Quantum-sound Property Tests for Linear and Affine Linear Functions

Jerry Zhang
Mentor: David Cui

October 12-13, 2024
MIT PRIMES Conference

Motivation

- Suppose Alice has an arbitrary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

f

Motivation

- Suppose Alice has an arbitrary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

$$\text{Ex. } \mathrm{odd}_5(01100) = 0$$

f

Motivation

- Suppose Alice has an arbitrary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- Alice claims that her function is linear (i.e. $f(x) + f(y) = f(x + y)$ for all $x, y \in \mathbb{F}_2^n$)

f

Motivation

- Suppose Alice has an arbitrary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- Alice claims that her function is linear (i.e. $f(x) + f(y) = f(x + y)$ for all $x, y \in \mathbb{F}_2^n$)

$$\begin{aligned} \text{Ex. } \mathrm{odd}_5(01100) + \mathrm{odd}_5(10101) &= 0 + 1 = 1 \\ \mathrm{odd}_5(01100 + 10101) = \mathrm{odd}_5(11001) &= 1 \end{aligned}$$

Our verifier wants to verify if she actually does.

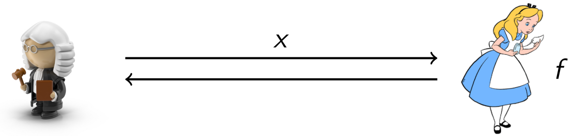
f

Motivation

- Suppose Alice has an arbitrary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- Alice claims that her function is linear (i.e. $f(x) + f(y) = f(x+y)$ for all $x, y \in \mathbb{F}_2^n$)

$$\begin{aligned} \text{Ex. } \mathrm{odd}_5(01100) + \mathrm{odd}_5(10101) &= 0 + 1 = 1 \\ \mathrm{odd}_5(01100 + 10101) = \mathrm{odd}_5(11001) &= 1 \end{aligned}$$

Our verifier wants to verify if she actually does.

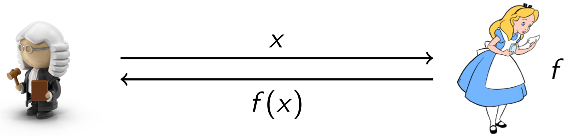


Motivation

- Suppose Alice has an arbitrary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- Alice claims that her function is linear (i.e. $f(x) + f(y) = f(x + y)$ for all $x, y \in \mathbb{F}_2^n$)

$$\begin{aligned} \text{Ex. } \operatorname{odd}_5(01100) + \operatorname{odd}_5(10101) &= 0 + 1 = 1 \\ \operatorname{odd}_5(01100 + 10101) = \operatorname{odd}_5(11001) &= 1 \end{aligned}$$

Our verifier wants to verify if she actually does.

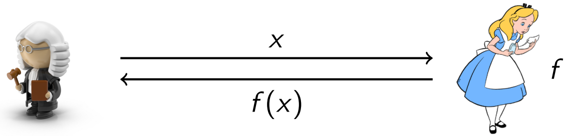


Motivation

- Suppose Alice has an arbitrary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- Alice claims that her function is linear (i.e. $f(x) + f(y) = f(x+y)$ for all $x, y \in \mathbb{F}_2^n$)

  $$\begin{aligned} \text{Ex. } \mathrm{odd}_5(01100) + \mathrm{odd}_5(10101) &= 0 + 1 = 1 \\ \mathrm{odd}_5(01100 + 10101) = \mathrm{odd}_5(11001) &= 1 \end{aligned}$$

  Our verifier wants to verify if she actually does.
- Naive approach: test all possible pairs (x, y) (this is inefficient)

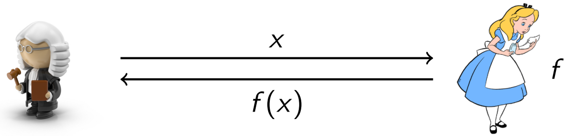


Motivation

- Suppose Alice has an arbitrary function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.
- Alice claims that her function is linear (i.e. $f(x) + f(y) = f(x + y)$ for all $x, y \in \mathbb{F}_2^n$)

$$\text{Ex. } \operatorname{odd}_5(01100) + \operatorname{odd}_5(10101) = 0 + 1 = 1$$
$$\operatorname{odd}_5(01100 + 10101) = \operatorname{odd}_5(11001) = 1$$

  Our verifier wants to verify if she actually does.
- Naive approach: test all possible pairs (x, y) (this is inefficient)
- We can use randomness to verify if the prover is actually saying what they have.



