Space complexity of cutting planes refutations

Nicola Galesi, Pavel Pudlák, Neil Thapen

Nicola Galesi
Sapienza - University of Rome

June 19, 2015

Cutting planes proofs

A refutational system for CNFs as linear inequalities

$$\bigvee_{i \in P} x_i \vee \bigvee_{i \in N} \neg x_i \quad \longmapsto \quad \sum_{i \in P} x_i + \sum_{i \in N} (1 - x_i) \geq 1.$$

Rules: *Axioms, Linear Combination, Cut Rule*
$x \geq 0$, $-x \geq -1$

$$\frac{\sum \lambda_i^1 x_i \geq t_1 \qquad \cdots \qquad \sum \lambda_i^k x_i \geq t_k}{\sum \left(\sum_j s_j \lambda_i^j \right) x_i \geq \sum_j s_j t_j} \qquad \text{and} \qquad \frac{\sum s \lambda_i x_i \geq t}{\sum \lambda_i x_i \geq \lceil t/s \rceil}$$

where $s_1, \ldots, s_k$ and s must be strictly positive integers, and the linear combination rule can take any number of premises.

Refuting CNFs in CP

An example of CP derivation

$$\dfrac{\dfrac{\dfrac{x + y \geq 1 \qquad x + (1 - y) \geq 1}{2x \geq 1}}{x \geq 1} \qquad \dfrac{\dfrac{(1 - x) + y \geq 1 \qquad (1 - x) + (1 - y) \geq 1}{-2x \geq -1}}{-x \geq 0}}{0 \geq 1}$$

Memory configurations

A *memory configuration M* is a set of linear inequalities.

A *CP derivation of I from F* is given by a sequence $M_0, \ldots, M_\ell$ of *memory configurations*

The sequence must satisfy that :

- M_0 is empty,
- that $I \in M_\ell$, and that
- for each $i < \ell$, M_{i+1} is obtained from M_i in one of three ways:
  - **Axiom download**: $M_{i+1} = M_i \cup \{J\}$ for some $J \in F$
  - **Inference**: $M_{i+1} = M_i \cup \{J\}$ where J follows from M_i by an inference rule, or is a Boolean axiom
  - **Erasure**: $M_{i+1} \subset M_i$.

A *CP refutation of F* is a *CP* derivation of $0 \geq 1$ from F.

Space measures

Three measures of the space taken by a memory configuration M.

- The **inequality space** is the number of inequalities in M.
- The **variable space** is the sum, over all inequalities J in M, of the number of distinct variables appearing in J with a non-zero coefficient.
- the **total space**, the sum, over all inequalities J in M, of the length in binary of all non-zero coefficients in J and of the constant term of J (ignoring signs).

For each measure, the corresponding space of a refutation Π is the *maximum* space of any configuration M_i in Π. The corresponding space needed to refute a set of inequalities F is the *minimum* space of any refutation of F.

Space Complexity for Resolution

A memory configuration M contains *clauses* instead of linear inequalities.

- The **clause space** is the number of clauses in M.
- The **total space** is the overall number of variables (with repetitions) appearing in M

Many works studying clause space for Resolution. n number of vars.

- several $\Omega(n)$ lower bounds (PHP, random 3CNFs,.....) [ET99,ABRW00,....]
- straightforward $n+1$ upper bound.

Few works exploring total space for Resolution.

- $\Omega(n^2)$ lower bounds (PHP [ABRW00], random k-CNFs [BGT14, BBGHMW15]))
- straightforward $O(n^2)$ upper bound.

Res vs CP

Focus on *proof size* to compare proof strength of CP and Res.

- CP efficiently simulates Resolution (see example).
- CP is exponentially stronger than Resolution: PHP ha poly size CP proofs, but requires exp size proofs in Resolution

Almost no result for space in CP

Göös and Pitassi [GP14] give a family of CNFs of size m which cannot simultaneously be refuted with small inequality space and small length — the space s and length ℓ of every CP refutation must satisfy $s \log \ell \geq m^{1/4-o(1)}$.

