On the Descriptive Complexity of Groups without Abelian Normal Subgroups

(Extended Abstract)

Joshua A. Grochow
Department of Computer Science University of Colorado Boulder, CO USA
Department of Mathematics University of Colorado Boulder, CO USA
jgrochow@colorado.edu

Michael Levet
Department of Computer Science, College of Charleston, SC USA
levetm@cofc.edu

In this paper, we explore the descriptive complexity theory of finite groups by examining the power of the second Ehrenfeucht–Fraïssé bijective pebble game in Hella's (*Ann. Pure Appl. Log.*, 1989) hierarchy. This is a Spoiler–Duplicator game in which Spoiler can place up to two pebbles each round. While it trivially solves graph isomorphism, it may be nontrivial for finite groups, and other ternary relational structures. We first provide a novel generalization of Weisfeiler–Leman (WL) coloring, which we call *2-ary* WL. We then show that the 2-ary WL is equivalent to the second Ehrenfeucht–Fraïssé bijective pebble game in Hella's hierarchy.

Our main result is that, in the pebble game characterization, only $O(1)$ pebbles and $O(1)$ rounds are sufficient to identify all groups without Abelian normal subgroups (a class of groups for which isomorphism testing is known to be in P; Babai, Codenotti, & Qiao, ICALP 2012). In particular, we show that within the first few rounds, Spoiler can force Duplicator to select an isomorphism between two such groups at each subsequent round. By Hella's results (*ibid.*), this is equivalent to saying that these groups are identified by formulas in first-order logic with generalized 2-ary quantifiers, using only $O(1)$ variables and $O(1)$ quantifier depth.

1 Introduction

Descriptive complexity theory studies the relationship between the complexity of describing a given problem in some logic, and the complexity of solving the problem by an algorithm. When the problems involved are isomorphism problems, Immerman and Lander [44] showed that complexity of a logical sentence describing the isomorphism type of a graph was essentially the same as the Weisfeiler–Leman coloring dimension of that graph, and the complexity of an Ehrenfeucht–Fraïssé pebble game (see also [17]).

It is a well-known open question whether there is a logic that exactly captures the complexity class P on unordered (unlabeled) structures; on ordered structures such a logic was given by Immerman [43] and Vardi [67]. The difference between these two settings is essentially the GRAPH CANONIZATION problem, whose solution allows one to turn an unordered graph into an ordered graph in an isomorphism-preserving way.

One natural approach in trying to capture P on unordered structures is thus to attempt to extend first-order logic FO by generalized quantifiers (c.f., Mostowski [60] and Lindstrom [57]) in the hopes that the augmented logics can characterize finite graphs up to isomorphism, thus reducing the unordered case

A. Achilleos and D. Della Monica (Eds.): Fourteenth
International Symposium on Games, Automata, Logics,
and Formal Verification (GandALF 2023).
EPTCS 390, 2023, pp. 185–202, doi:10.4204/EPTCS.390.12

to the previously solved ordered case. A now-classical approach, initiated by Immerman [43], was to augment fixed-point logic with counting quantifiers, which can be analyzed in terms of an equivalence induced by (variable confined) fragments of first-order logic with counting. However, Cai, Fürer, & Immerman [17] showed that $\mathsf{FO}+\mathsf{LFP}$ plus counting does not capture P on finite graphs. More generally, Flum & Grohe have characterized when FO plus counting captures P on unordered structures [26].

The approach of Cai, Fürer, & Immerman (ibid., see also [44]) was to prove a three-way equivalence: between (1) counting logics, (2) the higher-dimensional Weisfeiler–Leman coloring procedure, and (3) Ehrenfeucht–Fraïssé pebble games. Ehrenfeucht–Fraïssé pebble games [24, 27] have long been an important tool in proving the inexpressibility of certain properties in various logics; in this case, they used such games to show that the logics could not express the difference between certain pairs of non-isomorphic graphs. Consequently, Cai, Fürer, & Immerman ruled out the Weisfeiler–Leman algorithm as a polynomial-time isomorphism test for graphs, which resolved a long-standing open question in isomorphism testing. Nonetheless, the Weisfeiler–Leman coloring procedure is a key subroutine in many algorithms for GRAPH ISOMORPHISM, including Babai's quasi-polynomial-time algorithm [4]. It is thus interesting to study its properties and its distinguishing power.

While the result of Cai, Fürer, & Immerman ruled out Weisfeiler–Leman as a polynomial-time isomorphism test for graphs, for *groups* it remains an interesting open question. The general WL procedure for groups was introduced by Brachter & Schweitzer [12] and has been studied in several papers since then [13, 30]. Outside the scope of WL, it is known that GROUP ISOMORPHISM is AC^0-reducible to GRAPH ISOMORPHISM, and there is no AC^0 reduction in the opposite direction [19]. For this and other reasons, group isomorphism is believed to be the easier of the two problems, so it is possible that WL—and more generally, tools from descriptive complexity—could yield stronger results for groups than for graphs.

On graphs, which are binary relational structures, if Spoiler is allowed to pebble two elements per turn, then Spoiler can win on any pair of non-isomorphic graphs. However, groups are ternary relational structures (the relation is $\{(a,b,c) : ab = c\}$), so such a game may yield nontrivial insights into the descriptive complexity of finite groups. Hella [41, 42] introduced such games in a more general context, and showed that allowing Spoiler to pebble q elements per round corresponded to the generalized q-ary quantifiers of Mostowski [60] and Lindstrom [57]. When $q = 1$, Hella shows that this pebble game is equivalent in power to the FO plus counting logics mentioned above. Our focus in this paper is to study the power of the $q = 2$-ary game for identifying finite groups.

Main Results. In this paper, we initiate the study of Hella's 2-ary Ehrenfeucht–Fraïssé-style pebble game, in the setting of groups. Our main result is that this pebble game efficiently characterizes isomorphism in a class of groups for which isomorphism testing is known to be in P, but only by quite a nontrivial algorithm (see remark below). The full version of this paper appears on arXiv [29].

Theorem 1.1. *Let G be a group with no Abelian normal subgroups (a.k.a. Fitting-free or semisimple), and let H be arbitrary. If $G \not\cong H$, then Spoiler has a winning strategy in the Ehrenfeucht–Fraïssé game at the second level of Hella's hierarchy, using 9 pebbles and $O(1)$ rounds.*

In proving Thm. 1.1, we show that with the use of only a few pebbles, Spoiler can effectively force Duplicator to select an isomorphism of G and H. We contrast this with the setting of Weisfeiler–Leman (which is equivalent to the 1-ary pebble game), for which the best upper bound we have on the WL-dimension is the trivial bound of $\log n$. Furthermore, we do not have any lower bounds on the WL-dimension for semisimple groups.

Remark 1.2. Every group G can be written as an extension of its solvable radical $\text{Rad}(G)$ by the quotient

$G/\mathrm{Rad}(G)$, which does not have Abelian normal subgroups. As such, the latter class of groups is quite natural, both group-theoretically and computationally. Computationally, it has been used in algorithms for general finite groups both in theory (e.g., [5, 6]) and in practice (e.g., [18]). Isomorphism testing in this family of groups can be solved efficiently in practice [18], and is known to be in P through a series of two papers [7, 8].

In Section 3 we also complete the picture by giving a Weisfeiler–Leman-style coloring procedure and showing that it corresponds precisely to Hella's q-ary pebble games and q-ary generalized Lindstrom quantifiers [57]. When the groups are given by their multiplication tables, this procedure runs in time $n^{\Theta(\log^2 n)}$ by reduction to GRAPH ISOMORPHISM. We note that Hella's results deal with infinitary logics [41, 42]. However, as we are dealing with finite groups, the infinitary quantifiers and connectives are not necessary (see the discussion in [42], right above Theorem 5.3).

Further Related Work. Despite the fact that Weisfeiler–Leman is insufficient to place GRAPH ISOMORPHISM (GI) into PTIME, it remains an active area of research. For instance, Weisfeiler–Leman is a key subroutine in Babai's quasipolynomial-time GI algorithm [4]. Furthermore, Weisfeiler–Leman has led to advances in simultaneously developing both efficient isomorphism tests and the descriptive complexity theory for finite graphs- see for instance, [32, 38, 49, 50, 34, 36, 35, 51, 1, 2, 64]. Weisfeiler–Leman also has close connections to the Sherali–Adams hierarchy in linear programming [37].

The complexity of the GROUP ISOMORPHISM (GPI) problem is a well-known open question. In the Cayley (multiplication) table model, GPI belongs to $\mathsf{NP} \cap \mathsf{coAM}$. The generator-enumerator algorithm, attributed to Tarjan in 1978 [59], has time complexity $n^{\log_p(n)+O(1)}$, where n is the order of the group and p is the smallest prime dividing n. This bound has escaped largely unscathed: Rosenbaum [63] (see [55, Sec. 2.2]) improved this to $n^{(1/4)\log_p(n)+O(1)}$. And even the impressive body of work on practical algorithms for this problem, led by Eick, Holt, Leedham-Green and O'Brien (e. g., [11, 25, 10, 18]) still results in an $n^{\Theta(\log n)}$-time algorithm in the general case (see [70, Page 2]). In the past several years, there have been significant advances on algorithms with worst-case guarantees on the serial runtime for special cases of this problem including Abelian groups [47, 68, 65], direct product decompositions [69, 48], groups with no Abelian normal subgroups [7, 8], coprime and tame group extensions [54, 62, 9, 31], low-genus p-groups and their quotients [56, 15], Hamiltonian groups [20], and groups of almost all orders [23].

