Zero Equivalence Testing

A. Würfl

21. September 2004

Height of a Polynomial

Definitions

Let $P(X) = p_0X^d + \cdots + p_{d-1}X + p_d$, where $p_0 \neq 0$. Then

Height of a Polynomial

Definitions

Let $P(X) = p_0 X^d + \cdots + p_{d-1} X + p_d$, where $p_0 \neq 0$. Then

- *height* of P(X):
  $||P||_\infty = max\{|p_0|, |p_1|, \ldots, |p_d|\}$

Height of a Polynomial

Definitions

Let $P(X) = p_0X^d + \cdots + p_{d-1}X + p_d$, where $p_0 \neq 0$. Then

- *height* of P(X):
  $||P||_\infty = max\{|p_0|, |p_1|, \ldots, |p_d|\}$
- *2-norm* of $P(X)$:
  $||P||_2 = \left(|p_0|^2 + \cdots + |p_d|^2\right)^{\frac{1}{2}}$

Height of a Polynomial

Definitions

Let $P(X) = p_0X^d + \cdots + p_{d-1}X + p_d$, where $p_0 \neq 0$. Then

- *height* of P(X):
  $||P||_\infty = max\{|p_0|, |p_1|, \ldots, |p_d|\}$
- *2-norm* of $P(X)$:
  $||P||_2 = \left(|p_0|^2 + \cdots + |p_d|^2\right)^{\frac{1}{2}}$
- We use $|P|$ for $||P||_\infty$ and $||P||$ for $||P||_2$

Relationship between these bounds

Propostion 81 *Let P be a univariate polynomial of degree d over $\mathbb{C}$. Then*

$$|P| \leq ||P|| \leq \sqrt{d+1}|P|$$

Definition

Denote the zeros of P(X) by $\alpha_1, \ldots, \alpha_d$. We define M(P) to be

$$M(P) = |p_0| \prod_{1 \leq i \leq d} max\{1, |\alpha_i|\}$$

This norm is called the *M-norm*.

Uniform Coefficient Bounds

Three Different Norms

Uniform Coefficient Bounds

Three Different Norms

- the height of a polynomial, $|P|$

Uniform Coefficient Bounds

Three Different Norms

- the height of a polynomial, $|P|$
- the 2-norm, $||P||$

Uniform Coefficient Bounds

Three Different Norms

- the height of a polynomial, $|P|$
- the 2-norm, $||P||$
- the M-norm, $M(P)$

Relations between these norms

Relations between these norms

- **Propostion 85 (Landau)** *Let $P(X)$ be a univariate polynomial over $\mathbb{C}$, then*

$$M(P) \leq ||P||.$$

Relations between these norms

- **Propostion 85 (Landau)** *Let P(X) be a univariate polynomial over* $\mathbb{C}$*, then*

$$M(P) \leq ||P||.$$

- **Propostion 86** *Let P(X) be a polynomial in* $\mathbb{C}[X]$ *of degree* d*, then*

$$2^{-d}|P| \leq M(P) \leq \sqrt{d+1}|P|.$$

Size of a Polynomial´s Zeros

Propostion 92 (Cauchy)

Let $P(X) = X^d + p_1 X^{d-1} + \cdots + p_d$ be a non-constant, monic polynomial with coefficients in $\mathbb{C}$. Then each root of $P(X)$, α, satisfies the inequality

$$|\alpha| \leq 1 + max\{1, |p_1|, \ldots, |p_n|\} = 1 + |P|.$$

Skip Proof

Proof

Assume $|\alpha|$ is greater than 1, otherwise the proposition is obvious. By taking the absolute value of

$$\alpha^d = -(p_1\alpha^{d-1} + \ldots + p_n),$$

Proof

Assume $|\alpha|$ is greater than 1, otherwise the proposition is obvious. By taking the absolute value of

$$\alpha^d = -(p_1\alpha^{d-1} + \ldots + p_n),$$

we have

$$|\alpha|^d = |p_1\alpha^{d-1} + \ldots + p_n| \leq |\alpha^{d-1} + \ldots + 1| \cdot |P| \leq \frac{|\alpha|^d}{|\alpha| - 1}|P|.$$

Proof

Assume $|\alpha|$ is greater than 1, otherwise the proposition is obvious. By taking the absolute value of

$$\alpha^d = -(p_1\alpha^{d-1} + \ldots + p_n),$$

we have

$$|\alpha|^d = |p_1\alpha^{d-1} + \ldots + p_n| \leq |\alpha^{d-1} + \ldots + 1| \cdot |P| \leq \frac{|\alpha|^d}{|\alpha| - 1}|P|.$$

Since $|\alpha| > 1$, we can multiply by $|\alpha| - 1$ which gives $|\alpha| \leq 1 + |P|$.

