Completeness for Parity Problems*

Leslie G. Valiant

Division of Engineering and Applied Sciences, Harvard University
Cambridge, MA 02138, USA

Abstract. In this talk we shall review recent work on holographic algorithms and circuits. This work can be interpreted as offering formulations of the question of whether computations within such complexity classes as NP, $\oplus$P, BQP, or #P, can be efficiently computed classically using linear algebra. The central part of the theory is the consideration of gadgets that map simple combinatorial constraints into gates, assemblies of which can be evaluated efficiently using linear algebra. The combinatorial constraints that appear most fruitful to investigate are the simplest ones that correspond to problems complete in these complexity classes. With this motivation we shall in this note consider the parity class $\oplus$P for which our understanding of complete problems is particularly limited. For example, among the numerous search problems for which the existence of solutions can be determined in P and the counting problem is known to be #P-complete, the #P-completeness proof does not generally translate to a $\oplus$P-completeness proof. We observe that in one case it does, and enumerate several natural problems for which the complexity of parity is currently unresolved. We go on to consider two examples of NP-complete problems for which $\oplus$P-completeness can be proved but is not immediate: Hamiltonian circuits for planar degree three graphs, and satisfiability of read-twice Boolean formulae.

1 Introduction

The class $\oplus$P is the class of sets S such that there is a polynomial time nondeterministic Turing machine that on input $x \in S$ has an odd number of accepting computations, and on input x $\notin S$ has an even number of accepting computations ([V79], [PZ83], [GP86]). It formalizes the question of the parity of the number of solutions to combinatorial problems. It is known that $\oplus$P has at least the computational power of NP, since NP is reducible to $\oplus$P via (one-sided) randomized reduction [VV86]. Also, the polynomial hierarchy is reducible to it via two sided randomized reductions [TO92]. The class FewP of sets for which there exist NP machines with few accepting computations is a subclass of it [CH90]. Further, there exist decision problems, such as graph isomorphism, that are not known to be in P but are known to be in $\oplus$P [AK02]. The class $\oplus$P has been related to other complexity classes via relativization [BBF98].

* This research was supported in part by grants NSF-CCR-03-10882, NSF-CCR-98-77049, and NSF-CCF-04-27129.

L. Wang (Ed.): COCOON 2005, LNCS 3595, pp. 1–8, 2005.

2 Some Easily Computed Parity Problems

There are several problems for which counting the number of solutions is #P-complete while computing the parity, i.e. whether there is an odd or even number of solutions, is polynomial time computable. The prime example is that of perfect matchings in bipartite graphs where exact counting corresponds to computing the permanent of a 0/1 matrix. The parity problem corresponds to computing the permanent modulo two, which is the same as the determinant modulo two, and is therefore computable in polynomial time via linear algebra computations. Many variants of this matching problem, such as those in which the matchings need not be perfect, or the graph bipartite, also have polynomially computable parity problems for similar reasons.

A further category of problems with polynomially computable parity is that of *read-twice formulae*. These are formulae where each variable occurs at most twice. In particular, we consider formulae that are *conjunctive* in the sense that they consist of conjunctions of clauses that each depend on at most three variables. In [V02] it is shown, by parity preserving reductions to matchings, that the parity of such read-twice formulae can be computed in P provided the clauses are (any mixture) of the following forms: a clause dependent on at most two variables, or a clause of any of the forms $xyz, x(y=z), x'yz+xy'z+xyz', x(y+z), x \oplus y \oplus z = 1, xy+yz+zx, x+(y=z), xy+(y=z)$, where each of these forms also allows any of x, y, z to be replaced by their negations x', y', or z'. (We note that with respect to the existence of solutions, a complete analysis of the relative expressivity of read-twice formulae composed of any one of these forms can be found in [CB05]).

Remarkably, there are a large number of natural parity problems for which we currently have no hint as to their complexity. In particular, almost any #P-complete problem for which existence of solutions is known to be in P, but not via matchings, is a potential such open problem. The following are notable examples:

(i) $\oplus$2SAT - the parity of the number of solutions of 2-CNF formulae.
(ii) The parity of the number of solutions of read-twice monotone formulae.
(iii) The parity of the number of solutions of read-twice 3-CNF formulae.

All three are open even if the formulae is restricted to be planar, and (ii) and (iii) are open if the formulae are not restricted to be read-twice.

3 Some $\oplus$P-Complete Problems

One can define $\oplus$P-completeness with respect to various reductions. In this paper we shall use the term in the sense of polynomial time many-one (Karp) reductions.

We first consider NP search problems for which the existence of solutions can be decided in polynomial time. There are numerous NP search problems for which the existence of solutions can be determined in P but counting their