Polynomial Calculus

Leo Bhebhe

Polynomial Calculus

What is a polynomial Calculus?

The polynomial calculus (PC) is a refutation system for unsatisfiable sets of polynomial equations over a field.

Fix field *F* and let $P \subseteq F[x_1,\ldots,x_n]$ be the finite set of multivariate polynomials over *F*

An axiom of PC is a polynomial $p \in P$ or $x_i^2 - x_i$, for $1 \le i \le n$

There are two rules of inference of PC

- *Multiplication by a variable*: From p infer $x_i \cdot p$, where $1 \le i \le n$
- *Linear combination*: From p, p', infer $a \cdot p + b \cdot p'$, where $a, b \in F$

Derive constant polynomial **1**

Degree = maximum degree of polynomial appearing in the proof

Can find proof of **degree d** in time $\mathbf{n}^{O(d)}$ using Groebner basis-like algorithm (linear algebra)

Polynomial Calculus

Derivation

A derivation of polynomial q from P is a finite sequence $\prod = (p_1, \dots, p_m)$

- Where $q = p_m$ and for each $1 \le i \le m$
- Either $p_i \in P$ or there exists $1 \le j < i$ such that $p_i = x_k p_j$ for some $1 \le k \le n$
- Or there exists $1 \le j, k < i$ such that $p_i = ap_j + bp_k$

By $P \vdash_d q$, we denote that q has a derivation $\prod = (p_1, \dots, p_m)$ from P of degree at most d.
That is $\max\{\deg(p_i) : 1 \le i \le m\} \le d$

Finally $P \vdash_{d,m} q$ means that $P \vdash_d q$ and additionally that the number of lines in the derivation $\prod = (p_1, \dots, p_m)$ is m.
A PC refutation of P is a derivation of 1 from P.

The degree of refutation $\prod = (p_1, \dots, p_m)$ is $\min\{\deg(p_i) : 1 \le i \le m\}$

The PC degree of unsatisfiable set P of polynomials, denoted $\deg(P)$ is the minimum degree of a refutation of P.

Polynomial Calculus

Derivation

In both NS and PC, a refutation of unsatisfiable CNF formulas $\wedge_{i=1}^{r} C_i$ is a formal manifestation that

$$1 \in I = \left\langle qc_1, \ldots, qc_r, x_1^2 - x, \ldots, x_n^2 - x^n \right\rangle$$

For NS, 1 is explicitly given as a linear combination over $F\left[x_1, \ldots, x_n\right]$ of the qc_i and $(x_1^2 - x)$

While PC, a derivation of the fact that 1 belongs to I is given stepwise

It follows that the degree of a PC refutation of a formula A is at most the degree of an NS refutation of A.

Polynomial Calculus

Example of Derivation

Consider the unsatisfiable CNF formula obtained by taking the conjunction of

$$x_1, \neg x_1 \vee x_2, \neg x_2 \vee x_3, \ldots, x_{n-1} \vee x_n, \neg x_n$$

Using the the q_A translation, we have the polynomials

$$1 - x_1, x_1 - x_1 x_2, x_2 - x_2 x_3, \ldots, x_{n-1} - x_{n-1} x_n, x_n$$

Consider the following derivation:

1. $x_1 - x_1 x_2$, axiom
2. $x_2 - x_2 x_3$, axiom
3. $x_1 x_2 x_3 - x_2 x_3$, multiplication of (1) by $-x_3$
4. $x_1 x_2 - x_1 x_2 x_3$, multiplication of (2) by x_1
5. $x_1 - x_1 x_2 x_3$, addition of (1),(4)
6. $x_1 - x_1 x_3$, addition of (3),(5)

The last line represents $\neg x_1 \vee x_3$

By repeating this we can derive $\neg x_1 \vee x_n$, i.e. $x_1 - x_1 x_n$

1. $x_1 - x_1 x_n$, derived from the above.
2. x_n, axiom.
3. $x_1 x_n$, multiplication of (1) by x_1
4. x_1, addition of (1),(3)
5. $1 - x_1$, axiom
6. 1, addition of (4),(5)

