The following compilation of participant contributions is only intended as a lead-in to the AIM workshop “Generic Case Complexity.” This material is not for public distribution. Corrections and new material are welcomed and can be sent to workshops@aimath.org.

Table of Contents

A. Participant Contributions ................................................. 3
   1. Diekert, Volker
   2. Duncan, Andrew
   3. Elder, Murray
   4. Gurevich, Yuri
   5. Kahrobaei, Delaram
   6. Kambites, Mark
   7. Kapovich, Ilya
   8. Kharlampovich, Olga
   9. Miasnikov, Alexei
  10. Myasnikov, Alexey
  11. Riley, Tim
  12. Schupp, Paul
  13. Shpilrain, Vladimir
  14. Steinwandt, Rainer
  15. Teutsch, Jason
  16. Ventura, Enric
  17. Weidmann, Richard
  18. Wetzel, Susanne
A.1 Diekert, Volker

My background is algebraic number theory and theoretical computer science. I am interested in algorithmic questions for groups and monoids and other algebraic structures.

The interest in the workshop is to combine algebraic methods with methods from combinatorics on words, algorithms, and complexity theory.

Recent research contributions in this area concern Word Equations and are related to question to determine the borderline between decidability and undecidability of for the (existential) theory with (regular) constraints.

A word equation is a simple object: It is just a pair of words in constants and unknowns (also called variables). The pair is written as an equation and the question is whether or we can replace the unknowns with words over the constants such that the equation becomes an identity. In the positive case we say that the equation is solvable.

Word Equations is supposed to be an NP-complete problem, we have however a PSPACE upper bound, only No strategy is known to find hard instances in practice. At least I do not know of any.

The framework of generic case complexity might also lead to better understanding of Word Equations.

As an example: There is a simple strategy for solving word equations where every variable occurs at most twice, so called quadratic equations: The strategy is non-deterministic and can be described as follows. We guess which variables can be replaced by the empty word, these variables are canceled. After that we may assume that the equation is either of the form (where $x, y$ are variables and $a$ is a constant):

$$x \cdots = a$$

or

$$x \cdots = y \cdots$$

with $x \neq y$.

We may either write $x = az$ or, by symmetry, $x = yz$, where $z$ is a new variable. Replacing the occurrences of $x$ by $az$ or $yz$ respectively, we obtain a new equation where $x$ does not occur any more and $z$ occurs at most twice. On the left we may cancel either $a$ or $y$, and then $y$ also occurs at most twice. Hence we end up with something new, but where the number of variables is the same as before and every variable occurs at most twice. The length of the equation did not increase, but either the number of variables or the length of a minimal solution did decrease. Therefore the non-deterministic procedure will find a solution, if there is any. We can transform this in a deterministic back tracking algorithm. What is the generic time complexity of this algorithm?

Another recent interest of mine concerns non-archimedean words and non-standard Cayley graphs as introduced by Miasnikov et al.

A.2 Duncan, Andrew

I work mainly in combinatorial and geometric group theory and in particular on decision problems and algorithms. At present I’m specially interested in partially commutative groups and monoids and their algorithmic properties. Partially commutative groups are well known to mathematicians (as right-angled Artin groups) and partially commutative monoids are well known to computer scientists (as trace monoids) and in addition they seem an ideal
class in which to attempt to generalise the theory of free and/or abelian groups and/or monoids. It would be interesting at this workshop to discuss generic complexity of problems for such groups, monoids (and algebras) from the point of view, and with the expertise of, both computer scientists and mathematicians.

I am also interested in quantum computation and its implications for complexity theory and cryptography. I should like to find the appropriate framework for generic quantum complexity and to see how, if at all, this differs from classical generic complexity and from standard quantum complexity.

**A.3 Elder, Murray**

I have been working on the problem of computing which subgroups of Thompson’s group occur generically or with non-zero probability. Such problems seem to depend heavily of the choice of measure on the set of subgroups, the way you represent elements, and so on. I would like to see the development of a more robust definition of random subgroups and other things, if that is possible. And also keen to explore the other applications and results in generic complexity of things other than groups.

**A.4 Gurevich, Yuri**

The area of generic case complexity is a close relative of the area of zero-one laws in finite model theory. The difference is that, in finite model theory, the objects of interest, e.g. graphs, are finite and are represented by themselves. In the case of generic case complexity the objects of interests are infinite, e.g. groups, and only their representations are finite. For somebody who has been interested in zero-one laws for a long time, the twist is fascinating.

