REASONING IN PROPOSITIONAL LOGIC USING GRÖBNER BASES L I

The SATISFIABILITY problem

Given a propositional logic formula in conjunctive normal form (CNF), is it possible to find assignment satisfying all clauses / constraints?

Example CNF formula

$$\boxed{\begin{aligned} F = \; & (x \vee y) \\ \wedge \; & (\overline{x} \vee z) \\ \wedge \; & (\overline{z} \vee w) \\ \wedge \; & (x \vee \overline{y}) \\ \wedge \; & (\overline{z} \vee \overline{w}) \end{aligned}}$$

- x variable / positive literal
- $\overline{x}$ negated variable / negative literal
- $(\overline{x} \vee z)$ clause true if x false or z true
- Formula true if all clauses true.

Is this formula satisfiable?
Can this problem be solved efficiently?

Size of input = total # literals (with repetitions)

Efficient algorithm: $\exists$ some polynomial P such that running time on F is at most $P(\text{size}(F))$ Interested in how performance scales as instance size increases

One of the Millennium Prize Problems (P vs. NP) — so we will not solve it today...

Make problem easier: study concrete computational models = concrete algorithmic approaches

Today: Gröbner basis calculations (essentially)

Want to prove impossibility results = efficient algorithms don't exist (in given framework) = lower bounds

How to do this?
Constructive results = upper bounds: clear what to do:

- Present algorithm
- Analyze correctness
- Analyze worst-case running time

But how can we prove lower bounds against all algorithms?!

Any algorithm must certify (implicitly) correctness of answer.
So analyze smallest size of such certificates.

If formula F satisfiable ⇒ always ∃ small certificate

So focus on unsatisfiable inputs.

And (today) study algebraic methods for certifying unsatisfiability

2 III

POLYNOMIAL CALCULUS [Clegg-Edmonds-Impagliazzo '96]

Translate clauses to polynomials

$x \vee y$	$x \cdot y = 0$	$x^2 - x = 0$
$\bar{x} \vee z$	$(1-x)z = 0$	$y^2 - y = 0$
$\bar{z} \vee w$	$(1-z)w = 0$	$z^2 - z = 0$
$x \vee \bar{y}$	$x(1-y) = 0$	$w^2 - w = 0$
$\bar{z} \vee \bar{w}$	$(1-z)(1-w) = 0$	

Only $\{0,1\}$ solutions
$0 \equiv$ true
$1 \equiv$ false

In general: $x \mapsto x$, $\bar{x} \mapsto (1-x)$, clause $\mapsto$ product

$\mathbb{F}$ fixed field $(\mathbb{Q}, \mathbb{R}, GF(p), \ldots)$

$GF(p)$: Integers mod prime p a.k.a. $\mathbb{Z}_p$

$\vec{x} = (x_1, \ldots, x_n)$

Polynomial equations (not only from CNFs)

$$(*) \quad \boxed{\begin{cases} P_j(\vec{x}) = 0 \\ x_i^2 - x_i = 0 \end{cases}} \qquad \begin{array}{l} j \in [m] = \{1, 2, \ldots, m\} \\ i \in [n] \end{array}$$

n = #variables throughout this talk

Look at IDEAL $I \subseteq \mathbb{F}[\vec{x}]$ generated by these polynomials (drop "$=0$" from now on)

(1) $P_j(\vec{x}) \in I$

(2) $x_i^2 - x_i \in I$

(3) If $P, Q \in I$, then $\alpha P + \beta Q \in I$; $\alpha, \beta \in \mathbb{F}$

(4) If $P \in I$, $R \in \mathbb{F}[\vec{x}]$, $RP \in I$

Notation
$\langle P_1, \ldots, P_m, x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$

HILBERT'S NULLSTELLENSATZ

$(*)$ has no solution $\Longleftrightarrow 1 \in \langle P_1, \ldots, P_m, x_i^2 - x_i \rangle$

($\Longleftrightarrow$ Variety is empty)

($\Leftarrow$) Obvious

($\Rightarrow$) Requires a proof (but is true)

Polynomial calculus (PC) refutation of $(*)$: Sequence of derivation steps showing that $1 \in$ ideal I generated by input

Sequence of polynomials

$(S_1, S_2, \ldots, S_L)$

such that

$S_L = 1$

and every S_j derived from S_i, $i<j$, by

$$\frac{}{P_j} \text{ Input axiom} \qquad \frac{}{x_i^2 - x_i} \text{ Boolean axiom}$$

$$\frac{P \qquad Q}{\alpha P + \beta Q} \ \alpha, \beta \in \mathbb{F} \text{ linear combination} \qquad \frac{P}{xP} \text{ multiplication}$$

Insist on all polynomials written out as linear combinations of monomials.