Polynomial Calculus

An easy proof by induction on the number of inferences proves that

- If there's a polynomial calculus refutation of CNF formula A, then A is not satisfiable
- Given a Nullstellensatz refutation, we can obviously furnish a refutation in the polynomial calculus, of the same degree or less
- Hence it follows that PC is complete, with degree bound of *n* for unsatisfiable CNF formulas on n variables

Polynomial Calculus

Theorem 5.5.7 Completeness of a polynomial calculus

If there is no 0,1 solution of the polynomial equations $p(x_1,\ldots,x_n)$ for all $p \in P \subseteq F[x_1,\ldots,x_n]$

Then there's a degree $n+1$ derivation of 1 from $P \cup \{x_i^2 - x_1,\ldots,x_n^2 - x_n\}$ in PC

Theorem 5.5.1 (D. Hilbert) yields a PC derivation of 1 from $P \cup \{x_i^2 - x_1,\ldots,x_n^2 - x_n\}$

In that derivation by judicious application of axioms $x_i^2 - x_1,\ldots,x_n^2 - x_n$ can ensure that the degree is never larger than $n+1$

Corollary 5.5.3 (Folklore). PC is implicationally complete; i.e.

$$(\forall x_1,\ldots,x_n \in F)\left[\bigwedge_{i=1}^{m} p_i(x_1,\ldots,x_n) = 0 \rightarrow q_i(x_1,\ldots,x_n) = 0\right]$$

That implies that $p_1,\ldots,p_m \vdash_{PC} q$

The following alternate proof of completeness of PC for CNF formulas yields the simple, but important fact that constant width resolution refutations can be polynomial simulated by a constant degree polynomial calculus refutations

Polynomial Calculus

Completeness of a polynomial calculus

- The following alternate proof of completeness of PC for CNF formulas yields the simple, but important fact that
  - Constant width resolution refutations can be polynomial simulated by a constant degree polynomial calculus refutations
  - This is formalized in the following theorem (Next slide) :

Polynomial Calculus

Theorem 5.5.8

If the set C of clauses has a resolution refutation of width w, then C has a polynomial calculus refutation of degree at most 2w.

$$\frac{A \cup B \cup \{x\} \quad\ldots\ldots\quad B \cup C \cup \{\bar{x}\}}{A \cup B \cup C}$$

Where $A = \{\alpha_1, \ldots, \alpha_r\}$, $B = \{l_1, \ldots, l_r\}$ and $C = \{\beta_1, \ldots, \beta_r\}$

And literals $\alpha_1 l_1 \beta_1$ range among variables $x_1, \ldots, x_n$ and their negations.

Recall that $q_A = \prod_{\bar{x} \in A} x \cdot \prod_{x \in A} (1 - x)$ and Define polynomials q_B and q_C analogously for clauses B and C.

Polynomial Calculus

Theorem 5.5.8

With these convetions, $A \cup B \cup \{x\}$ is represented by the polynomial $(1-x) \cdot q_A \cdot q_B$

And $A \cup B \cup \{\bar{x}\}$ is represented by $x \cdot q_A \cdot q_B$

By successive multiplications, we obtain

$$(1-x) \cdot q_A \cdot q_B \cdot q_C$$

$$x \cdot q_A \cdot q_B \cdot q_C$$

So, by addition we have $q_A \cdot q_B \cdot q_C$, which represents the solvent

Clearly the degree of the derivation is at most $1+\deg(q_A)+\deg(q_B)+\deg(q_C)$

Hence at most twice the width of any clause appearing in the resolution derivation

Polynomial Calculus

Definition 5.5.5

A degree d pseudoideal I in is a vector subspace of $F[x_1,\ldots,x_n]$, say V consisting of polynomials of degree at most d, such that if $p \in I$ and $\deg(p) < d$, then for $1 \le i \le n$, $x_i p \in I$.

Let $p_1,\ldots,p_k \in F[x_1,\ldots,x_n]$ be multivariate polynomials od degree at most d.