Discriminants and Zero Separation

The Vandermonde Matrix

As usual denote the zeros of P(X) by $\alpha_1, \ldots, \alpha_d$ and consider the matrix

$$P_D = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{d-1} \\ \vdots & & \vdots & \ldots & \vdots \\ 1 & \alpha_d & \alpha_d^2 & \ldots & \alpha_d^{d-1} \end{pmatrix}$$

Discriminants and Zero Separation

The Vandermonde Matrix

As usual denote the zeros of P(X) by $\alpha_1, \ldots, \alpha_d$ and consider the matrix

$$P_D = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{d-1} \\ \vdots & & \vdots & \ldots & \vdots \\ 1 & \alpha_d & \alpha_d^2 & \ldots & \alpha_d^{d-1} \end{pmatrix}$$

This is a *Vandermonde matrix*. Its determinant is equal to the product of the difference of the zeros of $P(X)$:

$$det|P_D| = \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j) \, .$$

Discriminant

Definition

The *discriminant* of $P(X)$ is defined to be

$$\mathbf{D}(P) = p_0^{2d-2} det|P_D|^2$$

Proposition 94

If P(X) is a univariate polynomial over $\mathbb{C}$ of degree d and leading coefficient p_0 then the absolute value of the discriminant of P(X) is bounded by

$$|\mathbf{D}(P)| \geq d^d M(P)^{2(d-1)} \geq d^d ||P||^{2(d-1)}.$$

Proposition 95

Let $P(X)$ be a univariate, square free polynomial over $\mathbb{Z}$ of degree d. Denote the number of real zeros of $P(X)$ by r_1 and the number of complex zeros by $2r_2$. Then

$$|\mathbf{D}(P)| \geq (60.1)^{r_1}(22.2)^{2r_2}e^{-254},$$
$$|\mathbf{D}(P)| \geq (58.6)^{r_1}(21.8)^{2r_2}e^{-70},$$

Proposition 95

Let $P(X)$ be a univariate, square free polynomial over $\mathbb{Z}$ of degree d. Denote the number of real zeros of $P(X)$ by r_1 and the number of complex zeros by $2r_2$. Then

$$|\mathbf{D}(P)| \geq (60.1)^{r_1}(22.2)^{2r_2}e^{-254},$$
$$|\mathbf{D}(P)| \geq (58.6)^{r_1}(21.8)^{2r_2}e^{-70},$$

Assuming the generalized Riemann hypothesis

$$|\mathbf{D}(P)| \geq (188.3)^{r_1}(41.6)^{2r_2}e^{-3.7\times 10^8}$$

Riemann Hypothesis

Zero Separation

Definition

We define the *zero separation* of P to be

$$\Delta(P) = \min_{i \neq j} |a_i - a_j|.$$

Proposition 96 (Mahler)

Let $P(x)$ be a square free polynomial of degree d with discriminant $D(P)$. Then

$$\Delta(P) > \sqrt{\frac{3|D(P)|}{d^{d+2}}} M(P)^{1-d}$$

Proposition 96 (Mahler)

Let $P(x)$ be a square free polynomial of degree d with discriminant $D(P)$. Then

$$\Delta(P) > \sqrt{\frac{3|D(P)|}{d^{d+2}}} M(P)^{1-d}$$

Using Proposition 85 we have

$$\Delta(P) > \sqrt{\frac{3|D(P)|}{d^{d+2}}} ||P||^{1-d}.$$

Zero Equivalence Testing

The Black Box Approach

Let $P(X_1, \ldots, X_v)$ be some symoblic expression over a ring R. $\mathcal{B}_P$ is a *black box* representing P if $\mathcal{B}_P(X_1, \ldots, X_v)$ returns $P(x_1, \ldots, x_v)$.

