Lecture 5— Lower bound for polynomial calculus

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

Tuesday — November 10th, 2015 (This document was updated on June 21, 2017)

We are going to show a lower bound on the refutation size for random 3*-XOR. The lower bound holds for polynomial calculus under every field where* $1+1$ *is different from* 0 *and* 1 *(in particular it does not hold for* $\mathbb{F}_2$*).*

We recall from last lecture that a polynomial calculus derivation over the field $\mathbb{F}$ from polynomials $p_1, \ldots, p_m$ is a sequence of steps using the following rules.

Boolean axiom: $\dfrac{}{x_i^2 - x_i}$ for some $i \in [n]$.

Initial axiom: $\dfrac{}{p_j}$ for some $j \in [m]$;

Linear combination: $\dfrac{p \qquad q}{\alpha p + \beta q}$ for some $\alpha, \beta \in \mathbb{F}$;

Multiplication: $\dfrac{p}{x_i p}$ for some variable x_i with $i \in [n]$.

Definition (Pc degree and size)**.** *The* size *of a polynomial calculus proof is the number of monomials (with repetition) that occur in a proof, intented as the sum of the number of monomials in each polynomial among all polynomials in the proof.*[1] *The* degree *of a polynomial calculus proof is a the maximum degree among all polynomials in the proof.*[2]

Degree versus size

We want to use degree lower bounds to get size lower bounds, and we use a theorem very similar to the one we showed already for resolution, due to Impagliazzo, Pudlák, Sgall (1999).[3] They prove the theorem for Pc but the proof extends to Pcr pretty much immediately. The proof is more or less the same as in resolution.

Theorem 1 (Impagliazzo, Pudlák, Sgall, 2001)**.** *Consider a* k*-CNF formula* ϕ *of* n *variables that has a* Pc *(*Pcr*) refutation of size* S*. Then* ϕ *has also a* Pc *(*Pcr*) refutation of degree at most*

$$k + O\left(\sqrt{n \ln S}\right).$$

Corollary 2. *Consider a* k*-CNF formula* ϕ *of* n *variables. Let* S *the size of the smallest* Pc *(*Pcr*) refutation of* ϕ*, and let* D *be the smallest degree among the refutations of* ϕ*. Then it holds that*

$$S \geq \exp\left(\Omega\left(\frac{(D-k)^2}{n}\right)\right).$$

[1] In the proof all polynomials are expressed as linear combinations of distinct monomials. The number of monomial in a polynomial $p = \sum_m \alpha_m m$ is the number of non zero coefficients α_m.

[2] The degree of a multivariate monomial $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ is $\sum_i d_i$. The degree of a multivariate polynomial is the maximum degree among its monomials.

[3] Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999

Exercise 3. Look again at the proof of the size-width tradeoff for resolution in lecture 3, and convince yourself that the proof can be adapted to Pc and Pcr.

As for resolution, we know that the theorem cannot be improved because there is a formula with a small refutation which requires $\Theta(\sqrt{n})$ degree.[4]

[4] Nicola Galesi and Massimo Lauria. Optimality of size-degree tradeoffs for polynomial calculus. *ACM Transaction on Computational Logic*, 12:4:1–4:22, October 2010

Theorem 4 (Galesi and Lauria, 2010)**.** *There exists a* 3*-CNF over* $O(m^2)$ *variables so that*

- *has* $O(m^3)$ *clauses;*
- *has a* Pc *refutation of length* $m^{O(1)}$ *and degree* $m + O(1)$*;*
- *requires refutation degree* $\Omega(m)$.

Linear system modulo 2

In this class we deal with linear systems modulo 2. Each linear equation

$$x_1 + x_2 + \cdots + x_k = b \pmod 2 \tag{1}$$

for $b \in \{0,1\}$ can be encoded encoding as

Clause encoding. 2^{k-1} clauses of width k;

Polynomial encoding. ($\mathrm{char}(\mathbb{F}) = 2$)

$$x_1 + x_2 + \cdots + x_k = b\ ; \tag{2}$$

Polynomial encoding. ($\mathrm{char}(\mathbb{F}) \neq 2$)

$$\prod_i (1 - 2x_i) = -1^b\ . \tag{3}$$

Example 5. The clause encoding of $x_1 + x_2 + x_3 = 1 \pmod 2$ under any field is

$$\begin{aligned}(1-x_1)(1-x_2)(1-x_3) &= 0\\ x_1x_2(1-x_3) &= 0\\ x_1(1-x_2)x_3 &= 0\\ (1-x_1)x_2x_3 &= 0\end{aligned}$$

and its polynomial encoding under a field of charachteristic $\neq 2$ is

$$(1-2x_1)(1-2x_2)(1-2x_3) = 0. \tag{4}$$

Furthermore there is a $O(1)$ size and degree transformation between the two encoding. As shown by the following exercise.

