Electronic Colloquium on Computational Complexity, Report No. 74 (2008)

Factoring groups efficiently.

Neeraj Kayal *
kayaln@dimacs.rutgers.edu

Timur Nezhmetdinov †
tin209@lehigh.edu

July 18, 2008

Abstract

We give a polynomial time algorithm that computes a decomposition of a finite group G given in the form of its multiplication table. That is, given G, the algorithm outputs two subgroups A and B of G such that G is the direct product of A and B, if such a decomposition exists.

1 Introduction

Given two groups A and B one of the most natural ways to form a new group is the direct product, denoted $A \times B$. As a set, the direct product group is the Cartesian product of A and B consisting of ordered pairs (a, b) and the group operation is component-wise.

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2).$$

Given groups A and B, its trivial to compute the group $G = A \times B$. In this article, we consider the inverse problem of factoring or decomposing a group G as a direct product of two of its subgroups. There are some very natural motivations for such a study. The fundamental theorem of finite abelian groups (Theorem 2) states that any finite abelian group can be written uniquely upto permutation as the direct product of cyclic groups of prime power order. This theorem means that the problem of finding an isomorphism between two given abelian groups [Kav07] is essentially the same as the problem of factoring an abelian group. In the general case, the Remak-Krull-Shimidt theorem (Theorem 3) tells us that the factorization of a group as a direct product of indecomposable groups is "unique" in the sense that the isomorphism class of each of the components of the factorization is uniquely determined. This means that all such decompositions are structurally the same. This motivates us to devise an efficient algorithm which finds such a factorization.

Algorithm outline.

Notice that if we have an algorithm that computes *any nontrivial* factorization $G = A \times B$, we can efficiently compute the complete factorization of G into indecomposable subgroups by recursing on A and B. Therefore we formulate our problem as follows: given a group G, find subgroups A and B such that $G = A \times B$ and both A and B are nontrivial subgroups of G. The algorithm is devised in stages, at each stage we solve a progressively harder version of the GroupDecomposition problem until we arrive at a complete solution to the problem. Each stage uses the solution of the previous stage as a subroutine.

- *G is abelian.* The proof of the fundamental theorem of finite abelian groups (Theorem 2) is constructive and gives a polynomial-time algorithm. This case has also been studied previously and a linear time algorithm is given in [CF07].
- *The subgroup A is known.* In this case we have to just find a B such that $G = A \times B$. We call it the GroupDivision problem and in section 4, an algorithm is devised in two substages.

*DIMACS Center, Rutgers University
†Lehigh University. This work was done while visiting DIMACS under REU program

ISSN 1433-8092

- B is abelian.
- B is nonabelian.

- *A is unknown but an abelian A exists.* We call this the SemiAbelianGroupDecomposition problem and the algorithm is given in section 5.
- *A is unknown and all indecomposable direct factors of G are nonabelian.* In section 6 we describe the algorithm for this most general form of GroupDecomposition .

Let us now assume that we have an efficient algorithm for both GroupDivision and for SemiAbelianGroupDecomposition and outline the algorithm for solving GroupDecomposition using these subroutines. One of the main sources of difficulty in devising an efficient algorithm is that the decomposition of a group is not unique. Indeed, there can be superpolynomially many different decompositions of G. We first analyze the different ways a group can decompose and come up with some invariants which do not depend on the particular decomposition at hand.

Invariants of decomposition (Corollary 6). Let G be a finite group with

$$G = G_1 \times G_2 \times \ldots \times G_t$$

with each G_i indecomposable. If G has another decomposition

$$G = H_1 \times H_2 \times \ldots \times H_t$$

with each H_j indecomposable, then after an appropriate reindexing of the H_j's, we have that $\forall i \in [t] : G_i \cong H_i$ and also

$$\forall i \in [t] : \mathrm{Comm}_G(\prod_{j \neq i} G_j) = \mathrm{Comm}_G(\prod_{j \neq i} H_j),$$

where for any $A \subseteq G$, $\mathrm{Comm}_G(A)$ is the subgroup of G consisting of all the elements of G that commutes with every element of A.

With this set of "invariants" in mind, let us proceed to describe the algorithm. Assume G is decomposable and let us fix a decomposition of G,

$$G = G_1 \times G_2 \times \ldots \times G_t.$$

with each G_i indecomposable. Let $Z_1 \stackrel{\text{def}}{=} \mathrm{Comm}_G(G_2 \times \ldots \times G_t)$. We claim that it is enough to compute Z_1 in order to solve GroupDecomposition . To see this, notice that $Z_1 = G_1 \times \mathrm{Cent}(G_2 \times \ldots \times G_t)$. By a repeated application of the subroutine SemiAbelianGroupDecomposition , we can obtain a decomposition of Z_1 into

$$Z_1 = H_1 \times Y,$$

where Y is an abelian group and H_1 has no abelian direct factors. In theorem 5 we show that any such decomposition of Z_1 has the following properties:

1. H_1 is indecomposable and isomorphic to G_1.
2. $\exists Y_1 \trianglelefteq G$ such that $G = H_1 \times Y_1$.

Having obtained H_1, we obtain an appropriate Y_1 by invoking GroupDivision on (G, H_1) and thereby get a decomposition of G.
We will now outline the procedure used to compute Z_1. From the given group G, we construct a graph Γ_G which has the following properties:

1. The nodes of G correspond to conjugacy classes of G; however not all conjugacy classes of G are nodes of Γ_G. For a connected component Λ of Γ_G, let $\mathrm{Elts}(\Lambda) \subseteq G$ denote the set of all $g \in G$ that are members of some conjugacy class occuring in Λ.

2. (Proposition 13). If a decomposition of G contains t nonabelian indecomposable components then the number of connected components in Γ_G is at least t.