Probabilistic Techniques

Proposition 97

Let A be an integral domain, $P \in A[X_1, \dots, X_v]$ and the degree of P in each of X_i be bounded by d_i. Let $Z_v(B)$ be the number of zeros of P, $\vec{x}$ such that X_i is chosen from a set with B elements, $B \gg d$. Then

$$Z_v(B) \leq (d_1 + d_2 + \ldots + d_v)B^{v-1}.$$

Proof

Proposition 98 (Zippel)

Let $P \in A[X_1, \ldots, X_v]$ be a polynomial of total degree D over an integral domain A. Let $\mathcal{S}$ be a subset of A of cardinality B. Then

$$\mathcal{P}(P(x_1, \ldots, x_v) = 0 | x_i \in \mathcal{S}) \leq \frac{D}{B}.$$

Proof Proposition 97

A Probabilistic Algorithm for Zero Equivalence

$$
\begin{array}{l}
\mathtt{PZeroEquiv}(\mathcal{B}_P, v, D, \epsilon) \;\; \mathtt{:=} \; \{ \\
\quad\quad k \leftarrow 4(log 1/\epsilon)/(\log vD); \\
\quad\quad \mathtt{loop} \;\; \mathtt{for} \;\; 0 \le i < k \;\; \mathtt{do} \;\; \{ \\
\quad\quad\quad \mathtt{if} \;\; \mathcal{B}_P(2^i, 3^i, \ldots, p_v^i) \neq 0 \;\; \mathtt{then} \;\; \mathtt{return(false);} \\
\quad\quad \} \\
\quad\quad \mathtt{return(true);} \\
\}
\end{array}
$$

Deterministic Results

Proposition 100

Let $P(\vec{X})$ be a non-zero polynomial in $R[\vec{X}]$ with at most T terms and with monomial exponent vectors $\vec{e}_i$. Assume there exists an n-tuple $\vec{x}$ (in some R-module) such that the $\vec{x}^{\vec{e}_i}$ are distinct. Then not all of $P(\vec{x}^0), P(\vec{x}^1), P(\vec{x}^2), \ldots, P(\vec{x}^{T-1})$ are zero.

Without Degree Bounds

Proposition 101 (Grigor´ev and Karpinski)

Let $P(\vec{X})$ be a polynomial in v variables over a ring of characteristic zero, A, and assume that P has no more than T monomials. Then there exists a set of v-tuples, $\{\vec{x}_0, \ldots, \vec{x}_{T-1}\}$ such that either $P(\vec{x}_i) \neq 0$ for some $\vec{x}_i$ or P is identically zero.

Skip Proof

Proof

Let $\vec{x} = (2, 3, 5, \ldots, p_v)$, where the entries are the canonical images of the prime numbers of $\mathbb{Z}$ in A. By unique factorization of $\mathbb{Z}$, the monomials $\vec{x}^{\vec{e}_i}$ are distinict, and thus by Proposition 100 either P is identiacally zero or does not vanish at every element of the set $\{\vec{x}^0, \ldots, \vec{x}^{T-1}\}$.

A Deterministic Algorithm Without Degree Bounds

$$
\begin{array}{l}
\mathtt{GKZeroEquiv}(\mathcal{B}_P, n, T) := \{ \\
\quad \mathtt{loop\ for}\ 0 \leq i < T\ \ \mathtt{do}\ \{ \\
\quad\quad \mathtt{if}\ \mathcal{B}_P(2^i, 3^i, \ldots, p_v^i) \neq 0\ \ \mathtt{then}\ \ \mathtt{return(false);} \\
\quad \} \\
\quad \mathtt{return(true);} \\
\}
\end{array}
$$

With Degree Bounds

Linear Substitution

Let R be a field, then $R[Z]$ is a unique factorization domain and $Z+1, Z+2, \ldots$ are primes.

With Degree Bounds

Linear Substitution

Let R be a field, then $R[Z]$ is a unique factorization domain and $Z+1, Z+2, \ldots$ are primes.
Denote by $\vec{Z}$ the vector $(Z+1, Z+2, \ldots, Z+v)$. Thus the $\vec{Z}^{\vec{e}_i}$ are distinct.