Exercise 6. Show that from the standard polynomial encoding of the 2^{k-1} clauses we can derive the polynomial encoding in the appropriate field, and vice versa, with a derivation of length $2^{O(k)}$ and degree $k + O(1)$.

Because of the previous exercise it does not matter really if we use the clause encoding or the polynomial encoding for our upper and lower bounds. Now we see that under a field of characteristic 2 there is a very simple refutation of any unsatisfiable 3-XOR.

Proposition 7. *Let ϕ be CNF encoding of an unsatisfiable 3-XOR system over n variables. Formula ϕ has a* Pc *refutation of size $(|\phi|^2)$ and degree $O(1)$, assuming the underlying field is $\mathbb{F}_2$.*

Proof. Formula ϕ has m constraints, each encoded as 4 clauses. For each constraint we can derive the corresponding Equation (2) in length $O(1)$ and degree $O(1)$. Once we do that we can refute the linear system by summing a subset of the equations and obtaining $1 = 0$. □

Multiplicative encoding of linear equation mod 2.

If the field has characteristic different from 2 then we cannot deal with linear equations mod 2 as efficiently. We will use the polynomial encoding as in Equation (3). To ease notation we do a **linear change of variables**, that maps $y_i \leftarrow (-1)^{x_i}$.

$$y_i \qquad 1 - 2x_i \tag{5}$$

$$y_1 \cdots y_k = (-1)^b \qquad (1 - 2x_1) \cdots (1 - 2x_k) = (-1)^b \tag{6}$$

$$y_i^2 = 1 \qquad x_i^2 = x_i \ . \tag{7}$$

Remark 8. *The translation between y_i variables and x_i variable is invertible and is linear. Therefore a refutation of degree d over one notation exists if and only if exists in the other notation.*

Definition 9. *A **multilinear** monomial is a monomial where all variables are raised to a power at most one.*

Exercise 10. Show that a Pc refutation can be transformed into another refutation at most a constant times bigger, with at most additional $O(1)$ degree where at most one variable has degree 2 in any monomial.

Exercise 11. Show that a function $f : \{0,1\}^n \longrightarrow \mathbb{F}$ has a unique representation as a linear combination of multilinear monomials

$$\prod_{i \in I} x_i \qquad \text{for } I \in [n]. \tag{8}$$

and another unique representation as a linear combination of multilinear monomials

$$\prod_{i \in I} y_i \qquad \text{for } I \in [n]. \tag{9}$$

(Hint: the functions from $\{0,1\}^n$ to $\mathbb{F}$ form a vector space over $\mathbb{F}$ of dimension 2^n.)

Why the multiplicative encoding? Linear equations in $\mathbb{F}_2$ can be simulated multiplicatively in other fields using this mapping and, as we will see later, this is more or less the form of the Pc refutation in other fields of other characteristics: summing equations $x_1 + x_2 + x_3 + x_4 = 1$ with $x_2 + x_3 +$

$x_5 + x_6 = 1$ under $\mathbb{F}_2$ gives $x_1 + x_4 + x_5 + x_6 = 0$. While multiplying $y_1y_2y_3y_4 = -1$ and $y_2y_5y_5y_6 = 1$ gives $y_1y_4y_5x_6 = 1$.

Actually last product gives $y_1y_2^2y_3^2y_4y_5x_6 = 1$ but we can use axioms y_i^2. We can remove the squared variables as soon as they occur and that costs at most additional degree 2 in the proof.

The lower bound result and strategy.

We consider random 3-XORs over n variables and m clauses. The formula is obtained by sampling m times with repetition from the set of all $2\binom{n}{3}$ parity constraints on 3 variables. We will use the following properties of the random 3-XOR.

