Generalized Boolean Satisfiability
ZAP II: Theory

Jessica Davies
Knowledge Representation and Reasoning

March 23, 2006
Outline

- Motivation and Intuition
- Group Theory Background
- Augmented Resolution
- Proof lengths of our examples
- DPLL in the new setting
- Experimental results
- Summary
- Discussion
Motivation

• None admits a poly-sized proof for clique colouring

• Is there a representation such that:
  1. Exponential savings in size of representation
  2. Poly-size proofs of the 3 problems exist
  3. DPLL is still efficient

Yes!
Intuition – Pigeon Hole

- “no two pigeons are in the same hole”:
  \[ \neg p_{ik} \lor \neg p_{jk} \quad \forall \ i \neq j, \ k \]

- One axiom represents \( \binom{n}{2} \) clauses

- Generate other clauses by permuting the literals
**Intuition – Parity Axioms**

\[ x_1 + x_2 + x_3 \equiv 1 \pmod{2} \]

equivalent to the 4 clauses

\[
\begin{align*}
    x_1 &\lor x_2 &\lor x_3 &\quad &\neg x_1 &\lor x_2 &\lor \neg x_3 \\
    x_1 &\lor \neg x_2 &\lor \neg x_3 &\quad &\neg x_1 &\lor \neg x_2 &\lor x_3
\end{align*}
\]

How can the other three clauses be generated from the first using permutations?
Intuition – Parity Axioms cont.

1. \( x_1 \lor x_2 \lor x_3 \)
2. \( x_1 \lor \neg x_2 \lor \neg x_3 \)
3. \( \neg x_1 \lor x_2 \lor \neg x_3 \)
4. \( \neg x_1 \lor \neg x_2 \lor x_3 \)

Permutations:

1 -> 1: ()
1 -> 2: \((x_2 \neg x_2)(x_3 \neg x_3)\)
1 -> 3: \((x_1 \neg x_1)(x_3 \neg x_3)\)
1 -> 4: \((x_1 \neg x_1) (x_2 \neg x_2)\)
Set of permutations for the parity clause:

\[ S = \{(), (x_2 \rightarrow x_2)(x_3 \rightarrow x_3), (x_1 \rightarrow x_1)(x_3 \rightarrow x_3), (x_1 \rightarrow x_1)(x_2 \rightarrow x_2)\} \]

Compose elements of \( S \):

\[
(x_2 \rightarrow x_2)(x_3 \rightarrow x_3)(x_1 \rightarrow x_1)(x_3 \rightarrow x_3) = (x_1 \rightarrow x_1)(x_2 \rightarrow x_2)
\]

\[
(x_2 \rightarrow x_2)(x_3 \rightarrow x_3)(x_1 \rightarrow x_1)(x_2 \rightarrow x_2) = (x_1 \rightarrow x_1)(x_3 \rightarrow x_3)
\]

\[
(x_1 \rightarrow x_1)(x_3 \rightarrow x_3)(x_1 \rightarrow x_1)(x_2 \rightarrow x_2) = (x_2 \rightarrow x_2)(x_3 \rightarrow x_3)
\]

- \( S \) is closed under function composition

\[
(x_2 \rightarrow x_2)(x_3 \rightarrow x_3)(x_2 \rightarrow x_2)(x_3 \rightarrow x_3) = (x_1)(x_2)(x_3)(x_4) = ()
\]

- Each element of \( S \) is its own inverse
Group Theory

- Set of permutations $S$:
  - closed under the composition operator (which is associative)
  - contains an identity ($\varepsilon$)
  - every element has an inverse
  $\Rightarrow S$ with composition operator is a group

- Groups:
  - structured set with operator
  - properties have been studied intensively

- If a set of clauses intuitively has structure, its set of permutations will be a group
Group Theory - Definitions

- \( \text{Sym}(n) \) – the Symmetric group on \( n \) elements
  - the group made up of all permutations of \( \{1, \ldots, n\} \)

