CS294: Probabilistically Checkable and Interactive Proofs January 26, 2017

Arthur-Merlin Games and the Goldwasser-Sipser protocol

Instructor: Alessandro Chiesa & Igor Shinkar *Scribe: Bryan O'Gorman*

1 Introduction

We begin with an interactive proof system for the Graph Non-Isomorphism (GNI) problem: given a pair of graphs (G_0, G_1), decide if they are *not* isomorphic.

Proof System 1 (IP for GNI) *The following is a private-coin, 2-round IP protocol for* GNI*, with perfect completeness and soundness* $1/2$*:*

- *The Verifier picks* $b \in \{0,1\}$ *and* $\pi \in S_n$ *uniformly, and sends* $\pi(G_b)$ *to the Prover.*
- *The Prover chooses* $\tilde{b} \in \{0,1\}$ *such that* $\Pi(G_b) \equiv G_{\tilde{b}}$*, and sends* $\tilde{b}$ *to the Verifier.*
- *The Verifier accepts if and only if* $\tilde{b} = b$*.*

If $G_0 \not\equiv G_1$, then the Prover can determine whether $\pi(G_b) \equiv G_0$ or $\pi(G_b) \equiv G_1$, and return $\tilde{b} = b$ accordingly. Otherwise, $\pi(G_b) \equiv G_0 \equiv G_1$, and the Prover can do no better (or worse) than guessing randomly: $\Pr[\text{ACCEPT}] = \Pr_{b,\pi}\left[\tilde{b} = b\right] = 1/2$. By repeating the protocol in parallel, the soundness can be arbitrarily amplified.

That the randomness (b, π) is hidden from the Prover is essential to the soundness of this protocol, which invites the following question: is there a *public-coin* IP protocol for GNI? After introducing the requisite foundation, we will show such a protocol at the end of lecture.

Theorem 2 GNI *has a public-coin interactive proof system with 2 rounds.*

2 Arthur-Merlin Protocols

IP protocols as introduced by Goldwasser and Sipser [GS86] generalize the Arthur-Merlin protocols previously introduced by Babai [Bab85]. In an Arthur-Merlin protocol, Arthur and Merlin take the roles of the Verifier and Prover, respectively, and Arthur's actions are limited either to rolling coins and sending the result to Merlin or to deciding to terminate by accepting or rejecting. In a general IP protocol, however, Arthur is allowed to keep the randomness private. Thus we have the following complexity classes.

Definition 3 *The class* $\text{AM}[k]$ *(resp.* $\text{MA}[k]$*) is the set of languages that have a public-coin,* k*-round interactive proof system in which the Verifier (resp. Prover) acts first.*

(Note that there is no material difference between the definition given here and Babai's original in which the Verifier is constrained to sending only the randomness to the Prover.) In fact, this Arthur-Merlin hierarchy almost completely collapses:

Theorem 4 *For all constant $k \geq 2$,* $\mathrm{AM}[2] = \mathrm{AM}[k] = \mathrm{MA}[k+1]$. *[Bab85]*

Corollary 5 $\mathrm{MA} \subset \mathrm{AM}$.

Therefore, we can unambiguously define $AM \triangleq AM[2]$. More generally, we have interactive proof systems with *private coins*:

Definition 6 *The class* $\mathrm{IP}[k]$ *is the set of languages that have a private-coin, k-round interactive proof system.*

There is another way of characterizing AM and MA that gives an interesting perspective into their difference.

Fact 7 *Let $V : (x, \pi, r) \mapsto \{0,1\}$ be the predicate indicating whether the Verifier accepts, where x is the instance, π is the proof sent by the Prover, and r is the randomness sampled by the Verifier. Then*

- $\mathrm{AM} = \left\{ L : \exists V \begin{cases} \Pr_r \left[\exists \pi V(x,\pi,r) = 1\right] > 2/3, & x \in L, \\ \Pr_r \left[\exists \pi V(x,\pi,r) = 1\right] < 1/3, & x \notin L \end{cases} \right\}$
- $\mathrm{MA} = \left\{ L : \exists V \begin{cases} \exists \pi \Pr_r \left[V(x,\pi,r) = 1\right] > 2/3, & x \in L, \\ \forall \pi \Pr_r \left[V(x,\pi,r) = 1\right] < 1/3, & x \notin L \end{cases} \right\}$

Note the distinction between whether or not the quantification of the proof is conditioned on the randomness or not; in this sense, one difference between AM and MA is whether or not the predicate V is deterministic or random, respectively.