**A.5 Kahrobaei, Delaram**

Generic methods have proved useful in cryptanalysis of braid group cryptosystems. I am interested to see if I can apply these methods in cryptoanalysis of polycyclic groups.

**A.6 Kambites, Mark**

I am interested in many aspects of algebra, complexity and cryptography, but at present I am starting to look at (i) the development of a theory of generic-case complexity for algorithmic problems in semigroup theory and (ii) the possibility of using more general (than just groups) non-commutative semigroups as a basis for the development of cryptographic systems. I would like to discuss these possibilities with people who have expertise in cryptography (both group-theoretic and more general) and in generic case complexity methods in group theory.

**A.7 Kapovich, Ilya**

I am interested in generic-case complexity of various group-theoretic algorithms and in the algebraic properties of random group-theoretic objects (e.g. groups defined by “random” presentations, “random” group elements, etc). In particular, I am studying various rigidity properties of generic groups, such as Nielsen Uniqueness Property, isomorphism rigidity, estimating Delzant’s T-invariant, counting the number of isomorphism classes of groups in terms of their presentations, finite quotients and homology of random groups, and so on.
A.8 Kharlampovich, Olga

I would like to discuss the following topics:

1. Approaches to the construction of a group with generically undecidable word problem. Generic complexity of the word problem for modules and solvable groups.
2. Algorithmic problems for compressed words (straight line programs) in free groups and some other classes of groups (torsion free hyperbolic, fully residually free).
3. Complexity of solution of equations in free group and word equations (all the questions mentioned by V. Diekert).

A.9 Miasnikov, Alexei

I think it would be good if the following topics would be discussed:

1) Generic complexity and its relations to other complexity classes
2) Generic complexity and cryptography
3) Generic complexity of algorithmic problems in algebra:
4) Generic properties of algebraic objects: elements, subgroups, groups, morphisms.
5) Discussion on generic complexity of some particular algorithmic problems: Presburger Arithmetic, Grobner basis, equations in free groups, etc.

A.10 Myasnikov, Alexey

Generic complexity originated in combinatorial group theory and there was substantial progress made in recent years. However, generic complexity is still little known outside of the community. I would like to see more applications of generic complexity in traditional areas of computer science.

In particular I’m interested in applications of GC to cryptographic complexity including the theory of basic primitives and notions like one-way functions, computational indistinguishability and so on. Another area of interest, which may gain from generic complexity is analysis of heuristic search and optimization algorithms.

A.11 Riley, Tim

I work in Geometric Group Theory. Geometric points-of-view on algorithmic complexity are of particular interest to me. I study filling functions such as the Dehn (a.k.a. isoperimetric) function, the isodiametric function, the filling length function, as well as others that are less well-known. These concern the geometry of discs filling loops in spaces; in the setting of finitely presented groups the discs are van Kampen diagrams and the functions relate to the algorithmic complexity of the group’s word problem. Filling functions are usually defined as worst-case complexity measures. I would like to better understand their generic-case analogues and the applications these have in group-based cryptography.

Attempts have been made to use group-theoretic decision (and search) problems such as the word and conjugacy problems in cryptographic protocols. The geometry of the underlying group relates to the security of the protocol. I have some grasp on techniques for building finitely generated groups, particularly finitely presented groups in which van Kampen diagrams display prescribed geometric features. I am keen to tease concrete problems or wish-lists in this setting out of the generic-complexity and group-based-cryptography experts at the workshop.
**A.12 Schupp, Paul**

There is now an awareness that worst-case complexity may not give a good overall picture of the performance of an algorithm or the difficulty of a particular problem. As one of the originators of studying generic-case complexity, I continue to be interested in establishing new results and broadening the general approach. It now seems interesting to try to prove results about partial computability where the fraction of inputs for which a partial algorithm works tends to a positive limit \( \lambda \) where \( 0 < \lambda < 1 \).

There is a possibility that assumptions about the relationship between generic and worst-case complexity classes could be used to prove interesting results.

Let \( \mathcal{GP} \) denote the set of languages generically decidable in polynomial time. The statement \( \mathcal{NP} - \mathcal{GP} \neq \emptyset \) says that there are languages in \( \mathcal{NP} \) which require nondeterminism on set of inputs which is non-negligible relative to any deterministic polynomial-time partial algorithm. Is this a good candidate for a reasonable assumption which is stronger than \( \mathcal{NP} \neq \mathcal{P} \)?