Key motivation for GPI is due to its close relation to GI. In the Cayley (verbose) model, GPI reduces to GI [71], while GI reduces to the succinct GPI problem [40, 58] (recently simplified [39]). In light of Babai's breakthrough result that GI is quasipolynomial-time solvable [4], GPI in the Cayley model is a key barrier to improving the complexity of GI. Both verbose GPI and GI are considered to be candidate NP-intermediate problems, that is, problems that belong to NP, but are neither in P nor NP-complete [53]. There is considerable evidence suggesting that GI is not NP-complete [66, 16, 45, 4, 52, 3]. As verbose GPI reduces to GI, this evidence also suggests that GPI is not NP-complete. It is also known that GI is strictly harder than GPI under AC^0 reductions [19].

While the descriptive complexity of graphs has been extensively studied, the work on the descriptive complexity of groups is scant compared to the algorithmic literature on GROUP ISOMORPHISM (GPI). There has been work relating first order logics and groups [61], as well as work examining the descriptive complexity of finite abelian groups [28]. Recently, Brachter & Schweitzer [12] introduced three variants of Weisfeiler–Leman for groups, including corresponding logics and pebble games. These pebble games correspond to the first level of Hella's hierarchy [41, 42]. In particular, Brachter & Schweitzer showed that 3-dimensional Weisfeiler–Leman can distinguish p-groups arising from the CFI graphs [17] via Mekler's construction [58], suggesting that $\mathsf{FO} + \mathsf{LFP} + \mathsf{C}$ may indeed capture PTIME on groups. Determining whether even $o(\log n)$-dimensional Weisfeiler–Leman can resolve GPI is an open question.

The use on Weisfeiler–Leman for groups is quite new. To the best of our knowledge, using Weisfeiler–Leman for GROUP ISOMORPHISM testing was first attempted by Brooksbank, Grochow, Li, Qiao, & Wilson [14]. Brachter & Schweitzer [12] subsequently introduced three variants of Weisfeiler–Leman for groups that more closely resemble that of graphs. In particular, Brachter & Schweitzer [12] characterized their algorithms in terms of logics and Ehrenfeucht–Fraïssé pebble games. The relationship between the works of Brachter & Schweitzer and Brooksbank, Grochow, Li, Qiao, & Wilson [14] is an interesting question.

In subsequent work, Brachter & Schweitzer [13] further developed the descriptive complexity of finite groups. They showed in particular that low-dimensional Weisfeiler–Leman can detect key group-theoretic invariants such as composition series, radicals, and quotient structure. Furthermore, they also showed that Weisfeiler–Leman can identify direct products in polynomial-time, provided it can also identify the indecomposable direct factors in polynomial-time. Grochow & Levet [30] extended this result to show that Weisfeiler–Leman can compute direct products in parallel, provided it can identify each of the indecomposable direct factors in parallel. Additionally, Grochow & Levet showed that constant-dimensional Weisfeiler–Leman can in a constant number of rounds identify coprime extensions $H \ltimes N$, where the normal Hall subgroup N is Abelian and the complement H is $O(1)$-generated. This placed isomorphism testing into L; the previous bound for isomorphism testing in this family was P [62]. Grochow & Levet also ruled out $\mathsf{FO} + \mathsf{LFP}$ as a candidate logic for capturing PTIME on finite groups, by showing that the count-free Weisfeiler–Leman algorithm cannot even identify Abelian groups in polynomial-time.

2 Preliminaries

We recall the bijective pebble game of Hella [41, 42], in the context of WL on graphs as that is likely more familiar to more readers. This game is often used to show that two graphs X and Y cannot be distinguished by k-WL. The game is an Ehrenfeucht–Fraïssé game, with two players: Spoiler and Duplicator. Each graph begins with $k+1$ pebbles, $p_1, \dots, p_{k+1}$ for X and $p'_1, \dots, p'_{k+1}$ for Y, which are placed beside the graphs. Each round proceeds as follows.

1. Spoiler chooses $i \in [k+1]$, and picks up pebbles p_i, p'_i.
2. We check the winning condition, which will be formalized later.[1]
3. Duplicator chooses a bijection $f : V(X) \to V(Y)$.
4. Spoiler places p_i on some vertex $v \in V(X)$. Then p'_i is placed on $f(v)$.

In a given round, let $v_1, \dots, v_m$ be the vertices of X pebbled at the end of step 1 (in the list above), and let $v'_1, \dots, v'_m$ be the corresponding pebbled vertices of Y. Spoiler wins precisely if the map $v_\ell \mapsto v'_\ell$ is not an isomorphism of the induced subgraphs $X[\{v_1, \dots, v_m\}]$ and $Y[\{v'_1, \dots, v'_m\}]$. Otherwise, at that point, Duplicator wins the game. Spoiler wins, by definition, at round 0 if X and Y do not have the same number of vertices. We note that X and Y are not distinguished by the first r rounds of k-WL if and only if Duplicator wins the first r rounds of the $(k+1)$-pebble game [41, 42, 17].

[1] In the literature, some authors check the winning condition at this point, and others check the winning condition at the end of each round. The choice merely has the effect of changing the number of required pebbles by at most 1 in ordinary WL, or at most q in the q-ary version, and changing the number of rounds by at most 1. We have chosen this convention for consistency with other works on WL specific to groups [12, 13, 30].

Hella [41, 42] exhibited a hierarchy of pebble games where, for $q \geq 1$, Spoiler could pebble a sequence of $1 \leq j \leq q$ elements $(v_1, \ldots, v_j) \mapsto (f(v_1), \ldots, f(v_j))$ in a single round; more formally, following the description above, in step 1, Spoiler picks up q pebbles $p_{i_1}, \ldots, p_{i_q}$ and their partners $p'_{i_1}, \ldots, p'_{i_q}$, with step 4 changed accordingly. The case of $q = 1$ corresponds to the case of Weisfeiler–Leman. As remarked by Hella [42, p. 6, just before §4], the q-ary game immediately identifies all relational structures of arity $\leq q$. For example, the $q = 2$ game on graphs solves GI: for if two graphs X and Y are non-isomorphic, then any bijection $f : V(X) \to V(Y)$ that Duplicator selects must map an adjacent pair of vertices u, v in X to a non-adjacent pair $f(u), f(v)$ in Y or vice-versa. Spoiler immediately wins by pebbling $(u, v) \mapsto (f(u), f(v))$. However, as groups are ternary relational structures (the relation being $\{(a,b,c) : a,b,c \in G, ab = c\}$), the $q = 2$ case can, at least in principle, be non-trivial on groups.

Brachter & Schweitzer [12] adapted Hella's [41, 42] pebble games in the $q = 1$ case to the setting of groups, obtaining three different versions. Their Version III involves reducing to graphs and playing the pebble game on graphs, so we don't consider it further here. Versions I and II are both played on the groups G and H directly.

Both versions are played identically as for graphs, with the only difference being the winning condition. We recall the following standard definitions in order to describe these winning conditions.

Definition 2.1. Let G, H be two groups. Given k-tuples $\overline{g} = (g_1, \ldots, g_k) \in G^k$ and $\overline{h} = (h_1, \ldots, h_k) \in H^k$, we say $(\overline{g}, \overline{h})$ ...

1. *...gives a well-defined map* if $g_i = g_j \Leftrightarrow h_i = h_j$ for all $i \neq j$;

2. ...are *partially isomorphic* or *give a partial isomorphism* if they give a well-defined map, and for all i, j, k we have $g_i g_j = g_k \Leftrightarrow h_i h_j = h_k$;

3. ...are *marked isomorphic* or *give a marked isomorphism* if it gives a well-defined map, and the map extends to an isomorphism $\langle g_1, \ldots, g_k \rangle \to \langle h_1, \ldots, h_k \rangle$.

Let $v_1, \ldots, v_m$ be the group elements of G pebbled at the end of step 1, and let $v'_1, \ldots, v'_m$ be the corresponding pebbled vertices of H. In Version I, Spoiler wins precisely if $(\overline{v}, \overline{v'})$ does not give a partial isomorphism, and in Version II Spoiler wins precisely if $(\overline{v}, \overline{v'})$ does not give a marked isomorphism.

Both Versions I and II may be generalized to allow Spoiler to pebble up to q group elements at a single round, for some $q \geq 1$. Mimicking the proof above for $q = 2$ for graphs, we have that $q = 3$ is sufficient to solve GPI in a single round. The distinguishing power, however, of the $q = 2$ game for groups remains unclear, and is the main subject of this paper. As we are interested in the round complexity, we introduce the following notation.

Definition 2.2 (Notation for pebbles, rounds, arity, and WL version)**.** Let $k \geq 2, r \geq 1$, $q \geq 1$, and $J \in \{I, II\}$. Denote (k,r)-WL_J^q to be the k-pebble, r-round, q-ary Version J pebble game.

We refer to q as the *arity* of the pebble game, as it corresponds to the arity of generalized quantifiers[2] in a logic whose distinguishing power is equivalent to that of the game:

Remark 2.3 (Equivalence with logics with generalized 2-ary quantifiers)**.** Hella [41] describes the game (essentially the same as our description, but with no restriction on number of pebbles, and a transfinite number of rounds) for general q at the bottom of p. 245, for arbitrary relational structures. We restrict to the case of $q = 2$, a finite number of pebbles and rounds, and the (relational) language of groups. Hella proves that this game is equivalent to first-order logic with arbitrary q-ary equantifiers in [41, Thm. 2.5].

