Formalizing Randomized Matching Algorithms

Stephen Cook

Joint work with Dai Tri Man Lê

Department of Computer Science
University of Toronto
Canada

The Banff Workshop on Proof Complexity 2011

Feasible reasoning with VPV

The VPV theory

- A universal theory based on Cook's theory *PV* ('75) associated with complexity class P (polytime)
- With symbols for all polytime functions and their defining axioms based on Cobham's Theorem ('65).
- Induction on polytime predicates: a derived result via binary search.
- Proposition translation: polynomial size extended Frege proofs

Feasible reasoning with VPV

The VPV theory

- A universal theory based on Cook's theory *PV* ('75) associated with complexity class P (polytime)
- With symbols for all polytime functions and their defining axioms based on Cobham's Theorem ('65).
- Induction on polytime predicates: a derived result via binary search.
- Proposition translation: polynomial size extended Frege proofs

- We are mainly interested in Π_2 (and Π_1) theorems $\forall X \exists Y \varphi(X, Y)$, where φ represents a polytime predicate.
- A proof in *VPV* is feasibly constructive: can extract a polytime function $F(X)$ and a correctness proof of $\forall X \varphi(X, F(X))$.
- Induction is restricted to polytime "concepts".

Feasible proofs

Polytime algorithms usually have feasible correctness proofs, e.g.,

- the "augmenting-path" algorithm: finding a maximum matching
- the Hungarian algorithm: finding a minimum-weight matching
- ...

(formalized in *VPV*, see the full version on our websites)

Feasible proofs

Polytime algorithms usually have feasible correctness proofs, e.g.,

- the "augmenting-path" algorithm: finding a maximum matching
- the Hungarian algorithm: finding a minimum-weight matching
- ...

(formalized in *VPV*, see the full version on our websites)

Main Question

How about randomized algorithms and probabilistic reasoning?

"Formalizing Randomized Matching Algorithms"

How about randomized algorithms?

Two fundamental randomized matching algorithms

1. RNC^2 algorithm for testing if a bipartite graph has a perfect matching (Lovász '79)
2. RNC^2 algorithm for finding a perfect matching of a bipartite graph (Mulmuley-Vazirani-Vazirani '87)

Recall that:

$$\boxed{\begin{array}{c}\text{Log-Space} \subseteq \mathsf{NC}^2 \subseteq \mathsf{P} \\ \mathsf{RNC}^2 \subseteq \mathsf{RP}\end{array}}$$

Remark

The two algorithms above also work for general undirected graphs, but we only consider bipartite graphs.

How about randomized algorithms?

Two fundamental randomized matching algorithms

1. RNC^2 algorithm for testing if a bipartite graph has a perfect matching (Lovász '79)
2. RNC^2 algorithm for finding a perfect matching of a bipartite graph (Mulmuley-Vazirani-Vazirani '87)

Recall that:

$$\boxed{\begin{array}{c}\text{Log-Space} \subseteq \mathsf{NC}^2 \subseteq \mathsf{P} \\ \mathsf{RNC}^2 \subseteq \mathsf{RP}\end{array}}$$

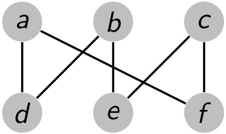
Remark

The two algorithms above also work for general undirected graphs, but we only consider bipartite graphs.

Lovász's Algorithm

Problem:

Given a bipartite graph G, decide if G has a perfect matching.



$$\begin{array}{c c} & \begin{array}{ccc} d & e & f \end{array} \\ \begin{array}{c} a \\ b \\ c \end{array} & \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \end{array} \xrightarrow[\text{distinct variables}]{\text{replace ones with}} M_G = \begin{bmatrix} x_{11} & 0 & x_{13} \\ x_{21} & x_{22} & 0 \\ 0 & x_{32} & x_{33} \end{bmatrix}$$

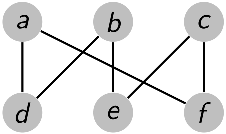
Edmonds' Theorem (provable in VPV)

G has a perfect matching if and only if $\mathrm{Det}(M_G)$ is not identically zero.

Lovász's Algorithm

Problem:

Given a bipartite graph G, decide if G has a perfect matching.



$$\begin{array}{c|ccc} & d & e & f \\ \hline a & 1 & 0 & 1 \\ b & 1 & 1 & 0 \\ c & 0 & 1 & 1 \end{array} \quad \xrightarrow{\text{replace ones with distinct variables}} \quad M_G = \begin{bmatrix} x_{11} & 0 & x_{13} \\ x_{21} & x_{22} & 0 \\ 0 & x_{32} & x_{33} \end{bmatrix}$$

Edmonds' Theorem (provable in VPV)

G has a perfect matching if and only if $\mathrm{Det}(M_G)$ is not identically zero.

The usual proof is not feasible since...

it uses the formula $\mathrm{Det}(A) = \sum_{\sigma \in S_n} (-1)^{\mathrm{sgn}(\sigma)} \prod_{i=1}^{n} A(i, \sigma(i))$, which has $n!$ terms.

