Polishchuk-Spielman Bivariate Testing and An Application

Ziyang Jin[1]

[1]Theory Student Seminar
University of Toronto
27 Feb 2025

Table of Contents

UNIVERSITY OF TORONTO

Definitions

Let $\mathcal{F}$ be a finite field. We consider bivariate polynomials over a domain $X \times Y$, where $X = \{x_1, \dots, x_n\} \subseteq \mathcal{F}$ and $Y = \{y_1, \dots, y_n\} \subseteq \mathcal{F}$.

A polynomial $p(x, y)$ has degree (d, e) if it has degree at most d is x and degree at most e in y. When we say a polynomial of degree d, we mean a polynomial of degree at most d. We use them interchangeably.

Suppose we have a function $f(x, y)$ on $X \times Y$. We can represent $f(x, y)$ in matrix form as follows:

$$M = \begin{pmatrix} f(x_1, y_1) & f(x_1, y_2) & \dots & f(x_1, y_n) \\ f(x_2, y_1) & f(x_2, y_2) & \dots & f(x_2, y_n) \\ \vdots & \vdots & \ddots & \vdots \\ f(x_n, y_1) & f(x_n, y_2) & \dots & f(x_n, y_n) \end{pmatrix}.$$

Rows and Columns of the Matrix

If we look at each column $j \in [n]$, then y_j is fixed. Each column can be viewed as a univariate function with variable x evaluated on X.

$$M = \begin{pmatrix} f(x_1, y_1) & f(x_1, y_2) & \dots & f(x_1, y_n) \\ f(x_2, y_1) & f(x_2, y_2) & \dots & f(x_2, y_n) \\ \vdots & \vdots & \ddots & \vdots \\ f(x_n, y_1) & f(x_n, y_2) & \dots & f(x_n, y_n) \end{pmatrix}.$$

If we look at each row $i \in [n]$, then x_i is fixed. Each row can be viewed as a univariate function with variable y evaluated on Y.

Matrix Representation of a Function

Suppose an adversary gives us a matrix over $\mathcal{F}$

$$M = \begin{pmatrix} v_{1,1} & v_{1,2} & \dots & v_{1,n} \\ v_{2,1} & v_{2,2} & \dots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n,1} & v_{n,2} & \dots & v_{n,n} \end{pmatrix}.$$

This can be viewed exactly the same as

$$M = \begin{pmatrix} f(x_1, y_1) & f(x_1, y_2) & \dots & f(x_1, y_n) \\ f(x_2, y_1) & f(x_2, y_2) & \dots & f(x_2, y_n) \\ \vdots & \vdots & \ddots & \vdots \\ f(x_n, y_1) & f(x_n, y_2) & \dots & f(x_n, y_n) \end{pmatrix},$$

because M uniquely defines $f(x, y)$.

Well-Known Theorem

Question: *How do we know if matrix M represents a bivariate polynomial?*

Well-Known Theorem

Question: *How do we know if matrix M represents a bivariate polynomial?*

Theorem (Well-known)

Let $f(x, y)$ be a function on $X \times Y$ such that for $j \in [n]$, $f(x, y_j)$ agrees with some degree d polynomial in x on X, and for $i \in [n]$, $f(x_i, y)$ agrees on Y with some degree e polynomial in y. Then, there exists a polynomial $P(x, y)$ of degree (d, e) such that $f(x, y)$ agrees with $P(x, y)$ everywhere on $X \times Y$.