PC refutation of example formula

1.	xy	Input	$x \vee y$
2.	$x - xy$	Input	$x \vee \overline{y}$
3.	x	LinComb (1,2)	
4.	xz	Mult (3)	
5.	$z - xz$	Input	$\overline{x} \vee z$
6.	z	LinComb (4,5)	
7.	$w - zw$	Input	$\overline{z} \vee w$
8.	$1 - w - z + zw$	Input	$\overline{z} \vee \overline{w}$
9.	$1 - z$	LinComb (7,8)	
10.	1	LinComb (6,9)	

No use of Boolean axioms – not needed for CNFs, but can increase efficiency

Degree: Largest total degree in refutation 2
Length: # steps in refutation 10
Size: # monomials in refutation (counted with repetitions) 17

Take minimum over all refutations
Defines the degree / length / size of refuting a set of polynomials

$\boxed{\text{powers of all variables} = 1}$

W.l.o.g. All polynomials multilinear (because of $x_i^2 - x_i$)

Can fold multilinearization into multiplication step. Technically, work in

$\mathbb{F}[\vec{x}] / \langle x_1^2 - x_1, \ldots, x_n^2 - x_n \rangle$

Why insist on polynomial = linear combination of monomials?

1. Somewhat reasonable representation — will find it used in practice

2. Don't know how to prove lower bounds for (potentially) smarter representations, e.g.) binary decision diagrams.

[Leads to deep questions in computational complexity theory]

<u>FACT 1</u> For PC with "multilinearization for free" any unsatisfiable CNF formula F is refutable in length $\sim (\text{size}(F))$

But polynomials can be exponentially large...

Focus instead on <u>size</u> and <u>degree</u>

More algorithmically relevant

<u>THM 2</u> [CEI 96]
If $\exists$ PC refutation in degree d, then $\exists$ PC refutation in size $n^{O(d)}$

[$\exists$ universal constant k s.t. size is $\leq n^{kd}$]

Proof sketch: Run Buchberger's algorithm, but only consider S-polynomials of degree $\leq d$. Details not important for us now

THM 2 is asymptotically tight (in the exponent) in the worst case [Atserias, Lauria, Nordström '16]

So: degree small $\Rightarrow$ size small
Far less obvious: ~~Deg~~ size small $\Rightarrow$ degree (somewhat) small

THM 3 [Impagliazzo, Pudlák, Sgall '99]
Let minimal refutation size S
degree D
Initial degree of input K
variables $= n$ [as always]
Then

$$S \geqq \exp\left(\Omega\left(\frac{(D-K)^2}{n}\right)\right)$$

i.e., $\exists$ universal constant k.

In particular: linear degree lower bound
$\Downarrow$
exponential size lower bound

Proof not hard, but will skip it due to time constraints

Hence, to prove ~~degree~~ size lower bounds, focus on degree!

Thm 3 also essentially tight by [Galesi-Lauria '10]

MOTIVATING EXAMPLE 1: PIGEONHOLE PRINCIPLE FORMULA $\mathcal{L}$ VIII

"$n+1$ pigeons don't fit into n pigeonholes"
How hard to prove algebraically?

Slight twist.

Consider bipartite graph $G=(U \dot{\cup} V, E)$
$|U| = n+1$, $|V| = n$, constant left degree
$U = [n+1]$ $V = [n]$
Allow pigeon i to go to hole j s.t. $(i,j) \in E$

Standard PHP $=$ $G = K_{n+1,n}$

The sparser the graph, the easier to see contradiction (can be made formal)

CNF encoding $x_{u,v}$ = "pigeon u flies to v"

$$\bigvee_{v \in N(u)} x_{u,v} \qquad u \in U$$

$$\overline{x}_{u,v} \vee \overline{x}_{u',v} \qquad v \in V,\ u,u' \in N(v),\ u \neq u'$$

$$\overline{x}_{u,v} \vee \overline{x}_{u,v'} \qquad u \in U,\ v,v' \in N(u),\ v \neq v'$$

Is this hard for PC?

Open since [Alekhnovich–Razborov '01] (and earlier)

Resolved in [Mikša–Nordström '15]
Exponentially hard if G "well-connected"
(e.g., random bipartite graph with constant left degree)

MOTIVATING EXAMPLE 2: GRAPH k-COLOURING

"Given $G=(V,E)$ and $k \in \mathbb{N}^+$, can vertices be coloured with k colours in such a way that $\forall (u,v) \in E$ u and v have distinct colours"

NP-complete problem $\Rightarrow$ should be hard for Gröbner bases (and all other approaches)

Given $G=(V,E)$ and k too small, can we find examples where Gröbner bases cannot certify non-k-colourability efficiently?

