Propositional Proof Systems (p. 348-359)

Petri Savola

Laboratory for Theoretical Computer Science, TKK

19.11.2007
Outline

- Basics of cutting planes
- Cutting planes and $PHP$
- Polynomial size refutation for generalized version of $PHP$
- Special case of cutting planes: $CP_q$
- Proof that $CP_q$ p-simulates $CP$
- Normal form for $CP$ proofs
- Summary
Cutting planes (basics)

- Take negation of the tautology which needs to be proved.
- Transform the formula into CNF form.
- Then for each clause write an inequality.
- Derive a contradiction using axioms, rules of inference and the inequalities.
Degen’s generalization of PHP

- Given positive integers \( m \) and \( k \), if there is a function \( f : \{0, \ldots, mk\} \to \{0, \ldots, k - 1\} \) then there is \( j < k \) for which \( f^{-1}(j) \) has size greater than \( m \).
- Note that \( PHP_k^{k+1} \) is a special case of this \((m = 1)\).
- Denote the set of size \( n \) subsets of \( \{0, \ldots, m - 1\} \) by \([m]^n\). Then Degen’s generalization can be expressed the following way

\[
\bigwedge_{0 \leq i \leq mk} \bigvee_{0 \leq j < k} p_{i,j} \rightarrow \bigvee_{0 \leq j < k} \bigvee_{I \in [mk+1]^{m+1}} \bigwedge_{i \in I} p_{i,j} \tag{1}
\]
Degen’s generalization of PHP

Denote formula (1) by $D_{m,k}$. Clearly $\neg D_{m,k}$ is a CNF-formula, so for each of its clauses we can write CP-inequalities. We obtain

- $\sum_{j=0}^{k-1} p_{i,j} \geq 1$ for $0 \leq i \leq mk$
- $-p_{i_1,j} - p_{i_2,j} - \ldots - p_{i_{m+1},j} \geq -m$ for $0 \leq j < k$ and $0 \leq i_1 < i_2 < \ldots < i_{m+1} \leq mk$.
- Total number of $mk + 1 + \binom{mk+1}{m+1}k$ inequalities.
- Let $E_{m,k}$ denote these inequalities.
Degen's generalization of PHP

Theorem 5.6.3
There are $O(k^5)$ size CP refutations of $E_{2,k}$.

Proof. For all $0 \leq i_1 < i_2 < i_3 \leq 2k$ and all $0 \leq r < k$ we have
$2 \geq p_{i_1,r} + p_{i_2,r} + p_{i_3,r}$.

- Hence also $2 \geq p_{i_1,r} + p_{i_2,r} + p_{i_2+1,r}$ holds.
- By applying Claim 2 we obtain (after applying it $2k - 3$ times)
$2 \geq p_{0,r} + \ldots + p_{2k,r}$ for each $0 \leq r < k$.
- We can sum up all these $k$ inequalities to obtain
$2k \geq \sum_{i=0}^{2k} \sum_{j=0}^{k-1} p_{i,j}$.
- But we also have $\sum_{j=0}^{k-1} p_{i,j} \geq 1$ for each $0 \leq i \leq 2k$.
- By summing these up we get $\sum_{i=0}^{2k} \sum_{j=0}^{k-1} p_{i,j} \geq 2k + 1$ which leads
into the contradiction $2k \geq 2k + 1$.

The book claims the proof size is $O(k^5)$. 
Degen’s generalization of PHP

Claim 2
Assume that $3 \leq s \leq 2k$ and for all $0 \leq i_1 < \ldots < i_s \leq 2k$ such that $i_2, \ldots, i_s$ are consecutive, and for all $0 \leq r < k$, it is the case that $2 \geq p_{i_1,r} + \ldots + p_{i_s,r}$.