Proof: Recall that a degree d univariate polynomial is uniquely determined by its values at $d+1$ points. For $1 \le j \le e+1$, let $p_j(x)$ be the degree d polynomial that agrees with $f(x, y_j)$. For $1 \le j \le e+1$, let $\delta_j(y)$ be the degree e polynomial in y such that

$$\delta_j(y_k) = \begin{cases} 1, & \text{if } j = k, \text{ and} \\ 0, & \text{if } 1 \le k \le e+1, \text{ but } j \ne k. \end{cases}$$

We let $P(x, y) = \sum_{j=1}^{e+1} \delta_j(y) p_j(x)$. It is clear that P has degree (d, e). Moreover, $P(x, y_j) = f(x, y_j)$ for all $x \in X$ and $1 \le j \le d+1$. To see that in fact $P(x, y) = f(x, y)$ for all $(x, y) \in X \times Y$, observe that P and f agree at $e+1$ points in column y. Since f agrees with some degree e polynomial in column y, that polynomial must be the restriction of P to column y. $\square$

Proof Explained

Every column p_j has degree d. We pick the first $e+1$ columns.

$$M = \begin{pmatrix} p_1(x_1) & p_2(x_1) & \dots & p_{e+1}(x_1) & \dots & f(x_1, y_n) \\ p_1(x_2) & p_2(x_2) & \dots & p_{e+1}(x_2) & \dots & f(x_2, y_n) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ p_1(x_n) & p_2(x_n) & \dots & p_{e+1}(x_n) & \dots & f(x_n, y_n) \end{pmatrix}.$$

By Lagrange Interpolation, each δ_j has degree e.

$$\delta_1(y) = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \end{pmatrix} = \frac{(y-y_2)}{(y_1-y_2)} \frac{(y-y_3)}{(y_1-y_3)} \dots \frac{(y-y_{e+1})}{(y_1-y_{e+1})}$$

$$\delta_j(y_k) = \prod_{j=1, j \neq k}^{e+1} \frac{y-y_j}{y_k-y_j}.$$

The bivariate polynomial is

$$P(x, y) = \sum_{j=1}^{e+1} \delta_j(y) p_j(x).$$

UNIVERSITY OF TORONTO

Applying the Well-Known Theorem

Suppose an adversary gives you a matrix

$$M = \begin{pmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,n} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n,1} & v_{n,2} & \cdots & v_{n,n} \end{pmatrix},$$

and you want to know if M represents some bivariate polynomial of degree (d, d). *What can you do?*

Applying the Well-Known Theorem

Suppose an adversary gives you a matrix

$$M = \begin{pmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,n} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n,1} & v_{n,2} & \cdots & v_{n,n} \end{pmatrix},$$

and you want to know if M represents some bivariate polynomial of degree (d, d). *What can you do?*

- We can test if a row/column agrees with some polynomial of degree d by interpolating any $d + 1$ points and check if all other points lie on the polynomial.
- If we know that every row agrees with some polynomial of degree d, and every column agrees with some polynomial of degree d. We can apply the well-known theorem we just saw.

An Imperfect World

What if some rows/columns do not fully agree with some polynomial of degree d?

Question: *How do we know if matrix M is "very close" to a bivariate polynomial?*

An Imperfect World

Maybe we can fix some places such that every row agrees with some polynomial of degree at most d.

$$M = \begin{pmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,n} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n,1} & v_{n,2} & \cdots & v_{n,n} \end{pmatrix}.$$

Maybe we can fix some places such that every column agrees with some polynomial of degree at most d.

$$M = \begin{pmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,n} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n,1} & v_{n,2} & \cdots & v_{n,n} \end{pmatrix}.$$

Hard to fix both the rows and the columns simultaneously!

Rows and Columns

Consider a bivariate polynomial $R(x, y)$ of degree (d, n). Every row f_i is a univariate polynomial in x with degree at most d.

$$R(x,y) = \begin{pmatrix} f_1(x_1) & f_1(x_2) & \dots & f_1(x_n) \\ f_2(x_1) & f_2(x_2) & \dots & f_2(x_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_n(x_1) & f_n(x_2) & \dots & f_n(x_n) \end{pmatrix}.$$

Consider a bivariate polynomial $C(x, y)$ of degree (n, d). Every column g_j is a univariate polynomial in y with degree at most d.