- \( W_n \) – the subgroup of \( \text{Sym}(2n) \) s.t. \(-l_1\) is mapped to \(-l_2\) whenever \( l_1 \) is mapped to \( l_2 \)

- Generators: \( \langle x \rangle \) is the group generated by the element \( x \)
  - \( \langle x \rangle = \{1, x, x^2, x^3, \ldots, x^{m-1}\} \) where \( m \) is the smallest number s.t. \( x^m = 1 \)
  - Every group has a set of \( \leq \log_2|G| \) generators
    - can find in poly time
Progress

- Motivation and Intuition
- Group Theory Background
  - Augmented Resolution
    - Proof lengths of our examples
    - DPLL in the new setting
    - Experimental results
- Summary
- Discussion
Reasoning and Inference

- Reasoning with augmented clauses:
  - lifted form of resolution, watched literals for UP, and clause learning
- Let's start with resolution, since the size of resolution proofs determines the complexity of DPLL
Augmented Clauses

- Augmented clause \((c, G)\)
  - \(c\) is the prototypical clause
  - \(G\) is a group of permutations
  - \(c^G = \{g(c) \mid g \in G\}\) - set of ground clauses represented
  - Note that if some clauses are not related to others, they can still be represented as \((c, \{I\})\)
Augmented Resolution

- Result of resolving \((c_1, G_1)\) and \((c_2, G_2)\)
  - ideally another augmented clause \((c, G)\)
  - \((c, G)\) should capture all clauses which can be produced by resolving clauses in \((c_1, G_1)\) and \((c_2, G_2)\)
- But this is not possible!
  
  \[
  (c_1, G) = (a \lor b, (bc)) \rightarrow \{(a \lor b), (a \lor c)\}
  \]
  
  \[
  (c_2, G) = (\neg a \lor d, (dc)) \rightarrow \{\neg a \lor d, (\neg a \lor c)\}
  \]

  Resolving ground clauses produces:

  \[
  \{(b \lor d), (b \lor c), (c \lor d), (c)\}
  \]
Augmented Resolution – cont.

- Conditions for satisfactory resolution rule:
  1. \((c_1, G_1) \land (c_2, G_2) \Rightarrow (c, G)\)
  2. \(\text{resolve}(c_1, c_2)\) is an instance of \((c, G)\)
  3. \(G_1 \leq H_1, G_2 \leq H_2 \Rightarrow (c, G)\) is a resolvant of \((c_1, H_1)\) and \((c_2, H_2)\)

- 4., 5. & 6. on pages 501-502
Augmented Resolution Rule

- Resolvent of \((c_1, G_1), (c_2, G_2)\) is any clause \((\text{resolve}(c_1, c_2), G)\) s.t.
  - \(G \leq \text{stab}(c_i, H_i) \cap W_n\) where \(H_1 \leq G_1, H_2 \leq G_2\)
- What is \(\text{stab}(c_i, H_i)\) ???
  - subgroup of Sym(2n)
  - \(\omega \in \text{stab}(c_i, H_i)\) iff \(\omega\) behaves the same as some \(h_1 \in H_1\) on \((c_1, H_1)\), and behaves the same as some \(h_2 \in H_2\) on \((c_2, H_2)\),
Properties of Augmented Resolution

- Time to find resolvent:
  - in NP ⇒ worst case exponential in size of augmented clauses
  - but: augmented clauses exponentially smaller than CNF encoding
  - ∴ poly in the CNF encoding

- One augmented resolution step: how many resolutions between ground clauses?
Progress

- Motivation and Intuition
- Group Theory Background
- Augmented Resolution
  - Proof lengths of our examples
  - DPLL in the new setting
- Experimental results
- Summary
- Discussion
Proof Lengths

