Problem set 2 — Polynomial calculus and cutting planes

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

(This document was updated on June 21, 2017)

Due: Tuesday, November 24th, 2015 at 15:05. Submit your solutions as a PDF file by e-mail to lauria.massimo@gmail.com with the subject line

`Problem set 2: ⟨your full name⟩`

Name the PDF file `PS2⟨YourFullName⟩.pdf` (with your name coded in ASCII without national characters and no spaces), and also state your name (in both national and latin character) and e-mail address at the top of the first page. Solutions should be written in LaTeX or some other math-aware typesetting system. Please try to be precise and to the point in your solutions and refrain from vague statements. If you are not confident with English please limit yourself to simple, short and clear sentences. Nevertheless the solutions needs to be explained in reasonable precision. *Write so that a fellow student of yours can read, understand, and verify your solutions.*

Collaboration: Discussions of ideas in groups of two people are allowed—and indeed, encouraged—but you should write down your own solution individually and understand all aspects of it fully. You should also acknowledge any collaboration. State at the beginning of the problem set if you have been collaborating with someone and if so with whom.

Reference material: Some of the problems are "classic" and hence it might be easy to find solutions on the Internet, in textbooks or in research papers. **Please don't do that.**

☺ You can use and refer to anything said during the lectures or written in the lecture notes.

☹ You cannot use textbooks/internet/papers to find the answer to the problems in the set.

☺ You can refer to research papers/textbooks/internet for those proofs that we saw in class, either because they are missing from the lecture notes or because you feel the lecture notes are not clear enough.

☹ The previous permission does not apply to missing pieces of those proofs that the lecturer explicitly asked you to prove as an exercise.

It is hard to pin down 100% formal rules on what all this means—when in doubt, ask the lecturer. Obviously these rules are designed with honest students in mind. I am confident that there is no need to develop rules against malicious students.

Assessment of the final grade: Some of the problems are meant to be quite challenging and you are not necessarily expected to solve all of them. As a general guideline, **a total score of 70 should be sufficient to pass**. Partial score may be given for partial solutions and for partially (but mostly) correct solutions. Please refrain from providing answers if you are not confident of their correctness. The tentative plan it to have three problem sets, published:

- at the 3rd lecture;
- at the 6th or 7th lecture;
- at the 10th lecture.

Passing three problem sets is sufficient to pass the course. If a student fails to pass one problem set by a small amount of points, he/she could still pass the course if he/she has a good score (well above pass) at the other two problem sets. How good depends on how far for the threshold the student was in the failed problem set.

The total points and the passing thresholds of the three problem sets may be different. Beware that the each passing threshold may be lowered (but never increased!) during the grading.

Polynomial calculus

Problem 1 (5 points)**.** *Recall the polymonial encoding of a clause as in, e.g.*

$$x \vee \bar{y} \vee \bar{z} \vee u \qquad x(1-y)(1-z)u\ . \tag{1}$$

Show that there is a clause of k literals for which the polynomial encoding has one monomial, and another clause of k literals for which the polynomial encoding has 2^k monomials.

Problem 2 (15 points)**.** *Consider $P = \{p_1, \ldots, p_m\}$ and a polynomial q, all defined over n variables and of degree at most d. Prove that P logically implies[1] q if and only if $P \vdash q$, and furthermore in the latter case there is a derivation of q from P with size at most $2^{O(n)}$ and degree $max\{n+1, d\}$.*

[1] P logically implies q if for any common root of P under $\{0,1\}$ assignment is a root of q.

Problem 3 (5 points)**.** *Show that any polynomial calculus derivation can be transformed, with a linear blow-up in size and constant blow up in degree, into a derivation where at most one variable is raised to a power greater than* 1 *(assuming this holds for the initial and the target polynomials).*

Problem 4 (10 points)**.** *Let p be a polynomial of degree d and $\widehat{p}$ its multilinearized version (i.e. all variables in all monomials are raised to the power of* 1*). Show that $p \vdash_d \widehat{p}$ and that $\widehat{p} \vdash_d p$.*

Problem 5 (10 points)**.** *Consider an unsatisfiable CNF formula ϕ. Show that if ϕ has a resolution refutation of width W, then ϕ has a* Pc *refutation of degree $W+1$ regardless the field $\mathbb{F}$.*

Problem 6 (10 points)**.** *Polynomial calculus with resolution (*Pcr*) is a variant of* Pc *where we have additional twin variables $\bar{x}_1, \ldots, \bar{x_n}$.*

Clauses are encoded as monomials, e.g.

$$x \vee \bar{y} \vee \bar{z} \vee u \qquad x\bar{y}\bar{z}u\ , \tag{2}$$

and additionally we have the negation axioms $\overline{1 - x_i - \bar{x}_i}$ for every $i \in [n]$.

Consider an unsatisfiable CNF formula ϕ. Show that if ϕ has a resolution refutation of width W and size S, then ϕ has a Pcr *refutation of degree $W+1$ and size $O(S)$ regardless of the field $\mathbb{F}$.*

Problem 7 (5 points)**.** *Show that the smallest degree of a* Pc *derivation $P \vdash q$ and the smallest degree of a* Pcr *derivation of q from P are the same.*

For the next exercise we need to know what an ideal generated by polynomials is.

Definition (Ideals)**.** *The ideal I generated by a set of polynomials $p_1, \ldots, p_m$ is denoted as $\langle p_1, \ldots, p_m \rangle$. We give the classic definition plus two definitions specialized for discussing about* Pc *and* Pcr *derivation.*

- *The* ideal I *generated by* $p_1, \ldots, p_m$ *is the set of polynomials of the form*

$$\sum_{j \in [m]} g_j p_j \tag{3}$$

for some $g_1, \ldots g_m$ *in* $\mathbb{F}[x_1, \ldots, x_n]$.

