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

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

Lecturer: Massimo Lauria

This 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 ($\mathsf{PC}_>$). In the last lecture we already showed that for a random k-XOR formula the required degree D is large, therefore this part will conclude the proof of the lower bound for the degree of $\mathsf{PC}_>$ refutations of random k-XORs.

The content of this lecture completes the proof of the following theorem, started in the previous lecture.

Theorem 1. *For each $k \geq 3$ and $\delta > 0$ there exists α, such that a random k-XOR formula ϕ in n variables and Δn clauses, where $\Delta \geq 1 + \frac{\ln 2}{2\delta^2}$, with high probability has the following properties:*

1. *At most $\left(\frac{1}{2} + \delta\right) \Delta n$ parity constraints of ϕ can be simultaneously satisfied,*
2. *any $\mathsf{PC}_>$ refutation of ϕ requires degree αn.*

In the previous lecture we showed that any Binomial Calculus refutation of the random k-XOR requires degree $\Omega(n)$ with high probability, and the missing piece that we will discuss in this lecture is the fact that the Binomial Calculus is, up to a factor 2, equivalent to $\mathsf{PC}_>$ with respect to degree. The main reason algebraic proofs are powerful is that it is possible to make use of monomial cancellation. The following lemma from [BGIP01] shows that cancellations do not help in binomial calculus.

Lemma 2. *Assume that*

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

where each $(t_i - t'_i) = 0$ has a BC proof of degree d, then f can be written as

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

where for each i, binomial equation $(s_i - s'_i) = 0$ has a BC proof of degree d and all monomials in the terms $\{s_i, s'_i\}_i$ occur with non-zero coefficients in the polynomial 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:

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

Without loss of generality each t'_j in the sum above is different from m. Moreover, as m does not appear in f, it must hold that $\sum_{j\in A}\alpha_j = 0$. Fix some $i \in A$.

Then

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

Where the second equality holds because $\sum_{j\in A}\alpha_j = 0$.

Notice that each $(t'_i - t'_j) = 0$ is a linear combination of $(m - t'_i) = 0$ and $(m - t'_j) = 0$ that can be both be derived in BC using degree at most d, by hypothesis. Hence we showed how to prune m from the RHS of (1), without introducing any new monomial. In order to get the result we prune all monomials that are not in f from (1). □

Corollary 3. *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 we apply Lemma 2. □

Next theorem is the core part of the degree lower bound and is due to [Gri01].

Theorem 4. *Given a k-XOR formula ϕ. If the minimum degree to refute the binomial encoding of ϕ in Binomial Calculus 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 for the equational part of $\mathsf{PC}_>$. By applying Corollary 3 we can suppose without loss of generality 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 cancellations.

Observe that for each j it holds that $\deg(h_j^2) \le d$[1].

Now we are going to define a linear operator $L : \mathbb{R}[Y] \to \mathbb{R}$ that maps any polynomial p' derivable in degree d to 0, that maps 1 to 1 and that maps any squared polynomial to a non negative number. The existence of this operator shows that there cannot be any refutation of the initial formula ϕ within degree d because applying the operator to both sides we get the contradiction $0 \ge 1$.

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

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

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

[1] Pick h_{j^*} with the highest degree term. The leading term of h_{j^*} cannot cancel out in the sum $\sum_j h_j^2$ because all its occurrences will have positive coefficients (because of the squaring). Hence to satisfy (2) it should appear also in p'. Since all monomials in p' have degree not greater than d, it must be the case that $\deg(h_{j^*}^2) \le d$

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. Then take squares $m^2 = a^2$. 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 $\alpha^2 = 1$, i.e., 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 a binomial equation $am - a'm' = 0$ derivable in degree d. We can prove in BC that $m = \alpha$ if and only if we can prove in the same degree that $m' = \alpha \frac{a}{a'}$. Hence $L(m)$ is non-zero if and only if $L(m')$ is non-zero, and in that case $L(am - a'm') = aL(m) - a'L(m') = 0$.

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, namely polynomials as $p = \sum_{S \subseteq [n]} \alpha_S y_S$, 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 notice that when BC derives $y_{S\Delta T} = \pm 1$ and $y_{T\Delta U} = \pm 1$ in degree d then using BC derives $y_{S\Delta U} = \pm 1$ too in degree d. Therefore every connected component of G is a clique.

Now we consider each connected component one by one. A 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 $I \in A$ $J \in B$ $L(y_{I\Delta J}) = -1$. 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

$$L(y_{S\Delta T}) L(y_{T\Delta U}) L(y_{S\Delta U}) = L(y_\emptyset) = L(1) = 1. \tag{4}$$

Now we prove a that $L(p^2) \geq 0$. The cross products between monomials in different connected components will be set to zero by operator L therefore we can focus on each single component. Let $\mathcal{S}$ be a sub-polynomial 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 $L(p^2) \geq 0$. Lets evaluate the operator L over $\mathcal{S}$.

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

This shows that L acts not negatively on each (S), and therefore on p^2. □

The proof of Theorem 4 concludes the proof of the lower bound stated in Theorem 1.

References

[BGIP01] Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.*, 62(2):267–289, 2001.

[Gri01] Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1):613–622, 2001.