Proposition 12. *There are $\Delta > 0$ and $\alpha > 0$ such that if we pick a random 3-XOR over n variables with $m = \Delta n$ parity constraints we have with high probability that*

- *the formula linear system is unsatisfiable;*
- *every set $S \subseteq [m]$ of at most αn equations has at least $\epsilon|S|$ variables occurring in exactly one equation among S;*
- *every set of at most αn equations is satisfiable.*[5]

[5] This actually follows from the previous item, can you see why?

Lemma 13 (Gaussian width lower bound)**.** *Consider 3-XOR that satisfies the properties of Proposition 12. Then any degree 1 refutation in* Pc *under field $\mathbb{F}_2$ has a line with $\Omega(n)$ variables.*

Proof. Under $\mathbb{F}_2$ the 3-XOR is encoded as linear equations, and each line in a degree 1 refutation is just the sum of a subset of the initial equations.

For any line L in the proof consider $\mu(L)$ to be the smallest initial constraints that where summed to derive that line. For initial constraints $\mu(L) = 1$, and $\mu(''0 = 1'') \geq \alpha n$. The latter is because for a sum to give $0 = 1$ all variables must appear in an even number of constraints, but any set of at most αn equations has variable occurring exactly once. Since μ can at most double at each addition step, there is a line L for which $\frac{\alpha n}{2} \leq \mu(L) \leq \alpha n$. There are at least $\epsilon\mu(L) = \Omega(n)$ variables that occur uniquely in those initial equations, therefore L has $\Omega(n)$ variables. □

The following theorem has been proved in Ben-Sasson, Impagliazzo (1999) using techniques from Grigoriev et al. (2001)[6].

Theorem 14. *Let ϕ a random 3-XOR as above, encoded as a CNF formula. With high probability any polynomial calculus refutation of ϕ under a field of characteristic different from 2 requires size $2^{\Omega(n)}$.*

[6] Eli Ben-Sasson and Russell Impagliazzo. Random CNFs are hard for the polynomial calculus. In *40th Annual Symposium on Foundations of Computer Science*, pages 415–421, 1999; and 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

proof preliminaries. With high probability the 3-XOR satisfied the properties in Proposition 12. Assuming these properties we are going to prove an $\Omega(n)$ degree lower bound for the Pc refutation. Because of Exercise 6 we can assume that the 3-XOR system is given in the polynomial encoding and

because of Remark 8 we can assume that everything is encoded using the y_i variables. Therefore we actually want to show that refuting the system of equations

$$y_{i_1(j)}y_{i_2(j)}y_{i_3(j)} = (-1)^{b_j} \qquad j \in [m] \tag{10}$$
$$y_i^2 = 1 \qquad i \in [n] \tag{11}$$

requires a degree $\Omega(n)$ refutation. To do that we show that a refutation of degree d in this field can be used to produce a degree 1 proof under field $\mathbb{F}_2$ where at least one line mentions $2d$ variables. The degree lower bound follows then by Lemma 13, and the size lower bound follows directly from Corollary 2. □

A simple form for refutations

We will argue that any refutation under fields of characteristic different from 2 have a very simplified form, which is essentially a multiplicative encoding of the degree 1 refutation under $\mathbb{F}_2$. Take the set E_d of the binomial equations

$$m_1 = \pm m_2$$

where m_1 and m_2 are polynomials over y_i variables, obtained as

- polynomial encoding under field of characteristic different from 2 of initial parities of the 3-XOR formula;
- if $m_1 = \pm m_2 \in E_d$ and $y_i m_1 = \pm y_i m_2$ has degree at most d, then $y_i m_1 = \pm y_i m_2$ is in E_d;
- if $m_1 = \pm m_2 \in E_d$ then $m_2 = \pm m_1 \in E_d$;
- if $m_1 = \alpha m_2 \in E_d$ and $m_2 = \beta m_3 \in E_d$ then $m_1 = \alpha\beta m_3$.

Exercise 15. Consider derivations from 3-XOR in which all proof lines have the form of multilinear binomial $m_1 \pm m_2 = 0$. Show that $m_1 = \pm m_2 \in E_d$ if and only if $m_1 \pm m_2 = 0$ has such derivation in degree d.

