Lecture 6— Cutting planes proofs

Massimo Lauria — lauria.massimo@gmail.com
Office 1107, Ookayama West 8th Building

Friday — November 13th, 2015 (This document was updated on June 21, 2017)

We introduce cutting planes, a proof system originally devised for integer programming. We explain how to use the interpolation method to prove lower bounds for cutting planes, and we prove a lower bound for the clique-coloring formula.

Cutting planes proof system

We can express decisions problems like SAT by the means of *integer programs*. In this lecture we discuss a proof system that witness their unsatisfiability: cutting planes.[1]. In this proof system we go back to the natural encoding of true as 1 and false as 0.[2] First we translate any clause into a linear inequality with integer coefficients. The clause

$$x \vee \bar{y} \vee \bar{z} \vee u \tag{1}$$

for example translates into

$$x + (1 - y) + (1 - z) + u \geq 1 \tag{2}$$

or equivalently

$$x - y - z + u \geq -1 \tag{3}$$

which has a solution over $\{0,1\}$ values if and only if the clause is satisfied. Therefore an integer program that encodes a CNF has the form of

$$\begin{aligned} &Ax \geq b \\ &x_i \in \{0,1\} \text{ for every } i; \end{aligned}$$

where the matrix A has only integer values. There is no **known** efficient algorithm that solves integer programs; a viable strategy is to *relax* the integer programs to something easier to manage. In this case we consider linear programs.[3]

In cutting planes we transform in the most naive way the integral constraints into fractional linear constraints (i.e. $x_i \in \{0,1\}$ into $0 \leq x_i \leq 1$) and leave the other constraints alone. Once we relax the integer program we have a lot of new fractional solutions that were not allowed before. Consider, for example, the program that asks for an independent set of size 2 in the complete graph of 4 vertices.

[1] William Cook, Collette R. Coullard, and György Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987

[2] This is the inverse of the encoding in polynomial calculus.

[3] Jiří Matoušek and Bernd Gärtner. *Understanding and using linear programming*. Springer, 2007

$$
\begin{aligned}
&x_1 + x_2 + x_3 + x_4 \geq 2\\
&x_1 + x_2 \leq 1\\
&x_1 + x_3 \leq 1\\
&x_1 + x_4 \leq 1\\
&x_2 + x_3 \leq 1\\
&x_2 + x_4 \leq 1\\
&x_3 + x_4 \leq 1\\
&x_1 \in \{0,1\},\ x_2 \in \{0,1\},\ x_3 \in \{0,1\},\ x_3 \in \{0,1\}.
\end{aligned}
$$

The program has no *integer solution* but if we relax the constraints and allow $0 \leq x_i \leq 1$, then the linear program has a *fractional solution* by setting all variables to $\frac{1}{2}$. Cutting planes rule must be such that we can get rid of of suprious fractional solutions.[4]

[4] We can formally think that proof lines are inequalities in the standard form $a^T x \geq \gamma$, but we will use other form as $a^T x \leq \gamma$, $a^T x = \gamma$ or even $\gamma' \leq a^T x \geq \gamma$. Each such form can be easily written as one or two inequalities in standard form.

Boolean axiom $\dfrac{}{x_i \leq 1}$ and $\dfrac{}{x_i \geq 0}$ for some $i \in [n]$;

Initial axiom $\dfrac{}{\sum a_i x_i \geq \gamma}$ the encoding of some clauses of the CNF;

Combination $\dfrac{\sum_i a_i x_i \geq \gamma \qquad \sum_i b_i x_i \geq \delta}{\sum_i (\alpha a_i + \beta b_i) x_i \geq \alpha\gamma + \beta\delta}$ for some non negative integers α, β;

Division and rounding $\dfrac{\sum a_i x_i \geq \gamma}{\sum \frac{a_i}{c} x_i \geq \lceil \frac{\gamma}{c} \rceil}$ for some positive integer c that divides all a_i.