Then $I_{d,n}(p_1,\ldots,p_k)$ denotes the smallest degree d pseudo-ideal of $F[x_1,\ldots,x_n]$

Theorem 5.5.9

For any multilinear polynomials

$$p_1,\ldots,p_k,q \in F[x_1,\ldots,x]/ < x_1^2 - x_1,\ldots,x_1,\ldots,x_n^2 - x_n >$$

Of degree at most d,

$$p_1,\ldots,p_k \vdash_d q \Leftrightarrow q \in I_{d,n}(p_1,\ldots,p_k)$$

Polynomial Calculus

Proof

Let $V = \{q \in F[x_1,\ldots,x] : p_1,\ldots,p_k \quad {}_d q$

We first show direction from left to the right, $V \subseteq I_{d,n}(p_1,\ldots,p_k)$ by induction on the number of m of inferences in the derivation of q from $p_1,\ldots,p_k$

If $p_1,\ldots,p_k \vdash_{d,1} q$ then $q \in \{p_1,\ldots,p_k\}$, so that $q \in I_{d,n}(p_1,\ldots,p_k)$

Suppose now that $\prod = (r_1,\ldots,r_{m+1})$ is a derivation of $q = r_{m+1}$ of degree at most d from $p_1,\ldots,p_k$

Case 1. $\deg(p) < d$ and $q = x_i \cdot r_j$, for some $1 \leq i \leq n$ and $1 \leq j \leq m$

Then by definition, $q \in I_{d,n}(p_1,\ldots,p_k)$

Case 2. $q = ar + br'$ for some $a, b \in F$ and $r, r' \in \{r_1,\ldots,r_m\}$

Since $I_{d,n}(p_1,\ldots,p_k)$ is a vector space, and hence closed under the formation of linear

Polynomial Calculus

Proof

Now consider the right to left, i.e. $I_{d,n}(p_1,\ldots,p_k) \subseteq V$

By definition $p_1,\ldots,p_k \subseteq V$ and V is closed under linear combinations over F

And if $q \in V$ is of degree less than d, then for $1 \le i \le n$, $x_i q \in V$.

By definition $I_{d,n}(p_1,\ldots,p_k)$ is the smallest vector space satisfying these same properties, and so $I_{d,n}(p_1,\ldots,p_k) \subseteq V$

Polynomial Calculus

Theorem 5.5.10

Algorithm CONSTRUCTBASIS$_d$ produces a basis of vector space $I_{d,n}(p_1,\ldots,p_k)$

Theorem 5.5.12

The degree d bounded polynomial calculus is automizable;

That is there's an algorithm A_d, which when given polynomials

$(p_1,\ldots,p_k) \in F[(x_1,\ldots,x_n)]$ *of degree at most d having no* 0, 1 *solution,*

yields a derivation of $1 \in \langle p_1,\ldots,p_k, x_1^2 - x_1,\ldots,x_n^2 - x_n \rangle$ *in time* $O(n^{3d})$

More generally, if $q \in I_{d,n}(p_1,\ldots,p_k)$, *then Ad yields a PC derivation this fact.*

Polynomial Calculus

Fourier Basis

Let $q_0 = 0$, (i.e. FALSE is represented by 1), $q_1 = -1$, (i.e. TRUE is represented by -1)

$q_{x_i} = y_i$ (i.e. the propositional variable x_i is represented by the algebraic variable y_i)

$q_{\neg A} = -q_A, q_{A \vee B} = \dfrac{q_A q_B + q_A + q_B - 1}{2}$ $\quad q_{A \wedge B_i} = \dfrac{-q_A q_B + q_A + q_B + 1}{2}$ and $q_{A \oplus B} = q_A \cdot q_B$

When working with Fourier basis, rather than the auxiliary polynomials $x_i^2 - x_i$

We use the auxiliary polynomials $y_i^2 - 1$ which ensures $x_i^2 - x_i$ takes value (-+)

Propositional formula A variables $x_1, \ldots, x_n$ when using Fourier basis will be written in the form $(y_1, \ldots, y_m) \in F[(y_1, \ldots, y_m)]$ where $y_1 = 1 - 2x_i$

