Foundations of Computing

Lecture 24

Arkady Yerukhimovich

April 20, 2023

Outline

Lecture 23 Review

- The class co-$\mathcal{NP}$
- Interactive Proofs
- GNI $\in \mathcal{IP}$

Our Goal For Today

Prove that co-$\mathcal{NP} \subseteq \mathcal{IP}$

Graph Non-Isomorphism

Question

How can we prove that two graphs G_0 and G_1 are NOT isomorphic?

The Protocol:

1. V chooses $b \leftarrow \{0, 1\}$, and applies a random permutation π to the vertices of G_b and sends this graph G^* to P
2. P determines if G^* is isomorphic to G_0 and sends $b' = 0$ if so, or $b' = 1$ otherwise back to V
3. V accepts if $b' = b$

Why This Works:

Graph Non-Isomorphism

Question

How can we prove that two graphs G_0 and G_1 are NOT isomorphic?

The Protocol:

1. V chooses $b \leftarrow \{0,1\}$, and applies a random permutation π to the vertices of G_b and sends this graph G^* to P
2. P determines if G^* is isomorphic to G_0 and sends $b' = 0$ if so, or $b' = 1$ otherwise back to V
3. V accepts if $b' = b$

Why This Works:

1. (Completeness) Suppose that G_0 and G_1 are not isomorphic.
   - Then G^* can only be isomorphic to one of the two graphs
   - P can perfectly determine which one this is
   - So $\Pr[b' = b] = 1$

Graph Non-Isomorphism

Question

How can we prove that two graphs G_0 and G_1 are NOT isomorphic?

The Protocol:

1. V chooses $b \leftarrow \{0,1\}$, and applies a random permutation π to the vertices of G_b and sends this graph G^* to P
2. P determines if G^* is isomorphic to G_0 and sends $b' = 0$ if so, or $b' = 1$ otherwise back to V
3. V accepts if $b' = b$

Why This Works:

1. (Completeness) Suppose that G_0 and G_1 are not isomorphic.
   - Then G^* can only be isomorphic to one of the two graphs
   - P can perfectly determine which one this is
   - So $\Pr[b' = b] = 1$
2. (Soundness) Suppose that G_0 and G_1 are isomorphic
   - Then G^* is isomorphic to both G_0 and G_1
   - P has no way to tell which one V started from
   - Thus, $\Pr[b' = b] = 1/2$

A co-$\mathcal{NP}$ Complete Problem

3-UNSAT

3-UNSAT$= \{\langle\phi\rangle \mid \phi$ is an unsatisfiable 3-CNF formula$\}$

$(x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3)$

A co-$\mathcal{NP}$ Complete Problem

3-UNSAT

3-UNSAT$= \{\langle\phi\rangle \mid \phi$ is an unsatisfiable 3-CNF formula$\}$

- If we can give $\mathcal{IP}$ proof for 3-UNSAT, we can give an $\mathcal{IP}$ proof for any $L \in$ co-$\mathcal{NP}$

A co-$\mathcal{NP}$ Complete Problem

3-UNSAT

3-UNSAT$= \{\langle\phi\rangle \mid \phi$ is an unsatisfiable 3-CNF formula$\}$

- If we can give $\mathcal{IP}$ proof for 3-UNSAT, we can give an $\mathcal{IP}$ proof for any $L \in$ co-$\mathcal{NP}$

The Challenge

A co-$\mathcal{NP}$ Complete Problem

3-UNSAT

$$\text{3-UNSAT} = \{\langle\phi\rangle \mid \phi \text{ is an unsatisfiable 3-CNF formula}\}$$

- If we can give $\mathcal{IP}$ proof for 3-UNSAT, we can give an $\mathcal{IP}$ proof for any $L \in$ co-$\mathcal{NP}$

The Challenge

- Need to prove that for all inputs x, $\phi(x) = 0$

A co-$\mathcal{NP}$ Complete Problem

3-UNSAT

3-UNSAT$= \{\langle\phi\rangle \mid \phi$ is an unsatisfiable 3-CNF formula$\}$

- If we can give $\mathcal{IP}$ proof for 3-UNSAT, we can give an $\mathcal{IP}$ proof for any $L \in$ co-$\mathcal{NP}$