The division and rounding strengthen the inequality, and indeed there may be feasible fractional solutions of the linear program that are removed by the new improved inequality. The rationale behind the rule is that since the coefficients on the left side are integer and all the variables have values in $\{0,1\}$, then the left side must have integer value as well and therefore we can round up the right side without removing any integer solution. Such integer cuts were introduced by Gomory[5] to solve integer programs. The idea is first to find a feasible solution, maybe with the simplex method. If the solution is not integer, it can be cut with an application of division and rounding rule, and the search may continue. (See Figure 1.)

[5] Ralph E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64(5):275–278, 1958

Definition 1. *The* length *of a cutting planes derivation is the number its lines. The* rank *of a cutting planes refutation is as follows*

- *the rank of axioms is* 0*;*
- *the rank of an inequality obtained by combination is the maximum rank among the premises;*
- *the rank of an inequality obtained by division and rounding is one more than the rank of its premise.*

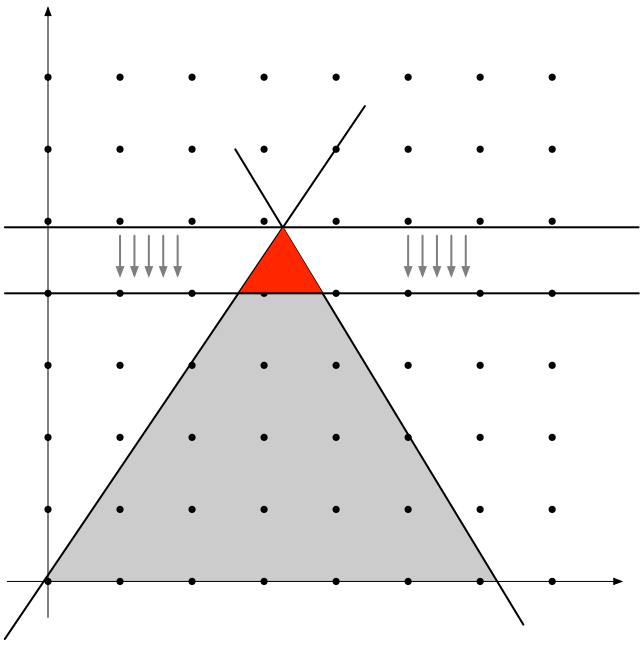

Figure 1: The effect of a Gomory integer cut, i.e. a division and rounding step. The red part does not contain any integer solution and is removed by the polytope.

The size *of a cutting planes derivation is the sum, among all inequalities and all coefficients in the derivation, of the length of they binary representation.*[6] *A refutation in cutting planes is a derivation of* $0 \geq 1$.

[6] We won't discuss too much about the size of coefficients in this lecture, but it is indeed an important issue in cutting planes proofs.

Exercise 2. Show that any resolution refutation of size s for a formula of n variables can be translated in a cutting plane refutation of size $O(ns)$.

Exercise 3. Consider the set of inequalities

$$x_i + x_j \leq 1 \quad \text{for } 1 \leq i < j \leq n. \tag{4}$$

Show how to derive the inequality

$$\sum_{i=1}^{n} x_i \leq 1\,. \tag{5}$$

in length $O(n^2)$.

Exercise 4. Try to solve the previous exercise with a derivation of rank $O(\log n)$. Any proof length is fine.

The relaxed linear program defines a bounded polytope $\mathcal{P} \subseteq [0,1]^n$. All inequalities derived by combination rule are valid for $\mathcal{P}$ too, but every time we use the rounding rule we cut away part of the polytope. In the end we produce a sequence

$$\mathcal{P} \supseteq \mathcal{P}_1 \supseteq \mathcal{P}_2 \ldots \mathcal{P}_\ell = \emptyset. \tag{6}$$

Interpolation method

We are going to show a lower bound for cutting planes proofs, due to Pudlák.[7] This is essentially the only lower bounds know for general cutting planes proofs. Lower bound for restricted version of cutting planes were proved already in[8]. Consider an unsatisfiable formula on three sets of variables x, y, z of the form

$$A(x,y) \wedge B(x,z) \ . \tag{7}$$

For every assignment $\vec{v}$ to the x variables it must be the case that either $A(\vec{v},y)$ or $B(\vec{v},z)$ is unsatisfiable (or both).

