Electronic Colloquium on Computational Complexity, Comment 1 on Report No. 12 (1999)

Rather late in the day, we'd like to add a couple of comments regarding Theorem 16 in the report, which says that computing the number of paths in planar width-2 BPs is complete for NC^1 under ACC^0 (mod 5) reductions.

1. The Theorem in the report claims completeness, but as is clear from the proof, only hardness is established. In fact, as far as we know, whether paths in planar width 2 branching programs can be counted in Boolean NC^1 is still open.

2. The hardness proof as stated is flawed, but fixable. Here's the way the proof is stated.

   (a) The 2x2 integer matrices with determinant 1 mod 5, with the binary operation of matrix multiplication in Z_5, form a non-solvable group (commonly denoted SL(2,5)). So, by Barrington's result ([Bar89]), the word problem over this group is complete for NC^1.

   (b) By [Gur90] (FOCS 99 Thm 3.1), every matrix over non-negative integers with determinant 1 can be written as a product of a sequence of triangular matrices each either $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ or $L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. So the word problem over SL(2,5) reduces to the word problem over L and U. This product is a width-2 planar BP.

   (c) Hence every NC^1 language can be reduced to counting paths mod 5 in a width 2 planar BP.

   The flaw is in step (b). The matrices U and L have determinant 1 over the integers. Thus any product over U and L will have determinant 1 over the integers. It cannot produce a matrix with determinant, say, 6 or 11. But such matrices are present in SL(2,5). Using U, L, one cannot produce matrices like $\begin{pmatrix} 3 & 3 \\ 1 & 3 \end{pmatrix}$ or $\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$.

   So to use Gurevich's construction, one first needs to show that for every matrix M in SL(2,5), there is a matrix N with non-negative integers, with determinant 1 over integers, such that each entry of N is equivalent, modulo 5, to the corresponding entry in M. It turns out that this statement is indeed true, but it is not needed at all. Even Gurevich's construction is not needed. Just replace step (b) in the proof by the following:

   (b') Dickson's theorem for finite groups (see for instance [Gor68]) tells us that SL(2,5) is exactly the group generated by $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ and T. But the first matrix is just L^2, so L and T generate SL(2,5).

References

[Bar89] D.A. Barrington. Bounded-width polynomial size branching programs recognize exactly those languages in NC^1. *Journal of Computer and System Sciences*, 38:150–164, 1989.

[Gor68] D. Gorenstein. *Finite groups.* Harper and Row, New York, 1968.

[Gur90] Y. Gurevich. Matrix decomposition problem is complete for the average case. In *SFCS '90: Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, pages 802–811 vol.2, 1990.

ISSN 1433-8092