The Challenge

- Need to prove that for all inputs x, $\phi(x) = 0$
- But, there are $2^{|x|}$ possible such x

A co-$\mathcal{NP}$ Complete Problem

3-UNSAT

3-UNSAT$= \{\langle\phi\rangle \mid \phi$ is an unsatisfiable 3-CNF formula$\}$

- If we can give $\mathcal{IP}$ proof for 3-UNSAT, we can give an $\mathcal{IP}$ proof for any $L \in$ co-$\mathcal{NP}$

The Challenge

- Need to prove that for all inputs x, $\phi(x) = 0$
- But, there are $2^{|x|}$ possible such x
- How can we prove properties about all possible x at once?

Arithmeti~~c~~ation

z

Arithmetication

Idea

For n inputs $x_1, x_2, \ldots, x_n$, construct a polynomial $\Phi(x_1, \ldots, x_n)$ s.t.

$$\Phi(x_1, \ldots, x_n) = 0 \text{ if and only if } \phi(x_1, \ldots, x_n) \text{ is unsatisfiable}$$

Arithmetication

Idea

For n inputs $x_1, x_2, \ldots, x_n$, construct a polynomial $\Phi(x_1, \ldots, x_n)$ s.t.

$$\Phi(x_1, \ldots, x_n) = 0 \text{ if and only if } \phi(x_1, \ldots, x_n) \text{ is unsatisfiable}$$

Constructing Φ:

$$(x_1 \vee x_2 \vee x_3) \wedge (\bar{x}_1 \vee x_4 \vee x_3)$$

$$(x_1 \vee x_2 \vee x_3) \to (x_1 + x_2 + x_3)$$

$$(\bar{x}_1 \vee x_4 \vee x_3) \to ((1-x_1) + x_4 + x_3)$$

Arithmetication

Idea

For n inputs $x_1, x_2, \ldots, x_n$, construct a polynomial $\Phi(x_1, \ldots, x_n)$ s.t.

$$\Phi(x_1, \ldots, x_n) = 0 \text{ if and only if } \phi(x_1, \ldots, x_n) \text{ is unsatisfiable}$$

Constructing Φ:

- Identify $0 =$false, and positive integer $=$ true

Arithmetication

Idea

For n inputs $x_1, x_2, \ldots, x_n$, construct a polynomial $\Phi(x_1, \ldots, x_n)$ s.t.

$$\Phi(x_1, \ldots, x_n) = 0 \text{ if and only if } \phi(x_1, \ldots, x_n) \text{ is unsatisfiable}$$

Constructing Φ:

- Identify $0 =$false, and positive integer $=$ true
- $x_i \rightarrow x_i$, $\overline{x_i} \rightarrow (1 - x_i)$

Arithmetication

Idea

For n inputs $x_1, x_2, \ldots, x_n$, construct a polynomial $\Phi(x_1, \ldots, x_n)$ s.t.

$$\Phi(x_1, \ldots, x_n) = 0 \text{ if and only if } \phi(x_1, \ldots, x_n) \text{ is unsatisfiable}$$

Constructing Φ:

- Identify 0 =false, and positive integer = true
- $x_i \to x_i$, $\overline{x_i} \to (1 - x_i)$
- Replace $\vee$ with $+$

Arithmetication

Idea

For n inputs $x_1, x_2, \ldots, x_n$, construct a polynomial $\Phi(x_1, \ldots, x_n)$ s.t.

$$\Phi(x_1, \ldots, x_n) = 0 \text{ if and only if } \phi(x_1, \ldots, x_n) \text{ is unsatisfiable}$$

Constructing Φ:

- Identify 0 =false, and positive integer = true
- $x_i \to x_i$, $\overline{x_i} \to (1 - x_i)$
- Replace $\vee$ with $+$
- Replace $\wedge$ with $\times$

Arithmetication

Idea

For n inputs $x_1, x_2, \ldots, x_n$, construct a polynomial $\Phi(x_1, \ldots, x_n)$ s.t.

$$\Phi(x_1, \ldots, x_n) = 0 \text{ if and only if } \phi(x_1, \ldots, x_n) \text{ is unsatisfiable}$$

Constructing Φ:

- Identify 0 =false, and positive integer = true
- $x_i \to x_i$, $\overline{x_i} \to (1 - x_i)$
- Replace $\vee$ with $+$
- Replace $\wedge$ with $\times$

$$\phi(x) = (x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee x_3)$$

$$(x_1 + x_2 + x_3) \cdot ((1 - x_1) + x_2 + x_3)$$

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

- Φ has degree equal to the number (m) of clauses of ϕ
- $\Phi(x_1, \ldots, x_n) \leq 3^m$
- Any clause takes on a positive value iff at least one of its literals is 1
- $\Phi(x_1, \ldots, x_n) > 0$ iff all of its clauses are > 0
- $\Phi(x_1, \ldots, x_n) > 0$ if $\phi(x_1, \ldots, x_n) = TRUE$
- $\Phi(x_1, \ldots, x_n) = 0$ if $\phi(x_1, \ldots, x_n) = FALSE$

$$\phi \in \text{3-UNSAT} \iff \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \underline{\Phi(x_1, \ldots, x_n)} = 0$$

$\Phi(0, \ldots, 0) + \Phi(0, \ldots, 1) + \ldots$ 2^n

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

- Φ has degree equal to the number (m) of clauses of ϕ

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

- Φ has degree equal to the number (m) of clauses of ϕ
- $\Phi(x_1, \ldots, x_n) \leq 3^m$

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

- Φ has degree equal to the number (m) of clauses of ϕ
- $\Phi(x_1, \ldots, x_n) \leq 3^m$
- Any clause takes on a positive value iff at least one of its literals is 1

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

- Φ has degree equal to the number (m) of clauses of ϕ
- $\Phi(x_1, \ldots, x_n) \leq 3^m$
- Any clause takes on a positive value iff at least one of its literals is 1
- $\Phi(x) > 0$ iff all of its clauses are > 0

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

- Φ has degree equal to the number (m) of clauses of ϕ
- $\Phi(x_1, \ldots, x_n) \leq 3^m$
- Any clause takes on a positive value iff at least one of its literals is 1
- $\Phi(x) > 0$ iff all of its clauses are > 0
- $\Phi(x_1, \ldots, x_n) > 0$ if $\phi(x_1, \ldots, x_n) = TRUE$

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

- Φ has degree equal to the number (m) of clauses of ϕ
- $\Phi(x_1, \ldots, x_n) \leq 3^m$
- Any clause takes on a positive value iff at least one of its literals is 1
- $\Phi(x) > 0$ iff all of its clauses are > 0
- $\Phi(x_1, \ldots, x_n) > 0$ if $\phi(x_1, \ldots, x_n) = TRUE$
- $\Phi(x_1, \ldots, x_n) = 0$ if $\phi(x_1, \ldots, x_n) = FALSE$

Properties of Φ

$$\Phi(x) = (x_1 + x_2 + x_3)((1 - x_1) + x_2 + x_3)$$

Consider the value of Φ when the $x_i \in \{0, 1\}$

- Φ has degree equal to the number (m) of clauses of ϕ
- $\Phi(x_1, \ldots, x_n) \leq 3^m$
- Any clause takes on a positive value iff at least one of its literals is 1
- $\Phi(x) > 0$ iff all of its clauses are > 0
- $\Phi(x_1, \ldots, x_n) > 0$ if $\phi(x_1, \ldots, x_n) = TRUE$
- $\Phi(x_1, \ldots, x_n) = 0$ if $\phi(x_1, \ldots, x_n) = FALSE$

$\leq 3^m \cdot 2^n$

$$\phi \in \text{3-UNSAT} \iff \boxed{\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n)} = 0 \bmod q$$

For any prime $q > 2^n 3^m$

Observations

Arithmetization

$$\phi \in \text{3-UNSAT} \quad \Longleftrightarrow \quad \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$$

For any prime $q > 2^n 3^m$

Observations

Arithmetization

$$\phi \in \text{3-UNSAT} \iff \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$$

For any prime $q > 2^n 3^m$

- To prove ϕ is unsatisfiable, enough to prove that expression on the right equals 0
- To do so, we can use the power of algebra:

Observations

Arithmetization

$$\phi \in \text{3-UNSAT} \iff \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$$

For any prime $q > 2^n 3^m$

- To prove ϕ is unsatisfiable, enough to prove that expression on the right equals 0
- To do so, we can use the power of algebra:
  - A polynomial of degree m has at most m roots

