LECTURE NOTES

#19 Apr 6, 1995
Jing Wu

Theorem Let , $= \{A_i(\vec{p}, \vec{q})\} \cup \{B_j(\vec{p}, \vec{r})\}$ have a resolution refutation of length n, then there is a interpolant $C(\vec{p})$ such that

$$\bigwedge_i A_i(\vec{p}, \vec{q}) \Rightarrow C(\vec{p})$$

and

$$C(\vec{p}) \Rightarrow \neg \bigwedge_j (B_j(\vec{p}, \vec{r}))$$

and $C(\vec{p})$ has circuits of size $O(n)$.

Proof of theorem

For each expression E in our resolution refutation, we will have a gate C_E in our circuit. (The circuit $C_\Box$ for the final clause in the refutation will be the circuit $C(\vec{p})$) as follows.

1. $E = A_i(\vec{p}, \vec{q})$, then C_E is the constant 0.

2. $E = B_j(\vec{p}, \vec{r})$, then C_E is the constant 1.

3. $E = F \cup G$ from $(F \cup \{p_i\}, G \cup \{\overline{p_i}\})$

$$C_E ::= (\overline{p_i} \wedge C_{F \cup \{p_i\}}) \vee (p_i \wedge C_{G \cup \{\overline{p_i}\}})$$

4. $E = F \cup G$ from $(F \cup \{q_i\}, G \cup \{\overline{q_i}\})$

$$C_E ::= C_{F \cup \{q_i\}} \vee C_{G \cup \{\overline{q_i}\}}$$

5. $E = F \cup G$ from $(F \cup \{r_i\}, G \cup \{\overline{r_i}\})$

$$C_E ::= C_{F\cup\{r_i\}} \wedge C_{G\cup\{\overline{r_i}\}}$$

(Note, output circuit $C_\Box$ has input only for 0, 1, p_i, $\overline{p_i}$).

In order to finish the proof of the theorem, we must prove the following lemma. (This is clearly sufficient to prove the theorem, since the output gate of this circuit of $C_\Box$, and $\tau(\Box) = \bot$ for *every* τ. Note that a truth assignment τ is the same as an input assignment to the circuit $C_\Box$.)

Lemma If τ is a assignment such that $\tau(E) = \bot$, then

$$\tau(C_E) = \bot \Longrightarrow \exists i\ \tau(A_i) = \bot$$

$$\tau(C_E) = \top \Longrightarrow \exists i\ \tau(B_i) = \bot$$

(Note C_E does not compute E).

Proof

1. If $E = A_i(\vec{p}, \vec{q})$, then $\tau(C_E) = \bot$. The hypothesis of the lemma is that $\tau(A_i(\vec{p}, \vec{q}) = \bot$, so the claim holds trivially in this case.

2. $E = B_j(\vec{p}, \vec{r})$, then $\tau(C_E) = \top$ and $\tau(B_j(\vec{p}, \vec{r})) = \bot$, similar to case 1.

3. $E = F \cup G$ from $(F \cup \{p_i\}, G \cup \{\overline{p_i}\})$

$$C_E ::= (\overline{p_i} \wedge C_{F\cup\{p_i\}}) \vee (p_i \wedge C_{G\cup\{\overline{p_i}\}})$$

If $\tau(E) = \bot$ then $\tau(F) = \tau(G) = \bot$

If $\tau(C_E) = \bot$, then

case a: $\tau(p_i) = \top$, then $\tau(C_{G\cup\{\overline{p_i}\}}) = \bot$ and $\tau(G \cup \{\overline{p_i}\}) = \bot$. By induction hypothesis, $\exists i\ \tau(A_i) = \bot$.

case b: $\tau(\overline{p_i}) = \top$, then $\tau(C_{F\cup\{p_i\}}) = \bot$ and $\tau(F \cup \{p_i\}) = \bot$. By induction hypothesis, $\exists i\ \tau(A_i) = \bot$.

