8. Sum of squares lower bounds for 3-SAT and 3-XOR Part 2/2.

http://www.csc.kth.se/~lauria/sos14/

Lecturer: Massimo Lauria

Disclaimer: this lecture note has not yet been reviewed by the main lecturer. It is released as it is for the convenience of the students.

The whole lecture is devote to show that if a k-XOR formula ϕ requires degree D refutations in Binomial Calculus (BC), then it requires degree $D/2$ Positivstellensatz Calculus refutations ($\mathsf{PC}_>$).

Lemma 1. *Assume that*

$$f = \sum_i \alpha_i (t_i - t'_i) \tag{1}$$

where $(t_i - t'_i)$ has a BC refutation of degree d, then f can be written as

$$f = \sum_i \beta_i (s_i - s'_i)$$

where for each i $(s_i - s'_i)$ has a BC refutation of degree d and all monomials in the terms $\{s_i, s'_i\}_i$ are in f.

Proof. Assume that some monomial m appears in the RHS of (1) but not in f. We show that we can prune that monomial from the sum without affecting f. Hence, repeating this process we end with the desired expression. To show how the pruning works consider the sum S_m of all terms of the RHS of equation (1) containing m:

$$S_m = \sum_{j \in A} \alpha_j (m - t'_j).$$

Wlog each t'_j in the sum above is not containing m. Moreover as m doesn't appear in f it m must be canceled out, that is $\sum_{j \in A} \alpha_j = 0$. Fix $i \in A$ such that t'_i is one of the t'_j of the equation above.

Then

$$S_m = \sum_{j \in A} \alpha_j m - \sum_{j \in A} \alpha_j t'_j \overset{\sum_{j \in A} \alpha_j = 0}{=} \sum_{j \in A} \alpha_j t'_i - \sum_{j \in A} \alpha_j t'_j = \sum_{j \in A} \alpha_j (t'_i - t'_j).$$

Moreover $(t'_i - t'_j)$ for each $j \in A$ can be derived in BC using degree at most d as by hypothesis both $(m - t'_i)$ and $(m - t'_j)$ can be derived in BC using degree at most d. Hence we showed how to prune m from the RHS of (1). □

Corollary 2. *If $f = 0$ is deduced in degree d by the equational part of $\mathsf{PC}_>$ then $f = \sum_j \alpha_j (t_j - t'_j)$, where each $(t_j - t'_j)$ has a derivation in degree d in BC and there are no cancelations.*

Proof. By induction. At the beginning of the $\mathsf{PC}_>$ we have binomials. Then at each inference step apply Lemma 1. □

Theorem 3. *Given a k-XOR formula ϕ. If the minimum degree to refute the binomial encoding of ϕ in Binomial Calculus (BC) is D, then the minimum degree to refute the polynomial encoding of ϕ in Positivstellensatz Calculus ($\mathsf{PC}_>$) is at least $D/2$.*

Proof. Suppose by contradiction that there exists a proof of degree $d < D/2$ of the polynomial encoding P of ϕ in $\mathsf{PC}_>$. That is we have an equation of the form

$$p' = 1 + \sum_j h_j^2, \tag{2}$$

where $p' = 0$ is inferred from P according to the inference rules of $\mathsf{PC}_>$. By applying Corollary 2 wlog we can suppose that $p' = \sum_i \alpha_i (t_i - t_i')$, where each $(t_j - t_j')$ has a BC derivation in degree d and there are no cancelations.

Observe that for each j $\deg(h_j^2) \leq d$[1] , and not just $\deg(\sum_j h_j^2) \leq d$.

Let us consider the linear operator $L : \mathbb{R}[Y] \to \mathbb{R}$ defined as follows: $L(1) = 1$ and for each monomial m

$$L(m) := \begin{cases} \alpha & \text{if } m - \alpha \text{ with } \alpha \in \mathbb{R} \text{ has a BC proof from } P \text{ of degree} \leq d, \\ 0 & \text{otherwise.} \end{cases}$$

If we look just at monomials (and polynomials) of degree at most d this operator is well defined and moreover in that case $L(m) \in \{-1, 0, 1\}$. In fact otherwise we could build the following BC refutation of P: start with a BC derivation of $m = a$, for some $a \in \mathbb{R} \setminus \{-1, 1\}$, of degree $d < D/2$. Then take squares: $m^2 = a^2$, but as in the encoding P of ϕ we have the equations $y_i^2 = 1$ for each variable $y_i \in Y$ then $m^2 = 1$. Hence we would have derived $a^2 = 1$, ie a BC refutation of P of degree $2d < D$. That is not possible, as D is the minimal degree needed to refute P in BC.