No explicit lower bound, no explicit upper bound was known so far.

Contradictions

The *complete tree contradiction* CT_n is a CNF in n variables $x_0, \ldots, x_{n-1}$, with 2^n clauses. For each assignment α, it contains the clause

$$\bigvee_{i \in Z} x_i \vee \bigvee_{i \in A} \neg x_i$$

where $A = \{i : \alpha(x_i) = 1\}$ and $Z = \{i : \alpha(x_i) = 0\}$. This clause is falsified by α and by no other assignment.

The *pigeonhole principle* PHP_n

- $x_{ij} + x_{i'j} \leq 1$, $i \neq i' < n+1, j < n$. (injectivity)
- $\sum_{j<n} x_{ij} \geq 1$, $i < n+1$. (totality)

Results for cutting planes

Theorem

CT_n has a CP refutation with inequality space 5.

Observations

- In *Res* and *PCR*, CT_n requires (clause and monomial space) $\Omega(n)$
- proof uses coefficients of value $O(2^n)$

Consequences

1. Any set of linear unsatisfiable linear inequalities (in particular UNSAT CNFs) has proof of **inequality space** 5.
2. $O(n^2)$ **total space** is sufficient to refute any unsatisfiable set of linear inequalities[1]
3. any UNSAT set $\mathcal{L}$ of linear inequalities over n variables, with max coefficient M, can refuted using **coefficients of value** bounded by $\max\{L, 2^n\}$
4. any UNSAT set $\mathcal{L}$ of linear inequalities over n variables can be refuted in **variable space** $O(n)$

[1] Notice that, restricted to CNFs, the upper bound follows from the $O(n^2)$ upper bound for total space in resolution

Consequences

Proposition

Let F be an unsatisfiable CNF. The minimal width of refuting F in resolution is at most the variable space of refuting F in CP.

Use *Res* width lower bounds to get optimality for variable space.

Theorem

With high probability the variable space of refuting a random k-CNF in CP is $\Theta(n)$.

Cutting planes with bounded coefficients

CP^k: coefficients bounded in absolute value by k.

Theorem (CCT)

CP^2 is exponentially stronger than Res.

Proof

- PHP_n has poly size CP^2 proofs.
- CP^2 p-simulates Res

Known proofs of PHP_n either use constant space and linear coefficients, or $O(\log n)$*spaceandconstantcoefficients*

Results for cutting planes with bounded coefficients

Theorem

PHP_n has polynomial size CP^2 refutations with inequality space 5.

Theorem

For any constant $k \in \mathbb{N}$, the complete tree contradiction CT_n requires inequality space $\Omega(\log \log \log n)$ to refute in CP^k.

Proof sketch for CT_n upper bound

Theorem

CT_n has a CP refutation with inequality space 5.

Obs: let $b \geq 1$. In space 3,

$$\frac{\frac{\sum_{i \in S} \lambda_i x_i + \sum_{i \in T} \lambda_i (1 - x_i) \geq b}{\vdots}}{\sum_{i \in S} x_i + \sum_{i \in T} (1 - x_i) \geq 1}.$$

Proof

- $c \geq \max\{b, \lambda_i\}$.
- Add $(c - \lambda_i) x_i \geq 0$ to the inequality for each $i \in S$
- Add $(c - \lambda_i)(1 - x_i) \geq 0$ for each $i \in T$.
- Divide by c and round.

Proof sketch for CT_n upper bound

Let $a < 2^n$. Then $(a)_0, \ldots, (a)_{n-1}$ for the bits of the binary expansion of a, so that $a = \sum 2^i (a)_i$.

I_b for the clause of CT_n which is falsified exactly by the assignment $x_i \mapsto (b)_i$.