If $\tau(C_E) = \top$, then

case a: $\tau(p_i) = \top$, then $\tau(C_{G\cup\{\overline{p_i}\}}) = \top$ and $\tau(G \cup \{\overline{p_i}\}) = \bot$. By induction hypothesis, $\exists i\ \tau(B_i) = \bot$.

case b: $\tau(\overline{p_i}) = \top$, then $\tau(C_{F\cup\{p_i\}}) = \top$ and $\tau(F \cup \{p_i\}) = \bot$. By induction hypothesis, $\exists i\ \tau(B_i) = \bot$.

4. $E = F \cup G$ from $(F \cup \{q_i\}, G \cup \{\overline{q_i}\})$

$$C_E ::= C_{F\cup\{q_i\}} \vee C_{G\cup\{\overline{q_i}\}}$$

If $\tau(E) = \bot$ then $\tau(F) = \tau(G) = \bot$.

If $\tau(C_E) = \bot$, then $\tau(C_{F\cup\{q_i\}}) = \tau(C_{G\cup\{\overline{q_i}\}}) = \bot$.

case a: $\tau(q_i) = \top$, then $\tau(C_{G\cup\{\overline{q_i}\}}) = \bot$ and $\tau(G \cup \{\overline{q_i}\}) = \bot$. By induction hypothesis, $\exists i\ \tau(A_i) = \bot$.

case b: $\tau(\overline{q_i}) = \top$, then $\tau(C_{F\cup\{q_i\}}) = \bot$ and $\tau(F \cup \{q_i\}) = \bot$. By induction hypothesis, $\exists i\ \tau(A_i) = \bot$.

If $\tau(C_E) = \top$, then at least one of $\tau(C_{F\cup\{q_i\}})$ and $\tau(C_{G\cup\{\overline{q_i}\}})$ is true. Also, at least one of $\tau(F \cup \{q_i\})$ and $\tau(G \cup \{\overline{q_i}\})$ is true. Note that:

If $\tau(F \cup \{q_i\}) = \bot$ and $\tau(C_{F\cup\{q_i\}}) = \top$, then by inductive hypothesis, $\exists j\ B_j(\vec{p}, \vec{r}) = \bot$.

If $\tau(G \cup \{\overline{q_i}\}) = \bot$ and $\tau(C_{G\cup\{\overline{q_i}\}}) = \top$, then by inductive hypothesis, $\exists j\ B_j(\vec{p}, \vec{r}) = \bot$.

Thus we need only worry about the cases where

case a:

$$\tau(F \cup \{q_i\}) = \bot,\ \tau(C_{F\cup\{q_i\}}) = \bot;\ \tau(G \cup \{\overline{q_i}\}) = \top, \tau(C_{G\cup\{\overline{q_i}\}}) = \top$$

case b:

$$\tau(F \cup \{q_i\}) = \top,\ \tau(C_{F\cup\{q_i\}}) = \top;\ \tau(G \cup \{\overline{q_i}\}) = \bot, \tau(C_{G\cup\{\overline{q_i}\}}) = \bot$$

but note $C_{F\cup\{q_i\}})$, $C_{G\cup\{\overline{q_i}\}}$, and $B_j(\vec{p},\vec{r})$ don't have q_i as a variable. Thus if $\tau'(q_i) = \begin{cases} \bot & \text{if } \tau(q_i) = \top \\ \top & \text{otherwise} \end{cases}$ and $\tau = \tau'$ on all other variables, then we have that

case a: $\tau'(C_{F\cup\{q_i\}}) = \bot$ (since $\tau(F) = \tau'(F) = \bot$ and $\tau(F\cup\{q_i\}) = \top$ and $\tau(F \cup \{q_i\}) = \top$. By induction hypothesis, $\exists j\ \tau'(B_j) = \bot$, and $\tau'(B_j) = \tau(B_j)$.

case b: Similar to case a.