[2] As our focus in this paper is not on the viewpoint of generalized quantifiers, we refer the reader to [41] for details.

Observation 2.4. *In the* 2*-ary pebble game, we may assume that Duplicator selects bijections that preserve inverses.*

Proof. Suppose not. First, Duplicator must select bijections that preserve the identity, for if not, Spoiler pebbles $1_G \mapsto f(1) \neq 1_H$ and wins immediately. Next, let $f : G \to H$ be a bijection such that $f(g^{-1}) \neq f(g)^{-1}$. Spoiler pebbles $(g, g^{-1}) \mapsto (f(g), f(g^{-1}))$. Now $gg^{-1} = 1$, while $f(g)f(g^{-1}) \neq 1$. So Spoiler wins. □

We frequently use this observation without mention.

3 Higher-arity Weisfeiler-Leman-style coloring corresponding to higher arity pebble games

Given a k-tuple $\overline{x} = (x_1, \ldots, x_k) \in G^k$, a pair of distinct indices $i, j \in [k]$, and a pair of group elements y, z, we define $\overline{x}_{(i,j)\leftarrow(y,z)}$ to be the k-tuple $\overline{x}'$ that agrees with $\overline{x}$ on all indices besides i, j, and with $x'_i = y, x'_j = z$. If $i = j$, we require $y = z$, and we denote this $\overline{x}_{i\leftarrow y}$.

Finally, two graphs Γ_1, Γ_2, with edge-colorings $c_i \colon E(\Gamma_i) \to C$ to some color set C (for $i = 1, 2$) are color isomorphic if there is a graph isomorphism $\varphi \colon V(\Gamma_1) \to V(\Gamma_2)$ that also preserves colors, in the sense that $c_1((u, v)) = c_2((\varphi(u), \varphi(v))$ for all edges $(u, v) \in E(\Gamma_1)$.

Definition 3.1 (2-ary k-dimensional Weisfeiler-Leman coloring)**.** Let G, H be two groups of the same order, let $k \geq 1$. For all k-tuples $\overline{x}, \overline{y} \in G^k \cup H^k$:

- (Initial coloring, Version I) $\chi_0^{2,I}(\overline{x}) = \chi_0^{2,I}(\overline{y})$ iff $\overline{x}, \overline{y}$ are partially isomorphic.
- (Initial coloring, Version II) $\chi_0^{2,II}(\overline{x}) = \chi_0^{2,II}(\overline{y})$ iff $\overline{x}, \overline{y}$ have the same marked isomorphism type.
- (Color refinement) Given a coloring $\chi \colon G^k \cup H^k \to C$, the color refinement operator R defines a new coloring $R(\chi)$ as follows. For each k-tuple $\overline{x} \in G^k$ (resp., H^k), we define an edge-colored graph $\Gamma_{\overline{x},\chi,i,j}$. If $i = j$, it is the graph on vertex set $V(\Gamma_{\overline{x},\chi,i,i}) = G$ (resp., H) with all self-loops and no other edges, where the color of each self-loop (g, g) is $\chi(\overline{x}_{i\leftarrow g})$. If $i \neq j$, it is the complete directed graph with self-loops on vertex set G (resp., H), where the color of each edge (y, z) is $\chi(\overline{x}_{(i,j)\leftarrow(y,z)})$. For an edge-colored graph Γ, we use $[\Gamma]$ to denote its edge-colored isomorphism class. We then define
$$R(\chi)(\overline{x}) = \left(\chi(\overline{x}); [\Gamma_{\overline{x},\chi,1,1}], [\Gamma_{\overline{x},\chi,1,2}], \ldots, [\Gamma_{\overline{x},\chi,k-1,k}], [\Gamma_{\overline{x},\chi,k,k}]\right).$$
That is, the new color consists of the old color, as well as the tuple of $\binom{k+1}{2}$ edge-colored isomorphism types of the graphs $\Gamma_{\overline{x},\chi,i,j}$.

The refinement operator may be iterated: $R^t(\chi) := R(R^{t-1}(\chi))$, and we define the *stable refinement* of χ as $R^t(\chi)$ where the partition induced by $R^t(\chi)$ on $G^k \cup H^k$ is the same as that induced by $R^{t+1}(\chi)$. We denote the stable refinement by $R^\infty(\chi)$.

Finally, for $J \in \{I, II\}$ and all $r \geq 0$, we define $\chi_{r+1}^{2,J} = R(\chi_r^{2,J})$, and $\chi_\infty^{2,J} := R^\infty(\chi_0^{2,J})$.

Remark 3.2. Brachter & Schweitzer [12] introduced Versions I and II of 1-ary WL, which are equivalent up to a small additive constant in the WL-dimension [12] and $O(\log n)$ rounds [30]. For the purpose of comparison, we introduce Versions I and II of 2-ary WL. We will see later that only one additional round suffices in the 2-ary case (see Thm. 3.7). The differences in Versions I and II of WL (both the 1-ary and 2-ary variants) arise from whether the group is viewed as a structure with a ternary relational structure (Version I) or as a structure with a binary function (Version II).

Remark 3.3. Since it was one of our stumbling blocks in coming up with this generalized coloring, we clarify here how this indeed generalizes the usual 1-ary WL coloring procedure. In the 1-ary "oblivious" k-WL procedure (see [33, §5], equivalent to ordinary WL), the color of a k-tuple $\overline{x}$ is refined using its old color, together with a k-tuple of multisets

$$(\{\{\chi(x_{1\leftarrow y}) : y \in G\}\}, \{\{\chi(x_{2\leftarrow y}) : y \in G\}\}, \dots, \{\{\chi(x_{k\leftarrow y}) : y \in G\}\}).$$

For each i, note that two multisets $\{\{\chi(x_{i\leftarrow y}) : y \in G\}\}$ and $\{\{\chi(x'_{i\leftarrow y}) : y \in G\}\}$ are equal iff the graphs $\Gamma_{\overline{x},\chi,i,i}$ and $\Gamma_{\overline{x}',\chi,i,i}$ are color-isomorphic. That is, edge-colored graphs with only self-loops and no other edges are essentially the same, up to isomorphism, as multisets. Our procedure generalizes this by also considering graphs with other edges, which (as we'll see in the proof of equivalence, which will appear in the full version) are used to encode the choice of 2 simultaneous pebbles by Spoiler in each move of the game.

Theorem 3.4. *Let G,H be two groups of order n, with $\overline{x} \in G^k, \overline{y} \in H^k$. Starting from the initial pebbling $x_i \mapsto y_i$ for all $i = 1,\dots,k$, Spoiler has a winning strategy in the k-pebble, r-round, 2-ary Version J pebble game (for $J \in \{I,II\}$) iff $\chi_r^{2,J}(\overline{x}) \neq \chi_r^{2,J}(\overline{y})$.*

Proof. To appear in the full version. □

Corollary 3.5. *For two groups G,H of the same order and any $k \geq 1$, the following are equivalent:*

1. *The 2-ary k-pebble game does not distinguish two groups G,H*
2. *The multisets of stable colors on G^k and H^k are the same, that is, $\{\{\chi_\infty^{2,J}(\overline{x}) : \overline{x} \in G^k\}\} = \{\{\chi_\infty^{2,J}(\overline{y}) : \overline{y} \in H^k\}\}$*
3. *$\chi_\infty^{2,J}((1_G, 1_G, \dots, 1_G)) = \chi_\infty^{2,J}((1_H, \dots, 1_H))$.*

The analogous result holds in the $q = 1$ case, going back to [12].

Proof. To appear in the full version. □

Remark 3.6. For arbitrary relational structures with relations of arity $a+1$, the a-order pebble game may still be nontrivial, as pointed out in Hella [42, p. 6, just before §4]. Our coloring procedure generalizes in the following way to this more general setting, and the proof of the equivalence between the coloring procedure and Hella's pebble game is the same as the above, *mutatis mutandis*. The main change is that for an a-th order pebble game, instead of just considering a graph on edges of size 1 (when $i = j$) or 2 (when $i \neq j$), we consider an a'-uniform directed hypergraph, where each hyperedge consists of a list of a' vertices, for all $1 \leq a' \leq a$. This gives a coloring equivalent of the logical and game characterizations provided by Hella; this trifecta is partly why we feel it is justified to call this a "higher-arity Weisfeiler–Leman" coloring procedure.

We note that there has been some work on equivalences with specific binary and higher-arity quantifiers: see for instance, the invertible map game of Dawar & Holm [21] which generalizes rank logic, in which Spoiler can place multiple pebbles, but the bijections Duplicator selects must satisfy additional structure. Subsequently, Dawar & Vagnozzi [22] provided a generalization of Weisfeiler–Leman that further subsumes the invertible map game. We note that Dawar & Vagnozzi's "$WL_{k,r}$", although it looks superficially like our r-ary k-WL, is in fact quite different: in particular, their refinement step "flattens" a multiset of multisets into its multiset union, which loses information compared to our 2-ary (resp., r-ary) game; indeed, they show that their $\mathrm{WL}_{*,r}$ is equivalent to ordinary (1-ary) WL for any fixed r, whereas already 2-ary WL can solve GI. In general, the relationship between Hella's 2-ary game and the works of Dawar & Holm and Dawar & Vagnozzi remains open.

3.1 Equivalence between 2-ary (k,r)-WL Versions I and II

In this section we show that, up to additive constants in the number of pebbles and rounds, 2-ary WL Versions I and II are equivalent in their distinguishing power. For two different WL versions W, W', we write $W \preceq W'$ to mean that if W distinguishes two groups G and H, then so does W'.