With Degree Bounds

Linear Substitution

Let R be a field, then $R[Z]$ is a unique factorization domain and $Z+1, Z+2, \ldots$ are primes.
Denote by $\vec{Z}$ the vector $(Z+1, Z+2, \ldots, Z+v)$. Thus the $\vec{Z}^{\vec{e}_i}$ are distinct.
Sending

$$(X_1, \ldots, X_v) \mapsto (Z+1, \ldots, Z+v) = \vec{Z}$$

maps $P(\vec{X})$ into a univariate polynomial.

A Deterministic Algorithm Using Linear Substitution

```
SDZeroEquiv(B_P, v, D, T) := {
    loop for 0 ≤ i < T do {
        loop for 0 ≤ z ≤ ivD do {
            if B_P((z+1)^i, (z+2)^i, ..., (z+v)^i) ≠ 0
                then return(false);
        }
    }
    return(true);
}
```

$$\mathit{SDZeroEquiv}(\mathcal{B}_P, v, D, T) := \{$$
$$\quad \mathit{loop\ for}\ 0 \leq i < T\ \mathit{do}\ \{$$
$$\quad\quad \mathit{loop\ for}\ 0 \leq z \leq ivD\ \mathit{do}\ \{$$
$$\quad\quad\quad \mathit{if}\ \mathcal{B}_P((z+1)^i, (z+2)^i, \ldots, (z+v)^i) \neq 0$$
$$\quad\quad\quad\quad \mathit{then\ return(false);}$$
$$\quad\quad \}$$
$$\quad \}$$
$$\quad \mathit{return(true);}$$
$$\}$$

Proposition 104

Let $P(x)$ be a univariate polynomial with coefficients in $\mathbb{R}$. The number of positive real zeros of $P(x)$ is less than $terms(p)$.

Nonlinear Substitution

Instead of using the simple linear substitution, we use:

$$(X_1, X_2, \ldots, X_v) \mapsto (Z^{u_1}, Z^{u_2}, \ldots, Z^{u_v})$$

where the u_i are positive integers. We call this substitution a *nonlinear substitution*.

Nonlinear Substitution

Instead of using the simple linear substitution, we use:

$$(X_1, X_2, \ldots, X_v) \mapsto (Z^{u_1}, Z^{u_2}, \ldots, Z^{u_v})$$

where the u_i are positive integers. We call this substitution a *nonlinear substitution*.
The nonlinear substitution sends monomials in $P(\vec{X})$ to univariate monomials in Z, so that $P(Z^{\vec{u}})$ has no more non-zero terms than $P(\vec{X})$.

Nonlinear Substitution

Instead of using the simple linear substitution, we use:

$$(X_1, X_2, \ldots, X_v) \mapsto (Z^{u_1}, Z^{u_2}, \ldots, Z^{u_v})$$

where the u_i are positive integers. We call this substitution a *nonlinear substitution*.

The nonlinear substitution sends monomials in $P(\vec{X})$ to univariate monomials in Z, so that $P(Z^{\vec{u}})$ has no more non-zero terms than $P(\vec{X})$.

Difficulty: finding a vector $\vec{u}$ such that $P(Z^{\vec{u}})$ is not identically zero

Definition

Let $\mathcal{U}$ be a set of v-tuples with components in $\mathbb{Z}$. $\mathcal{U}$ is said to be **maximally independent** *if every subset of n elements of $\mathcal{U}$ is R-linearly independent.*

Definition

Let $\mathcal{U}$ be a set of v-tuples with components in $\mathbb{Z}$. $\mathcal{U}$ is said to be **maximally independent** *if every subset of n elements of $\mathcal{U}$ is R-linearly independent.*

Idea:

The exponents $u_1, \ldots, u_v$ should come from a large set of maximally independent v-tuples.

Construction of a maximally independent set of v-tuples

Let p be a prime such that $S < p < 2S$. Using the following definition for $\mathcal{U}_{S,v}$

$$\mathcal{U}_{S,v} = \begin{array}{l} \{(1, i, i^2 \bmod p, \ldots, i^{v-1} \bmod p) | 1 \leq i \leq v\} \\ \{((i+1)^{-1} \bmod p, \ldots, (i+v)^{-1} \bmod p) | 1 \leq i \leq v\} \end{array}$$

Construction of a maximally independent set of v-tuples

Let p be a prime such that $S < p < 2S$. Using the following definition for $\mathcal{U}_{S,v}$

$$\mathcal{U}_{S,v} = \begin{array}{l} \{(1, i, i^2 \bmod p, \ldots, i^{v-1} \bmod p) | 1 \leq i \leq v\} \\ \{((i+1)^{-1} \bmod p, \ldots, (i+v)^{-1} \bmod p) | 1 \leq i \leq v\} \end{array}$$

we obtain a set of maximally independent v-tuples $\mathcal{U}_{S,v}$, where the components of each vetor are positive and less than 2S.