For $a \in \mathbb{N}$, define the inequality T_a as

$$T_a : \sum 2^i x_i \geq a.$$

The assignments falsifying T_a are exactly those lexicographically strictly less than a. In other words, T_a is equivalent to the conjunction of the inequalities I_b over all $b < a$,

Proof sketch for CT_n upper bound

Claim

For $a < 2^n$, in space 5

$$T_a, I_a \vdash T_{a+1}$$

.

Then we proceed deriving $T_0, T_1, T_2, \ldots, T_{2^n-1}$ and finally deriving a contradiction from T_{2^n-1} and I_{2^n-1}.

Proof sketch for CT_n upper bound

For the inductive step, fix $a < 2^n$. Let

$$A = \{i < n : (a)_i = 1\} \qquad Z = \{i < n : (a)_i = 0\}$$

. Define two inequalities

$$M_a : \sum_{i \in Z} x_i \geq 1 \qquad\qquad L_a^k : \; x_k + \sum_{\substack{i > k \\ i \in Z}} x_i \geq 1, \quad k \in A.$$

Obs if $\beta \geq a$, then β satisfies L_a^k for each $k \in A$. If $\beta > a$, then β also satisfies M_a.

Proof sketch for CT_n upper bound

In space at most 5:

Claim 1 $T_a, I_a \vdash M_a$

Claim 2 $T_a \vdash L_a^k$, for any $k \in A$.

Using these two claims, we can then show

Claim 3 We can derive T_{a+1} from T_a and I_a in space 4.

Claim 1

$I_a = \sum_{i \in Z} x_i + \sum_{i \in A} (1 - x_i) \geq 1.$

From Axioms get:

$$\sum_{i \in Z} (2^i - 1) x_i \geq 0 \qquad \text{and} \qquad \sum_{i \in A} (2^i - 1)(1 - x_i) \geq 0.$$

Sum axioms with T_a, and I_a and get

$$2 \sum_{i \in Z} 2^i x_i \geq 1.$$

Use **Obs** to get M_a

Claim 2

Rearrangements of T_a, plus axioms multiplied by the right coefficients plus **Obs**

Claim 3

- Write M_a in the REG1
- For each $k \in A$, we use Claim 2 to write L_a^k in REG2, and then multiply it by 2^k, giving

$$2^k x_k + 2^k \sum_{\substack{i>k \\ i \in Z}} x_i \geq 2^k.$$

- Repeat for each $k \in A$ in turn, each time adding the result to REG1. At the end of this process, REG 1 contains the inequality

$$\sum_{k \in A} 2^k x_k + \sum_{i \in Z} \left(\sum_{\substack{k<i \\ k \in A}} 2^k \right) x_i + \sum_{i \in Z} x_i \geq 1 + \sum_{k \in A} 2^k.$$

- Right hand side is $a + 1$. Use axioms multiplied by the right coefficients to get T_{a+1}

PHP_n using space 5 in CP^2

Standard proofs of the PHP_n

1. from axioms $x_{ij} + x_{i'j} \leq 1$ derive for all $j < n$

$$\sum_{i<n+1} x_{ij} \leq 1$$

2. sum over all $j < n$ getting: $\sum_{j<n} \sum_{i<n+1} x_{ij} < n$
3. sum for all $i < n + 1$ the axioms $\sum_{j<n} x_{ij} \geq 1$ getting: $\sum_{j<n} \sum_{i<n+1} x_{ij} \geq n$

Claim: space efficient sum

Claim

Given inequalities $y_i + y_j \leq 1$ for all $i < j \leq n$, we can derive $\sum_{i=1}^{n} y_i \leq 1$ in polynomial size and in space 4, using coefficients bounded by 2.

