Simple Stochastic Games and Propositional Proof Systems

Toniann Pitassi
Joint work with Lei Huang

University of Toronto

Proof Complexity

A propositional proof system is a polynomial-time onto function $S : \{0,1\}^* \rightarrow UNSAT$

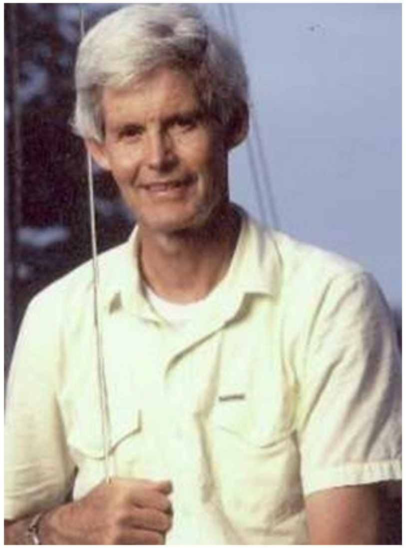
Intuitively, S maps (encodings of) proofs to (encodings of) unsatisfiable formulas.

S is polynomially bounded if for every unsatisfiable f, there exists a string (proof) a, $|a| = poly(|f|)$,
and $S(a)=f$.

Cook's Program

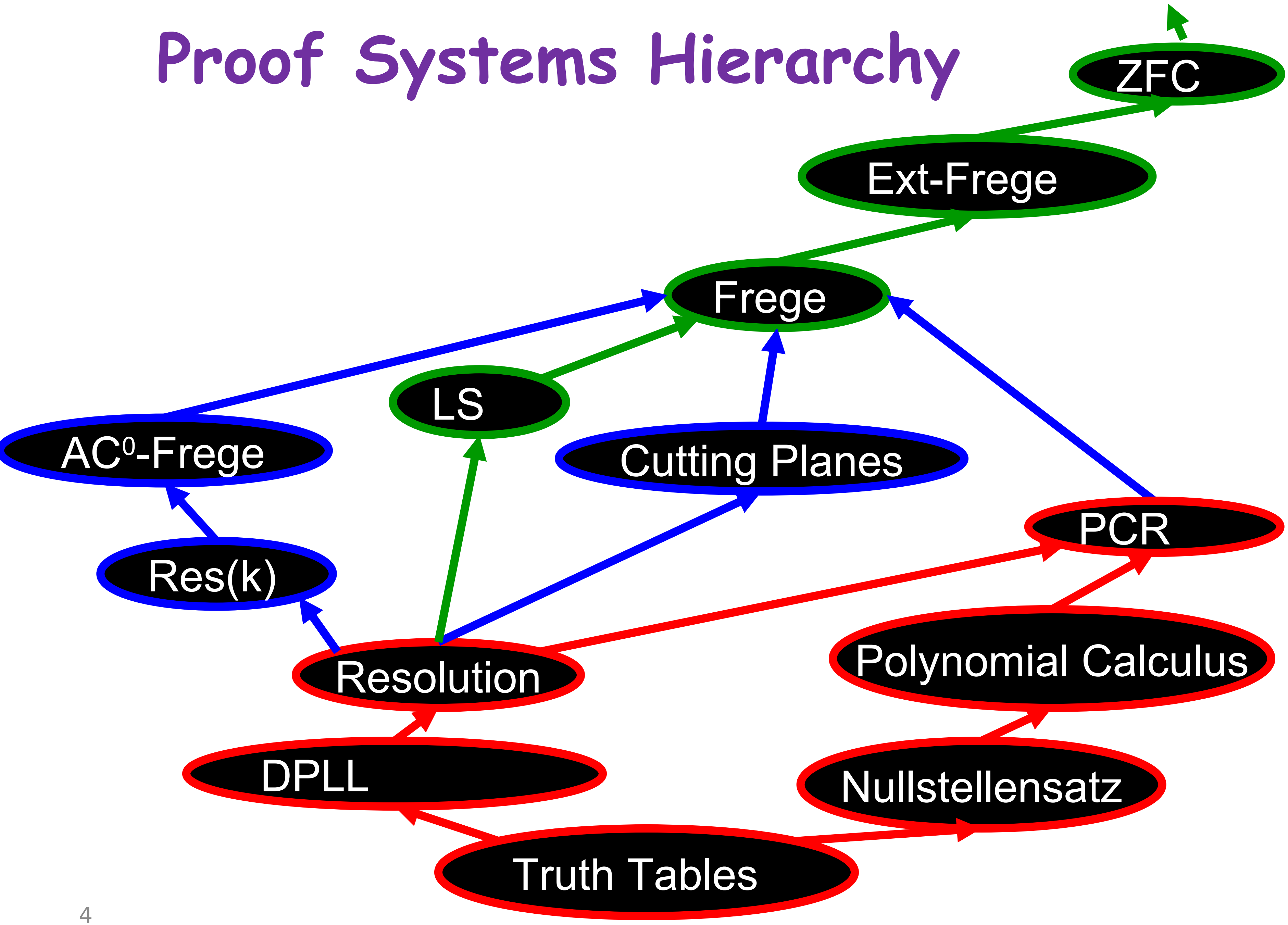
Theorem. [Cook, Reckhow]