3. (Proposition 13). Let $G = G_1 \times \ldots \times G_t$, with each G_i indecomposable. There exists a partition

$$[s] = S_1 \uplus \ldots \uplus S_t$$

such that for any i,

$$G_i \pmod{Z} = \prod_{j \in S_i} \langle \mathrm{Elts}(\Lambda_j) \rangle \pmod{Z}.$$

4. (Proposition 15). Let Z be the center of G and let $\Lambda_1, \ldots, \Lambda_s$ be the set of connected components of Γ_G. Then $s \leq \log |G|$ and G/Z has a decomposition given by

$$G/Z = \langle \mathrm{Elts}(\Lambda_1) \rangle \pmod{Z} \times \ldots \times \langle \mathrm{Elts}(\Lambda_s) \rangle \pmod{Z}.$$

Now given only the group G and the constructed graph Γ_G, we do not apriori know what the set $S_1 \subseteq [s]$ is. But $s = O(\log |G|)$, so we can simply iterate over all possible sets S_1 in just $|G|$ iterations. Let us therefore assume that we have the appropriate S_1. Then the sought-after set Z_1 can be obtained as follows:

$$Z_1 \stackrel{\text{def}}{=} \mathrm{Comm}_G(\bigcup_{j \notin S_1} \mathrm{Elts}(\Lambda_j)).$$

This completes the outline of the algorithm. Let us summarize the algorithm.

Algorithm I. GroupDecomposition
Input. A group G in the form of a Cayley table.

1. Construct the conjugacy class graph Γ_G associated to the group G.
2. Compute the connected components $\Lambda_1, \ldots, \Lambda_s$ of Γ_G.
3. For each $S_1 \subseteq [s]$ do the following:
   (a) Let $Z_1 \stackrel{\text{def}}{=} \mathrm{Comm}_G(\left\langle \bigcup_{j \notin S_1} \mathrm{Elts}(\Lambda_j) \right\rangle)$.
   (b) By repeated invocations to SemiAbelianGroupDecomposition determine $H_1, Y \trianglelefteq G$ such that $Z_1 = H_1 \times Y$ and H_1 has no abelian direct factors and Y is abelian.
   (c) Invoke GroupDivision on (G, H_1) to determine if there exists a $Y_1 \trianglelefteq G$ such that $G = H_1 \times Y_1$. If such a Y_1 is found then **output** (H_1, Y_1).
4. If no decomposition has been found, **output** *NO SUCH DECOMPOSITION*.

The rest of this article is organized as follows. In section 3 we analyze the different ways that a group can decompose and specify some invariants. In section 4 we give the algorithm for GroupDivision and prove its correctness. In section 5, we give the algorithm for SemiAbelianGroupDecomposition and prove its correctness. In section 6 we describe the construction of the graph Γ_G and prove the properties claimed above. We complete the proof of correctness of our algorithm for GroupDecomposition in section 7. In section 8 we conclude with some open problems.

2 Preliminaries.

2.1 Notation and Terminology.

For a positive integer n, $[n]$ denotes the set $\{1, 2, \ldots, n\}$. $\mathrm{Cent}(G)$ will denote the center of a group G and $|G|$ its size. For an element $a \in G$, we will denote $|\langle a \rangle|$ by $\mathrm{ord}(a)$. We will denote the conjugacy class of the

element a by $\mathcal{C}_a$, i.e.

$$\mathcal{C}_a \stackrel{\text{def}}{=} \{g \cdot a \cdot g^{-1} \mid g \in G\} \subset G.$$

Let $A, B \subseteq G$. We write $A \leq G$ when A is a subgroup of G and $A \trianglelefteq G$ when A is a normal subgroup of G. The subgroup of G generated by the elements of A is denoted as $\langle A \rangle$. $\text{Comm}_G(A)$ will denote the subgroup of elements of G that commute with every element of A. i.e.

$$\text{Comm}_G(A) \stackrel{\text{def}}{=} \{g \in G \mid a \cdot g = g \cdot a \ \ \forall a \in A\}.$$

We will denote by $[A, B]$ the subgroup of G generated by the set of elements

$$\{a \cdot b \cdot a^{-1} \cdot b^{-1} | a \in A, \ b \in B\}.$$

We shall denote by $A \cdot B$ the set

$$\{a \cdot b \mid a \in A, b \in B\} \subseteq G.$$

We say that a group G is *decomposable* if there exist nontrivial subgroups A and B such that $G = A \times B$ and *indecomposable* otherwise. When A is a normal subroup of G we will denote by $B \pmod A$ the set of cosets $\{A \cdot b \mid b \in B\}$ of the quotient group G/A. We will say that a subgroup A of G is *a direct factor* of G if there exists another subgroup B of G such that $G = A \times B$ and we will call B a *direct complement* of A.
The canonical projection endomorphisms. When a group G has a decomposition

$$G = G_1 \times G_2 \times \ldots \times G_t$$

then associated with this decomposition is a set of endomorphisms $\pi_1, \ldots, \pi_t$ of G with

$$\pi_i : G \mapsto G_i, \quad \pi_i(g_1 \cdot g_2 \cdot \ldots \cdot g_t) = g_i.$$

where $g = g_1 \cdot g_2 \cdot \ldots \cdot g_t \in G$ $(\forall i \in [t] : \ g_i \in G_i)$ is an arbitary element of G. The π_i's we call the *canonical projection endomorphisms* of the above decomposition.

2.2 Background.

Theorem 1. *(Expressing G as a diret product of A and B, cf. [Her75]) Let G be a finite group and A, B be subgroups of G. Then $G = A \times B$ if and only if the following three conditions hold:*

- *Both A and B are normal subgroups of G.*
- $|G| = |A| \cdot |B|$.
- $A \bigcap B = \{e\}$.

Theorem 2. *(The fundamental theorem of finite abelian groups, cf. [Her75]) Every finite abelian group G can be as the written product of cyclic groups of prime power order.*

Theorem 3. *(Remak-Krull-Schmidt, cf. [Hun74]) Let G be a finite group. If*

$$G = G_1 \times G_2 \times \ldots \times G_s$$

and

$$G = H_1 \times H_2 \times \ldots \times H_t$$

with each G_i, H_j indecomposable, then $s = t$ and after reindexing $G_i \cong H_i$ for every i and for each $r < t$,

$$G = G_1 \times \ldots \times G_r \times H_{r+1} \times \ldots \times H_t.$$

Notice that the uniqueness statement is stronger than simply saying that the indecomposable factors are determined upto isomorphism.

