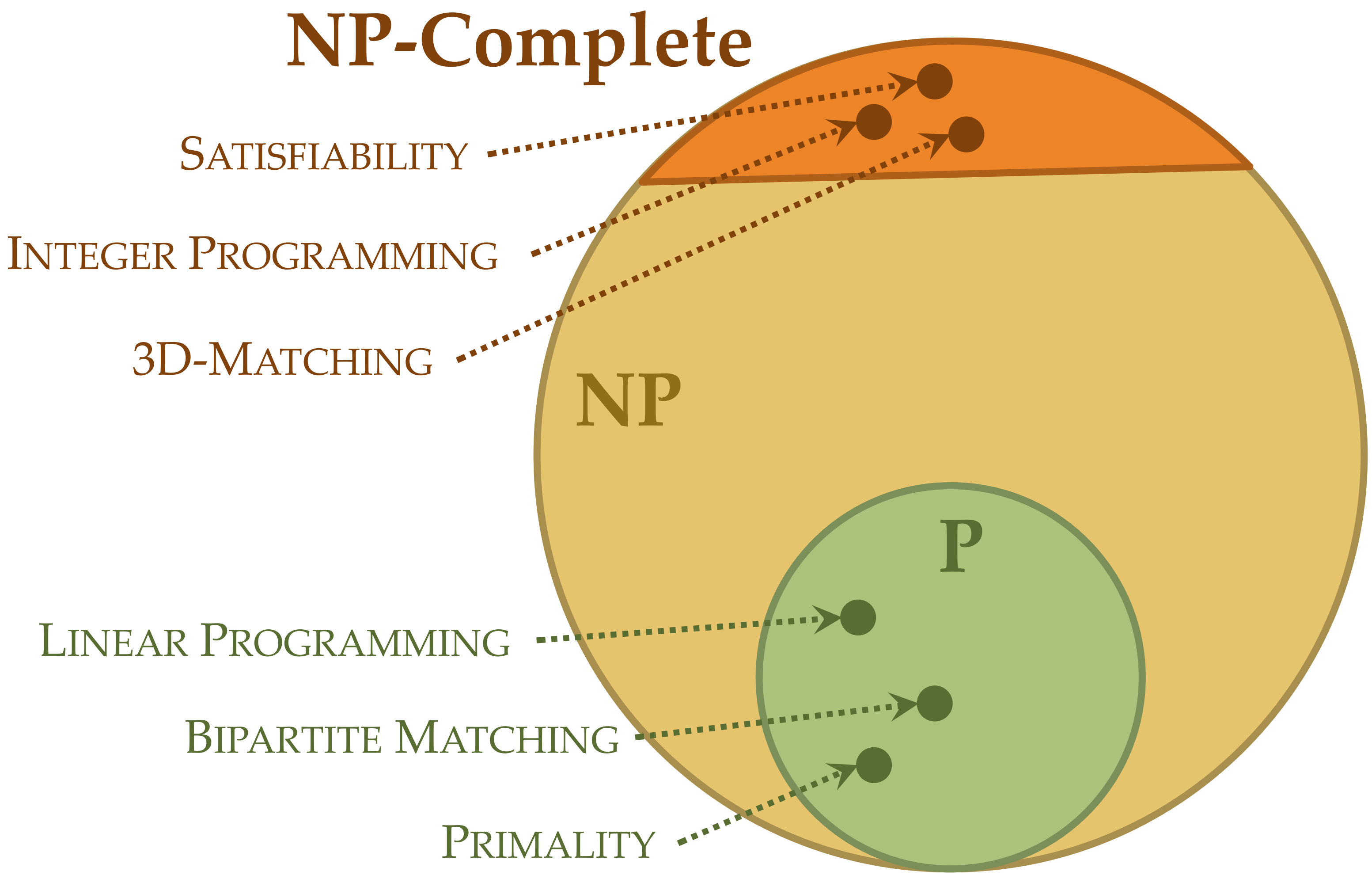
PPP-Completeness with Connections to Cryptography

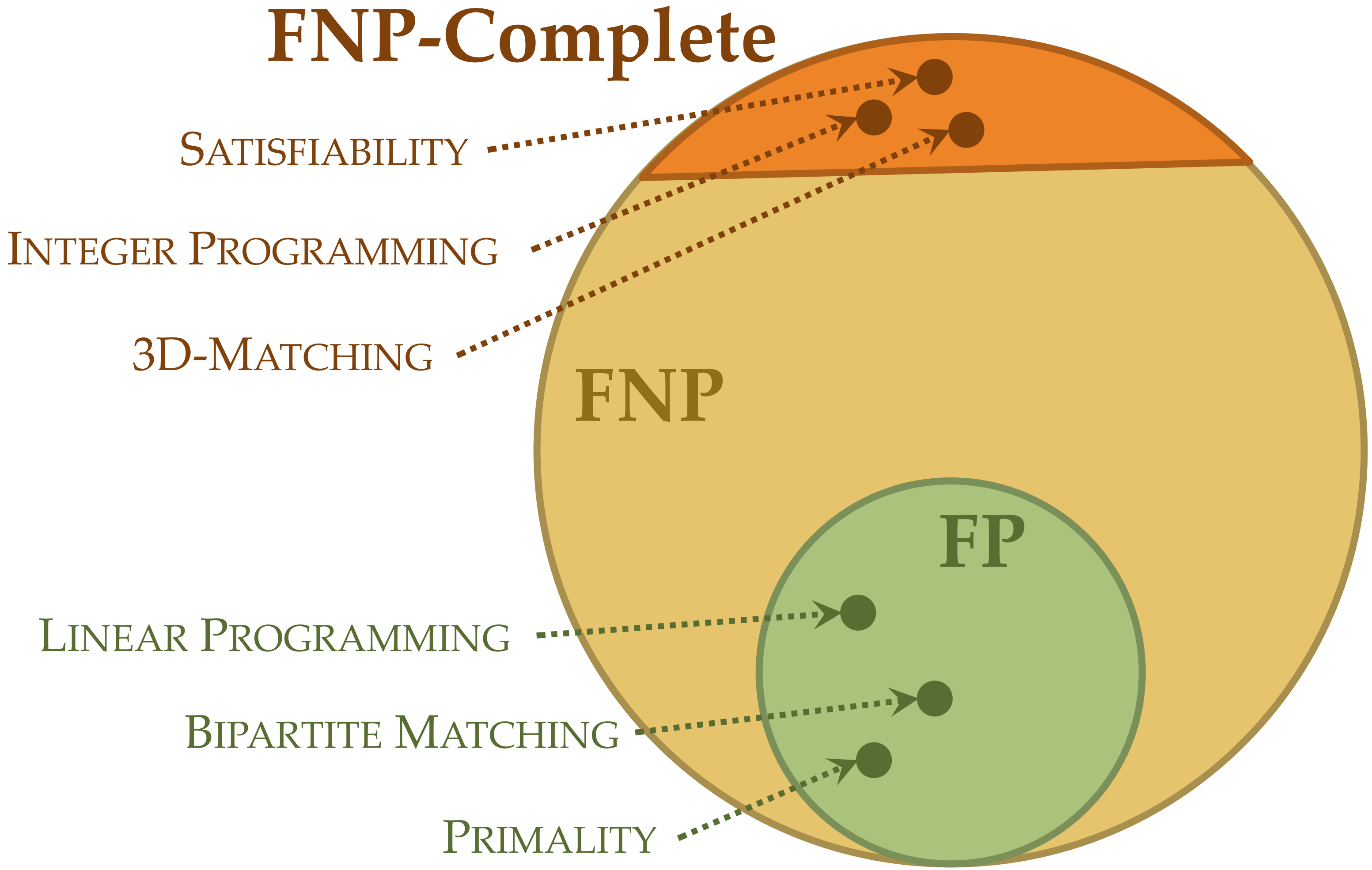
Katerina Sotiraki
MIT

based on work with M. Göös, P. Kamath, M. Zampetakis, G. Zirdelis

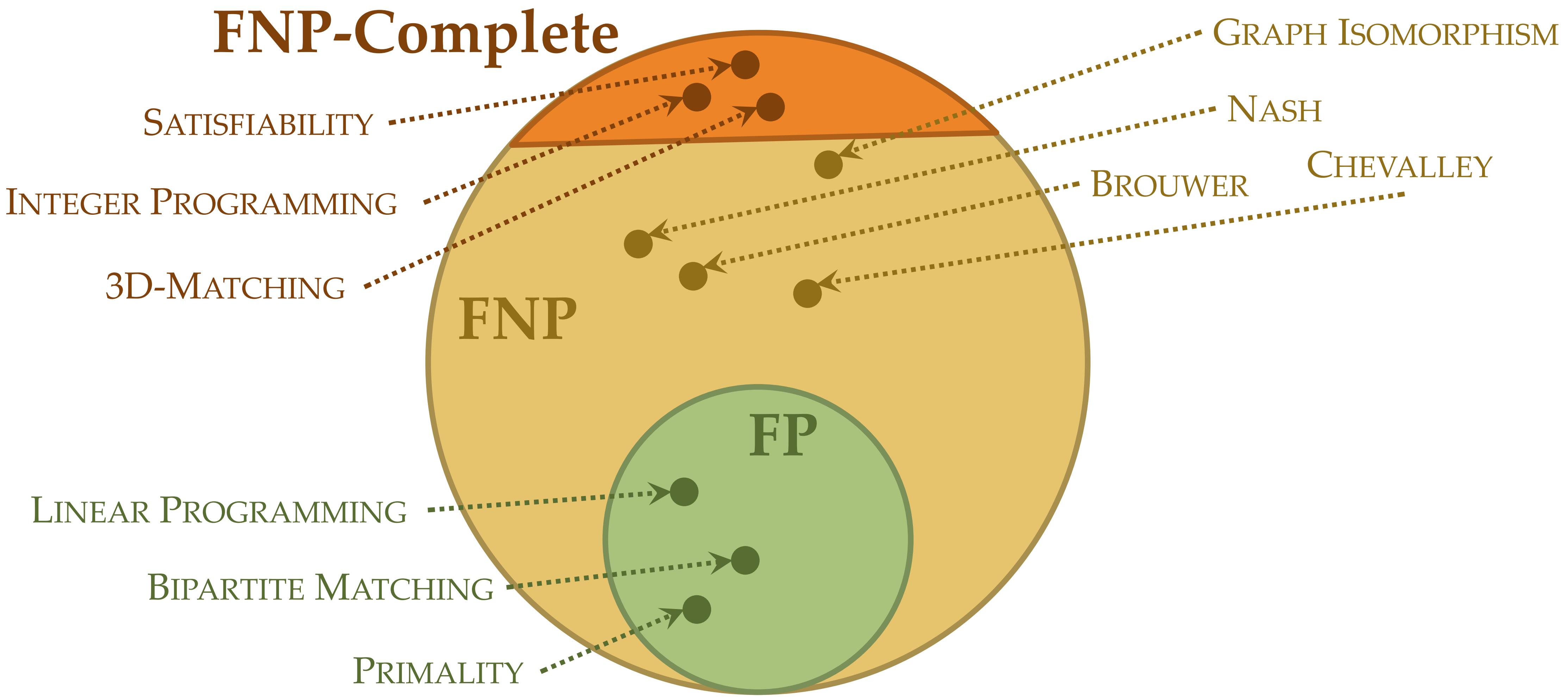
DECISION PROBLEMS: P vs. NP



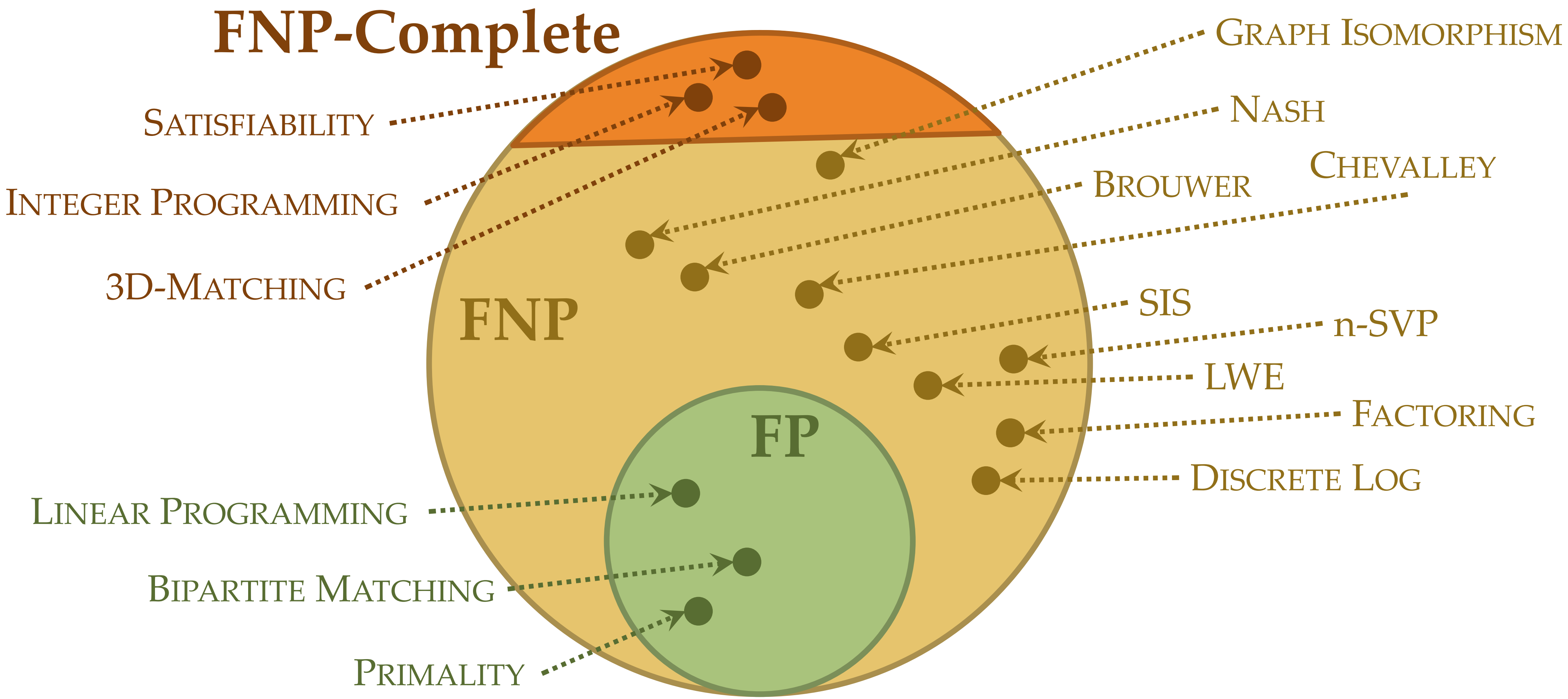
SEARCH PROBLEMS



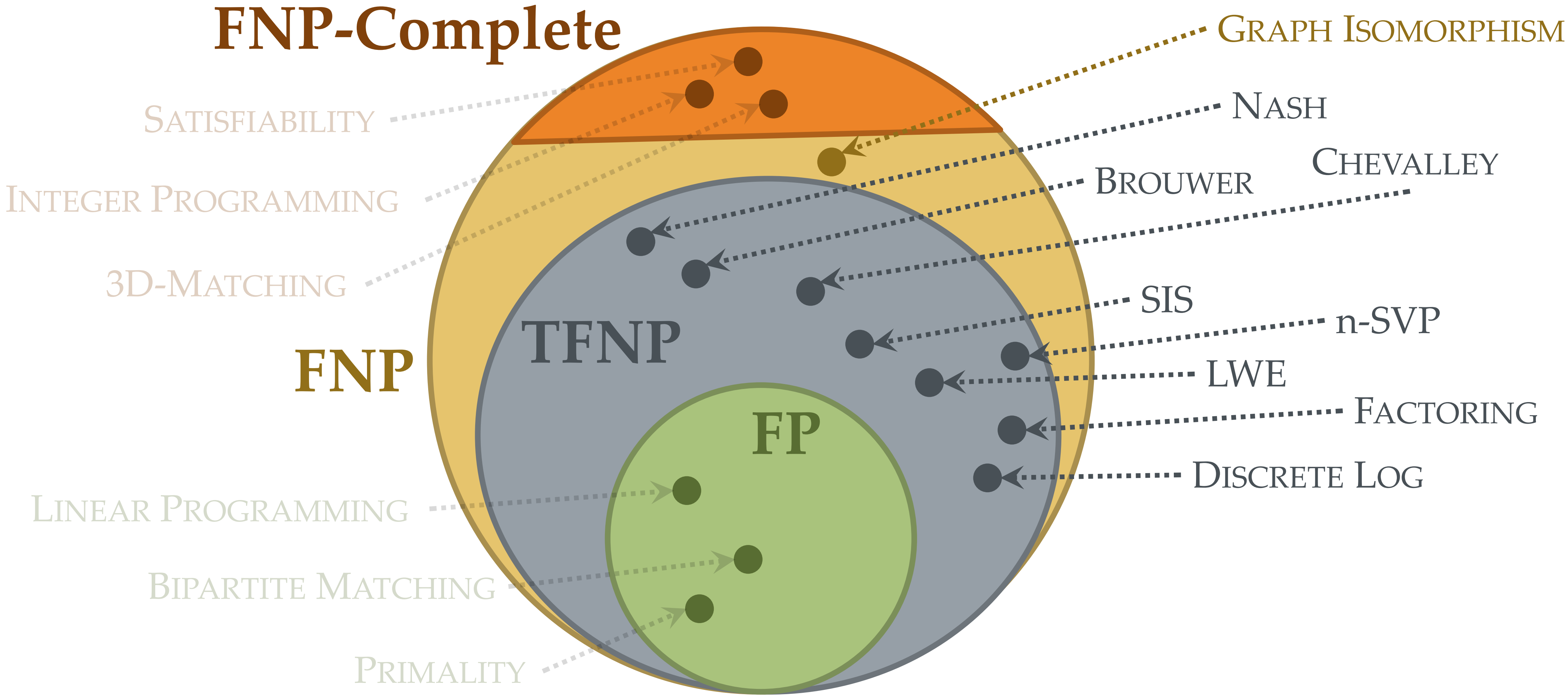
SEARCH PROBLEMS



SEARCH PROBLEMS



TOTAL SEARCH PROBLEMS



COMPLEXITY OF TOTAL SEARCH PROBLEMS

FNP: class of search problems whose decision version is in NP.

TFNP: class of total search problems of FNP, i.e. a solution always exists.

COMPLEXITY OF TOTAL SEARCH PROBLEMS

FNP: class of search problems whose decision version is in NP.

TFNP: class of total search problems of FNP, i.e. a solution always exists.

Theorem [Johnson Papadimitriou Yannakakis '88, Megiddo Papadimitriou '91]:
If some problem $L \in$ **TFNP** is **FNP**-complete under *deterministic* reductions then **NP** = **co-NP.**

COMPLEXITY OF TOTAL SEARCH PROBLEMS

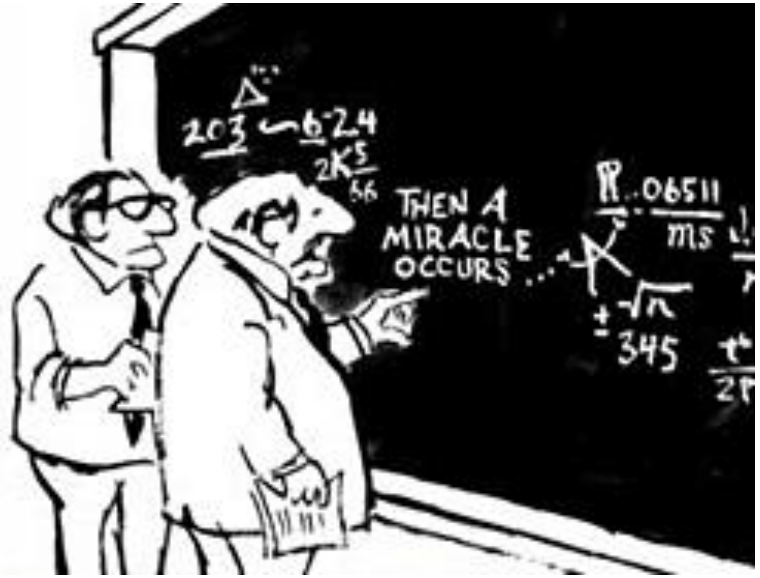
FNP: class of search problems whose decision version is in NP.

TFNP: class of total search problems of FNP, i.e. a solution always exists.

Theorem [Johnson Papadimitriou Yannakakis '88, Megiddo Papadimitriou '91]:
If some problem $L \in$ **TFNP** is **FNP**-complete under *deterministic* reductions then **NP** = **co-NP.**

Theorem [Mahmoody Xiao '09]:
If some problem $L \in$ **TFNP** is **FNP**-complete under *randomized* reductions then SAT is checkable.

A COMPLEXITY THEORY OF TOTAL SEARCH PROBLEMS?



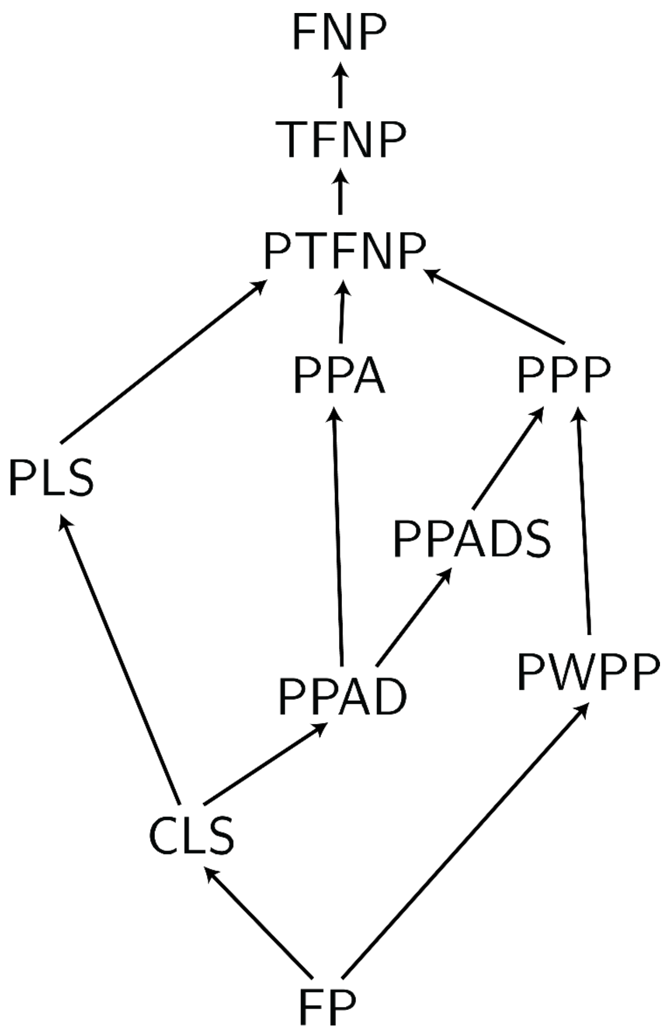
"Total search problems should be classified in terms of the profound mathematical principles that are invoked to establish their totality."

Papadimitriou '94

COMPLEXITY OF TOTAL SEARCH PROBLEMS

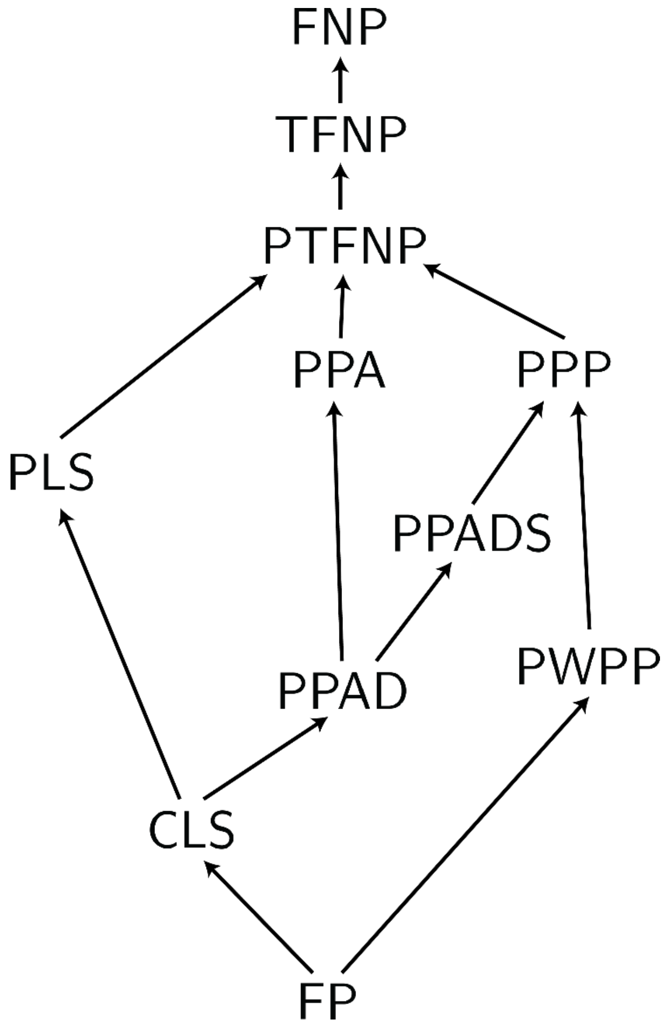
TFNP: class of total search problems of FNP, i.e. a solution always exists [Megiddo Papadimitriou 91]

Subclasses of TFNP introduced by [Johnson Papadimitriou Yannakakis 88], [Papadimitriou 94], [Daskalakis Papadimitriou 11], [Jerabek 16]



COMPLEXITY OF TOTAL SEARCH PROBLEMS

Many applications in game theory, economics, social choice, (discrete / continuous) optimization
e.g. [JYP88], [BCE+98], [EGG06], [CDDT09], [DP11], [R15], [R16], [BIQ+17], [GP17], [DTZ18], [FG18] …



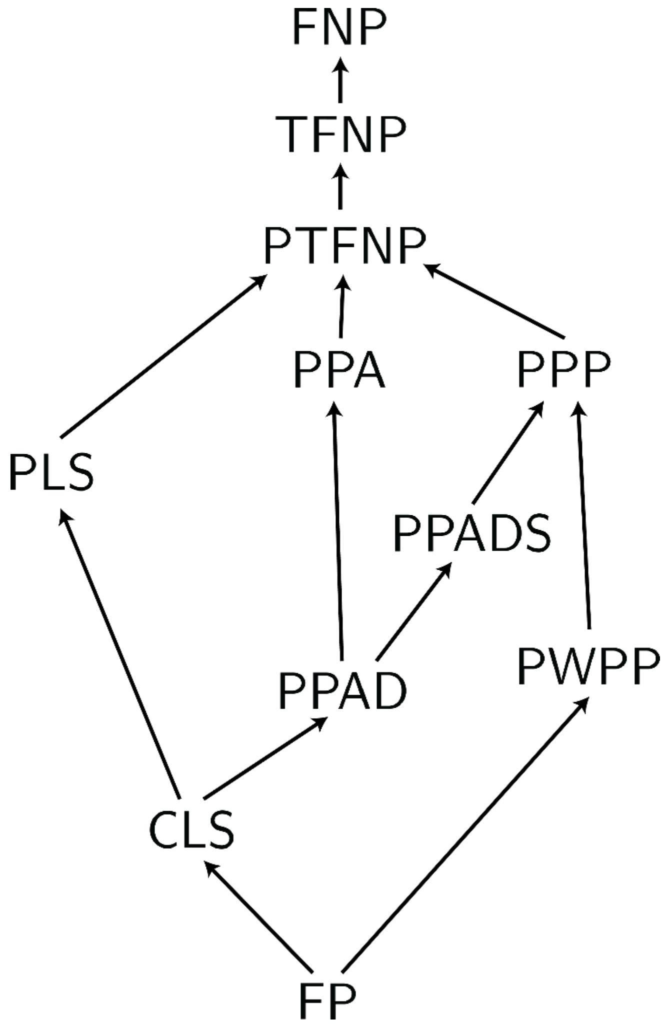
COMPLEXITY OF TOTAL SEARCH PROBLEMS

Many applications in game theory, economics, social choice, (discrete / continuous) optimization
e.g. [JYP88], [BCE+98], [EGG06], [CDDT09], [DP11], [R15], [R16], [BIQ+17], [GP17], [DTZ18], [FG18] …

Most celebrated result:

NASH is PPAD-complete

[Daskalakis Goldberg Papadimitriou 06], [Chen Deng Teng 06]