The BLR Test

Definition (BLR Test)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a function.

1. Choose $x, y \sim \mathbb{F}_2^n$.
2. Query f at x, y, and $x + y$.
3. Accept if $f(x) + f(y) = f(x + y)$.

The BLR Test

Definition (BLR Test)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a function.

1. Choose $x, y \sim \mathbb{F}_2^n$.
2. Query f at x, y, and $x + y$.
3. Accept if $f(x) + f(y) = f(x + y)$.

- Blum, Luby, and Rubinfield showed that, given the above test accepts with high probability, f is close to being linear. [1, 2]

The BLR Test

Definition (BLR Test)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a function.

1. Choose $x, y \sim \mathbb{F}_2^n$.
2. Query f at x, y, and $x + y$.
3. Accept if $f(x) + f(y) = f(x + y)$.

- Blum, Luby, and Rubinfield showed that, given the above test accepts with high probability, f is close to being linear. [1, 2]
- More formally: If the test accepts with probability $1 - \epsilon$, f differs from a linear function at a proportion of at most ϵ entries.

The BLR Test

Definition (BLR Test)

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a function.

1. Choose $x, y \sim \mathbb{F}_2^n$.
2. Query f at x, y, and $x + y$.
3. Accept if $f(x) + f(y) = f(x + y)$.

- Blum, Luby, and Rubinfield showed that, given the above test accepts with high probability, f is close to being linear. [1, 2]
- More formally: If the test accepts with probability $1 - \epsilon$, f differs from a linear function at a proportion of at most ϵ entries.
- It is much faster, but it only tests approximate linearity.

$$\text{Ex. } \mathrm{odd}_5'(x) = \mathrm{odd}_5(x) \ \ \forall x \neq 00000, \ \mathrm{odd}_5'(00000) = 1$$

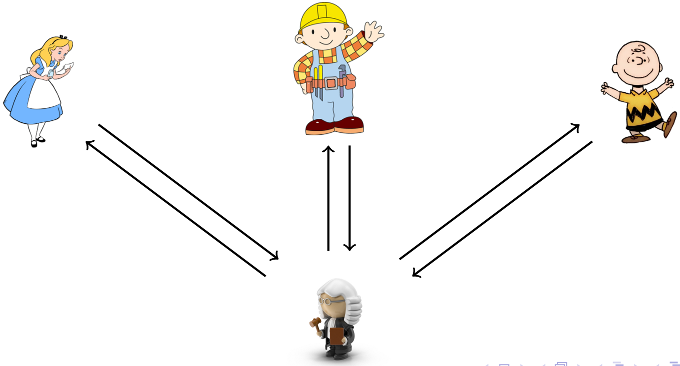
The BLR Test (cont.)

This naturally leads us to a more "distributed" version of the BLR test.

The BLR Test (cont.)

This naturally leads us to a more "distributed" version of the BLR test.

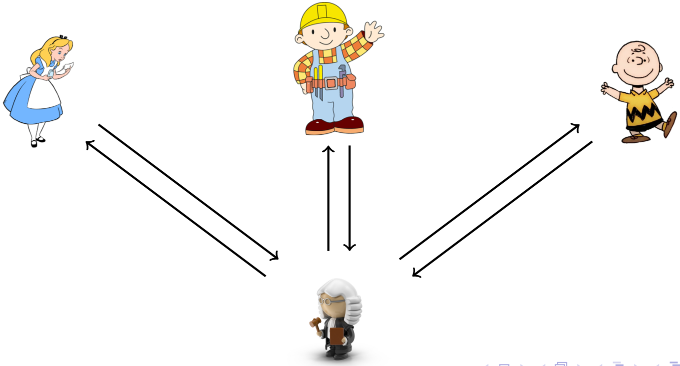
- Suppose that we have three provers, say Alice, Bob and Charlie, each with functions $f(x), g(x), h(x)$ respectively that a verifier can query.