NP = coNP iff there exists a polynomially bounded proof system.



Prove lower bounds for increasingly more powerful proof systems

Proof Systems Hierarchy



Main Lower Bound Tool: Feasible Interpolation

Main Idea: Associate a search problem, Search(f) with f. Show that a short refutation of f implies Search(f) is easy.

Interpolation statement: $f = A(p,q) \wedge B(p,r)$

Search(f)[α]: Given an assignment $p=\alpha$, determine if A or B is UNSAT.

Proof system S has (monotone) feasible interpolation if there is a (monotone) interpolant circuit for ($A \wedge B$) of size poly(size of the shortest S-proof of $A \wedge B$).

Feasible interpolation property implies superpolynomial lower bounds (for S).

Feasible Interpolation : Important interpolant formulas

Example 1. [Clique-coclique examples] Lower bounds for Res, CP

A(p,q) : q is a k-clique in graph p

B(p,r) : r is a (k-1)-coloring of graph p

Example 2. [Reflection principle for S] Complete formulas for S

A(p,q): q is a satisfying assignment for p

B(p,r) : r is a polysized S-proof of p

Example 3. [SAT $\not\subset$P/poly] Independence of lower bounds

A(p,q): q codes a polysized circuit for p

B(p,r): r codes a polysized circuit for $p\oplus$SAT

Feasible Interpolation and Automatizability

S is automatizable if there exists an algorithm A such that:
for all unsat f, A(f) returns an S-refutation of f, and
runtime of A(f) is poly in size of smallest S-refutation of f.

S is weakly automatizable if there exists a proof system that p-simulates S and that is automatizable.

Automatizability (for S) implies weak automatizability

Weakly automatizability (for S) implies feasible interpolation.

Limitations of Interpolation/Automatizability

Theorem [KP] If one-way functions exist then Extended Frege systems to not have feasible interpolation.

Theorem [BPR] If DH is hard, then any proof system that p-simulates TC_0-Frege does not have feasible interpolation.

Theorem AC_0(k)-Frege does not have feasible interpolation if DH cannot be solved in time $\exp(n^{2/k})$.

- Best alg for DH runs in time $\exp(n^{1/2})$; number field sieve conjectured to solve DH in time $\exp(n^{1/3})$.
- Thus feasible interpolation of AC_0(k)- Frege unresolved for $k<5$
- Even for Resolution, weak automatizability is unresolved.

  [AR]: Resolution not automatizable under FPT assumption.

Open Problem

- Are low depth Frege systems automatizable? Weakly automatizable?
- Problem is in NP intersect coNP
- No evidence one way or the other

Our Main Result

We connect automatizability/feasible interpolation to the complexity of simple stochastic games (SSG).

Theorem.