Lovász's Algorithm

$$\begin{array}{cc} & \begin{array}{ccc} d & e & f \end{array} \\ \begin{array}{c} a \\ b \\ c \end{array} & \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \end{array} \xrightarrow{\text{replace ones with distinct variables}} M_G = \begin{bmatrix} x_{11} & 0 & x_{13} \\ x_{21} & x_{22} & 0 \\ 0 & x_{32} & x_{33} \end{bmatrix}$$

Edmonds' Theorem (provable in VPV)

G has a perfect matching if and only if $\mathrm{Det}(M_G)$ is not identically zero.

Lovász's Algorithm

$$\begin{array}{c|ccc} & d & e & f \\ a & 1 & 0 & 1 \\ b & 1 & 1 & 0 \\ c & 0 & 1 & 1 \end{array} \quad \xrightarrow{\text{replace ones with distinct variables}} \quad M_G = \begin{bmatrix} x_{11} & 0 & x_{13} \\ x_{21} & x_{22} & 0 \\ 0 & x_{32} & x_{33} \end{bmatrix}$$

Edmonds' Theorem (provable in VPV)

G has a perfect matching if and only if $\mathrm{Det}(M_G)$ is not identically zero.

Lovász's RNC^2 Algorithm

- Observation: instance of the polynomial identity testing problem
- $\mathrm{Det}(M_G^{n\times n})$ is a polynomial in n^2 variables x_{ij} with degree at most n.
  - $\mathrm{Det}(M_G^{n\times n})$ is called the *Edmonds' polynomial* of G.
- Pick n^2 random values r_{ij} from $S = \{0, \ldots, 2n\}$
  1. if $\mathrm{Det}(M_G) \equiv 0$, then $\mathrm{Det}(M_G)(\vec{r}) = 0$
  2. if $\mathrm{Det}(M_G) \not\equiv 0$, then $\Pr_{\vec{r}\in_R S^{n^2}}\left[\mathrm{Det}(M_G)(\vec{r}) \neq 0\right] \geq 1/2$
- (2) follows from the Schwartz-Zippel Lemma

Obstacle #1 - Talking about probability

- Given a polytime predicate $A(X, R)$,

$$\Pr_{R\in\{0,1\}^n}\left[A(X,R)\right] = \frac{|\{R \in \{0,1\}^n \mid A(X,R)\}|}{2^n}$$

- The function $F(X) := \left|\left\{R \in \{0,1\}^n \mid A(X,R)\right\}\right|$ is in #P.
- #P problems are generally harder than NP problems

Cardinality comparison for large sets

Definition (Jeřábek 2004 – simplified)

Let $\Gamma, \Delta \subseteq \{0,1\}^n$ be polytime definable sets, Γ is "larger" than Δ if there exists a polytime surjective function $F : \Gamma \twoheadrightarrow \Delta$.

A bit of history

A series of papers by Jeřábek (2004–2009) justifying and utilizing the above definition

- A very sophisticated framework
- Based on approximate counting techniques
- Related to the theory of derandomization and pseudorandomness
- Application: formalizing probabilistic complexity classes

Obstacle #1 - Talking about probability

- Given a polytime predicate $A(X, R)$,

$$\Pr_{R\in\{0,1\}^n}\left[A(X,R)\right] = \frac{|\{R \in \{0,1\}^n \mid A(X,R)\}|}{2^n}$$

- The function $F(X) := \left|\left\{R \in \{0,1\}^n \mid A(X,R)\right\}\right|$ is in #P.
- #P problems are generally harder than NP problems

Obstacle #1 - Talking about probability

- Given a polytime predicate $A(X, R)$,

$$\Pr_{R\in\{0,1\}^n}\big[A(X,R)\big] = \frac{|\{R \in \{0,1\}^n \mid A(X,R)\}|}{2^n}$$

- The function $F(X) := |\{R \in \{0,1\}^n \mid A(X,R)\}|$ is in $\#\mathrm{P}$.
- $\#$P problems are generally harder than NP problems

Solution [Jeřábek '04]

- We want to show $\Pr_{R\in\{0,1\}^n}\big[A(X,R)\big] \leq r/s$, it suffices to show

$$|\{R \in \{0,1\}^n \mid A(X,R)\}| \cdot s \leq 2^n \cdot r$$

- Key idea: construct in *VPV* a polytime surjection

$$G : \{0,1\}^n \times [r] \twoheadrightarrow \{R \in \{0,1\}^n \mid A(X,R)\} \times [s],$$

  where $[m] := \{1, \ldots, m\}$.