$(x-a)(x-b)(x-c)\ldots$

Observations

Arithmetization

$$\phi \in \text{3-UNSAT} \iff \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$$

For any prime $q > 2^n 3^m$

- To prove ϕ is unsatisfiable, enough to prove that expression on the right equals 0
- To do so, we can use the power of algebra:
  - A polynomial of degree m has at most m roots
  - Two different polynomials of degree m can only agree in at most m points

$f_1(x) \neq f_2(x)$

$f_1(x) - f_2(x) = 0$ iff $f_1(x) = f_2(x)$

Observations

Arithmetization

$$\phi \in \text{3-UNSAT} \iff \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$$

For any prime $q > 2^n 3^m$

- To prove ϕ is unsatisfiable, enough to prove that expression on the right equals 0
- To do so, we can use the power of algebra:
  - A polynomial of degree m has at most m roots
  - Two different polynomials of degree m can only agree in at most m points

Key Idea

Observations

Arithmetization

$$\phi \in \text{3-UNSAT} \iff \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$$

For any prime $q > 2^n 3^m$

- To prove ϕ is unsatisfiable, enough to prove that expression on the right equals 0
- To do so, we can use the power of algebra:
  - A polynomial of degree m has at most m roots
  - Two different polynomials of degree m can only agree in at most m points

Key Idea

- We only need to prove properties of Φ on inputs $x_i \in \{0, 1\}$

Observations

Arithmetization

$$\phi \in \text{3-UNSAT} \iff \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$$

For any prime $q > 2^n 3^m$

- To prove ϕ is unsatisfiable, enough to prove that expression on the right equals 0
- To do so, we can use the power of algebra:
  - A polynomial of degree m has at most m roots
  - Two different polynomials of degree m can only agree in at most m points

Key Idea

- We only need to prove properties of Φ on inputs $x_i \in \{0, 1\}$
- We will use the values of Φ on $x_i \in [0, \ldots, q - 1]$ to check these properties

Nested Polynomials

Nested Polynomials

Goal

Prove that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

Nested Polynomials

P_1

$\sum_{x_1} \left(\sum_{x_2} \cdots \sum_{x_n} \right)$

Goal

Prove that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$

$P_1(0) + P_1(1) = P(x)$

Nested Polynomials

Goal

Prove that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$
- Define $P_2(x_2) = \sum_{x_3 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, x_2 \ldots, x_n)$

$$P_1(r_1) = P_2(0) + P_2(1)$$

Nested Polynomials

Goal

Prove that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$
- Define $P_2(x_2) = \sum_{x_3 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, x_2 \ldots, x_n)$
- Define $P_i(x_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$

Nested Polynomials

Goal

Prove that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$
- Define $P_2(x_2) = \sum_{x_3 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, x_2 \ldots, x_n)$
- Define $P_i(x_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$

$$P_i(0) + P_i(1) = P_{i-1}(r_i)$$

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \boxed{\Phi(x_1, \ldots, x_n)} = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$
2. V chooses prime $q > 2^n 3^m$

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$
2. V chooses prime $q > 2^n 3^m$
3. V sets $v_0 = 0$

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$
2. V chooses prime $q > 2^n 3^m$
3. V sets $v_0 = 0$
4. Repeat the following for $i = 1$ to n

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$
2. V chooses prime $q > 2^n 3^m$
3. V sets $v_0 = 0$
4. Repeat the following for $i = 1$ to n
    1. P sends poly $P_i(y)$ of degree $\leq m$

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$
2. V chooses prime $q > 2^n 3^m$
3. V sets $v_0 = 0$
4. Repeat the following for $i = 1$ to n
    1. P sends poly $P_i(y)$ of degree $\leq m$
    2. V does the following:

Sum-check Protocol

$P_1(0) + P_1(1) \doteq$

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$
2. V chooses prime $q > 2^n 3^m$
3. V sets $v_0 = 0$
4. Repeat the following for $i = 1$ to n
    1. P sends poly $P_i(y)$ of degree $\leq m$
    2. V does the following:
        - V checks that $P_i(0) + P_i(1) = v_{i-1} \bmod q$

