On the Complexities of Intersection Problems in Permutation Groups

Takunari Miyazaki

Abstract. Motivated by the question of determining the difference in complexity between the graph-isomorphism and graph-automorphism problems, we study the relationship between the *coset-intersection* (C-INT) and *group-intersection* (G-INT) problems in permutation groups. We report that G-INT is related to C-INT asymmetrically under Ogiwara and Watanabe's notions of *left* and *right* sets. This asymmetry suggests that, for given two permutation groups that intersect nontrivially, finding the least nonidentity element in the intersection is likely to be easier than finding the largest nonidentity element in the intersection under the natural lexicographic ordering. Also as a consequence, unless it belongs to P, C-INT (resp. G-INT) is not many-one reducible in polynomial time to any sparse set.

Mathematics Subject Classification (2000). Primary 68Q25; Secondary 20B40.

Determining the complexity of the graph-isomorphism (GI) problem, i.e., the decision problem of testing whether or not two given graphs are isomorphic, is a long-standing unsolved fundamental question in complexity theory. To this date, GI has not been known to be in P nor NP-complete; furthermore, there is strong evidence to suggest that the problem is unlikely to be NP-complete (see, e.g., [4]).

Of the significant affirmative results concerning GI, including Luks's classic polynomial-time algorithm to test isomorphism of graphs of bounded valence [6], many have successfully exploited the problem's close relationship with a class of permutation-group problems usually represented by the following problem (cf. [7]).

Let $\mathrm{Sym}(\Omega)$ denote the *symmetric group* of all permutations on a set Ω of n points. As usual, we assume that permutation groups are specified by generators.

Problem 1. Coset intersection (C-INT).
Instance: $G, H \leq \mathrm{Sym}(\Omega)$ *and* $x \in \mathrm{Sym}(\Omega)$.
Question: *Is* $G \cap Hx \neq \emptyset$*?*

Indeed, GI is $\leq_m^p$-reducible, i.e., many-one reducible in polynomial time, to C-INT, but the converse is not known under any polynomial-time reducibility.

Motivated by this relationship and practical applications in computational group theory (such as the popular software system GAP [3]), since the early 1980s, the *polynomial-time theory of permutation groups* has flourished, with its mathematical elegance and depth, as an important research area of its own (cf. [7]).

An important open question concerning GI is to determine its relative complexity against the graph-automorphism problem (GA), i.e., the decision problem of testing whether or not a given graph has a nontrivial automorphism. Both GI and GA share many important similarities, but there are also some indications to suggest that the problems are unlikely to be equivalent (cf. [4]). As with GI, GA has not been known to be in P. Whereas GA has been shown be $\leq_m^p$-reducible to GI in [5], for the reverse direction, GI has not been even known to be $\leq_T^p$-reducible, i.e., Turing reducible in polynomial time, to GA.

In the polynomial-time theory of permutation groups, as GI is generalized to C-INT, GA is similarly generalized to

Problem 2. Group intersection (G-INT).
Instance: $G, H \leq \mathrm{Sym}(\Omega)$.
Question: *Is* $G \cap H \neq 1$*?*

It is easy to show that GA is $\leq_m^p$-reducible to G-INT, but, just like GI against C-INT, the converse is not known under any polynomial-time reducibility. As GI and C-INT share many common complexity-theoretic properties,[1] so do GA and G-INT (cf. [1], [4]). Indeed, such similarities suggest that the relative complexity between GI and GA appears to parallel that between C-INT and G-INT.

In this note, motivated by the importance of determining GI's relative complexity against GA, we pose and investigate the question of determining C-INT's relative complexity against G-INT. We report some new evidence to support this suggested parallelism. A paper that amplifies this note with complete proofs will appear elsewhere. The author wishes to acknowledge Professors Seinosuke Toda and Osamu Watanabe for their insightful comments and encouragement.

We will use the following standard notational conventions (cf. [7]).