$$C(x,y) = \begin{pmatrix} g_1(y_1) & g_2(y_1) & \dots & g_n(y_1) \\ g_1(y_2) & g_2(y_2) & \dots & g_n(y_2) \\ \vdots & \vdots & \ddots & \vdots \\ g_1(y_n) & g_2(y_n) & \dots & g_n(y_n) \end{pmatrix}.$$

Polishchuk-Spielman Bivariate Testing Theorem

Theorem 9 (Bivariate Testing). *Let $\mathcal{F}$ be a field, let $X = \{x_1, \ldots, x_n\} \subseteq \mathcal{F}$, and let $Y = \{y_1, \ldots, y_n\} \subseteq \mathcal{F}$. Let $R(x, y)$ be a polynomial over $\mathcal{F}$ of degree (d, n) and let $C(x, y)$ be a polynomial over $\mathcal{F}$ of degree (n, d). If*

$$\operatorname*{Prob}_{(x,y)\in X\times Y}[R(x, y) \neq C(x, y)] < \delta^2,$$

and $n > 2\delta n + 2d$, then there exists a polynomial $Q(x, y)$ of degree (d, d) such that

$$\operatorname*{Prob}_{(x,y)\in X\times Y}[R(x, y) \neq Q(x, y) \text{ or } C(x, y) \neq Q(x, y)] < 2\delta^2.$$

What does it mean?

We can fix some places in M to obtain $R(x, y)$, and separately fix some other places in M to obtain $C(x, y)$. If the total number of places we fixed among both $R(x, y)$ and $C(x, y)$ is at most $\delta^2 n^2$, then M is actually very close to a bivariate polynomial $Q(x, y)$ of degree (d, d).

$$M = \begin{pmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,n} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n,1} & v_{n,2} & \cdots & v_{n,n} \end{pmatrix}.$$

(PS: In practice, if M is really close to $Q(x, y)$. Observe that we can view M as a bivariate Reed-Muller code, then we can recover $Q(x, y)$.)

Proof 1

Lemma (3)

Let $S \subset X \times Y$ be a set of size at most $(\delta n)^2$, where δn is an integer. Then there exists a non-zero polynomial $E(x, y)$ of degree $(\delta n, \delta n)$ such that $E(x, y) = 0$ for all $(x, y) \in S$.

The proof is obvious: $E(x, y)$ has $(\delta n + 1)^2$ unknowns and there are $(\delta n)^2$ restrictions.

Let S be the subset of $X \times Y$ on which R and C disagree. Then we have

$$R(x, y)E(x, y) = C(x, y)E(x, y) \text{ for all } (x, y) \in X \times Y.$$

Observe $C(x, y)E(x, y)$ is a polynomial of degree $(n + \delta n, d + \delta n)$ and $R(x, y)E(x, y)$ is a polynomial of degree $(d + \delta n, n + \delta n)$.

Proof 2

By the well-known theorem, there exists a polynomial $P(x, y)$ of degree $(d + \delta n, d + \delta n)$ such that

$$R(x, y)E(x, y) = C(x, y)E(x, y) = P(x, y)$$

for all $(x, y) \in X \times Y$.

Proof 2

By the well-known theorem, there exists a polynomial $P(x, y)$ of degree $(d + \delta n, d + \delta n)$ such that

$$R(x, y)E(x, y) = C(x, y)E(x, y) = P(x, y)$$

for all $(x, y) \in X \times Y$.

It is natural to continue the proof by dividing P by E. However, the most we can say is that

$$\frac{P(x, y)}{E(x, y)} = R(x, y) = C(x, y),$$

for all $(x, y) \in X \times Y$ such that $E(x, y) \neq 0$.

Proof 2

By the well-known theorem, there exists a polynomial $P(x, y)$ of degree $(d + \delta n, d + \delta n)$ such that

$$R(x, y)E(x, y) = C(x, y)E(x, y) = P(x, y)$$

for all $(x, y) \in X \times Y$.