Definition 5. *Given a formula $A(x,y) \wedge B(x,z)$, a function $I(x)$ with $\{0,1\}$ values* interpolates *the formula if for for every assignment $\vec{v}$,*

$$I(\vec{v}) = \begin{cases} 0 & \textit{implies } A(\vec{v},y) \textit{ is unsatisfiable;} \\ 1 & \textit{implies } B(\vec{v},z) \textit{ is unsatisfiable.} \end{cases} \tag{8}$$

Essentially

$$A(x,y) \longrightarrow I(x) \longrightarrow \neg B(x,z) \ . \tag{9}$$

The formula that interests us is the clique-coloring formula, which claims that a graph of n has simultaneously a $(k-1)$-coloring and a k-clique, for the specific value of $k = \lfloor \frac{1}{8}(n \log n)^{2/3} \rfloor$.

$$F_n = \mathrm{Clique}_n(x,y) \wedge \mathrm{Color}_n(x,z) \tag{10}$$

where x_{ij} are $\binom{n}{2}$ variables that encode the edges of a graph; y_i encode the k-clique; $z_{i,c}$ are $[k-1] \times [n]$ variables that encode a $(k-1)$-coloring for the graph x.

The formula Clique_n is a conjunction of the following inequalities

$$\sum_{i \in [n]} y_i = k \tag{11}$$

$$x_{ij} \geq y_i + y_j - 1 \ . \tag{12}$$

The formula Color_n is a conjunction of the following inequalities

$$\sum_{c \in [k-1]} z_{i,c} = 1 \qquad \text{for every } i \in [n]; \tag{13}$$

$$x_{i_1,i_2} + z_{i_1,c} + z_{i_2,c} \leq 2 \qquad \text{for every } c \in [k-1], i_1 < i_2 \in [n]. \tag{14}$$

Exercise 6. Show that the interpolant for this formula, given the $\binom{n}{2}$ variables x_{ij} that encode a graph, outputs 0 if the graph is $k-1$ colorable, and outputs 1 if the graph contains a k-clique.

Next theorem, due to Pudlak (1997)[9] show that such interpolant has no monotone real circuit of small size.

Definition 7. *A* monotone real circuit *is a circuit that takes an input in $\mathbb{R}^n$ and it is a composition of binary and unary non decreasing functions. A monotone real circuit computes a boolean function f if is has the same values on $\{0,1\}^n$.*

[7] Pavel Pudlák. Lower bounds for Resolution and Cutting Plane proofs and monotone computations. *Journal of Symbolic Logic*, 62(3):981–998, 1997

[8] Russell Impagliazzo, Toniann Pitassi, and Alasdair Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Logic in Computer Science, 1994. LICS'94. Proceedings., Symposium on*, pages 220–228. IEEE, 1994; and Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. Lower bounds for cutting planes proofs with small coefficients. *The Journal of Symbolic Logic*, 62(3):pp. 708–728, 1997

[9] Pavel Pudlák. Lower bounds for Resolution and Cutting Plane proofs and monotone computations. *Journal of Symbolic Logic*, 62(3):981–998, 1997

Theorem 8 (Pudlak, 1997)**.** *Let $f\colon \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ be a monotone boolean function which is 0 on all $k-1$-colorable graphs and is 1 on all graphs with a k-clique, with $k = \lfloor (n/\log n)^{2/3}/8 \rfloor$. Then every monotone real circuit computing f has size $2^{\Omega(n/\log n)^{1/3}}$.*

Monotone interpolation of cutting planes

The interpolation method to prove proof system lower bounds is due to Krajíček [10] and follows the intuition that from a proof it is sometime possible to efficiently extract some computation. If that computation is unfeasible, then the proof must be long.

