Polynomial Identity Testing

Anil Maheshwari

anil@scs.carleton.ca
School of Computer Science
Carleton University
Canada

Outline

Polynomial Identity Testing

String Equality Testing

Alice-Bob String Testing Problem

Assume Alice has a binary string $A = a_1 a_2 \ldots a_n$ and Bob has a binary string $B = b_1 b_2 \ldots b_n$. What is minimum amount of communication required to test whether $A = B$?

Randomized Algorithm

Define $A(x) = \sum_{i=1}^{n} a_i x^i$ and $B(x) = \sum_{i=1}^{n} b_i x^i$, where $x \in F$.
F is a Field defined with modular arithmetic for a large prime number p.

Algorithm:

1. Pick a random element $\alpha \in F$
2. Alice computes $A(\alpha)$ and sends $(\alpha, A(\alpha))$ to Bob
3. Bob computes $B(\alpha)$
4. Bob communicates to Alice True if $B(\alpha) = A(\alpha)$, else False

Analysis of Randomized Algorithm

Case I: $A = B$: Algorithms reports TRUE as $A(\alpha) = B(\alpha)$ no matter what is the value $\alpha \in F$

Case II: Assume $A \neq B$.
Can algorithm make an error?

Yes, if α is the root of the polynomial $(A - B)x = 0$.

Pr(a random element of F is root of $(A - B)x$) $\leq n/|F|$

Question: How to increase the success probability?

Communication Complexity: $O(\log |F|)$ bits.

Polynomials of degree d

Two polynomials $\mathcal{P}(x)$ and $\mathcal{Q}(x)$ of degree d.
Output: Is $\mathcal{P}(x) \equiv \mathcal{Q}(x)$?

Example: Is $(2-x)(x-5)(x^2-12) = -x^4 + 7x^3 + 2x^2 - 84x + 120$?

Answer: Expand and Check.
Alternatively, evaluate the polynomials at a random point in $\{1, \ldots, 100d\}$.

For example
$x = 20$, both of them evaluate to -104760.
$x = 29$, both of them evaluate to -537192

$\implies$ Check whether $\mathcal{P}(x) - \mathcal{Q}(x) = 0$?

Polynomials of degree d

Suppose $\mathcal{P}(x) \not\equiv \mathcal{Q}(x)$.
For Example:
$\mathcal{P}(x) = 2x^4 - 20x^3 + 50x^2 - 80x + 21$
$\mathcal{Q}(x) = x^4 - 8x^3 + x^2 - 2x - 19$
$\mathcal{P}(x) - \mathcal{Q}(x) = (x-1)(x-2)(x-4)(x-5) \neq 0$

What is the probability that a random element $\alpha \in \{1, \ldots, 100d\}$ will satisfy $\mathcal{P}(\alpha) - \mathcal{Q}(\alpha) = 0$?

If the random element $\alpha \in \{1, 2, 4, 5\}$ than $\mathcal{P}(\alpha) - \mathcal{Q}(\alpha) = 0$.

Probability of making an error $\leq \frac{d}{100d} = \frac{4}{400} = 0.01$

$\implies$ Probability of determining that $\mathcal{P}(x) \not\equiv \mathcal{Q}(x) \geq 1 - 0.01 = 0.99$

How can we improve the probability of success?

Decreasing Failure Probability

If $\mathcal{P}(x) \not\equiv \mathcal{Q}(x)$, probability of failure is $\leq \frac{d}{100d} = \frac{1}{100} = 0.01$

What if we repeat this experiment with multiple values of $\alpha \in \{1, \ldots, 100d\}$.

How to choose multiple values of α?

Choice 1: With replacement (same value may be chosen multiple times)

Choice 2: Without replacement (all chosen values are distinct)

With or Without Replacement Sampling

Decreasing Failure Probability - With Replacement

Consider repeating the experiment $k > 0$ times **with** replacement.
If in any of the trials we find that $\mathcal{P}(\alpha) - \mathcal{Q}(\alpha) \neq 0$, we report $\mathcal{P}(x) \not\equiv \mathcal{Q}(x)$, otherwise we report $\mathcal{P}(x) \equiv \mathcal{Q}(x)$.

Observe:
- If in any of the k trials, we find $\mathcal{P}(\alpha) - \mathcal{Q}(\alpha) \neq 0$, then for sure $\mathcal{P}(x) \not\equiv \mathcal{Q}(x)$, and we answer correctly.

