On Symmetric Circuits and FPC

Anuj Dawar

University of Cambridge Computer Laboratory

joint work with Matthew Anderson

Highlights, 20 September 2013
Is there a logic for $P$?

A property of *graphs* (or other relational structures) in $P$ is recognised by a family of Boolean circuits $C_n$:
Is there a logic for P?

A property of *graphs* (or other relational structures) in $P$ is recognised by a family of Boolean circuits $C_n$:

- inputs to $C_n$ are $n^2$ *potential edges*, each taking value 0 or 1;
Is there a logic for P?

A property of graphs (or other relational structures) in $P$ is recognised by a family of Boolean circuits $C_n$:

- inputs to $C_n$ are $n^2$ potential edges, each taking value 0 or 1;
- the size of $C_n$ is bounded by a polynomial $p(n)$;
Is there a logic for P?

A property of graphs (or other relational structures) in P is recognised by a family of Boolean circuits $C_n$:

- inputs to $C_n$ are $n^2$ potential edges, each taking value 0 or 1;
- the size of $C_n$ is bounded by a polynomial $p(n)$;
- the family is uniform, so the function $n \mapsto C_n$ is in P (or DLogTime).
Is there a logic for $\mathbb{P}$?

A property of *graphs* (or other relational structures) in $\mathbb{P}$ is recognised by a family of Boolean circuits $C_n$:

- inputs to $C_n$ are $n^2$ potential edges, each taking value 0 or 1;
- the size of $C_n$ is bounded by a polynomial $p(n)$;
- the family is uniform, so the function $n \mapsto C_n$ is in $\mathbb{P}$ (or DLogTime).

$C_n$ is *invariant* if the output is unchanged under a permutation of the inputs induced by a permutation of $[n]$. 

Anuj Dawar  
September 2013
Is there a logic for $\mathsf{P}$?

A property of *graphs* (or other relational structures) in $\mathsf{P}$ is recognised by a family of Boolean circuits $C_n$:

- inputs to $C_n$ are $n^2$ potential edges, each taking value 0 or 1;
- the size of $C_n$ is bounded by a polynomial $p(n)$;
- the family is uniform, so the function $n \mapsto C_n$ is in $\mathsf{P}$ (or $\mathsf{DLogTime}$).

$C_n$ is *invariant* if the output is unchanged under a permutation of the inputs induced by a permutation of $[n]$.

*Note:* dropping the uniformity condition gives us $\mathsf{P/poly}$.

*Note also:* it makes no difference if the circuits are over the **Boolean basis** $\{\text{AND, OR, NOT}\}$ or a richer basis (within $\mathsf{P}$).
Symmetric Circuits

Say $C_n$ is *symmetric* if any permutation of $[n]$ applied to its inputs can be extended to an automorphism of $C_n$. 
Say $C_n$ is *symmetric* if any permutation of $[n]$ applied to its inputs can be extended to an automorphism of $C_n$.

- Any symmetric circuit is invariant.
Say $C_n$ is symmetric if any permutation of $[n]$ applied to its inputs can be extended to an automorphism of $C_n$.

- Any symmetric circuit is invariant.
- Any formula of FP translates into a uniform family of polynomial-size symmetric Boolean circuits.
- Any formula of FPC translates into a uniform family of polynomial-size symmetric threshold (or majority) circuits.
Symmetric Circuits

- There is trivially a polynomial-size family of symmetric circuits $C_n$ deciding whether $n$ is even.
Symmetric Circuits

- There is trivially a polynomial-size family of symmetric circuits $C_n$ deciding whether $n$ is even.
- Is there a polynomial-size family of symmetric Boolean circuits deciding if an $n$ vertex graph has an even number of edges? No – as we shall see.
Symmetric Circuits

- There is trivially a polynomial-size family of symmetric circuits $C_n$ deciding whether $n$ is even.
- Is there a polynomial-size family of symmetric Boolean circuits deciding if an $n$ vertex graph has an even number of edges? No – as we shall see.
- Are polynomial-size families of uniform symmetric threshold circuits more powerful than Boolean circuits? Yes – follows from above.
Symmetric Circuits

- There is trivially a polynomial-size family of symmetric circuits $C_n$ deciding whether $n$ is even.
- Is there a polynomial-size family of symmetric Boolean circuits deciding if an $n$ vertex graph has an even number of edges? 
  *No – as we shall see.*
- Are polynomial-size families of uniform symmetric threshold circuits more powerful than Boolean circuits? 
  *Yes – follows from above.*
- Can every invariant circuit be translated into an equivalent symmetric threshold circuit, with only polynomial blow-up? 
  *No – as we shall see.*
Main Results

Theorem
A class of graphs is accepted by a $\mathbf{P}$-uniform, polynomial-size, symmetric family of Boolean circuits iff it is definable by an $\mathbf{FP}$ formula interpreted in $G \uplus ([n], <)$. 
Main Results

Theorem
A class of graphs is accepted by a \( P \)-uniform, polynomial-size, symmetric family of Boolean circuits \textit{iff} it is definable by an \( FP \) formula interpreted in \( G \uplus ([n], <) \).