The BLR Test (cont.)

This naturally leads us to a more "distributed" version of the BLR test.

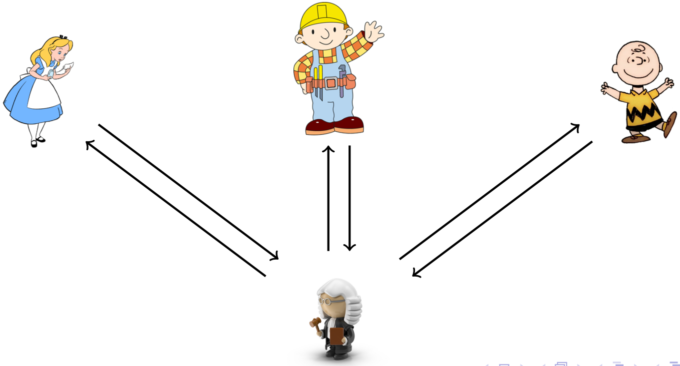
- Suppose that we have three provers, say Alice, Bob and Charlie, each with functions $f(x), g(x), h(x)$ respectively that a verifier can query.
- Alice, Bob, and Charlie cannot communicate.



The BLR Test (cont.)

This naturally leads us to a more "distributed" version of the BLR test.

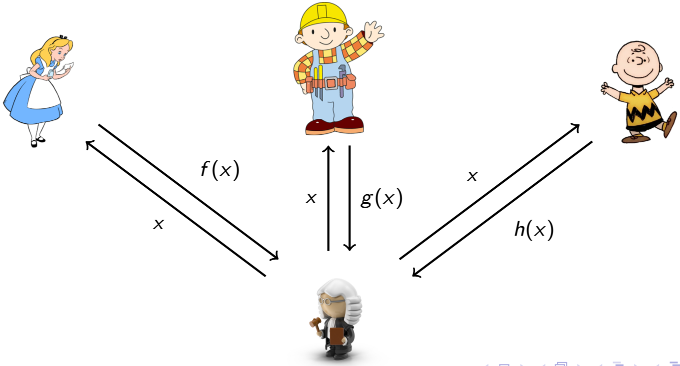
- Suppose that we have three provers, say Alice, Bob and Charlie, each with functions $f(x), g(x), h(x)$ respectively that a verifier can query.
- Alice, Bob, and Charlie cannot communicate.
- The verifier wants to determine if f, g and h are all equal to some linear function.



The BLR Test (cont.)

This naturally leads us to a more "distributed" version of the BLR test.

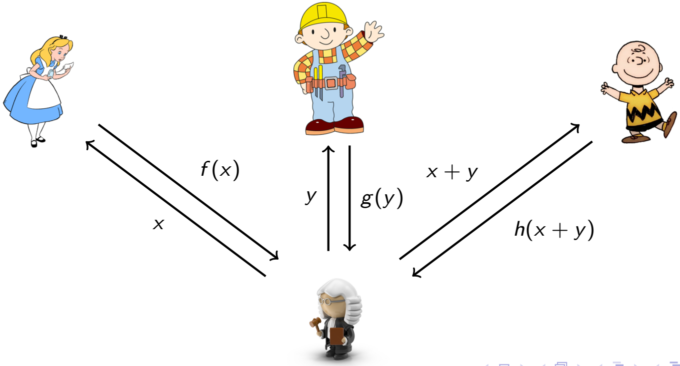
- Suppose that we have three provers, say Alice, Bob and Charlie, each with functions $f(x), g(x), h(x)$ respectively that a verifier can query.
- Alice, Bob, and Charlie cannot communicate.
- The verifier wants to determine if f, g and h are all equal to some linear function.



The BLR Test (cont.)

This naturally leads us to a more "distributed" version of the BLR test.

- Suppose that we have three provers, say Alice, Bob and Charlie, each with functions $f(x), g(x), h(x)$ respectively that a verifier can query.
- Alice, Bob, and Charlie cannot communicate.
- The verifier wants to determine if f, g and h are all equal to some linear function.