- Suppose, $\mathcal{P}(x) \not\equiv \mathcal{Q}(x)$, but in each of the trials we find that $\mathcal{P}(\alpha) - \mathcal{Q}(\alpha) = 0$
Probability of making error $\leq \left(\frac{d}{100d}\right)^k = \left(\frac{1}{100}\right)^k$.
For example with $k = 2$, the probability of error is $\leq 0.01^2 = 0.0001$

Decreasing Failure Probability - Without Replacement

Consider repeating the experiment $k > 0$ times **without** replacement.
If in any of the trials we find that $\mathcal{P}(\alpha) - \mathcal{Q}(\alpha) \neq 0$, we report $\mathcal{P}(x) \not\equiv \mathcal{Q}(x)$, otherwise we report $\mathcal{P}(x) \equiv \mathcal{Q}(x)$.

Observe:
- If in any of the k trials, we find $\mathcal{P}(\alpha) - \mathcal{Q}(\alpha) \neq 0$, then for sure $\mathcal{P}(x) \not\equiv \mathcal{Q}(x)$, and we answer correctly.

- Suppose, $\mathcal{P}(x) \not\equiv \mathcal{Q}(x)$, but in each of the trials we find that $\mathcal{P}(\alpha) - \mathcal{Q}(\alpha) = 0$
Let us call events $E_1, \ldots, E_k$ be the k-events where event E_i states that the random number chosen in the i-th trial is a root of the polynomial $\mathcal{P}(x) - \mathcal{Q}(x)$.

Probability of getting a wrong answer is $Pr(E_1 \cap E_2 \cap \ldots \cap E_k)$

Decreasing Failure Probability - Without Replacement (contd.)

Recall that $Pr(A \cap B) = Pr(A|B) \cdot Pr(B)$, assuming $Pr(B) \neq 0$

$Pr(E_1 \cap E_2 \cap \ldots \cap E_k)$
$= Pr(E_k|E_1 \cap E_2 \cap \ldots \cap E_{k-1}) \cdot Pr(E_1 \cap E_2 \cap \ldots \cap E_{k-1})$
$= Pr(E_k|E_1 \cap E_2 \cap \ldots \cap E_{k-1}) \cdot Pr(E_{k-1}|E_1 \cap E_2 \cap \ldots \cap E_{k-2}) \cdot Pr(E_1 \cap E_2 \cap \ldots \cap E_{k-2})$
$\ldots$
$= Pr(E_1) \cdot Pr(E_1|E_2) \cdot Pr(E_3|E_1 \cap E_2) \cdots Pr(E_k|E_1 \cap E_2 \cap \ldots \cap E_{k-1})$

Question: How to bound $Pr(E_j|E_1 \cap E_2 \cap \ldots \cap E_{j-1})$?

We have already chosen $j-1$ roots for the events $E_1, \ldots, E_{j-1}$. Only $\leq d-(j-1)$ roots are remaining.
Probability of choosing one of the remaining roots (defining the event E_j)
$Pr(E_j|E_1 \cap E_2 \cap \ldots \cap E_{j-1}) \leq \frac{d-(j-1)}{100d-(j-1)} < \frac{d}{100d} = \frac{1}{100}$

Thus, $Pr(E_1 \cap E_2 \cap \ldots \cap E_k) \leq \prod_{j=1}^{k} \frac{d-(j-1)}{100d-(j-1)} \leq \left(\frac{1}{100}\right)^k$

Decreasing Failure Probability - Without Replacement (contd.)

For $k \geq 2$, $Pr(E_1 \cap E_2 \cap \ldots \cap E_k) \leq \prod_{j=1}^{k} \frac{d-(j-1)}{100d-(j-1)} < \left(\frac{1}{100}\right)^k$.

For example, for $k = 2$ and $d = 4$, the probability of error is $\leq \left(\frac{4}{400}\right)\left(\frac{3}{399}\right) = 0.000075 < 0.01^2 (= 0.0001)$

Ideally we should use **without replacement** strategy, but
- Analysis is tedious.
- Bit complex to code

In practice, employ **with replacement** strategy
- Analysis is simpler
- Probability of making an error is still negligible
- Easier to code

Matrix Product Verification

Verifying Matrix Product

Input: Three $n \times n$ real matrices A, B and C.
Output: Is $C = AB$?