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$
2. V chooses prime $q > 2^n 3^m$
3. V sets $v_0 = 0$
4. Repeat the following for $i = 1$ to n
   1. P sends poly $P_i(y)$ of degree $\leq m$
   2. V does the following:
      - V checks that $P_i(0) + P_i(1) = v_{i-1} \bmod q$
      - V picks $r_i \in [0, \ldots, q-1]$, sets $v_i = P_i(r_i)$ and sends r_i to P

Sum-check Protocol

Goal

Prove that $\sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

1. Both P, and V have ϕ, P constructs poly Φ. V can't construct Φ, but can evaluate $\Phi(x_1, \ldots, x_n)$
2. V chooses prime $q > 2^n 3^m$
3. V sets $v_0 = 0$
4. Repeat the following for $i = 1$ to n
   1. P sends poly $P_i(y)$ of degree $\leq m$
   2. V does the following:
      - V checks that $P_i(0) + P_i(1) = v_{i-1} \bmod q$
      - V picks $r_i \in [0, \ldots, q-1]$, sets $v_i = P_i(r_i)$ and sends r_i to P
5. V accepts if $\Phi(r_1, \ldots, r_n) = v_n \bmod q$

Completeness

If ϕ is not satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \mod q$

Completeness

If ϕ is not satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \mod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$

Completeness

If ϕ is not satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$
  - $P_1(0) + P_1(1) = P(x) = 0 = v_0$

Completeness

If ϕ is not satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$
  - $P_1(0) + P_1(1) = P(x) = 0 = v_0$

- Define $P_2(x_2) = \sum_{x_3 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, x_2 \ldots, x_n)$

Completeness

If ϕ is not satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$
  - $P_1(0) + P_1(1) = P(x) = 0 = v_0$
- Define $P_2(x_2) = \sum_{x_3 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, x_2 \ldots, x_n)$
  - $P_2(0) + P_2(1) = P_1(r_1) = v_1$

Completeness

If ϕ is not satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$
  - $P_1(0) + P_1(1) = P(x) = 0 = v_0$
- Define $P_2(x_2) = \sum_{x_3 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, x_2 \ldots, x_n)$
  - $P_2(0) + P_2(1) = P_1(r_1) = v_1$
- Define $P_i(x_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$

Completeness

If ϕ is not satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) = 0 \bmod q$

- Define $P_1(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, x_2 \ldots, x_n)$
  - $P_1(0) + P_1(1) = P(x) \underline{= 0} = v_0$
- Define $P_2(x_2) = \sum_{x_3 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, x_2 \ldots, x_n)$
  - $\underline{P_2(0) + P_2(1) = P_1(r_1)} = v_1$
- Define $P_i(x_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$

If P chooses the polys P_i as specified, he will pass all the checks, so V accepts

Soundness

If ϕ is satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) \neq 0 \bmod q$

Soundness

If ϕ is satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) \neq 0 \bmod q$

- Malicious P is trying to prove that $v_0 = 0$

Soundness

If ϕ is satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) \neq 0 \bmod q$

- Malicious P is trying to prove that $v_0 = 0$
- In iteration i, P is trying to prove that

$$v_{i-1} = \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

Soundness

If ϕ is satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) \neq 0 \bmod q$

- Malicious P is trying to prove that $v_0 = 0$
- In iteration i, P is trying to prove that

$$v_{i-1} = \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

  - P sends poly P_i'

Soundness

If ϕ is satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) \neq 0 \bmod q$

- Malicious P is trying to prove that $v_0 = 0$
- In iteration i, P is trying to prove that

$$v_{i-1} = \sum_{x_i \in \{0,1\}} \left(\cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n) \right)$$

P_i

  - P sends poly P'_i
  - V checks that $P'_i(0) + P'_i(1) = v_{i-1}$, if so he picks r_i

Soundness

If ϕ is satisfiable

Know that $P(x) = \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(x_1, \ldots, x_n) \neq 0 \bmod q$

- Malicious P is trying to prove that $v_0 = 0$
- In iteration i, P is trying to prove that

$$v_{i-1} = \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

  - P sends poly P'_i
  - V checks that $P'_i(0) + P'_i(1) = v_{i-1}$, if so he picks r_i
- Now, P needs to prove that