The Distributed BLR

More formally:

Definition

Let provers A, B, C have functions $f, g, h : \mathbb{F}_2^n \to \mathbb{F}_2$. The verifier performs the following tests each with probability $1/2$:

1. (*Consistency*) Select $x \sim \mathbb{F}_2^n$. Query $f(x), g(x)$, and $h(x)$. Accept if $f(x) = g(x) = h(x)$.
2. (*Linearity*) Select $x, y \sim \mathbb{F}_2^n$. Query $f(x), g(y)$, and $h(x+y)$. Accept if $f(x) + g(x) = h(x+y)$.

The Distributed BLR

More formally:

Definition

Let provers A, B, C have functions $f, g, h : \mathbb{F}_2^n \to \mathbb{F}_2$. The verifier performs the following tests each with probability $1/2$:

1. (*Consistency*) Select $x \sim \mathbb{F}_2^n$. Query $f(x), g(x)$, and $h(x)$. Accept if $f(x) = g(x) = h(x)$.
2. (*Linearity*) Select $x, y \sim \mathbb{F}_2^n$. Query $f(x), g(y)$, and $h(x+y)$. Accept if $f(x) + g(x) = h(x+y)$.

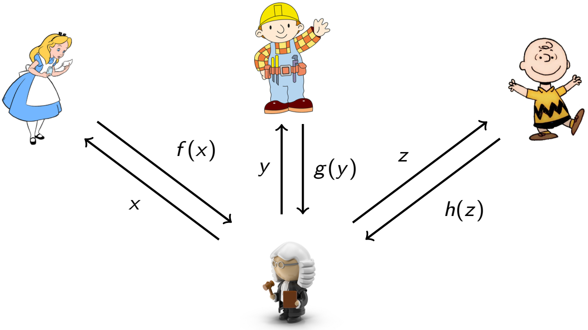
The provers can have a number of different strategies that they may use.

Strategies

- A **determinstic strategy** is given by (not necessarily linear) functions $f, g, h : \mathbb{F}_2^n \to \mathbb{F}_2$ which the provers use to respond.

Strategies

- A **determinstic strategy** is given by (not necessarily linear) functions $f, g, h : \mathbb{F}_2^n \to \mathbb{F}_2$ which the provers use to respond.

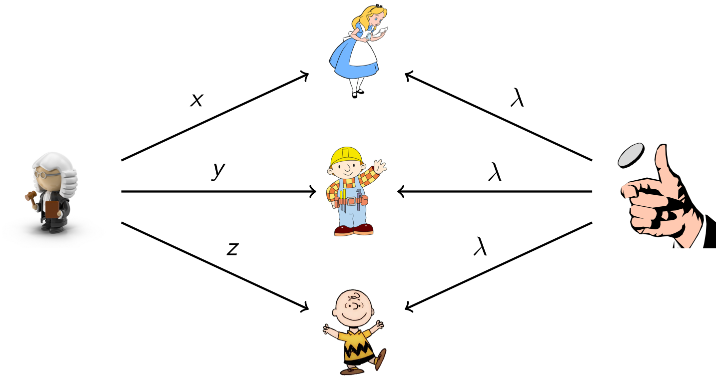


Strategies (cont.)

- A **strategy with shared randomness** is a probabilistic mixture of deterministic strategies given by $\{(p(\lambda), f_\lambda, g_\lambda, h_\lambda)\}_\lambda$ for $f_\lambda, g_\lambda, h_\lambda : \mathbb{F}_2^n \to \mathbb{F}_2$ and $p(\lambda) \in [0, 1]$.

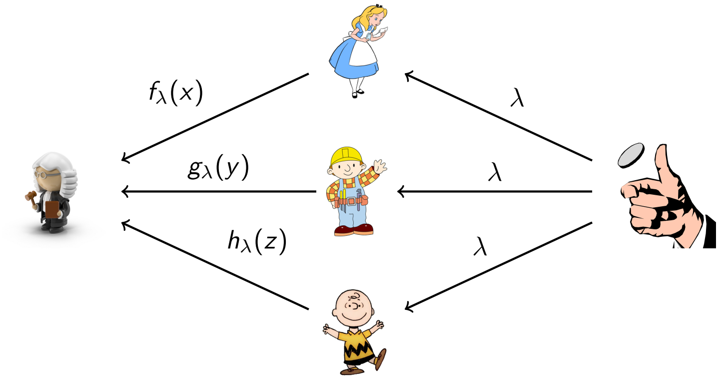
Strategies (cont.)