3 Invariants of group factorization.

The main source of difficulty in devising an efficient algorithm for the decomposition of a group lies in the fact that the decomposition need not be unique. Let us therefore analyze what one decomposition should be in reference of another.

Lemma 4. *For a group G, suppose that $G = A \times B$. Then for a subset $C \subset G$,*

$$G = C \times B \Longleftrightarrow C = \{\alpha \cdot \phi(\alpha) \mid \alpha \in A\},\ \textit{where } \phi : A \mapsto \textit{Cent}(B) \textit{ is a homomorphism.}$$

Proof. ($\Leftarrow$). We have $C = \{\alpha \cdot \phi(\alpha) \mid \alpha \in A\}$, where $\phi : A \mapsto \mathrm{Cent}(B)$ is a homomorphism.

Claim 4.1. *C is a normal subgroup of G.*

Proof of Claim 4.1: Let $g = a \cdot b$ with $a \in A, b \in B$ be an arbitary element of G. For an arbitary element $c = \alpha \cdot \phi(\alpha) \in C$, we have

$$\begin{array}{rcll} g \cdot c \cdot g^{-1} & = & (a \cdot b) \cdot (\alpha \cdot \phi(\alpha)) \cdot (a^{-1} \cdot b^{-1}) & \\ & = & (a \cdot \alpha \cdot a^{-1}) \cdot (b \cdot \phi(\alpha) \cdot b^{-1}) & \\ & = & (a \cdot \alpha \cdot a^{-1}) \cdot (\phi(\alpha)) & \text{since } \phi(\alpha) \in \mathrm{Cent}(B) \\ & = & (a \cdot \alpha \cdot a^{-1}) \cdot (\phi(a) \cdot \phi(\alpha) \cdot \phi(a)^{-1}) & \text{since } \phi(\alpha) \in \mathrm{Cent}(B) \\ & = & (a \cdot \alpha \cdot a^{-1}) \cdot \phi(a \cdot \alpha \cdot a^{-1}) & \text{since } \phi \text{ is a homomorphism} \\ & \in & C & \end{array}$$

□

To verify the second requirement of Theorem 1, we have $|G| = |A| \cdot |B| = |C| \cdot |B|$.

Claim 4.2. *$C \bigcap B = \{e\}$.*

Proof of Claim 4.2: Suppose that $c = \alpha \cdot \phi(\alpha) \in C$ also belongs to B. Since $c \in B$ and $G = A \times B$, the A-component of c must be e. That is $\alpha = e$ and therefore $\phi(\alpha) = e$ since ϕ is a homomorphism. Thus $c = e$ and hence $C \bigcap B = \{e\}$. □

By an application of Theorem 1, we get $G = C \times B$, as required.
($\Rightarrow$). Assume that $G = A \times B = C \times B$. Fix the decomposition $G = A \times B$ as a reference. Since any element of C commutes with every element of B, the B-coordinate of every element of C must be in the center of B and furthermore the set of A-coordinates of C must be all of A. Also for every $\alpha \in A$, there must exist a unique element of C whose A-coordinate is α. So let $C = \{\alpha \cdot \phi(\alpha) \mid \alpha \in A\}$ with $\phi(\alpha) \in \mathrm{Cent}(B)$. We need to show that ϕ is a homomorphism. C is closed under multiplication and therefore for any two elements $(\alpha_1 \cdot \phi(\alpha_1))$ and $(\alpha_2 \cdot \phi(\alpha_2))$ of C, we must have

$$(\alpha_1 \cdot \phi(\alpha_1)) \cdot (\alpha_2 \cdot \phi(\alpha_2)) = (\alpha_1 \cdot \alpha_2) \cdot (\phi(\alpha_1) \cdot \phi(\alpha_2)) \in C.$$

In this way, we would get two different elements of C, viz. $(\alpha_1 \cdot \alpha_2) \cdot (\phi(\alpha_1) \cdot \phi(\alpha_2))$ and $(\alpha_1 \cdot \alpha_2) \cdot (\phi(\alpha_1 \cdot \alpha_2))$ which have the same A-component unless

$$\phi(\alpha_1 \cdot \alpha_2) = \phi(\alpha_1) \cdot \phi(\alpha_2).$$

Thus, $\phi : A \mapsto \mathrm{Cent}(B)$ is a homomorphism, as required. □

Theorem 5. *(Characterization of the various decompositions of a group.) Let G be a finite group with*

$$G = G_1 \times G_2 \times \ldots \times G_t \tag{1}$$

with each G_i indecomposable. For $i \in [t]$, define M_i to be the normal subgroup of G as follows:

$$M_i \stackrel{\text{def}}{=} G_1 \times \ldots \times G_{i-1} \times G_{i+1} \times \ldots \times G_t,$$

so that $G = G_i \times M_i \forall i \in [t]$. *If* G *has another decomposition*

$$G = H_1 \times H_2 \times \ldots \times H_t \tag{2}$$

(the number of H_j*'s must equal* t *by Theorem 3) with each* H_j *indecomposable, then there exist* t *homomorphisms* $\{\phi_r : G_r \mapsto Cent(M_r)\}_{r\in[t]}$ *so that after reindexing, for each* $r \in [t]$,

$$H_r = \{\alpha \cdot \phi_r(\alpha) \mid \alpha \in G_r,\ \phi_r(\alpha) \in Cent(M_r)\}$$

Proof. Corresponding to the decomposition of G in equation (1), let $\pi_i : G \mapsto G_i$ be the i-th canonical projection endomorphism. Similarly, coresponding to the decomposition of G in equation (2), let $\sigma_j : G \mapsto H_j$ be the j-th canonical projection endomorphism of G.