Theorem
A class of graphs is accepted by a \( P \)-uniform, polynomial-size, symmetric family of threshold circuits \textit{iff} it is definable in \( FPC \).
Main Results

Theorem
A class of graphs is accepted by a \(P\)-uniform, polynomial-size, symmetric family of Boolean circuits iff it is definable by an \(FP\) formula interpreted in \(G \uplus ([n], <)\).

Theorem
A class of graphs is accepted by a \(P\)-uniform, polynomial-size, symmetric family of threshold circuits iff it is definable in \(FPC\).

This gives a natural and purely circuit-based characterisation of \(FPC\) definability.
Main Technical Tools

For a gate $g$ in a symmetric circuit $C_n$, say that a partition $\mathcal{P}$ supports $g$ if every permutation that fixes each $P \in \mathcal{P}$ also fixes $g$. 

Anuj Dawar  
September 2013
Main Technical Tools

For a gate $g$ in a symmetric circuit $C_n$, say that a partition $\mathcal{P}$ supports $g$ if every permutation that fixes each $P \in \mathcal{P}$ also fixes $g$.

$$\text{Stab}^•(\mathcal{P}) \subseteq \text{Stab}(g) \subseteq \text{Stab}(\mathcal{P})$$
Main Technical Tools

For a gate $g$ in a symmetric circuit $C_n$, say that a partition $\mathcal{P}$ supports $g$ if every permutation that fixes each $P \in \mathcal{P}$ also fixes $g$.

$$\text{Stab}^\bullet(\mathcal{P}) \subseteq \text{Stab}(g) \subseteq \text{Stab}(\mathcal{P})$$

- Each $g$ has a unique coarsest support, $\text{Supp}(g)$.
- An upper bound on $\text{Stab}(g)$ gives us a lower bound on the orbit of $g$. 
Main Technical Tools

For a gate $g$ in a symmetric circuit $C_n$, say that a partition $\mathcal{P}$ supports $g$ if every permutation that fixes each $P \in \mathcal{P}$ also fixes $g$.

$$\text{Stab}^\bullet(\mathcal{P}) \subseteq \text{Stab}(g) \subseteq \text{Stab}(\mathcal{P})$$

- Each $g$ has a unique coarsest support, $\text{Supp}(g)$.
- An upper bound on $\text{Stab}(g)$ gives us a lower bound on the orbit of $g$.

Conversely, knowing that the orbit of $g$ is at most polynomial in $n$ gives us bounds on $\text{Supp}(g)$. 

Anuj Dawar September 2013
Support Theorem

For a circuit $C$, $\text{Supp}(C)$ denotes the maximum over all gates $g$ in $C$ of the size of the union of all but the largest part in $\text{Supp}(g)$.
Support Theorem

For a circuit \( C \), \( \text{Supp}(C) \) denotes the maximum over all gates \( g \) in \( C \) of the size of the union of all but the largest part in \( \text{Supp}(g) \).

**Theorem**

*For any \( 1 > \epsilon \geq \frac{2}{3} \), let \( C \) be a symmetric \( s \)-gate circuit over \([n]\) with \( n \geq \frac{48}{\epsilon} \), and \( s \leq 2^{n^{1-\epsilon}} \). Then*

\[
\text{Supp}(C) \leq \frac{20 \log s}{\epsilon \log n}.
\]
Support Theorem

For a circuit $C$, $\text{Supp}(C)$ denotes the maximum over all gates $g$ in $C$ of the size of the union of all but the largest part in $\text{Supp}(g)$.

**Theorem**

For any $1 > \epsilon \geq \frac{2}{3}$, let $C$ be a symmetric $s$-gate circuit over $[n]$ with $n \geq \frac{48}{\epsilon}$, and $s \leq 2^{n^{1-\epsilon}}$. Then

$$\text{Supp}(C) \leq \frac{20 \log s}{\epsilon \log n}.$$ 

**Corollary**

Polynomial-size symmetric circuits have constant support.
Translating Symmetric Circuits to Formulas

Given a polynomial-time function \( n \mapsto C_n \) that generates symmetric circuits:

1. There is a formula of FP interpreted on \( ([n], <) \) that defines a structure \( C_n \).
2. Label gates with their support partition.
3. Transform labels into tuples by duplicating gates.
4. Determine equality test indicating edges of \( C_n \).
5. Evaluate circuit on unordered universe (in FP for a Boolean circuit, in FPC for one with threshold gates.)
<table>
<thead>
<tr>
<th>Logic</th>
<th>Circuits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FP</strong> on structures with a disjoint number sort ([n], &lt;).</td>
<td>Poly-size <em>symmetric</em> Boolean circuits.</td>
</tr>
<tr>
<td>Additional predicates on number sort.</td>
<td>Non-uniformity (of function (n \mapsto C_n)).</td>
</tr>
<tr>
<td>Connections between element sort and number sort (FPC and FPrk).</td>
<td>Additional gates (<em>counting</em> and <em>rank</em>).</td>
</tr>
<tr>
<td>Choiceless polynomial time.</td>
<td>Breaking symmetry (how?).</td>
</tr>
</tbody>
</table>