1. $AC_0(2)$-Frege+IGOP has feasible interp → SSG in P
2. $AC_0(3)$-Frege has feasible interpolation → SSG in P

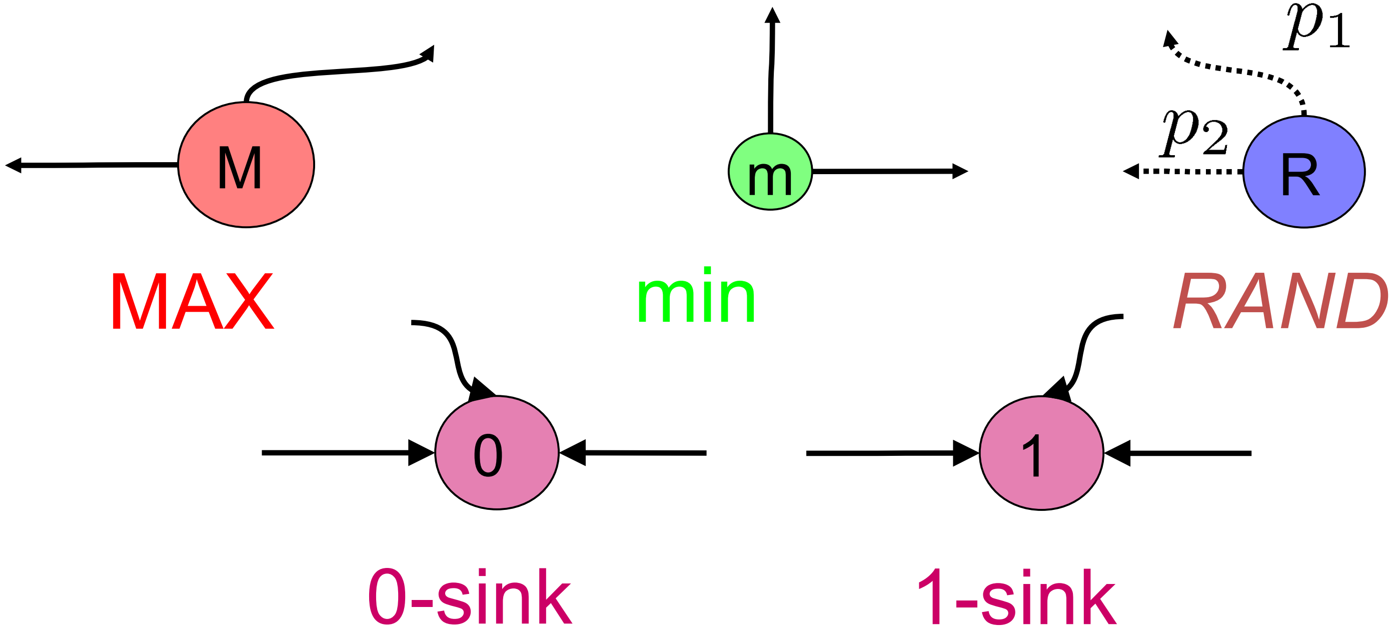
Theorem [Atserias, Menerva, 2010]

$AC_0(2)$- Frege automatizable → MPG (mean payoff games) in P.

$AC_0(3)$- Frege has feasible interpolation → MPG in P.

Our proofs are very different at a high level.

Simple Stochastic game (SSGs)
Reachability version [Condon (1992)]



No weights

All prob. are ½

Objective: Max / Min the prob. of getting to the 1-sink

Usually G is assumed to halt with probability 1

The SSG Problem

- Given a pair of strategies σ, τ -he value of a $v_{\sigma,\tau}(i) = P[\text{reach 1-sink under } \sigma, \tau]$
- Every $v(i) = \min_{\tau} \max_{\sigma} v_{\sigma,\tau}(i)$ ue.
- Values v(i) $(v(1), \ldots, v(n))$ are rational numbers requiring only n bits $\exists$
- **v** = is th $v(i)\ \forall i$ *ue vector* of G
- Theorem: pure positional strategies (for both Max and Min player) achieving
- **Is there a poly-time decision alg for**

The SSG Problem

Condon had it right:

[Anderson, BroMilterson]:

``SSG is polynomially equivalent to essentially all important 2-player zero sum perfect info stochastic games''

- Minimum stable circuit problem
- Generalized linear complementarity problem
- Stochastic parity games
- Stochastic mean payoff games

The SSG Problem

[Zwick] Other (non stochastic) games are polynomially reducible to SSGs:

- Mean payoff games
- Parity games

Mean Payoff Games:

Two player infinite game on a bipartite graph (V_1,V_2,E)

Edge (i,j) has payoff $w_{i,j}$

Player 1 tries to maximize average payoff

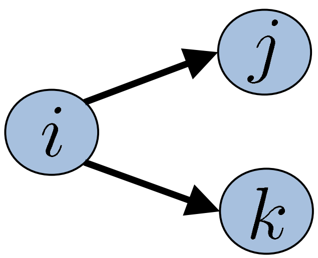
Previous Work

Complexity of SSG decision problem is unresolved:

- SSG decision problem is in NP$\cap$coNP [Condon 92]
  - Unlikely to be NP-complete
- SSG restricted to any two node types is in P [Derman72, Condon 92]
- The best known algorithms so far are
  - Poly($|V_{Rand}|!$) [Gimbert, Horn 09]
  - exp($\sqrt{n}$) [Ludwig 95]
- SSG is in both PLS and PPAD [Juba 05]
  - Unlikely to be a complete problem

The Complexity of SSGs: SSG in NP∩ coNP

Any game can be polynomially reduced to a stopping game where the values v_i of the vertices of the stopping game are the unique solution to the following equations:



$$v_i = \begin{cases} \max\{v_j, v_k\} & i \in V_{MAX} \\ \min\{v_j, v_k\} & i \in V_{min} \\ \frac{1}{2}(v_j + v_k) & i \in V_{RAND} \end{cases}$$

$$v_{0\text{-sink}} = 0 \qquad v_{1\text{-sink}} = 1$$

Note: Optimal solution is always stable (satisfies the above equations). For stopping games, stable solution is unique.

Corollary: Decision version in NP ∩ co-NP

SSG in PPAD

- Let G’ be stopping game for G
- Best strategy is fixed point for I(G’)
- Fixed point for I(G’) in PPAD via Brower fixed pt

SSG in PLS

- PLS graph where vertices are the strategies for max player
- Two strategies neighbors if they differ on one edge
- Local max equals global max
- Local improvement algorithm polytime if discount factor is constant; exponential-time in general

Our Main Result

We connect the automatizability/feasible interpolation question to the complexity of simple stochastic games

Theorem: depth-2 Frege + IGOP weakly automatizable (or has feasible interp) → SSG in P.

Remark: Since IGOP provable in depth-3 Frege, this implies depth-3 Frege weakly automatizable (or has feasible interpolation) → SSG in P.

Depth-3 Frege has feasible interpolation implies SSG in P

Given a game G, construct an equivalent stopping game, G′.

For G′, construct a formula F(G′) = A(G′,v) ∧ B(G′,w), where

A: v is a stable value vector for G′ with value > ½

B: w is a stable value vector for G′ with value <= ½

Main Lemma: F(G′) has a polysize depth-3 Frege proof.

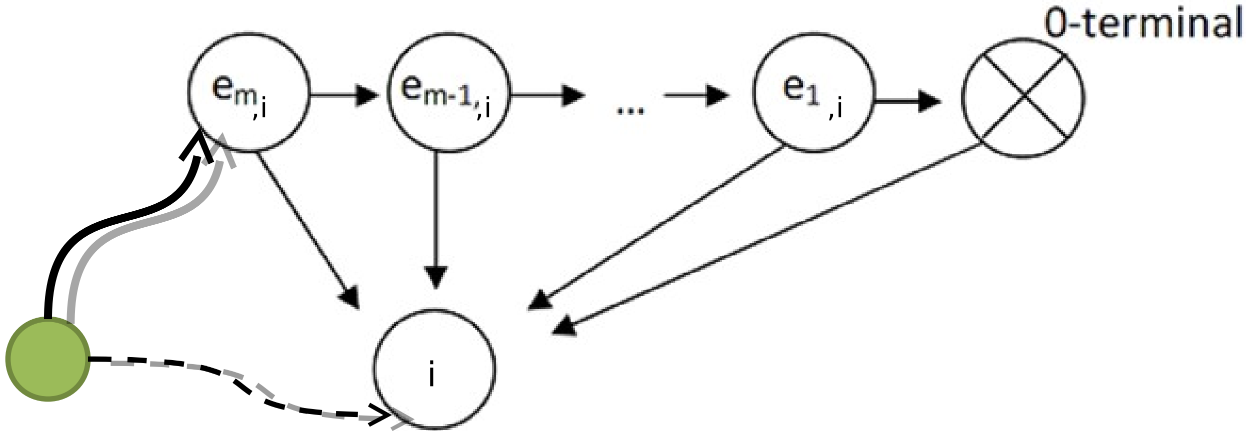
F(G′) has a polysize depth-2 Frege + IGOP proof.