Theorem 3.7. *Let $k \geq 2, r \geq 1$. We have that:*

$$(k,r)\text{-}WL_I^2 \preceq (k,r)\text{-}WL_{II}^2 \preceq (k+2,r+1)\text{-}WL_I^2.$$

Proof. To appear in the full version. □

4 Descriptive Complexity of Semisimple Groups

In this section, we show that the $(O(1),O(1))$-WL_{II}^2 pebble game can identify groups with no Abelian normal subgroups,[3] also known as semisimple groups. We begin with some preliminaries.

4.1 Preliminaries

Semisimple groups are motivated by the following characteristic filtration:

$$1 \leq \text{Rad}(G) \leq \text{Soc}^*(G) \leq \text{PKer}(G) \leq G,$$

which arises in the computational complexity community where it is known as the Babai–Beals filtration [5], as well as in the development of practical algorithms for computer algebra systems (c.f., [18]). We now explain the terms of this chain. Here, $\text{Rad}(G)$ is the *solvable radical*, which is the unique maximal solvable normal subgroup of G; recall that a group N is solvable if the sequence $N^{(0)} := N$, $N^{(i)} = [N^{(i-1)}, N^{(i-1)}]$ terminates in the trivial group after finitely many steps, and $[A,B]$ denotes the subgroup generated by $\{aba^{-1}b^{-1} : a \in A, b \in B\}$. The socle of a group, denoted $\text{Soc}(G)$, is the subgroup generated by all the minimal normal subgroups of G. $\text{Soc}^*(G)$ is the preimage of the socle $\text{Soc}(G/\text{Rad}(G))$ under the natural projection map $\pi : G \to G/\text{Rad}(G)$. To define PKer, we start by examining the action on $\text{Soc}(G/\text{Rad}(G)) \cong \text{Soc}^*(G)/\text{Rad}(G)$ that is induced by the action of G on $\text{Soc}^*(G)$ by conjugation. As $\text{Soc}^*(G)/\text{Rad}(G) \cong \text{Soc}(G/\text{Rad}(G))$ is the direct product of finite, non-Abelian simple groups $T_1, \ldots, T_k$, this action permutes the k simple factors, yielding a homomorphism $\varphi : G \to S_k$. The kernel of this action is denoted $\text{PKer}(G)$.

When $\text{Rad}(G)$ is trivial, G has no Abelian normal subgroups (and vice versa). We refer to such groups as *semisimple* (following [7, 8]) or trivial-Fitting (following [18]). As a semisimple group G has no Abelian normal subgroups, we have that $\text{Soc}(G)$ is the direct product of non-Abelian simple groups. As the conjugation action of G on $\text{Soc}(G)$ permutes the direct factors of $\text{Soc}(G)$, there exists a faithful permutation representation $\alpha : G \to G^* \leq \text{Aut}(\text{Soc}(G))$. G is determined by $\text{Soc}(G)$ and the action α. Let H be a semisimple group with the associated action $\beta : H \to \text{Aut}(\text{Soc}(H))$. We have that $G \cong H$ precisely if $\text{Soc}(G) \cong \text{Soc}(H)$ via an isomorphism that makes α equivalent to β in the sense introduced next.

We now introduce the notion of permutational isomorphism, which is our notion of equivalence for α and β. Let A and B be finite sets, and let $\pi : A \to B$ be a bijection. For $\sigma \in \text{Sym}(A)$, let $\sigma^\pi \in \text{Sym}(B)$

[3] In many places, we will use $O(1)$ for number of pebbles or rounds; we believe all of these can be replaced with particular numbers by a straightforward, if tedious, analysis of our proofs. However, since our focus is on the fact that these numbers are constant rather than on the exact values, we use the $O(1)$ notation.

be defined by $\sigma^\pi := \pi^{-1}\sigma\pi$. For a set $\Sigma \subseteq \mathrm{Sym}(A)$, denote $\Sigma^\pi := \{\sigma^\pi : \sigma \in \Sigma\}$. Let $K \leq \mathrm{Sym}(A)$ and $L \leq \mathrm{Sym}(B)$ be permutation groups. A bijection $\pi : A \to B$ is a *permutational isomorphism* $K \to L$ if $K^\pi = L$.

The following lemma, applied with $R = \mathrm{Soc}(G)$ and $S = \mathrm{Soc}(H)$, gives a precise characterization of semisimple groups in terms of the associated actions.

Lemma 4.1 ([7, Lemma 3.1], cf. [18, §3])**.** *Let G and H be groups, with $R \triangleleft G$ and $S \triangleleft H$ groups with trivial centralizers. Let $\alpha : G \to \mathrm{Aut}(R)$ and $\beta : H \to \mathrm{Aut}(S)$ be faithful permutation representations of G and H via the conjugation action on R and S, respectively. Let $f : R \to S$ be an isomorphism. Then f extends to an isomorphism $\hat{f} : G \to H$ if and only if f is a permutational isomorphism between $G^* = Im(\alpha)$ and $H^* = Im(\beta)$; and if so, $\hat{f} = \alpha f^* \beta^{-1}$, where $f^* : G^* \to H^*$ is the isomorphism induced by f.*

We also need the following standard group-theoretic lemmas. The first provides a key condition for identifying whether a non-Abelian simple group belongs to the socle. Namely, if $S_1 \cong S_2$ are non-Abelian simple groups where S_1 is in the socle and S_2 is not in the socle, then the normal closures of S_1 and S_2 are non-isomorphic. In particular, the normal closure of S_1 is a direct product of non-Abelian simple groups, while the normal closure of S_2 is not a direct product of non-Abelian simple groups. We will apply this condition later when S_1 is a simple direct factor of $\mathrm{Soc}(G)$; in which case, the normal closure of S_1 is of the form S_1^k.

Lemma 4.2 (c.f. [30, Lemma 6.5])**.** *Let G be a finite semisimple group. A subgroup $S \leq G$ is contained in $Soc(G)$ if and only if the normal closure of S is a direct product of nonabelian simple groups.*

Lemma 4.3 (c.f. [30, Lemma 6.6])**.** *Let $S_1, \ldots, S_k \leq G$ be nonabelian simple subgroups such that for all distinct $i, j \in [k]$ we have $[S_i, S_j] = 1$. Then $\langle S_1, \ldots, S_k\rangle = S_1 S_2 \cdots S_k = S_1 \times \cdots \times S_k$.*

4.2 Main Results

We show that the second Ehrenfeucht–Fraïssé game in Hella's hierarchy can identify both $\mathrm{Soc}(G)$ and the conjugation action when G is semisimple. We first show that this pebble game can identify whether a group is semisimple. Namely, if G is semisimple and H is not semisimple, then Spoiler can distinguish G from H.

Proposition 4.4. *Let G be a semisimple group of order n, and let H be an arbitrary group of order n. If H is not semisimple, then Spoiler can win in the $(4,2)$-WL_{II}^2 game.*

Proof. To appear in the full version. □

We now apply Lemma 4.2 to show that Duplicator must map the direct factors of $\mathrm{Soc}(G)$ to isomorphic direct factors of $\mathrm{Soc}(H)$.

Lemma 4.5. *Let G, H be finite groups of order n. Let $Fac(Soc(G))$ denote the set of simple direct factors of $Soc(G)$. Let $S \in Fac(Soc(G))$ be a non-Abelian simple group, with $S = \langle x, y\rangle$. If Duplicator selects a bijection $f\colon G \to H$ such that:*

(a) $S \ncong \langle f(x), f(y)\rangle$, then Spoiler can win in the $(2,1)$-WL_{II}^2 game; or

(b) $f(S) \neq \langle f(x), f(y)\rangle$, then Spoiler can win in the $(4,2)$-WL_{II}^2 pebble game.

Note that the lemma does not require $f|_S\colon S \to f(S)$ to actually be an isomorphism, only that S and $f(S)$ are isomorphic.

Proof. To appear in the full version. □

Proposition 4.6. *Let G be a semisimple group of order n, and let H be an arbitrary group of order n. Let $f : G \to H$ be the bijection Duplicator selects. If there exists $S \in Fac(Soc(G))$ such that $f(S) \notin Fac(Soc(H))$ or $f(S) \not\cong S$, then Spoiler can win in the $(4,2)$-WL_{II}^2 pebble game.*

Proof. To appear in the full version. □

Lemma 4.7. *Let G,H be groups of order n, let S be a nonabelian simple group in $Fac(Soc(G))$. Let $f, f' : G \to H$ be two bijections selected by Duplicator at two different rounds. If $f(S) \cap f'(S) \neq 1$, then $f(S) = f'(S)$, or Spoiler can win in the $(4,2)$-WL_{II}^2 pebble game.*

Proof. By Prop. 4.6, both $f(S)$ and $f'(S)$ must be simple normal subgroups of $\mathrm{Soc}(H)$ (or Spoiler wins with 4 pebbles and 2 rounds). Since they intersect nontrivially, but distinct simple normal subgroups of $\mathrm{Soc}(H)$ intersect trivially, the two must be equal. □

We next introduce the notion of weight.

Definition 4.8. Let $\mathrm{Soc}(G) = S_1 \times \cdots \times S_k$ where each S_i is a simple normal subgroup of $\mathrm{Soc}(G)$. For any $s \in \mathrm{Soc}(G)$, write $s = s_1 s_2 \cdots s_k$ where each $s_i \in S_i$, and define the *weight* of s, denote $\mathrm{wt}(s)$, as the number of i's such that $s_i \neq 1$.

