of the Australian Mathematical Society*, 101(3):335 – 355, May 2016.
  - [GK00] R. M. Guralnick and W. M. Kantor, Probabilistic generation of finite simple groups, *J. Algebra* **234** (2000), 743–792.
  - [Gu73] W. H. Gustafson. What is the probability that two group elements commute? *American Mathematical Monthly*, 80(9):1031-34, 1973.

- [IK08] W. Imrich and S. Klavzar. *Product graphs*. Wiley-Interscience, New York, 2000.
- [Ke11] T. M. Keller, Finite groups have even more conjugacy classes. *Israel J. Math.* **181** (2011), 433–444.
- [La03] E. Landau, Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante, *Math. Ann.* **56** (1903), 671–676.
- [MN87] A. McIver and P. Neumann. Enumerating finite groups. *Quarterly Journal of Mathematics*, 38(4):473-488, 1987.
- [P68] D. S. Passman. *Permutation Groups*. Dover Publ. (reprint), New York, 2012.
- [Py92] L. Pyber. Finite groups have many conjugacy classes. *J. London Math. Soc.*, s2-46(2):239-249, 1992.
- [SW13] R.M. Solomon and A.J. Woldar. Simple groups are characterized by their non-commuting graphs. *Journal of Group Theory*, 16:793–824, 2013.
- [Tay92] D. E. Taylor, *The Classical Groups*, Heldermann Verlag, Berlin, 1992.