COMPLEXITY OF TOTAL SEARCH PROBLEMS

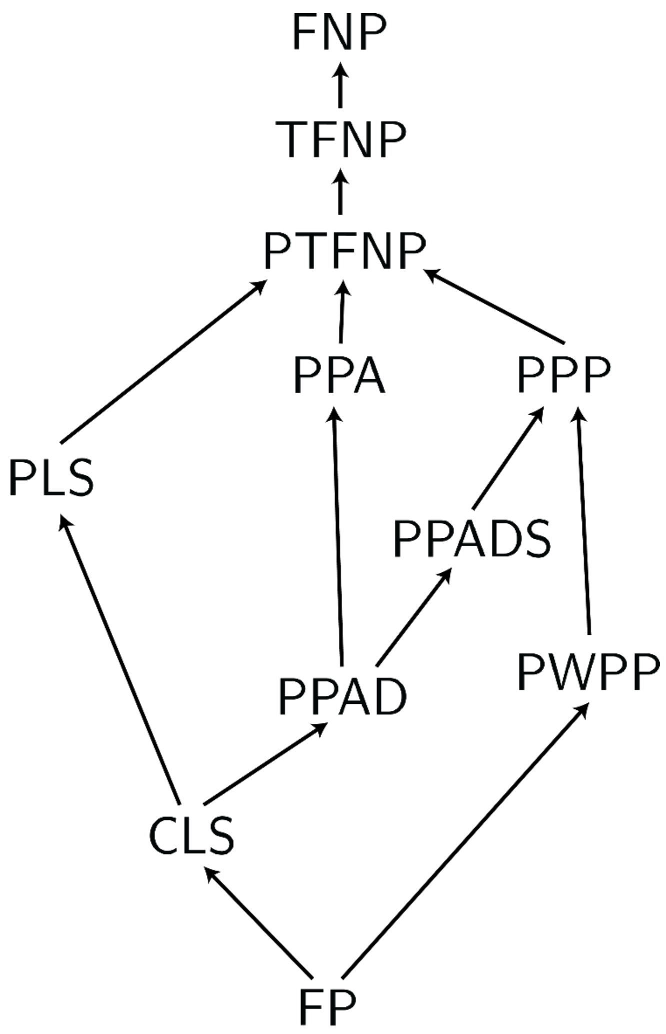
Many applications in game theory, economics, social choice, (discrete / continuous) optimization
e.g. [JYP88], [BCE+98], [EGG06], [CDDT09], [DP11], [R15], [R16], [BIQ+17], [GP17], [DTZ18], [FG18] …

Most celebrated result:

NASH is PPAD-complete

[Daskalakis Goldberg Papadimitriou 06], [Chen Deng Teng 06]

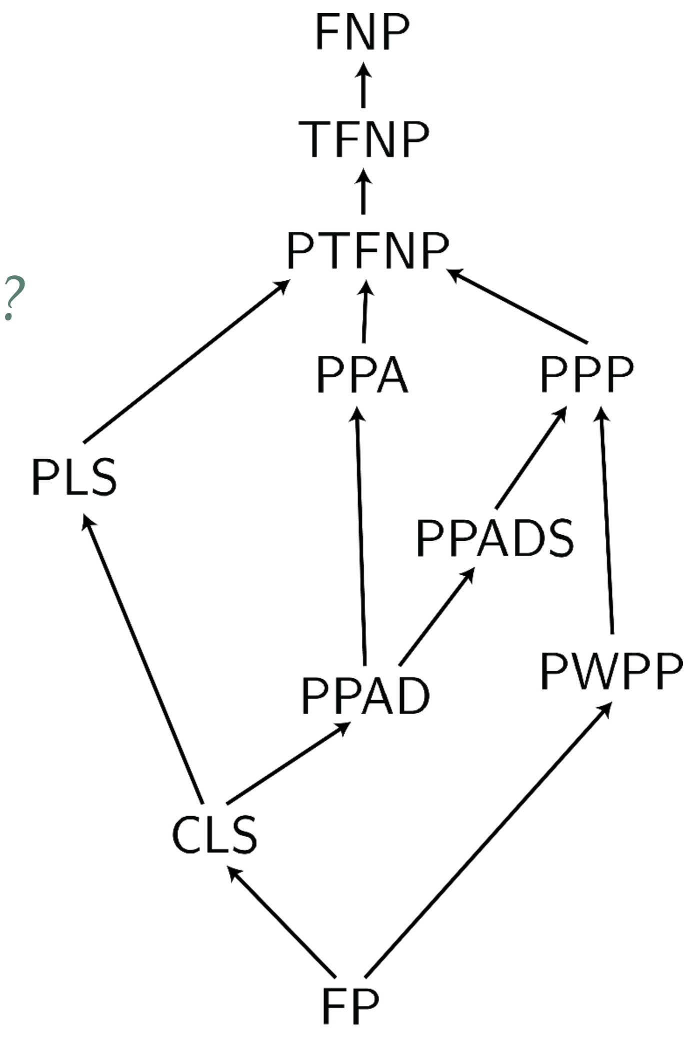
Many applications in Cryptography [B06], [J16]
[BPR15], [GPS16], [HY17], [CHKPRR19],[KNY17]…



COMPLEXITY OF TOTAL SEARCH PROBLEMS

*Are there **natural** complete problems for* **TFNP** *subclasses?*

Natural: a problem that does not explicitly contain a circuit or a Turing machine as part of the input.



NATURAL PROBLEMS

Natural: a problem that does not explicitly contain a circuit or a Turing machine as part of the input.

Example:

INPUT: Given the description M of a non-deterministic Turing machine and an input x.

OUTPUT: The value $M(x)$.

NATURAL PROBLEMS

Natural: a problem that does not explicitly contain a circuit or a Turing machine as part of the input.

Example:

INPUT: Given the description M of a non-deterministic Turing machine and an input x.

OUTPUT: The value $M(x)$.

Theorem
This problem is NP-complete.

NATURAL PROBLEMS

Natural: a problem that does not explicitly contain a circuit or a Turing machine as part of the input.

Example:

INPUT: Given the description M of a non-deterministic Turing machine and an input x.

OUTPUT: The value $M(x)$.

Theorem
This problem is NP-complete.

Theorem (Cook-Levin)
SAT is NP-complete.

NATURAL PROBLEMS

Natural: a problem that does not explicitly contain a circuit or a Turing machine as part of the input.

Example:

INPUT: Given the description M of a non-deterministic Turing machine and an input x.

OUTPUT: The value $M(x)$.

Theorem
This problem is NP-complete.

Theorem (Cook-Levin)
SAT is NP-complete.

TSP

… … …

SUBSET SUM

NATURAL PROBLEMS

Natural: a problem that does not explicitly contain a circuit or a Turing machine as part of the input.

Example:

INPUT: Given the description M of a non-deterministic Turing machine and an input x.

OUTPUT: The value $M(x)$.

Not natural!

Theorem
This problem is NP-complete.

Theorem (Cook-Levin)
SAT is NP-complete.

TSP

… … …

SUBSET SUM

NATURAL PROBLEMS

Natural: a problem that does not explicitly contain a circuit or a Turing machine as part of the input.

Example:

INPUT: Given the description M of a non-deterministic Turing machine and an input x.

OUTPUT: The value $M(x)$.

Natural!

Theorem
This problem is NP-complete.

Theorem (Cook-Levin)
SAT is NP-complete.

TSP

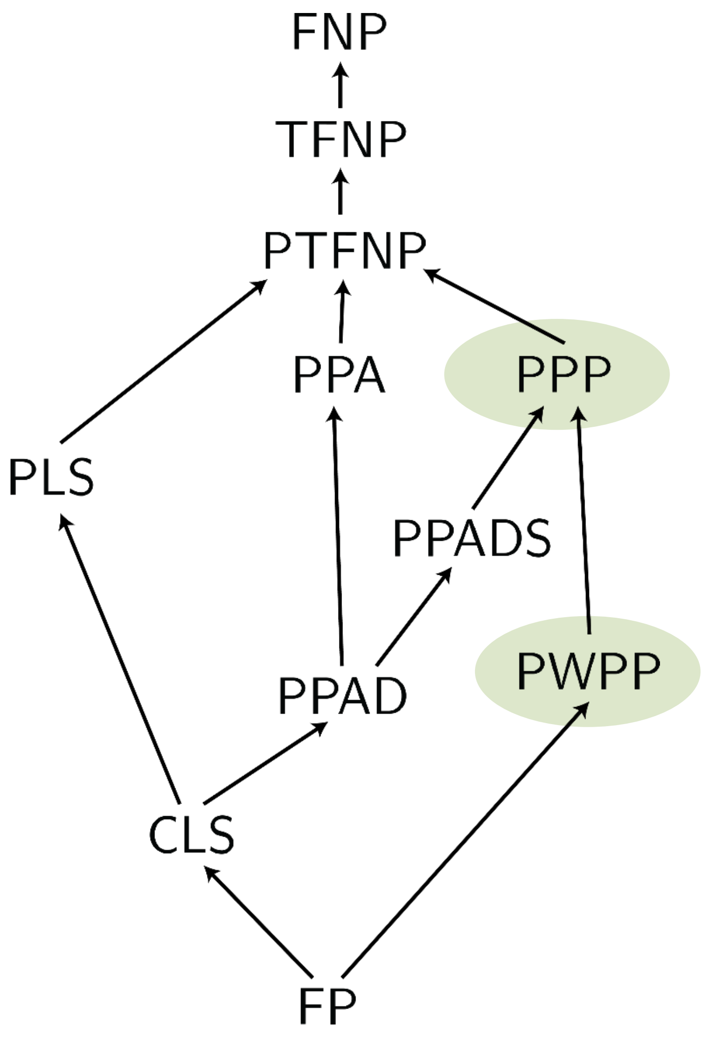
... ...

SUBSET SUM

COMPLEXITY OF TOTAL SEARCH PROBLEMS

Theorem [S Zampetakis Zirdelis 18]:
The first natural complete problems for PPP and PWPP

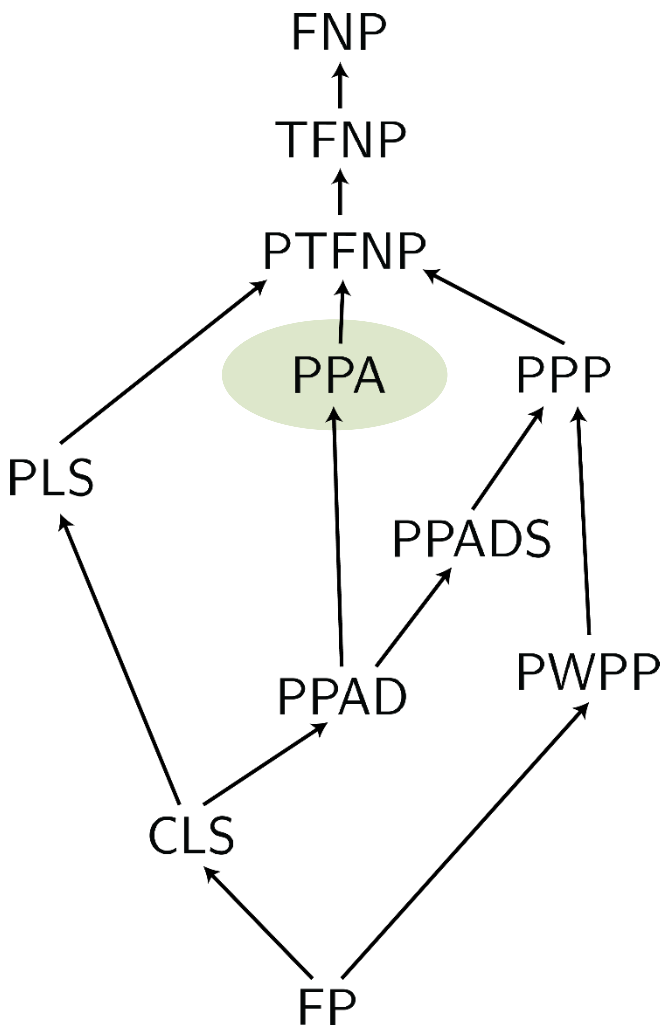
There are natural collision-resistant hash functions that are universal in a *worst-case* sense based on generalizations of SIS.



COMPLEXITY OF TOTAL SEARCH PROBLEMS

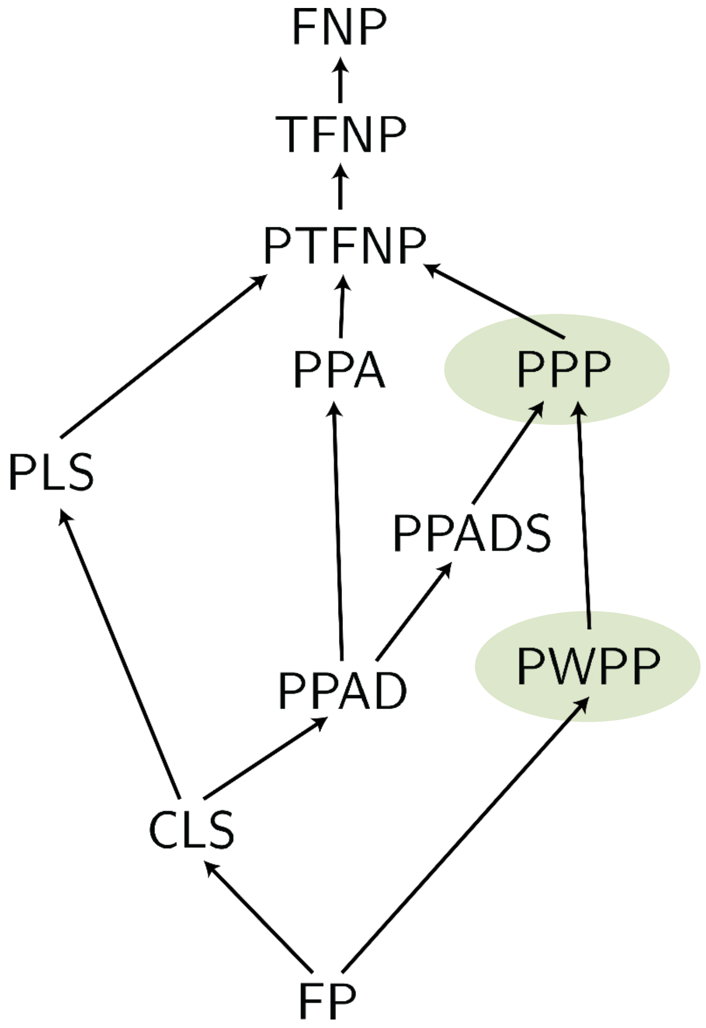
Theorem [Göös Kamath S Zampetakis 19] **:**
The first natural complete problems for PPA_p for any prime p.

For some parameter range, SIS is no harder than the computational analogue of Chevalley-Warning Theorem.



COMPLEXITY OF TOTAL SEARCH PROBLEMS

PPP, PWPP → Pigeonhole principle



Theorem [S Zampetakis Zirdelis 18]:
The first natural complete problems for PPP and PWPP

POLYNOMIAL PIGEONHOLE PRINCIPLE

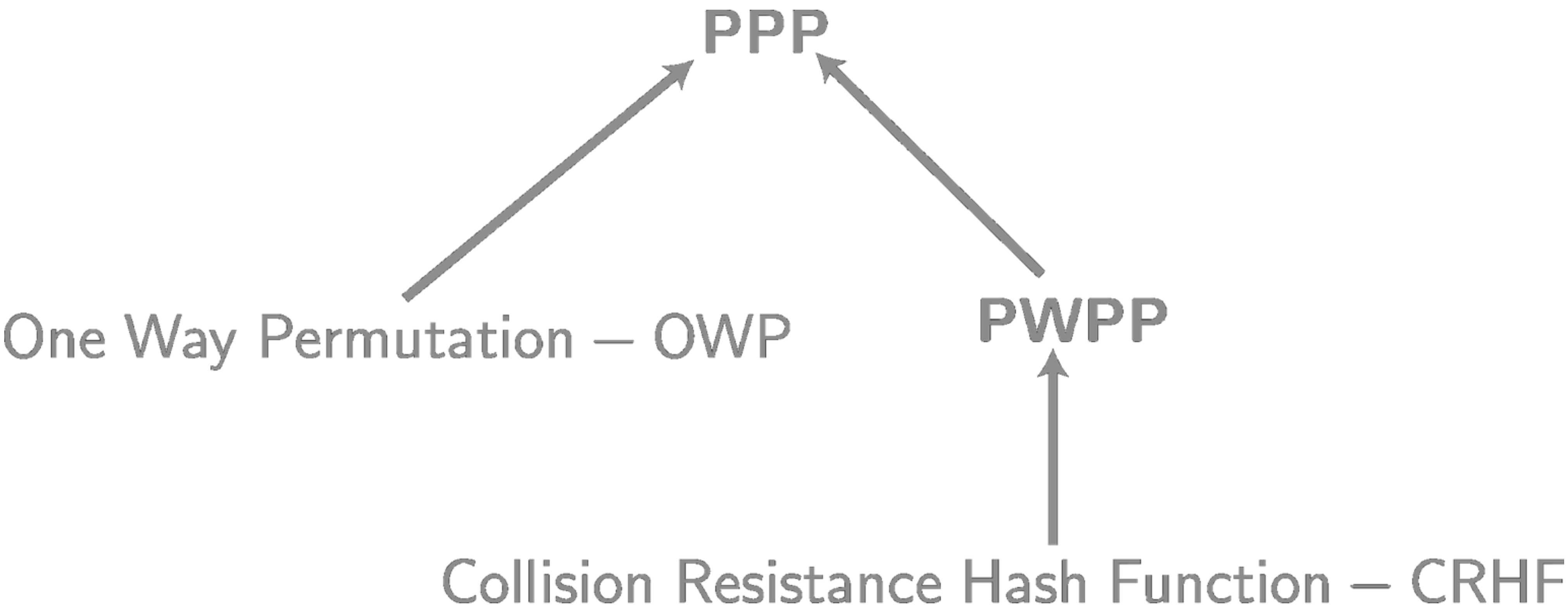
PPP:
Given a circuit $C : \{0,1\}^n \to \{0,1\}^n$. Find:

1. An $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{0}$ or
2. a collision, i.e. $\mathbf{x} \neq \mathbf{y}$ s.t. $C(\mathbf{x}) = C(\mathbf{y})$.

POLYNOMIAL WEAK PIGEONHOLE PRINCIPLE

PWPP:
Given a circuit $C : \{0,1\}^n \to \{0,1\}^m$, with $m < n$.
Find a collision, i.e. $\mathbf{x} \neq \mathbf{y}$ s.t. $C(\mathbf{x}) = C(\mathbf{y})$.

PPP/PWPP AND CRYPTOGRAPHY



PPP & LATTICES

MINKOWSKI
INPUT: A basis $\mathbf{B} \in \mathbb{Z}^{n \times n}$.
OUTPUT: A vector $\mathbf{x}$ in the lattice $\mathcal{L}(\mathbf{B})$ such that $\|\mathbf{x}\|_\infty \leq \det^{1/n}(\mathbf{B})$.

PPP & LATTICES

(HermiteSVP$_\infty$)
Minkowski
Input: A basis $\mathbf{B} \in \mathbb{Z}^{n \times n}$.
Output: A vector $\mathbf{x}$ in the lattice $\mathcal{L}(\mathbf{B})$ such that $\|\mathbf{x}\|_\infty \leq \det^{1/n}(\mathbf{B})$.

PPP & LATTICES

MINKOWSKI
INPUT: A basis $\mathbf{B} \in \mathbb{Z}^{n \times n}$.
OUTPUT: A vector $\mathbf{x}$ in the lattice $\mathcal{L}(\mathbf{B})$ such that $\|\mathbf{x}\|_\infty \leq \det^{1/n}(\mathbf{B})$.

PPP & LATTICES

MINKOWSKI
INPUT: A basis $\mathbf{B} \in \mathbb{Z}^{n \times n}$.
OUTPUT: A vector $\mathbf{x}$ in the lattice $\mathcal{L}(\mathbf{B})$ such that $\|\mathbf{x}\|_\infty \leq \det^{1/n}(\mathbf{B})$.

Theorem [S. Zampetakis Zirdelis '18, Ban Jain Papadimitiou Psomas Rubinstein '19]
MINKOWSKI is in PPP.

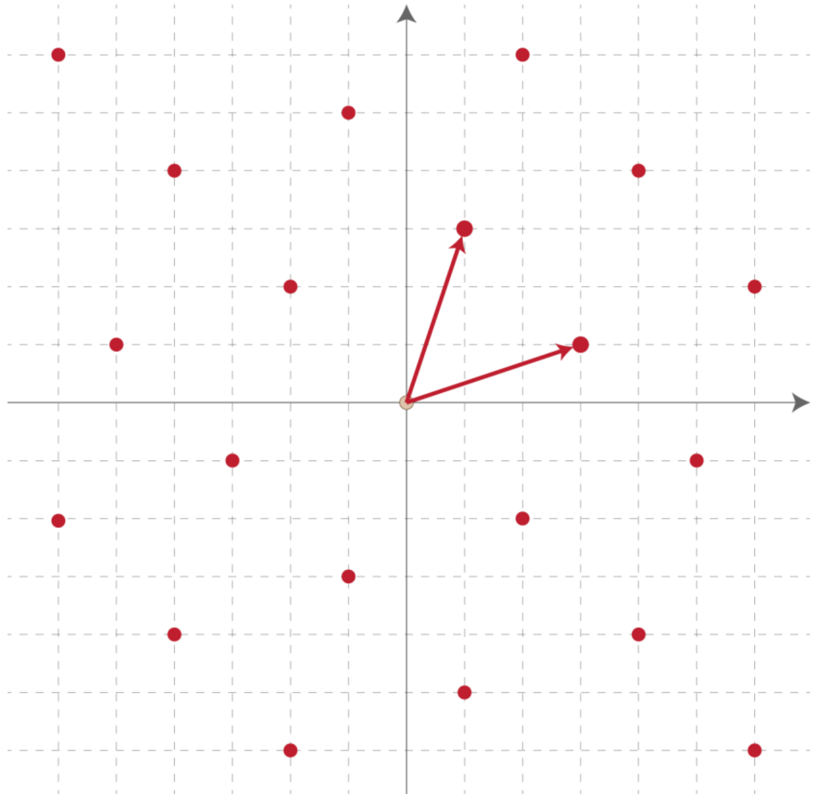
POLYNOMIAL PIGEONHOLE PRINCIPLE

PPP:

Given a circuit $C : \{0,1\}^n \to \{0,1\}^n$. Find:

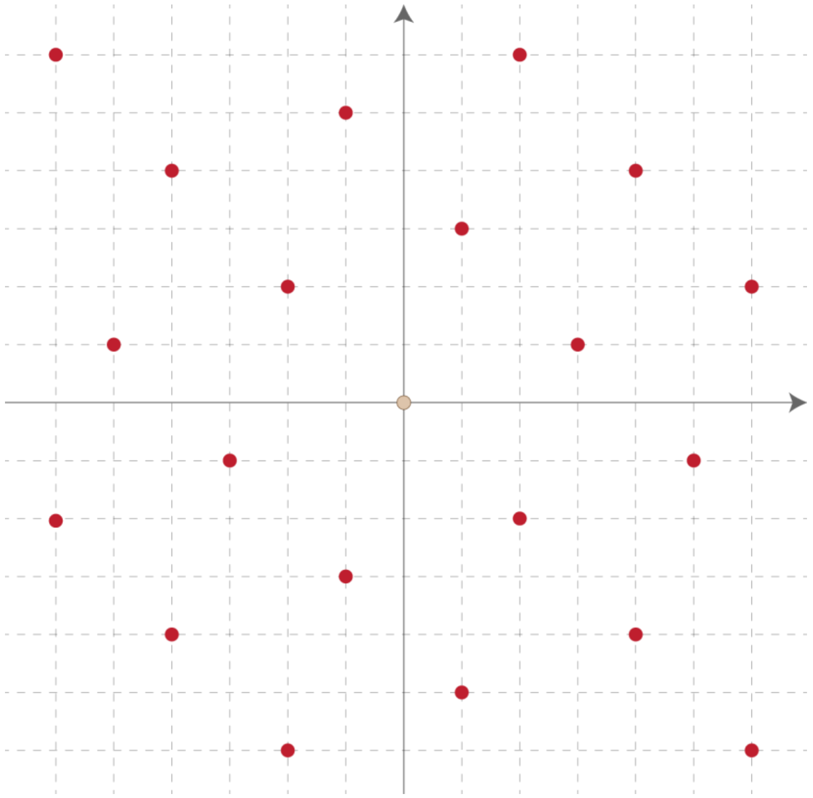
1. An $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{0}$ or
2. a collision, i.e. $\mathbf{x} \neq \mathbf{y}$ s.t. $C(\mathbf{x}) = C(\mathbf{y})$.