Note that the definition of weight is well-defined since the S_i are the unique subsets of $\mathrm{Soc}(G)$ that are simple normal subgroup of $\mathrm{Soc}(G)$, so the decomposition $s = s_1 s_2 \ldots s_k$ is unique up to the order of the factors. (This is essentially a particular instance of the "rank lemma" from [30], which intuitively states that WL detects in $O(\log n)$ rounds the set of elements for a given subgroup provided that it also identifies the generators. As we are now in the setting of 2-ary WL we give the full proof, which also has tighter bounds on the number of rounds.)

Lemma 4.9 (Weight Lemma)**.** *Let G,H be semisimple groups of order n. If Duplicator selects a bijection $f : G \to H$ that does not map $Soc(G)$ bijectively to $Soc(H)$, or does not preserve the weight of every element in $Soc(G)$, then Spoiler can win in the $(4,3)$-WL_{II}^2 game.*

Proof. To appear in the full version. □

Lemma 4.10. *Let G and H be semisimple groups with isomorphic socles. Let $S_1, S_2 \in Fac(Soc(G))$ be distinct. Let $f : G \to H$ be the bijection that Duplicator selects. If there exist $x_i \in S_i$ such that $f(x_1x_2) \neq f(x_1)f(x_2)$, then Spoiler can win in the $(4,3)$-WL_{II}^2 pebble game.*

Proof. By Lem. 4.9, we may assume that $\mathrm{wt}(s) = \mathrm{wt}(f(s))$ for all $s \in \mathrm{Soc}(G)$; otherwise, Spoiler wins with at most 4 pebbles and 3 rounds. As $f(x_1x_2)$ has weight 2, $f(x_1x_2)$ belongs to the direct product of two simple factors in $\mathrm{Fac}(\mathrm{Soc}(H))$, so it can be written $f(x_1x_2) = y_1y_2$ with each y_i in distinct simple factors in $\mathrm{Fac}(\mathrm{Soc}(H))$. Without loss of generality suppose that $y_1 \neq f(x_1)$. Spoiler pebbles $(x_1, x_1x_2) \mapsto (f(x_1), f(x_1x_2))$. Now $\mathrm{wt}(x_1^{-1} \cdot x_1x_2) = 1$, while $\mathrm{wt}(f(x_1)^{-1} \cdot f(x_1x_2)) \geq 2$. (Note that we cannot quite yet directly apply Lem. 4.9, because we have not yet identified a single element x such that $\mathrm{wt}(x) \neq \mathrm{wt}(f(x))$.)

On the next round, Duplicator selects another bijection f'. Spoiler now pebbles $x_2 \mapsto f'(x_2)$. Because $\mathrm{wt}(x_1^{-1} \cdot x_1x_2) = 1$ but $\mathrm{wt}(f(x_1)^{-1} f(x_1x_2)) \geq 2$, and f' preserves weight by Lem. 4.9, we have $f'(x_2) \neq f'(x_1)^{-1} f'(x_1x_2)$. Thus, the pebbled map $(x_1, x_2, x_1x_2) \mapsto (f'(x_1), f(x_2), f(x_1x_2))$ does not extend to an isomorphism, and so Spoiler wins with 3 pebbles and 2 rounds. □

Recall that if G is semisimple, then $G \leq \text{Aut}(\text{Soc}(G))$. Now each minimal normal subgroup $N \trianglelefteq G$ is of the form $N = S^k$, where S is a non-Abelian simple group. So $\text{Aut}(N) = \text{Aut}(S) \wr \text{Sym}(k)$. In particular,

$$G \leq \prod_{\substack{N \trianglelefteq G \\ N \text{ is minimal normal}}} \text{Aut}(N).$$

So if $g \in G$, then the conjugation action of g on $\text{Soc}(G)$ acts by (i) automorphism on each simple direct factor of $\text{Soc}(G)$, and (ii) by permuting the direct factors of $\text{Soc}(G)$. Provided generators of the direct factors of the socle are pebbled, Spoiler can detect inconsistencies of the automorphism action. However, doing so directly would be too expensive as there could be $\Theta(\log|G|)$ generators, so we employ a more subtle approach with a similar outcome. By Lem. 4.9, Duplicator must select bijections $f : G \to H$ that preserve weight. That is, if $s \in \text{Soc}(G)$, then $\text{wt}(s) = \text{wt}(f(s))$. We use Lem. 4.9 in tandem with the fact that the direct factors of the socle commute to effectively pebble the set of all the generators at once. Namely, suppose that $\text{Fac}(\text{Soc}(G)) = \{S_1, \ldots, S_k\}$, where $S_i = \langle x_i, y_i \rangle$. Let $x := x_1 \cdots x_k$ and $y := y_1 \cdots y_k$. We will show that it suffices for Spoiler to pebble (x, y) rather than individually pebbling generators for each S_i (this will still allow the factors to be permuted, but that is all).

Lemma 4.11. *Let G and H be semisimple groups with isomorphic socles, and write $Fac(Soc(G)) = \{S_1, \ldots, S_m\}$, with $S_i = \langle x_i, y_i \rangle$. Let $f : G \to H$ be the bijection that Duplicator selects, and suppose that (i) for all i, $f(S_i) \cong S_i$ (though $f|_{S_i}$ need not be an isomorphism) and $f(S_i) \in Fac(Soc(H))$, (ii) for every $s \in Soc(G)$, $wt(s) = wt(f(s))$, and (iii) for all i, $f(S_i) = \langle f(x), f(y) \rangle$.*

Now suppose that Spoiler pebbles $(x_1 \cdots x_m, y_1 \cdots y_m) \mapsto (f(x_1 \cdots x_m), f(y_1 \cdots y_m))$. As f preserves weight, we may write $f(x_1 \cdots x_m) = h_1 \cdots h_m$ and $f(y_1 \cdots y_m) = z_1 \cdots z_m$ with $h_i, z_i \in f(S_i)$ for all i.

Let $f' : G \to H$ be the bijection that Duplicator selects at any subsequent round in which the pebble used above has not moved. If any of the following hold, then Spoiler can win in the WL_{II}^2 pebble game with 5 additional pebbles and 5 additional rounds:

(a) f' does not satisfy conditions (i)–(iii),

(b) there exists an $i \in [m]$ such that $f'(x_i) \notin \{h_1, \ldots, h_m\}$ or $f'(y_i) \notin \{z_1, \ldots, z_m\}$

(c) $f'|_{S_i}$ is not an isomorphism

(d) there exists $g \in G$ and $i \in [m]$ such that $gS_ig^{-1} = S_i$ and for some $x \in S_i$, the following holds: $f'(gxg^{-1}) \neq f'(g)f'(x)f'(g)^{-1}$.

Proof. To appear in the full version. □

Lem. 4.11 provides enough to establish that Spoiler can force Duplicator to select at each round a bijection that restricts to an isomorphism on the socles.

Proposition 4.12. *(Same assumptions as Lem. 4.11.) Let G and H be semisimple groups with isomorphic socles, with $Fac(Soc(G)) = \{S_1, \ldots, S_m\}$, with $S_i = \langle x_i, y_i \rangle$. Let $f_0 : G \to H$ be the bijection that Duplicator selects, and suppose that (i) for all i, $f_0(S_i) \cong S_i$ (though $f_0|_{S_i}$ need not be an isomorphism) and $f_0(S_i) \in Fac(Soc(H))$, (ii) for every $s \in Soc(G)$, $wt(s) = wt(f_0(s))$, and (iii) for all i, $f_0(S_i) = \langle f_0(x), f_0(y) \rangle$. Now suppose that Spoiler pebbles $(x_1 \cdots x_m, y_1 \cdots y_m) \mapsto (f_0(x_1 \cdots x_m), f_0(y_1 \cdots y_m))$.*

Let $f' : G \to H$ be the bijection that Duplicator selects at any subsequent round in which the pebbles used above have not moved. Then $f'|_{Soc(G)} : Soc(G) \to Soc(H)$ must be an isomorphism, or Spoiler can win in 4 more rounds using at most 6 more pebbles (for a total of 7 pebbles and 5 rounds) in the WL_{II}^2 pebble game.

Proof. To appear in the full version. □

Remark 4.13. Brachter & Schweitzer [13, Lemma 5.22] previously showed that (1-ary) Weisfeiler–Leman can decide whether two groups have isomorphic socles. However, their results did not solve the search problem; that is, they did not show Duplicator must select bijections that restrict to an isomorphism on the socle even in the case for semisimple groups. This contrasts with Lem. 4.12, where we show that 2-ary WL effectively solves the search problem. This is an important ingredient in our proof that the $(7, O(1))$-WL_{II}^{2} pebble game solves isomorphism for semisimple groups.

We obtain as a corollary of Lem. 4.11 and Lem. 4.12 that if G and H are semisimple, then Duplicator must select bijections that restrict to isomorphisms of $\text{PKer}(G)$ and $\text{PKer}(H)$.

Corollary 4.14. *Let G and H be semisimple groups of order n. Let Fac(Soc(G))* $:= \{S_1, \ldots, S_m\}$*, and suppose that* $S_i = \langle x_i, y_i \rangle$*. Let* $x := x_1 \cdots x_m$ *and* $y := y_1 \cdots y_m$*. and Let* $f : G \to H$ *be the bijection that Duplicator selects. Spoiler begins by pebbling* $(x,y) \mapsto (f(x), f(y))$*. Let* $f' : G \to H$ *be the bijection that Duplicator selects at the next round. If* $f'|_{\text{PKer}(G)} : \text{PKer}(G) \to \text{PKer}(H)$ *is not an isomorphism, then Spoiler can win with* 5 *additional pebbles and* 5 *additional rounds in the* WL_{II}^{2} *pebble game.*

Proof. To appear in the full version. □

We now show that if G and H are not permutationally equivalent, then Spoiler can win.