Claim 5.1. *There exists a reindexing of the* H_j*'s such that for all* $i \in [t]$, *both the maps*

$$\pi_i \mid_{H_i} : H_i \mapsto G_i \quad \textit{and} \quad \sigma_i \mid_{G_i} : G_i \mapsto H_i$$

are isomorphisms.

Sketch of proof of Claim 5.1: The claim follows from the proof of Theorem 3 (cf. [Hun74]). We sketch it below. Call an endomorphism $\theta : G \mapsto G$ a *normal* endomorphism if $\forall a, g \in G,\ g \cdot \theta(a) \cdot g^{-1} = \theta(g \cdot a \cdot g^{-1})$. It is easily verified that the canonical projection endomorphisms π_i's and σ_j's are all normal endomorphisms of G. The composition of any two normal endomorphisms is also a normal endomorphism. Thus for any i and j, both the maps $\pi_i \cdot \sigma_j$ and $\sigma_j \cdot \pi_i$ are normal endomorphisms. In particular $(\pi_i \cdot \sigma_j) \mid_{G_i}$, the restriction of $(\pi_i \cdot \sigma_j)$ to the subgroup G_i of G is a normal endomorphism of G_i and similarly $(\sigma_j \cdot \pi_i) \mid_{H_j}$ is a normal endomorphism of H_j. For any normal endomorphism θ of a finite group A, there exists an integer $n \in \mathbb{Z}_{\geq 1}$ such that

$$A = \mathrm{Im}(\theta^n) \times \mathrm{Ker}(\theta^n).$$

By the indecomposability of the G_i's and the H_j's we have that each $(\pi_i \cdot \sigma_j) \mid_{G_i}$ and $(\sigma_j \cdot \pi_i) \mid_{H_j}$ is either an automorphism or is nilpotent (a nilpotent endomorphism θ is an endomorphism which satisfies $\mathrm{Im}(\theta^n) = \{e\}$ for some positive integer n). Fix an $i \in [t]$. If for some j, $(\pi_i \cdot \sigma_j) \mid_{G_i}$ is an automorphism then it follows that $\sigma_j \mid_{G_i}$ and $\pi_i \mid_{H_j}$ are both isomorphisms from G_i to H_j and from H_j to G_i respectively. Suppose not, then it must be that both $(\pi_i \cdot \sigma_j) \mid_{G_i}$ and $(\sigma_j \cdot \pi_i) \mid_{H_j}$ are nilpotent endomorphisms of G_i and H_j respectively. For any two endomorphisms $\theta_1 : A \mapsto A$ and $\theta_2 : A \mapsto A$ of a group A, define their sum as folows:

$$\forall a \in A : (\theta_1 + \theta_2)(a) = \theta_1(a) \cdot \theta_2(a).$$

In general, the sum of two endomorphisms of G need not be an endomorphism of G. Nevertheless, if θ_1 and θ_2 are both nilpotent endomorphisms and if their sum is an endomorphism then it is also a nilpotent endomorphism. Now consider the set of endomorphisms $(\pi_i \cdot \sigma_j) \mid_{G_i}$ of G_i. Their sum is the identity endomorphism of G_i so that not all of them can be nilpotent. In this way, for every i we get a j such that $\sigma_j \mid_{G_i}$ and $\pi_i \mid_{H_j}$ are both isomorphisms from G_i to H_j and from H_j to G_i respectively. Continuing this reasoning we get that there exists a reindexing of the H_j's such that for all $i \in [t]$, both the maps

$$\pi_i \mid_{H_i} : H_i \mapsto G_i \quad \text{and} \quad \sigma_i \mid_{G_i} : G_i \mapsto H_i$$

are isomorphisms. □

Lets fix the reindexing provided by the above claim. Now consider an arbitary H_r with respect to the reference decomposition $G = G_r \times M_r$. Since the projection map $\pi_r \mid_{H_r} : H_r \mapsto G_r$ is an isomorphism, it is in particular a bijection so that for every $\alpha \in G_r$, there exists a unique element of H_r, whose G_r-coordinate is α. Thus, there exists a map $\phi_r : G_r \mapsto M_r$ such that the set H_r is of the form

$$H_r := \{\alpha \cdot \phi_r(\alpha) \mid \alpha \in G_r,\ \phi_r(\alpha) \in M_r\}.$$

Also, since H_r is closed under multiplication, it follows that ϕ_r is a homomorphism from G_r to M_r. Now fix $\beta = \alpha \cdot \phi_r(\alpha) \in H_r$ and a $j \neq r$. Since β is in in H_r, it commutes with every element of H_j and therefore for all $\gamma \in H_j$, we have

$$\begin{array}{rrcl} & \beta \cdot \gamma \cdot \beta^{-1} & = & \gamma \\ \Rightarrow & \pi_j(\beta \cdot \gamma \cdot \beta^{-1}) & = & \pi_j(\gamma) \\ \Rightarrow & \beta \cdot \pi_j(\gamma) \cdot \beta^{-1} & = & \pi_j(\gamma) \end{array}$$

Now since $\pi_j \mid_{H_j} : H_j \mapsto G_j$ is an isomorphism we have that $\forall \theta \in G_j$

$$\begin{array}{rrcl} & \beta \cdot \theta \cdot \beta^{-1} & = & \theta \\ \Rightarrow & \alpha \cdot \phi_r(\alpha) \cdot \theta \cdot \phi_r(\alpha)^{-1} \cdot \alpha^{-1} & = & \theta \\ \Rightarrow & \phi_r(\alpha) \cdot \theta \cdot \phi_r(\alpha)^{-1} & = & \theta \end{array}$$

and thus $\phi(\alpha) \in M_r$ commutes with every element of G_j for $j \neq r$. Since

$$M_r = \prod_{j \neq r} G_j,$$

it follows that $\phi_r(\alpha) \in \text{Cent}(M_r)$. In this way,

$$H_r = \{\alpha \cdot \phi_r(\alpha) \mid \alpha \in G_r,\ \phi_r(\alpha) \in \text{Cent}(M_r)\}$$

