Takunari Miyazaki

Research Summary

My general research area concerns the design and analysis of algebraic algorithms and computational complexity theory in an interdisciplinary subject of abstract algebra and computer science known as *computational algebra*. Overall, my projects have been on questions in *computational group theory*: a subject involving the examination of the computational complexity as well as practical tractability of problems in groups. With continuing international efforts, computational group theory is considered to be one of the oldest and most successful disciplines that have enjoyed exploring and fostering the interplay of modern mathematics and computer science (cf. [**16**]). Two computer algebra systems are particularly known for their rich libraries in groups: GAP [**5**] and Magma [**3**]; indeed, systems such as these have served as key tools for profound discoveries in combinatorics, group theory, as well as other parts of mathematics and science (cf. [**15**] and [**16**]).

Although there are numerous instances of applications, an important motivation for our research is relationship with the *graph-isomorphism* problem (ISO) in combinatorics: given two graphs, test whether or not they are isomorphic. The problem is of fundamental importance in theoretical computer science because of its as yet unresolved membership status in the complexity classes **P** and **NP**-complete. In practice, ISO is not particularly regarded to be difficult. For example, B. McKay's system *nauty* [**11**], available as part of both GAP and Magma, is widely known for its remarkable performance; yet, my work [**12**] has demonstrated that there are certain difficult instances. Graph-isomorphism algorithms have found many important applications in a wide range of areas exhibiting symmetries, including networks, boolean circuits, coding theory, constraint-satisfaction problems, and chemistry (cf. [**4**], [**6**], and [**9**]).

Around 1980, E. M. Luks investigated ISO and formalized several group-theoretic problems that possess similar complexity-theoretic characteristics as ISO [**7**]. Using groups of *permutations*, he then introduced a novel divide-and-conquer paradigm to solve ISO in polynomial-time for graphs with bounded vertex degrees. For general graphs, his algorithm also offers the fastest time presently known.

In computational situations, a group G is specified by a generating set S of its elements (that is, a subset $S \subset G$ such that every element of G is a word in elements of S). Critical to our group-theoretic approach to ISO is a generalization in permutation groups known as the *set-stabilizer* problem (SET-STAB): given a permutation group G on a set Ω and a subset $\Delta \subset \Omega$, find the subgroup of G stabilizing Δ. By the Jordan–Hölder theorem, one of the oldest results in finite group theory, an arbitrary finite group G decomposes into a set of simple groups known as the *composition factors* of G. Finite *solvable groups* are the class of finite groups all of whose composition factors are abelian groups. More generally, for an integer constant $d > 0$, consider the class Γ_d: finite groups all of whose nonabelian composition factors lie in the symmetric group of permutations on d letters. A key observation here is that, for a graph X with vertex degrees at most $d+1$ and an edge e of X, the group of the automorphisms of X fixing e belongs to Γ_d. Indeed, Luks's main result is a polynomial-time algorithm for SET-STAB in Γ_d; thus, establishing the claim that ISO belongs to **P** for graphs with bounded vertex degrees.

Since then, advances of polynomial-time algorithms for permutation groups have been remarkable. For a permutation group G, problems classified in **P** include testing *membership* of an arbitrary permutation in G; finding $|G|$, the composition factors of G. Particularly impressive are a large library of practical implementations based on these asymptotically efficient algorithms (cf. [**5**]). Essentially all of these algorithms have their roots in the pioneering techniques of C. C. Sims proposed earlier in the late sixties [**18**].

My first paper [**12**] investigates ISO from a practical viewpoint with theoretical questions. In particular, the study focuses on the underlying backtrack algorithms of the system *nauty*. Although *nauty* is believed to perform remarkably well in general, it is shown that there is an infinite family of pairs of cubic graphs, constructed deterministically, that admits an elementary version of Luks's polynomial-time algorithm but drives such backtrack methods to provable exponential-time complexity. In permutation groups, implemented procedures to solve important problems such as SET-STAB also rely on similar backtrack methods using both combinatorial and group-theoretic heuristics. There are still many questions to be answered concerning their intrinsic complexity and how these algorithms can be improved.

In many areas of mathematics and science, *matrices* are considered to be more natural and desirable objects for group representation; indeed, matrix representations have played prominent rôles in fundamental disciplines such as finite group theory, harmonic analysis, and quantum physics and chemistry (see, e.g., [**17**]). My Ph.D. dissertation investigates polynomial-time computation in matrix groups [**13**]. Of particular interest are matrix-group problems that generalize the fundamental problems ISO and SET-STAB. The main results are instances where the problems admit polynomial-time solutions and methods that enable such efficiency.

In matrix groups, there are two important generalizations of SET-STAB. For a matrix group G on a vector space V over a finite field k, the *vector-stabilizer* problem (VEC-STAB) asks: given a vector $v \in V$, find the subgroup of G stabilizing v; more generally, the *subspace-stabilizer* problem (SUBSP-STAB) asks: given a subspace $W \subset V$, find the subgroup of G stabilizing W.