Notation. Let $G \leq \mathrm{Sym}(\Omega)$. For $g \in G$, we denote the images of $\alpha \in \Omega$ and $\Delta \subseteq \Omega$ under g by α^g and Δ^g, respectively. For $\alpha \in \Omega$, the *point stabilizer of* α *in* G is the subgroup $G_\alpha := \{g \in G \mid \alpha^g = \alpha\}$. For $\Delta \subseteq \Omega$, the *point-wise stabilizer of* Δ *in* G is the subgroup $G_\Delta := \{g \in G \mid \delta^g = \delta \text{ for all } \delta \in \Delta\}$, whereas the *subset stabilizer of* Δ *in* G is the subgroup $\mathrm{Stab}_G(\Delta) := \{g \in G \mid \Delta^g = \Delta\}$.

We throughout assume that $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ with a linear ordering $<$ such that $\alpha_1 < \cdots < \alpha_n$. This ordering naturally induces a lexicographic ordering $\prec$ on $\mathrm{Sym}(\Omega)$: for distinct $x, y \in \mathrm{Sym}(\Omega)$, we define $x \prec y$ if $\alpha^x < \alpha^y$ for the least $\alpha \in \Omega$ such that $\alpha^x \neq \alpha^y$. If $\Delta_i := \{\alpha_1, \ldots, \alpha_{i-1}\}$ for an integer $i \leq n$, then we write $G^{(i)} := G_{\Delta_i}$ (in particular, $G^{(1)} = G$ and $G^{(n)} = 1$).

[1] In particular, as GI is $\leq_T^p$-equivalent to the problem of finding generators for automorphism groups of graphs, C-INT is $\leq_T^p$-equivalent to the problem of finding generators for intersections of permutation groups (cf. [4], [7]).

1. Elementary Properties

To begin, we recall the following fundamental result of permutation-group manipulation obtained by means of the *Schreier–Sims* method (cf. [2], [10]).

Lemma 1 (Sims, Furst–Hopcroft–Luks). *Given* $G \leq \mathrm{Sym}(\Omega)$*, in polynomial time one can find a series of point-wise stabilizers* $G = G^{(1)} \geq \cdots \geq G^{(n)} = 1$ *and, for* $i = 1, \ldots, n-1$*, complete sets of right coset representatives for* $G^{(i+1)}$ *in* $G^{(i)}$.

We first observe the following basic relationship.

Theorem 2. G-INT $\leq_m^p$ C-INT.

The proof of this theorem appeals to Lemma 1 and the fact that C-INT has a polynomial-time *or*-function. Since *or*-functions and *and*-functions may be of independent interest, we summarize below what we currently know about C-INT and G-INT with respect to such functions.

Let Σ be an alphabet, $A \subseteq \Sigma^*$ and m be an integer ≥ 2. An *or*-function for A is a map $f : (\Sigma^*)^m \to \Sigma^*$ such that, for any $x_1, \ldots, x_m \in \Sigma^*$, $f(x_1, \ldots, x_m) \in A$ if and only if at least one of the x_i's belongs to A. An *and*-function for A is defined analogously. If A has a polynomial-time *or*/*and*-function, then, for given $B \subseteq \Sigma^*$, to assert that $B \leq_m^p A$, it is sufficient to prove that B is $\leq_{dtt}^p/\leq_{ctt}^p$-reducible, i.e., disjunctive/conjunctive truth-table reducible in polynomial time, to A (cf. [4]).

In [5], Lozano and Torán have constructed both polynomial-time *or*-function and *and*-function for GI and a polynomial-time *or*-function for GA. Using direct products of groups, we generalize these properties of GI and GA in

Proposition 3. C-INT *has polynomial-time or-function and and-function, whereas* G-INT *has a polynomial-time or-function.*

Whether there is an *and*-function for GA is an open question. Similarly, it is not known whether there is an *and*-function for G-INT.

2. An Asymmetric Property and Reductions to Sparse Sets

Our main result concerns the complexities of C-INT and G-INT with respect to the notions of left and right sets introduced by Ogiwara and Watanabe in [9]. Such sets are particularly known for their "totally ordered self-reducible structures" and play critical rôles in their work to generalize the following fundamental theorem of Mahaney: P $\neq$ NP *if and only if no sparse set is* NP*-complete under* $\leq_m^p$*-reducibility* [8]; here, a *sparse* set is a set of low information content in which the number of strings of length n is polynomially bounded in n (cf. [4]).