In order to apply L to equation (2) we want to prove the followings:

1. if $t - t'$ has a BC derivation of degree at most d from P then $L(t - t') = 0$;
2. for each polynomial $p \in \mathbb{R}[Y]$ of degree at most $d/2$ $L(p^2) \geq 0$.

Then, from equation (2), it follows an immediate contradiction

$$0 = L(p') = 1 + \sum_j L(h_j^2) \geq 1.$$

Property 1 is obvious: consider $am - a'm' = 0$. If we can prove in BC that $m = \alpha$, we can always by transitivity do the same for m'.

The rest of the proof is devoted to prove property 2: as $L(y^2 m) = L(m)$ we can focus on $p \in \mathbb{R}[Y]$ over multilinear monomials. Let $p = \sum_{S \subseteq [n]} \alpha_S y_S$, where $y_S := \prod_{i \in S} y_i$. Then

$$L(p^2) = \sum_{S,T} \alpha_S \alpha_T L(y_S y_T) = \sum_{S,T} \alpha_S \alpha_T L(y_{S \Delta T}). \tag{3}$$

Define now an undirected graph $G = (V, E)$ with vertex set the y_S with S appearing in p and $(y_S, y_T) \in E$ iff $L(y_{S\Delta T}) = \pm 1$. Then L induce a natural labeling mapping E into $\{-1, 1\}$. Notice that for each $S \subseteq [n]$ (y_S, y_S) is always in E as $L(y_{S\Delta S}) = L(1) = 1$.

Moreover if BC derives $y_{S\Delta T} = \pm 1$ and $y_{T\Delta U} = \pm 1$ in degree d then using inference BC derives in degree d $y_{S\Delta U} = \pm 1$: every connected component of G is a clique. Moreover each connected component of G can be split into two vertex sets A, B such that for each I, J in the same vertex set $L(y_{I\Delta J}) = 1$ and for $I \in A$ $J \in B$ $L(y_{I\Delta J}) = -1$.

[1] By contradiction suppose that for some j $\deg(h_j^2) > d$, then the leading term of h_j can't cancel out in the sum $\sum_j h_j^2$, hence it should appear also in p'. But this is not possible as all monomials in p' have degree not greater than d.

To prove the last statement it is sufficient to prove that for each triangle the product of the values of the labeling of its edges is 1. Let $\{y_S, y_T, y_U\}$ be the vertexes of a triangle in G, then

$$L(y_{S\Delta T})L(y_{T\Delta U})L(y_{S\Delta U}) = L(y_\emptyset) = L(1) = 1.$$

We prove a stronger result than $L(p^2) \geq 0$: we prove that this is true wrt every connected component of G. More precisely let $\mathcal{S}$ be a sub-polinomial of the RHS of equation (3) giving rise in G to a connected component and let A and B as above. We show that $\mathcal{S} \geq 0$. From this will follow immediately that $L(p^2) \geq 0$.

$$\begin{aligned}\mathcal{S} = \sum_{I,J\in A} \alpha_I\alpha_J L(y_{I\Delta J}) + \sum_{I,J\in B} \alpha_I\alpha_J L(y_{I\Delta J}) + \sum_{I\in A, J\in B} 2\alpha_I\alpha_J L(y_{I\Delta J}) = \\ = \sum_{I,J\in A} \alpha_I\alpha_J + \sum_{I,J\in B} \alpha_I\alpha_J - \sum_{I\in A, J\in B} 2\alpha_I\alpha_J = \\ = \left(\sum_{I\in A} \alpha_I\right)^2 + \left(\sum_{J\in B} \alpha_J\right)^2 - \sum_{I\in A, J\in B} 2\alpha_I\alpha_J = \\ = \left(\sum_{I\in A} \alpha_I - \sum_{J\in B} \alpha_J\right)^2 \geq 0.\end{aligned}$$

□

References