It is natural to continue the proof by dividing P by E. However, the most we can say is that

$$\frac{P(x, y)}{E(x, y)} = R(x, y) = C(x, y),$$

for all $(x, y) \in X \times Y$ such that $E(x, y) \neq 0$. We can show that if n is sufficiently large, then E in fact divides P.

Proof 3

Lemma (4)

Let $P(x,y), E(x,y), R(x,y), C(x,y)$ be polynomials of degree $(\delta n + d, \delta n + d), (\delta n, \delta n), (d, n), (n, d)$ respectively such that $R(x,y)E(x,y) = C(x,y)E(x,y) = P(x,y)$ for all $(x,y) \in X \times Y$. If $|X| > \delta n + d$ and $|Y| > \delta n + d$, then for all $y_0 \in Y$ and for all $x_0 \in X$, $P(x, y_0) \equiv R(x, y_0)E(x, y_0)$ and $P(x_0, y) \equiv C(x_0, y)E(x_0, y)$.

The proof is obvious: For fixed y_0, $P(x, y_0)$ and $R(x, y_0)E(x, y_0)$ both have degree $\delta n + d$, and they agree on at least $d + \delta n + 1$ points.

UNIVERSITY OF TORONTO

Proof 4

Lemma (8)

Let $E(x, y)$ be a polynomial of degree (b, a) and let $P(x, y)$ be a polynomial of degree $(b + d, a + d)$. If there exists distinct $x_1, \ldots, x_n$ such that $E(x_i, y)$ divides $P(x_i, y)$ for $i \in [n]$, distinct $y_1, \ldots, y_n$ such that $E(x, y_i)$ divides $P(x, y_i)$ for $i \in [n]$ and if

$$n > \min\{2b + 2d, 2a + 2d\},$$

then $E(x, y)$ divides $P(x, y)$.

The proof is not obvious. We will skip it for time sake.

Recall the main Theorem

Theorem 9 (Bivariate Testing). *Let $\mathcal{F}$ be a field, let $X = \{x_1, \ldots, x_n\} \subseteq \mathcal{F}$, and let $Y = \{y_1, \ldots, y_n\} \subseteq \mathcal{F}$. Let $R(x, y)$ be a polynomial over $\mathcal{F}$ of degree (d, n) and let $C(x, y)$ be a polynomial over $\mathcal{F}$ of degree (n, d). If*

$$\operatorname*{Prob}_{(x,y)\in X\times Y}[R(x, y) \neq C(x, y)] < \delta^2,$$

and $n > 2\delta n + 2d$, then there exists a polynomial $Q(x, y)$ of degree (d, d) such that

$$\operatorname*{Prob}_{(x,y)\in X\times Y}[R(x, y) \neq Q(x, y) \text{ or } C(x, y) \neq Q(x, y)] < 2\delta^2.$$

UNIVERSITY OF TORONTO

Proof 5

Summary of our proof so far: Let S be the set of points where $R(x, y) \neq C(x, y)$. By Lemma 3, there exists an error correcting polynomial $E(x, y)$ of degree $(\delta n, \delta n)$ such that E vanishes on S. By Lemma 4 and Lemma 8, there exists a polynomial $Q(x, y)$ of degree (d, d) such that

$$R(x, y)E(x, y) = C(x, y)E(x, y) = Q(x, y)E(x, y),$$

for all $(x, y) \in X \times Y$.

Proof 5

Summary of our proof so far: Let S be the set of points where $R(x,y) \neq C(x,y)$. By Lemma 3, there exists an error correcting polynomial $E(x,y)$ of degree $(\delta n, \delta n)$ such that E vanishes on S. By Lemma 4 and Lemma 8, there exists a polynomial $Q(x,y)$ of degree (d,d) such that

$$R(x,y)E(x,y) = C(x,y)E(x,y) = Q(x,y)E(x,y),$$

for all $(x,y) \in X \times Y$.