5. $E = F \cup G$ from $(F \cup \{r_i\}, G \cup \{\overline{r_i}\})$

$$C_E ::= C_{F\cup\{r_i\}} \wedge C_{G\cup\{\overline{r_i}\}}$$

This is similar to case 4.

$\boxed{2}$

$\boxed{1}$

Theorem(monotone)
Let , $= \{A_i(\vec{p},\vec{q})\} \cup \{B_j(\vec{p},\vec{r})\}$ have a refutation of length n, where **either** the $\vec{p}$ variables occur only positively in the A_i's **or** they occur only negatively in the B_j's. Then there is a monotone circuit $C(\vec{p})$ of size

$$O(n)$$

such that for every τ,

$$\tau(C(\vec{p})) = \bot \Longrightarrow \exists i\ \tau(A_i(\vec{p},\vec{q})) = \bot$$

$$\tau(C(\vec{p})) = \top \Longrightarrow \exists j\ \tau(B_j(\vec{p},\vec{r})) = \bot$$

Note: in order to get a monotone circuit, we need to assume that the p_l's either appear only positively in A_i or only negatively in B_j.

Proof We present the proof only in the case when the p_l's occur only negatively in the B_j's; the other case is similar.

We will build a circuit C_E for each expression E in the resolution refutation.

1. $E = A_i(\vec{p}, \vec{q})$, then C_E is the constant 0.

2. $E = B_j(\vec{p}, \vec{r})$, then C_E is the constant 1.

3. $E = F \cup G$ from $(F \cup \{p_i\}, G \cup \{\overline{p_i}\}$[1]

$$C_E ::= C_{F\cup\{p_i\}} \vee (p_i \wedge C_{G\cup\{\overline{p_i}\}})$$

4. $E = F \cup G$ from $(F \cup \{q_i\}, G \cup \{\overline{q_i}\})$

$$C_E ::= C_{F\cup\{q_i\}} \vee C_{G\cup\{\overline{q_i}\}}$$

5. $E = F \cup G$ from $(F \cup \{r_i\}, G \cup \{\overline{r_i}\})$

$$C_E ::= C_{F\cup\{r_i\}} \wedge C_{G\cup\{\overline{r_i}\}}$$

Clearly, $C_\Box$ is a monotone circuit of size $O(n)$. As in the proof of the preceding theorem, we base our proof of correctness on a lemma that we prove by induction. The statement of the lemma for this monotone construction is more complicated than the statement of the corresponding lemma in the preceding result. (Thanks to Sam Buss, for providing this corrected lemma, based on a paper of Pudlák.)

For any clause E appearing in the refutation, define two "sub-clauses" E^A and E^B as follows. E^A is the disjunction of all the literals occuring in E that involve q-variables and p-variables; that is, all of the literals involving r-variables are "erased". E^B is the disjunction of all of the literals occuring

[1]To prove the theorem when the p_i's occur only positively in the A_j's, define C_E to be $(p_i \vee C_{F\cup\{p_i\}}) \wedge C_{G\cup\{\overline{p_i}\}}$ in this case.

in E that involve r-variables and the *negative* p-literals; that is, all q-variables and all non-negated p-variables are "erased". Note that E^A and E^B are not necessarily disjoint.[2]

Note that the following lemma is clearly sufficient to prove the theorem, since $\Box^A = \Box^B = \Box$, and the output gate of the circuit is $C_\Box$.

Lemma(monotone)

$$\tau(E^A) = \bot \text{ and } \tau(C_E) = \bot \Longrightarrow \exists i\ \tau(A_i) = \bot$$

$$\tau(E^B) = \bot \text{ and } \tau(C_E) = \top \Longrightarrow \exists i\ \tau(B_i) = \bot$$

Proof of this lemma:

By induction on where E appears in the resolution refutation.