Lemma 4.15. *(Same assumptions as Lem. 4.11.) Let G and H be semisimple groups with isomorphic socles, with* $Fac(Soc(G)) = \{S_1, \ldots, S_m\}$*, with* $S_i = \langle x_i, y_i \rangle$*. Let* $f_0 : G \to H$ *be the bijection that Duplicator selects, and suppose that (i) for all i,* $f_0(S_i) \cong S_i$ *(though* $f_0|_{S_i}$ *need not be an isomorphism) and* $f_0(S_i) \in Fac(Soc(H))$*, (ii) for every* $s \in Soc(G)$*,* $wt(s) = wt(f_0(s))$*, and (iii) for all i,* $f_0(S_i) = \langle f_0(x), f_0(y) \rangle$*. Now suppose that Spoiler pebbles* $(x_1 \cdots x_m, y_1 \cdots y_m) \mapsto (f_0(x_1 \cdots x_m), f_0(y_1 \cdots y_m))$*.*

Let $f' : G \to H$ *be the bijection that Duplicator selects at the next round. Suppose that there exist* $g \in G$ *and* $i \in [m]$ *such that* $f'(gS_ig^{-1}) = f'(S_j)$*, but* $f'(g)f'(S_i)f'(g)^{-1} = f'(S_k)$ *for some* $k \neq j$*. Then Spoiler can win with* 4 *additional pebbles and* 4 *additional rounds in the* WL_{II}^{2} *pebble game.*

Proof. To appear in the full version. □

Theorem 4.16. *Let G be a semisimple group and H an arbitrary group of order n, not isomorphic to G. Then Spoiler has a winning strategy in the* $(9, O(1))$-WL_{II}^{2} *pebble game.*

Proof. If H is not semisimple, then by Prop. 4.4, Spoiler wins with 4 pebbles and 2 rounds. So we now suppose H is semisimple.

Let $\text{Fac}(\text{Soc}(G)) = \{S_1, \ldots, S_k\}$, and let x_i, y_i be generators of S_i for each i. Let f be the bijection chosen by Duplicator. Spoiler pebbles $(x_1x_2 \cdots x_k, y_1y_2, \ldots, y_k) \mapsto (f(x_1 \cdots x_k), f(y_1 \cdots y_k))$. On subsequent rounds, we thus have satisfied the hypotheses of Lem. 4.11 and Prop. 4.12. Spoiler will never move this pebble, and thus all subsequent bijections chosen by Duplicator must restrict to isomorphisms on the socle (or Spoiler wins with at most 7 pebbles and $O(1)$ rounds).

Recall from Lem. 4.1 that $G \cong H$ iff there is an isomorphism $\mu \colon \text{Soc}(G) \to \text{Soc}(H)$ that induces a permutational isomorphism $\mu^* \colon G^* \to H^*$. Thus, since $G \ncong H$, there must be some $g \in G$ and $s \in \text{Soc}(G)$ such that $f(gsg^{-1}) \neq f(g)f(s)f(g)^{-1}$. Write $s = s_1 \cdots s_k$ with each $s_i \in S_i$ (not necessarily nontrivial).

We claim that there exists some i such that $f(gs_ig^{-1}) \neq f(g)f(s_i)f(g)^{-1}$. For suppose not, then we have

$$\begin{aligned} f(gsg^{-1}) &= f(gs_1g^{-1}gs_2g^{-1}\cdots gs_kg^{-1}) \\ &= f(gs_1g^{-1})f(gs_2g^{-1})\cdots f(gs_kg^{-1}) \\ &= f(g)f(s_1)f(g)^{-1}f(g)f(s_2)f(g)^{-1}\cdots f(g)f(s_k)f(g)^{-1} \\ &= f(g)f(s_1\cdots s_k)f(g)^{-1} = f(g)f(s)f(g)^{-1}, \end{aligned}$$

a contradiction. For simplicity of notation, without loss of generality we may assume $i = 1$, so we now have $f(gs_1g)^{-1} \neq f(g)f(s_1)f(g)^{-1}$.

We break the argument into cases:

1. If $gs_1g^{-1} \in S_1$, then we have $gS_1g^{-1} = S_1$ (any two distinct simple normal factors of the socle intersect trivially), we have by Lem. 4.11 (d) that Spoiler can win with at most 5 additional pebbles (for a total of 7 pebbles) and 5 additional rounds (for a total of 6 rounds).
2. If $gs_1g^{-1} \in S_j$ for $j \neq 1$ and $f(g)f(s_1)f(g)^{-1} \notin f(S_j)$, we have by Lem. 4.15 that Spoiler can win with at most 4 additional pebbles (for a total of 6 pebbles) and 4 additional rounds (for a total of 5 rounds).
3. Suppose now that $gs_1g^{-1} \in S_j$ for some $j \neq 1$ and $f(g)f(s_1)f(g)^{-1} \in f(S_j)$. Spoiler begins by pebbling $(g, gs_1g^{-1}) \mapsto (f(g), f(gs_1g^{-1}))$. Let $f' : G \to H$ be the bijection that Duplicator selects at the next round. As $gs_1g^{-1} \in S_j$ is pebbled, we have that $f'(S_j) = f(S_j)$ by Lem. 4.7 (or Spoiler wins with 4 additional pebbles and 2 additional rounds). Now by assumption, $gS_1g^{-1} = S_j$ and $f(g)f(S_1)f(g)^{-1} = f(S_j)$. So as $g \mapsto f(g)$ is pebbled, we claim that we may assume $f'(S_1) = f(S_1)$. For suppose not; then we have $g^{-1}S_jg = S_1$ but $f'(g)^{-1}f'(S_j)f'(g) = f(g)^{-1}f(S_j)f(g) = f(S_1) \neq f'(S_1)$. But then Spoiler can with win with 4 additional pebbles (for a total of 8 pebbles) and 4 additional rounds (for a total of 7 rounds) by Lem. 4.15. Thus we have $f'(S_1) = f(S_1)$.

   In particular, we have that $f'(x_1) = f(x_1)$ and $f'(y_1) = f(y_1)$, by the same argument as in the proof of Lem. 4.11 (c). As $S_1 = \langle x_1, y_1 \rangle$, we have that $f'(s_1) = f(s_1)$, since they are both isomorphisms on the socle by Prop. 4.12. Spoiler now pebbles $(x_1, y_1) \mapsto (f'(x_1), f'(y_1))$. As the pebbled map $(g, x_1, y_1, gs_1g^{-1}) \mapsto (f(g), f'(x_1), f'(y_1), f'(gs_1g^{-1}))$ does not extend to an isomorphism, Spoiler wins. In this case, Spoiler used at most 8 pebbles and 7 rounds.

Note that the ninth pebble is the one we pick up prior to checking the winning condition. □

5 Conclusion

We exhibited a novel Weisfeiler–Leman algorithm that provides an algorithmic characterization of the second Ehrenfeucht–Fraïssé game in Hella's [41, 42] hierarchy. We also showed that this Ehrenfeucht–Fraïssé game can identify groups without Abelian normal subgroups using $O(1)$ pebbles and $O(1)$ rounds. In particular, within the first few rounds, Spoiler can force Duplicator to select an isomorphism at each subsequent round. This effectively solves the search problem in the pebble game characterization.

Our work leaves several directions for further research.

Question 5.1. Can the constant-dimensional 2-ary Wesifeiler–Leman algorithm be implemented in time $n^{o(\log n)}$?

Question 5.2. What is the (1-ary) Weisfeiler–Leman dimension of groups without Abelian normal subgroups?

Question 5.3. Show that the second Ehrenfeucht–Fraïssé game in Hella's hierarchy can identify coprime extensions of the form $H \ltimes N$ with both H, N Abelian (the analogue of [62]). More generally, an analogue of Babai–Qiao [9] would be to show that when $|H|, |N|$ are coprime and N is Abelian, that Spoiler can distinguish $H \ltimes N$ from any non-isomorphic group using a constant number of pebbles that is no more than that which is required to identify H (or the maximum of that of H and a constant independent of N, H).

Question 5.4. Let $p > 2$ be prime, and let G be a p-group with bounded genus. Show that in the second Ehrenfeucht–Fraïssé game in Hella's hierarchy, Spoiler has a winning strategy using a constant number of pebbles. This is a descriptive complexity analogue of [15, 46]. It would even be of interest to start with the case where G has bounded genus over a field extension $K/\mathbb{F}_p$ of bounded degree.

In the setting of groups, Hella's hierarchy collapses to some $q \leq 3$, since 3-ary WL can identify all ternary relational structures, including groups. It remains open to determine whether this hierarchy collapses further to either $q = 1$ or $q = 2$. Even if it does not collapse, it would also be of interest to determine whether the 1-ary and 2-ary games are equivalent. Algorithmically, this is equivalent to determining whether 1-ary and 2-ary WL are have the same distinguishing power.

Question 5.5. Does there exist an infinite family of non-isomorphic pairs of groups $\{(G_n, H_n)\}$ for which Spoiler requires $\omega(1)$ pebbles to distinguish G_n from H_n? We ask this question for the Ehrenfeucht–Fraïssé games at both the first and second levels of Hella's hierarchy.