Now we need to show the $< 2\delta^2$ part. Note that in any row where $E(x,y) \neq 0$, Q agrees with R on that entire row. However, E has degree $(\delta n, \delta n)$ so it can be (in the worst case) identically zero on at most δn rows. So E must be non-zero on at least $(1-\delta)n$ rows. Thus, Q must agree with R on at least $(1-\delta)n$ rows. Similarly, Q must agree with C on at least $(1-\delta)n$ rows.

Proof 6

Therefore, we have R and C agree on the intersection of $(1-\delta)n$ columns and rows. This is already a lot of points, but we will show that they agree on many more points.

Recall S is the set of points where $R(x, y) \neq C(x, y)$. Let T be the set of points where $R(x, y) = C(x, y)$, but $Q(x, y) \neq R(x, y)$ (and also $Q(x, y) \neq C(x, y)$). If we show $|T| \leq |S|$, we are done with the $< 2\delta^2$ part.

We say a row/column is *bad* if Q disagrees on R/C on that row/column. Let b_r be the number of bad rows and let b_c be the number of bad columns. Call *good* any row/column that is not bad. We say that a row and column disagree if R and C take different values at their intersection.

Proof 7

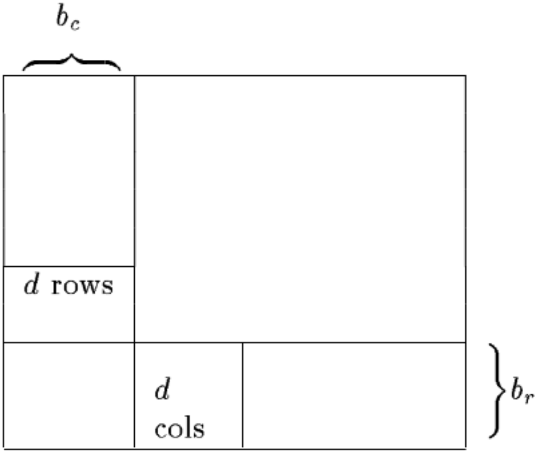
Observe there can be at most $d + b_r$ points of T in any bad column: if a column has more than $d + b_r$ points (e.g. $d + b_r + 1$ points) of T, note that $R(x, y) = C(x, y)$ in T, then it must have at least $d + 1$ points in good rows where Q agrees with R and therefore Q, implying that column is in fact good.

Recall $n > 2\delta n + 2d$. Thus, every bad column must have at least $n/2$ points of S in the intersection of that column with the good rows. Similarly, every bad row must have at least $n/2$ points of S in the intersection of that row with the good columns.

Hence, the points of T in every column is less than the points of S; the points if T in every row is less than the points of S. Therefore, $|T| \leq |S|$.

Proof 8

Here is a picture illustration. The basic idea is that the points of T must lie in the lower left-hand corner.



Testing Reed-Solomon Codeword

Let n be a natural number and let Σ be an alphabet. Let $x \in \Sigma^n$ be a string, and we use x_i to denote the ith symbol of x. We say x is δ-*close* to a string $y \in \Sigma^n$ if $|\{i \mid x_i \neq y_i\}| \leq \delta n$. I.e. x and y agree on all but at most a δ-fraction of the symbols.

Suppose you are given an array of values. How do you test that it is a Reed-Solomon codeword?

UNIVERSITY OF TORONTO

Testing Reed-Solomon Codeword

Let n be a natural number and let Σ be an alphabet. Let $x \in \Sigma^n$ be a string, and we use x_i to denote the ith symbol of x. We say x is δ-*close* to a string $y \in \Sigma^n$ if $|\{i \mid x_i \neq y_i\}| \leq \delta n$. I.e. x and y agree on all but at most a δ-fraction of the symbols.

Suppose you are given an array of values. How do you test that it is a Reed-Solomon codeword?

What if you are only allowed to query very few values from the array?