For an alphabet Σ, assume a lexicographic ordering $<$ on Σ^*. Recall that, for $L \in$ NP and a polynomial p, a *p-witness set* for L is $A \in$ P such that, for all $x \in \Sigma^*$, $x \in L$ if and only if there is $w \in \Sigma^{p(|x|)}$ such that $x\#w \in A$. The *left set* of a p-witness set A, denoted by $\mathrm{Left}(A, p)$, is the set of all strings $x\#y$ for $x \in \Sigma^*$ and $y \in \Sigma^{p(|x|)}$ such that there is $w \in \Sigma^{p(|x|)}$ for which $y \leq w$ and $x\#w \in A$. The *right set* of such A, denoted by $\mathrm{Right}(A,p)$, is defined analogously with respect to $\geq$ in place of $\leq$. Our main result is

Theorem 4. *There is a p-witness set A for* G-INT *such that* $\mathrm{Left}(A,p) \equiv_m^p$ C-INT *and* $\mathrm{Right}(A,p) \equiv_m^p$ G-INT.

This asymmetry then implies that, under the natural lexicographic ordering $\prec$ on $\mathrm{Sym}(\Omega)$ induced by the ordering $<$ on Ω, for given $G, H \leq \mathrm{Sym}(\Omega)$ for which $G \cap H \neq 1$, finding the least element $1 \neq a \in G \cap H$ is indeed likely to be easier than finding the largest element $1 \neq b \in G \cap H$; more precisely, we have

Corollary 5. *Given $G, H \leq \mathrm{Sym}(\Omega)$ for which $G \cap H \neq 1$, the problem of finding the least element $1 \neq a \in G \cap H$ is $\leq_T^p$-equivalent to* G-INT*, whereas the problem of finding the largest element $1 \neq b \in G \cap H$ is $\leq_T^p$-equivalent to* C-INT.

Theorem 4 is an analogue of the asymmetric property Lozano and Torán have previously observed for GA against GI in [5]. We remark however that, as with GI, C-INT is $\leq_m^p$-equivalent to both the left and right sets of a p-witness set for C-INT.

The proof of Theorem 4 is a group-theoretic generalization of the method of Lozano and Torán, while retaining some combinatorial flavor.

To prepare for an outline of the proof, we first recall from [7, Proposition 4.4] that C-INT is in fact $\leq_m^p$-equivalent to

Problem 3. Subset transporter (TRANS).
Instance: $G \leq \mathrm{Sym}(\Omega)$ *and* $\Delta, \Gamma \subseteq \Omega$.
Question: *Is there any $g \in G$ such that $\Delta^g = \Gamma$?*

Inspired by this equivalence, we also see that G-INT is $\leq_m^p$-equivalent to

Problem 4. Subset stabilizer (STAB).
Instance: $G \leq \mathrm{Sym}(\Omega)$ *and* $\Delta \subseteq \Omega$.
Question: *Is* $\mathrm{Stab}_G(\Delta) \neq 1$*?*

Next, to consider STAB with respect to a left set, we define

Problem 5. Left subset-stabilizer (L-STAB).
Instance: $G \leq \mathrm{Sym}(\Omega)$*,* $\Delta \subseteq \Omega$ *and* $x \in \mathrm{Sym}(\Omega)$.
Question: *Is there any $1 \neq a \in \mathrm{Stab}_G(\Delta)$ such that $x \preceq a$?*

We define its 'right' version, the right subset-stabilizer (R-STAB) problem, analogously with respect to $\succeq$ in place of $\preceq$.

Outline of the proof of Theorem 4. The theorem follows from the $\leq_m^p$-equivalences L-STAB $\equiv_m^p$ TRANS and R-STAB $\equiv_m^p$ STAB. In the following, we outline reductions to derive these equivalences.