- A **strategy with shared randomness** is a probabilistic mixture of deterministic strategies given by $\{(p(\lambda), f_\lambda, g_\lambda, h_\lambda)\}_\lambda$ for $f_\lambda, g_\lambda, h_\lambda : \mathbb{F}_2^n \to \mathbb{F}_2$ and $p(\lambda) \in [0, 1]$.



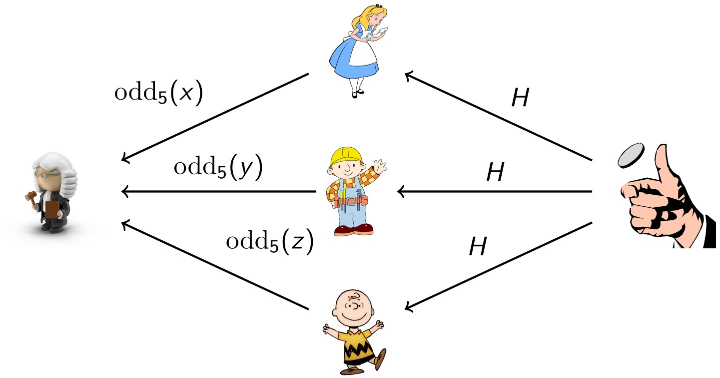
Strategies (cont.)

- A **strategy with shared randomness** is a probabilistic mixture of deterministic strategies given by $\{(p(\lambda), f_\lambda, g_\lambda, h_\lambda)\}_\lambda$ for $f_\lambda, g_\lambda, h_\lambda : \mathbb{F}_2^n \to \mathbb{F}_2$ and $p(\lambda) \in [0, 1]$.



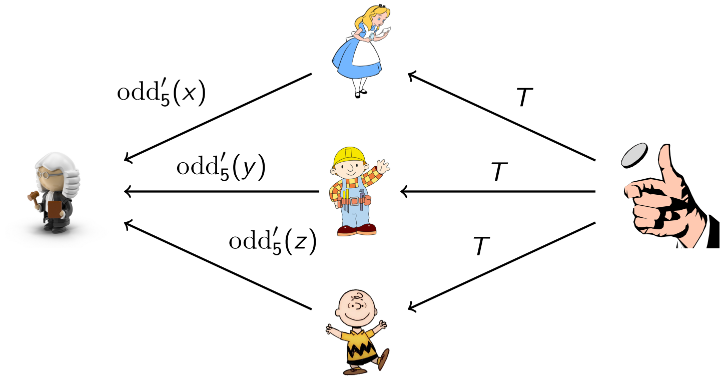
Strategies (cont.)

- A **strategy with shared randomness** is a probabilistic mixture of deterministic strategies given by $\{(p(\lambda), f_\lambda, g_\lambda, h_\lambda)\}_\lambda$ for $f_\lambda, g_\lambda, h_\lambda : \mathbb{F}_2^n \to \mathbb{F}_2$ and $p(\lambda) \in [0, 1]$.



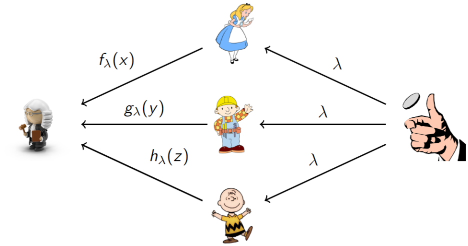
Strategies (cont.)

- A **strategy with shared randomness** is a probabilistic mixture of deterministic strategies given by $\{(p(\lambda), f_\lambda, g_\lambda, h_\lambda)\}_\lambda$ for $f_\lambda, g_\lambda, h_\lambda : \mathbb{F}_2^n \to \mathbb{F}_2$ and $p(\lambda) \in [0, 1]$.



Strategies (cont.)