□

Corollary 6. *(Invariants of decompositions). Let G be a finite group with center Z and*

$$G = G_1 \times G_2 \times \ldots \times G_t \tag{3}$$

with each G_i indecomposable. If G has another decomposition

$$G = H_1 \times H_2 \times \ldots \times H_t \tag{4}$$

with each H_j indecomposable, then after an appropriate reindexing of the H_j's, we have:

1. *G_i $(mod\ Z) = H_i$ $(mod\ Z)$.*
2. *$\forall i \in [t]:\ Comm_G(\prod_{j \neq i} G_j) = Comm_G(\prod_{j \neq i} H_j)$.*

Proof. Fix a reindexing of the H_j's as demonstrated by the above theorem. Notice that

$$Z \stackrel{\text{def}}{=} \text{Cent}(G) = \text{Cent}(G_1) \times \text{Cent}(G_2) \times \ldots \times \text{Cent}(G_t).$$

As in the theorem above let M_i be defined as $M_i \stackrel{\text{def}}{=} \prod_{j \neq i} G_j$ so that $\forall i \in [t]$,

$$\text{Cent}(M_i) = \text{Cent}(\prod_{j \neq i} G_j) \subseteq Z$$

Now $\forall i \in [t]$, we have $H_i = \{\alpha \cdot \phi_i(\alpha) \mid \alpha \in G_i,\ \phi_i(\alpha) \in \text{Cent}(M_i)\}$. But $\text{Cent}(M_i) \trianglelefteq Z$ so that

$$G_i \ (\text{mod}\ Z) = H_i \ (\text{mod}\ Z).$$

This proves part 1 of the corollary.

Now consider an arbitary $g \in \prod_{j \neq i} G_j$. By part 1, we have that for any suich g, there exists a $z \in Z$ such that $g \cdot z \in \prod_{j \neq i} H_j$. Since the set of elements that commutes with g is the same as the set of elements that commutes with $g \cdot z$, we get that

$$\text{Comm}_G(\prod_{j \neq i} G_j) = \text{Comm}_G(\prod_{j \neq i} H_j).$$

This completes the proof of part 2 of the corollary. □

This corollary gives some quantities which are invariant across different decompositions the group G. Indeed, our decomposition algorithm computes these invariants as an intermediate step on the way to obtaining a decomposition of G.

4 An algorithm for GroupDivision

In this section we solve the group division problem which is used in step 3 of Algorithm I. Let us recall that GroupDivision is the following problem: given a group G and a normal subgroup $A \trianglelefteq G$, find a $B \trianglelefteq G$ such that $G = A \times B$, if such a decomposition exists. We will solve this problem itself in two stages. First, we devise an efficient algorithm assuming that the quotient group G/A is abelian and then use this as a subroutine in the algorithm for the general case.

4.1 When the quotient group G/A is abelian.

In this case we can assume that $G = A \times B$ where B is abelian. Observe that in this case, for every coset $A \cdot g$ of A in G, we can pick an element $b \in A \cdot g$ such that $b \in \mathrm{Cent}(G)$ and $\mathrm{ord}_G(b) = \mathrm{ord}_{G/A}(A \cdot g)$. Also, the quotient group G/A is abelian and therefore using the abelian group decomposition algorithm, we can efficiently find a complete decomposition of G/A. So let

$$G/A = \langle A \cdot g_1 \rangle \times \ldots \times \langle A \cdot g_t \rangle$$

Now from each coset $A \cdot g_i$ we pick a representative element b_i such that $b_i \in \mathrm{Cent}(G)$ and $\mathrm{ord}_G(b_i) = \mathrm{ord}_{G/A}(A \cdot b_i)$. For any such set of b_i's, its an easy verification that $G = A \times \langle b_1 \rangle \times \ldots \times \langle b_t \rangle$.

4.2 When the quotient group G/A is nonabelian.

We first give the algorithm and then prove its correctness.

Algorithm II. GroupDivision
Input. A group G and a normal subgroup A of G.
Output. A subgroup C of G such that $G = A \times C$, if such a C exists.

1. Compute $T \stackrel{\text{def}}{=} \left\langle \{a \cdot g \cdot a^{-1} \cdot g^{-1} \mid a \in \mathrm{Comm}_G(A), g \in G\} \right\rangle$.
2. If T is not a normal subgroup of G then **output** *NO SUCH DECOMPOSITION.*
3. Compute $\tilde{G} \stackrel{\text{def}}{=} G/T$ and $\tilde{A} \stackrel{\text{def}}{=} \{T \cdot a \mid a \in A\} \trianglelefteq \tilde{G}$.
4. Verify that $T \bigcap A = \{e\}$. If not, output *NO SUCH DECOMPOSITION.* If yes, then we deduce that the canonical map $a \mapsto Ta$ is an isomorphism from A to $\tilde{A}$.
5. Using the abelian group division algorithm given above, determine if there exists a $\tilde{B} \trianglelefteq \tilde{G}$, *with* $\tilde{B}$ *abelian*, so that $\tilde{G} = \tilde{A} \times \tilde{B}$. If so, determine elements $Tg_1, Tg_2, \ldots, Tg_t \in G/T$ such that
$$\tilde{G} = \tilde{A} \times \langle Tg_1 \rangle \times \langle Tg_2 \rangle \times \ldots \times \langle Tg_t \rangle .$$
6. From each coset Tg_i, pick *any* representative element c_i. Compute $C \stackrel{\text{def}}{=} \langle T \bigcup \{c_1, \ldots, c_t\} \rangle \leq G$.
7. If $G = A \times C$ then **output** C else **output** *NO SUCH DECOMPOSITION.*

