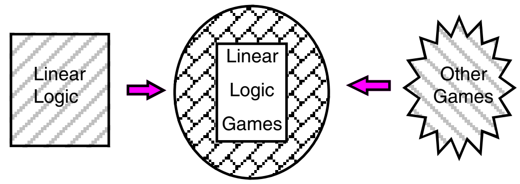
Proof Games and Probability

John Mitchell
joint work-in-progress with
P. Lincoln A. Scedrov

Larger study



Use concepts from complexity theory to study linear logic

Game Semantics

- Associate a game with each formula
- Valid iff player has winning strategy
- Compositionality:
  - » Connectives as constructions on games
- Why do this?
  - » Technical: implicit quantifier alternation
  - » Intuitive: explicit representation of context

Classical Prop. Logic (QBF)

- Players $\forall$, $\exists$

$$\forall x\ \exists y\ \forall z\ [\ (x \vee y \vee \neg z)\ \wedge$$
$$(\neg x \vee \neg y \vee z)\ \wedge\ \ldots\ ]$$

- Formula valid iff $\exists$ has winning strategy
- Think of three players: $\forall$, $\exists$, referee

Linear Logic

- Prior work by
  - » Blass, Abramsky and Jagadeesan and ...
  - » Hyland and Ong, Lamarche ...
- This talk:
  - » Specific games of bounded length
  - » Handle additives, no MIX-ing, ...
  - » Faithful to complexity results (w/o !. ?)
- Other work: approximation, score fctns

Proof Games

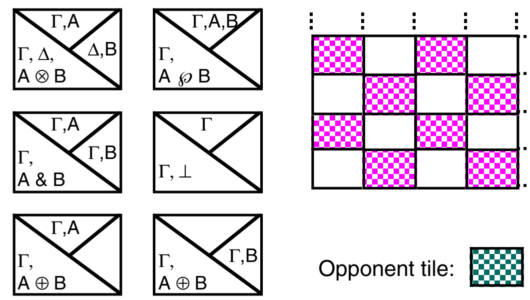
- Board
  - » infinite rectangular grid
- Prover tiles
  - » instances of proof rules
- Skeptic (opponent) tiles
  - » black squares that block prover
- Judge (referee) chooses winner at end

Several Related Games

- Solitaire
- Simple play with opponent
  - » Use opponent to shorten game
- Probabilistic opponent
  - » Simplify opponent's strategy

(same tiles and board)

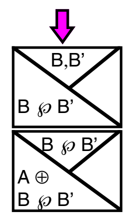
Board and tiles



Solitaire

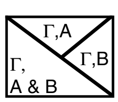
- Prover places tiles, from lower left
- Opponent goes out for coffee
- Referee scores
  - » win if all exposed sequents are axioms
- Winning strategy iff
  starting sequent is provable

A win at solitaire



Pros and Cons

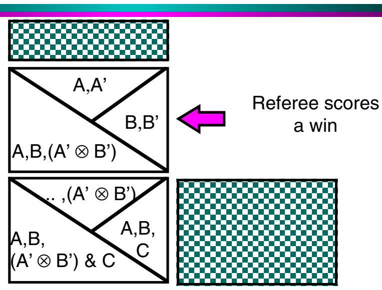
- Complete game interpretation of MALL
- Just a re-presentation of proof system
- Game is not much fun to play
- Long plays of game due to &
  - » want game linear in size of starting sequent



Second Form

- Player and opponent alternate
- Referee declares win/lose as before
- Shorter games
  - » Develop one branch of proof tree
- Winning strategy iff provable

Win on unprovable sequent

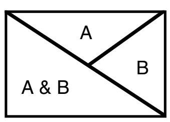


Pros and Cons

- Characterization of provability
- More like a game
- But players must be "smart"
  - » Winning strategy requires PSPACE
  - » Optimal opponent strategy also PSPACE (*approximate argument by symmetry*)
- If both players PSPACE, no point in playing