- Representational Efficiency
- Proof Lengths

<table>
<thead>
<tr>
<th>clause type</th>
<th>Boolean axioms</th>
<th>generators</th>
<th>total size</th>
</tr>
</thead>
<tbody>
<tr>
<td>cardinality</td>
<td>$\binom{m}{k-1}$</td>
<td>2</td>
<td>$m + 1$</td>
</tr>
<tr>
<td>parity</td>
<td>$2^{k-1}$</td>
<td>3</td>
<td>$k + 5$</td>
</tr>
<tr>
<td>QPROP</td>
<td>$d^v$</td>
<td>2$v$</td>
<td>$\nu(d + 1)$</td>
</tr>
</tbody>
</table>

| SAT         | —              | EEE        | —         | watched literals | relevance |
| cardinality | exponential    | P?E        | not unique| watched literals | relevance |
| pseudo-Boolean | exponential    | P?E        | unique    | watched literals | + strengthening |
| symmetry    | —              | EEE*       | not believed in P | same as SAT | same as SAT |
| QPROP       | exponential    | ???        | in P using reasons | exp improvement | + first-order |
| ZAP         | exponential    | PPP        |           |                   |          |
\textbf{Modified DPLL}

\begin{verbatim}
RBL(C, D, P):

1    \langle x, y \rangle \leftarrow \text{UNIT-PROPAGATE}(C \cup D, P)
2    \textbf{if } x = \text{true}
3        \textbf{then } \langle c, G \rangle \leftarrow y
4            \textbf{if } c \text{ is empty}
5                \textbf{then return } \text{FAILURE}
6                \textbf{else remove successive elements from } P \text{ so that } c \text{ is unit}
7                D \leftarrow D \cup \{c\}
8                \text{remove from } D \text{ all augmented clauses without } k\text{-relevant instances}
9                \textbf{return } RBL(C, D, P)
10\textbf{else } P \leftarrow y
11    \textbf{if } P \text{ is a solution to } C
12        \textbf{then return } P
13    \textbf{else } l \leftarrow \text{a literal not assigned a value by } P
14        \textbf{return } RBL(C, \langle P, (l, \text{true}) \rangle)
\end{verbatim}
Experimental Results

Pigeon Hole

Parity

Clique Colouring
**Summary**

- New representation language of augmented clauses
- New inference rule: augmented resolution

<table>
<thead>
<tr>
<th></th>
<th>efficiency of rep'n</th>
<th>proof length</th>
<th>resolution</th>
<th>propagation technique</th>
<th>learning method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAT</strong></td>
<td>exponential</td>
<td>EEE</td>
<td>—</td>
<td>watched literals</td>
<td>relevance</td>
</tr>
<tr>
<td><strong>cardinality</strong></td>
<td>exponential</td>
<td>P?E</td>
<td>not unique</td>
<td>watched literals</td>
<td>relevance</td>
</tr>
<tr>
<td><strong>pseudo-Boolean</strong></td>
<td>exponential</td>
<td>P?E</td>
<td>unique</td>
<td>watched literals</td>
<td>+ strengthening</td>
</tr>
<tr>
<td><strong>symmetry</strong></td>
<td>—</td>
<td>EEE*</td>
<td>not believed in P</td>
<td>same as SAT</td>
<td>same as SAT</td>
</tr>
<tr>
<td><strong>QPROP</strong></td>
<td>exponential</td>
<td>???</td>
<td>in P using reasons</td>
<td>exp improvement</td>
<td>+ first-order</td>
</tr>
<tr>
<td><strong>ZAP</strong></td>
<td>exponential</td>
<td>PPP</td>
<td>in P using reasons</td>
<td>watched literals, exp improvement</td>
<td>+ first-order + parity + others</td>
</tr>
</tbody>
</table>
Discussion

- How often does group structure occur?
- How hard is it to find existing group structure?
- What about the completeness of augmented resolution?
- How does this representation subsume cardinality, pseudo-boolean, QPROP?