[10] Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997

Lemma 9. *Consider an unsatisfiable integer program*

$$\begin{aligned} Ax + By &\geq \Gamma \\ Cx + Dz &\geq \Gamma' \end{aligned}$$

$$x_i \in \{0,1\} \quad y_i \in \{0,1\} \quad z_i \in \{0,1\}$$

in which C has only non positive entries and that has a cutting planes refutation of length ℓ. Then there is a monotone real circuit *of size $O(\ell)$ that computes the interpolant $I(x)$ of the program.*

Proof sketch. We split the refutation in two derivation, one from formula $Ax + By \geq \Gamma$ and one from formula $Cx + Dz \geq \Gamma'$. Each line in one each of the two derivations corresponds to a line in the original one, obtained with the same inference. For each line in the cutting planes proof[11]

[11] For convenience we put the x variables on the right side.

$$b^T y + c^T z \geq \gamma - a^T x \tag{15}$$

we associate two lines

$$b^T y \geq \gamma_1 - a_1^T x \qquad c^T z \geq \gamma_2 - a_2^T x \tag{16}$$

so that for every $\vec{v}$ it holds that

$$(\gamma_1 - a_1^T \vec{v}) + (\gamma_2 - a_2^T \vec{v}) \geq \gamma - a^T \vec{v}\,. \tag{17}$$

At the end of the proof $\gamma - a^T \vec{v} = 1$ therefore either $(\gamma_1 - a_1^T \vec{v})$ or $(\gamma_2 - a_2^T \vec{v})$ is strictly positive. This means that the proof on that side is actually a refutation.

To prove the lemma we need to show we can compute $\gamma_2 - a_2^T x$ with a monotone real gates applied to the values computed at previous steps or to the input. Notice that since matrix C is non positive, at the axiom download step $\gamma_2 - a_2^T x$ is a non decreasing function. After showing that for every to monotone gate used at every step we get a valid interpolant for the initial formula. Indeed if $\gamma_2 = a_2^T x$ is positive (e.g. greater than $1/2$) then the right side or the decomposition is a valid refutation for $B(x,z)$. □

Corollary 10. *Any cutting planes refutation of F_n has length $2^{\Omega(\sqrt[3]{n/\log n})}$.*

Proof. The interpolant of formula F_n can be computed as a monotone real circuit of size proportional to the size of its cutting planes refutation by Lemma 9, because the x variable occur on the Clique_n formula all non positive, if written in standard form. Observe that for every assignment of variables x, if x has a k-clique, then Color_n is unsatisfiable and Clique_n is not, so the interpolant outputs 1, vice versa if the graph is $(k-1)$-colorable, then Clique_n is unsatisfiable and Color_n is not. Theorem 8 gives the result. □

Exercise 11. Observe that the lower bound only depends on the coefficients of variable x_i in F_n. In particular look at Equations (11) and (13) and show that if the same equations are encoded differently (maybe with additional variables), the result holds the same as long the new encoding does not use variables x_i.

Exercise 12. Show that there exists a 3-CNF that has no cutting planes refutation of polynomial size.

References

[BPR97] Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. Lower bounds for cutting planes proofs with small coefficients. *The Journal of Symbolic Logic*, 62(3):pp. 708–728, 1997.

[CCT87] William Cook, Collette R. Coullard, and György Turán. On the complexity of cutting-plane proofs. *Discrete Applied Mathematics*, 18(1):25–38, 1987.

[Gom58] Ralph E. Gomory. Outline of an algorithm for integer solutions to linear programs. *Bulletin of the American Mathematical Society*, 64(5):275–278, 1958.

[IPU94] Russell Impagliazzo, Toniann Pitassi, and Alasdair Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Logic in Computer Science, 1994. LICS'94. Proceedings., Symposium on*, pages 220–228. IEEE, 1994.

[Kra97] Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.

[MG07] Jiří Matoušek and Bernd Gärtner. *Understanding and using linear programming*. Springer, 2007.

[Pud97] Pavel Pudlák. Lower bounds for Resolution and Cutting Plane proofs and monotone computations. *Journal of Symbolic Logic*, 62(3):981–998, 1997.