1st Approach: Evaluate AB and compare with C.
- Requires computation of AB
- Time Complexity: $O(n^3), O(n^{\log_2 7}), \ldots$

2nd Approach: Find almost the right answer

Randomized algorithm for matrix product testing

Step 1: Compute a (uniformly at) random Boolean vector r of dimension n.

Step 2: Compute $A(Br)$ and Cr

Step3: If $A(Br) \neq Cr$, report $AB \neq C$,
Otherwise, report $AB = C$

Analysis of Randomized Algorithm

Time Complexity:

Computation of the product of $n \times n$ matrix with a vector of size n takes $\Theta(n^2)$ time.

Thus,
- Computation of Br takes $O(n^2)$ time resulting in a vector of size n
- Computation of $A(Br)$ takes $O(n^2)$ time
- Computation of Cr takes $O(n^2)$ time
- Testing $Cr = A(Br)$ takes $O(n)$ time.

Total Complexity = $O(n^2)$

Correctness

- If $ABr \neq Cr \implies AB \neq C$.

- But if $ABr = Cr$, AB may or may not be equal to C.
(algorithm incurs one-sided error)

Bounding Failure Probability

One-sided error

Let r be a (uniform) random n-dimensional Boolean vector and $C \neq AB$.
$Pr(ABr = Cr) \leq \frac{1}{2}$

Proof: Let $D = C - AB$. Since $C \neq AB$, $D \neq 0$.
Moreover, since $ABr = Cr \implies (AB - C)r = 0 \implies Dr = 0$.
Since $D \neq 0$, there is an entry, say $d_{ij} \neq 0$.
Since $Dr = 0$, we have that $\sum_{k=1}^{n} d_{ik} r_k = 0$.

We can express $r_j = -\frac{\sum_{k=1}^{j-1} d_{ik} r_k + \sum_{k=j+1}^{n} d_{ik} r_k}{d_{ij}}$
Since only a specific value of r_j satisfies this equation, and we can choose r_j to be either 0 or 1 with equal probability, thus $Pr(Dr = 0) \leq \frac{1}{2}$.

$\square$

To increase the success probability, we can run the experiment k times.
Error probability $\leq \left(\frac{1}{2}\right)^k$
Running Time = $O(kn^2)$

Schwartz-Zippel Lemma

Determine if the multivariate polynomial $\mathcal{Q}(x_1, x_2, \ldots, x_n) \equiv 0$?

Example I:

$$\mathcal{Q}(x_1, x_2, x_3, x_4) = (x_1^3 - x_2^2)(-x_1^2 - x_3^4)(x_4^3 - 2x_1x_2) \equiv 0$$

Example II:

$$\text{Det} \begin{vmatrix} x_1 - x_2^2 & x_3 - x_1 & x_4^2 & x_4 - x_1 \\ -x_2^4 & x_2 - x_4 & 2x_3 - 7x_1 & x_2^2 - x_3^2 \\ x_1^3 & x_2 - x_1 & x_4 - x_3 & x_2^3 \\ x_2^3 & x_4 - 2x_2 & x_1 - x_3^2 & x_1^3 - x_2^3 \end{vmatrix} \equiv 0$$

Schwartz–Zippel Lemma

Let $\mathcal{Q}(x_1, x_2, \ldots, x_n) \not\equiv 0$ be a multivariate polynomial of total degree d, where each x_i takes value from a finite field $\mathcal{F}$. Fix any finite set $S \subseteq \mathcal{F}$ and let $r_1, \ldots, r_n$ be chosen uniformly at random from S. Then $Pr(\mathcal{Q}(r_1, \ldots, r_n) = 0) \leq \frac{d}{|S|}$

Proof: Technique: Induction on number of variables n.
Base Case: $n = 1$. Degree d polynomial in a single variable x_1 has at most d distinct roots. Thus $Pr(\mathcal{Q}(x_1 = r_1) = 0) \leq \frac{d}{|S|}$, as this polynomial is zero only if r_1 is a root of $\mathcal{Q}$, where r_1 is a random element from S.

Assume the induction hypothesis holds for all polynomials of fewer than n-variables.

Observe that $\mathcal{Q}(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{k} x_1^i \mathcal{Q}_i(x_2, \ldots, x_n)$, where $k \leq d$ is the highest degree of x_1 in $\mathcal{Q}(x_1, x_2, \ldots, x_n)$. Note that $\mathcal{Q}_k(x_2, \ldots, x_n) \neq 0$ and moreover its degree is $d - k < d$.

Schwartz–Zippel Lemma (Proof contd.)