- A **strategy with shared randomness** is a probabilistic mixture of deterministic strategies given by $\{(p(\lambda), f_\lambda, g_\lambda, h_\lambda)\}_\lambda$ for $f_\lambda, g_\lambda, h_\lambda : \mathbb{F}_2^n \to \mathbb{F}_2$ and $p(\lambda) \in [0, 1]$ for each λ.



- We may model this as a joint probability distribution over the outputs:

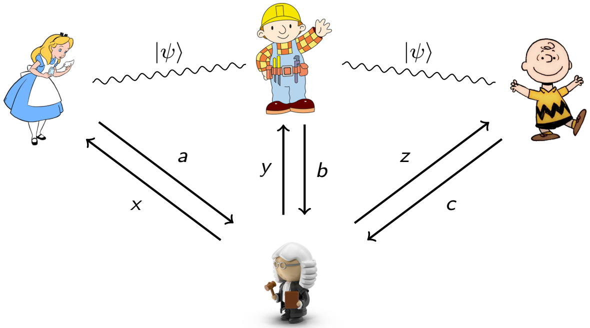
$$p(a, b, c|x, y, z) = \sum_\lambda p(\lambda)\delta_{f_\lambda(x)=a}\delta_{g_\lambda(y)=b}\delta_{h_\lambda(z)=c}$$

where $\delta_{j=k} = 1$ if $j = k$ and 0 otherwise.

Strategies (cont.)

- An **entangled strategy** $(A, B, C, |\psi\rangle)$ is a strategy where the players each have measurements $\{A_x^a\}$, $\{B_y^b\}$ and $\{C_z^c\}$ and share entanglement, or a state $|\psi\rangle$. They make measurements on the state depending on x, y and z, deciding the distribution:

$$p(a, b, c|x, y, z) = \langle\psi|A_x^a \otimes B_y^b \otimes C_z^c|\psi\rangle$$



Strategies (cont.)

Definition

Let provers A, B, C have some strategy. The verifier performs the following tests each with probability $1/2$:

1. (*Consistency*) Select $x \sim \mathbb{F}_2^n$. Send x to A, B, C, and receive outputs a, b, c. Accept if $a = b = c$.
2. (*Linearity*) Select $x, y \sim \mathbb{F}_2^n$. Send x to A, y to B and $x + y$ to C. Receive outputs a, b, c. Accept if $a + b = c$.

The **winning probability** of a strategy is

$$\frac{1}{2} \mathop{\mathbb{E}}_{x,y \sim \mathbb{F}_2^n} \left[\sum_{a,b \in \mathbb{F}_2} p(a, b, a+b | x, y, x+y) \right] + \frac{1}{2} \mathop{\mathbb{E}}_{x \sim \mathbb{F}_2^n} \left[\sum_{a \in \mathbb{F}_2} p(a, a, a | x, x, x) \right]$$

Strategies (cont.)

The **total variational distance** between two strategies p and q is

$$\|p - q\|_{\mathrm{TV}} = \mathop{\mathbb{E}}_{x,y,z \sim \mathbb{F}_2^n} \left[\sum_{a,b,c} |p(a,b,c|x,y,z) - q(a,b,c|x,y,z)| \right]$$

Strategies (cont.)

The **total variational distance** between two strategies p and q is

$$\|p - q\|_{\mathrm{TV}} = \mathop{\mathbb{E}}_{x,y,z \sim \mathbb{F}_2^n} \left[\sum_{a,b,c} |p(a,b,c|x,y,z) - q(a,b,c|x,y,z)| \right]$$

- Small variational distance $\iff$ p and q are close

Strategies (cont.)

The **total variational distance** between two strategies p and q is

$$\|p - q\|_{\mathrm{TV}} = \mathop{\mathbb{E}}_{x,y,z \sim \mathbb{F}_2^n} \left[\sum_{a,b,c} |p(a,b,c|x,y,z) - q(a,b,c|x,y,z)| \right]$$

- Small variational distance $\iff$ p and q are close
- A small variational distance allows us to essentially "replace" one strategy with another

Quantum-soundness of the BLR

Now recall the 3 prover BLR test:

Definition

Let provers A, B, C have some strategy. The verifier performs the following tests each with probability $1/2$:

1. (*Consistency*) Select $x \sim \mathbb{F}_2^n$. Send x to A, B, C, and receive outputs a, b, c. Accept if $a = b = c$.
2. (*Linearity*) Select $x, y \sim \mathbb{F}_2^n$. Send x to A, y to B and $x + y$ to C. Receive outputs a, b, c. Accept if $a + b = c$.

