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 $\Pi_2$ (and $\Pi_1$) theorems $\forall X \exists Y \varphi(X, Y)$, where $\varphi$ 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. \( \text{RNC}^2 \) algorithm for **testing** if a bipartite graph has a perfect matching (Lovász '79)
2. \( \text{RNC}^2 \) algorithm for **finding** a perfect matching of a bipartite graph (Mulmuley-Vazirani-Vazirani '87)

Recall that:

\[
\text{Log-Space} \subseteq \text{NC}^2 \subseteq \text{P} \\
\text{RNC}^2 \subseteq \text{RP}
\]

**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:

\[ \text{Log-Space} \subseteq \text{NC}^2 \subseteq \text{P} \]
\[ \text{RNC}^2 \subseteq \text{RP} \]

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.

$G$ has a perfect matching if and only if $\det(M_G)$ is not identically zero.

**Edmonds’ Theorem (provable in VPV)**

Replace ones with distinct variables to form $M_G$.

$$ M_G = \begin{bmatrix} x_{11} & 0 & x_{13} \\ x_{21} & x_{22} & 0 \\ 0 & x_{32} & x_{33} \end{bmatrix} $$

$$ \begin{bmatrix} d & e & f \\ a & 1 & 0 & 1 \\ b & 1 & 1 & 0 \\ c & 0 & 1 & 1 \end{bmatrix} \rightarrow \text{distinct variables} $$
Lovász’s Algorithm

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

$\begin{bmatrix} d & e & f \\ a & 1 & 0 & 1 \\ b & 1 & 1 & 0 \\ c & 0 & 1 & 1 \end{bmatrix}$ 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 $\det(M_G)$ is not identically zero.

The usual proof is not feasible since...

it uses the formula $\det(A) = \sum_{\sigma \in S_n} (-1)^{\text{sgn}(\sigma)} \prod_{i=1}^{n} A(i, \sigma(i))$, which has $n!$ terms.
**Lovász’s Algorithm**

<table>
<thead>
<tr>
<th></th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

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 \( \text{Det}(M_G) \) is not identically zero.
Lovász’s Algorithm

\[
\begin{bmatrix}
d & e & f \\
a & 1 & 0 & 1 \\
b & 1 & 1 & 0 \\
c & 0 & 1 & 1 \\
\end{bmatrix}
\]
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 \( \text{Det}(M_G) \) is not identically zero.

Lovász’s RNC\(^2\) Algorithm

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

- Given a polytime predicate $A(X, R)$,
  \[
  \Pr_{R \in \{0,1\}^n}[A(X, R)] = \frac{|\{R \in \{0,1\}^n \mid A(X, R)\}|}{2^n}
  \]

- The function $F(X) := |\{R \in \{0,1\}^n \mid A(X, R)\}|$ is in $\#P$.

- $\#P$ 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, $\Gamma$ is “larger” than $\Delta$ if there exists a polytime surjective function $F : \Gamma \rightarrow \Delta$.

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

- The function \( F(X) := |\{R \in \{0, 1\}^n \mid A(X, R)\}| \) is in \( \#P \).

- \( \#P \) problems are generally harder than NP problems.
Obstacle #1 - Talking about probability

- Given a polytime predicate $A(X, R)$,
  \[ \Pr_{R \in \{0,1\}^n}[A(X, R)] = \frac{|\{R \in \{0,1\}^n \mid A(X, R)\}|}{2^n} \]

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

Solution [Jeřábek ’04]

- We want to show $\Pr_{R \in \{0,1\}^n}[A(X, R)] \leq r/s$, 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
  \[ G : \{0,1\}^n \times [r] \to \{R \in \{0,1\}^n \mid A(X, R)\} \times [s], \]
  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

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

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

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

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

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,

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

- 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

$$F : [n] \times S^{n^2 - 1} \rightarrow \{\vec{r} \in S^{n^2} | \text{Det}(M_{G})(\vec{r}) = 0\}.$$ 

- The degree of the Edmonds’ polynomial $\text{Det}(M_{G})$ is at most $n$.
- The surjection $F$ witnesses that

$$\operatorname{Pr}_{\vec{r} \in S^{n^2}}[\text{Det}(M_{G})(\vec{r}) = 0] = \frac{|\{\vec{r} \in S^{n^2} | \text{Det}(M_{G})(\vec{r}) = 0\}|}{S^{n^2}} \leq \frac{n}{s}.$$
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

$$\Pr[\text{the min-weight perfect matching is unique}] \text{ is high.}$$
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, VNC²?

Future work

1. How about RNC² 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)