2.1 Perfect completeness

Not only can we arbitrarily amplify completeness and soundness through parallel repetition, but it can be shown that any AM system can be modified so that it has perfect completeness.

Definition 8 *The class* $\mathrm{AM}_{c,s}$ *is the set of languages with 2-round Arthur-Merlin protocols with completeness c and soundness s.*

Fact 9 $\mathrm{AM}_{\frac{2}{3},\frac{1}{3}} \subset \mathrm{AM}_{1-2^{-n^2},2^{-n^2}}$ *and* $\mathrm{MA}_{\frac{2}{3},\frac{1}{3}} \subset \mathrm{MA}_{1-2^{-n^2},2^{-n^2}}$.

Theorem 10 $\mathrm{AM}_{\frac{2}{3},\frac{1}{3}} = \mathrm{AM}_{1,\frac{1}{2}} = \mathrm{AM}_{1,2^{-n}} = \mathrm{AM}$.

With this notation, we can state a more specific version of Theorem 2:

Theorem 11 $\exists 0 < s < c < 1$ *such that* $\mathrm{GNI} \in \mathrm{AM}_{c,s}$.

2.2 Public versus private coins

While we won't prove it here, we can make a much more general statement than Theorem 2: for every language L with a k-round IP system, L has a $k+2$ round *public-coin* IP system. More formally, we have the following theorem due to Goldwasser and Sipser [GS86]:

Theorem 12 $\forall k, \mathrm{IP}[k] \subset \mathrm{AM}[k+2]$

The main ideas of the proof of the above theorem are contained in the proof of Theorem 2. The essence of the proof is to reformulate the problem as one about the size of a certain set. Given a pair of graphs (G_0, G_1), let

$$S = \{(H, \pi) : \pi \in \mathrm{aut}(H) \wedge (H \equiv G_0 \vee H \equiv G_1)\}. \tag{1}$$

Then

$$|S| = \begin{cases} 2 \cdot n!, & G_0 \not\equiv G_1, \\ n!, & G_0 \equiv G_1. \end{cases} \tag{2}$$

Now, we would like an AM protocol that convinces the Verifier that $|S| = N$ and not $|S| = N/2$, where $N = 2 \cdot n!$. We can do so using hashing.

3 Hashing

We'll briefly introduce the relevent ideas from hashing that we'll need to construct the AM system for GNI.

Definition 13 *A family of functions* $\mathcal{H}_{m,k} = \left\{h : \{0,1\}^m \to \{0,1\}^k\right\}$, *where* $k < m$, *is called a* pairwise independent hash family *if for all* $x \neq x' \in \{0,1\}^m$ *and* $y, y' \in \{0,1\}^k$,

$$\Pr_{h \in \mathcal{H}_{m,k}}[h(x) = y \wedge h(x') = y'] = 2^{-2k}. \tag{3}$$

Lemma 14 *There exists a pairwise independent hash family* $\mathcal{H}_{m,k}$ *of size* 2^{2m}*; therefore, a function* $h \in \mathcal{H}_{m,k}$ *can be sampled using* $2m$ *bits.*

Proof: Let

$$\mathcal{H} = \left\{h_{a,b}(x) = a \cdot x + b \mod 2^k : a, b \in \mathbb{F}_{2^m}\right\}, \tag{4}$$

where multiplication is within the field $\mathbb{F}_{2^m}$. Fix $x \neq x' \in \{0,1\}^m$ and $y, y' \in \{0,1\}^k$. Then

$$\begin{aligned} \Pr_{h \in \mathcal{H}_{m,k}}[h(x) = y \wedge h(x') = y'] &= \Pr_{h \in \mathcal{H}_{m,k}}\left[\left(ax + b = y \mod 2^k\right) \wedge \left(ax' + b = y' \mod 2^k\right)\right] \\ &= \Pr_{h \in \mathcal{H}_{m,k}}\left[\left(a = (y - y')(x - x')^{-1} \mod 2^k\right) \wedge \left(b = y - ax \mod 2^k\right)\right] = 2^{-2k}. \end{aligned} \tag{5}$$

□

Going forward, we will assume $\mathcal{H}_{m,k}$ is as defined in Equation 4.

