

Are There Interactive Protocols for Co-NP Languages?

Lance Fortnow*
Michael Sipser†
MIT Math Dept.‡
Cambridge, MA 02139

Keywords: Interactive Protocol, co-NP, Oracle

1 Introduction

An interactive protocol, as described in [7], is a game between two players, a infinitely powerful prover and a probabilistic polynomial time verifier. The prover and verifier have a conversation and then the verifier either accepts or rejects. A language L has an interactive protocol when the prover can convince the verifier to accept a string x if and only if x is in the language L .

Goldreich, Micali and Wigderson show that graph non-isomorphism, a problem not known to be in NP, has an interactive protocol [6].

It is not known whether all problems in co-NP have interactive protocols. We conjecture that co-NP-complete problems do not have interactive protocols. However, a proof of such a statement would imply several well known unproven complexity conjectures such as $P \neq NP$. This paper instead exhibits an oracle such that relative to this oracle there exists a language in co-NP that does not have an interactive protocol. From this we get that techniques which relativize will not settle our conjecture.

2 Definitions

Let P be an infinitely powerful Turing machine and V be a probabilistic polynomial time machine which share the same input tape and can communicate with each other. Formally, we think of P as being a function from the input and the conversation so far to a message. We put no restrictions on the complexity of this function other than that the lengths of the messages produced by this function must be bounded by a polynomial in the size of the input.

P and V form an interactive protocol for a language L if:

1. If $x \in L$ then $\Pr(P \text{ and } V \text{ on } x \text{ accept}) \geq \frac{2}{3}$.
2. If $x \notin L$ then for all provers P^* , $\Pr(P^* \text{ and } V \text{ on } x \text{ accept}) \leq \frac{1}{3}$.

IP is the class of all languages which have interactive protocols.

A *round* of an interactive protocol is a message from the verifier to the prover followed by a message from the prover to the verifier. In general, interactive protocols can have a polynomial number of rounds.

From [8] we can assume that all the verifier's messages are independent coin tosses of the same length at each round.

We can enumerate all possible polynomial time verifiers in the standard manner, letting V_i be bounded in time by n^i , where n is the size of the input.

*supported by an Office of Naval Research fellowship

†supported by NSF Grant DCR-8602062 and Air Force Grant AFOSR-86-0078

‡This work was done while both authors were at the University of California at Berkeley.

3 Main Theorem

Theorem 1 *There exists an oracle A and a language $L \in \text{co-NP}^A$ such that $L \notin \text{IP}^A$.*

Proof For any oracle A , let

$$L(A) = \{1^n : A \text{ contains all strings of length } n\}$$

It is clear that $L(A) \in \text{co-NP}^A$ for all oracles A .

We will create the oracle A in stages. In each stage we look at some finite set of strings. For each string in this set, we decide whether to include or exclude this string from A . In stage i , we choose the set of strings so that $L(A)$ does not have an interactive protocol with verifier V_i . Thus after the construction, $L(A)$ can not have an interactive protocol and we have proved our theorem.

STAGE i :

Pick N_i large enough so $2^{N_i} > 3(N_i)^i$ and no oracle queries of length N_i have been asked in any previous step. Let $p_i = (N_i)^i$.

We will determine some strings of A such that either $1^{N_i} \in L(A)$ and no prover can convince V_i to accept 1^{N_i} or $1^{N_i} \notin L(A)$ but there is a prover that will cause V_i to accept.

Every time V_i makes an oracle query which hasn't been previously answered we answer yes. If there aren't any provers P such that P and V_i accept on input 1^{N_i} with probability at least $\frac{2}{3}$ then we put in the oracle A all strings of length N_i and every other previously unset string that V_i asks about for any prover. This completes step i . Note that V_i can only make queries of length less than p_i so we will always be able to find N_{i+1} in step $i+1$.

Otherwise we have some prover P such that P and V_i will accept 1^{N_i} with probability at least $\frac{2}{3}$. On any computation path (which is determined by V_i 's coin tosses), V_i can ask at most p_i oracle queries of length N_i . Since the same number of coin tosses are used at each round, the probability of each computation path is identical. There is some oracle query x of length N_i that appears in at most $p_i/2^{N_i}$ of the computation paths of V_i . By the way we chose N_i this means the oracle query x appears in less than one third of the computation paths of V_i . Put all strings of length N_i except for x in the oracle A . Also place in the oracle A every string queried by V_i on every possible communication with P . P will convince V_i to accept with probability greater than one third since more than a third of the computation paths are the same as before. So we are done with step i . \square

Corollary 1 *Techniques which relativize will not settle whether $\text{co-NP} \subseteq \text{IP}$.*

Proof Let B be the standard oracle which makes $\text{P}^B = \text{NP}^B$ [3]. Then $\text{co-NP}^B = \text{P}^B$, so $\text{co-NP}^B \subseteq \text{IP}^B$. Thus any proof that proves or disproves $\text{co-NP} \subseteq \text{IP}$ can not relativize. \square

4 Conclusions

This paper tries to understand the kinds of languages which can have interactive protocols. There have been some related results subsequent to this research.

AM is the class of languages which have one round interactive protocols where the verifier's message is just random coin tosses [2]. Goldwasser and Sipser [8] show that any language with a bounded round interactive protocol is in AM. Boppana, Hastad, and Zachos [4] show that if $\text{co-NP} \subseteq \text{AM}$ then the polynomial time hierarchy collapses to the second level.

Fortnow, Rompel and Sipser [5] have shown that Theorem 1 holds for multiple provers.

Towards the other direction of this paper, Aiello, Goldwasser and Hastad [1] exhibit an oracle where relativized to this oracle, IP is not even contained in the polynomial time hierarchy. AM has been shown to be in Π_2^P [2].

Open problems include trying to improve this result, showing perhaps a collapse of the polynomial time hierarchy if $\text{co-NP} \subseteq \text{IP}$. Also of interest are any other results which help us understand the complexity of interactive proof systems.

References

- [1] Aiello, W., S. Goldwasser and J. Hastad, “On the power of Interaction”, *Proc. 27th FOCS*, 1986, pp.368-379.
- [2] Babai, L., “Trading Group Theory for Randomness”, *Proc. 17th STOC*, 1985, pp. 421-429.
- [3] Baker, T., J. Gill and R. Solovay, “Relativizations of the $P = NP$ question”, *SIAM J. Comput.*, **4** (1975), 431-442.
- [4] Boppana, R., J. Hastad and S. Zachos, “Does co-NP Have Short Interactive Proofs?”, *IPL*, to appear.
- [5] Fortnow, L., J. Rompel and M. Sipser, “On the Power of Multi-Prover Interactive Protocols”, *Proc. 3rd Structure in Complexity Theory Conference*, 1988, to appear.
- [6] Goldreich, O., S. Micali and A. Wigderson, “Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design”, *Proc. 27th FOCS*, 1986, pp. 174-187.
- [7] Goldwasser, S., S. Micali and C. Rackoff, “The Knowledge Complexity of Interactive Proof-Systems”, *Proc. 17th STOC*, 1985, pp. 291-304.
- [8] Goldwasser, S. and M. Sipser, “Private Coins versus Public Coins in Interactive Proof Systems”. In S. Micali, editor, *Randomness and Computation*, Volume 5 of *Advances in Computing Research*, JAI Press, 1987. Extended Abstract available in *Proc. 18th STOC*, 1986, pp. 59-68.