Question raised by series of papers by De Loera et al., which present algebra-based methods that work very well in practice

CNF encoding

$x_{v,i}$ = "vertex v gets colour i"

$\bigvee_{i \in [k]} x_{v,i}$

$\overline{x}_{v,i} \vee \overline{x}_{v,j}$ $\qquad v \in V \quad i,j \in [k],\ i \neq j$

$\overline{x}_{u,i} \vee \overline{x}_{v,i}$ $\qquad (u,v) \in E,\ \cancel{j}\ i \in [k]$

Exponential lower bounds in [Lauria-Nordström '17] building heavily on [Mikša-Nordström '15]

FRAMEWORK FOR PROVING PC DEGREE LOWER BOUNDS | X

[Razborov '98], [Alekhnovich - Razborov '01]

This presentation ~~based~~ based on [Mikša - Nordström '15]

RECALL: Always multilinear polynomials

Mod out $x_i^2 - x_i$, $i \in [n]$

MONOMIAL $m = \prod_{i \in T} x_i$

TERM $t = \alpha \cdot m$ $\alpha \in \mathbb{F}$, m monomial

IDEAL $I = \langle P_1, \ldots, P_\ell \rangle$: smallest set of polynomials in $\mathbb{F}[\vec{x}]$ closed under

- linear combinations of elements in I
- multiplication by any polynomial in $\mathbb{F}[\vec{x}]$
- (and contains $P_1, \ldots, P_\ell$)

Fix ADMISSIBLE ORDERING of monomials/terms

- $\deg(m_1) < \deg(m_2) \Rightarrow m_1 \prec m_2$
- If m doesn't contain variables in m_1 or m_2 and $m_1 \prec m_2$, then $m m_1 \prec m m_2$

For simplicity, say

- $x_1 \prec x_2 \prec x_3 \prec \ldots \prec x_n$
- For ~~same~~ same degree, sort lexicographically

LEADING TERM $\boxed{LT(P)}$ = largest term w.r.t. $\prec$

Term t REDUCIBLE modulo ideal I if $\exists\, Q \in I$ s.t. $LT(Q) = t$; IRREDUCIBLE o/w

FACT 4 Any P can be written uniquely as $\boxed{P = Q + R}$

where $Q \in I$

R linear combination of irreducible terms

"P reduces to R mod I"

$$\boxed{R_I(P) = R}$$

Polynomial calculus derivations in degree $\leq d$: Degree-bounded version of ideal "PSEUDO-IDEAL"

Try to define d-PSEUDO-REDUCTION OPERATOR capturing what can be derived in degree d.

Requirments

R1. R^* is linear $R^*(\alpha P + \beta Q) = \alpha R^*(P) + \beta R^*(Q)$

R2. $R^*(1) \neq 0$

R3. $R^*(P_j) = 0$ for all input polynomials in $(*)$

R4 $R^*(xt) = R^*(x R^*(t))$ for all terms t of degree $\deg(t) < d$

LEMMA 5 [Razborov '98]
If $(*)$ has d-pseudoreduction operator, then any polynomial calculus refutation of $(*)$ has to have degree $> d$.

Note Implication, not equivalence

Proof sketch

Given PC derivation in degree $\leq d$
$(S_1, S_2, \ldots, S_L)$

Argue by induction that $R^*(S_i) = 0$.
But $R^*(1) \neq 0$, so cannot derive contradiction

Base case Input axioms OK by R3.

Inductive step ~~Linear~~ Linear combination clear by linearity.

Suppose $R^*(P_j) = 0$ and consider xP_j
$P_j = \sum_{t \in P_j} t$ sum of terms

$$R^*(xP_j) = R^*\left(\sum_{t \in P_j} xt\right)$$

$$= \sum_{t \in P_j} R^*(xt) \quad \text{[by linearity]}$$

$$= \sum_{t \in P_j} R^*(xR^*(t)) \quad \text{[by R4]}$$

$$= R^*\left(\sum_{t \in P_j} xR^*(t)\right) \quad \text{[linearity]}$$

$$= R^*\left(xR^*\left(\sum_{t \in P_j} t\right)\right) \quad \text{linearity}$$

$$= R^*(xR^*(P_j)) = R(x \cdot 0) = R(0) = 0$$

If (*) were satisfiable, could take
R^* to be actual reduction operator
modulo ideal $\langle P_1, \ldots, P_m \rangle$