Recall that the game at the first level of Hella's hierarchy is equivalent to Weisfeiler–Leman [17, 41, 42], and so a lower bound against either of these games provides a lower bound against Weisfeiler–Leman. More generally, it would also be of interest to investigate Hella's hierarchy on higher arity structures. For a q-ary relational structure, the q-ary pebble game suffices to decide isomorphism. Are there interesting, natural classes of higher arity structures for which Hella's hierarchy collapses further to some level $q' < q$?

Acknowledgment

The authors would like to thank Pascal Schweitzer and the anonymous referees for feedback on earlier versions of some of the results in this paper, as well as discussions more directly relevant to the paper. JAG would like to thank Martin Grohe for helpful correspondence about WL versus "oblivious WL." JAG was partially supported by NSF award DMS-1750319 and NSF CAREER award CCF-2047756 and during this work. ML was partially supported by J. Grochow startup funds, NSF award CISE-2047756, and a Summer Research Fellowship through the Department of Computer Science at the University of Colorado Boulder.

References

[1] Miklos Ajtai & Ronald Fagin (1990): *Reachability is harder for directed than for undirected finite graphs.* Journal of Symbolic Logic 55(1), p. 113–150, doi:10.2307/2274958.

[2] Sanjeev Arora & Ronald Fagin (1997): *On winning strategies in Ehrenfeucht–Fraïssé games.* Theoretical Computer Science 174(1), pp. 97–121, doi:10.1016/S0304-3975(96)00015-1.

[3] V. Arvind & Piyush P. Kurur (2006): *Graph Isomorphism is in SPP.* Information and Computation 204(5), pp. 835–852, doi:10.1016/j.ic.2006.02.002.

[4] László Babai (2016): *Graph isomorphism in quasipolynomial time [extended abstract]*. In: *STOC'16—Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, ACM, New York, pp. 684–697, doi:10.1145/2897518.2897542. Preprint of full version at arXiv:1512.03547v2 [cs.DS].

[5] László Babai & Robert Beals (1999): *A polynomial-time theory of black box groups I*. In: *Groups St Andrews 1997 in Bath, I*, doi:10.1017/CBO9781107360228.004.

[6] László Babai, Robert Beals & Ákos Seress (2009): *Polynomial-Time Theory of Matrix Groups*. In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, Association for Computing Machinery, p. 55–64, doi:10.1145/1536414.1536425.

[7] László Babai, Paolo Codenotti, Joshua A. Grochow & Youming Qiao (2011): *Code equivalence and group isomorphism*. In: *Proceedings of the Twenty-Second Annual ACM–SIAM Symposium on Discrete Algorithms (SODA11)*, SIAM, Philadelphia, PA, pp. 1395–1408, doi:10.1137/1.9781611973082.107.

[8] László Babai, Paolo Codenotti & Youming Qiao (2012): *Polynomial-Time Isomorphism Test for Groups with No Abelian Normal Subgroups - (Extended Abstract)*. In: *International Colloquium on Automata, Languages, and Programming (ICALP)*, pp. 51–62, doi:10.1007/978-3-642-31594-7_5.

[9] László Babai & Youming Qiao (2012): *Polynomial-time Isomorphism Test for Groups with Abelian Sylow Towers*. In: *29th STACS*, Springer LNCS 6651, pp. 453 – 464, doi:10.4230/LIPIcs.STACS.2012.453.

[10] Hans Ulrich Besche & Bettina Eick (1999): *Construction of finite groups*. *J. Symb. Comput.* 27(4), pp. 387–404, doi:10.1006/jsco.1998.0258.

[11] Hans Ulrich Besche, Bettina Eick & E.A. O'Brien (2002): *A Millennium Project: Constructing Small Groups*. *Intern. J. Alg. and Comput* 12, pp. 623–644, doi:10.1142/S0218196702001115.

[12] Jendrik Brachter & Pascal Schweitzer (2020): *On the Weisfeiler–Leman Dimension of Finite Groups*. In Holger Hermanns, Lijun Zhang, Naoki Kobayashi & Dale Miller, editors: *LICS '20: 35th Annual ACM/IEEE Symposium on Logic in Computer Science, Saarbrücken, Germany, July 8-11, 2020*, ACM, pp. 287–300, doi:10.1145/3373718.3394786.

[13] Jendrik Brachter & Pascal Schweitzer (2021): *A Systematic Study of Isomorphism Invariants of Finite Groups via the Weisfeiler–Leman Dimension*. arXiv:2111.11908 [math.GR].

[14] Peter A. Brooksbank, Joshua A. Grochow, Yinan Li, Youming Qiao & James B. Wilson (2019): *Incorporating Weisfeiler–Leman into algorithms for group isomorphism*. arXiv:1905.02518 [cs.CC].

[15] Peter A. Brooksbank, Joshua Maglione & James B. Wilson (2017): *A fast isomorphism test for groups whose Lie algebra has genus 2*. *Journal of Algebra* 473, pp. 545–590, doi:10.1016/j.jalgebra.2016.12.007.

[16] Harry Buhrman & Steven Homer (1992): *Superpolynomial Circuits, Almost Sparse Oracles and the Exponential Hierarchy*. In R. K. Shyamasundar, editor: *Foundations of Software Technology and Theoretical Computer Science, 12th Conference, New Delhi, India, December 18-20, 1992, Proceedings*, *Lecture Notes in Computer Science* 652, Springer, pp. 116–127, doi:10.1007/3-540-56287-7_99.

[17] Jin-Yi Cai, Martin Fürer & Neil Immerman (1992): *An optimal lower bound on the number of variables for graph identification*. *Combinatorica* 12(4), pp. 389–410, doi:10.1007/BF01305232. Originally appeared in SFCS '89.

[18] John J. Cannon & Derek F. Holt (2003): *Automorphism group computation and isomorphism testing in finite groups*. *J. Symb. Comput.* 35, pp. 241–267, doi:10.1016/S0747-7171(02)00133-5.

[19] Arkadev Chattopadhyay, Jacobo Torán & Fabian Wagner (2013): *Graph isomorphism is not* AC^0*-reducible to group isomorphism*. *ACM Trans. Comput. Theory* 5(4), pp. Art. 13, 13, doi:10.1145/2540088. Preliminary version appeared in FSTTCS '10; ECCC Tech. Report TR10-117.

[20] Bireswar Das & Shivdutt Sharma (2019): *Nearly Linear Time Isomorphism Algorithms for Some Nonabelian Group Classes*. In René van Bevern & Gregory Kucherov, editors: *Computer Science – Theory and Applications*, Springer International Publishing, Cham, pp. 80–92, doi:10.1007/s00224-020-10010-z.

[21] Anuj Dawar & Bjarki Holm (2012): *Pebble Games with Algebraic Rules*. In Artur Czumaj, Kurt Mehlhorn, Andrew Pitts & Roger Wattenhofer, editors: *Automata, Languages, and Programming*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 251–262, doi:10.1007/978-3-642-31585-5_25.

[22] Anuj Dawar & Danny Vagnozzi (2020): *Generalizations of k-dimensional Weisfeiler–Leman stabilization*. *Moscow Journal of Combinatorics and Number Theory* 9, pp. 229–252, doi:10.2140/moscow.2020.9.229.

[23] Heiko Dietrich & James B. Wilson (2022): *Polynomial-time isomorphism testing for groups of most finite orders*, doi:10.1109/FOCS52979.2021.00053.

[24] A. Ehrenfeucht (1960/61): *An application of games to the completeness problem for formalized theories*. *Fund. Math.* 49, pp. 129–141, doi:10.4064/fm-49-2-129-141.

[25] Bettina Eick, C. R. Leedham-Green & E. A. O'Brien (2002): *Constructing automorphism groups of p-groups*. *Comm. Algebra* 30(5), pp. 2271–2295, doi:10.1081/AGB-120003468.

[26] Jörg Flum & Martin Grohe (2000): *On Fixed-Point Logic with Counting*. *The Journal of Symbolic Logic* 65(2), pp. 777–787, doi:10.2307/2586569.

[27] Roland Fraïssé (1954): *Sur quelques classifications des systèmes de relations*. *Publ. Sci. Univ. Alger. Sér. A* 1, pp. 35–182 (1955).

[28] Walid Gomaa (2010): *Descriptive Complexity of Finite Abelian Groups*. *IJAC* 20, pp. 1087–1116, doi:10.1142/S0218196710006047.

[29] Joshua A. Grochow & Michael Levet (2022): *On the Descriptive Complexity of Groups without Abelian Normal Subgroups*. arXiv:2209.13725.

[30] Joshua A. Grochow & Michael Levet (2022): *On the parallel complexity of Group Isomorphism and canonization via Weisfeiler–Leman*. arXiv:2112.11487 [cs.DS].

[31] Joshua A. Grochow & Youming Qiao (2015): *Polynomial-Time Isomorphism Test of Groups that are Tame Extensions - (Extended Abstract)*. In: *Algorithms and Computation - 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings*, pp. 578–589, doi:10.1007/978-3-662-48971-0_49.

[32] Martin Grohe (2017): *Descriptive complexity, canonisation, and definable graph structure theory*. *Lecture Notes in Logic* 47, Association for Symbolic Logic, Ithaca, NY; Cambridge University Press, Cambridge, doi:10.1017/9781139028868.

[33] Martin Grohe (2021): *The logic of graph neural networks*. In: *LICS '21: Proceedings of the 36th Annual ACM/IEEE Symposium on Logic in Computer Science*, doi:10.1109/LICS52264.2021.9470677. Preprint arXiv:2104.14624 [cs.LG].