Derive $y_0 + \cdots + y_k \leq 1$ by induction on k

- Keep in REG 1 $y_0 + \cdots + y_k \leq 1$
- derive by induction on $i \leq k$, $y_0 + \cdots + y_i + y_{k+1} \leq 1$
  - base: axiom
  - ind: $y_0 + \cdots + y_i + y_{k+1} \leq 1$ [in REG 2]
  - $y_{i+1} + y_{k+1} \leq 1$ [AX]
  - $y_0 + \cdots + y_{i+1} \leq 1$ [weakening REG 1]
  - $y_0 + \cdots + y_{i+1} + y_{k+1}$ [sum + div by 2]

lower bound for CT_n

Main ideas

- charecterise classes of falsifying assignments for small space configurations of linear inequalites with bounded coefficients. If number coeff is small then we can upper bound the number assignments, but the characterization still give raise to many possible assignments.
- group together terms with the same coefficient
- counting argument

lower bound for CT_n

Definition

Call a set A of assignments s-symmetric if there is a partition of the variables into s or fewer blocks, such that A is closed under every permutation which preserves all blocks.

Example: 2-simmetric set of assignments
Variables partitioned in two sets as

$$\{\{x_1, x_2\}, \{x_3, x_4, x_5\}\}$$

$$A = \{[1, 0, 0, 0, 0], [0, 1, 0, 0, 0]\}$$

Idea of Partition: Variables with the same coefficient in the same element

lower bound for CT_n

Lemma

- *If I is as linear inequality with no more than b different coefficients, then the set of assignments falsifying I is b-symmetric.*
- *Suppose M contains c linear inequalities, such that no more than b different coefficients appear in any inequality. Then the set of assignments falsifying M is b^c-symmetric.*

Proof For the first part, the inequality I has the form

$$\lambda_1 \sum_{i \in B_1} x_i + \cdots + \lambda_b \sum_{i \in B_b} x_i \geq t.$$

The b-symmetry is witnessed by the blocks $B_1, \ldots, B_b$. For the second part, take the common refinement of the partitions for all of the inequalities in M.

lower bound for CT_n

- Suppose that CT_n has a *CP* refutation $M_1, \ldots, M_N$ in space *c*, in which no more than *b* different coefficients appear in any inequality.
- Let A_i be the set of assignments falsifying the *i*th configuration.
- Then $A_1, \ldots, A_N$ is a sequence of b^c-symmetric assignments, beginning with the empty set and ending with the set of all assignments, such that for each $i < N$ either $A_{i+1} \subseteq A_i$ or $A_{i+1} = A_i \cup \{\alpha\}$ for some assignment α.

k-assignments

k-assignment: contains exactly k ones and the rest to 0.

$S(s,k) = \{|A| : A \text{ is an } s\text{-symmetric set of } k\text{-assignments}\}$.

Lemma

$|S(s,k)| < n^s 2^{k^s}$.

Main theorem

Theorem

For $n \geq 2$, suppose that CT_n has a CP refutation in space c, in which no more than b different coefficients appear in any inequality. Then $b^c \geq \sqrt{\log \log n}$.

Proof Let $s = b^c$

- $A_1, \ldots, A_N$ be the sequence of s-symmetric assignments
- $A'_1, \ldots, A'_N$ be the sequence $A_1, \ldots, A_N$ restricted to k-assignments
- Then A'_1 is empty, A'_N consists of all k-assignments, and for each $i < N$ either $A'_{i+1} \subseteq A'_i$ or $A'_{i+1} = A'_i \cup \{\alpha\}$ for some k-assignment α.
- It follows that the sequence $|A'_1|, \ldots, |A'_N|$ must contain every number between 0 and $\binom{n}{k}$.
- Since each A'_i is still s-symmetric, this in particular means that for every number m between 0 and $\binom{n}{k}$, there is at least one s-symmetric set A of k-assignments with $|A| = m$.

It follows by the Lemma that $\binom{n}{k} < n^s 2^{k^s}$.
Contradiction if $k = 2^s$ and $s < \sqrt{\log \log n}$.

Focused open problems

A general problem is about the trade-off between inequality space and the size of coefficients.

- *Problem 1.* Can every unsatisfiable CNF be refuted in *CP* in constant space, if the coefficients are polynomially bounded?
- *Problem 2.* Can every unsatisfiable CNF be refuted in *CP* in linear total space?
- *Problem 3.* Prove a better space lower bound for CP^2.