MINKOWSKI IN PPP – PROOF



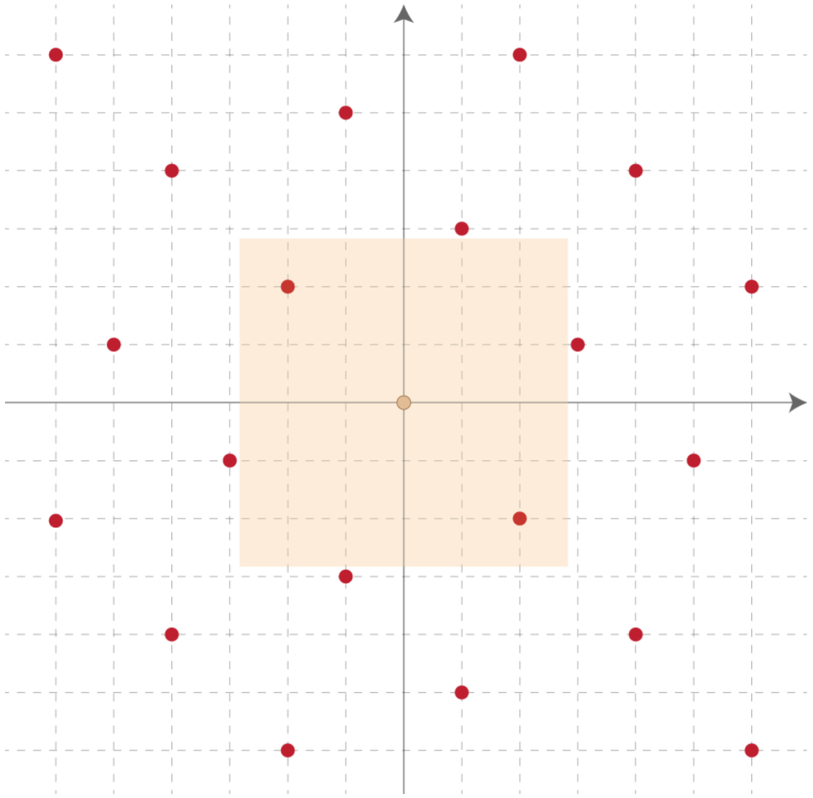
MINKOWSKI IN PPP – PROOF

$$\|\mathbf{x}\|_\infty \leq \det^{1/2}(\mathcal{L}) = \sqrt{8}$$

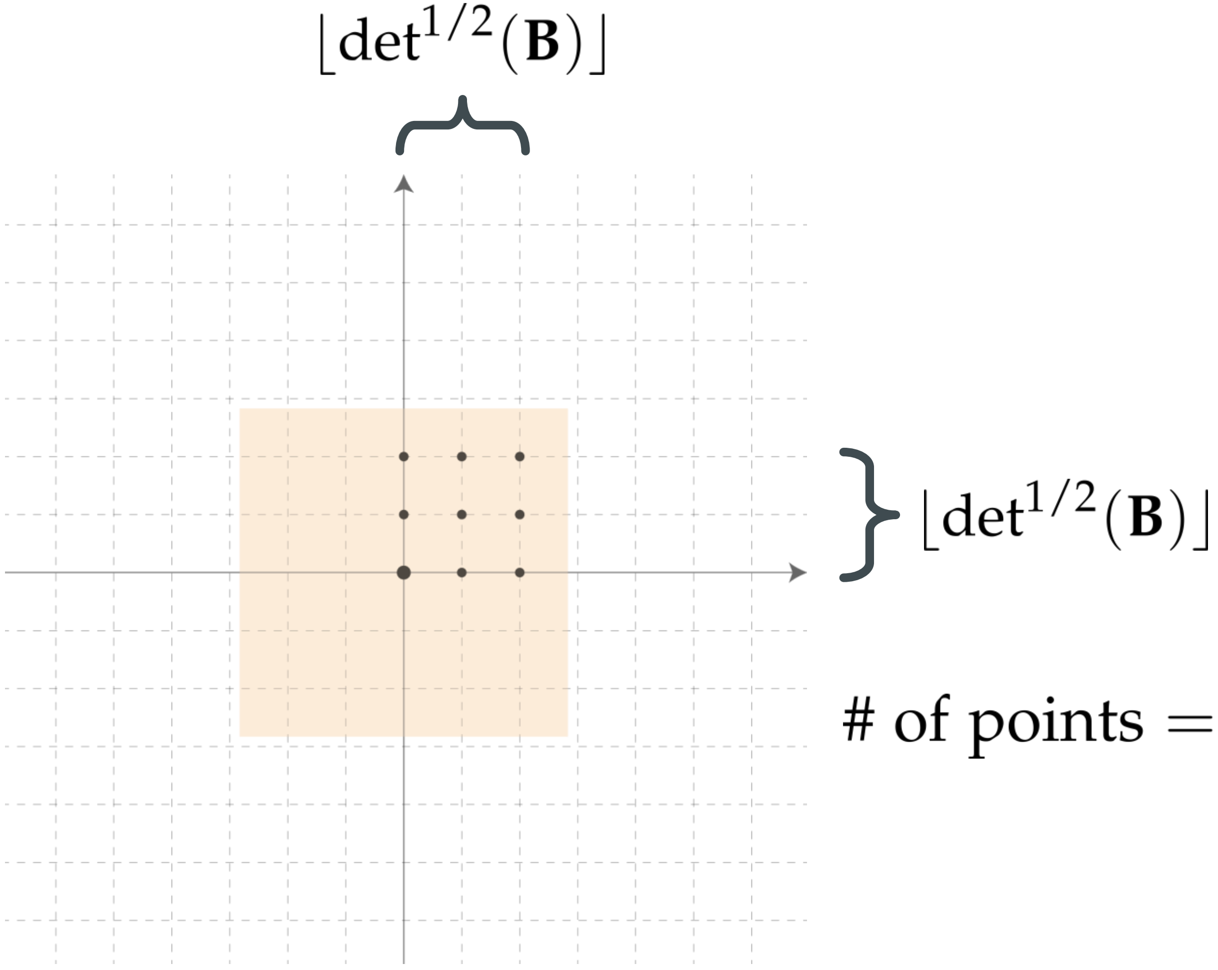


MINKOWSKI IN PPP – PROOF

$$\|\mathbf{x}\|_\infty \leq \det^{1/2}(\mathcal{L}) = \sqrt{8}$$



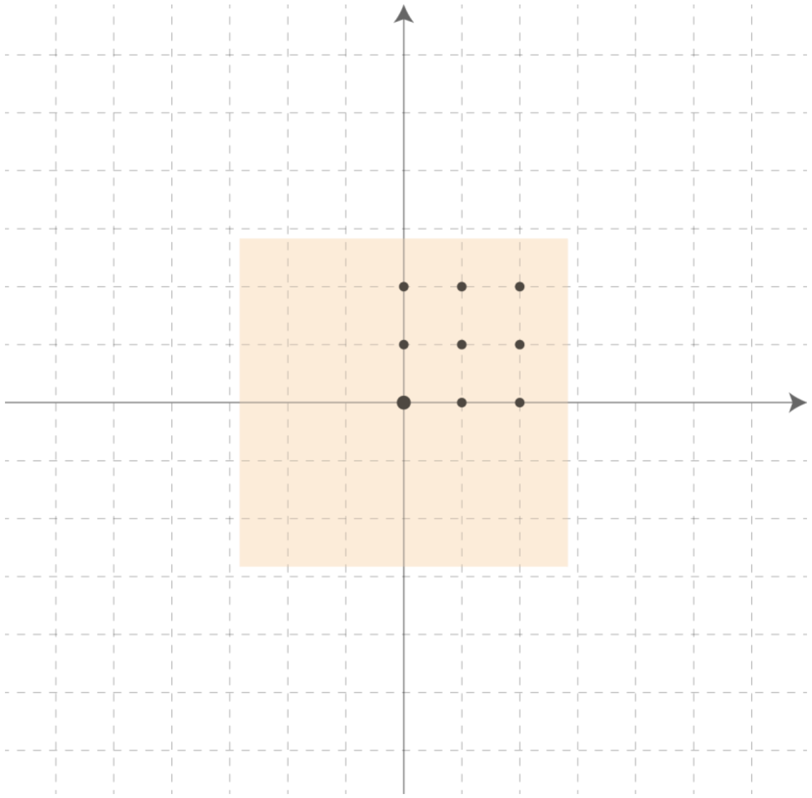
MINKOWSKI IN PPP – PROOF

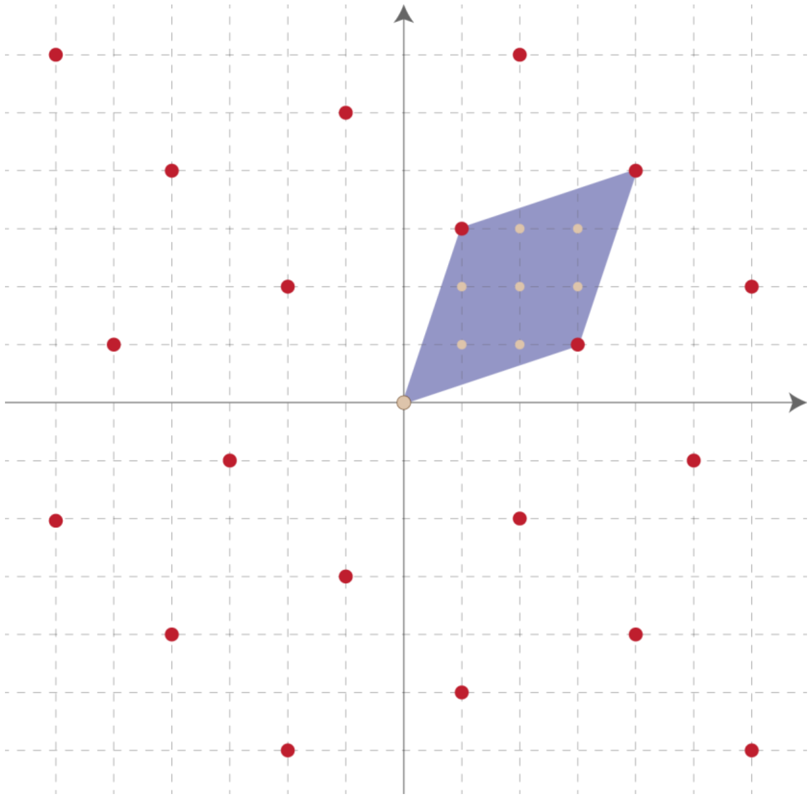


$\#$ of points $= 9$

MINKOWSKI IN PPP – PROOF

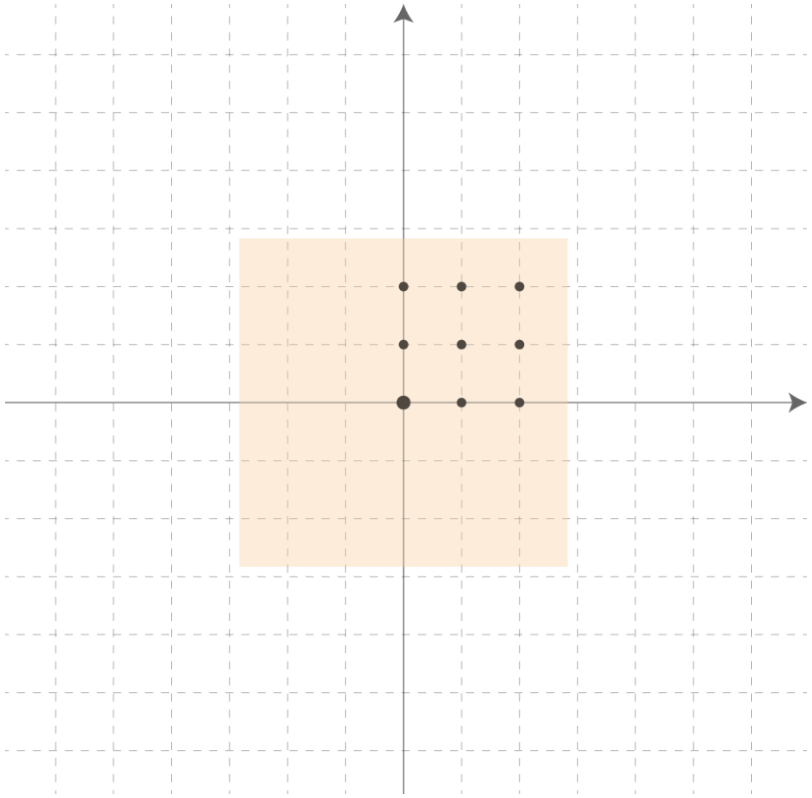
$$\text{\# of integer points in } P(\mathbf{B}) = |\det(\mathbf{B})| = 8$$



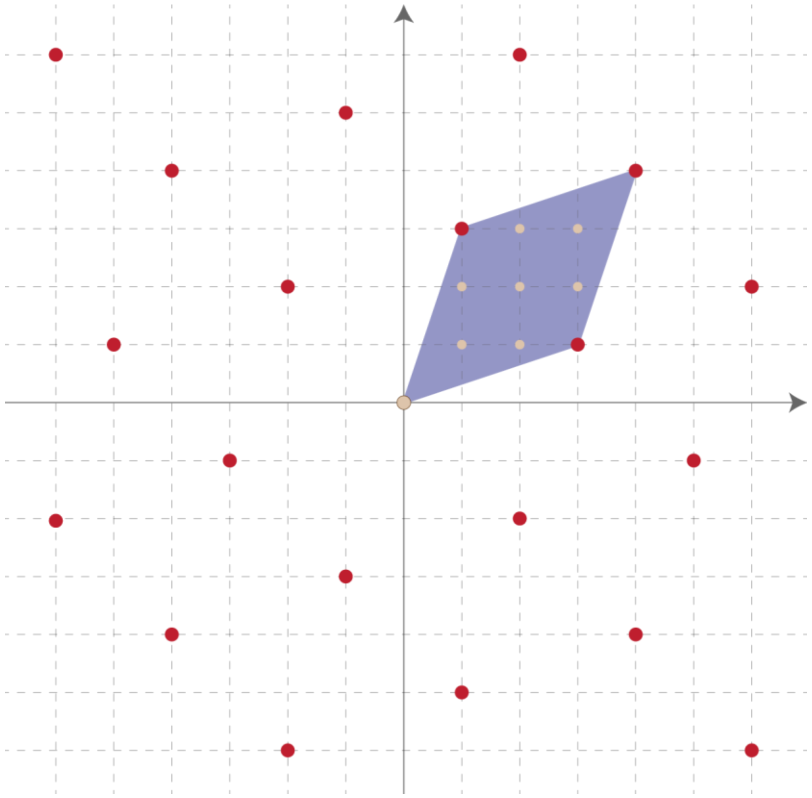


MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } P(\mathbf{B}) = |\det(\mathbf{B})| = 8$$



$(\text{mod } P(\mathbf{B}))$



POLYNOMIAL PIGEONHOLE PRINCIPLE

PPP:

Given a circuit $C : \{0,1\}^n \to \{0,1\}^n$. Find:

1. An $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{0}$ or
2. a collision, i.e. $\mathbf{x} \neq \mathbf{y}$ s.t. $C(\mathbf{x}) = C(\mathbf{y})$.

POLYNOMIAL PIGEONHOLE PRINCIPLE

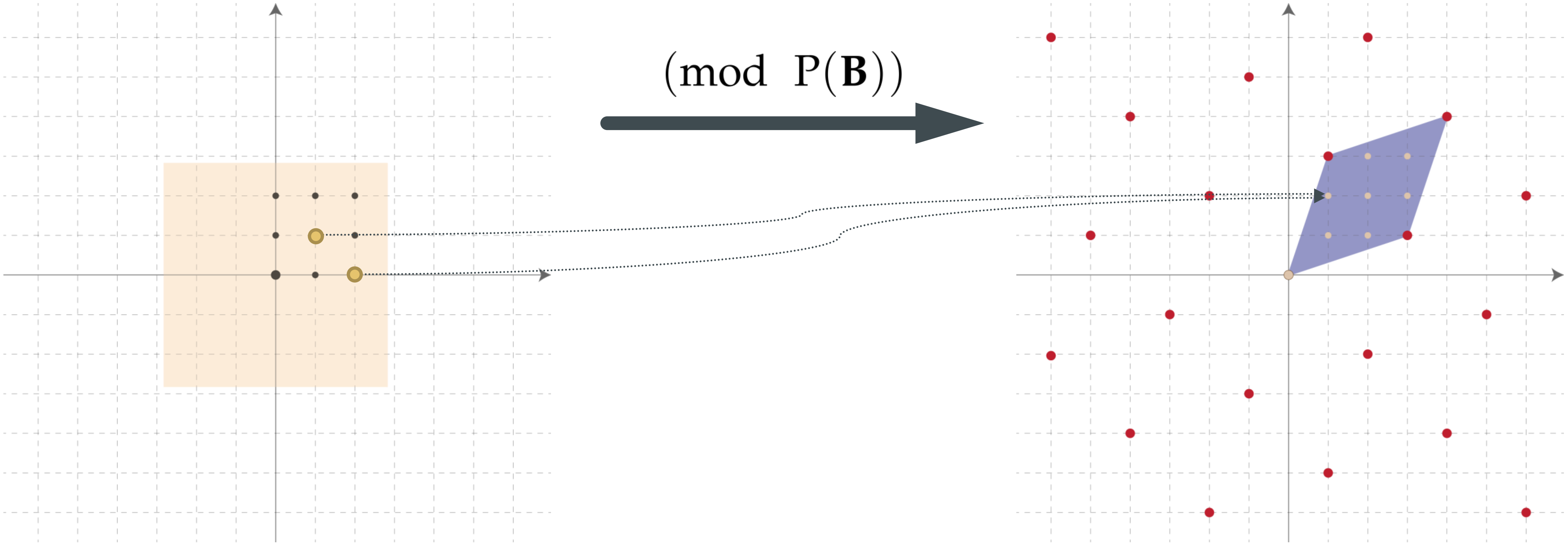
PPP:

Given a circuit $C : \{0,1\}^n \to \{0,1\}^n$. Find:

1. An $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{0}$ or
2. a collision, i.e. $\mathbf{x} \neq \mathbf{y}$ s.t. $C(\mathbf{x}) = C(\mathbf{y})$.

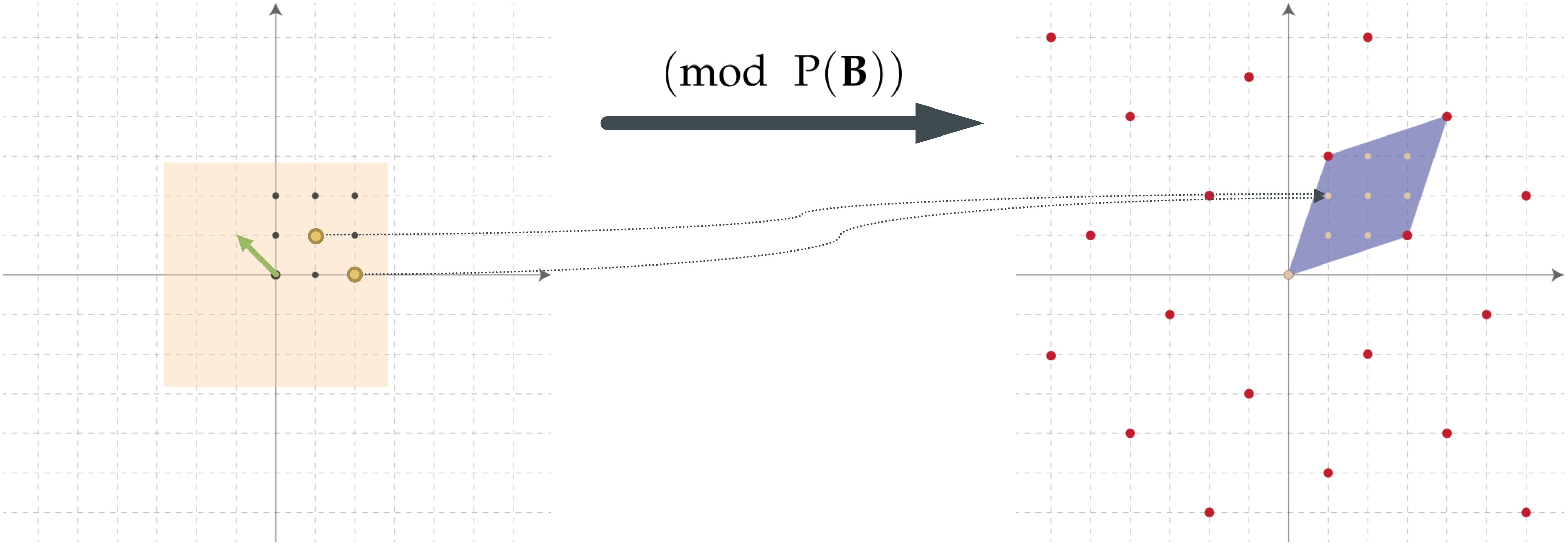
MINKOWSKI IN PPP – PROOF

$$\# \text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})| = 8$$



MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})| = 8$$



POLYNOMIAL PIGEONHOLE PRINCIPLE

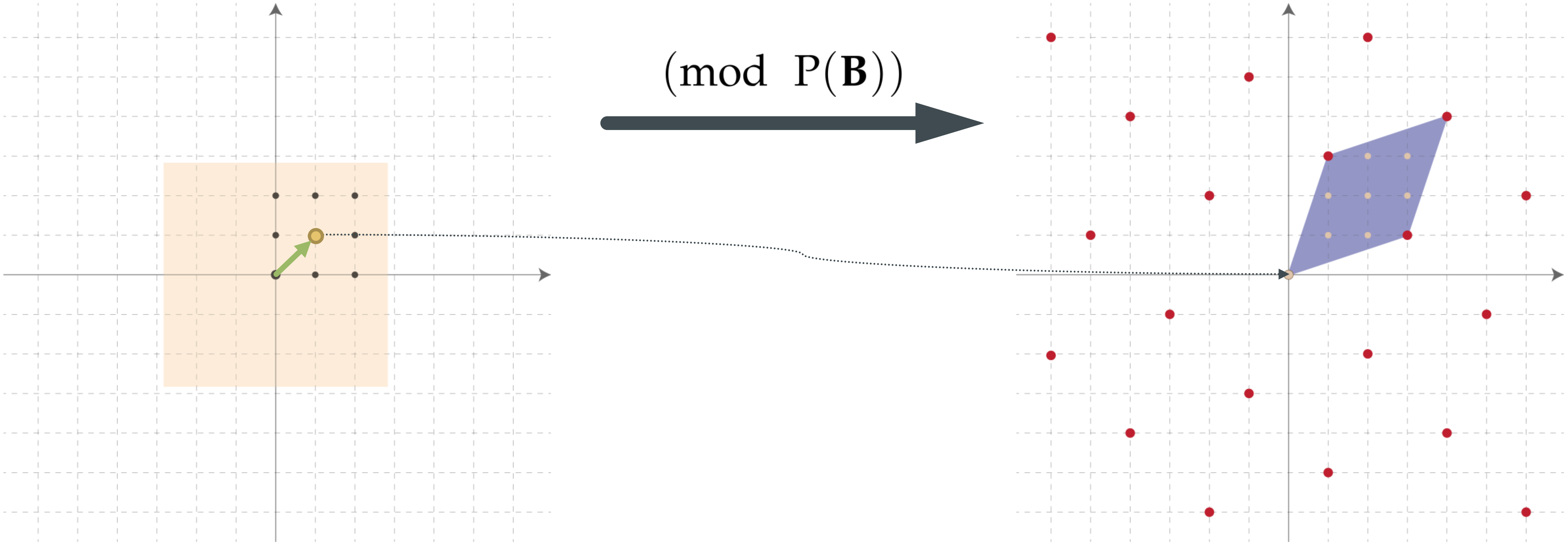
PPP:

Given a circuit $C : \{0,1\}^n \to \{0,1\}^n$. Find:

1. An $\mathbf{x}$ s.t. $\mathrm{C}(\mathbf{x}) = \mathbf{0}$ or
2. a collision, i.e. $\mathbf{x} \neq \mathbf{y}$ s.t. $\mathrm{C}(\mathbf{x}) = \mathrm{C}(\mathbf{y})$.

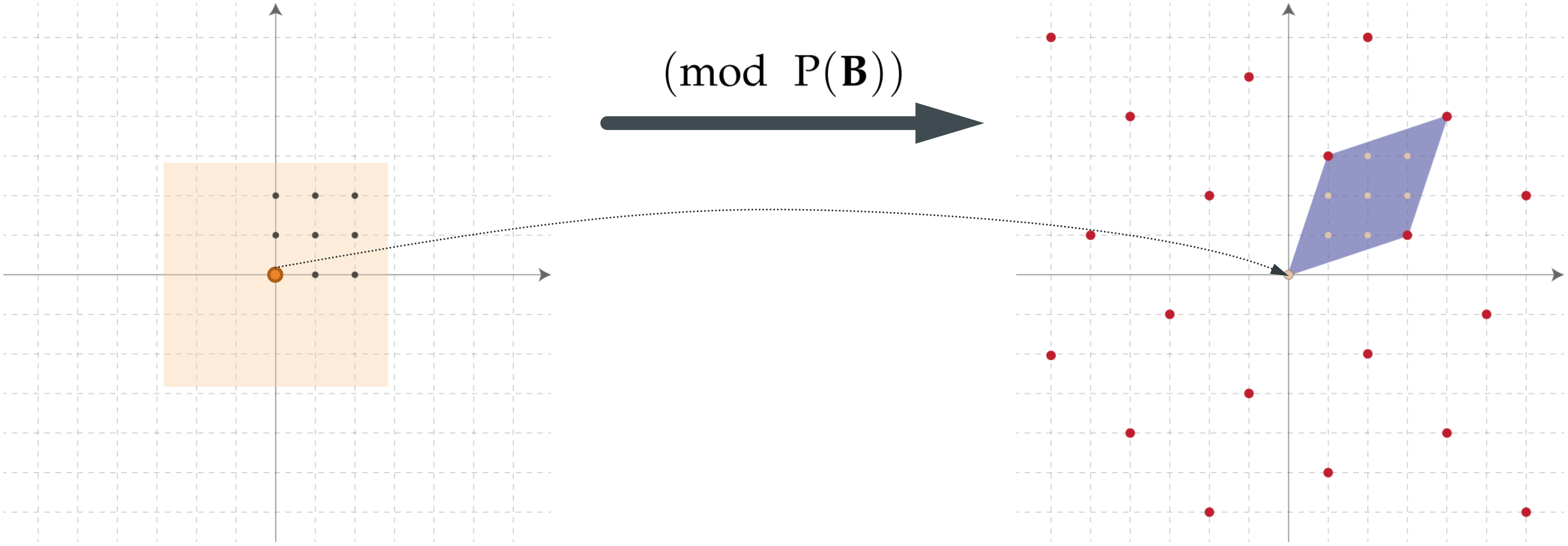
MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})| = 8$$



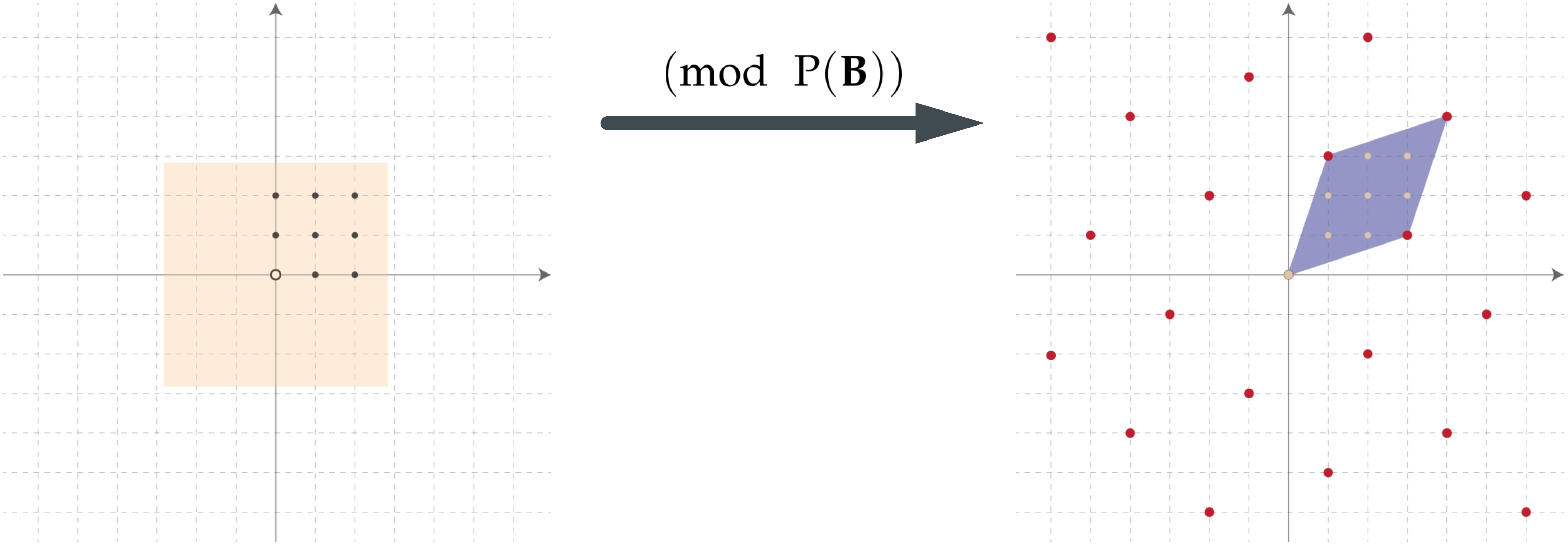
MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } P(\mathbf{B}) = |\det(\mathbf{B})| = 8$$



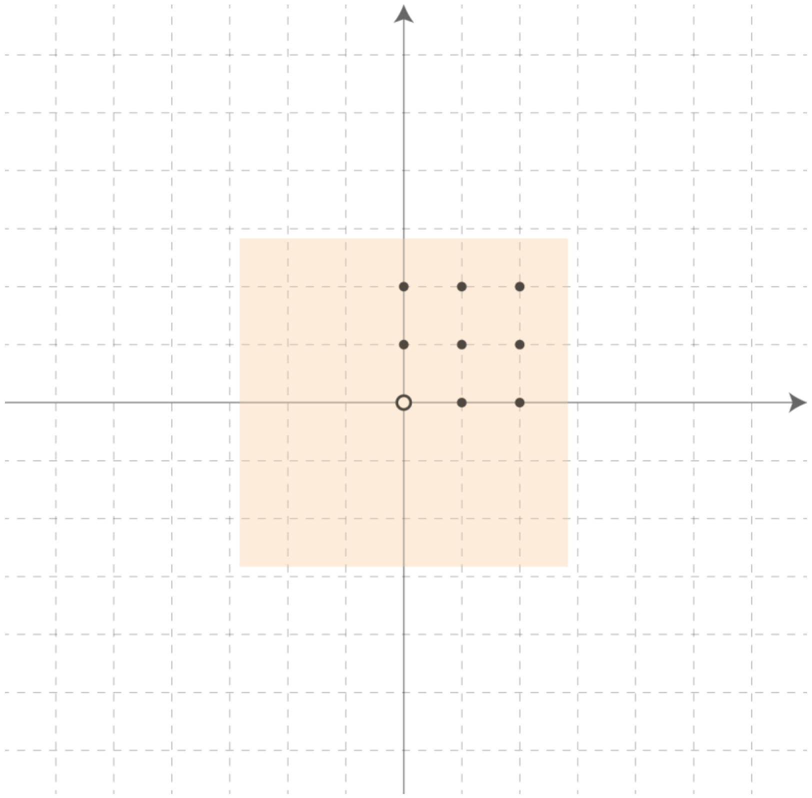
MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})| = 8$$



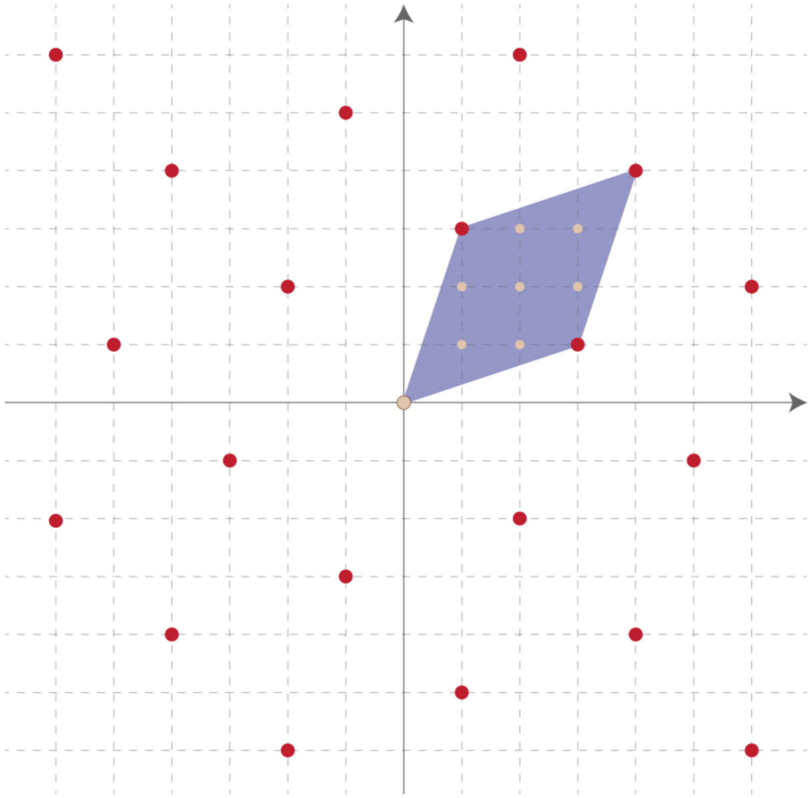
MINKOWSKI IN PPP – PROOF

$$\# \text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})| = 8$$



$$(\bmod \ \mathrm{P}(\mathbf{B}))$$

$$K = \# \text{ of points} = 8$$



POLYNOMIAL PIGEONHOLE PRINCIPLE

PPP:

Given a circuit $C : \{0,1\}^n \to \{0,1\}^n$. Find:

1. An $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{0}$ or
2. a collision, i.e. $\mathbf{x} \neq \mathbf{y}$ s.t. $C(\mathbf{x}) = C(\mathbf{y})$.