First, for TRANS $\leq_m^p$ L-STAB, consider an instance (G, Δ, Γ) for TRANS. Let $\Omega' := \{\alpha_{n+1}, \ldots, \alpha_{2n}\}$ as a copy of $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ and $\bar{\Omega} := \Omega \cup \Omega'$, where, for $\alpha_i, \alpha_j \in \bar{\Omega}$, $\alpha_i < \alpha_j$ if $i < j$. Let t be the transposition in $\mathrm{Sym}(\bar{\Omega})$ such that ${\alpha_i}^t = \alpha_{i+n}$ for $i = 1, \ldots, n$ and ${\alpha_j}^t = \alpha_{j-n}$ for $j = n+1, \ldots, 2n$. Now, consider the natural action of the wreath product $\bar{G} := G \wr \langle t \rangle$ on $\bar{\Omega}$. If Γ' is the corresponding copy of Γ in Ω', then there is $g \in G$ such that $\Delta^g = \Gamma$ if and only if there is $\bar{a} \in \bar{G}$ such that $(\Delta \cup \Gamma')^{\bar{a}} = \Delta \cup \Gamma'$ and $t \preceq \bar{a}$. Thus, to decide if $(G, \Delta, \Gamma) \in$ TRANS, it is sufficient to query the instance $(\bar{G}, \Delta \cup \Gamma', t)$ to L-STAB.

For L-STAB $\leq_m^p$ TRANS, since C-INT has an *or*-function by Proposition 3, we only need to prove that L-STAB $\leq_{dtt}^p$ C-INT. Consider an instance (G, Δ, x) for L-STAB; here, we may assume that $x \notin \mathrm{Stab}_G(\Delta)$. For each pair $\alpha_i, \alpha_j \in \Omega$ such that $\alpha_j > (\alpha_i)^x$, we perform the following as a $\leq_{dtt}^p$-reduction: Use Lemma 1 to construct, if it exists, the coset $G^{(i+1)} g_{ij}$ consisting of all $g \in G$ such that

$$\alpha_1{}^g = \alpha_1{}^x, \ldots, \alpha_{i-1}{}^g = \alpha_{i-1}{}^x \text{ and } \alpha_i{}^g = \alpha_j. \tag{1}$$

Then query the instance $(G^{(i+1)} g_{ij}, \mathrm{Stab}_{\mathrm{Sym}(\Omega)}(\Delta))$ to C-INT.

We now outline the proof of R-STAB $\equiv_m^p$ STAB. Clearly, we have STAB $\leq_m^p$ R-STAB. Now, for R-STAB $\leq_m^p$ STAB, as before, since G-INT has an *or*-function, it is sufficient to prove that R-STAB $\leq_{dtt}^p$ STAB. Consider an instance (G, Δ, x) for R-STAB such that $x \notin \mathrm{Stab}_G(\Delta)$. For each pair $\alpha_i, \alpha_j \in \Omega$ such that $\alpha_j < (\alpha_i)^x$, we perform the following as a $\leq_{dtt}^p$-reduction: If x stabilizes $\alpha_1, \ldots, \alpha_{i-1}$ point wise and $\alpha_j = \alpha_i$, then query the instance $(G^{(i+1)}, \Delta)$ to STAB. Otherwise, construct as before, if it exists, the coset $G^{(i+1)} g_{ij}$ consisting of all $g \in G$ that satisfy (1) and consider the following Cases 1 and 2. In Case 1, for $G^{(i+1)} g_{ij}$, we construct an instance I for STAB so that

(i) if there is $a \in G^{(i+1)} g_{ij}$ such that $\Delta^a = \Delta$, then $I \in$ STAB, and
(ii) $I \in$ STAB only if there is $1 \neq a \in \mathrm{Stab}_G(\Delta)$ such that $a \prec x$.

In Case 2, we decompose $G^{(i+1)} g_{ij}$ into a union of subcosets and, for each such subcoset, construct an instance for STAB so that the conditions (i) and (ii) hold.

Case 1. *There are a pair* $\alpha_k, \alpha_\ell \in \Omega$ *such that* $\alpha_k < \alpha_\ell \leq \alpha_i$, $g_{ij} \in G^{(k)}$ *and* $\alpha_\ell{}^{g_{ij}} = \alpha_k$. Let Ω' be a copy of Ω and Δ' be the corresponding copy of Δ in Ω'. For a transposition $t := (1\,2)$ and $T := \langle t \rangle$, under the natural action of the wreath product $A_{i+1} := G^{(i+1)} \wr T$ on $\Omega \cup \Omega'$, query the instance $I := (A_{i+1}, \Delta \cup \Delta'^{g_{ij}{}^{-1}})$ to STAB.