But how to construct pseudo-reduction?
We like ideals and understand how to
compute with them

Outrageous idea: With every low-degree
monomial m, associate subset $\mathcal{C}_m$ of
input axioms
Let ideal $\boxed{I_m = \langle P \mid P \in \mathcal{C}_m \rangle}$
Define $\boxed{R^*(m) = R_{I_m}(m)}$
Well-defined by linearity condition R1

$$R^*(P) = R^*\Big(\sum_{\alpha m \in P} \alpha m\Big) = \sum_{\alpha m \in P} \alpha R^*(m)$$

$$= \sum_{\alpha m \in P} \alpha \cdot R_{I_m}(m)$$

CHALLENGE: How to choose $\mathcal{C}_m$ for monomial m?
- Property R1 always OK by construction.
- But choose $\mathcal{C}_m$ too large, and R2 will fail
- Too small, and R3 or R4 might fail

Room for
- improved understanding
- new technical developments

Outline (simplified version of) approach from [MN15]

Given polynomials $P_1, \ldots, P_m$ over $x_1, \ldots, x_n$

Divide variables into groups V_j, $j \in [n']$

(doesn't have to be partition, but should have bounded overlap: any x_i occurs in few V_j)

overlap at most ℓ

Take some polynomials $P_{\ell+1}, \ldots, P_m$ and put in special set Q (satisfiable)

Build bipartite graph $G = (U \,\dot\cup\, V, E)$ with

- $U = \{P_1, \ldots, P_\ell\}$
- $V = \{V_1, \ldots, V_{n'}\}$
- Edge (P_i, V_j) if variable in V_j occurs in polynomial P_j

Assume $\boxed{|Vars(P_j)| \text{ bounded}}$ (true for the examples we are interested in)

Want to satisfy 2 conditions

G1. $G = (U \,\dot\cup\, V, E)$ is an $\boxed{(s, \delta)\text{-BOUNDARY EXPANDER}}$, i.e., for all $U' \subseteq U$, $|U'| \leq s$, the set of unique neighbours $\partial U' = \{V_j \in V \mid |N(V_j) \cap U'| = 1\}$ satisfies $|\partial U'| \geq \delta |U'|$

G2. For any edge (P_i, V_j) there is an assignment ρ to V_j such that $P_i(\rho) = 0$ and $\forall P_{i'} \in Q$ either $P_{i'}(\rho) = 0$ or ρ doesn't assign variables in $P_{i'}$ "ρ satisfies P_i plus everything in Q that it touches"

THM 6 [MN15]

If for (*) we can construct a graph $G(U \dot\cup V, E)$ satisfying G1 and G2, then the degree of refuting (*) in polynomial calculus is

$$> \frac{\delta s}{2\ell}$$

δ expansion factor
s expansion size guarantee
ℓ overlap for variables

Proof sketch (very vague)

We need to choose $\mathcal{E}_m$ for monomial m of degree $\deg(m) < d$.

Add m as "ghost vertex" on the left in G

Let $\mathcal{E}'_m$ = largest $U' \subseteq U$ of size $\leq s$ such that

$$\partial U' \subseteq N(m)$$

Let $\mathcal{E}_m = \mathcal{E}'_m \cup Q$

Property R1 (linearity) is by definition
For R2, $\mathcal{E}'_1 = \emptyset$ because of expansion, so $\mathcal{E}_1 = Q$. But Q is satisfiable, so $1 \notin \langle Q \rangle$, meaning that 1 is irreducible mod $\langle Q \rangle$ and $R^*(1) = R_{\langle Q \rangle}(1) = 1 \neq 0$

R3 and R4 are much trickier and are where the action is...

Can use this to prove lower bounds for PHP ([MN15])

L XVI

Lower bound for k-colouring:

Show that if k-colouring is always easy for PC, then PHP formulas can also be refuted efficiently in PC.

But this is not true...
Proof yield explicit example of hard graphs [Lauria - Nordström '17]

OPEN PROBLEMS

(1) For other proof systems / algorithms, know average-case lower bounds for colouring for randomly sampled graphs [$G(n,p)$ Erdős-Rényi]
Would be great to have for PC

(2) Given graph G, certify that G doesn't have k-clique (k vertices all pairwise connected.) Should require time $\sim n^k$ worst-case, and even average-case
Nothing known for Gröbner bases

(3) Unify with methods for proving lower bounds depending on field characteristic / field

(4) Lower bounds also for stronger ways of representing polynomials