Technical work is to prove uniqueness of stable value vector for stopping game G′, in low-depth Frege.

Corollary: If depth-3 Frege has feasible interpolation, then SSG in P.

Reduction and proof of Uniqueness for the Stopping Game

- For every G, there exists G' such that G' has exactly one stable solution

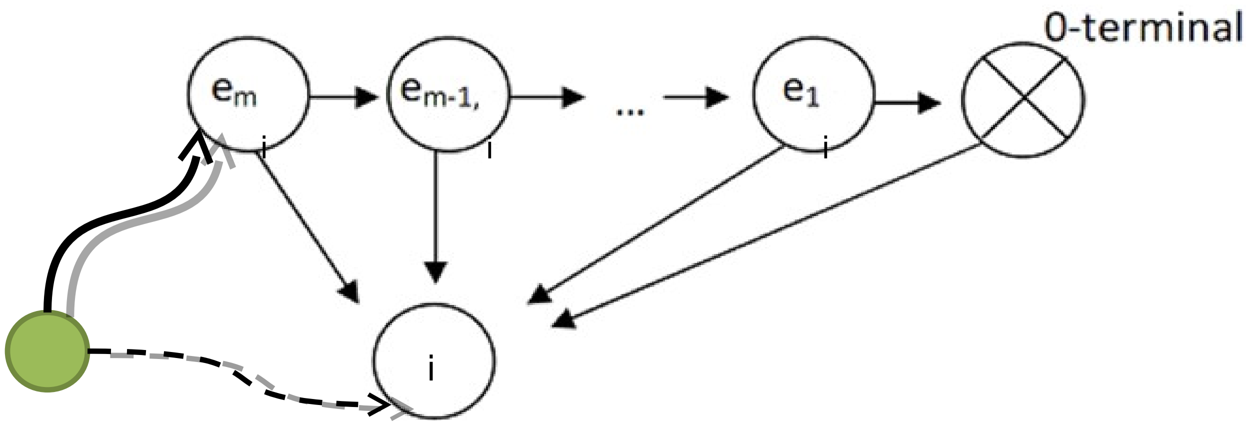


- Every edge into i is replaced by an edge into $e_{m,i}$

  $v(e_{m,i}) = (1 - 1/2^m)\, v(i)$

- G has value greater than ½ iff G' has value greater than ½.

Unique Solution – The Stopping Game



Lemma. For every G, G' has a unique stable solution

Main Idea: G' adds a discount factor: $v(e_{m,i}) = (1 - 1/2^m)\ v(i)$

Let v,w be two different stable value vectors, and let k be a node such that $\Delta(k) = |v(k)-w(k)|$ is locally maximal.

Case I: k is a max node, pointing to i and j.

Suppose $v(k)=v(e_{m,i})$, $w(k)=w(e_{m,i})$.

Since $v(e_{m,i}) = (1 - 1/2^m)\ v(i)$, $|v(k)-w(k)| = (1 - 1/2^m)\ |v(i) - w(i)|$

thus $|v(k)-w(k)|$ is not maximal.

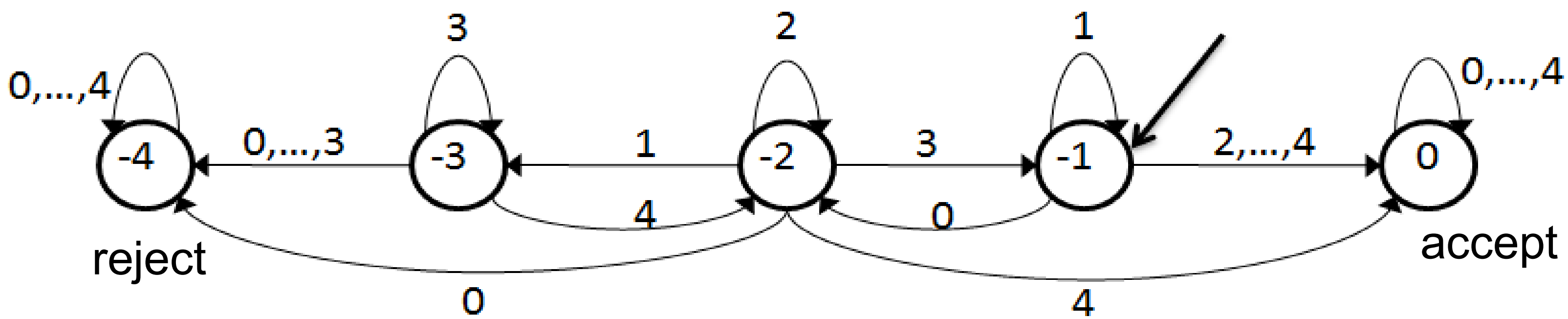
Main Lemma: Proving Uniqueness with depth-2 Frege proofs

