Short Interactive Proofs

based on the papers

Does co-NP have short interactive proofs?
[Boppana, Håstad, Zachos; 1987] Information Processing Letters

Arthur-Merlin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes
[L. Babai, S. Moran; (1988)] J. of Computer and System Sciences

presentation by
Chrysida Galanaki

Arthur-Merlin games

MA

$L \in$ MA if there exists a polynomial-time deterministic TM M, polynomials p, q, s.t. $\forall$ string $x, |x| = n$

- if $x \in L$ then $\exists z \; Pr_y[M(x, y, z) = 1] \geq \frac{2}{3}$
- if $x \notin L$ then $\forall z \; Pr_y[M(x, y, z) = 0] \geq \frac{2}{3}$

where $z \in \{0, 1\}^{q(n)}$ and $y \in \{0, 1\}^{p(n)}$

AM

$L \in$ AM if there exists a polynomial-time deterministic TM M, polynomials p, q, s.t. $\forall$ string $x, |x| = n$

- if $x \in L$ then $Pr_y[\exists z M(x, y, z) = 1] \geq \frac{2}{3}$
- if $x \notin L$ then $Pr_y[\forall z M(x, y, z) = 0] \geq \frac{2}{3}$

where $z \in \{0, 1\}^{q(n)}$ and $y \in \{0, 1\}^{p(n)}$

Lemma

For every language L in AM *and every polynomial q, there is a language M in* NP *and a polynomial p such that, for all strings x, the fractions of strings y of length $p(|x|)$ that satisfy $x \circ y \in M$ is*

- *at least $1 - 2^{-q(|x|)}$ for x in L, and*
- *at most $2^{-q(|x|)}$ for x not in L,*

t(n) : polynomially bounded function of $n = |x|$

- AM($t(n)$) and MA($t(n)$) are the classes of languages accepted by Arthur-Merlin games of length $\leq t(n)$.
- AM($poly$) $=$ MA($poly$) $= \cup\{\mathrm{AM}(n^k) : k > 0\}$ form the Arthur-Merlin hierarchy.

- MA(1) $= M =$ NP
- AM(1) $= A =$ BPP
- AM(2) $=$ AM

In the quantifier notation

- $\mathsf{NP} = (\exists/\forall), \text{co-}\mathsf{NP} = (\forall/\exists)$
- $\mathsf{RP} = (\exists^+/\forall)$
- $\mathsf{BPP} = (\exists^+/\exists^+) = (\exists^+\forall/\forall\exists^+) = (\forall\exists^+/\exists^+\forall)$
- $\mathsf{MA} = (\exists\forall/\forall\exists^+) \subseteq (\forall\exists/\exists^+\forall) = \mathsf{AM}$
- $\Pi_2^p = (\forall\exists/\exists\forall)$

Theorem (Collapse Theorem [Babai])

For any polynomially bounded $t(n) \leq 2$*,*

$$\mathsf{AM}(t(n)) = \mathsf{AM}(t(n)+1) = \mathsf{MA}(t(n)+1)$$

for constant $k \geq 2$

$$\mathsf{AM} = \mathsf{AM}(k) = \mathsf{MA}(k+1)$$

$$\mathsf{NP} \cup \mathsf{BPP} \subseteq \mathsf{MA} \subseteq \mathsf{AM} \subseteq \mathsf{AM}(poly) \subseteq \mathsf{PSPACE}$$

Theorem (Speedup Theorem [Babai, Moran])

For any $t(n) \leq 2$*,*

$$\mathsf{AM}(2t(n)) = \mathsf{AM}(t(n))$$

for constant $k \geq 2$

$$\mathsf{AM} = \mathsf{AM}(k) = \mathsf{MA}(k+1)$$

An Arthur-Merlin game is an Interactive Proof system

$$\mathsf{AM}(t(n)) \subseteq \mathsf{IP}(t(n))$$

Goldwasser and Sipser showed that

$$\mathsf{IP}(t(n)) \subseteq \mathsf{AM}(t(n)+2)$$

By the Collapse Theorem we have

$$\mathsf{AM}(t(n)) = \mathsf{IP}(t(n))$$

Lemma

If co-NP *is contained in* AM, *then* co-AM *is contained in* AM.

Proof.

Suppose $(\forall/\exists) \subseteq (\forall\exists/\exists^{+}\forall)$ then

$$\text{co-AM} = (\exists^{+}\forall/\forall\exists) \subseteq (\exists^{+}\forall\exists/\forall\exists^{+}\forall) \subseteq (\forall\exists^{+}\exists/\exists^{+}\forall\forall) \subseteq (\forall\exists/\exists^{+}\forall) = \text{AM}$$

□

Theorem ([Boppana, Hastad, Zachos])

If co-NP *is contained in* AM, *then the polynomial-time hierarchy is contained in* AM $\subseteq \Pi_2^p$.

Proof.

$\Sigma_1^p = \mathrm{NP} \subseteq \mathrm{AM}$

Assume $\sum_k^p \subseteq (\forall\exists/\exists^+\forall)$ then

$$\Sigma_{k+1}^p \subseteq (\exists\exists^+\forall/\forall\forall\exists) \subseteq (\exists\forall\exists/\forall\exists^+\forall) \subseteq (\forall\exists\exists/\exists^+\forall\forall) = (\forall\exists/\exists^+\forall) = \mathrm{AM}$$

$\square$

Corollary ([Boppana, Hastad, Zachos])

If the Graph Isomorphism is NP*-complete, then the polynomial-time hierarchy is contained in* AM $\subseteq \Pi_2^p$.

Proof.

Suppose Graph Isomorphism is NP-complete.
Graph Isomorphism $\in$ co-AM (Goldreich, Micali, Wigderson).
Then NP $\subseteq$ co-AM. Equivalently co-NP $\subseteq$ AM.
The polynomial-time hierarchy collapses to AM. □

Theorem ([Babai, Moran])

Graph nonisomorphism belongs to AM.

Proof.

Consider only connected graphs. X, Y connected, Z their disjoint union.
#automorphisms: $X \to a$, $Y \to b$, $Z \to c$

1. X and Y isomorphic $\Rightarrow c = 2ab$
2. X and Y NOT isomorphic $\Rightarrow c = ab$

Check (2) with approx. lower bound for a, b and approx upper bound for c of $2^{1/3}$.

- Lower bounds exist in result of Theorem: $\forall L \in \mathrm{NP}$, $\forall \varepsilon > 0$, an ε-approximate lower bound protocol of class MA exists.
- Upper bound
  $d =$#(distinct isomorphic copies of Z of its n vertices) $= n!/c$
  So, we need a lower bound for d, that exists due to the Theorem.

Question

Is Graph Isomorphism NP-complete?

Graph Isomorphism $\in$ NP

If it is NP-complete then Graph Nonisomorphism is co-NP-complete.

And because Graph Nonisomorphism $\in$ AM, all co-NP-complete problems are in AM.

Then co-NP $\subseteq$ AM and NP $\subseteq$ co-AM.

So, Graph Isomorphism is unlikely to be NP-complete.

References

- L. Babai, S. Moran, Arthur-Merlin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes, J. of Computer and System Sciences, (1988)
- L. Babai, Trading Group Theory for Randomness, ACM SToC, (1985)
- R. Boppana, J. Hastad, S.Zachos, Does coNP have short interactive proofs?, Information Processing Letters, (1987)
- S. Goldwasser, M. Sipser, Private coins versus public coins in interactive proof systems, ACM SToC, (1986)