POLYNOMIAL PIGEONHOLE PRINCIPLE

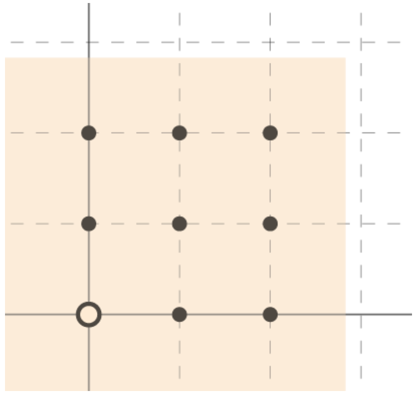
PPP:

Given a circuit $\boxed{C : [K] \to [K]}$. Find:

1. An $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{0}$ or
2. a collision, i.e. $\mathbf{x} \neq \mathbf{y}$ s.t. $C(\mathbf{x}) = C(\mathbf{y})$.

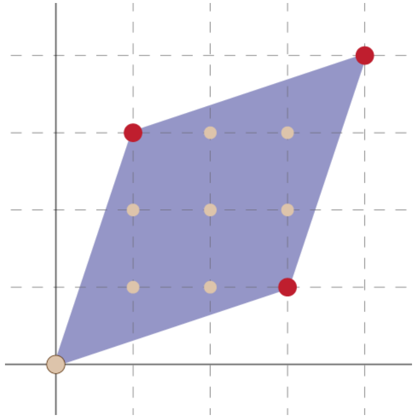
MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})|$$



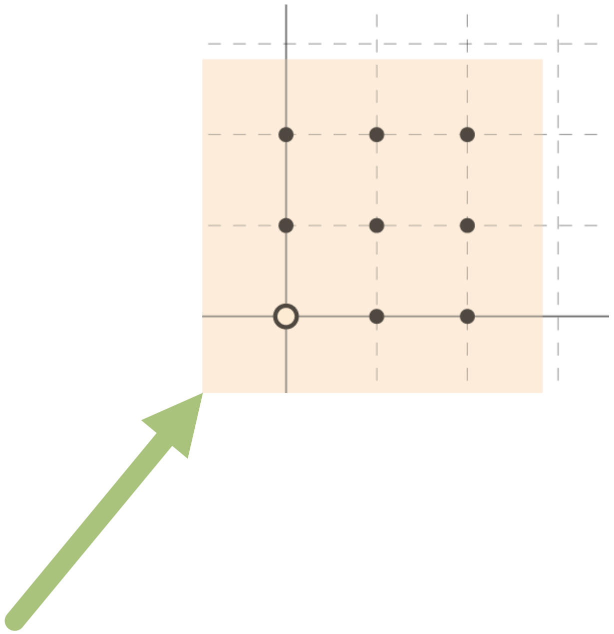
$$(\bmod\ \ \mathrm{P}(\mathbf{B}))$$

$$K = \#\text{ of points} = 8$$



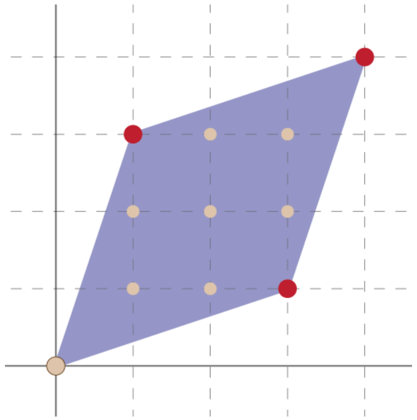
MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})|$$



$$(\mathrm{mod}\ \ \mathrm{P}(\mathbf{B}))$$

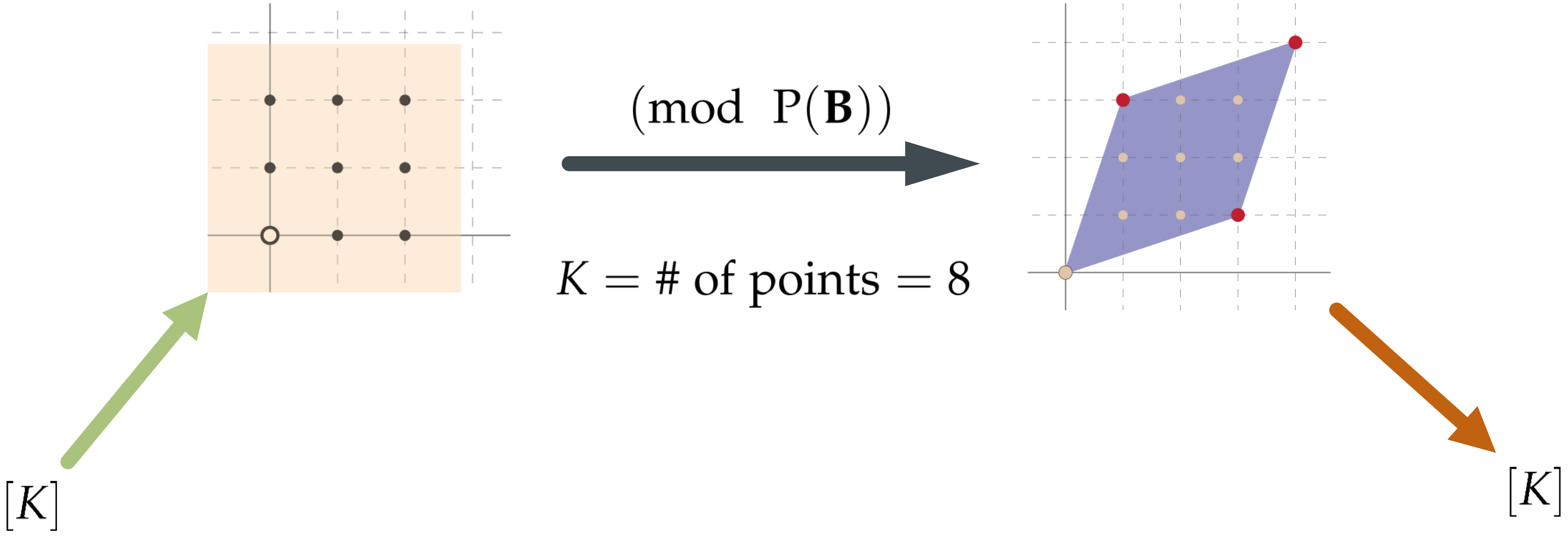
$$K = \#\text{ of points} = 8$$



$[K]$

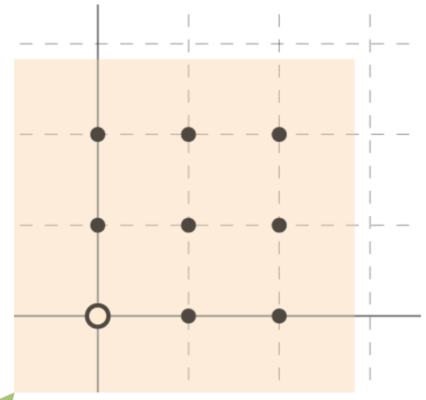
MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})|$$



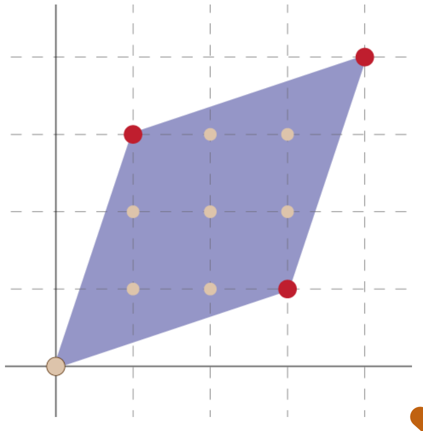
MINKOWSKI IN PPP – PROOF

$$\#\text{ of integer points in } \mathrm{P}(\mathbf{B}) = |\det(\mathbf{B})|$$



$(\mathrm{mod}\ \ \mathrm{P}(\mathbf{B}))$

$K = \#\text{ of points} = 8$



(Smith Normal Form of **B**)

$[K]$

$[K]$

SHORT INTEGER SOLUTION (SIS) PROBLEM

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)r$.

OUTPUT: $\mathbf{x}$ s.t. $\|\mathbf{x}\| \leq \beta$, $\mathbf{A}\mathbf{x} = \mathbf{0} \pmod q$

$\mathbf{x} \neq \mathbf{0}$

SHORT INTEGER SOLUTION (SIS) PROBLEM

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q) r$.

OUTPUT: $\mathbf{x}$ s.t. $\|\mathbf{x}\|_\infty \leq 1$, $\mathbf{A}\mathbf{x} = \mathbf{0} \pmod{q}$

$\mathbf{x} \neq \mathbf{0}$

SHORT INTEGER SOLUTION (SIS) PROBLEM

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q) r$.

OUTPUT: $\mathbf{x} \neq \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod{q}$

SHORT INTEGER SOLUTION (SIS) PROBLEM

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q) r$.

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod{q}$

Is this problem total?

SHORT INTEGER SOLUTION (SIS) PROBLEM

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q) r$.

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

domain size is 2^m

SHORT INTEGER SOLUTION (SIS) PROBLEM

INPUT: **A** $\in \mathbb{Z}_q^{r \times m}$, with $m > \log(q) r$.

OUTPUT: **x** **y** $\in \{0,1\}^m$ s.t. **A** **x** $=$ **A** **y** $\pmod{q}$

image size is q^r

SHORT INTEGER SOLUTION (SIS) PROBLEM

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q) r$.

OUTPUT: $\mathbf{x}, \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod{q}$

SHORT INTEGER SOLUTION (SIS) PROBLEM

The problem is total!

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $2^m > q^r$.

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod{q}$

SHORT INTEGER SOLUTION (SIS) PROBLEM

The problem is total!

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $2^m > q^r$.

OUTPUT: $\mathbf{x}, \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod{q}$

SHORT INTEGER SOLUTION (SIS) PROBLEM

The problem is in PWPP!

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $2^m > q^r$.

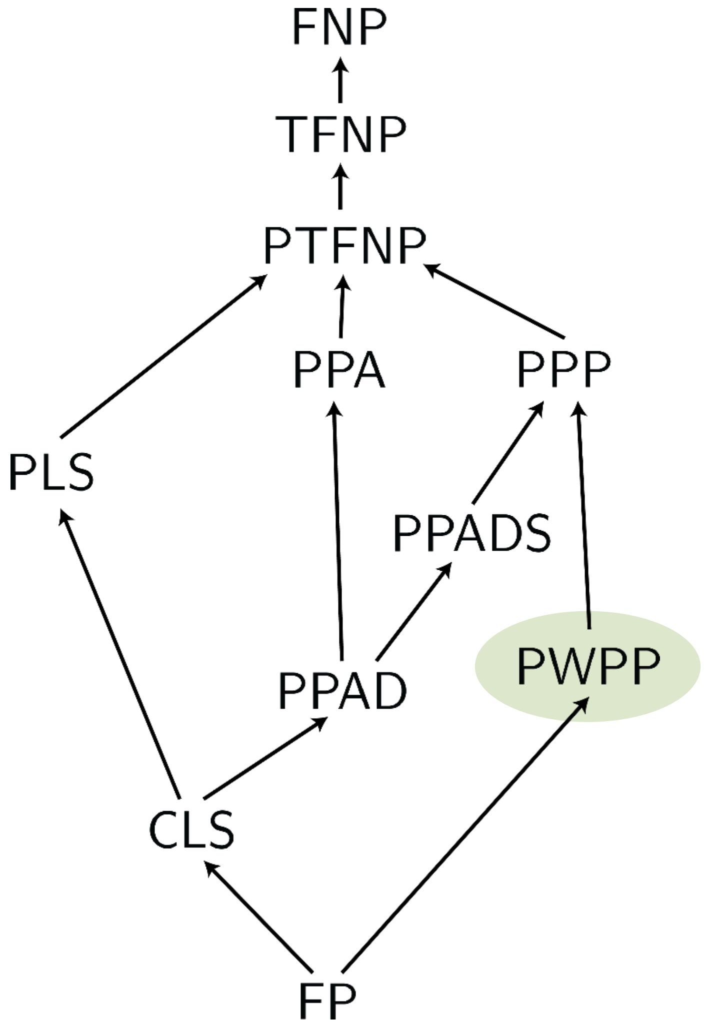
OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod{q}$

$$\mathcal{C}(\boldsymbol{x}) = \boldsymbol{A}\boldsymbol{x} \pmod{q}$$

COMPLEXITY OF TOTAL SEARCH PROBLEMS

Theorem [S Zampetakis Zirdelis 18]:
The first natural complete problems for PPP and PWPP

Constrained-SIS is PWPP-complete



PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: **A** $\in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r + d)$ **G** $\in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r + d)$ $\quad \mathbf{G} \in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r + d)$ $\quad \mathbf{G} \in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

$$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$$

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r + d)$ $\quad$ $\mathbf{G} \in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

$$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$$

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r + d)$ $\quad \mathbf{G} \in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

Input: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r + d)$ $\quad \mathbf{G} \in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

Output: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

$$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$$

Why is this problem total?

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r\times m}$, with $m > \log(q)(r+d)$ $\mathbf{G} \in \mathbb{Z}_q^{d\times m}$, and *binary invertible*

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

$$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$$

Why is this problem total?

BINARY INVERTIBLE MATRIX

BINARY INVERTIBLE MATRIX

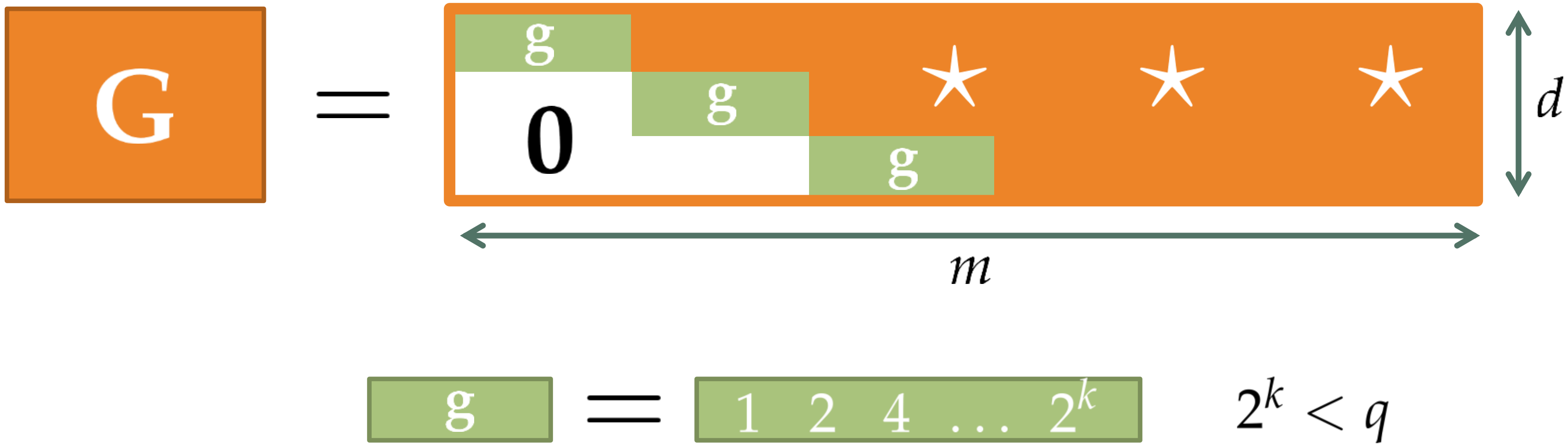
BINARY INVERTIBLE MATRIX

BINARY INVERTIBLE MATRIX

$$g = \begin{bmatrix} 1 & 2 & 4 & \dots & 2^k \end{bmatrix} \qquad 2^k < q$$

e.g. for m = 10, q = 8

BINARY INVERTIBLE MATRIX



e.g. for m = 10, q = 8

$$\mathbf{G} = \begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix}$$

BINARY INVERTIBLE MATRIX

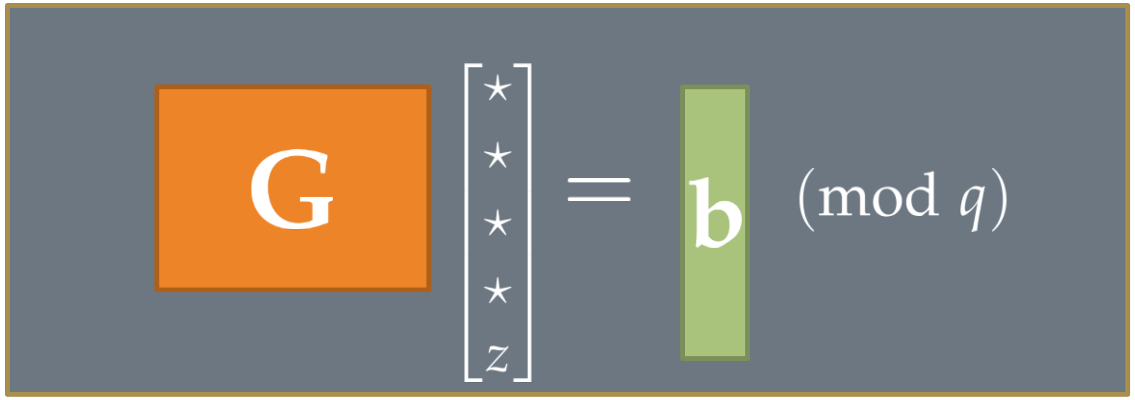
$$\mathbf{g} = \begin{bmatrix} 1 & 2 & 4 & \dots & 2^k \end{bmatrix} \qquad 2^k < q$$

e.g. for m = 10, q = 8

$$\mathbf{G} = \begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix}$$

BINARY INVERTIBLE MATRIX

BINARY INVERTIBLE MATRIX



Lemma
For any $\mathbf{b}$ and binary $\mathbf{z} \in \{0,1\}^{m-d\log(q)}$, we can efficiently compute a binary solution of the form $\mathbf{x} = [\star \ \ \star \cdots \star \ \ \mathbf{z}]$ for the equation $\mathbf{G}\mathbf{x} = \mathbf{b} \pmod q$.

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ z \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \pmod 8$$

$\leftrightarrow$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ x_7 \\ x_8 \\ x_9 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ x_7 \\ x_8 \\ x_9 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ x_7 \\ x_8 \\ x_9 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

$$x_7 + 2x_8 + 4x_9 = 1 \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ \star \\ \star \\ \star \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

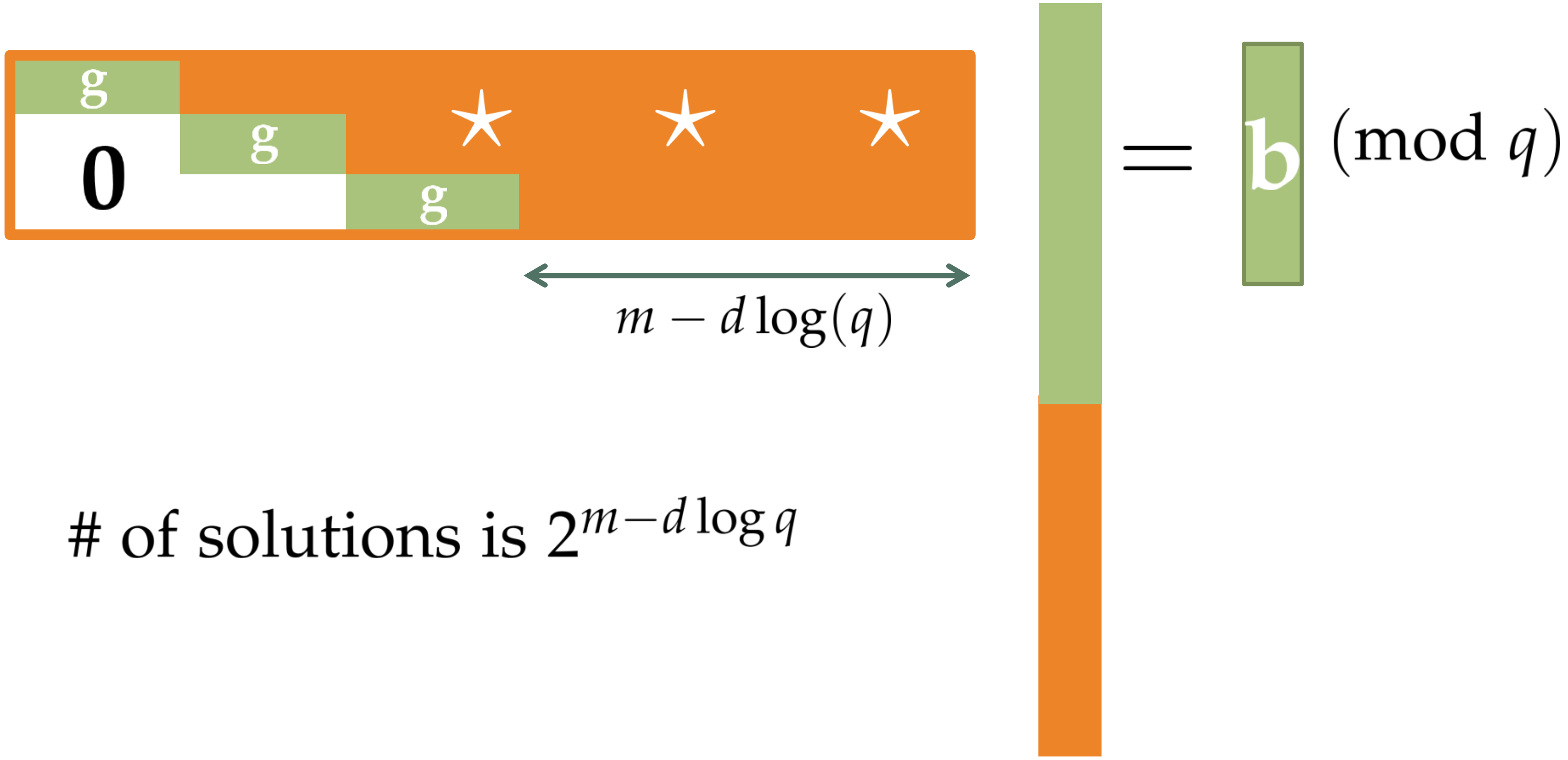
$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} \star \\ \star \\ \star \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

BINARY INVERTIBLE MATRIX

Example

$$\begin{bmatrix} 1 & 2 & 4 & 3 & 0 & 6 & 5 & 6 & 2 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 & 1 & 0 & 3 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 4 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 2 \\ 1 \end{bmatrix} \pmod 8$$

CONSTRAINED SIS IS TOTAL



# of solutions is $2^{m-d\log q}$

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r+d)$ $\mathbf{G} \in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ domain size is $2^{m-d\log(q)}$ $\mathbf{y} \pmod q$

$$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$$

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: **A** $\in \mathbb{Z}_q^{r\times m}$, with $m > \log(q)(r + d)$ **G** $\in \mathbb{Z}_q^{d\times m}$, and *binary invertible*

OUTPUT: **x** **y** $\in \{0,1\}^m$ s.t. **A** **x** $=$ **A** **y** $\pmod q$

G **x** $=$ **G** **y** $= \mathbf{0} \pmod q$

image size is q^r

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

The problem is total!

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, $\mathbf{G} \in \mathbb{Z}_q^{d \times m}$,

with $m > \log(q)(r + d)$ and *binary invertible*

OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

$$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$$

CONSTRAINED SIS IN PWPP

The problem is in PWPP!

INPUT: **A** $\in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r+d)$ **G** $\in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

$\mathcal{C}(z) =$ Find $\boldsymbol{x}$ such that $\boldsymbol{G}\boldsymbol{x} = \boldsymbol{0} \pmod{q}$ and $\boldsymbol{x} = [\star \ \star \ \boldsymbol{z}]$ and output $\boldsymbol{A}\boldsymbol{x} \pmod{q}$.

OUT

$$\mathbf{G}\,\mathbf{x} = \mathbf{G}\,\mathbf{y} = \mathbf{0} \pmod{q}$$

PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, with $m > \log(q)(r+d)$ $\quad \mathbf{G} \in \mathbb{Z}_q^{d \times m}$, and *binary invertible*

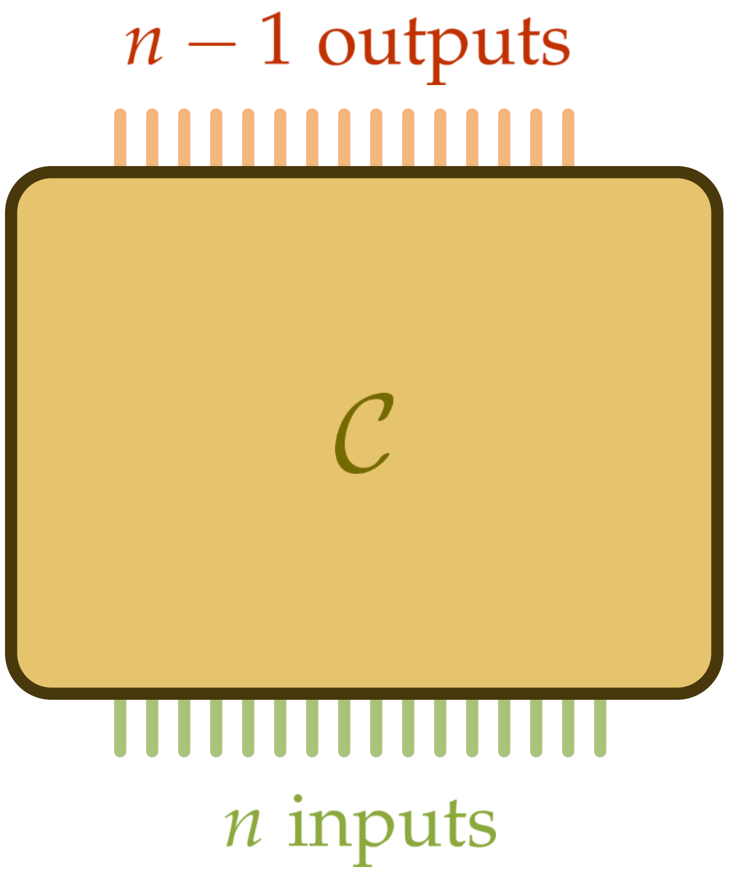
OUTPUT: $\mathbf{x}\ \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

$$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$$

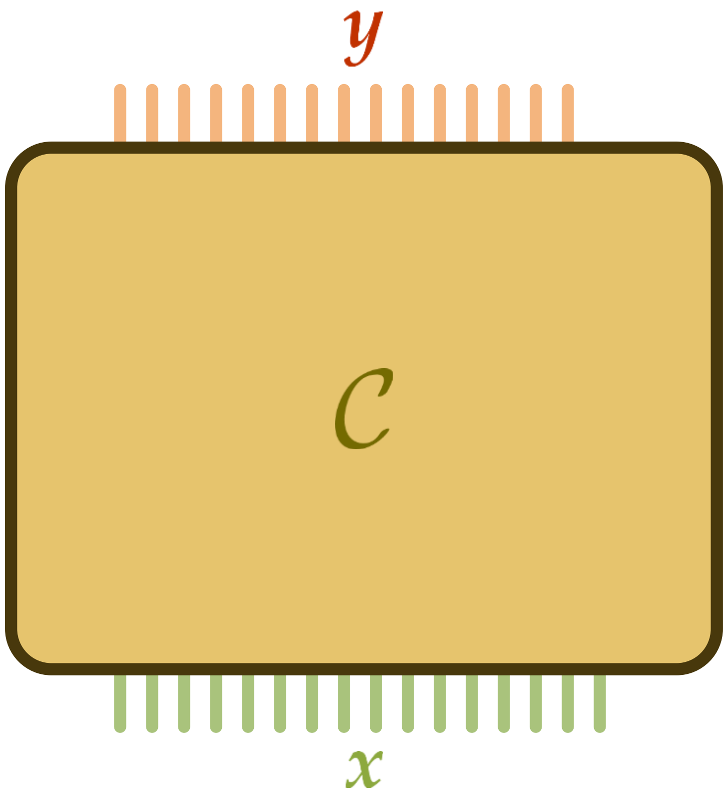
CONSTRAINED SIS IS PWPP-HARD

PWPP:
Given a circuit $C : \{0,1\}^n \to \{0,1\}^m$, with $m < n$.
Find a collision, i.e $\mathbf{x} \neq \mathbf{y}$ s.t. $C(\mathbf{x}) = C(\mathbf{y})$.