Case 2. *There are no pair in* Ω *that satisfy the condition of Case* 1. We reduce this case disjunctively to $n - i$ instances to which the method of Case 1 is applicable. Let k be the integer $\leq i$ such that $g_{ij} \in G^{(k)}$ but $g_{ij} \notin G^{(k+1)}$. For $\ell = i+1, \ldots, n$, we find, if it exists, $h_{\ell k} \in G^{(i+1)} g_{ij}$ such that $\alpha_\ell{}^{h_{\ell k}} = \alpha_k$ and apply the method of Case 1 for the subcoset $G_{\alpha_\ell}^{(i+1)} h_{\ell k}$ in place of $G^{(i+1)} g_{ij}$. □

In complexity theory, sparse sets are of great importance because the $\leq_T^p$-closure of sparse sets is known to be equal to the class of sets with polynomial-size circuits and thus the class P/poly—the class of sets decidable in polynomial time with the help of *short advice* (see, e.g., [4]). We now recall that $\overline{\text{C-INT}}$ has been shown to have a 2-round interactive proof and thus belong to NP/poly (cf. [1]). It is then natural to ask if C-INT and G-INT could belong to P/poly; that is, we ask if these problems could be polynomial-time reducible to sparse sets. By Ogiwara and Watanabe's generalization of Mahaney's theorem [9, Theorem 3.1], we have

Corollary 6. *For* $L = \text{C-INT}, \text{G-INT}$*, unless* $L \in \mathrm{P}$*,* L *is not* $\leq_m^p$*-reducible to any sparse set.*

We remark that, technically, the Ogiwara–Watanabe theorem applies to $\leq_{btt}^p$-reducibility, i.e., polynomial-time bounded truth-table reducibility, whose strength is between those of $\leq_m^p$-reducibility and $\leq_T^p$-reducibility (cf. [9]). Thus, Corollary 6 may also be generalized as follows: *For* $L = \text{C-INT}, \text{G-INT}$*, unless* $L \in \mathrm{P}$*,* L *is not* $\leq_{btt}^p$*-reducible to any sparse set.*

References

[1] L. Babai and S. Moran, *Arthur–Merlin games: a randomized proof system and a hierarchy of complexity classes*, J. Comput. System Sci. **36** (1988), 254–276.

[2] M. Furst, J. Hopcroft and E. Luks, *Polynomial-time algorithms for permutation groups*, 21st Annual Symposium on Foundations of Computer Science, Syracuse, N.Y., Oct. 13–15, 1980, IEEE Comput. Soc. Press, Washington, D.C., 1980, pp. 36–41.

[3] The GAP Group, GAP—*Groups, Algorithms and Programming*, version 4.4, Centre for Interdisciplinary Research in Computational Algebra, School of Mathematics and Statistics, University of St Andrews, St Andrews, 2006.

[4] J. Köbler, U. Schöning and J. Torán, *The graph isomorphism problem: its structural complexity*, Progr. Theoret. Comput. Sci., Birkhäuser, Boston, 1993.

[5] A. Lozano and J. Torán, *On the nonuniform complexity of the graph isomorphism problem*, Complexity Theory: Current Research (K. Ambos-Spies, S. Homer and U. Schöning, eds.), Cambridge Univ. Press, Cambridge, 1993, pp. 245–271.

[6] E. M. Luks, *Isomorphism of graphs of bounded valence can be tested in polynomial time*, J. Comput. System Sci. **25** (1982), 42–65.

[7] ———, *Permutation groups and polynomial-time computation*, Groups and Computation, Piscataway, N.J., Oct. 7–10, 1991 (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, R.I., 1993, pp. 139–175.

[8] S. Mahaney, *Sparse complete sets for* NP: *solution of a conjecture of Berman and Hartmanis*, J. Comput. System Sci. **25** (1982), 130–143.

[9] M. Ogiwara and O. Watanabe, *On polynomial-time bounded truth-table reducibility of* NP *sets to sparse sets*, SIAM J. Comput. **20** (1991), 471–483.

[10] C. C. Sims, *Computational methods in the study of permutation groups*, Computational Problems in Abstract Algebra, Oxford, Aug. 29–Sept. 2, 1967 (J. Leech, ed.), Pergamon Press, Oxford, 1970, pp. 169–183.

Takunari Miyazaki
Computer Science Department
Trinity College
Hartford, Connecticut 06106-3100
U.S.A.
e-mail: takunari.miyazaki@trincoll.edu