For every stopping game *G'* we want to prove that *G'* has a unique stable solution

ie. $\mathbf{v}=I_G(\mathbf{v})$ and $\mathbf{x}=I_g(\mathbf{x})$-->$\mathbf{x}=\mathbf{v}$

- Recall x(i) are rationals of the form p/q where $q=O(2^n)$ [Condon 92] so we can represent x(i) with bit strings of length O(n)
- Simulate the stopping game proof using small depth circuits for addition/subtraction/comparison of integers

Depth 2 Addition Circuits [AM]



Let $x_1..x_n$ be the bitwise sum of k binary numbers

Example (k=4): x=10341234

State after p digits read represents a range of possible values for the partial sum

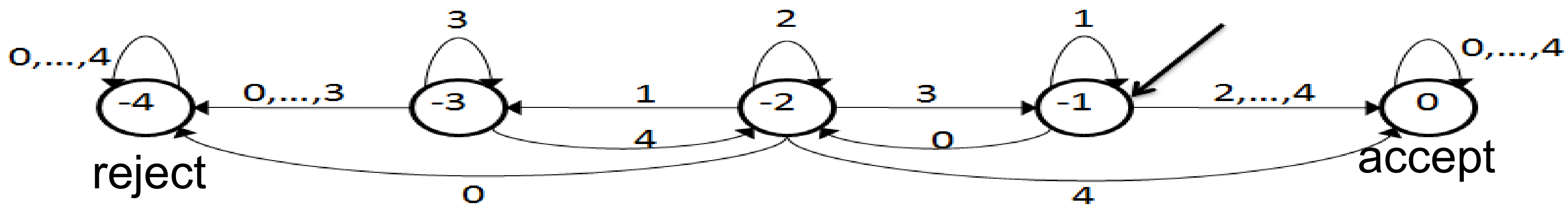
reject state: $[0, 2^p - k]$

accept state: $[2^p, k2^p]$

state -s: $2^p - s$

Finite state diagram, so only depends on a constant number of bits

Depth 2 Addition Circuits



A(i,x): true if we reach accept from i-1 to i

R(i,x): true if we reach reject from i-1 to i

A(i,x), R(i,x) depend only on a constant number of bits of x

C(x): true if an overflow bit is generated (there is some bit j where the circuit reaches accept and every bit from j to i does not reach reject)

$$\bigvee_{j \geq 1} \neg[A(1,x) \wedge A(2,x) \wedge .. \wedge A(j-1,x)] \wedge R(j,x)$$

C is a Δ_2^+ formula

IGOP: Integer-value Graph Ordering Principle

Let G be an undirected graph on n vertices, each vertex i labelled with an n-bit value value(i)

IGOP(G):

Each node of G is labelled by an n-bit integer value

IGOP(G) states that there exists a node i such that value(i) is greater than or equal to value(j) for all vertices j incident with i.

IGOP(G) expressible as a CNF formula in variables v(1), …, v(n), where $v(i)=v^1(i)\ldots v^n(i)$

IGOP: Integer-value Graph Ordering Principle

Fact: IGOP(G) has a depth-3 polysize Frege proof.

Idea: Prove that there exists a node i such that v(i) is maximal.

Open Problem: Does IGOP(G) have a polysize depth-2 Frege proof?

yes implies an improvement of our Main Theorem

no implies that SSGs are not reducible to MPGs.

Open Problems

- Our proof is very general; relies only on uniqueness of solution. Should also hold for the more general class of Shapley games.
- Does an efficient algorithm for SSGs imply feasible interpolation/automatizability of low-depth Frege?
- Prove that IGOP is not efficiently provable in depth-2 Frege.
- Is uniqueness of discount games depth-2 equivalent to IGOP?
- Study the relative complexity of proofs of totality for SSGs, MPGs, PLS, PPAD.

Thanks!