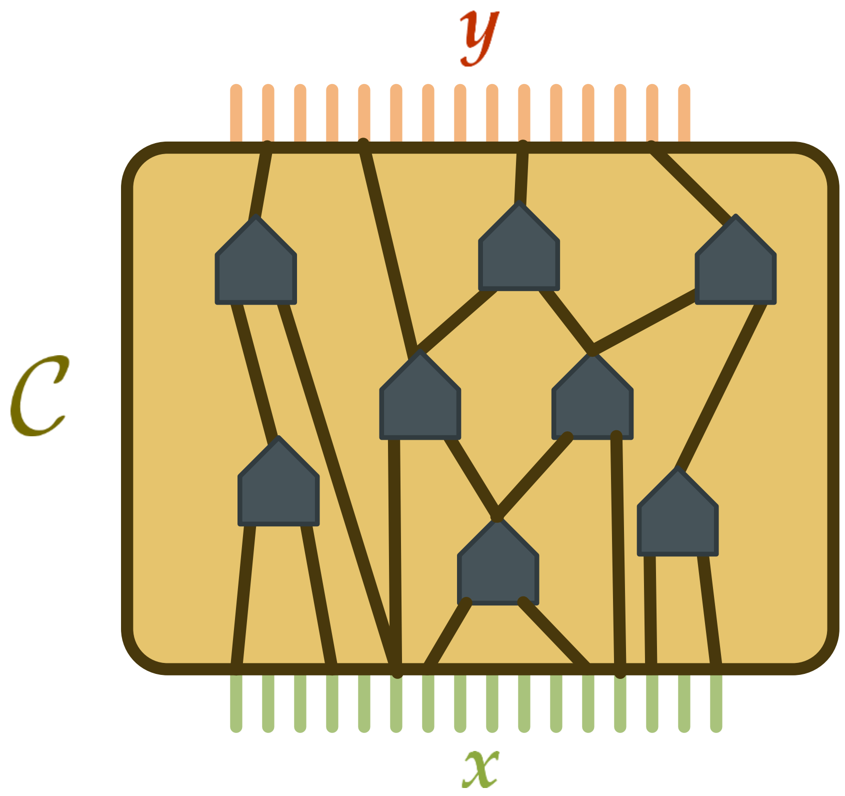
CONSTRAINED SIS IS PWPP-HARD



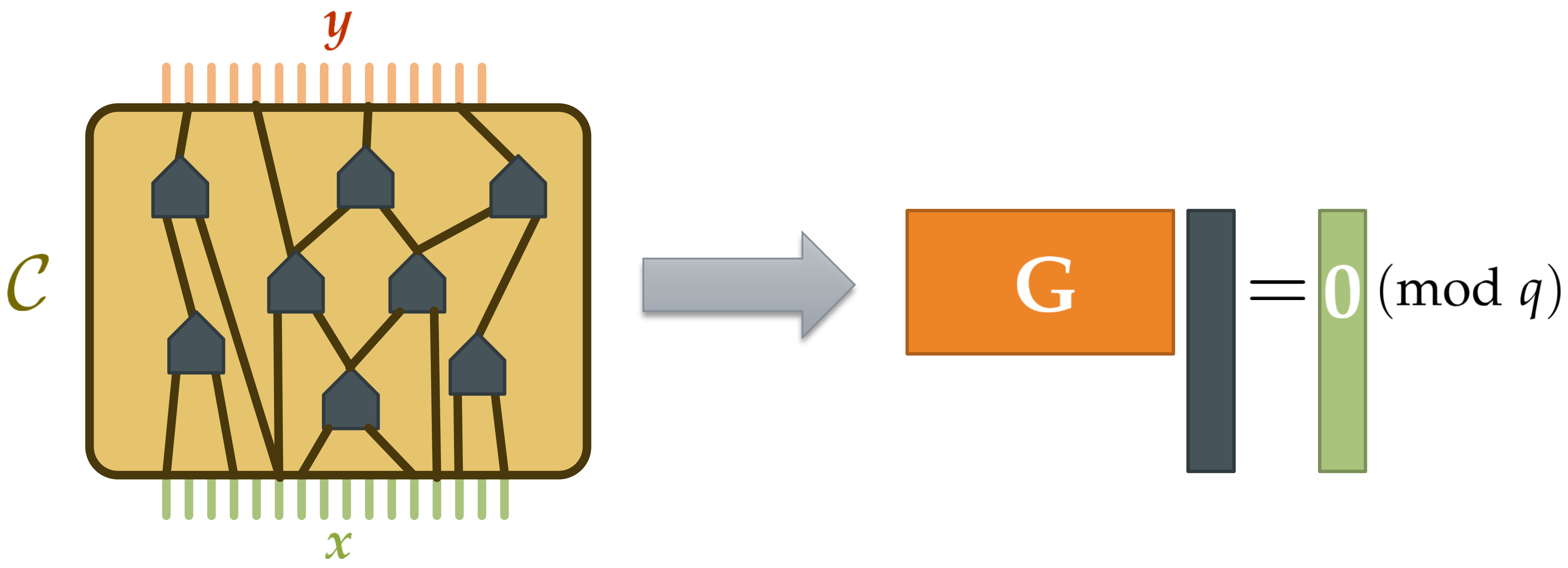
CONSTRAINED SIS IS PWPP-HARD



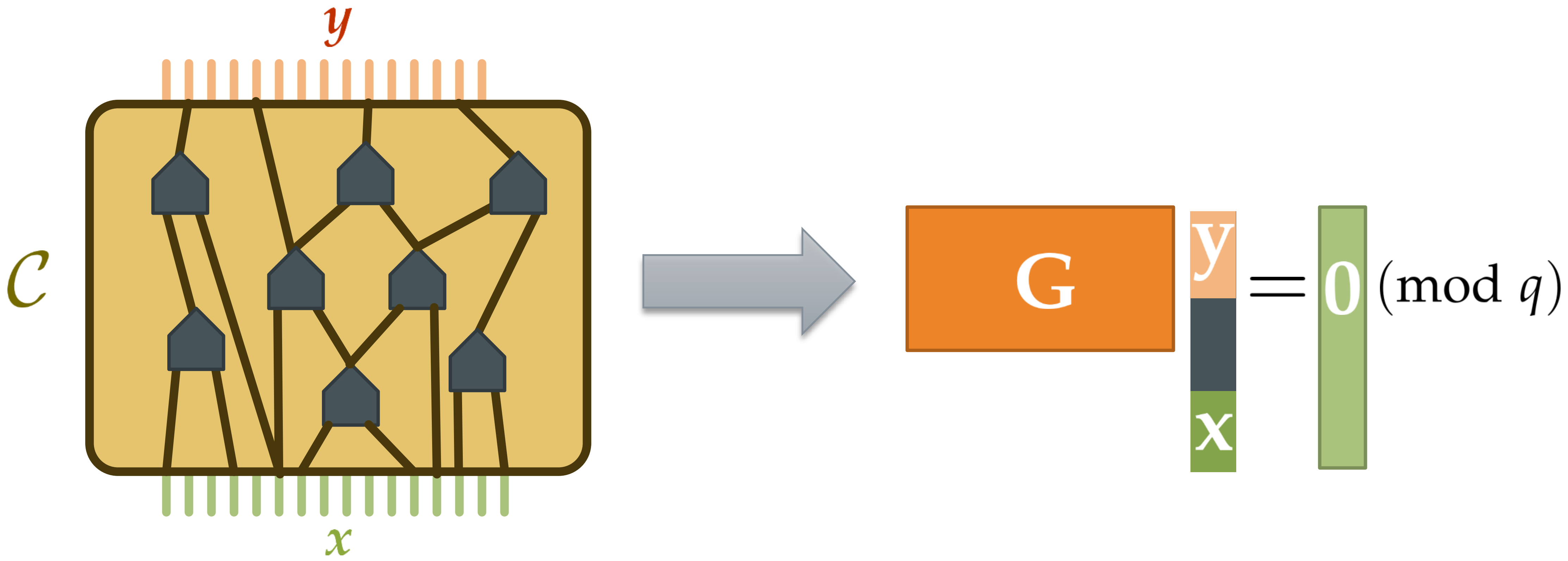
CONSTRAINED SIS IS PWPP-HARD



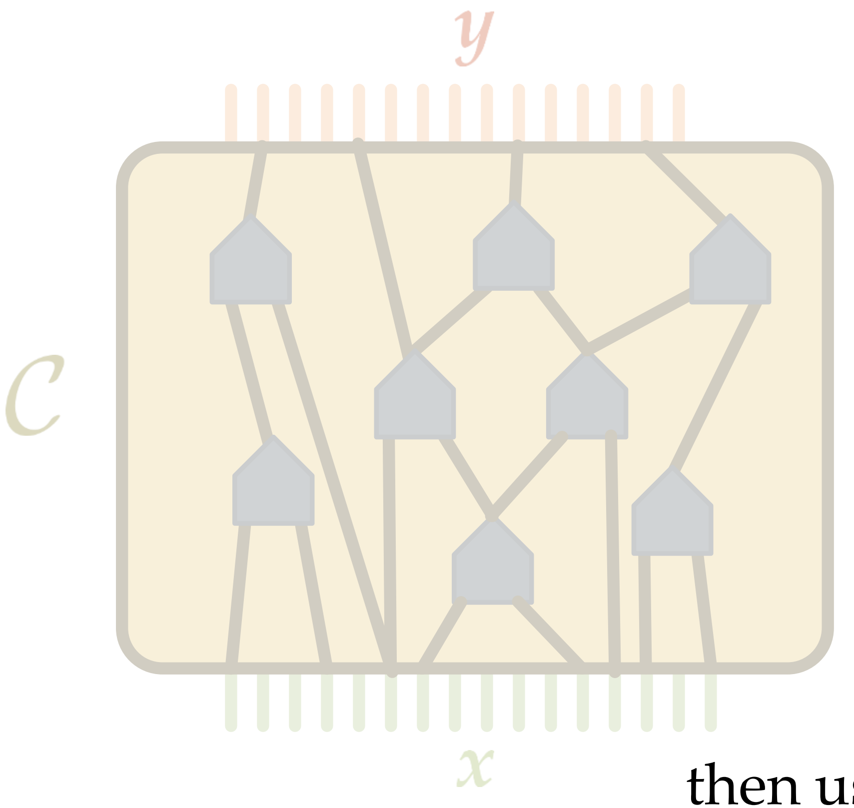
CONSTRAINED SIS IS PWPP-HARD



CONSTRAINED SIS IS PWPP-HARD

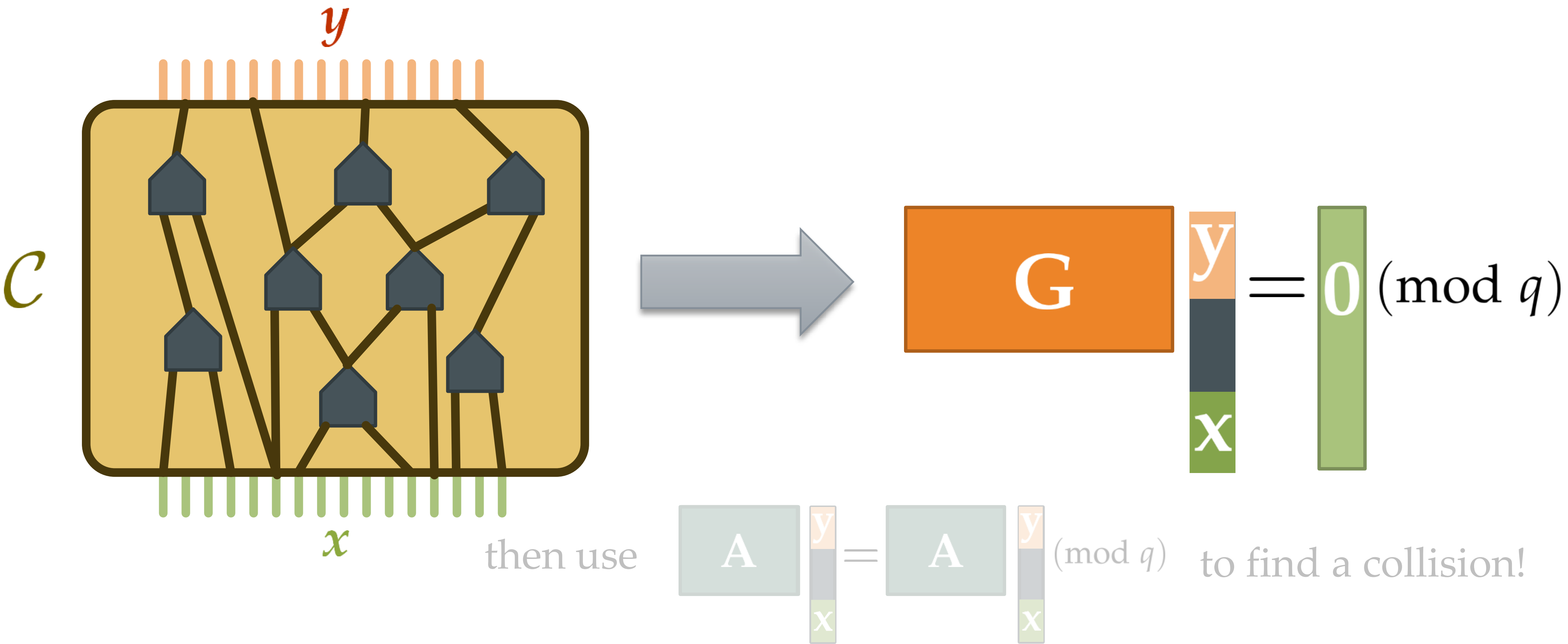


CONSTRAINED SIS IS PWPP-HARD

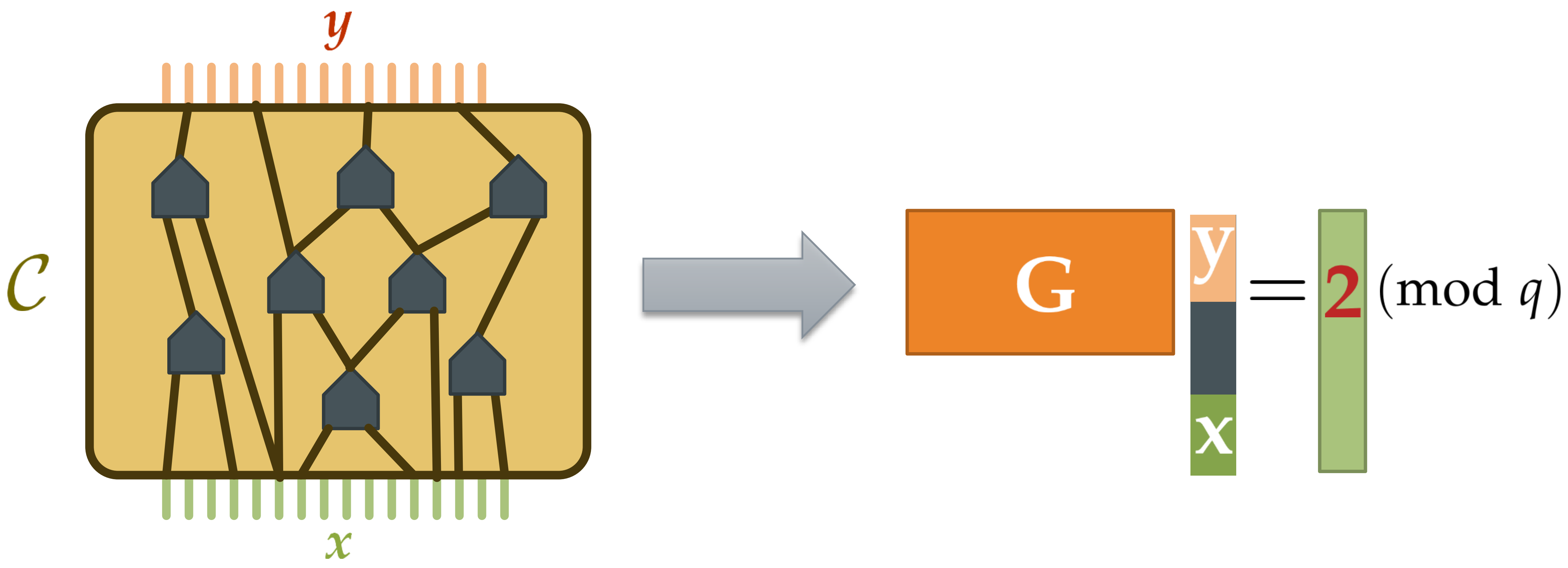


then use $\mathbf{A}\begin{bmatrix}\mathbf{y}\\ \mathbf{x}\end{bmatrix} = \mathbf{A}\begin{bmatrix}\mathbf{y}\\ \mathbf{x}\end{bmatrix} \pmod{q}$ to find a collision!

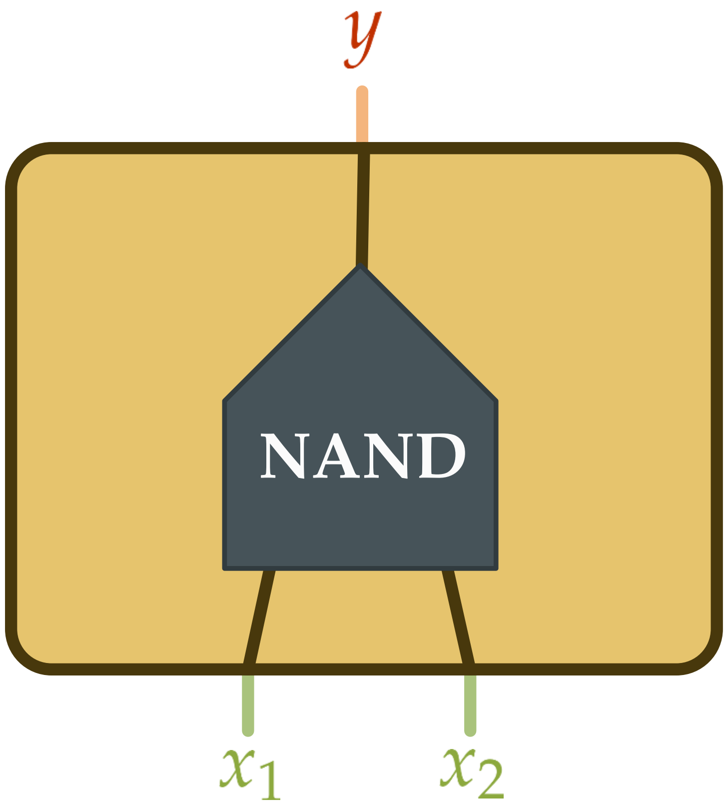
CONSTRAINED SIS IS PWPP-HARD



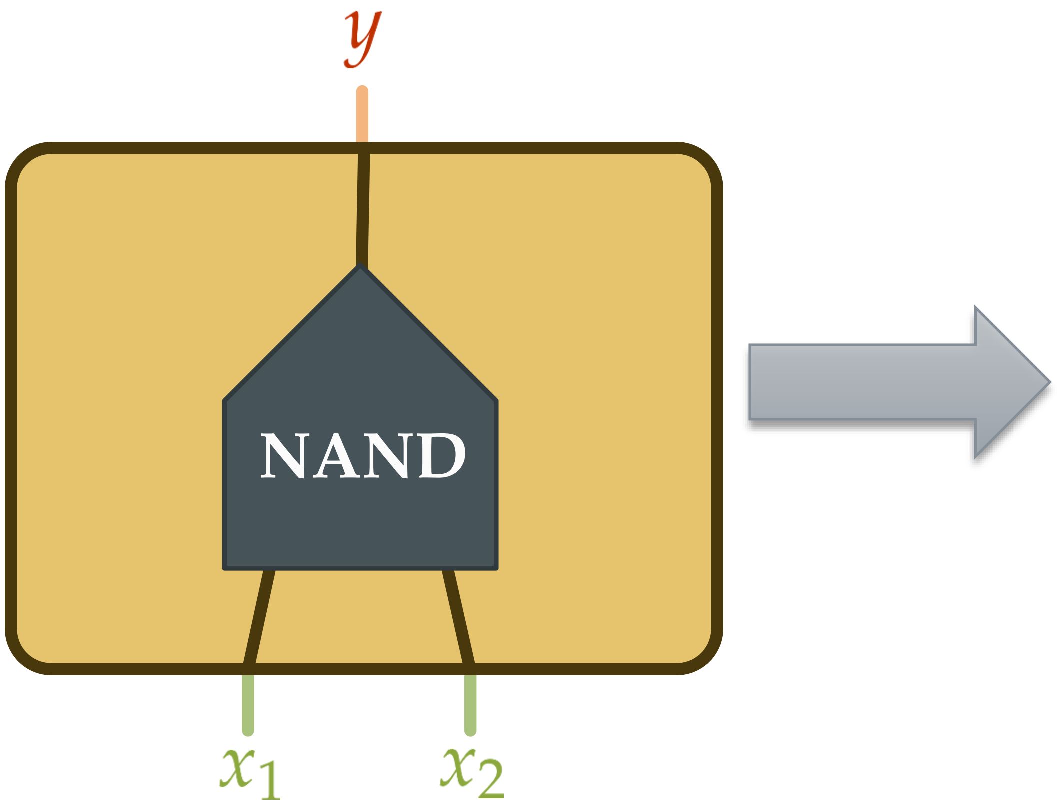
CONSTRAINED SIS IS PWPP-HARD



CONSTRAINED SIS IS PWPP-HARD



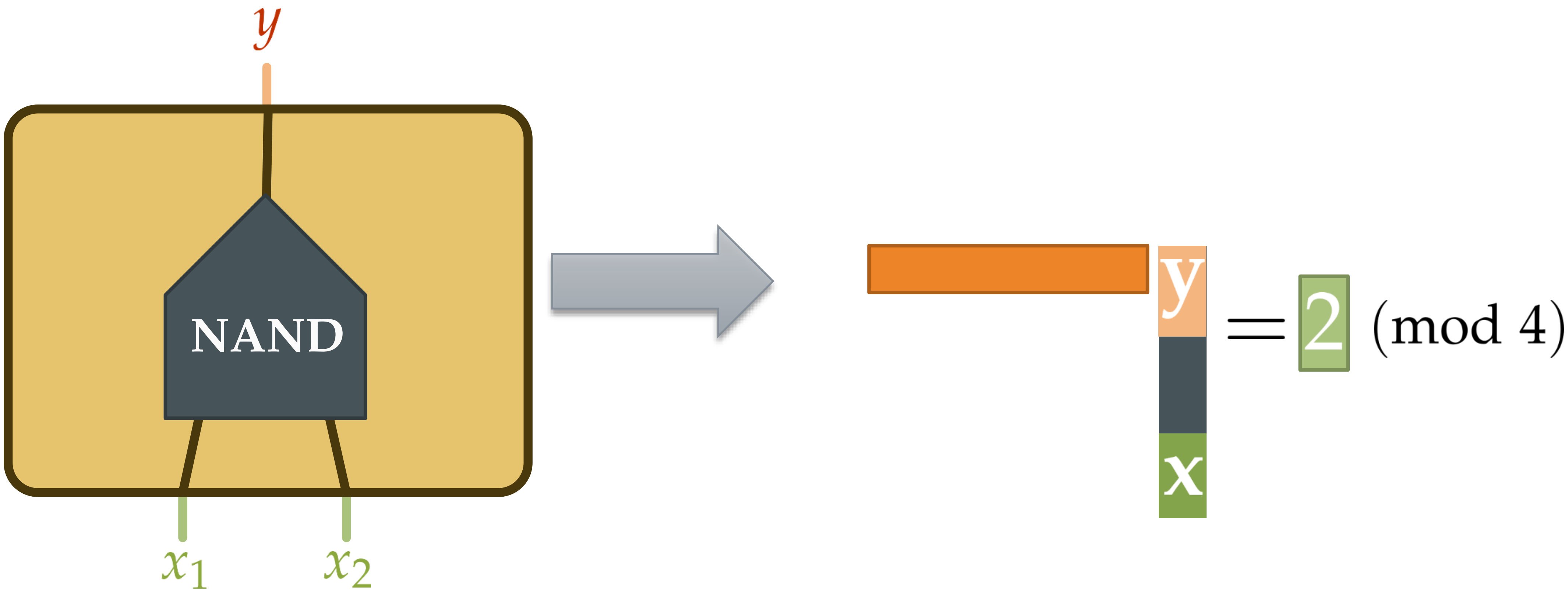
CONSTRAINED SIS IS PWPP-HARD



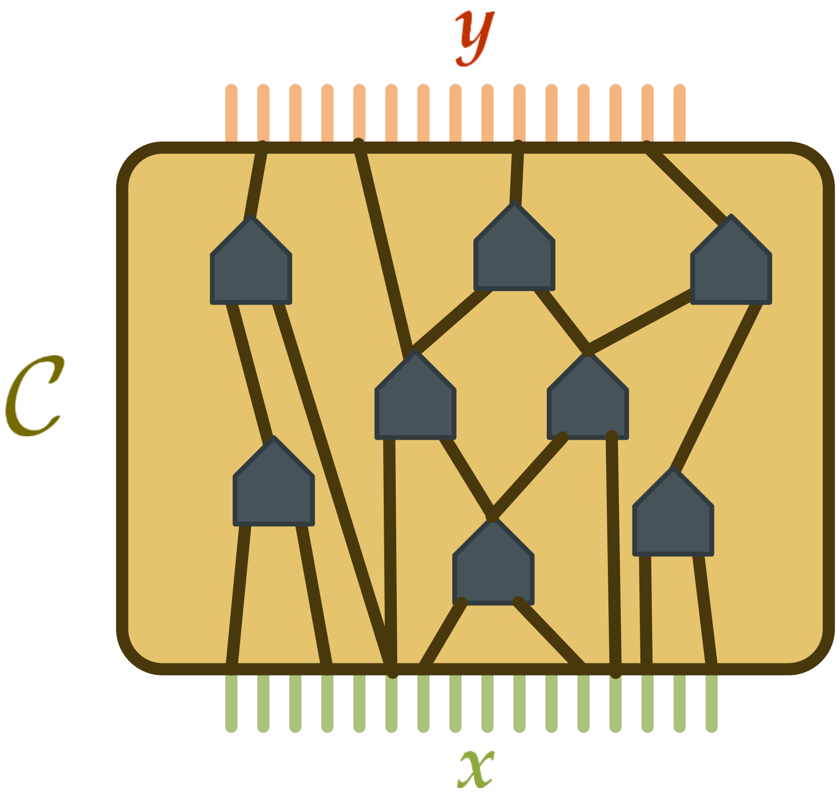
$$1 \cdot v + 2 \cdot y - x_1 - x_2 = 2 \pmod 4$$

0	1	0	0
1	1	0	1
1	1	1	0
0	0	1	1

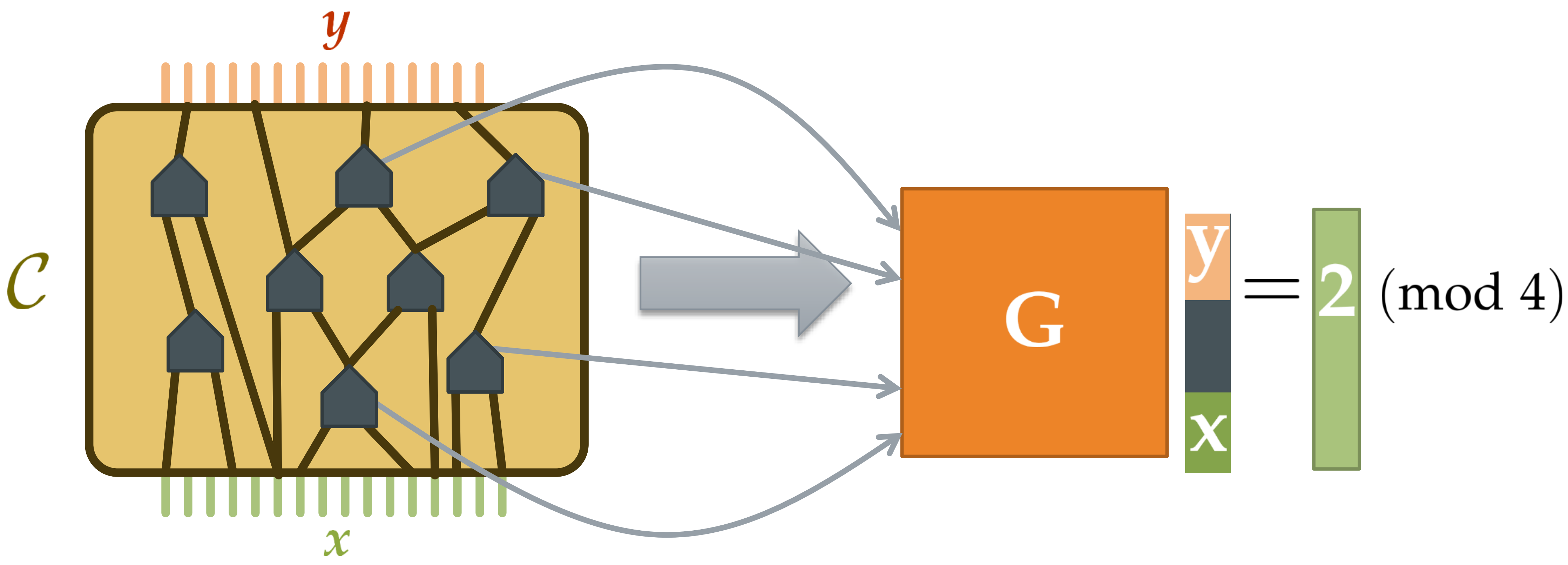
CONSTRAINED SIS IS PWPP-HARD



CONSTRAINED SIS IS PWPP-HARD

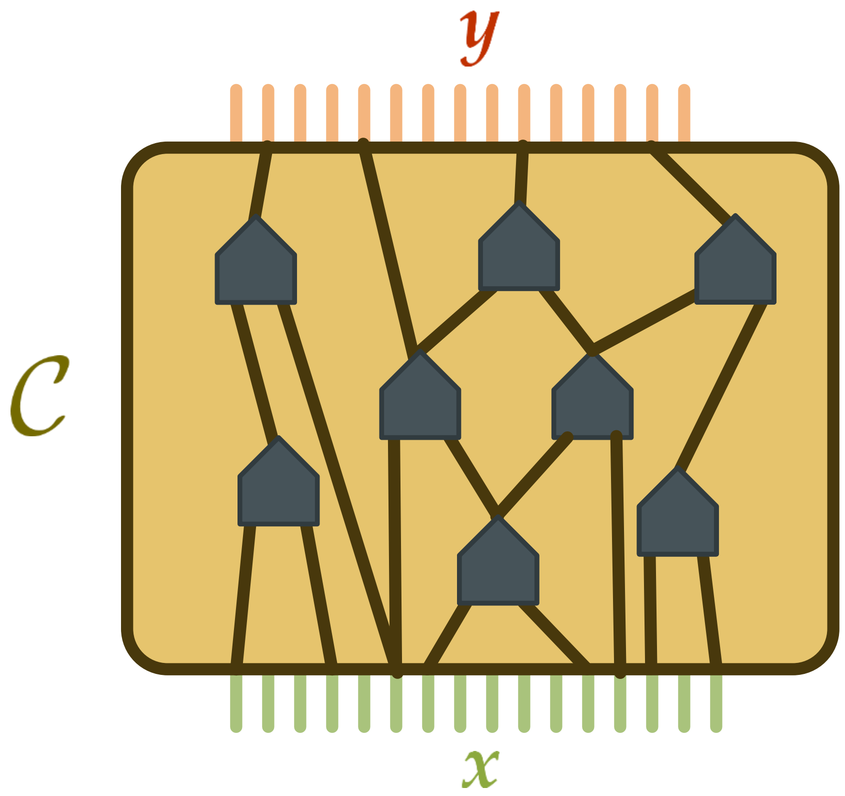


CONSTRAINED SIS IS PWPP-HARD

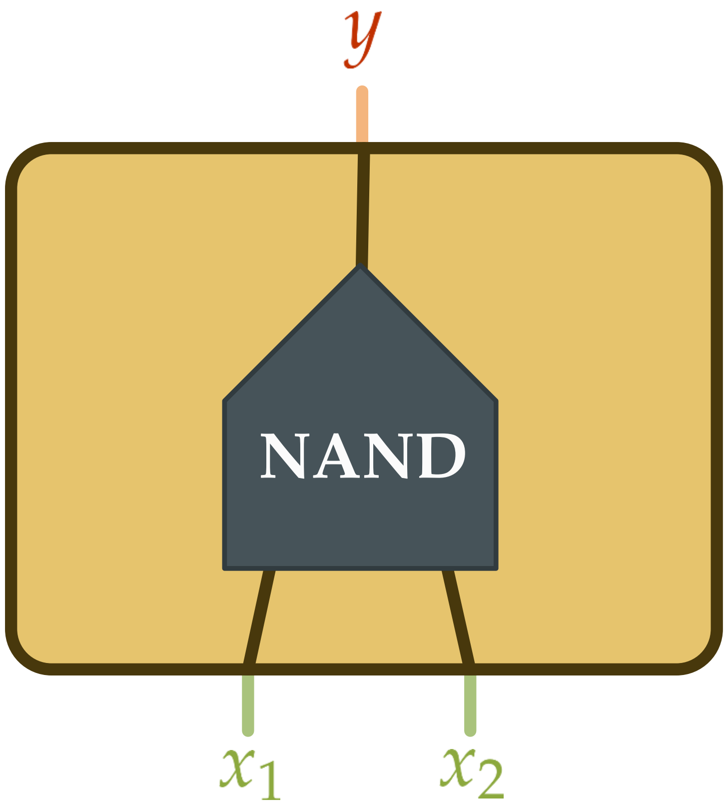


CONSTRAINED SIS IS PWPP-HARD

Is G binary invertible?