The algorithm clearly has polynomial running time and it remains for us to prove its correctness. To see whats going on in the algorithm above, let us assume that $G = A \times B$ and fix this decomposition of G. Its easy to verify that the subgroup T computed in step 1 is a normal subgroup of G and $T = [B, B]$. Also, $T = [B, B] \subseteq B$ and therefore $A \bigcap T$ must be $\{e\}$. This implies that the canonical mapping $a \mapsto T \cdot a$ is an isomorphism from A to $\tilde{A}$ This explains step 4 of the algorithm. Observe that the $\tilde{G}$ computed in step 3 has the decomposition

$$\tilde{G} = \tilde{A} \times (B/[B, B]).$$

But $B/[B,B]$ is an abelian group so we can use the previous algorithm and decompose $\tilde{G}$ into product of $\tilde{A}$ times a number of cyclic groups. By the end of step 6, we would have computed $c_1, \ldots, c_t \in G$ such that

$$\tilde{G} = \tilde{A} \times \tilde{C}, \quad \text{where } \tilde{C} \stackrel{\text{def}}{=} \langle Tc_1 \rangle \times \langle Tc_2 \rangle \times \ldots \times \langle Tc_t \rangle \leq G.$$

Proposition 7. *$C \trianglelefteq G$ and the elements of C and A together generate G. Furthermore, $C \bigcap A = \{e\}$.*

Proof. From the construction of C its clear that $T \leq C$ and that $C \pmod{T} = \tilde{C}$. So let us look at $\tilde{C}$ as a subgroup of $\tilde{G}$. Observe that in $\tilde{G}$, the subgroup $\tilde{C}$ being an abelian subgroup and a direct factor of $\tilde{G}$ is in the center of $\tilde{G}$. So for any $g \in G$ and $c \in C$ we have

$$\begin{array}{rrcl} & (Tg) \cdot (Tc) & = & (Tc) \cdot (Tg) \\ \Rightarrow & (Tg) \cdot (Tc) \cdot (Tg)^{-1} & = & Tc \\ \Rightarrow & T(g \cdot c \cdot g^{-1}) & = & Tc \\ \Rightarrow & (g \cdot c \cdot g^{-1}) & \in & Tc \\ \Rightarrow & (g \cdot c \cdot g^{-1}) & = & c \cdot t, \quad \text{for some } t \in T \\ \Rightarrow & (g \cdot c \cdot g^{-1}) & \in & C \quad (\text{since } c, t \in C) \end{array}$$

Thus C is a normal subgroup of G. Now suppose that $g \in A \bigcap C$. It also means that $Tg \in \tilde{A} \cap \tilde{C}$ so that $Tg = T$. This means $g \in T \subseteq B$. Thus $g \in A \bigcap B$ which means that $g = e$. □

Summarizing, we have A and C are normal subgroups of G that span G and have a trivial intersection which means that $G = A \times C$, as required to prove the correctness of the algorithm.

5 An algorithm for SemiAbelianGroupDecomposition

In this section, we solve the special case of GroupDecomposition when some of the indecomposable components of G are abelian groups. That is given G, we wish to find an abelian subgroup B and another subgroup A of G so that

$$G = A \times B, \quad \text{where } B \text{ is abelian.} \tag{5}$$

Since B is abelian, it has a decomposition into a direct product of cyclic groups. So let

$$B = \langle b_1 \rangle \times \ldots \times \langle b_t \rangle .$$

so that G becomes

$$G = A \times \langle b_1 \rangle \times \ldots \times \langle b_t \rangle .$$

Thus, if G has a decomposition of the form (5) then there exists a $b \in G$ such that $\langle b \rangle$ is a direct factor of G. Conversely, to find a decomposition of the form (5) it is sufficient to find a b such that $\langle b \rangle$ is a direct factor of G. Knowing B, we can find an appropriate direct complement of $\langle b \rangle$ efficiently using the algorithm for GroupDivision given previously. Lastly, given the group G, we find an appropriate b in polynomial-time by iterating over all the elements of G and using the algorithm for GroupDivision to verify whether $\langle b \rangle$ is a direct factor of G or not.

6 The conjugacy class graph of a group and its properties.

Here we give the construction of the *conjugacy class graph* of a group. Consider a group G which has a decomposition

$$G = A \times B.$$

Fixing this decomposition, consider the conjugacy class $\mathcal{C}_g$ of an arbitary element $g = \alpha \cdot \beta \in G$, where $\alpha \in A, \beta \in B$. Observe that $\mathcal{C}_g = \mathcal{C}_\alpha \cdot \mathcal{C}_\beta$ and the elements of $\mathcal{C}_\alpha$ and $\mathcal{C}_\beta$ commute. More generally, we have

Observation 8. *If $G = G_1 \times \ldots \times G_t$ and $g = g_1 \cdot \ldots \cdot g_t$ is an arbitary element of G, with each $g_i \in G_i$ then*

$$\mathcal{C}_g = \mathcal{C}_{g_1} \cdot \mathcal{C}_{g_2} \cdot \ldots \cdot \mathcal{C}_{g_t}.$$

Furthermore for all $i \neq j$ each element of $\mathcal{C}_{g_i}$ commutes with every element of $\mathcal{C}_{g_j}$.

For the rest of this section, we fix the group G and a reference decomposition

$$G = G_1 \times G_2 \times \ldots \times G_t.$$

Let $\{\pi_i : G \mapsto G_i \mid i \in [t]\}$ be the set of canonical projection endomorphisms associated with the above decomposition. If any of the G_i's are abelian groups then we can obtain a decomposition of G using the algorithm for SemiAbelianGroupDecomposition given in section 5. So henceforth we will assume that all the G_i's are nonabelian. Observation 8 above motivates the following definitions.

Definition 9. *We say that two conjugacy classes $\mathcal{C}_a$ and $\mathcal{C}_b$* commute *when for every $\alpha \in \mathcal{C}_a$ and $\beta \in \mathcal{C}_b$, α and β commute.*

Definition 10. *Call a conjugacy class* reducible *$\mathcal{C}_g$ if it is either a conjugacy class of an element from the center of G, or there exist two conjugacy classes $\mathcal{C}_a$ and $\mathcal{C}_b$ such that*

- *Neither a nor b belongs to the center of G.*
- *$\mathcal{C}_a$ and $\mathcal{C}_b$ commute.*
- *$\mathcal{C}_g = \mathcal{C}_a \cdot \mathcal{C}_b$*
- *$|\mathcal{C}_g| = |\mathcal{C}_a| \cdot |\mathcal{C}_b|$*

If a conjugacy class is not reducible, then call it irreducible.

