A Quick Update on the Open Problems in Blass-Gurevich-Shelah's article "On Polynomial Time Computations Over Unordered Structures"

Andreas Blass
Mathematics Department
University of Michigan

Yuri Gurevich
Microsoft Research

December 2005

The Blass-Gurevich-Shelah article in the title is [1]. The open problems are formulated in Section 7. They all are yes/no questions. There are two lists of open questions. The first list contains four open questions. And then there is a list of two additional open questions. Here we

- recall the six questions,
- review their current status, and
- use this opportunity to advertise a related open question by Benjamin Rossman.

This update is of December 2005. We presume that the reader is familiar with the article [1].

1 The Six Questions

1. Can a $\tilde{\text{C}}$PT+Card program distinguish between the (unpadded) Cai, Fürer, Immerman graphs $\mathfrak{G}^0_m$ and $\mathfrak{G}^1_m$ (as defined in Section 4) for all m?

2. Can isomorphism of 3-multipedes with shoes be decided by a $\tilde{\text{C}}$PT+Card program?

3. Can a $\tilde{\text{C}}$PT+Card program decide whether a given graph (not necessarily bipartite) admits a complete matching?

4. Can a $\tilde{\text{C}}$PT+Card program compute, up to sign, the determinant of an $I \times J$ matrix over a finite field (where $|I| = |J|$)?

5. If we add to $\tilde{\text{C}}$PT+Card the capacity to decide the existence of complete matchings in general graphs, can it then compute determinants over finite fields?

6. If we add to $\tilde{\text{C}}$PT+Card the capacity to compute determinants over finite fields, can it then decide the existence of complete matchings in general graphs?

2 Question 1

The first question has been answered positively.

Theorem 1 (Rossman) *The unpadded Cai-Fürer-Immerman graphs can be distinguished already in $\tilde{C}PT$ (and therefore in $\tilde{C}PT$+Card).*

It has been confirmed that the availability of hereditarily finite sets of arbitrarily high rank is essential.

Theorem 2 (Dawar & Richerby) *The Cai-Fürer-Immerman graphs cannot be distinguished in $\tilde{C}PT$+Card with any fixed bound on the set-theoretic rank of the sets used in HF(A).*

Both results are published in [3].

3 Questions 2, 3, 5 and 6

The second and third questions remain open. But the positive answer to the fourth question (see below) implies the positive answer to the fifth question and renders the fifth and sixth questions obsolete. The sixth question is equivalent to the third.

4 Questions 4

The fourth question was answered positively. The main part of the solution of the fourth problem is played by the well known Csanky algorithm [2] for computing the determinants of integer matrices in NC^2. Benjamin Rossman noticed that Csanky's algorithm is expressible in $\tilde{\mathrm{C}}$PT+Card.

In the rest of this section, we explain a $\tilde{\mathrm{C}}$PT+Card expressible algorithm that computes, up to sign, the determinant of any $I \times J$ matrix over any finite field F (where $|I| = |J|$). Note that Csanky's algorithm involves division by integers (up to the size of the matrix), so it seems, a priori, to work only in characteristic zero (or prime characteristics larger than the size of the matrix). Hence the need to "lift" to characteristic zero in the algorithm described below.

We start with the special case $J = I$. Let q be the order of F. If q is prime, use Csanky's algorithm over the integers and then reduce the result modulo q. Otherwise q is a power of a prime $p < q$, and F is the quotient $(\mathbb{Z}/p)[X]/(f(X))$ of the polynomial ring $(\mathbb{Z}/p)[X]$ in one variable X over the field of order p where $f(X)$ is the minimal polynomial of some primitive element of F. Construct a polynomial $g(X)$ over the integers whose reduction modulo p is $f(X)$. Csanky's algorithm works over the ring $R = \mathbb{Z}[X]/(g(X))$. F is the quotient of R over the ideal generated by p. Given a matrix over F whose determinant you want to compute, lift it to a matrix over R, and apply Csanky's algorithm to the lifted matrix. Then reduce the answer mod p to get back to F.

The general case reduces to the special case $J = I$. The idea of reduction is not new. It is the idea used to prove Theorem 36 in [1]. (The idea of the alternative proof of Theorem 36 pointed out in Remark 37 of [1] can be used as well.) Let A be a $\tilde{\text{C}}$PT+Card algorithm for computing the determinant of an H-square matrix for finite index set H, and let M be an $I \times J$ matrix. Although M^2 is not defined when $I \neq J$, $M \cdot M^t$ is defined, where the superscript t means transpose. Furthermore, $M \cdot M^t$ is an I-square matrix. Using the algorithm A, we can compute the determinant D of $M \cdot M^t$. The number D is the square of the determinant d of a matrix obtained from M by indexing its rows and columns with numbers $1, \ldots, |I|$.

Note that finding the square roots $\pm d$ of a field element D is a $\tilde{\text{C}}$PT operation relative to the size of the matrix plus the size of the field which is the input size in our case. (This issue was addressed in [1]; see Proposition 32 and the two paragraphs preceding it.) That completes the solution of the fourth problem.

5 A New Open Problem

Ben Rossman contributed another open problem:

Commutative Semigroup Subset Sum Given a commutative semigroup S e.g. in the form of the multiplication table and given a subset $X \subseteq S$ and an element $y \in S$, is y the sum of all elements of X?

We quote: "This is the most basic problem I can think of that appears difficult for $\tilde{\text{C}}$PT+Card but is obviously polynomial time. I don't even know the answer when S is an abelian group, or even a direct product of cyclic groups Z_2."

References

[1] Andreas Blass, Yuri Gurevich and Saharon Shelah, "On Polynomial Time Computations Over Unordered Structures", Journal of Symbolic Logic 67:3 (2002), 1093–1125.

[2] Laszlo Csanky, "Fast Parallel Matrix Inversion Algorithms", SIAM J. on Computing 5:4 (1976), 618–123.

[3] Anuj Dawar, David Richerby and Benjamin Rossman, "Choiceless Polynomial Time, Counting and the Cai-Furer-Immerman Graphs: Extended Abstract", Proceedings of WoLLIC 2005, the 12th Workshop on Logic, Language, Information and Computation in Florianópolis, Santa Catarina, Brazil, pages 13–24.