CONSTRAINED SIS IS PWPP-HARD

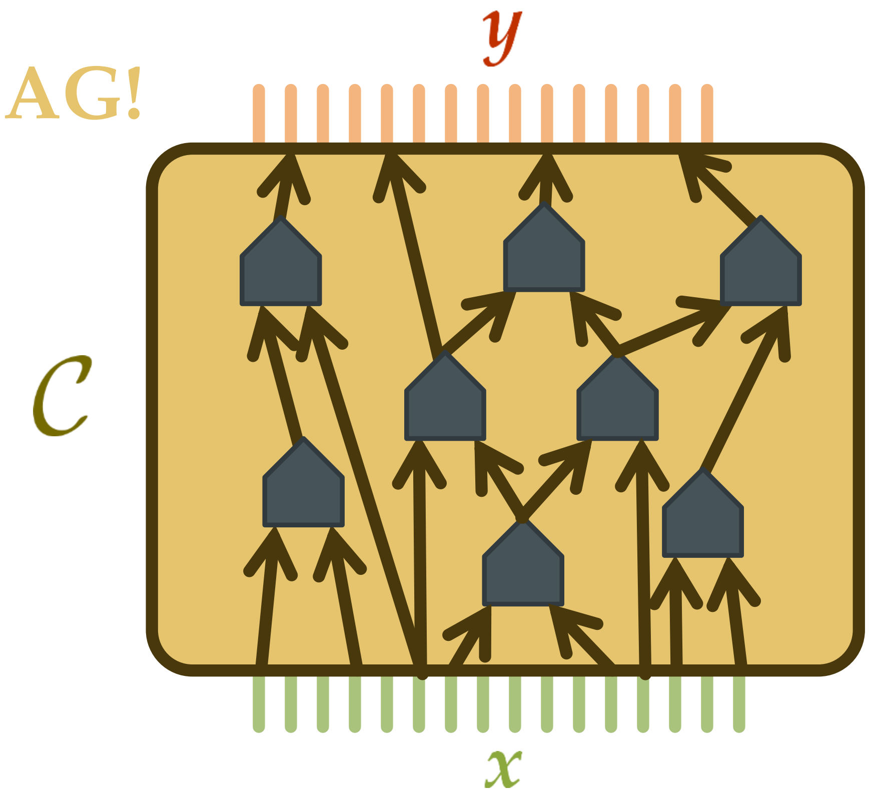


g

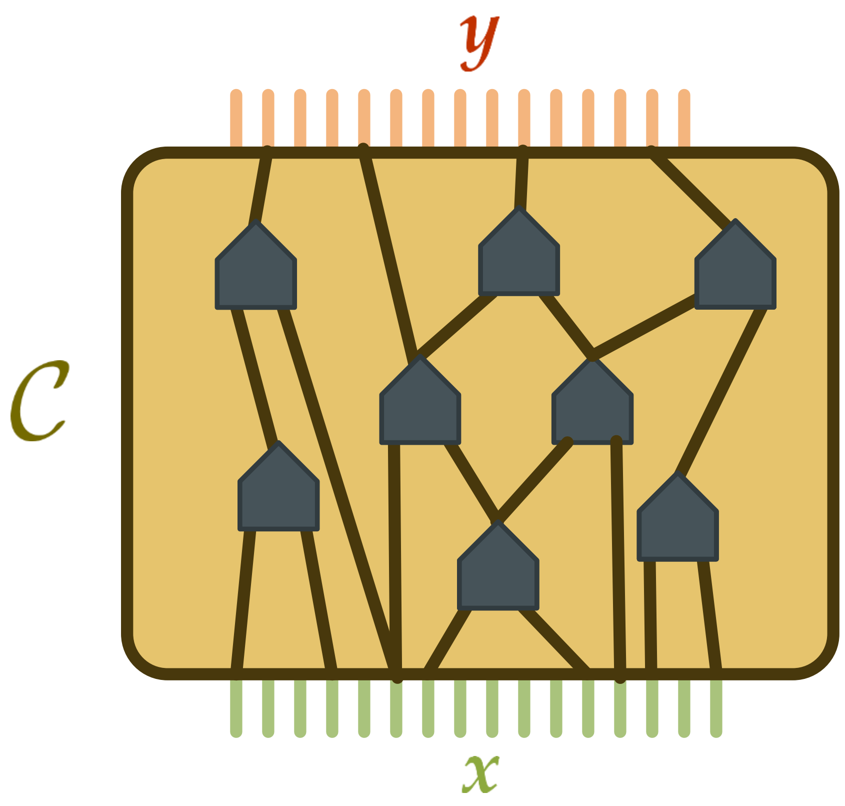
$$\boxed{1 \cdot v + 2 \cdot y} - x_1 - x_2 = 2 \pmod 4$$

CONSTRAINED SIS IS PWPP-HARD

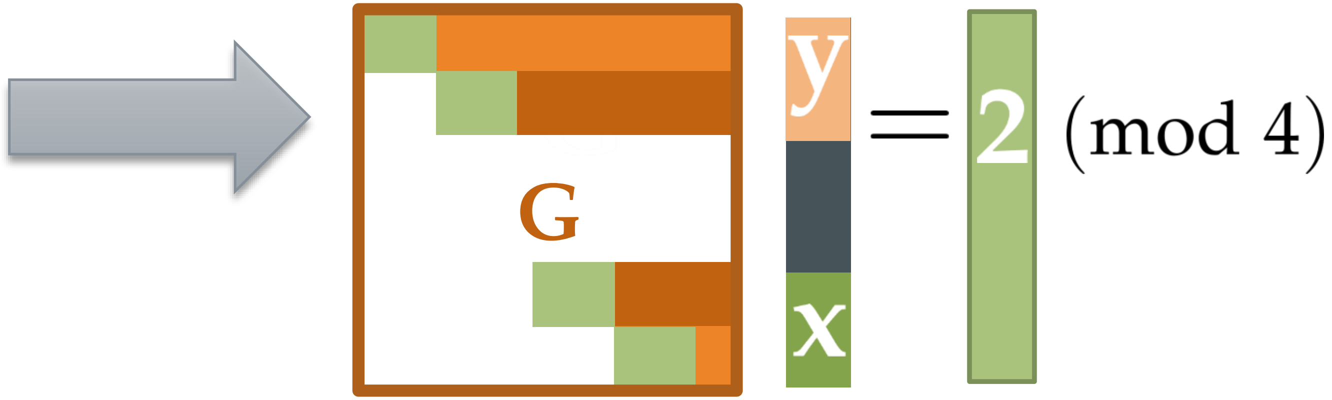
DAG!



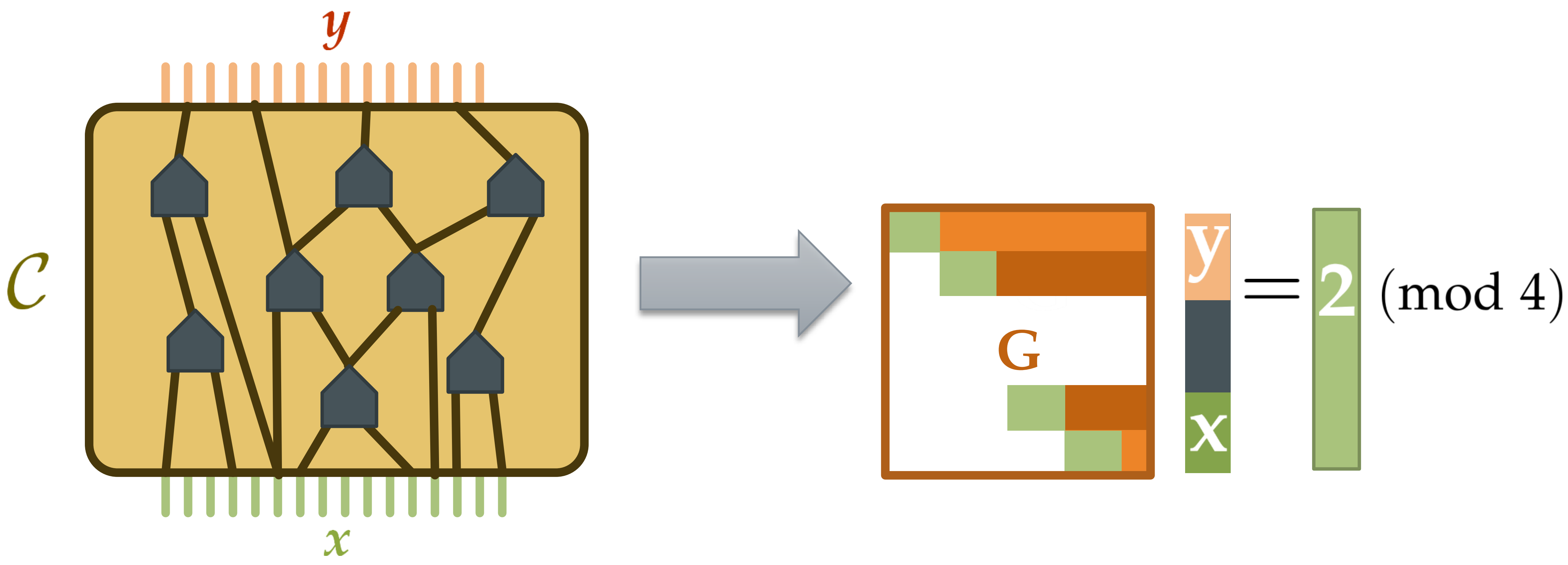
CONSTRAINED SIS IS PWPP-HARD



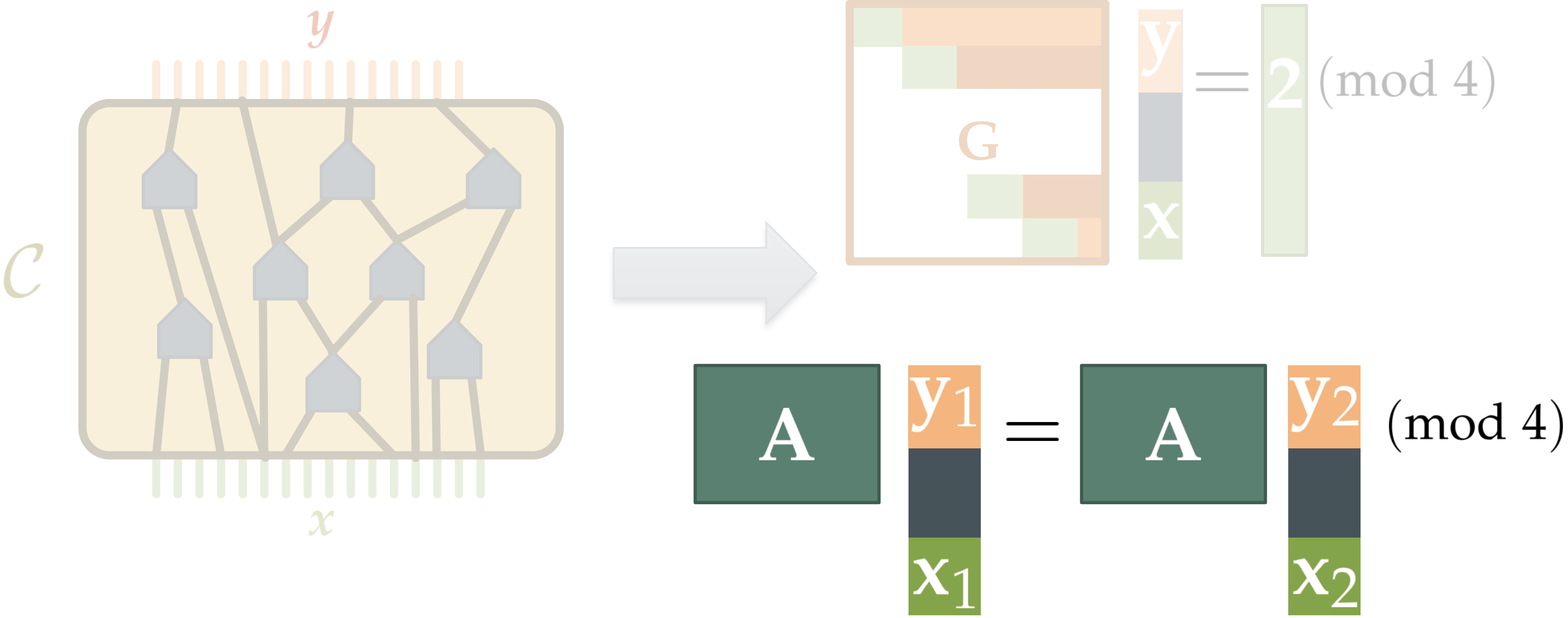
G is binary invertible



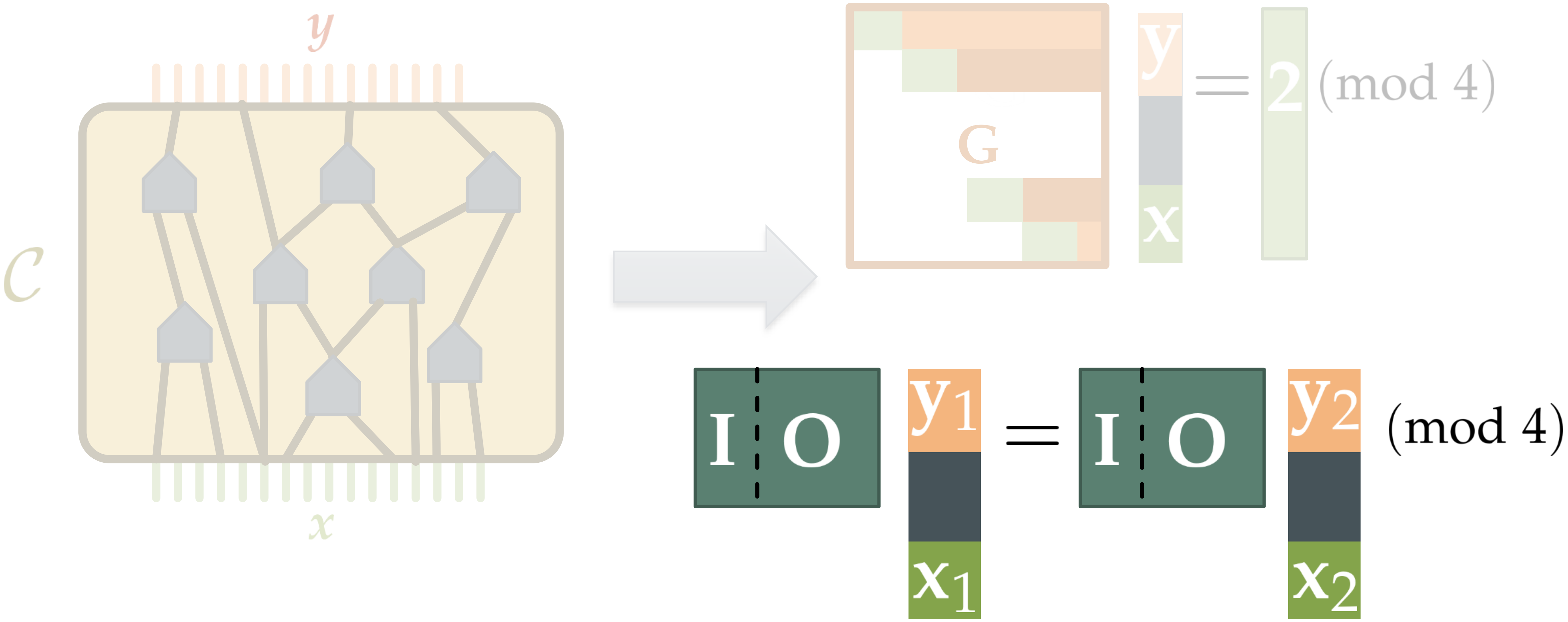
CONSTRAINED SIS IS PWPP-HARD



CONSTRAINED SIS IS PWPP-HARD



CONSTRAINED SIS IS PWPP-HARD



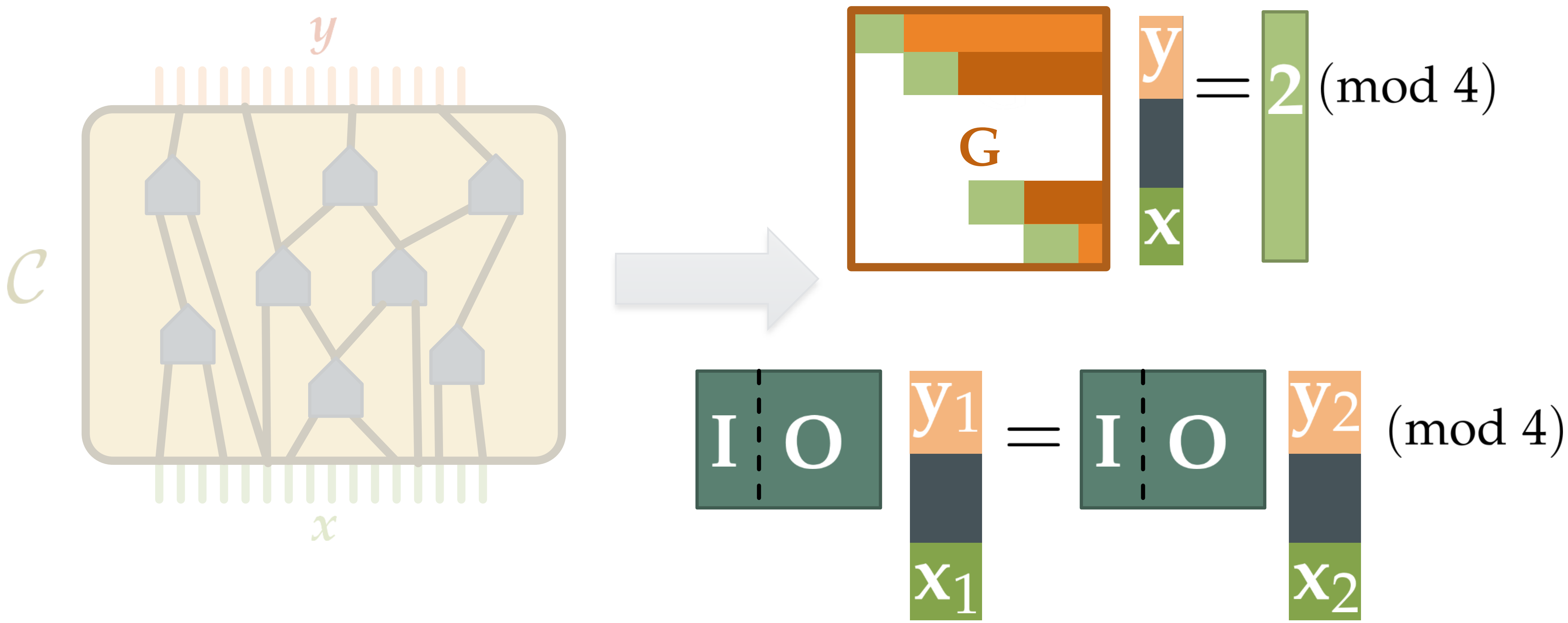
PWPP-COMPLETE PROBLEM: CONSTRAINED SIS

INPUT: $\mathbf{A} \in \mathbb{Z}_q^{r \times m}$, $\mathbf{G} \in \mathbb{Z}_q^{d \times m}$,
with $m > \log(q)(r + d)$ and *binary invertible*

OUTPUT: $\mathbf{x}, \mathbf{y} \in \{0,1\}^m$ s.t. $\mathbf{A}\mathbf{x} = \mathbf{A}\mathbf{y} \pmod q$

$$\mathbf{G}\mathbf{x} = \mathbf{G}\mathbf{y} = \mathbf{0} \pmod q$$

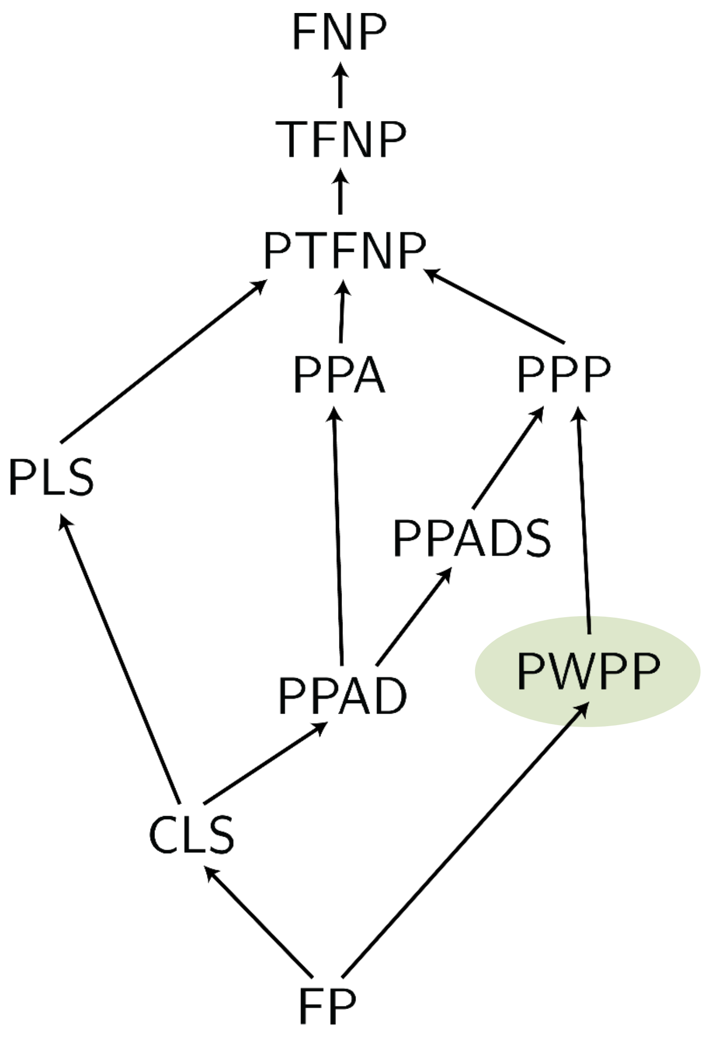
CONSTRAINED SIS IS PWPP-HARD



COMPLEXITY OF TOTAL SEARCH PROBLEMS

Theorem [S Zampetakis Zirdelis 18]:
The first natural complete problems for PPP and PWPP

Constrained-SIS is PWPP-complete



CRHF FROM cSIS

$\leftarrow \mathbb{Z}_q^{r\times m},\ m > \log(q)(r+d)$

KEY:

$\leftarrow$ binary invertible in $\mathbb{Z}_q^{d\times m}$

CRHF FROM cSIS

Input: $\mathbf{x} \in \{0,1\}^{\log(q)r}$

Output: $\mathbf{A} \begin{bmatrix} \mathbf{x}^* \\ \mathbf{x} \end{bmatrix} \pmod q$ where $\mathbf{G} \begin{bmatrix} \mathbf{x}^* \\ \mathbf{x} \end{bmatrix} = \mathbf{0} \pmod q$

CRHF FROM cSIS

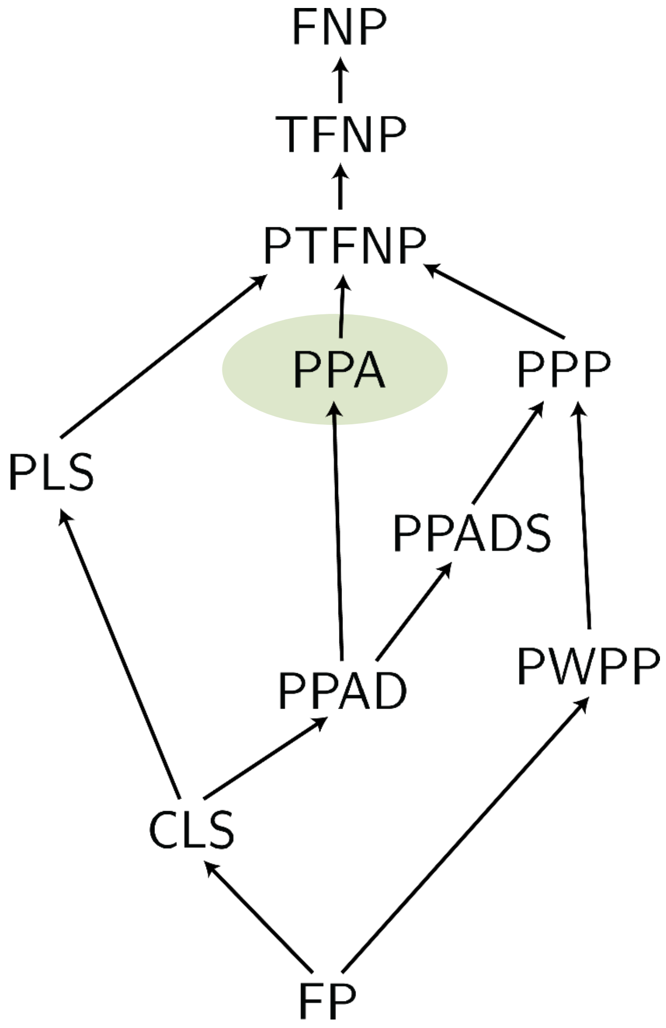
INPUT: $\mathbf{x} \in \{0,1\}^{\log(q)r}$

OUTPUT: $\mathbf{A} \begin{bmatrix} \mathbf{x}^* \\ \mathbf{x} \end{bmatrix} \pmod q$ where $\mathbf{G} \begin{bmatrix} \mathbf{x}^* \\ \mathbf{x} \end{bmatrix} = \mathbf{0} \pmod q$

*cSIS defines a **worst-case universal** collision-resistant hash function family.*

COMPLEXITY OF TOTAL SEARCH PROBLEMS

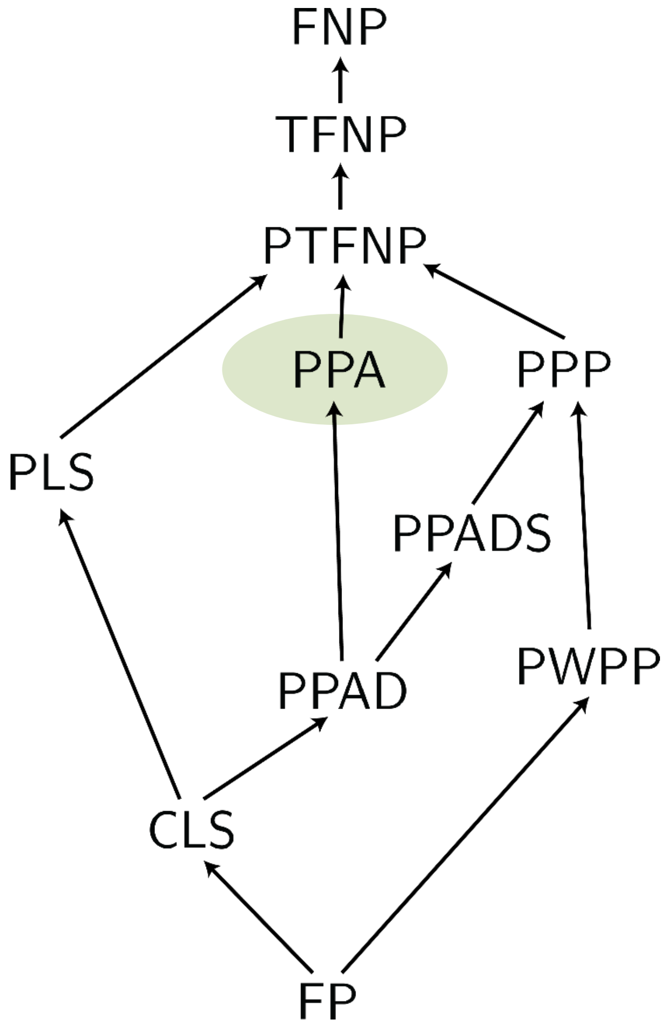
PPA → Parity arguments



Theorem [Göös Kamath S Zampetakis 19] :
The first natural complete problems for PPA_p for any prime p.