Proposition 106

For every non-zero polynomial $P(X_1, \ldots, X_v)$ with no more than T non-zero terms and the degree of each X_i bounded by D there is a $\vec{u}$ in $\mathcal{U}_{vT,v}$ such that $P(Z^{\vec{u}})$ is not identically zero. Furthermore, the degree of $P(Z^{\vec{u}})$ is less than $2v^2DT$ and $P(Z^{\vec{u}})$ has no more than T non-zero terms.

Proof

Zero Equivalence Algorithm Using Nonlinear Substitution

$$
\begin{array}{l}
\mathit{RDZeroEquiv}(\mathcal{B}_P, v, T) := \{ \\
\quad \mathit{loop\ for}\ \vec{u} \in \mathcal{U}_{vT,v}\ \ \mathit{do}\ \{ \\
\quad\quad \mathit{loop\ for}\ 0 \le z \le T\ \ \mathit{do}\ \{ \\
\quad\quad\quad \mathit{if}\ \mathcal{B}_P(z^{u_1}, z^{u_2}, \ldots, z^{u_v}) \neq 0 \\
\quad\quad\quad\quad \mathit{then\ return(false);} \\
\quad\quad \} \\
\quad \} \\
\quad \mathit{return(true);} \\
\}
\end{array}
$$

Complexity of different substitutions

	# poly	# terms	degree	points
Linear	T	$\leq vDT$	$\leq vDT$	$vDT^2 + T$
Nonlinear	vT	$\leq T$	$\leq v^2DT$	vT^2

Finite Fields

Problem:

Take the coeffiecient domain be $\mathbb{F}_p$ and consider the polynomial

$$M(X) = X^p - X.$$

M(X) vanishes for every element of $\mathbb{F}_p$.

Finite Fields

Problem:

Take the coeffiecient domain be $\mathbb{F}_p$ and consider the polynomial

$$M(X) = X^p - X.$$

M(X) vanishes for every element of $\mathbb{F}_p$.

This issue means that it is not possible to do *deterministic* zero testing for polynomials over a finite field *without degree bounds*. However, the problem is solvable if we have degree bounds on the black box.

Let $\mathcal{B}_Q$ be a black box for a polynomial Q. Assume Q is a univariate polynomial of degree d, with T terms, with coefficients in $\mathbb{F}_p$:

$$Q(X) = q_1 X^{e_1} + q_2 X^{e_2} + \ldots + q_T X^{e_T},$$

where $e_i \leq d$.

Let $\mathcal{B}_Q$ be a black box for a polynomial Q. Assume Q is a univariate polynomial of degree d, with T terms, with coefficients in $\mathbb{F}_p$:

$$Q(X) = q_1 X^{e_1} + q_2 X^{e_2} + \ldots + q_T X^{e_T},$$

where $e_i \leq d$. Using Proposition 100, the sequence of evaluation points, $1, m, m^2, \ldots$ will be a distinguishing sequence if each of the values

$$m^{e_1}, m^{e_2}, \ldots, m^{e_T}$$

are distinct.

Let $\mathcal{B}_Q$ be a black box for a polynomial Q. Assume Q is a univariate polynomial of degree d, with T terms, with coefficients in $\mathbb{F}_p$:

$$Q(X) = q_1 X^{e_1} + q_2 X^{e_2} + \ldots + q_T X^{e_T},$$

where $e_i \leq d$. Using Proposition 100, the sequence of evaluation points, $1, m, m^2, \ldots$ will be a distinguishing sequence if each of the values

$$m^{e_1}, m^{e_2}, \ldots, m^{e_T}$$

are distinct. If the multiplicative order of m is greater than d, then these values are certainly distinct.

Solution:

Enlarge the ground field $\mathbb{F}_p$ to $\mathbb{F}_{p^k}$ which does have elements of order d.