The Schwartz-Zippel Lemma

Let $P(X_1, \ldots, X_n)$ be a non-zero polynomial of degree D over a field $\mathbb{F}$. Let S be a finite subset of $\mathbb{F}$. Then

$$\Pr_{\vec{R} \in S^n}\left[P(\vec{R}) = 0\right] \leq \frac{D}{|S|}.$$

Obstacle #2

- The usual proof assumes we can rewrite

$$P(X_1, \ldots, X_n) = \sum_{J=0}^{D} X_1^J \cdot P_J(X_2, \ldots, X_n)$$

- This step is not feasible when P is given as arithmetic circuit or symbolic determinant

The Schwartz-Zippel Lemma

Let $P(X_1, \ldots, X_n)$ be a non-zero polynomial of degree D over a field $\mathbb{F}$. Let S be a finite subset of $\mathbb{F}$. Then

$$\Pr_{\vec{R} \in S^n}\left[P(\vec{R}) = 0\right] \leq \frac{D}{|S|}.$$

Obstacle #2

- The usual proof assumes we can rewrite

$$P(X_1, \ldots, X_n) = \sum_{J=0}^{D} X_1^J \cdot P_J(X_2, \ldots, X_n)$$

- This step is not feasible when P is given as arithmetic circuit or symbolic determinant

Solution

- Being less ambitious: restrict to the case of Edmonds' polynomials
- Take advantage of the special structure of Edmonds' polynomials

Edmonds' polynomials

$$\begin{array}{c|ccc} & d & e & f \\ a & 1 & 0 & 1 \\ b & 1 & 1 & 0 \\ c & 0 & 1 & 1 \end{array} \quad \xrightarrow{\text{replace ones with distinct variables}} \quad \text{Edmonds' matrix: } M_G = \begin{bmatrix} x_{11} & 0 & x_{13} \\ x_{21} & x_{22} & 0 \\ 0 & x_{32} & x_{33} \end{bmatrix}$$

Useful observation:

- Each variable x_{ij} appears at most once in M_G.
- From the above example, by the cofactor expansion,

$$\text{Det}(M_G) = -x_{33} \cdot \text{Det}\begin{pmatrix} x_{11} & 0 \\ x_{21} & x_{22} \end{pmatrix} + \text{Det}\begin{pmatrix} x_{11} & 0 & x_{13} \\ x_{21} & x_{22} & 0 \\ 0 & x_{32} & 0 \end{pmatrix}$$

- Thus, we can apply the idea in the original proof.

Schwartz-Zippel Lemma for Edmonds' polynomials

Theorem (provable in VPV)

Assume the bipartite graph G has a perfect matching.

- Let $S = \{0, \ldots, s-1\}$ be the sample set.
- Let $M_G^{n \times n}$ be the Edmonds' matrix of G.

Then we can construct polytime surjection

$$F : [n] \times S^{n^2-1} \twoheadrightarrow \{\vec{r} \in S^{n^2} \mid \mathrm{Det}(M_G)(\vec{r}) = 0\}.$$

- The degree of the Edmonds' polynomial $\mathrm{Det}(M_G)$ is at most n.
- The surjection F witnesses that

$$\Pr_{\vec{r} \in S^{n^2}}\left[\mathrm{Det}(M_G)(\vec{r}) = 0\right] = \frac{|\{\vec{r} \in S^{n^2} \mid \mathrm{Det}(M_G)(\vec{r}) = 0\}|}{s^{n^2}} \leq \frac{n}{s}$$

The Mulmuley-Vazirani-Vazirani Algorithm

- RNC^2 algorithm for finding a perfect matching of a bipartite graph
- Key idea: reduce to the problem of finding a **unique** min-weight perfect matching using **the isolating lemma**.

Obstacle

The isolating lemma seems too general to give a feasible proof.

Solution

Consider a specialized version of the isolating lemma.

Lemma

Given a bipartite graph G. Assume the family $\mathcal{F}$ of all perfect matchings of G is nonempty. If we assign random weights to the edges, then

$$\Pr\left[\textit{the min-weight perfect matching is unique}\right] \textit{ is high.}$$

Summary

Main motivation

Feasible proofs for randomized algorithms and probabilistic reasoning:
"Formalizing Randomized Matching Algorithms"

We demonstrate the techniques through two randomized algorithms:

1. RNC^2 algorithm for testing if a bipartite graph has a perfect matching (Lovász '79)
   - Schwartz-Zippel Lemma for Edmonds' polynomials
2. RNC^2 algorithm for finding a perfect matching of a bipartite graph (Mulmuley-Vazirani-Vazirani '87)
   - a specialized version of the isolating lemma for bipartite matchings.

Take advantage of special linear-algebraic properties of Edmonds' matrices and Edmonds' polynomials

Open problems and future work

Open questions

1. Can we prove in VPV more general version of the Schwartz-Zippel lemma?
2. Can we do better than VPV, for example, VNC^2?

Open problems and future work

Open questions

1. Can we prove in *VPV* more general version of the Schwartz-Zippel lemma?
2. Can we do better than *VPV*, for example, VNC^2?

Future work

1. How about RNC^2 matching algorithms for undirected graphs?
   - Use properties of the pfaffian
   - Need to generalize results from [Soltys '01] [Soltys-Cook '02]

   (with Lê)
2. Using Jeřábek's techniques to formalize constructive aspects of fundamental theorems that require probabilistic reasoning.
   - Theorems in cryptography, e.g., the Goldreich-Levin Theorem, construction of pseudorandom generator from one-way functions, etc.

   (with George and Lê)