Testing Reed-Solomon Codeword

Let n be a natural number and let Σ be an alphabet. Let $x \in \Sigma^n$ be a string, and we use x_i to denote the ith symbol of x. We say x is δ-*close* to a string $y \in \Sigma^n$ if $|\{i \mid x_i \neq y_i\}| \leq \delta n$. I.e. x and y agree on all but at most a δ-fraction of the symbols.

Suppose you are given an array of values. How do you test that it is a Reed-Solomon codeword?

What if you are only allowed to query very few values from the array? Not possible!

Testing Reed-Solomon Codeword

Let n be a natural number and let Σ be an alphabet. Let $x \in \Sigma^n$ be a string, and we use x_i to denote the ith symbol of x. We say x is δ-*close* to a string $y \in \Sigma^n$ if $|\{i \mid x_i \neq y_i\}| \leq \delta n$. I.e. x and y agree on all but at most a δ-fraction of the symbols.

Suppose you are given an array of values. How do you test that it is a Reed-Solomon codeword?

What if you are only allowed to query very few values from the array? Not possible! What if you can relax the requirement? You can build a proof system that shows the array of values is δ-close to some Reed-Solomon codeword.

PCPP

Definition (PCP of Proximity)

A *probabilistically checkable proof of proximity* (PCPP) system with soundness error $s \in (0, 1)$ and proximity parameter $\delta \in (0, 1)$ is a probabilistic proof system (P, V) in which the prover P on input (x, w) generates a proof π, and the verifier V can make at most q queries to the combined oracle (x, π), and the following holds.

- Completeness: For every $(x, w) \in \mathcal{R}$ (which means $x \in L_{\mathcal{R}}$), V accepts with probability 1.
- Soundness: For every x that is δ-far from $L_{\mathcal{R}}$, V accepts with probability at most s, regardless of the proof oracle π.

In this case, we write $L_{\mathcal{R}} \in \mathrm{PCPP}[r, q, \delta, s, \ell]$ where r is the verifier's randomness complexity, q is the query complexity, and ℓ is the length of the proof. We say a PCPP is an exact PCPP if the proximity parameter $\delta = 0$.

Application of Polishchuk-Spielman

Theorem (Theorem 3.2 in Ben-Sasson Sudan 05)

Let $\mathbb{F}_q$ be a finite field of order $q = 2^w$. Let S be a subset of $\mathbb{F}_q$ and S is $\mathbb{F}_2$-linear (i.e. for all $a, b \in S$, we have $a + b \in S$). Then, for any soundness error $s \in (0, 1)$ and any proximity parameter $\delta \in (0, 1)$, there exists an explicit construction of a PCPP to test if an array of values $r_1, \ldots, r_{|S|} \in \mathbb{F}_q$ is δ-close to some univariate polynomial of degree d evaluated at S, and the PCPP has randomness complexity $\log(q \cdot \text{polylog}(q))$, query complexity $\text{polylog}(q)$, and proof length $q \cdot \text{polylog}(q)$.

Application of Polishchuk-Spielman

Theorem (Theorem 3.2 in Ben-Sasson Sudan 05)

Let $\mathbb{F}_q$ be a finite field of order $q = 2^w$. Let S be a subset of $\mathbb{F}_q$ and S is $\mathbb{F}_2$-linear (i.e. for all $a, b \in S$, we have $a + b \in S$). Then, for any soundness error $s \in (0, 1)$ and any proximity parameter $\delta \in (0, 1)$, there exists an explicit construction of a PCPP to test if an array of values $r_1, \ldots, r_{|S|} \in \mathbb{F}_q$ is δ-close to some univariate polynomial of degree d evaluated at S, and the PCPP has randomness complexity $\log(q \cdot \text{polylog}(q))$, query complexity $\text{polylog}(q)$, and proof length $q \cdot \text{polylog}(q)$.

The core idea in the construction is to lay out the array of values as a bivariate polynomial and apply Polishchuk-Spielman! Maybe a good topic for my next TSS.

Q & A

Questions?

Thank you

Thank you!