- *The* ideal I *generated by* $p_1, \ldots, p_m$ *plus the boolean axioms is the set of polynomials of the form*

$$\sum_{j \in [m]} g_j p_j + \sum_{i \in [n]} h_i (x_i^2 - x_i) \tag{4}$$

for some $g_1, \ldots g_m, h_1, \ldots h_n$ *in* $\mathbb{F}[x_1, \ldots, x_n]$.

- *The* ideal I *generated by* $p_1, \ldots, p_m$ *plus the boolean axioms and the negation axioms is the set of polynomials of the form*

$$\sum_{j \in [m]} g_j p_j + \sum_{i \in [n]} h_i (x_i^2 - x_i) + \sum_{i \in [n]} \ell_i (1 - x_i - \bar{x}_i) \tag{5}$$

for some $g_1, \ldots, g_m$, $h_1, \ldots h_n$ *and* $\ell_1, \ldots, \ell_n$ *in* $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$.

It is clear that whenever $q \in \langle p_1, \ldots, p_m \rangle$ then $q(\vec{x}) = 0$ for any common root x of $p_1(\vec{x}), \ldots, p_m$. So q is a logical implication of the set of polynomials $p_1, \ldots, p_m$.

Problem 8 (10 points)**.** *Consider a set of polynomials* $P = \{p_1, \ldots, p_m\}$.

- *Then* q *has a* Pc *derivation if and only if* q *is in the ideal generated from* P *plus boolean axioms.*

- *Then* q *has a* Pcr *derivation if and only if* q *is in the ideal generated from* P *plus boolean axioms and negation axioms.*

Recall that the S-polynomial of q_1 and q_2, denoted as $S(q_1, q_2)$ is

$$\frac{LCM(LM(q_1), LM(q_2))}{LT(q_1)} \cdot q_1 - \frac{LCM(LM(q_1), LM(q_2))}{LT(q_2)} \cdot q_2 \tag{6}$$

Problem 9 (5 points)**.** *Prove that:*

- *for every* $\alpha \neq 0$ *and* $\beta \neq 0$, $S(q_1, q_2) = S(\alpha q_1, \beta q_2)$.

- *for every monomials* m_1, m_2 *and polynomials* q_1, q_2 *with* $LM(m_1 q_1) = LM(m_2 q_2)$*, then*

$$S(m_1 q_1, m_2 q_2) = m S(q_1, q_2)$$

for some monomial m.

Recall the algorithm to compute G_d in Lecture 4.

Problem 10 (10 points)**.** *Show that every* $g \in G_d$ *has a* Pc *proof of degree* d *from* P*, and that it is possible to extract such proof from the the running of the algorithm.*

Problem 11 (5 points)**.** *Show that the algorithm computes* G_d *it time* $n^{O(d)}$ *assuming* $P = \{p_1, \ldots, p_m\}$ *has size* $n^{O(1)}$*, where* n *is the number of variables in* P.

Problem 12 (20 points)**.** *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*

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

and hence

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

Look again at the proof of the size-width tradeoff for resolution in lecture 3 and in Ben-Sasson, Wigderson (2001)[2]*, and adapt that proof to* Pc *and* Pcr *to get the relations above.*

[2] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48(2):149–169, 2001

Problem 13 (10 points)**.** *Consider a linear equation*

$$x_1 + x_2 + \cdots + x_k = b \pmod 2 . \tag{7}$$

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 $k^{O(1)}2^k$ and degree $k + O(1)$.

Problem 14 (10 points)**.** *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.)

Cutting planes

Problem 15 (10 points)**.** *Show that any resolution refutation of size s for a formula of n variables can be translated in a cutting plane refutation of size $O(ns)$.*

Problem 16 (10 points)**.** *Consider the set of inequalities*

$$x_i + x_j \leq 1 \quad \text{for } 1 \leq i < j \leq n. \tag{10}$$

Show how to derive the inequality

$$\sum_{i=1}^{n} x_i \leq 1 . \tag{11}$$

in length $O(n^2)$.

Problem 17 (15 points)**.** *Try to solve the previous exercise with a derivation of rank $O(\log n)$. Any proof length is fine.*

Problem 18 (10 points)**.** *Consider the formula*

$$F_n = \mathrm{Clique}_n(x,y) \wedge \mathrm{Color}_n(x,z) \tag{12}$$

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, for $k = \lfloor \frac{1}{8}(n \log n)^{2/3} \rfloor$.

The formula Clique_n is a conjunction of the following inequalities

$$\sum_{i \in [n]} y_i = k \tag{13}$$

$$x_{ij} \geq y_i + y_j - 1\ . \tag{14}$$

The formula Color_n is a conjunction of the following inequalities

$$\sum_{c \in [k-1]} z_{i,c} = 1 \qquad \text{for every } i \in [n]; \tag{15}$$

$$x_{i_1,i_2} + z_{i_1,c} + z_{i_2,c} \leq 2 \qquad \text{for every } c \in [k-1], i_1 < i_2 \in [n]. \tag{16}$$

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.

Problem 19 (15 points)**.** *Look at Equations (13) and (15) 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 20 (10 points)**.** Show that there exists a 3-CNF that has no cutting planes refutation of polynomial size. (Use of course the results in Lecture 6 and in the previous exercises.)

References

[BSW01] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48(2):149–169, 2001.