1. If $E = A_i(\vec{p}, \vec{q})$, then for all τ, $\tau(C_E) = \bot$, so only the first implication in the Lemma needs to be considered. Note also that $E^A = E$, and thus if the hypothesis for the first implication holds, then trivially $\tau(A_i) = \bot$.

2. $E = B_j(\vec{p}, \vec{r})$, then $\tau(C_E) = \top$ and $E = E^B$. Thus this is similar to the previous case.

3. $E = F \cup G$ from $(F \cup \{p_i\}, G \cup \{\overline{p_i}\})$

$$C_E ::= (C_{F \cup \{p_i\}}) \vee (p_i \wedge C_{G \cup \{\overline{p_i}\}})$$

Case a: $\tau(E^A) = \bot$ and $\tau(C_E) = \bot$. We consider two cases, depending on $\tau(p_i)$.

[2]To prove the theorem when the p_i's occur only positively in the A_j's, define E^A to be the result of erasing the r-literals and the *positive* p-literals from E, and define E^B to the result of erasing the q-literals from E. The rest of the argument is similar.

If $\tau(p_i) = \top$, then $\tau((G \cup \{\overline{p_i}\})^A) = \tau(G^A \cup \{\overline{p_i}\}) = \bot$. Also, $\tau(C_{G\cup\{\overline{p_i}\}}) = \bot$. Thus, by induction, there is some j such that $\tau(A_j) = \bot$.

If $\tau(p_i) = \bot$, then $\tau((F \cup \{p_i\})^A) = \tau(F^A \cup \{p_i\}) = \bot$. Also, $\tau(C_{F\cup\{p_i\}}) = \bot$. Again, the claim follows by induction.

Case b: $\tau(E^B) = \bot$ and $\tau(C_E) = \top$.

In this case, note that $(F \cup \{p_i\})^B = F^B$ and thus $\tau(F \cup \{p_i\})^B = \bot$. Since $C_E = \top$, there are the following two cases.

If $\tau(C_{F\cup\{p_i\}}) = \top$, then the induction hypothesis implies that for some $j, \tau(B_j) = \bot$.

Otherwise, $\tau(p_i \wedge C_{G\cup\{\overline{p_i}\}}) = \top$. Thus $\tau((G \cup \{\overline{p_i}\})^B) = \bot$. Again, the induction hypothesis yields the desired result.

4. $E = F \cup G$ from $(F \cup \{q_i\}, G \cup \{\overline{q_i}\})$

$$C_E ::= C_{F\cup\{q_i\}} \vee C_{G\cup\{\overline{q_i}\}}$$

Case a: $\tau(E^A) = \bot$ and $\tau(C_E) = \bot$.

Note that $\tau(C_{F\cup\{q_i\}}) = \tau(C_{G\cup\{\overline{q_i}\}}) = \bot$. Also, either $\tau(F \cup \{p_i\}) = \bot$ or $\tau(G \cup \{\overline{p_i}\}) = \bot$. In either case, the induction hypothesis yields that for some j, $\tau(A_j) = \bot$.

Case b: $\tau(E^B) = \bot$ and $\tau(C_E) = \top$.

Note that $E^B = (F \cup \{q_i\})^B \cup (G \cup \{\overline{q_i}\})^B$, and thus $\tau((F \cup \{q_i\})^B) = \tau((G \cup \{\overline{q_i}\})^B) = \bot$. Also, since $\tau(C_E) = \top$, either $\tau(C_{F\cup\{q_i\}}) = \top$ or $\tau(C_{G\cup\{\overline{q_i}\}}) = \top$. In either case the induction hypothesis yields that for some j, $\tau(B_j) = \bot$.

5. $E = F \cup G$ from $(F \cup \{r_i\}, G \cup \{\overline{r_i}\})$

$$C_E ::= C_{F\cup\{r_i\}} \wedge C_{G\cup\{\overline{r_i}\}}$$

This is similar to case 4.

$\boxed{2}$

$\boxed{1}$