Thus, by setting $x_2 = r_2, \ldots, x_n = r_n$, and using I.H on $n-1$ variables, we have $Pr(\mathcal{Q}_k(r_2, \ldots, r_n) = 0) \leq \frac{d-k}{|S|}$

Assume that $\mathcal{Q}_k(r_2, \ldots, r_n) \neq 0$ and consider the single variable polynomial of degree k, $\mathcal{Q}(x_1, r_2, \ldots, r_n)$. By I.H. $Pr(\mathcal{Q}(x_1 = r_1, r_2, \ldots, r_n) = 0) \leq \frac{k}{|S|}$.

Hence,

$Pr(\mathcal{Q}(r_1, r_2, \ldots, r_n) = 0) = Pr(\mathcal{Q}(r_1, r_2, \ldots, r_n) = 0 | Pr(\mathcal{Q}_k(r_2, \ldots, r_n) = 0) \times Pr(\mathcal{Q}_k(r_2, \ldots, r_n) = 0) + Pr(\mathcal{Q}(r_1, r_2, \ldots, r_n) = 0 | Pr(\mathcal{Q}_k(r_2, \ldots, r_n) \neq 0) \times Pr(\mathcal{Q}_k(r_2, \ldots, r_n) \neq 0)$

$Pr(\mathcal{Q}(r_1, r_2, \ldots, r_n) = 0) \leq 1 \times \frac{d-k}{|S|} + \frac{k}{|S|} \times 1 = \frac{d}{|S|}$

$\square$

Testing Determinants

Is Det $\begin{vmatrix} x_1 - x_2^2 & x_3 - x_1 & x_4^2 & x_4 - x_1 \\ -x_2^4 & x_2 - x_4 & 2x_3 - 7x_1 & x_2^2 - x_3^2 \\ x_1^3 & x_2 - x_1 & x_4 - x_3 & x_2^3 \\ x_2^3 & x_4 - 2x_2 & x_1 - x_3^2 & x_1^3 - x_2^3 \end{vmatrix} \equiv 0$?

Choose a large enough prime number p, and choose random values for x_1, x_2, x_3, x_4 from $\{0, \ldots, p-1\}$.

Evaluate the determinant.

Probability of one sided error $\leq \frac{d}{p}$,
where d is the degree of the polynomial.

Bipartite Matching

Bipartite Matching

Let $G = (U \cup V, E)$ be a bipartite graph, where $|U| = |V| = n$.

$M \subseteq E$ is a perfect matching if

1. $|M| = n$
2. Edges in M are independent, i.e. vertex disjoint.

Adjacency Matrix

Define $n \times n$ matrix A where,

$$A_{ij} = \begin{cases} x_{ij}, \text{ if } u_i v_j \in E \\ 0, \text{ otherwise} \end{cases}$$

$$\begin{vmatrix} x_{11} & x_{12} & 0 \\ x_{21} & x_{22} & 0 \\ x_{31} & x_{32} & x_{33} \end{vmatrix}$$

$$\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ 0 & x_{22} & 0 \\ 0 & x_{32} & 0 \end{vmatrix}$$

Edmonds Theorem

Edmonds

A bipartite graph G has a perfect matching if and only if $det(A) \neq 0$.

Decision Problem

Input: Given a bipartite graph $G = (U \cup V, E)$, where $|U| = |V|$

Output: TRUE if G has perfect matching, otherwise FALSE

Randomized Algorithm:

1. Choose a large enough prime number p.
2. For each edge $u_i v_j$, set x_{ij} to be a random value in $\{0, \ldots, p-1\}$ uniformly at random.
3. Compute $det(A)$
4. Return TRUE iff $det(A) \neq 0$.

Analysis

1. Choose a large enough prime number.
2. For each edge u_iv_j, set x_{ij} to be a random value in $\{0, \ldots, p-1\}$ uniformly at random.
3. Compute $det(A)$
4. Return TRUE iff $det(A) \neq 0$.

Case 1: If G has no perfect matching $\implies det(A) = 0$

Case 2: If G has perfect matching $\implies det(A) \neq 0$ (Edmonds)

Degree of determinant polynomial is $\leq n = |U|$

Pr(det(A)=0 given that G has a perfect matching) $\leq n/p$ (Schwartz-Zippel)

Choose $p \approx 1000n$,
Probability of success $\geq 1 - 1/1000$

Finding a Perfect Matching

How to find a perfect matching

Isolation Lemma (MVV87)

Assume we have set system $\mathcal{S}$ on a ground set of n elements. Assign weights to each element uniformly and at random from $\{1, 2, \ldots, 2n\}$. The probability that there is a unique minimum weight set in $\mathcal{S}$ is $\geq \frac{1}{2}$

This result is counterintuitive:

- There are $\approx 2^n$ possible subsets on n-elements.