4 Goldwasser-Sipser Protocol

Now, we are prepared to complete our proof of Theorem 2, using a protocol due to Goldwasser and Sipser. The protocol is for the general problem of determining whether a set S is of size N or at most $N/2$. The only constraint on S is that membership therein can be efficiently determined given a witness. Specializing to the case when the set is as defined in Equation 1 gives the desired result for GNI.

Proof System 15 *Goldwasser-Sipser The following is a public-coin, 2-round IP (i.e. AM) protocol for determining whether the size of a set $S \subseteq \{0,1\}^m$ is N or at most $N/2$. First, choose a k such that $2^{k-2} \leq N \leq 2^{k-1}$, and let $p = N \cdot 2^{-k} \in [1/4, 1/2]$. S (implicitly), N, and k are known by both the Verifier and the Prover.*

- *The Verifier picks a random hash function $h_{a,b}$ from $\mathcal{H}_{m,k}$ by uniformly sampling $a, b \in \mathbb{F}_{2^m}$, as well as $y \in F_{2^k}$, then sends (a, b, y) to the Prover.*
- *The Prover finds an $x \in S$ such that $h(x) = y$, and sends this x together with a proof π of its membership in S back to the Verifier.*
- *The Verifier accepts iff the proof π certifies that $x \in S$.*

The following claim implies the completeness and soundness of the above protocol.

Claim 16
- *If $|S| = N$, then $\Pr_{h,y}[\exists x \in S : h(x) = y] \geq \frac{3}{4}\frac{|S|}{2^k} = \frac{3}{4}p$.*
- *If $|S| \leq N/2$, then $\Pr_{h,y}[\exists x \in S : h(x) = y] < \frac{|S|}{2^k} = \frac{p}{2}$.*

Proof: Let $S \subset \{0,1\}^m$ such that $|S| \leq 2^{k-1}$. Uniformly sample $h \in \mathcal{H}_{m,k}$ and $y \in \{0,1\}^k$. Then

$$\frac{3}{4}\frac{|S|}{2^k} \leq \Pr_{h,y}[\exists x \in S : h(x) = y] \leq \frac{|S|}{2^k}, \tag{6}$$

which immediately implies the claim. The upper bound is almost trivial; $|h(S)| \leq |S|$. To show the lower bound, fix y. Then

$$\begin{aligned}
\Pr_h[\exists x \in S : h(x) = y] &\geq \sum_{x \in S} \Pr_h[h(x) = y] - \sum_{x \neq x' \in S} \Pr_h[h(x) = y \wedge h(x') = y] \\
&= |S|\frac{1}{2^k} - \binom{S}{2} \cdot \frac{1}{2^{2k}} \\
&\geq \frac{|S|}{2^k} - \frac{1}{2}\left(\frac{|S|}{2^k}\right)^2 \\
&\geq \frac{|S|}{2^k} - \frac{1}{4}\frac{|S|}{2^k} = \frac{3}{4}\frac{|S|}{2^k}.
\end{aligned} \tag{7}$$

Because this holds for all y, the lower bound follows. □

The relationship between the public-coin Goldwasser-Sipser protocol for GNI and the private-coin one given at the beginning of lecture captures of the general proof that $\mathrm{IP}[k] \subset \mathrm{AM}[k+2]$. Consider S as the set of possible messages from the Verifier to the Prover. If the two graphs are isomorphic, then the message completely obscures the bit b that selects one of the graphs, while otherwise the message completely reveals it. Therefore, if the graphs are isomorphic then the mapping from the randomness to the message is 21, while otherwise it is 11. In the latter case, the set S of messages is twice as large.

References

[Bab85] László Babai, *Trading group theory for randomness*, Proceedings of the 17th Annual ACM Symposium on Theory of Computing, STOC '85, 1985, pp. 421–429.

[GS86] Shafi Goldwasser and Michael Sipser, *Private coins versus public coins in interactive proof systems*, Proceedings of the 18th Annual ACM Symposium on Theory of Computing, STOC '86, 1986, pp. 59–68.