[34] Martin Grohe & Sandra Kiefer (2019): *A Linear Upper Bound on the Weisfeiler–Leman Dimension of Graphs of Bounded Genus*. arXiv:1904.07216.

[35] Martin Grohe & Sandra Kiefer (2021): *Logarithmic Weisfeiler–Leman Identifies All Planar Graphs*. arXiv:2106.16218.

[36] Martin Grohe & Daniel Neuen (2019): *Canonisation and Definability for Graphs of Bounded Rank Width*. arXiv:1901.10330.

[37] Martin Grohe & Martin Otto (2015): *Pebble Games and linear equations*. *J. Symb. Log.* 80(3), pp. 797–844, doi:10.1017/jsl.2015.28.

[38] Martin Grohe & Oleg Verbitsky (2006): *Testing Graph Isomorphism in Parallel by Playing a Game*. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone & Ingo Wegener, editors: *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part I*, *Lecture Notes in Computer Science* 4051, Springer, pp. 3–14, doi:10.1007/11786986_2.

[39] Xiaoyu He & Youming Qiao (2021): *On the Baer–Lovász–Tutte construction of groups from graphs: Isomorphism types and homomorphism notions*. *Eur. J. Combin.* 98, p. 103404, doi:10.1016/j.ejc.2021.103404.

[40] Hermann Heineken & Hans Liebeck (1974): *The occurrence of finite groups in the automorphism group of nilpotent groups of class* 2. Arch. Math. (Basel) 25, pp. 8–16, doi:10.1007/BF01238631.

[41] Lauri Hella (1989): *Definability hierarchies of generalized quantifiers*. Annals of Pure and Applied Logic 43(3), pp. 235 – 271, doi:10.1016/0168-0072(89)90070-5.

[42] Lauri Hella (1996): *Logical Hierarchies in PTIME*. Information and Computation 129(1), pp. 1–19, doi:10.1006/inco.1996.0070.

[43] Neil Immerman (1986): *Relational Queries Computable in Polynomial Time*. Inf. Control. 68(1-3), pp. 86–104, doi:10.1016/S0019-9958(86)80029-8.

[44] Neil Immerman & Eric Lander (1990): *Describing Graphs: A First-Order Approach to Graph Canonization*. In Alan L. Selman, editor: Complexity Theory Retrospective: In Honor of Juris Hartmanis on the Occasion of His Sixtieth Birthday, July 5, 1988, Springer New York, New York, NY, pp. 59–81, doi:10.1007/978-1-4612-4478-3_5.

[45] Russell Impagliazzo, Ramamohan Paturi & Francis Zane (2001): *Which Problems Have Strongly Exponential Complexity?* Journal of Computer and System Sciences 63(4), pp. 512–530, doi:10.1006/jcss.2001.1774.

[46] Gábor Ivanyos & Youming Qiao (2019): *Algorithms Based on *-Algebras, and Their Applications to Isomorphism of Polynomials with One Secret, Group Isomorphism, and Polynomial Identity Testing*. SIAM J. Comput. 48(3), pp. 926–963, doi:10.1137/18M1165682.

[47] T. Kavitha (2007): *Linear time algorithms for Abelian group isomorphism and related problems*. Journal of Computer and System Sciences 73(6), pp. 986 – 996, doi:10.1016/j.jcss.2007.03.013.

[48] Neeraj Kayal & Timur Nezhmetdinov (2009): *Factoring Groups Efficiently*. In Susanne Albers, Alberto Marchetti-Spaccamela, Yossi Matias, Sotiris Nikoletseas & Wolfgang Thomas, editors: Automata, Languages and Programming, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 585–596, doi:10.1007/978-3-642-02927-1_49.

[49] Sandra Kiefer & Brendan D. McKay (2020): *The Iteration Number of Colour Refinement*. In Artur Czumaj, Anuj Dawar & Emanuela Merelli, editors: 47th International Colloquium on Automata, Languages, and Programming, ICALP 2020, July 8-11, 2020, Saarbrücken, Germany (Virtual Conference), LIPIcs 168, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 73:1–73:19, doi:10.4230/LIPIcs.ICALP.2020.73.

[50] Sandra Kiefer, Ilia Ponomarenko & Pascal Schweitzer (2019): *The Weisfeiler–Leman Dimension of Planar Graphs Is at Most 3*. J. ACM 66(6), doi:10.1145/3333003.

[51] Sandra Kiefer, Pascal Schweitzer & Erkal Selman (2022): *Graphs Identified by Logics with Counting*. ACM Trans. Comput. Log. 23(1), pp. 1:1–1:31, doi:10.1145/3417515.

[52] Johannes Köbler, Uwe Schöning & Jacobo Torán (1992): *Graph Isomorphism is Low for PP*. Comput. Complex. 2, pp. 301–330, doi:10.1007/BF01200427.

[53] Richard E. Ladner (1975): *On the Structure of Polynomial Time Reducibility*. J. ACM 22(1), p. 155–171, doi:10.1145/321864.321877.

[54] François Le Gall (2009): *Efficient Isomorphism Testing for a Class of Group Extensions*. In: Proc. 26th STACS, pp. 625–636, doi:10.4230/LIPIcs.STACS.2009.1830.

[55] François Le Gall & David J. Rosenbaum (2016): *On the Group and Color Isomorphism Problems*. arXiv:1609.08253 [cs.CC].

[56] Mark L. Lewis & James B. Wilson (2012): *Isomorphism in expanding families of indistinguishable groups*. Groups - Complexity - Cryptology 4(1), pp. 73–110, doi:10.1515/gcc-2012-0008.

[57] P. Lindstrom (1966): *First Order Predicate Logic with Generalized Quantifiers*. Theoria 32(3), pp. 186–195, doi:10.1111/j.1755-2567.1966.tb00600.x.

[58] Alan H. Mekler (1981): *Stability of Nilpotent Groups of Class 2 and Prime Exponent*. The Journal of Symbolic Logic 46(4), pp. 781–788, doi:10.2307/2273227. Available at http://www.jstor.org/stable/2273227.

[59] Gary L. Miller (1978): *On the $n^{\log n}$ Isomorphism Technique (A Preliminary Report)*. In: Proceedings of the Tenth Annual ACM Symposium on Theory of Computing, STOC '78, Association for Computing Machinery, New York, NY, USA, pp. 51–58, doi:10.1145/800133.804331.

[60] Andrzej Mostowski (1957): *On a generalization of quantifiers*. Fundamenta Mathematicae 44(1), pp. 12–36, doi:10.4064/fm-44-1-12-36. Available at http://eudml.org/doc/213418.

[61] André Nies & Katrin Tent (2017): *Describing finite groups by short first-order sentences*. Israel J. Math. 221(1), pp. 85–115, doi:10.1007/s11856-017-1563-2.

[62] Youming Qiao, Jayalal M. N. Sarma & Bangsheng Tang (2011): *On Isomorphism Testing of Groups with Normal Hall Subgroups*. In: Proc. 28th STACS, pp. 567–578, doi:10.4230/LIPIcs.STACS.2011.567.

[63] David J. Rosenbaum (2013): *Bidirectional Collision Detection and Faster Deterministic Isomorphism Testing*. arXiv:1304.3935 [cs.DS].

[64] Benjamin Rossman (2009): *Ehrenfeucht–Fraïssé Games on Random Structures*. In Hiroakira Ono, Makoto Kanazawa & Ruy J. G. B. de Queiroz, editors: Logic, Language, Information and Computation, 16th International Workshop, WoLLIC 2009, Tokyo, Japan, June 21-24, 2009. Proceedings, Lecture Notes in Computer Science 5514, Springer, pp. 350–364, doi:10.1007/978-3-642-02261-6_28.

[65] C. Savage (1980): *An $O(n^2)$ Algorithm for Abelian Group Isomorphism*. Technical Report, North Carolina State University.

[66] Uwe Schöning (1988): *Graph isomorphism is in the low hierarchy*. Journal of Computer and System Sciences 37(3), pp. 312 – 323, doi:10.1016/0022-0000(88)90010-4.

[67] Moshe Y. Vardi (1982): *The Complexity of Relational Query Languages (Extended Abstract)*. In Harry R. Lewis, Barbara B. Simons, Walter A. Burkhard & Lawrence H. Landweber, editors: Proceedings of the 14th Annual ACM Symposium on Theory of Computing, May 5-7, 1982, San Francisco, California, USA, ACM, pp. 137–146, doi:10.1145/800070.802186.

[68] Narayan Vikas (1996): *An $O(n)$ Algorithm for Abelian p-Group Isomorphism and an $O(n \log n)$ Algorithm for Abelian Group Isomorphism*. Journal of Computer and System Sciences 53(1), pp. 1–9, doi:10.1006/jcss.1996.0045.

[69] James B. Wilson (2012): *Existence, algorithms, and asymptotics of direct product decompositions, I*. Groups - Complexity - Cryptology 4(1), doi:10.1515/gcc-2012-0007.

[70] James B. Wilson (2019): *The Threshold for Subgroup Profiles to Agree is Logarithmic*. Theory of Computing 15(19), pp. 1–25, doi:10.4086/toc.2019.v015a019.

[71] V. N. Zemlyachenko, N. M. Korneenko & R. I. Tyshkevich (1985): *Graph isomorphism problem*. J. Soviet Math. 29(4), pp. 1426–1481, doi:10.1007/BF02104746.