Proposition 11. *If a conjugacy class $\mathcal{C}_g$ is irreducible then there exists a unique $i \in [t]$ such that $\pi_i(g) \notin Cent(G_i)$.*

Proof. If it happens that for all $i \in [t]$, $\pi_i(g) \in \mathrm{Cent}(G_i)$ then $g \in \mathrm{Cent}(G)$ so that the conjugacy class $\mathcal{C}_g$ is reducible by definition. If more than one $\pi_i(G)$ are noncentral elements then by observation 8, we would get that $\mathcal{C}_g$ is reducible. □

The converse of this proposition is not true in general. The above proposition implies that corresponding to a conjugacy class $\mathcal{C}_g$, there exists a unique G_i such that $\pi_i(g) \notin \mathrm{Cent}(G_i)$. Let us call this subgroup G_i the *indecomposable component associated to* the conjugacy class $\mathcal{C}_g$. Let us now define the *conjugacy class graph* Γ_G associated to a group G.

Definition 12. *The* graph *of a group G (denoted Γ_G) is a graph with irreducible conjugacy classes as nodes and such that a pair of nodes is connected by an edge iff the corresponding pair of conjugacy classes does* not *commute.*

The connected components of Γ_g can be computed efficiently and they give us information about the direct factors of G.

Proposition 13. *Let $\Lambda_1, \ldots, \Lambda_s$ be the connected components of Γ_G. Then $s \geq t$ and there is a partition*

$$[s] = S_1 \uplus S_2 \uplus \ldots \uplus S_t$$

such that $\left\langle \cup_{i \in S_j} Elts(\Lambda_i) \right\rangle \pmod Z = G_j \pmod Z$ for all j where $Z = Cent(G)$.

Proof. Let us consider two irreducible conjugacy classes $\mathcal{C}_g$ and $\mathcal{C}_h$. Let the indecomposable components associated with $\mathcal{C}_g$ and $\mathcal{C}_h$ be G_i and G_j respectively. Suppose that $i \neq j$. Then $\pi_j(g)$ and $\pi_i(h)$ are central elements of G so that every element of $\mathcal{C}_g$ commutes with every other element of $\mathcal{C}_h$. Thus there is no edge between the nodes corresponding to $\mathcal{C}_g$ and $\mathcal{C}_h$. This implies that if $\mathcal{C}_g$ and $\mathcal{C}_h$ are in the same connected component of Γ_G then the indecomposable components associated with $\mathcal{C}_g$ and $\mathcal{C}_h$ are the same. Each nonabelian component of G gives rise to at least one irreducible conjugacy class so that the number of connected components s of Γ_G is at least the number of indecomposable nonabelian components of G. The above argument shows that there exists a partition of $[s]$ into S_i such that $\left\langle \cup_{i \in S_j} \Lambda_i \right\rangle \pmod Z \subseteq G_j \pmod Z$ for all j. The inclusion is in fact an equality because all the irreducible conjugacy classes generate all the noncentral elements of G by construction. □

In general it is not true that the number of connected components of Γ_G equals the number of indecomposable nonabelian groups in the factorization of G. The irreducible conjugacy classes of each of the G_i may be divided into more than one component. However we have the following:

Proposition 14. *If the center of group G is trivial, then the number of connected components of its graph is equal to the number of indecomposable groups in the factorization of G. Moreover, the subgroups generated by the conjugacy classes of each of the components are normal disjoint subgroups which together span G; thus we have the factorization of G.*

Proof. The subgroups generated by conjugacy classes of each of the connected components of the graph are normal because the sets of generators are closed under conjugation. All of the subgroups together span the entire group because they are generated by all irreducible conjugacy classes which themselves span all reducible conjugacy classes. To show that the subgroups are pairwise disjoint: Suppose that two such subgroups have an element in common. Then the element can be expressed in terms of the generators of either of the two subgroups: $g_1 g_2 \cdots g_k = h_1 h_2 \cdots h_l$ where g_i are some generators of the first subgroup and h_i are some generators of the second subgroup. Since g_i and h_i commute with every element of other components than their own, so do their products. It follows that $g_1 g_2 \cdots g_k = h_1 h_2 \cdots h_l$ commutes with every element of each of the components. Because the components generate the group, the common element must be in the center of the group–hence identity.

This gives us a factorization of G, although we don't yet know that the factors are indecomposable subgroups. Suppose there is a factorization of greater length, i.e. with greater number of factors. Since each of the factors will give rise to at least one connected component of the graph, the number of factors cannot be greater than the number of components. Thus, the factorization that we obtained is a factorization into indecomposable subgroups. □

Using the proposition we can efficiently factor a group with a trivial center. When the center of the group is non-trivial it is no longer the case that each component of Γ_G generates one of the factors in the factorization of G. We would need to search through the partitions of the set of connected components to find the components associated to an indecomposable factor, say G_1. For that we need a bound on the number of components of the graph:

Proposition 15. *The number of connected components is bounded by* $\log |G|$.

Proof. Let Z be the center of G. We will prove that the components of the graph of G will correspond to the indecomposable factors of G/Z. The subgroups generated by the cosets of the elements of each of the components are normal since the sets of generators are closed under conjugation. Together they span the whole group G/Z since they spanned G before we took quotient (and they spanned G because they spanned Z and they spanned all the reducible conjugacy classes). Now let's show that the subgroups are pairwise disjoint. Suppose that there is an element in common: $Z g_1 g_2 \cdots g_k = Z h_1 h_2 \cdots h_l$ where g_i and h_i are from different components. Since the cosets are equal then for every $c_1 \in Z$, there is a $c_2 \in Z$, so that $c_1 g_1 g_2 \cdots g_k = c_2 h_1 h_2 \cdots h_l$. As in the previous proposition we can show that this element must lie in Z, so the common coset is in fact a coset of the identity, hence the subgroups are pairwise disjoint. Then the G/Z is isomorphic to the direct product of the subgroups. As each subgroup is nontrivial, we have that the number of the subgroups is bounded by $\log |G/Z|$. As the number of the subgroups is equal to the number of connected components of the graph of G the claim follows. □

7 Putting everything together

We now have all the component steps of Algorithm I. So let us conclude with the proof of correctness of Algoritm I.