As in permutation groups, a critical foundation is the ability to perform testing membership of an element in a group. Unfortunately, in matrix groups, the membership-testing problem is unlikely to be in $\mathbf{P}$ since the problem already subsumes a version of the well-known *discrete-logarithm* problem (from this point of view, membership-testing is often regarded as a multidimensional version of the discrete-logarithm problem). Nevertheless, in solvable matrix groups, assuming a polynomial bound on the primes in $|G|$ not dividing $|k|$, Luks has found polynomial-time solutions for membership-testing, finding $|G|$ and the composition factors of G, and also for the problems VEC-STAB and SUBSP-STAB [**8**].

Motivated by the fundamental results on SET-STAB in permutation groups, my dissertation work generalizes Luks's matrix-group algorithms from solvable groups to the important class Γ_d. In fact, assuming the same bound on these primes, it is shown that, in polynomial time, one can perform membership-testing and find $|G|$ and the composition factors of G, even in a broader class of matrix groups than those in Γ_d: matrix groups all of whose nonabelian composition factors have polynomially bounded orders. Furthermore, assuming a polynomial bound on the primes in $|G|$ and $|k|$, it is then shown that, via a divide-and-conquer paradigm, in polynomial time one can solve VEC-STAB and SUBSP-STAB in Γ_d. These polynomial-time algorithms exploit recent results in finite group theory such as [**1**]. My dissertation results will appear in articles [**10**] and [**14**].

In solvable groups, there are also significant connections between SUBSP-STAB and another entirely different generalization of SET-STAB in permutation groups. The goal of my current project is to generalize such connections with the class Γ_d. Furthermore, there are fundamental questions to be answered concerning VEC-STAB and SUBSP-STAB in the context of structural complexity theory as well.

Finally, I am interested in studying a variety of computational problems involving abstract algebra in other disciplines. As I have listed above, group-theoretic algorithms have offered insights and found applications in many areas. This is also true in the area of information security: various cryptographic protocols have been proposed under the assumption that certain group-theoretic problems are intractable (see, e.g., [**2**]). As one of my career objectives, I am interested in integrating my foundations on algebraic algorithms into such applied areas in innovative ways.

References

1. L. Babai, P. J. Cameron, and P. P. Pálfy, *On the orders of primitive groups with restricted nonabelian composition factors*, J. Algebra **79** (1982), 161–168.
2. G. Brassard, C. Crépeau, and M. Yung, *Constant-round perfect zero-knowledge computationally convincing protocols*, Theoret. Comput. Sci. **84** (1991), 23–52.
3. J. J. Cannon and C. Playoust, *An introduction to algebraic programming in* Magma, School of Mathematics and Statistics, University of Sydney, Sydney, 1996.
4. J. Crawford, M. Ginsberg, E. Luks, and A. Roy, *Symmetry-breaking predicates for search problems*, Proc. 5th Internat. Conf. on Principles of Knowledge Representation and Reasoning, Morgan Kaufmann, Palo Alto, Calif., 1996, pp. 148–159.
5. The GAP Group, GAP–*Groups, Algorithms, and Programming*, version 4.1, Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen; School of Mathematical and Computational Sciences, University of St Andrews, St Andrews, 1999.
6. R. Grund, R. Hager, F. Herrmann, A. Kerber, R. Laue, and W. Weber, *Groups, graphs and isomers*, Software Development in Chemistry 5 (J. Gmehling, ed.), Springer, Berlin, 1991, pp. 95–101.
7. E. M. Luks, *Isomorphism of graphs of bounded valence can be tested in polynomial time*, J. Comput. System Sci. **25** (1982), 42–65.
8. ———, *Computing in solvable matrix groups*, Proc. 33rd Annu. Sympos. on Foundations of Computer Science, IEEE Comput. Soc. Press, Los Alamitos, Calif., 1992, pp. 111–120.
9. ———, *Hypergraph isomorphism and structural equivalence of boolean functions*, Proc. 31st Annu. ACM Sympos. on Theory of Computing, ACM, New York, 1999, pp. 652–658.
10. E. M. Luks and T. Miyazaki, In preparation.
11. B. McKay, *nauty user's guide*, version 1.5, Tech. Rep. TR-CS-90-02, Computer Science Department, Australian National University, Canberra, 1990.
12. T. Miyazaki, *The complexity of McKay's canonical labeling algorithm*, Groups and Computation. II (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, R.I., 1997, pp. 239–256.
13. ———, *Polynomial-time computation in matrix groups*, Ph.D. dissertation, Tech. Rep. CIS-TR-99-11, Department of Computer and Information Science, University of Oregon, Eugene, 1999.
14. ———, *Deterministic algorithms for management of matrix groups*, submitted.
15. J. Neubüser, *Computing with groups and their character tables*, Phys. A **114A** (1982), 493–506.
16. Á. Seress, *An introduction to computational group theory*, Notices Amer. Math. Soc. **44** (1997), 671–679.
17. J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1971; English transl., *Linear representations of finite groups*, Graduate Texts in Math., vol. 42, Springer, New York, 1977.
18. C. C. Sims, *Computational methods in the study of permutation groups*, Computational Problems in Abstract Algebra (J. Leech, ed.), Pergamon Press, Oxford, 1970, pp. 169–183.