Quantum-soundness of the BLR

Now recall the 3 prover BLR test:

Definition

Let provers A, B, C have some strategy. The verifier performs the following tests each with probability $1/2$:

1. (*Consistency*) Select $x \sim \mathbb{F}_2^n$. Send x to A, B, C, and receive outputs a, b, c. Accept if $a = b = c$.
2. (*Linearity*) Select $x, y \sim \mathbb{F}_2^n$. Send x to A, y to B and $x + y$ to C. Receive outputs a, b, c. Accept if $a + b = c$.

- What if the provers have entangled strategies?

Quantum-soundness of the BLR (cont.)

- Instead of having functions f, g, h, Alice, Bob and Charlie now have measurements $\{A_x^a\}$, $\{B_y^b\}$ and $\{C_z^c\}$ with some shared entangled state $|\psi\rangle$.

Quantum-soundness of the BLR (cont.)

- Instead of having functions f, g, h, Alice, Bob and Charlie now have measurements $\{A_x^a\}$, $\{B_y^b\}$ and $\{C_z^c\}$ with some shared entangled state $|\psi\rangle$.
- We now wish to test if their strategies are close to some classical linear strategy.

Quantum-soundness of the BLR (cont.)

- Instead of having functions f, g, h, Alice, Bob and Charlie now have measurements $\{A_x^a\}$, $\{B_y^b\}$ and $\{C_z^c\}$ with some shared entangled state $|\psi\rangle$.

- We now wish to test if their strategies are close to some classical linear strategy.
- Can we use still the BLR linearity test for this?

Quantum-soundness of the BLR (cont.)

- Instead of having functions f, g, h, Alice, Bob and Charlie now have measurements $\{A_x^a\}$, $\{B_y^b\}$ and $\{C_z^c\}$ with some shared entangled state $|\psi\rangle$.

- We now wish to test if their strategies are close to some classical linear strategy.
- Can we use still the BLR linearity test for this?
- A crucial reduction: given a strategy A, B, C, that wins with probability p, we can reduce down to a case where $A = B = C$, and have a winning probability of at least p.

Quantum-soundness of the BLR (cont.)

- Instead of having functions f, g, h, Alice, Bob and Charlie now have measurements $\{A_x^a\}$, $\{B_y^b\}$ and $\{C_z^c\}$ with some shared entangled state $|\psi\rangle$.
- We now wish to test if their strategies are close to some classical linear strategy.
- Can we use still the BLR linearity test for this?
- A crucial reduction: given a strategy A, B, C, that wins with probability p, we can reduce down to a case where $A = B = C$, and have a winning probability of at least p.

  We call such a strategy **symmetric**.

Quantum-soundness of the BLR (cont.)

We still can!

Theorem (Ito-Vidick, 2012 [3])

Suppose three entangled provers succeed in the linearity test with probability 1-ϵ using a symmetric strategy $(|\psi\rangle, \{A_x^a\})$, and let its corresponding probability distributions be $\{p(a, b, c|x, y, z)\}$. Then there exists a classical linear strategy with shared randomness ℓ such that

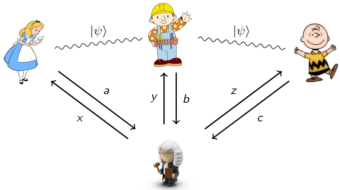
$$\|p - \ell\|_{\mathrm{TV}} \leq 6\sqrt{3\epsilon^{1/2}}$$

Quantum-soundness of the BLR (cont.)