COMPLEXITY OF TOTAL SEARCH PROBLEMS

PPA_p → Modulo p arguments

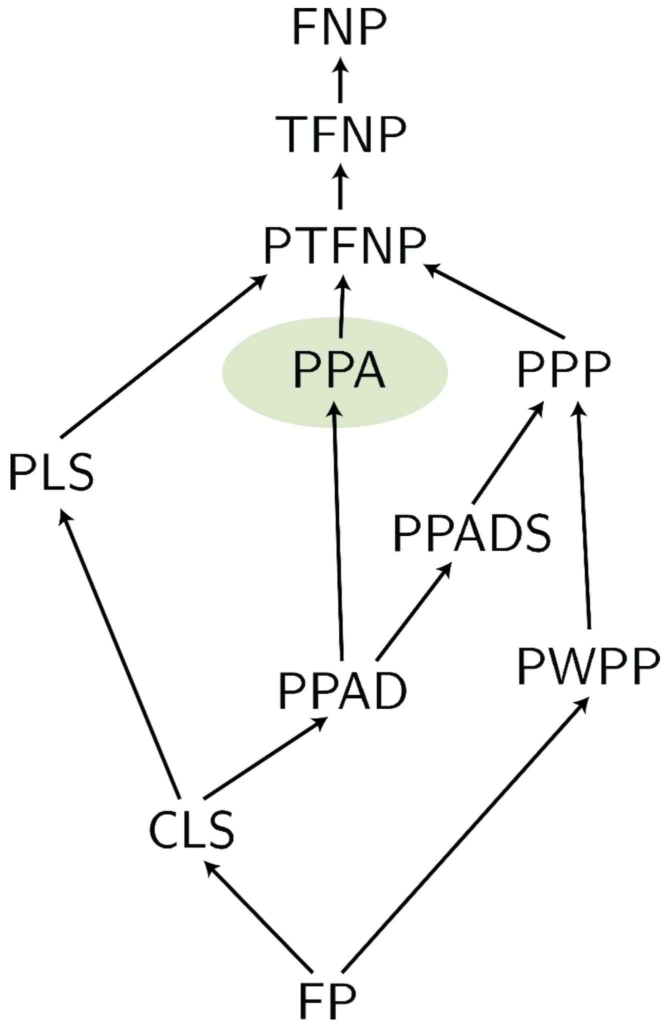


Theorem [Göös Kamath S Zampetakis 19] **:**
The first natural complete problems for PPA_p for any prime p.

COMPLEXITY OF TOTAL SEARCH PROBLEMS

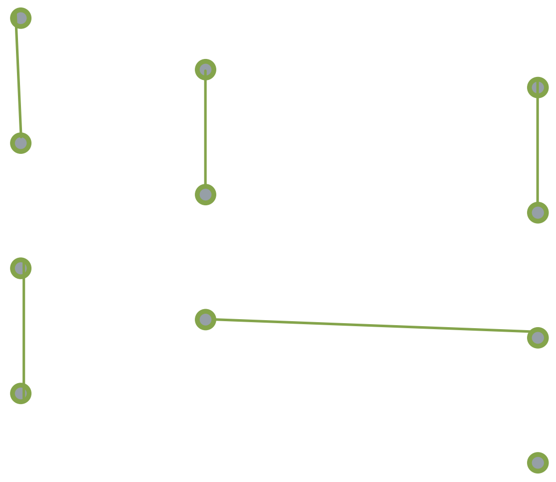
Theorem [Göös Kamath S Zampetakis 19] **:**
The first natural complete problems for PPA_p for any prime p.

SymmetricChevalley$_p$ is PPA_p-complete



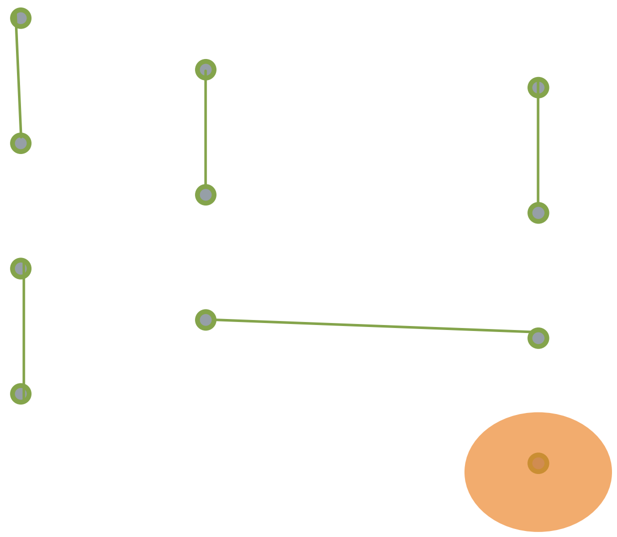
POLYNOMIAL PARITY ARGUMENT

A matching on an odd number of vertices has an isolated node.



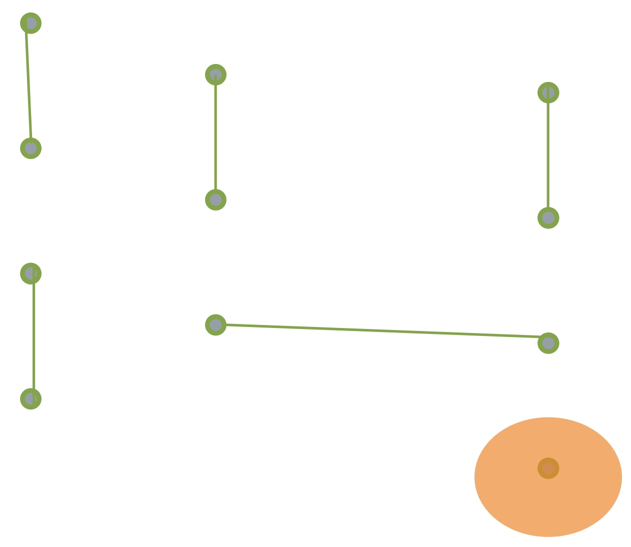
POLYNOMIAL PARITY ARGUMENT

A matching on an odd number of vertices has an isolated node.



POLYNOMIAL PARITY ARGUMENT

A matching on an odd number of vertices has an isolated node.



Tolopogy:
Borsuk-Ulam is PPA-complete [Aisenberga Bonet, Buss 15]

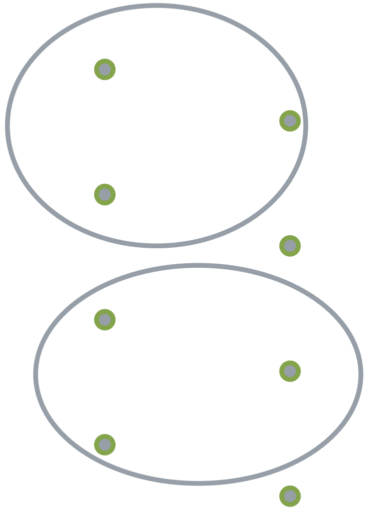
Fair division:
Consensus Halving, Necklace Splitting are PPA-complete
[Filos-Ratsikas Goldberg 18]

Computational Geometry:
Ham Sandwich is PPA-complete [Filos-Ratsikas Goldberg 19]

POLYNOMIAL MODULO p ARGUMENT

A p-dimensional matching on a non-multiple-of-p many vertices has an isolated node.

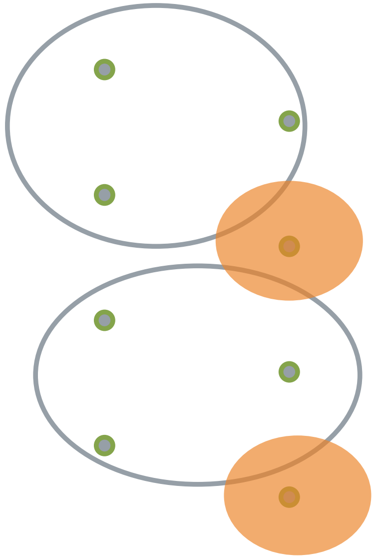
$p = 3$



POLYNOMIAL MODULO p ARGUMENT

A p-dimensional matching on a non-multiple-of-p many vertices has an isolated node.

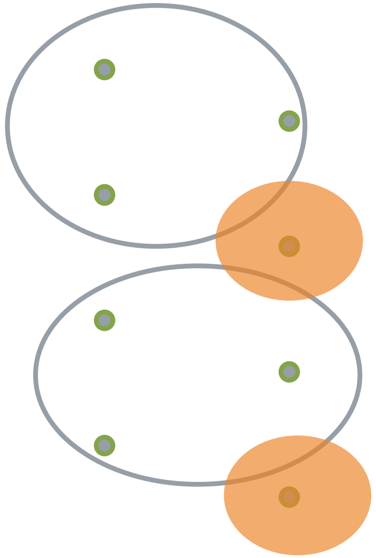
p = 3



POLYNOMIAL MODULO p ARGUMENT

A p-dimensional matching on a non-multiple-of-p many vertices has an isolated node.

p = 3

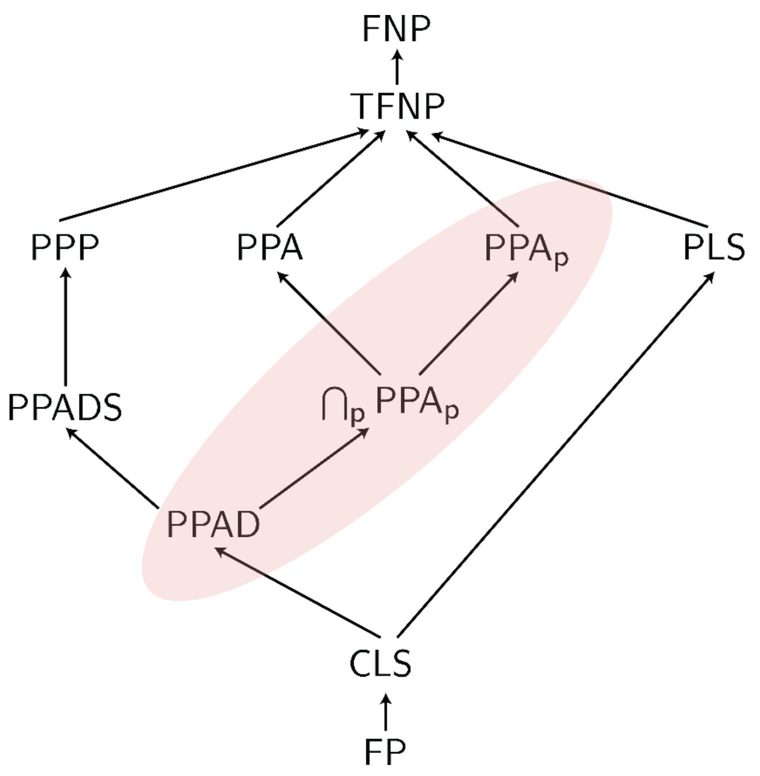


<u>Corresponding results:</u> [Filos-Ratsikas Hollender S. Zampetakis '20]

Tolopogy:
BSS THEOREM [Bárány Shlosman Szucs '81] *is* PPA_p*-complete*

Fair division:
Consensus 1/p-Division, p-Necklace Splitting are in PPA_p.

STRUCTURAL PROPERTIES



CHEVALLEY-WARNING THEOREM

For any prime p and a polynomial system

$$f_1(x_1, \ldots, x_m) = 0 \pmod{p}$$

$$f_2(x_1, \ldots, x_m) = 0 \pmod{p}$$

$$\ldots$$

$$f_n(x_1, \ldots, x_m) = 0 \pmod{p}$$

let $V_{\mathbf{f}} = \{\mathbf{x} \mid \mathbf{f}(\mathbf{x}) = 0 \pmod{p}\}$.

CHEVALLEY-WARNING THEOREM

For any prime p and a polynomial system

$$f_1(x_1, \ldots, x_m) = 0 \pmod{p}$$
$$f_2(x_1, \ldots, x_m) = 0 \pmod{p}$$
$$\ldots$$
$$f_n(x_1, \ldots, x_m) = 0 \pmod{p}$$

let $V_{\mathbf{f}} = \{\mathbf{x} \mid \mathbf{f}(\mathbf{x}) = 0 \pmod{p}\}$.

If $\sum_{i=1}^{n} \deg(f_i) < m$ then $|V_{\mathbf{f}}| \equiv 0 \pmod{p}$.

CHEVALLEY-WARNING THEOREM

For any prime p and a polynomial system

$$f_1(x_1, \ldots, x_m) = 0 \pmod{p}$$

$$f_2(x_1, \ldots, x_m) = 0 \pmod{p}$$

$$\ldots$$

$$f_n(x_1, \ldots, x_m) = 0 \pmod{p}$$

let $V_{\mathbf{f}} = \{\mathbf{x} \mid \mathbf{f}(\mathbf{x}) = 0 \pmod{p}\}$.

If $\sum_{i=1}^{n} \deg(f_i) < m$ then $|V_{\mathbf{f}}| \equiv 0 \pmod{p}$.

Chevalley-Warning Condition

CHEVALLEY-WARNING THEOREM

For any prime p let $\mathbf{f} \in \mathbb{F}_p[x_1, \ldots, x_m]^n$ be a system of polynomials with zero constant terms satisfying $\sum_{i=1}^{n} \deg(f_i) < m$, then $\mathbf{f}$ has a non-zero solution.

CHEVALLEY-WARNING THEOREM

For any prime p let $\mathbf{f} \in \mathbb{F}_p[x_1, \ldots, x_m]^n$ be a system of polynomials with zero constant terms satisfying $\sum_{i=1}^{n} \deg(f_i) < m$, then $\mathbf{f}$ has a non-zero solution.

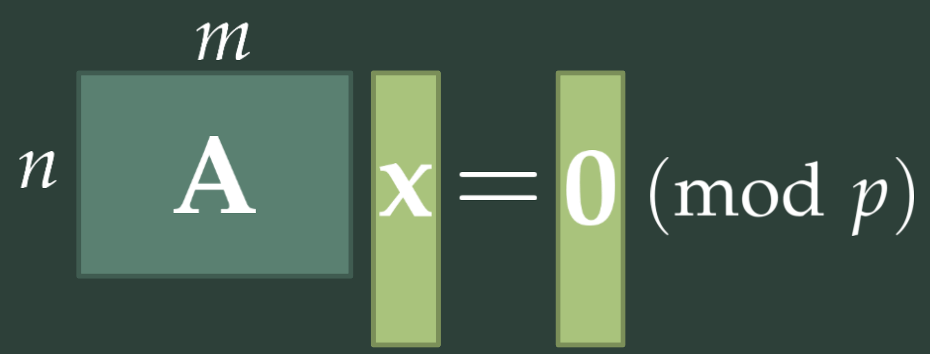
BIS$_p$ REDUCES TO CHEVALLEY$_p$

For any prime p and a matrix $\mathbf{A} \in \mathbb{F}_p^{n\times m}$

$$\underbrace{\mathbf{A}}_{n \times m}\,\mathbf{x} = \mathbf{0} \pmod{p}$$

BIS$_p$ REDUCES TO CHEVALLEY$_p$

For any prime p and a matrix $\mathbf{A} \in \mathbb{F}_p^{n \times m}$

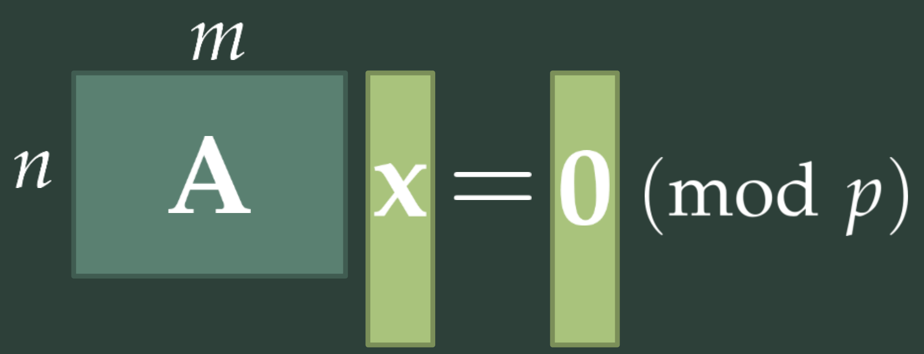


If $n(p-1) < m$ then there exists a *binary* solution $\mathbf{x}$, $\mathbf{x} \neq 0^m$.

BIS_p REDUCES TO CHEVALLEY_p

$\text{SIS}_p \leq \text{BIS}_p$

For any prime p and a matrix $\mathbf{A} \in \mathbb{F}_p^{n \times m}$



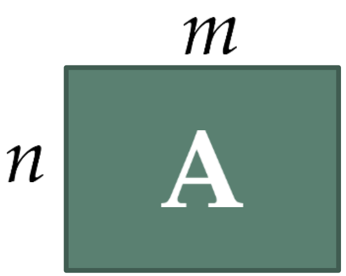
If $n(p-1) < m$ then there exists a *binary* solution $\mathbf{x}$, $\mathbf{x} \neq 0^m$.

BIS$_p$ REDUCES TO CHEVALLEY$_p$

For any prime p and $\mathbf{A} \in \mathbb{F}_p^{n \times m}$, the linear system $\mathbf{Ax} = \mathbf{0} \pmod{p}$ has a non-trivial binary solution if $m > n(p-1)$.

BIS_p REDUCES TO CHEVALLEY_p

For any prime p and $\mathbf{A} \in \mathbb{F}_p^{n \times m}$, the linear system $\mathbf{A}\mathbf{x} = \mathbf{0} \pmod{p}$ has a non-trivial binary solution if $m > n(p-1)$.



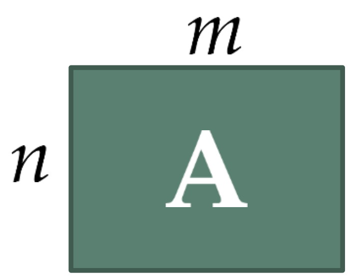
Proof:

Let $f_j(\mathbf{x}) = a_{1j}x_1^{p-1} + a_{2j}x_2^{p-1} + \cdots + a_{mj}x_m^{p-1}, j \in [n]$, then

$$\sum_{j=1}^{n} \deg(f_j) = n(p-1) < m.$$

BIS_p REDUCES TO CHEVALLEY_p

For any prime p and $\mathbf{A} \in \mathbb{F}_p^{n\times m}$, the linear system $\mathbf{Ax} = \mathbf{0} \pmod{p}$ has a non-trivial binary solution if $m > n(p-1)$.



Proof:

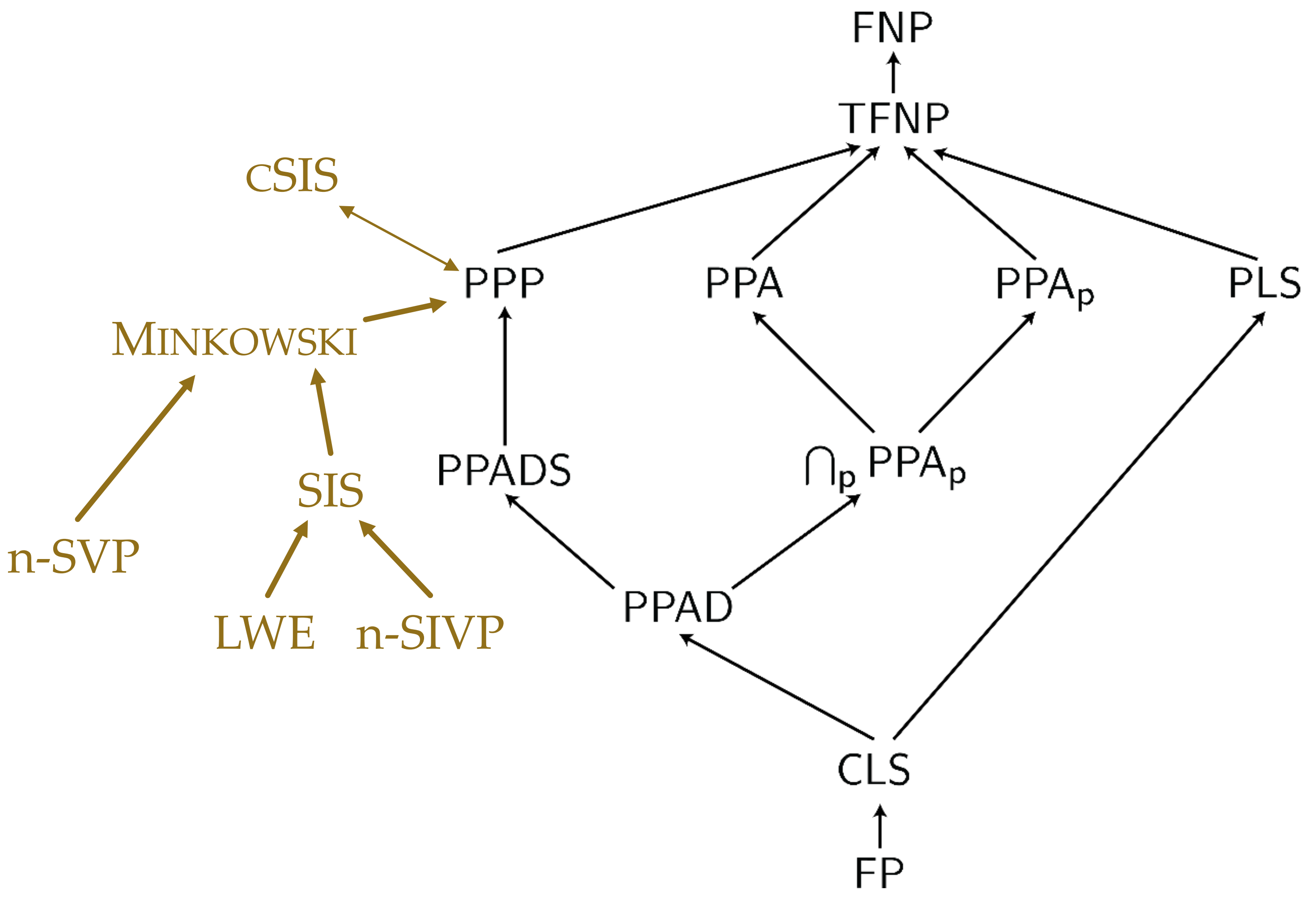
Let $f_j(\mathbf{x}) = a_{1j}x_1^{p-1} + a_{2j}x_2^{p-1} + \cdots + a_{mj}x_m^{p-1}, j \in [n]$, then

$$\sum_{j=1}^{n} \deg(f_j) = n(p-1) < m.$$

From CWT, there exists a non-zero solution.

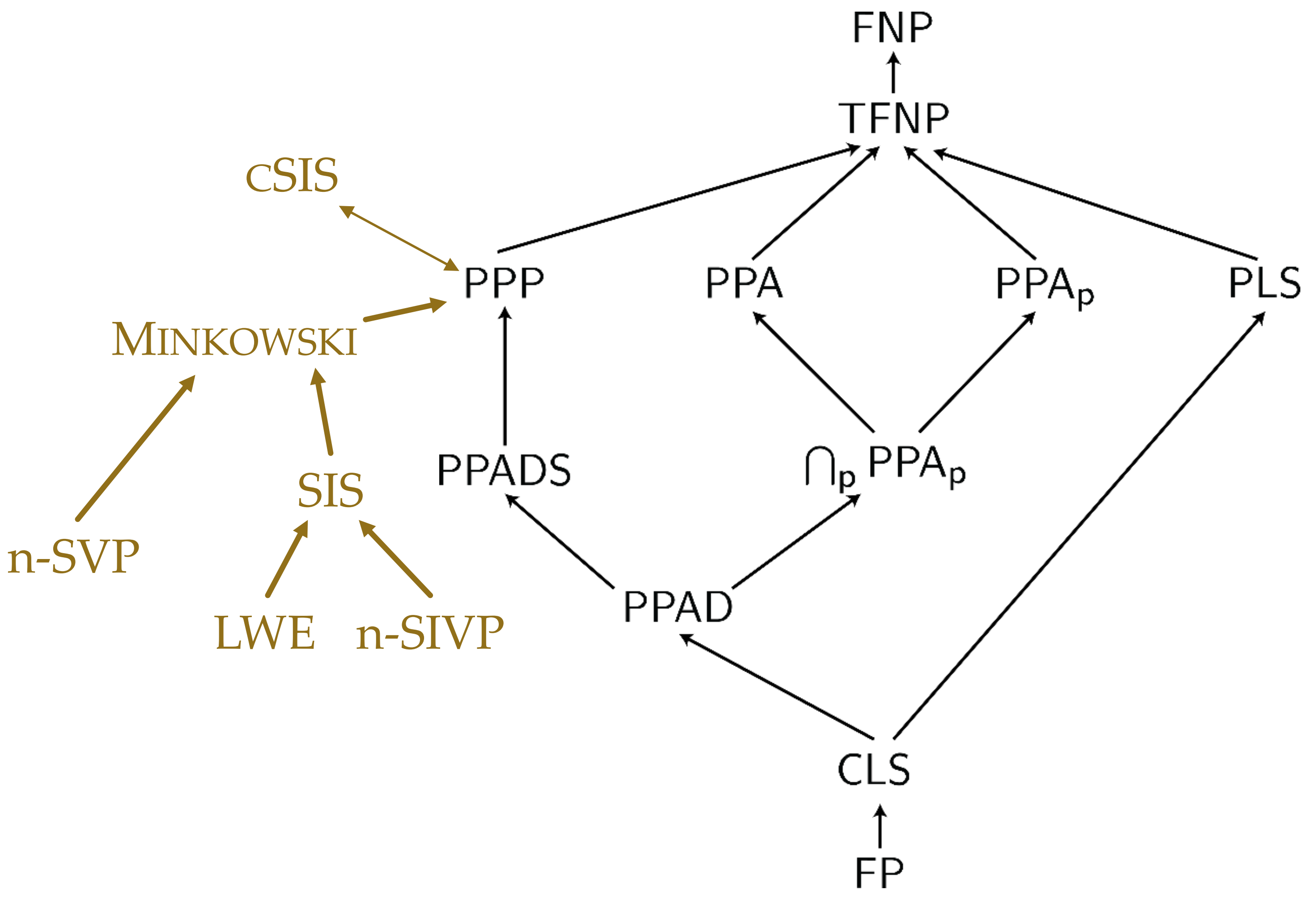
$$|V_{\mathbf{f}}| = 0 \pmod{p}$$

FUTURE DIRECTIONS - INCLUSIONS



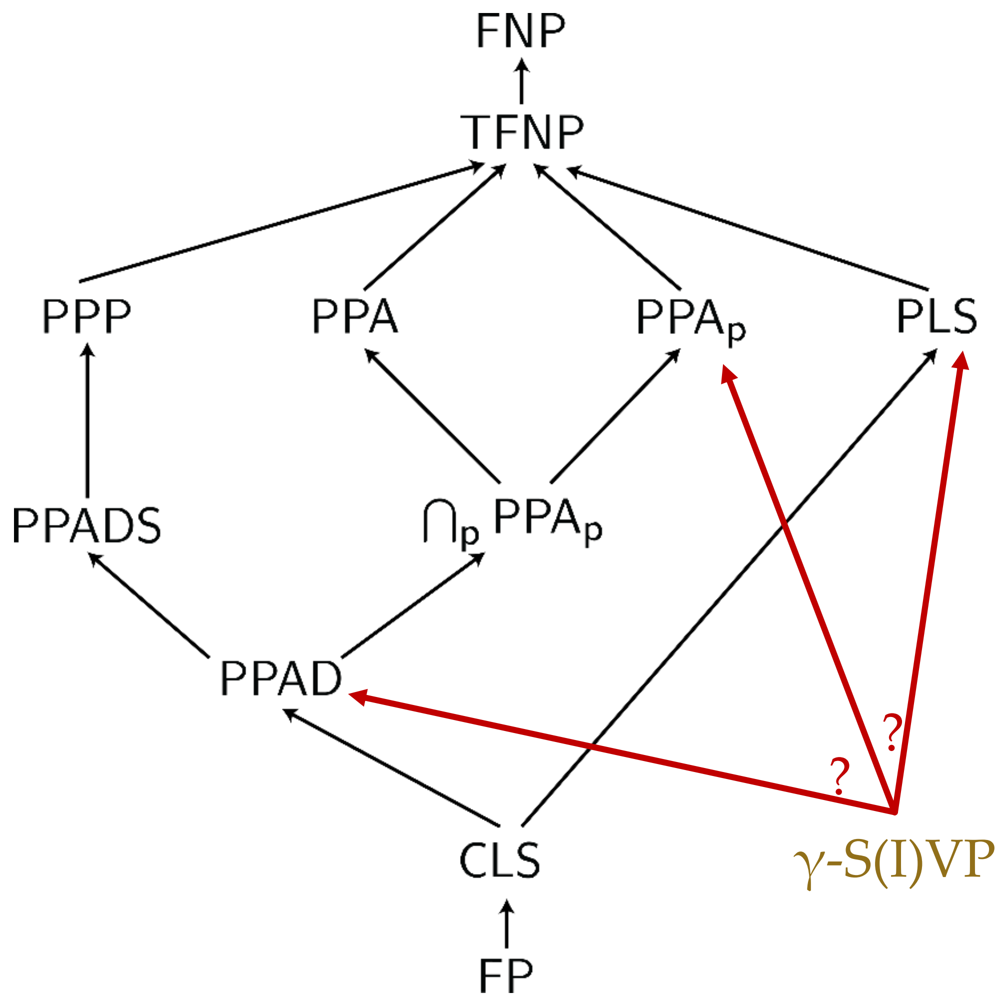
FUTURE DIRECTIONS - INCLUSIONS

1. $n^{1/2}$-SVP ?