$v_i = P_i(r_i)$

$$v_i = P'_i(r_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, r_i, x_{i+1} \ldots, x_n)$$

Soundness

- Suppose that

$$v_{i-1} \neq \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

Soundness

- Suppose that

$$v_{i-1} \neq \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

Must be the case for some i since $v_0 \neq 0$

Soundness

- Suppose that

$$v_{i-1} \neq \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

Must be the case for some i since $v_0 \neq 0$

- P succeeds in proving

$$v_i = P_i'(r_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, r_i, x_{i+1} \ldots, x_n)$$

with probability $\leq (n - i + 1)/q$

Soundness

- Suppose that

$$v_{i-1} \neq \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

  Must be the case for some i since $v_0 \neq 0$

- P succeeds in proving

$$v_i = P'_i(r_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, r_i, x_{i+1} \ldots, x_n)$$

  with probability $\leq (n - i + 1)/q$

Proof sketch:

Soundness

- Suppose that

$$v_{i-1} \neq \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

  Must be the case for some i since $v_0 \neq 0$

- P succeeds in proving

$$v_i = P'_i(r_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, r_i, x_{i+1} \ldots, x_n)$$

  with probability $\leq (n - i + 1)/q$

Proof sketch:

- Let $\hat{P}(x_i)$ be the poly P is supposed to send

Soundness

- Suppose that

$$v_{i-1} \neq \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

  Must be the case for some i since $v_0 \neq 0$

- P succeeds in proving

$$v_i = P'_i(r_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, r_i, x_{i+1} \ldots, x_n)$$

  with probability $\leq (n - i + 1)/q$

Proof sketch:

- Let $\hat{P}(x_i)$ be the poly P is supposed to send
- Let $P'(x_i)$ be the poly he does send

Soundness

- Suppose that

$$v_{i-1} \neq \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

  Must be the case for some i since $v_0 \neq 0$
- P succeeds in proving

$$v_i = P'_i(r_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, r_i, x_{i+1} \ldots, x_n)$$

  with probability $\leq (n - i + 1)/q$

Proof sketch:

- Let $\hat{P}(x_i)$ be the poly P is supposed to send
- Let $P'(x_i)$ be the poly he does send
- If $\hat{P} \neq P'$, then they agree in at most $n - i + 1$ points.

Soundness

- Suppose that

$$v_{i-1} \neq \sum_{x_i \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, x_i \ldots, x_n)$$

  Must be the case for some i since $v_0 \neq 0$
- P succeeds in proving

$$v_i = P_i'(r_i) = \sum_{x_{i+1} \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} \Phi(r_1, \ldots, r_{i-1}, r_i, x_{i+1} \ldots, x_n)$$

  with probability $\leq (n - i + 1)/q$

Proof sketch:

- Let $\hat{P}(x_i)$ be the poly P is supposed to send
- Let $P'(x_i)$ be the poly he does send
- If $\hat{P} \neq P'$, then they agree in at most $n - i + 1$ points. So, the probability that r_i is one of these is at most $(n - i + 1)/q$

What Is Going On Here

- To break soundness, P needs to make V think that Φ evaluates to 0 when it doesn't

What Is Going On Here

- To break soundness, P needs to make V think that Φ evaluates to 0 when it doesn't
- To do so, at some level of the recursion he must find a polynomial P' that agrees with the correct restriction of Φ (called P) on a randomly chosen point r_i

What Is Going On Here

- To break soundness, P needs to make V think that Φ evaluates to 0 when it doesn't
- To do so, at some level of the recursion he must find a polynomial P' that agrees with the correct restriction of Φ (called P) on a randomly chosen point r_i
- But, since all these polys are low degree, this is very unlikely

Conclusion

We have now proven that

$$\text{3-UNSAT} \in \mathcal{IP}$$

Conclusion

We have now proven that

$$\text{3-UNSAT} \in \mathcal{IP}$$

Implying that

$$\text{co-}\mathcal{NP} \subseteq \mathcal{IP}$$

Conclusion

We have now proven that

$$\text{3-UNSAT} \in \mathcal{IP}$$

Implying that

$$\text{co-}\mathcal{NP} \subseteq \mathcal{IP}$$

But, the proof is not short: Required $O(n)$ rounds of communication.