Solution:

Enlarge the ground field $\mathbb{F}_p$ to $\mathbb{F}_{p^k}$ which does have elements of order d.

- the characteristic of the ground field is very large, $p > 2^d$, $m = 2$ will suffice

Solution:

Enlarge the ground field $\mathbb{F}_p$ to $\mathbb{F}_{p^k}$ which does have elements of order d.

- the characteristic of the ground field is very large, $p > 2^d$, $m = 2$ will suffice
- if p is small we expand $\mathbb{F}_p$ by adjoining an element of degree k over $\mathbb{F}_p$, where $p^k > d$

Solution:

Enlarge the ground field $\mathbb{F}_p$ to $\mathbb{F}_{p^k}$ which does have elements of order d.

- the characteristic of the ground field is very large, $p > 2^d$, $m = 2$ will suffice
- if p is small we expand $\mathbb{F}_p$ by adjoining an element of degree k over $\mathbb{F}_p$, where $p^k > d$
- if p is very large we construct a degree extension of $\mathbb{F}_p$ of degree K, where $K > d$

Negative Results

Computational Complexity

The zero equivalence problem with only degree bounds, and no bound on the number of terms, is not solvable in deterministic polynomial time:

Negative Results

Computational Complexity

The zero equivalence problem with only degree bounds, and no bound on the number of terms, is not solvable in deterministic polynomial time:

Proposition 108

Given a black box representing a polynomial $P(\vec{X})$ in v variables and of degree less than D in each variable, any deterministic algorithm that determines if P is the zero polynomial runs in time at least $O(D^v)$.

Complexity of Zero Testing

	Probabilistic	Deterministic
degree bounds	$\log \frac{1}{\epsilon} \cdot \log^{r-1} vD$	$D^v \log^r D$
term bounds		$T^{r+1} \log^r v$

r is a constant corresponding to the type of arithmetic being used by $\mathcal{B}_P$. For classical arithmetic $r = 2$; for fast arithmetic r is slightly greater than 1.

Thank you for your attention!

Appendix

Proofs

Proof (Proposition 97)

There are at most d_v values of X_v at which P is identically zero. So for any of these d_v values of X_v and any value for the other X_i, P is zero. This comes to $d_v B^{v-1}$. For all other $b - d_v$ values of X_v we have a polynomial in $v - 1$ variables. The polynomial can have no more than $Z_{v-1}(B)$ zeros. Therefore,

$$Z_v(B) \leq d_v B^{v-1} + (B - d_v) Z_{v-1}(B).$$

Rather than solving this recurrence for Z_v, we solve it for $N_v = B^v - Z_v$. Since Z_1 is less than or equal to d_1, $N_v \geq (B - d_1)$. This is the basic step of the inductive proof. Writing the recurrence in terms of N_v we have

$$B^v - N_v(B) \leq d_v B^{v-1} + (B - d_v)(B^{v-1} - N_{v-1}(B)).$$

or

$$N_v(B) \geq (B - d_v)N_{v-1}(B),$$

the proposition follows with

$$B^v - (B - d_1)(B - d_2)\dots(B - d_v) \geq (d_1 + d_2 + \dots + d_v)B^{v-1}.$$

Back

Proof (Proposition 98)

We use induction on the number of variables as was done in the proof of the previous proposition.
For $v = 1$, f is univariate polynomial of degree D and can have no more than D zeros in A, so

$$\mathcal{P}(P(x_1) = 0 | x_1 \in \mathcal{S}) \leq \frac{D}{B}.$$

Assume the proposition is true for polynomials in $v-1$ variables. Let the degree of P in X_v be d_v and denote the leading coefficient of f with respect to X_v by f_0, *i.e.*,

$$P = p_0(X_1 \ldots, X_{v-1})X_v^d + \ldots.$$

The total degree of p_0 is no more than $D-d$, so the probability that $p_0 = 0$ is

$$\mathcal{P}(p_0(x_1, \ldots, x_v) = 0 | x_i \in \mathcal{S}) \leq \frac{D-d}{B}.$$