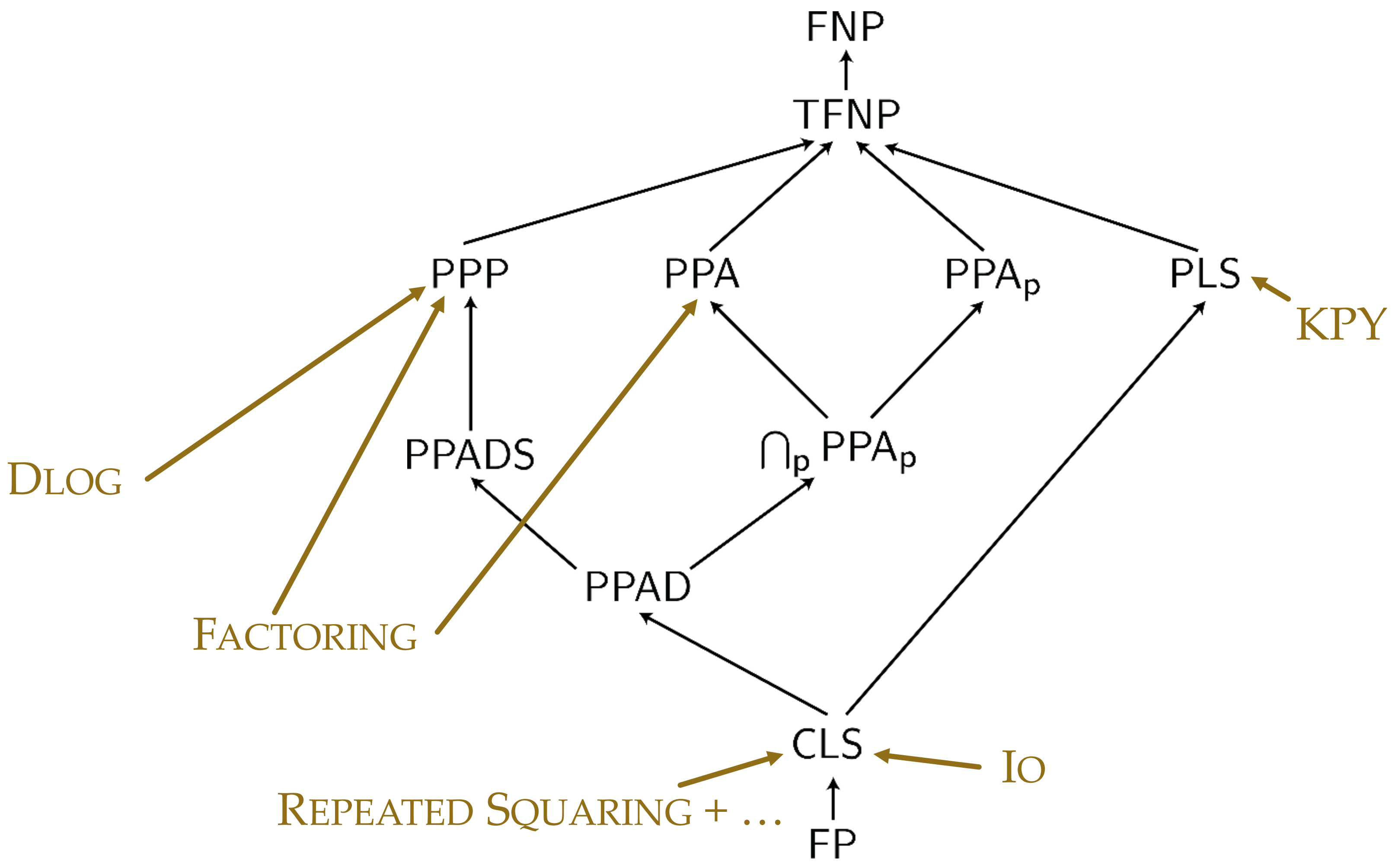
FUTURE DIRECTIONS - INCLUSIONS

1. $n^{1/2}$-SVP ?
2. Beyond PPP?



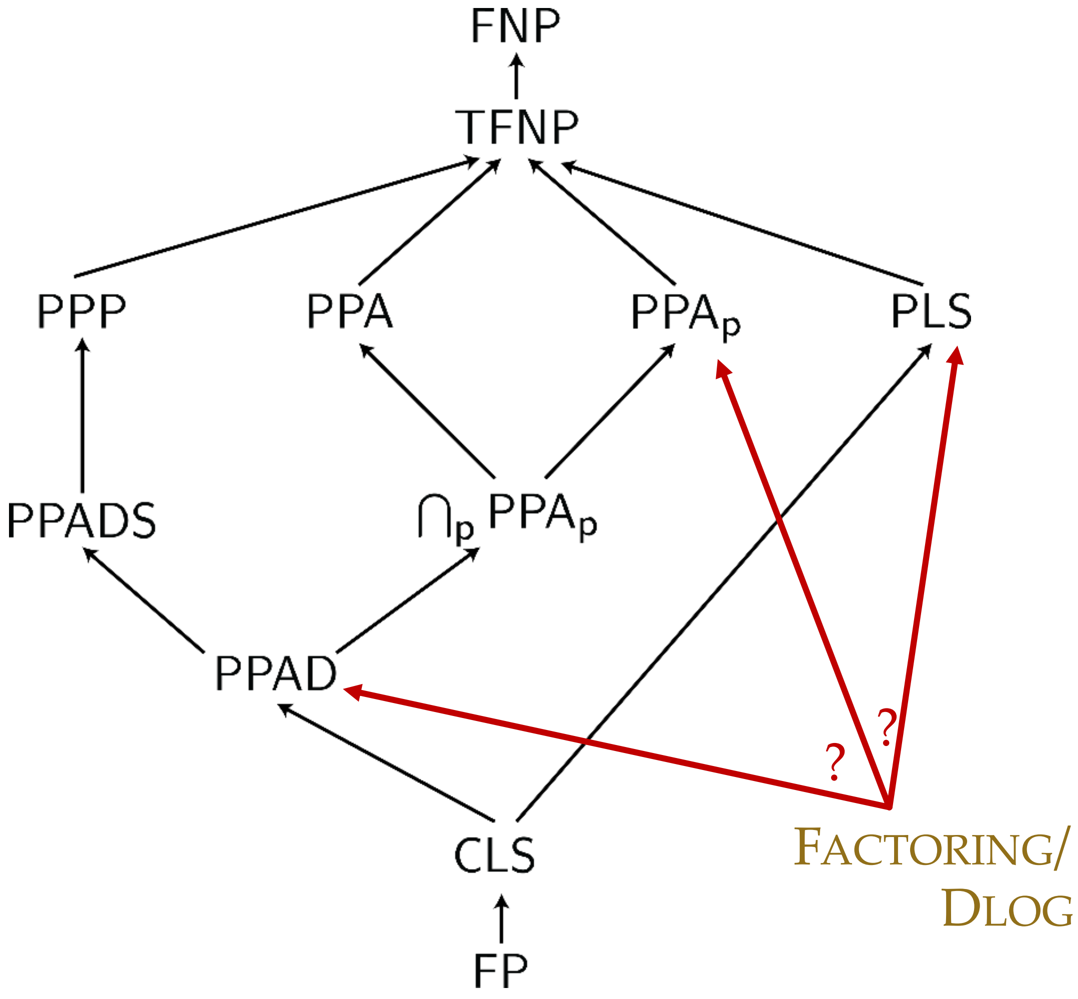
FUTURE DIRECTIONS - INCLUSIONS

1. $n^{1/2}$-SVP ?
2. Beyond PPP?
3. Other Assumptions?



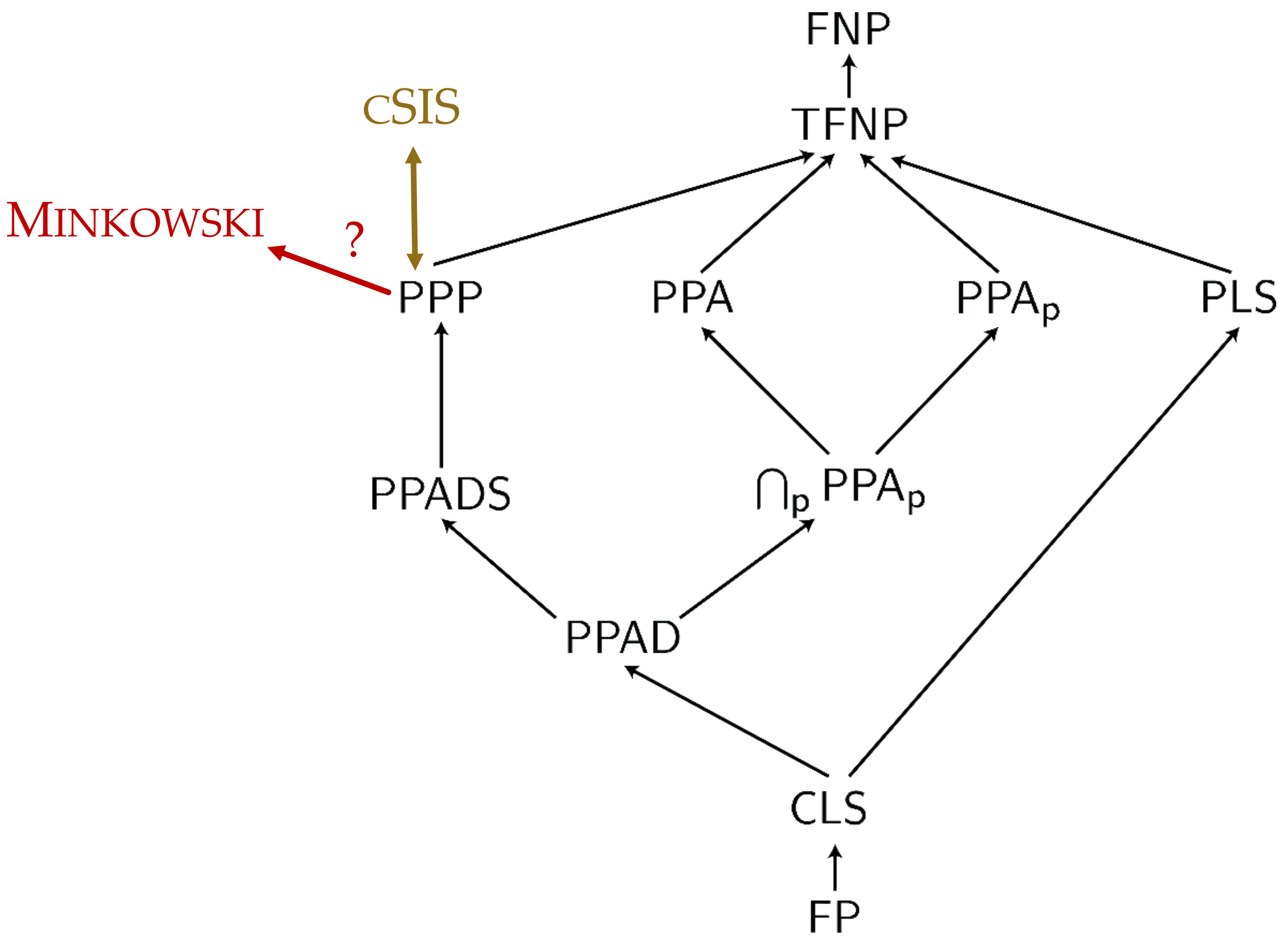
FUTURE DIRECTIONS - INCLUSIONS

1. $n^{1/2}$-SVP ?
2. Beyond PPP?
3. Other Assumptions?



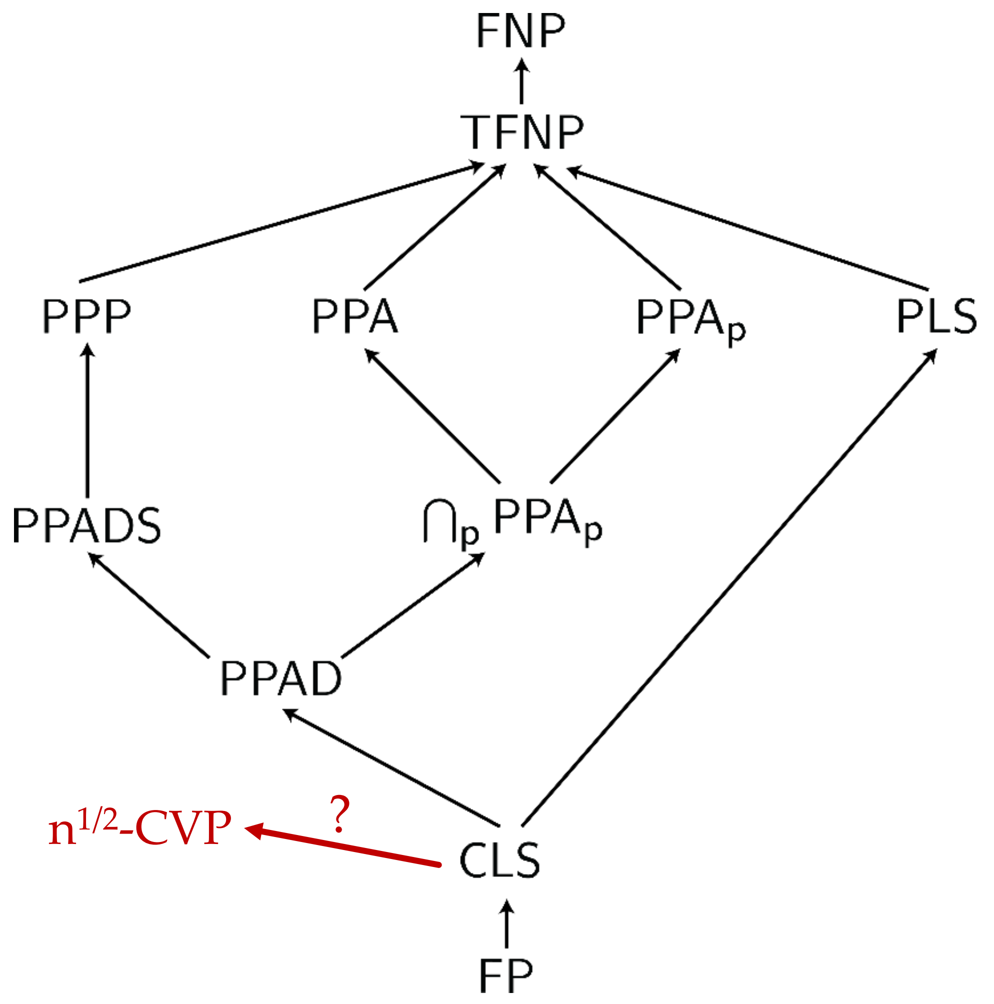
FUTURE DIRECTIONS - HARDNESS

1. MINKOWSKI ?



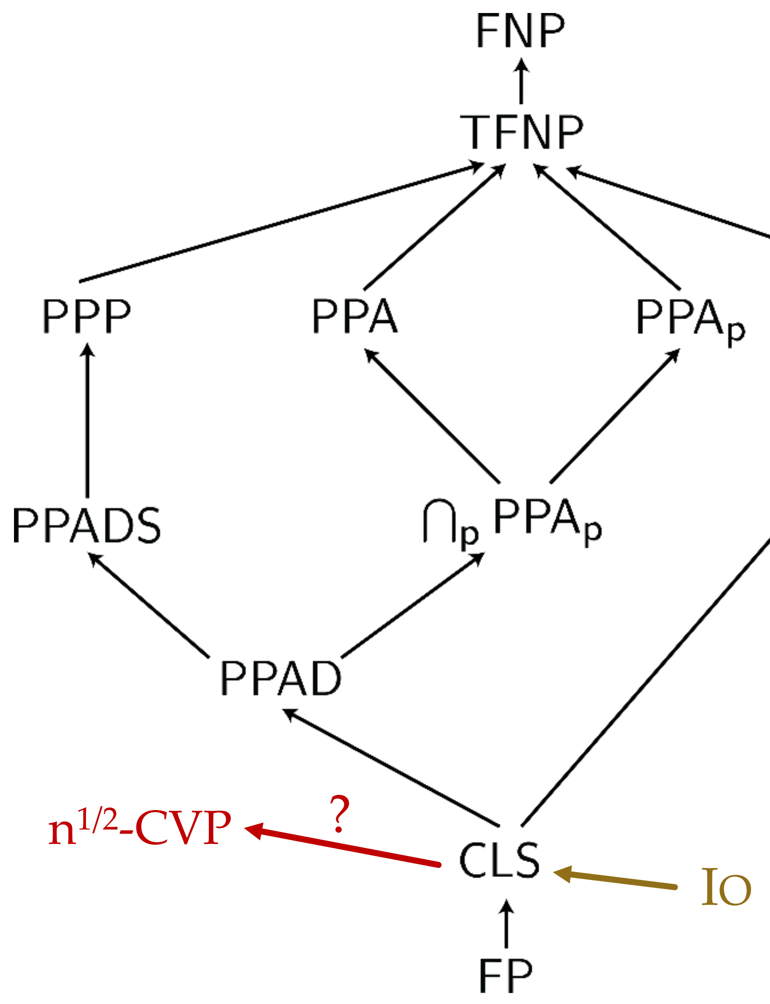
FUTURE DIRECTIONS - HARDNESS

1. MINKOWSKI ?
2. $n^{1/2}$-CVP ?
3. Beyond PPP?



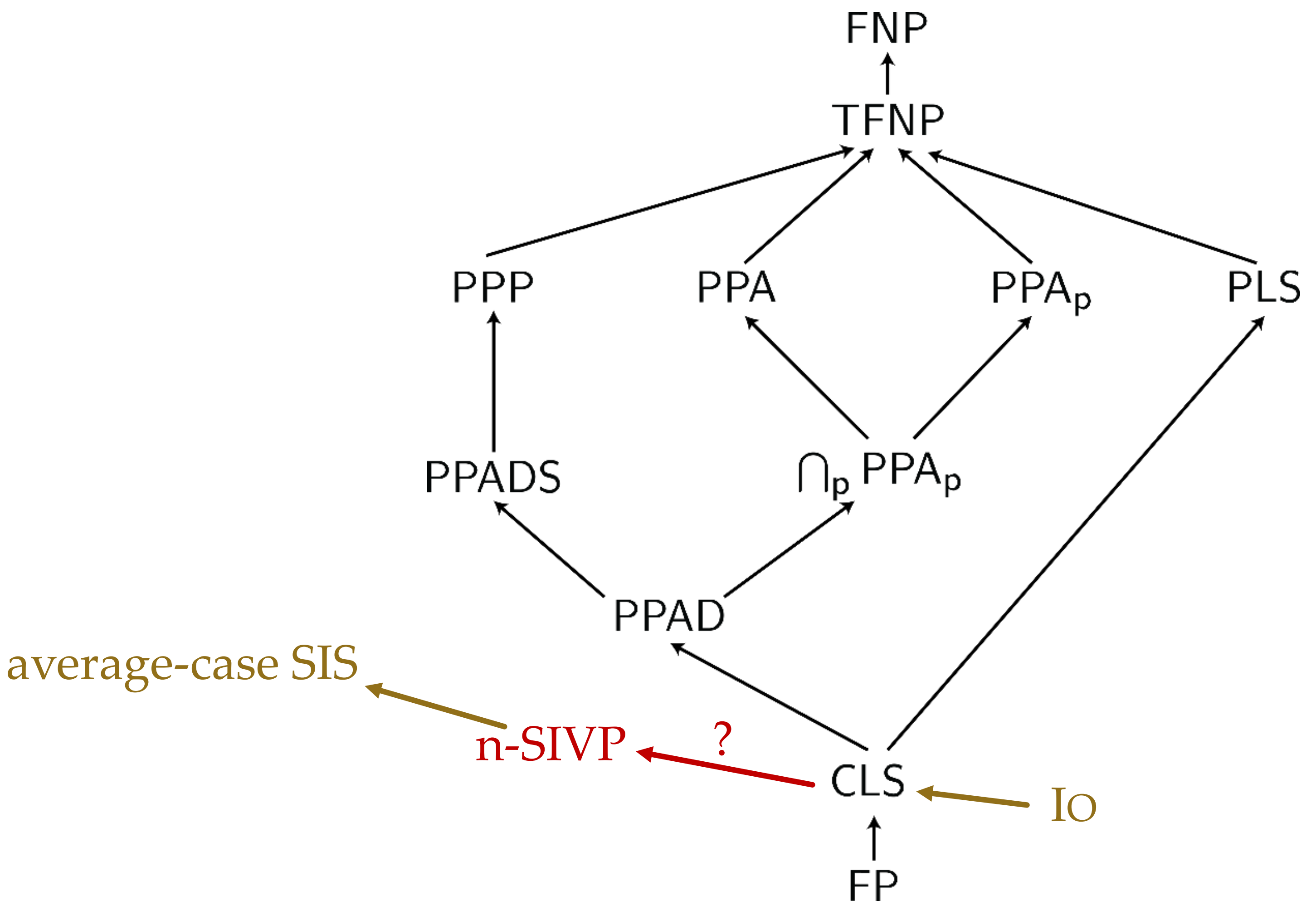
FUTURE DIRECTIONS - HARDNESS

1. MINKOWSKI ?
2. $n^{1/2}$-CVP ?
3. Beyond PPP?



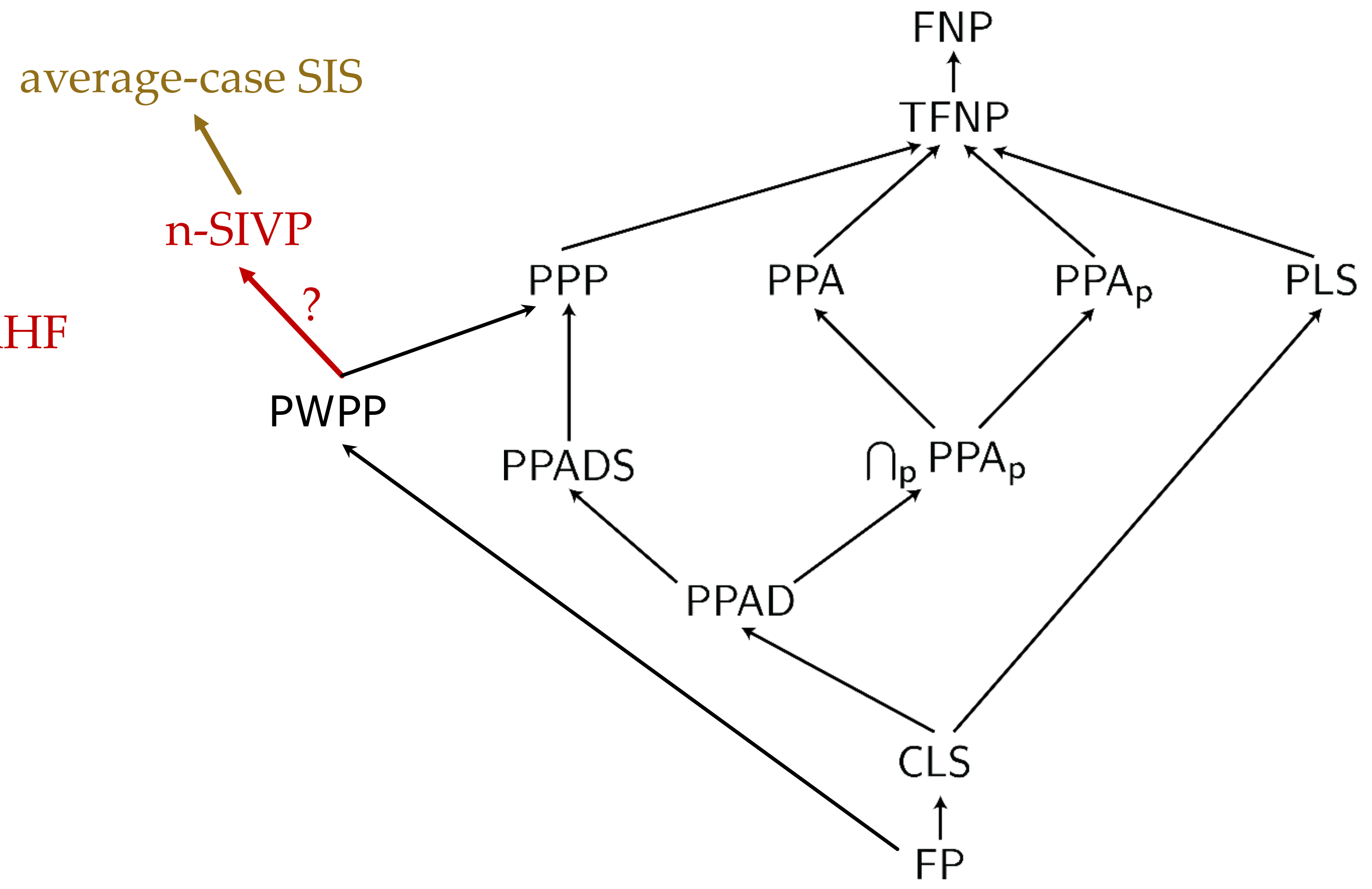
FUTURE DIRECTIONS - HARDNESS

1. MINKOWSKI ?
2. $n^{1/2}$-CVP ?
3. Beyond PPP?
4. n-SIVP ?



FUTURE DIRECTIONS - HARDNESS

1. MINKOWSKI ?
2. $n^{1/2}$-CVP ?
3. Beyond PPP?
4. n-SIVP ?
5. n-SIVP VS PWPP?
   natural and **universal** CRHF



FUTURE DIRECTIONS

- TFNP and Lattice Theory

  Is MINKOWSKI PPP-complete? Is SIS PPP-complete? Is there a hardness of approximation for PPP? Is $\sqrt{n}$-SVP in PPP? ***Is there a natural universal CRHF?***

FUTURE DIRECTIONS

- TFNP and Lattice Theory

  Is MINKOWSKI PPP-complete? Is SIS PPP-complete? Is there a hardness of approximation for PPP? Is $\sqrt{n}$-SVP in PPP? ***Is there a natural universal CRHF?***

- TFNP and Cryptographic assumptions

  Is SIS/DLOG/FACTORING PPAD-complete?

FUTURE DIRECTIONS

- TFNP and Lattice Theory
  Is MINKOWSKI PPP-complete? Is SIS PPP-complete? Is there a hardness of approximation for PPP? Is $\sqrt{n}$-SVP in PPP? ***Is there a natural universal CRHF?***

- TFNP and Cryptographic assumptions
  Is SIS/DLOG/FACTORING PPAD-complete?

- Cryptography from TFNP
  New cryptographic primitives from PPA? Is there a trapdoor for CHEVALLEY?

FUTURE DIRECTIONS

- TFNP and Lattice Theory
  Is MINKOWSKI PPP-complete? Is SIS PPP-complete? Is there a hardness of approximation for PPP? Is $\sqrt{n}$-SVP in PPP? ***Is there a natural universal CRHF?***

- TFNP and Cryptographic assumptions
  Is SIS/DLOG/FACTORING PPAD-complete?

- Cryptography from TFNP
  New cryptographic primitives from PPA? Is there a trapdoor for CHEVALLEY?

Thank you! ☺