Today

- Arthur-Merlin Proofs and Interactive Proofs.
- Classes: IP, AM and MA.

Resources and Complexity Classes

- Some resources to focus on.
  - Rounds of interaction
  - Verifier’s randomness: Public or private?
  - Error: one-sided vs. two-sided.
- Historically:
  - Public coins = Arthur-Merlin proofs
  - Private coins = interactive proofs.
- However ... Public coins = private coins (GMZ).
- Nowadays:
  - IP = class of all languages with poly-round interactive proofs.

Last time

- Saw an interactive proof (of chalk marks?).
- Extends to graph non-isomorphism, or any distinguishability property.
- Principal ingredients: interaction, randomness, secrecy.

- AM = class of languages with bounded round Arthur-Merlin proofs (specifically Arthur goes first, and Merlin second ... no third round!).
- MA = class of languages in which Merlin goes first, and Arthur second (so only advantage over NP is that this includes BPP).
Agenda for today

- Power of prover (IP in PSPACE)
- Goldwasser-Sipser protocol for approximate counting.
- Private coins, two-sided error = Public coins, one sided error.
- Sketch of AM[k] = AM.
- Next lecture onwards: IP = PSPACE.

The optimal prover

- Given a fixed verifier, what should a prover do?
- Can figure out what to do, optimally, by computing the following quantity:
- Given a history of interactions so far, what is the highest probability, over all provers, of the verifier accepting.
- Can compute this by induction on number of remaining rounds.
- Prover that does this is the optimal prover.

---

IP ⊆ PSPACE

Simple consequence of the explicit form of the optimal prover:

Proposition: IP ⊆ PSPACE.

Proof: Can compute “probability of acceptance by optimal responses” in PSPACE.

Round-preserving amplification

- Verifier can run $\ell$ iterations in parallel.
- Prover might as well be the $\ell$-wise direct product of optimal prover.
- Completeness/Soundness of new protocol = $\ell$th power of original protocol.
AM proof for approximate set size

Suppose $S \subseteq \{0,1\}^n$ has size either $|S| \geq \text{BIG} = 2^m$ or at most $\text{SMALL} = 2^m/100$, where e.g., $m = \sqrt{n}$. Further $x \in S$? can be determined by Arthur on its own.


Goldwasser-Sipser protocol

Claim: If $h$ is chosen from a nice p.w.i. family of hash functions, and $|S| \geq 2^m$, then for 2/3 of $y$’s, there exists $x \in S$ such that $h(x) = y$.

Claim: If $|S| \leq 2^m/100$, then no matter which $h$ we pick, at most $16/100 \leq 1/6$ for the $y$’s have $x \in S$ such that $h(x) = y$.

Goldwasser-Sipser protocol

Protocol: (reminiscent of Sipser-Lautemann)

- Merlin picks (random) hash function $h : \{0,1\}^n \rightarrow \{0,1\}^{m-4}$ and sends to verifier.

- Arthur picks $y \in \{0,1\}^{m-4}$ at random and sends to Merlin.

- Merlin responds with $x \in S$ such that $h(x) = y$.

IP[k] ⊆ AM[k]

Will only prove IP[1] ⊆ AM[O(1)]. Extension to general $k$ similar.

- Fix verifier with completeness 2/3, and soundness $1/poly$.

- Let $Q$ be set of possible questions.

- For $q \in Q$, let $S_q$ be set of random strings that lead to question $q$ being asked, where optimal prover leads to acceptance.

- Let $r$ be length of random strings.

- So either $\sum_{q \in Q} |S_q| \geq (2/3)2^r$.

- $\sum_{q \in Q} |S_q| \leq 1/poly(r)$. 
• For simplicity assume $|S_q| = 0$ or $2^l$ for every $q$.

• Will run two G-S protocols back to back.

• Will ask Merlin to prove $\#q$ such that $|S_q| = 2^l$ is at least $(2/3)2^{r-l}$.

• To do so, Merlin send $h$, Arthur queries with $y$ and Merlin sends $q \in Q$ such that $h(q) = y$.

• Arthur still needs to verify $|S_q| \geq 2^l$. Does this with another G-S protocol.

• Working out details .... get theorem.

One-sided error?

Can get one-sided error protocols using more ideas from Lautemann-Sipser (BPP in PH).
(Pick many hash functions; one of them always has a pre-image.)

Corollary: Can prove graph non-isomorphism without error or private coins! Can you come up with elementary protocol?

AM$[k] = AM$

Basic Idea:

• AM$[k] = BP \cdot \exists \ldots BP \cdot \exists \cdot P$.

• Can exchange $\exists \cdot BP$ for $BP \cdot \exists$ (as in Toda, Part 1, Step 2); and then collapse successive $BP$ and $\exists$.

Conclusion

At most three different classes:

• MA: Merlin speaks first and Arthur verifies claim probabilistically.

• AM: Arthur asks question at random and Merlin answer questions and then Arthur verifies (deterministically).

• IP: Number of rounds of interaction unbounded.