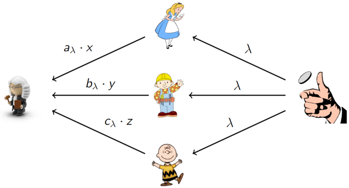
Theorem (Ito-Vidick, 2012[3])

Suppose three entangled provers succeed in the linearity test with probability 1-ϵ using a symmetric strategy $(|\psi\rangle, \{A^a_x\})$, and let its corresponding probability distributions be $\{p(a,b,c|x,y,z)\}$. Then there exists a classical linear strategy with shared randomness ℓ such that

$$\|p - \ell\|_{\mathrm{TV}} \leq 6\sqrt{3\epsilon^{1/2}}$$



$\longleftrightarrow$



Our Results

We generalize the results of Ito-Vidick to $\mathbb{F}_p$:

Theorem

Suppose three entangled provers succeed in the linearity test with probability 1-ϵ using a symmetric strategy $(|\psi\rangle, \{A_x^a\})$, and let its corresponding probability distributions be $\{p(a, b, c|x, y, z)\}$. Then there exists a classical linear strategy with shared randomness ℓ such that

$$\|p - \ell\|_{\mathrm{TV}} \leq 6\epsilon^{1/4}\sqrt{1 + 2\left(1 - \frac{1}{p}\right)}^{1/2}$$

The Affine Linearity Test

Let's recall the BLR once more:

Definition

Let provers A, B, C have some strategy. The verifier performs the following tests each with probability $1/2$:

1. (*Consistency*) Select $x \sim \mathbb{F}_2^n$. Send x to A, B, C, and receive outputs a, b, c. Accept if $a = b = c$.
2. (*Linearity*) Select $x, y \sim \mathbb{F}_2^n$. Send x to A, y to B and $x + y$ to C. Receive outputs a, b, c. Accept if $a + b = c$.

The Affine Linearity Test

Let's recall the BLR once more:

Definition

Let provers A, B, C have some strategy. The verifier performs the following tests each with probability $1/2$:

1. **(Consistency) Select $x \sim \mathbb{F}_2^n$. Send x to A, B, C, and receive outputs a, b, c. Accept if $a = b = c$.**
2. (*Linearity*) Select $x, y \sim \mathbb{F}_2^n$. Send x to A, y to B and $x + y$ to C. Receive outputs a, b, c. Accept if $a + b = c$.

- If we drop this portion, can we still say anything about the strategies the players use?

The Affine BLR

Classically, we can! We can still show the strategies are close to some deterministic *affine* linear strategy:

Lemma

Given a classical probabilistic strategy p which succeeds in the linearity part of the BLR test with probability $1-\epsilon$, there exists a deterministic affine linear strategy ℓ such that

$$\|p-\ell\|_{\mathrm{TV}} \leq 2\left(1-\left(1-\sqrt{\epsilon}\right)^{3}\right)$$

- Can we draw the same conclusion with quantum strategies?

Our Results (cont.)

We generalize this result to the affine linear test in $\mathbb{F}_p$:

Theorem

Suppose three entangled provers succeed in the affine linearity test (i.e. linearity test without consistency) with probability 1-ϵ using a symmetric strategy $(\sigma, \{A_x^a\})$. Then there exists a classical affine linear strategy with shared randomness ℓ such that

$$\|p - \ell\|_{\mathrm{TV}} \leq 3\sqrt{2}\epsilon^{1/4}\sqrt{1 + 2\sqrt{2}\left(1 - \frac{1}{p}\right)^{1/2}}$$

Acknowledgements

I would like to thank:

- my mentor David Cui for his support and encouragement
- and the MIT PRIMES organizers for their support

References

[1] M. Bellare et al. "Linearity testing in characteristic two". In: *IEEE Transactions on Information Theory* 42.6 (1996), pp. 1781–1795. DOI: 10.1109/18.556674.

[2] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. "Self-testing/correcting with applications to numerical problems". In: *Journal of Computer and System Sciences* 47.3 (1993), pp. 549–595. ISSN: 0022-0000. DOI: https://doi.org/10.1016/0022-0000(93)90044-W.

[3] Tsuyoshi Ito and Thomas Vidick. "A Multi-prover Interactive Proof for NEXP Sound against Entangled Provers". In: *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science* (2012), pp. 243–252. URL: https://api.semanticscholar.org/CorpusID:7553531.