Complexity of Strategies

- Player's optimum strategy on A ⊕ B must decide which of A, B provable
- Opponents optimum strategy on



similarly must decide which unprovable

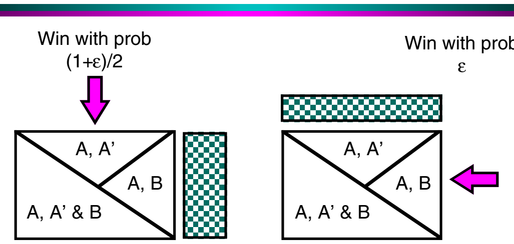
"Game Boy" Version

- Limited computational power
- Hours of in-flight entertainment
  - » probabilistic opponent, simple algorithm
  - » sometimes win on unprovable sequent
  - » sometimes lose on provable sequent
- Probabilistic characterization of provability

Randomized Opponent, Referee

- & rule is source of proof size
  - » Opponent flips a coin
- Other rules divide context
  - » Prover continues both branches
- Score "win" at $L_1, \ldots, L_k$ with
  - » probability $1/2 + \varepsilon/2$ if this is an axiom
  - » probability ε if *not* an axiom

Example play and scoring



- Win with probability $(1+\varepsilon)/4 + \varepsilon/2 = 1/4 + 3\varepsilon/4$

Why Randomized Referee ?

- Entire audience votes on yes/no question
  - US: Magna Carta before Battle of Hastings ?
  - UK: Is $\cup_k \mathrm{DSPACE}(\log^k n) \supseteq \cup_k \mathrm{DTIME}(n^k)$?
- Extra coffee break or banquet canceled
- Good voting strategy
  - If you know the answer, vote accordingly
  - If not, flip a coin

Characterization of Provability

- Strategy is *winning* if wins with prob >1/2
- Exists winning strategy against randomized opponent iff seq is provable
- Games are short, opponent and referee can be implemented as simple algorithms

Technical Problem

- Small bias away from 1/2
  - In voting analogy, depends on fraction who know the answer
  - For LL sequents, worst case $2^{-|\Gamma|}$
- Need high precision to estimate win
- Open problem: reformulate as IP game

FMU Course in Complexity

- NP: $x \in L \Leftrightarrow \exists y\, \exists z \ldots P(x,y,z,\ldots)$
- PSPACE: $x \in L \Leftrightarrow \forall y\, \exists z \ldots P(x,y,z,\ldots)$
- Games against nature
  $x \in L \Leftrightarrow$ ¶y $\exists z$ ¶w ... $P(x,y,z,\ldots) > 1/2$
- IP
  $x \in L \Rightarrow$ ¶y $\exists z$ ¶w ... $P(x,y,z,\ldots) > 3/4$
  $x \notin L \Rightarrow$ ¶y $\exists z$ ¶w ... $P(x,y,z,\ldots) < 1/4$
- Take P in Ptime or $\langle$ #coins, #queries $\rangle$

Alice and Bob

- Game on polynomial form
  $\prod_{x\in\{0,1\}} \sum_{y\in\{0,1\}} [(x+y) \cdot \prod_{z\in\{0,1\}} \ldots]$
- Alice tries to show value is not 0
- Computation mod prime p

Alice and Bob

- Form $a = \prod_{x\in\{0,1\}} \sum_{y\in\{0,1\}} [(x+y) \cdot \prod_{z\in\{0,1\}} \ldots]$
- Alice: $a = \prod_{x\in\{0,1\}} A(x) = 13$; $A(x) = 2x^2 + 8x + 6$
- Bob: *Check* $\prod_{x\in\{0,1\}} A(x) = 13$, *pick* $x \in \{0,\ldots,p\} = 9$
- Alice: $A(9) = \sum_{y\in\{0,1\}} B(y) = 6$; $B(y) = 2y^3 + y^2 + 3y$
- Bob: *Check* $\sum_{y\in\{0,1\}} B(y) = 6$, *pick* $y \in \{0,\ldots,p\} = 5$
- Repeat

Key ideas

- Generalize from {0,1} to N
- Instead of 0/1 tree traversal, explore general “surface”
- Q: How could we do this with LL ?

Conclusion and Open Problems

- Characterize LL by randomized games
- Want direct IP interpretation
  - » Logical presentation of complexity class?
- Other work: games with numeric score
  - » Hard to compute approximate score
- Relate to other game interpretations
  - » abstract vs. specific games
  - » infinite, deterministic vs. short, randomized