Proposition 16. *If $1 = -1 \in E_d$ then there is a degree 1 refutation under $\mathbb{F}_2$ where each linear equation mention at most $2d$ variables.*

proof sketch. Each $m_1 = \pm m_2$ can be represented as $m_1 m_2 = \pm 1$ by at most doubling the degree. Notice that

$$y_{i_1}y_{i_2}\cdots y_{i_k} = (-1)^b$$

is essentially

$$(-1)^{x_{i_1}+x_{i_2}+\cdots+x_{i_k}} = (-1)^b.$$

Therefore we can represent each $m_1 = \pm m_2 \in E_d$ as a degree 1 linear euqation under $\mathbb{F}_2$ with at most $2d$ variables. $1 = -1$ corresponds to $(-1)^0 = (-1)^1$ therefore it is represented by equation $0 = 1$ under $\mathbb{F}_2$. It is easy to see that these linear equation mod 2 can be derived in the same way the elements of E_d are derived, modulo translating from the multiplicative setting to the additive one. □

Corollary 17. *Consider* 3*-XOR that satisfies the properties of Proposition 12. If* $1 = -1 \in E_d$ *then* $d = \Omega(n)$.

The main theorem follows by showing that any refutation of 3-XOR in under fields of characteristic 2 is essentially representable in E_d without loss of degree.

Lemma 18. *Let* $P = \{m_1 = \pm 1, m_2 = \pm 1, \ldots, m_\ell = \pm 1\}$ *the polynomial encoding of a* 3*-XOR system. Consider any* q *such that* $P \vdash_d q$. *Then*

$$q = \sum c_i(m_i - \alpha_i m_i') \tag{12}$$

with $alpha_i = \pm 1$, *where for every* i, $m_i = \alpha m_i' \in E_d$, *and where every* m_i *and* m_i' *occur in* q *with non zero coefficient.*

Proof. This is obvious for initial parity constrains. And it is also easy to see that if q has such representation then xq has a representation without cancellations. Let q be a linear combination of some q_1, q_2 that have the desired representation. We obtain a representation

$$q = \sum_{i=1}^{\ell} c_i(m_i - \alpha_i m_i') \tag{13}$$

but there may be monomial cancellations. Consider a monomial m which is on the right side but not on the left side: without loss of generality the case where $LM(q) \prec m$ and that

$$q = \sum_{i=1}^{\ell} c_i(m - \alpha_i m_i) \tag{14}$$

with $\alpha_i = \pm 1$ and $m_i \prec m$ for every i and $m = \alpha_i m_i \in E_d$. Then we can rewrite q as

$$\begin{aligned}
&\sum_{i=1}^{\ell} c_i(m - \alpha_i m_i) = \\
&\sum_{i=1}^{\ell} c_i m - \sum_{i=1}^{\ell} c_i\alpha_i m_i = -\sum_{i=1}^{\ell} c_i\alpha_i m_i = -c_1\alpha_1 m_1 - \sum_{i=2}^{\ell} c_i\alpha_i m_i = \\
&\qquad \sum_{i=1}^{\ell} c_i\alpha_1 m_1 - c_1\alpha_1 m_1 - \sum_{i=2}^{\ell} c_i\alpha_i m_i = \\
&\qquad\qquad \sum_{i=2}^{\ell} c_i\alpha_1(m_1 - \frac{\alpha_i}{\alpha_1} m_i)\,.
\end{aligned} \tag{15}$$

Here we used that m was cancelled, hence it must be that $\sum_{i=1}^{\ell} c_i = 0$. □

This concludes the proof of Theorem 14.

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.

[BSI99] Eli Ben-Sasson and Russell Impagliazzo. Random CNFs are hard for the polynomial calculus. In *40th Annual Symposium on Foundations of Computer Science*, pages 415–421, 1999.

[GL10] Nicola Galesi and Massimo Lauria. Optimality of size-degree tradeoffs for polynomial calculus. *ACM Transaction on Computational Logic*, 12:4:1–4:22, October 2010.

[IPS99] Russell Impagliazzo, Pavel Pudlák, and Jiří Sgall. Lower bounds for the polynomial calculus and the gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, 1999.