Omitting the arguments of $x_1, \ldots, x_v$ and $x_1, \ldots, x_{v-1}$ for brevity, we can write

$$\begin{aligned}\mathcal{P}(P = 0) = \mathcal{P}(P = 0 \wedge p_0 = 0) \cdot \mathcal{P}(p_0 = 0) \\ + \mathcal{P}(P = 0 \wedge p_0 \neq 0) \cdot \mathcal{P}(p_0 \neq 0), \\ \leq \mathcal{P}(p_0) + \mathcal{P}(P = 0 \wedge p_0 \neq p).\end{aligned}$$

Assume that $p_0(x_1, \ldots, x_{v-1}) \neq 0$. $P(x_1, \ldots, x_{v-1}, X_v)$ is a polynomial of degree d, so there are at most d $x_v \in$ scr S such that $P(x_1, \ldots, x_v) = 0$. Consequently,

$$\mathcal{P}(P(x_1, \ldots, x_v) = 0 | x_i \in \mathcal{S}) \leq \frac{D-d}{B} + \frac{d}{B} = \frac{D}{B}.$$

Back

Proof (Proposition 106)

Let the non-zero terms of P be

$$P(\vec{X}) = c_1\vec{X}^{\vec{e}_1} + c_2\vec{X}^{\vec{e}_2} + \ldots + c_T\vec{X}^{\vec{e}_T}$$

The substitution $X_i \mapsto Z^{u_i}$ transforms this polynomial into

$$P(\vec{Z}) = c_1\vec{Z}^{\vec{e}_1\cdot\vec{u}} + c_2\vec{Z}^{\vec{e}_2\cdot\vec{u}} + \ldots + c_T\vec{Z}^{\vec{e}_T\cdot\vec{u}}$$

To find a substitution for which $P(Z^{\vec{u}})$ is not identically zero we require $\vec{u}$ satisfy

$$\vec{e}_1 \cdot \vec{u} \neq \vec{e}_i \cdot \vec{u},$$

or equivalently $(\vec{e}_i - \vec{e}_1)\cdot\vec{u} \neq 0$, for $2 \leq i < T$. Let $d = \vec{e}_1 \cdot \vec{u}_1$.

With such a substitution only one monomial in $P(\vec{X})$ will be mapped to a term in $P(Z)$ of degree d, namely the $c_1\vec{X}^{\vec{e}_1}$ term. Since $c_1 \neq 0$, $P(Z)$ cannot be identically zero; it must contain a Z^d term. Letting $L_i(\vec{w}) = (\vec{e}_i - \vec{e}_1) \cdot \vec{w}$, $2 \leq i < T$ we want to find a $\vec{u}$ at which none of the L_i vanish. Let $\vec{w}_1, \ldots, \vec{w}_v$ be destinct elements of $\mathcal{U}_{vT,v}$, so

$$\begin{pmatrix} \vec{w}_1 \\ \vdots \\ \vec{w}_v \end{pmatrix} \cdot (\vec{e}_i - \vec{e}_1) = A \cdot (\vec{e}_i - \vec{e}_1) = \begin{pmatrix} L_i(\vec{w}_1) \\ \vdots \\ L_i(\vec{w}_v) \end{pmatrix}$$

Since A is non-singular, the right hand side can only be zero if L_i is identically zero. Thus, L_i cannot vanish for more than $n-1$ of the elements of $\mathcal{U}_{vT,v}$. There are $T-1$ L_i´s. Since $(v-1)\cdot(T-1)$ is less than vT, there must be at least one element of $\mathcal{U}_{vT,v}$ for which none of the L_i vanish as desired. We denote such an element by $\vec{u}$. Each of the components of $\vec{u}$ is less than $2nT$, while the elements of $\vec{e}_i$ are less than D. Thus the degree of $P(Z^{\vec{u}})$ is less than $2v^2DT$.

Back

Riemann Hypothesis

In his 1859 paper *On the Number of Primes Less Than a Given Magnitude*, Bernhard Riemann (1826-1866) examined the properties of the function

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s},$$

for s a complex number. This function is analytic for real part of s greater than 1.

It is realted to the prime numbers by the Euler Product Formula

$$\zeta(s) = \prod_{p \text{ prim}} (1 - p^{-s})^{-1},$$

again definied for real part of s greater than one.

Riemann hypothesis

The nontrivial zeros of $\zeta(s)$ *have real part equal to* $\frac{1}{2}$.

Riemann hypothesis

The nontrivial zeros of $\zeta(s)$ have real part equal to $\frac{1}{2}$.

Back