- The weight of any non-empty set $X \in \mathcal{S}$ is in the range $1 \leq wt(X) \leq 2n^2$.

- We expect almost $\frac{2^n}{2n^2}$ sets for each weight

- Why with probability $\geq \frac{1}{2}$, minimum weight set is unique?

Proof of Isolation Lemma

This proof is credited to Joel Spencer - see wikipedia on Isolation Lemma.

For an element v, let $\mathcal{F}_v$ be sets in $\mathcal{S}$ that contains v and let $\mathcal{F}_{\bar{v}}$ be sets in $\mathcal{S}$ that do not contain v.

Let $\alpha(v) = \min_{A \in \mathcal{F}_{\bar{v}}} w(A) - \min_{B \in \mathcal{F}_v} w(B - \{v\})$.

Observation: $\alpha(v)$ depends only on weights of all other elements except the weight of v.

$\implies Pr(\alpha(v) = w(v)) = \frac{1}{2n}$

Thus, for some element v of ground set $Pr(\alpha(v) = w(v)) \leq \frac{1}{2}$ (by Union Bound)

Proof of Isolation Lemma (contd.)

Assume that there are two distinct sets X and Y that have minimum weight in $\mathcal{F}$. Consider an element $v \in X \setminus Y$.

Now observe that

$$\begin{aligned}
\alpha(v) &= \min_{A \in \mathcal{F}_{\bar{v}}} w(A) - \min_{B \in \mathcal{F}_v} w(B - \{v\}) \\
&= w(Y) - w(X - \{v\}) \\
&= w(v)
\end{aligned}$$

But this happens with probability at most $\frac{1}{2}$.
Thus with probability $\geq \frac{1}{2}$, the minimum weight set is unique.

$\square$

Finding a Perfect Matching

- Let $G = (U \cup V, E)$ and $|E| = m$.
- Assume G has a perfect matching.
- For each edge $e \in E$, assign a weight in $\{1, \ldots, 2m\}$ uniformly at random.
- Let $\mathcal{M}$= Set system consisting of all perfect matchings
- Isolation Lemma: $\exists M \in \mathcal{M}$ of unique minimum weight with probability $\geq 1/2$.

New Problem

Find (unique) minimum weight perfect matching M in G

Unique MWPM

Let unique MWPM has a total weight $W \leq 2m^2$.
For each edge $e = (u_i v_j) \in E$ with weight $w(e)$,
set $x_{ij} = 2^{w(e)}$ in det(A).

Consider the non-zero terms in the expansion of $det(A)$.

Observation: Only one term is 2^W and all other terms are $\geq 2^{W+1} = 2 * 2^W$.

Unique MWPM (contd.)

Note:

$$\frac{det(A)}{2^k} = \begin{cases} \text{odd, if } k = W \\ \text{even, if } k < W \\ \text{fractional, if } k > W \end{cases}$$

Algorithm:

1. Find k: Guess k and check parity of $\frac{det(A)}{2^k}$
2. For each edge $e = (uv)$, it is in unique MWPM if and only if MWPM in $G \setminus \{u, v\}$ has weight $W - w(e)$.

Note: Computation of det(A), Guess & Check k, and Testing $\forall e \in E$ is part of unique MWPM are parallelizable.

Matching in General Graphs

Let $G = (V, E)$ be a general graph.

Define

$$A_{ij} = \begin{cases} +x_{ij}, \text{ if } v_i v_j \in E \text{ and i<j} \\ -x_{ij}, \text{ if } v_i v_j \in E \text{ and i>j} \\ 0, \text{ otherwise} \end{cases}$$

Tutte

G has a perfect matching if and only if $det(A) \neq 0$.

References

References

1. Mitzenmacher and Upfal, Probability and Computing, Cambridge.
2. Motwani and Raghavan, Randomized Algorithm, Cambridge.
3. Mulmuley, Vazirani and Vazirani, Matching is as easy as matrix inversion, Combinatorica 7(1):105-113, 1987.
4. DeMillo and Lipton, A probabilistic remark on algebraic program testing, Information Processing Letters 7(4):193-195, 1978.