Theorem 16. *If the input to Algorithm I is a decomposable group G then it necessarily computes a nontrivial decomposition of G, otherwise it outputs* NO SUCH DECOMPOSITION. *Moreover, Algorithm I has running time polynomial in $|G|$.*

Proof. Clearly, if the group is indecomposable our algorithm outputs *NO SUCH DECOMPOSITION*. By Proposition 15, $s \leq \log |G|$ so that the number of iterations in step 3 is at most $|G|$. All the operations inside the loop (steps 3a to 3c) are polynomial-time computable so that the overall running time also poly($|G|$). It remains to show that if G is decomposable then our algorithm outputs a nontrivial decomposition. Let the given group G have a decomposition

$$G = G_1 \times \ldots \times G_t \tag{6}$$

with each G_i indecomposable. Let Z be the center of G. In the algorithm we iterate over all subsets of the connected components of Γ_G so let us assume that we have found the subset S_1 of indices of connected components corresponding to conjugacy class of elements of G_1. By Proposition 15 we have

$$G_2 \times G_3 \times \ldots \times G_t \pmod{Z} = \left\langle \cup_{j \notin S_1} \text{Elts}(\Lambda_j) \right\rangle \pmod{Z}.$$

This means that in step 3a we would have computed

$$\begin{aligned} Z_1 &\stackrel{\text{def}}{=} \text{Comm}_G(\left\langle \cup_{j \notin S_1} \text{Elts}(\Lambda_j) \right\rangle) \\ &= \text{Comm}_G(G_2 \times G_3 \times \ldots \times G_t) \\ &= G_1 \times \text{Cent}(G_2) \times \text{Cent}(G_3) \times \ldots \times \text{Cent}(G_t) \end{aligned}$$

Let us now consider the decomposition $Z_1 = H_1 \times Y$ obtained in step 3b of Algorithm I. By the Remak-Krull-Schmidt theorem (Theorem 3), all decompositions of Z_1 are isomorphic so that if H_1 is any direct factor of Z_1 which has no abelian direct factors then H_1 must be indecomposable and isomorphic to G_1. Furthermore by an application of theorem 5, we must have that H_1 must be of the form

$$H_1 = \{\alpha \cdot \phi(\alpha) \mid \alpha \in G_1,\ \phi(\alpha) \in (\text{Cent}(G_2) \times \text{Cent}(G_3) \times \ldots \times \text{Cent}(G_t))\},$$

where $\phi : H_1 \mapsto \text{Cent}(G_2) \times \text{Cent}(G_3) \times \ldots \times \text{Cent}(G_t)$ is a homomorphism. By lemma 4, we can replace G_1 by H_1 in the factorization (6) so that in fact

$$G = H_1 \times G_2 \times G_3 \times \ldots \times G_t.$$

In particular, this means that H_1 is a direct factor of G so that in step (3c), using the algorithm for GroupDivision , we necessarily recover a nontrivial factorization of G. □

8 Conclusion

In this article we showed how to decompose a given group G into a direct product of two subgroups. The original problem which motivated our problem is that of GroupIsomorphism .

Open Problem. GroupIsomorphism : Devise an efficient algorithm that given two groups G and H in the form of their Cayley tables (multiplication tables), determines whether they are isomorphic or not.

The Remak-Krull-Schmidt theorem (Theorem 3) together with our decomposition algorithm implies that it is necessary and sufficient to solve the GroupIsomorphism problem for indecomposable groups. Thus our algorithm can be viewed as a first towards an eventual solution to the GroupIsomorphism problem. There already exists a complete characterization of finite simple groups (i.e. groups which have no normal subgroups at all) and it is conceivable that some such algorithmic characterization can be formulated even for finite indecomposable groups which would lead to an eventual solution of GroupIsomorphism . There are many possible directions in which this work can be extended and algorithms sought for. For example, it would also be very interesting to extend our results to compactly represented groups such as permutation groups and matrix groups. A permutation group G is a subgroup of S_n, the group of permutations on the set $\{1, 2, \ldots, n\}$. The typical representation of a permutation group is by means of a generating set which consists of permutations $\sigma_1, \sigma_2, \ldots, \sigma_t \in S_n$. A matrix group is specified by means of a set of generating matrices over some finite field $\mathbb{F}_{p^r}$. We mention some of these algorithmic problems below.

1. SemidirectDecomposition : Given a group G, compute two subgroups A and B of G such that G is the semidirect product of A by B.

2. PermutationGroupDivision : Given $G \leq S_n$ and $A \trianglelefteq G$, determine whether there exists a $B \trianglelefteq G$ such that $G = A \times B$.

3. PermutationGroupDecomposition : Given a group $G \leq S_n$, compute $A, B \trianglelefteq G$ such that $G = A \times B$.

4. MatrixGroupDivision : Given $G \leq (\mathbb{F}_{p^r}^{t \times t})^*$ and $A \trianglelefteq G$, determine whether there exists a $B \trianglelefteq G$ such that $G = A \times B$.

5. MatrixGroupDecomposition : Given a group $G \leq (\mathbb{F}_{p^r}^{t \times t})^*$, compute $A, B \trianglelefteq G$ such that $G = A \times B$.

References

[CF07] Li Chen and Bin Fu. Linear and sublinear time algorithms for the basis of abelian groups. In *Electronic Colloquium on Computational Complexity, Technical report TR07-052*, 2007.

[Her75] I. N. Herstein. *Topics in Algebra*. John Wiley & Sons, New York, 2nd edition, 1975.

[Hun74] Thomas W. Hungerford. *Algebra*. Number 73 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1974.

[Kav07] T. Kavitha. Linear time algorithms for abelian group isomorphism and related problems. *J. Comput. Syst. Sci.*, 73(6):986–996, 2007.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de/