Then for all $0 \leq i_1 < \ldots < i_{s+1} \leq 2k$ such that $i_2, \ldots, i_{s+1}$ are consecutive, and for all $0 \leq r < k$, it is the case that $2 \geq p_{i_1,r} + \ldots + p_{i_{s+1},r}$.

Proof of Claim 2
The following inequalities hold

- $2 \geq p_{i_1,r} + \ldots + p_{i_s,r}$
- $2 \geq p_{i_2,r} + \ldots + p_{i_{s+1},r}$
- $2 \geq p_{i_1,r} + p_{i_3,r} + \ldots + p_{i_{s+1},r}$
- $2 \geq p_{i_1,r} + p_{i_2,r} + p_{i_{s+1},r}$

Summing them up we obtain $8 \geq 3p_{i_1,r} + \ldots + 3p_{i_{s+1},r}$ Division by 3 yields $2 = \left\lfloor \frac{8}{3} \right\rfloor \geq p_{i_1,r} + \ldots + p_{i_{s+1},r}$, which completes the proof.
Degen’s generalization of PHP

Theorem 5.6.4
Let $m \geq 2$ and $n = mk + 1$. Then there are $O(n^{m+3})$ size CP refutations of $E_{m,k}$, where the constant in the $O$-notation depends on $m$, and $O(n^{m+4})$ size CP refutations, where the constant is independent of $n, m$.

Proof. Generalization of Theorem 5.6.3. (details omitted)
Polynomial equivalence of CP₂ and CP

Example

- $9x + 12y \geq 11$ (1)
- $3(3x) + 3(4y) \geq 11$ (2)
- $x \geq 0 \rightarrow 3x \geq 0$ (3)
- $y \geq 0 \rightarrow 4y \geq 0$ (4)
- $(3 + 1)(3x) + (3 + 1)(4y) = 2^2(3x) + 2^2(4y) \geq 11$ (5)
- $3x + 4y \geq \left\lceil \frac{11}{2^2} \right\rceil = 2$ (6)
- $(6) + (2) \Rightarrow 4(3x) + 4(4y) \geq 13$ (7)
- $3x + 4y \geq 3$ (8)

We get the inequality (8) which we would obtain by dividing inequality (1) by three using only division by 2. CP₉ means that only division by $q$ is allowed.
Polynomial equivalence of \( \text{CP}_q \) and \( \text{CP} \)

**Theorem 5.6.5**
Let \( q > 1 \). Then \( \text{CP}_q \) p-simulates \( \text{CP} \).

*Proof.* Suppose a cutting plane proof contains a division inference \( c\alpha \geq M \rightsquigarrow \alpha \geq \lceil M/c \rceil \). This can be p-simulated by only using division by \( q \). For this we generate a sequence \( s_0 \leq s_1 \leq \ldots \leq \lceil M/c \rceil \) such that from \( \alpha \geq s_i \) and \( ca \geq M \) one can obtain \( \alpha \geq s_{i+1} \).

Choose \( p \) so that \( q^{p-1} < c \leq q^p \). We can assume that \( q^p / 2 < c \), because otherwise we can multiply the original inequality with \( m \) and then \( q^p / 2 < mc \leq q^p \) would hold.

\[ \alpha = \sum_{i=1}^{n} a_ix_i \]. Let \( s_0 \) be the sum of negative coefficients of \( \alpha \). Because \( x_i \geq 0 \) and \( x_i \leq 1 \) we can easily derive \( \alpha \geq s_0 \).
Proof continued

Define $s_{i+1} = \lceil \frac{(q^p - c)s_i + M}{q^p} \rceil$. (details about this later)

- $c\alpha \geq M$ (1)
- $c\alpha + q^p\alpha \geq q^p\alpha + M$ (2)
- $q^p\alpha \geq (q^p - c)\alpha + M$ (3)
- $\alpha \geq s_i$ (4)
- $(q^p - c)\alpha \geq (q^p - c)s_i$ (5)
- $(5) + (3) \Rightarrow q^p\alpha \geq (q^p - c)s_i + M$ (6)
- $\alpha \geq \lceil \frac{(q^p - c)s_i + M}{q^p} \rceil = s_{i+1}$ (7)
Generation of the sequence

- $s = M/c$
- $cs = M$
- $cs + sq^p = sq^p + M$
- $sq^p = (q^p - c)s + M$
- $s = \frac{(q^p - c)s + M}{q^p} = f(s)$

Then, $s_{n+1} = f(s_n)$.