To obtain degree lower bounds for PC derivation we focus on linear equations equations over GF(2). Fourier representation of linear equation $\sum_{1=1}^{r} x_i + a = 0$ over GF(2) is

$(-1)^{1-a} \prod_{i=1}^{r} \dfrac{1 - x_i}{2} = 0$ which will generally be written in the form $(-1)^{1-a} \prod_{i=1}^{r} y_i = 0$,

Where $y_1 = 1 - 2x_i$. Later introduced is the balanced Fourier representation of the form

$$\prod_{i=1}^{r/2} y_i + (-1)^{1-a} \cdot \prod_{i=[r/2]+1}^{r} y_i = 0$$

The Fourier basis allows for substantial simplification of lower bound arguments for NS and PC

Gaussian Calculus

Definition of Gaussian Calculus

The Gausian Calculus is a refutation system for unsatisfiable set of linear equations over field

Fix prime q, and let $L = \{l_i : 1 \le i \le m\}$ be a set of m linear equations over GF(q) where each l_i has the form

$$\sum_{j \in S_i} a_{i,j} x_j + b_i = 0, \quad \text{where } a_{i,j}, b_i \in \{0,1,\ldots,q-1\}$$

An axiom is a linear equation in L.

Gaussian Calculus

Inference rules of GC

The Gausian Calculus has two rules of inference

- *Scalar multiplication*: From linear equation l to the form

$$\sum_{j \in S} a_j x_j + b = 0$$

Infer the linear equation $\alpha \cdot l$ of the form

$$\sum_{j \in S} \alpha a_j x_j + \alpha b = 0, \text{ where } \alpha \in GF(q)$$

Addition: From linear equations l, l' respectively of the form

$$\sum_{j \in S} a_j x_j + c = 0$$

$$\sum_{j \in S} a_j x_j + d = 0$$

Infer the linear equation $l + l'$ of the form

$$\sum_{j \in S \cup S} (a_j + b_j) x_j + (c + d) = 0$$

Here, if $j \in S - S'$ then $b_j = 0$ if $j \in S' - S$, then $a_j = 0$

Gaussian Calculus

Derivation, refutation and width of GC

A GC derivation of l from L is a finite sequence $E_1, E_2, \ldots, E_r$ of linear equations, such that l is the equation E_r

And for each $1 \le j \le r$,

E_i is either an axiom (i.e. element of L) or

There exist $1 \le j < i$ such that E_i is obtained by scalar multiplication fro E_j or

There exist $1 \le j, k < i$ such that E_i is obtained by addition of E_i, E_k

Often we speak of E_i as the line of derivation.

A GC *refutation* is a derivation of 1=0 from L.

The *width* of a refutation $E_i, \ldots, E_r$ is the maximum number of variables appearing in any E_i , i.e. $\max\{|\mathrm{var}\, s(E_i)| : 1 \le i \le r\}$

The Gaussian width is unsatisfiable set L of linear equations is the minimum length of a refutation of L.

Gaussian Calculus

Completeness of GC

Standard Gaussian elimination proves that

- *Proves that Gaussian calculus is complete, in that if L is usatisfibale set of linear equations over filed F, then there's a refutation of L*

- *Yields that the number of lines in a refutation of an unsatisfiable set* $L = \{l_i : 1 \leq i \leq m\}$ of linear equations in variables $x_i, \ldots, x_n$ in $GF(q)$ is *mn.*

Summary

- The polynomial calculus is a refutation system for unsatisfiable sets of polynomial equations over a field.
- Refutation of a polynomial *P* is a derivation of 1 from *P*
- The degree of refutation is less or equal to the number of polynomials
- Completeness of PC for CNF formulas: constant width resolution refutations can be polynomially simulated by constant degree polynomial calculus refutations
- Automatizability of the polynomial calculus and characterization of degree *d* polynomial calculus derivations
- The Fourier basis which allows for substantial simplification of lower bound arguments for NS and PC
- Definition, derivation, refutation and width of Gaussian Calculus (Introduction)