**A.13 Shpilrain, Vladimir**

Bridging mathematics and cryptography is a major challenge these days. Because of the lack of new ideas in theoretical cryptography in the last several years, the whole area of cryptography is now drifting away from theoretical problems toward more practical ones which are of lesser interest to mathematicians.

The situation is further complicated by the fact that cryptographers frequently use the language which is too frivolous from a mathematician’s point of view. The most notorious example is using the euphemism “security proof” in place of “security evidence”; a somewhat less frequently used euphemism is “principle” in place of “assumption”. Since the language of mathematics tends to be more precise, this broadens the gap between mathematics and cryptography by creating a “language barrier”. Other elements of this language barrier include abbreviations which are, for some reason, very popular among cryptographers: CBC, HFE, DDH, DLP, MD, AES, IND, PKI - you name it!

In view of these unfortunate tendencies, I think that complexity theory may be an area providing a missing ground for a dialog between mathematicians and cryptographers. In particular, estimating (generic case) complexity of various algorithmic problems can provide an evidence (a “proof” in cryptographic lingo) of security of relevant cryptographic primitives. At the same time, study of generic case complexity opens many exciting research avenues in mathematics. Therefore, I believe this workshop should be beneficial to mathematicians and cryptographers (at least to those who are open to new ideas) as well as to complexity theorists.

**A.14 Steinwandt, Rainer**

A number of cryptographic proposals building on ideas from the theory of non-abelian groups have been made. After a number of cryptanalytic successes, however, it seems that the initial optimism has waned and that only few promising proposals remain.

I hope that this workshop helps in getting a clearer understanding of the cryptographic potential of non-abelian groups and of the concept of generic case complexity. So far the notion of generic case complexity is hardly encountered at major cryptographic research venues, and I hope that this workshop can help in clarifying the situation.
A.15 Teutsch, Jason

I have spent considerable time studying worst-case complexity, and I’m curious to learn about new complexity measures, especially as they relate to computability theory. The following question from the workshop webpage especially interests me:

Several hard problems e.g., the halting problem for Turing machines with semi-infinite tape, are generically easy. How general is this phenomenon? Find some decision problems which are not generically easy.

I’d like to see open problem and meet some new collaborators. I’m also interested to find connections with cryptography. For example, the set of Kolmogorov random strings are a natural instance of a “generic set,” as almost all finite strings are random. For this reason, it is natural to ask what Kolmogorov complexity has to say about generic-case complexity. Perhaps my dissertation work on shortest programs, which are generalized random strings, will be relevant here.

A.16 Ventura, Enric

My work is in the area of combinatorial and geometric group theory, specially about several aspects of free groups. Many problems about free groups have an interesting algorithmic component, which is usually the one I find more fascinating. With the irruption in the scene of the modern concept of “generic case complexity”, these algorithmic questions become even more interesting than before both, because of their intrinsic meaning within group theory itself, and because of possible applications to cryptography.

As an example, I can mention my recent work about the first part of the (very classical) Whitehead algorithm. The worst case complexity of the classical solution is clearly linear in the length, and exponential in the ambient rank. Although recent computer experiments pointed out that in practice it is much faster, the worst case complexity of the problem seemed to be genuinely exponential. However, we proved (joint work with P. Weil and A. Roig) that a surprisingly simple modification of the classical Whitehead algorithm (making use of the also classical Max Flow-Min Cut algorithm from computer science) turns out to be fully polynomial (in the worst-case sense). Is there an algebraic interpretation of “now”? Is there a similar result for the second part of Whitehead algorithm?

My recent contributions about genericity include: 1) “k-generated subgroups of a non-cyclic free group are strongly generically isomorphic to $F_k$”, 2) ”among all homomorphisms from $F_r$ to $F_s$ those being injective are strongly generic, and those being onto are strongly negligible”, 3) “generic pairs of subgroups of $F_k$ have trivial intersection”.

A.17 Weidmann, Richard

My work is the area of combinatorial and geometric group theory, in particular splittings of groups. While much of my research is concerned with abstract decidability questions the complexity of the generic case is clearly an important issue.

A.18 Wetzel, Susanne

Through this workshop I expect to learn more about generic case complexity. By having mathematicians and cryptographers at the workshop I expect that the interaction and discussions will lead to new ideas in solving some of the open problems as well as help
us identify additional interesting open problems. I also expect this workshop to spur new research collaborations.