- $(q^p - c)/q^p = 1 - c/q^p < 1$, because $c \leq q^p$.
- Thus $|f'(s)| < 1$ always, so the iteration converges into $M/c$.
- Also, this function has the property

  
  $s \geq f(s) \iff s \geq (1 - c/q^p)s + M/q^p \iff cs/q^p \geq M/q^p \iff cs \geq M$

  
  which trivially holds, because $cs = M$.

Then, $s_0 \leq s_1 \leq ... \leq s_i \leq M/c$. 


Convergence of the sequence

We have now proved that given \( c\alpha \geq M \) and \( \alpha \geq s_0 \) we can inductively prove \( \alpha \geq s_i \). And also \( s_i \) converges into \([M/c]\), so eventually we can prove \( \alpha \geq [M/c] \) using only division by \( q \). We still need to prove that the convergence is fast.

Denote \( a = (q^p - c)/q^p \) and \( b = M/q^p \). Then \( 1 - a = c/q^p \).

- \( s_1 \geq as_0 + b \)
- \( s_2 \geq as_1 + b \geq a(as_0 + b) + b \)
- \( \ldots \)
- \( s_j \geq b \sum_{i=0}^{j-1} a + a^j s_0 = b(1 - a^j)/(1 - a) + a^j s_0 = b/(1 - a) - a^j (b/(1 - a) - s_0) = M/c - a^j (M/c - s_0) \)

So, if \( a^j (M/c - s_0) < 1 \) we can see that the difference between \( s_j \) and \( M/c \) is less than one. Therefore we need at most \( j + 1 \) steps to prove \( \alpha \geq [M/c] \).

\( c > q^p/2 \Rightarrow (q^p - c) < q^p/2 \Rightarrow a < 1/2 \). Thus, \( a^j (M/c - s_0) < 1 \) holds if \( (1/2)^j (M/c - s_0) < 1 \) holds. By solving \( j \) we obtain \( j > \log_2(M/c - s_0) \) which completes the proof.
Normal Form for CP Proofs

Let $\Sigma = \{I_1, ..., I_p\}$ be an unsatisfiable set of linear inequalities, and suppose that absolute value of every coefficient and constant term in each inequality of $\Sigma$ is bounded by $B$. Let $A = pB$.

**Theorem 5.6.6**
Let $P$ be a CP refutation of $\Sigma$ having $l$ lines. Then there is a CP refutation $P'$ of $\Sigma$, such that $P'$ has $O(l^3 \log(A))$ lines and such that each coefficient and constant term appearing in $P'$ has absolute value equal to $O(l2^l A)$.

**Proof.** Long and hard to understand.

**Corollary 5.6.2**
Let $\Sigma$ be an unsatisfiable set of linear inequalities, and let $n$ denote the size $|\Sigma|$. If $P$ is a CP refutation of $\Sigma$ having $l$ lines, then there is a CP refutation $P'$ of $\Sigma$, such that $P'$ has $O(l^3 \log(n))$ lines and such that the size of the absolute value of each coefficient and constant term appearing in $P'$ is $O(l + \log(n))$. 
Summary

We should have learned today that...

- There is polynomial size CP proof for generalized version of PHP
- CP p-simulates $\text{CP}_q$ and $\text{CP}_q$ p-simulates CP so they are polynomially equivalent.
- The size of coefficients in a CP refutation depends polynomially on the length of the refutation and the size of the CNF formula.