Testing Linearity against Non-Signaling Strategies

Alessandro Chiesa **Peter Manohar** Igor Shinkar

UC Berkeley

What is linearity testing?

Linearity Testing

Linearity Testing

Given oracle access to $f:\{0,1\}^n \rightarrow \{0,1\}$ decide if:

(1) f is linear, **or**

(2) f is far from all linear functions.

Linearity Testing

Given oracle access to $f:\{0,1\}^n \rightarrow \{0,1\}$ decide if:

(1) f is linear, **or**

(2) f is far from all linear functions.

A simple and natural test:

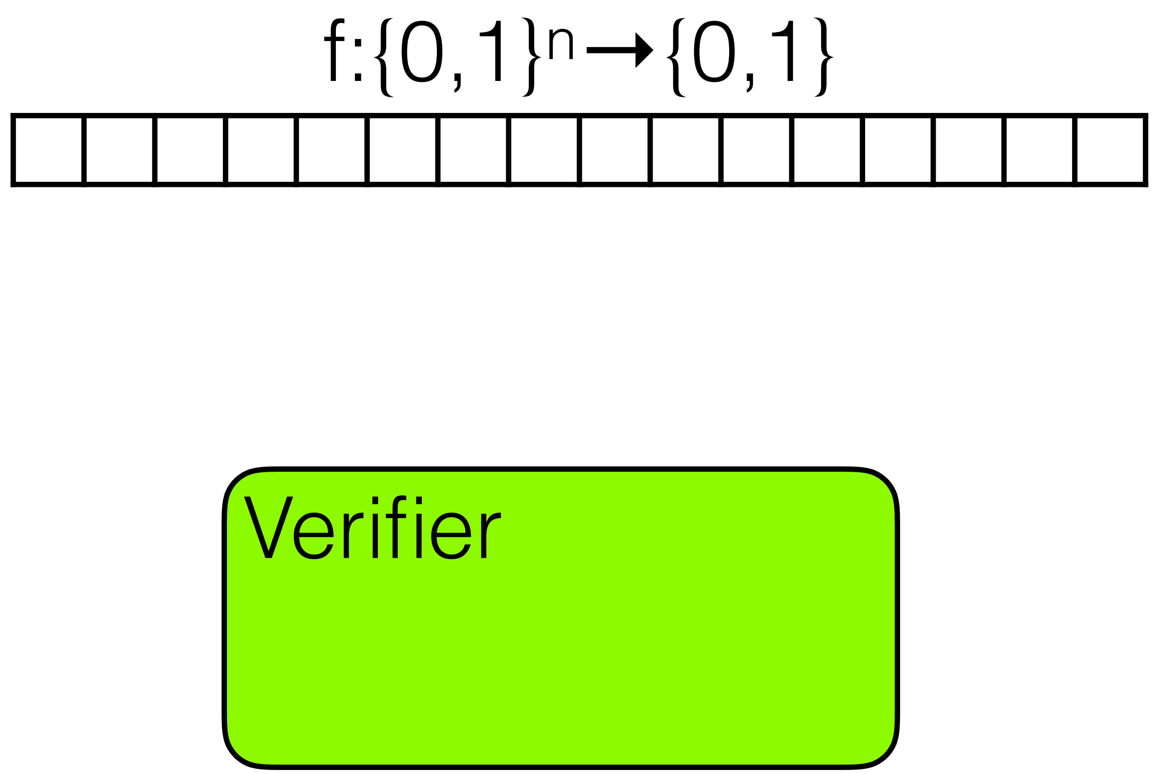
Linearity Testing

Given oracle access to $f:\{0,1\}^n \rightarrow \{0,1\}$ decide if:

(1) f is linear, **or**

(2) f is far from all linear functions.

A simple and natural test:



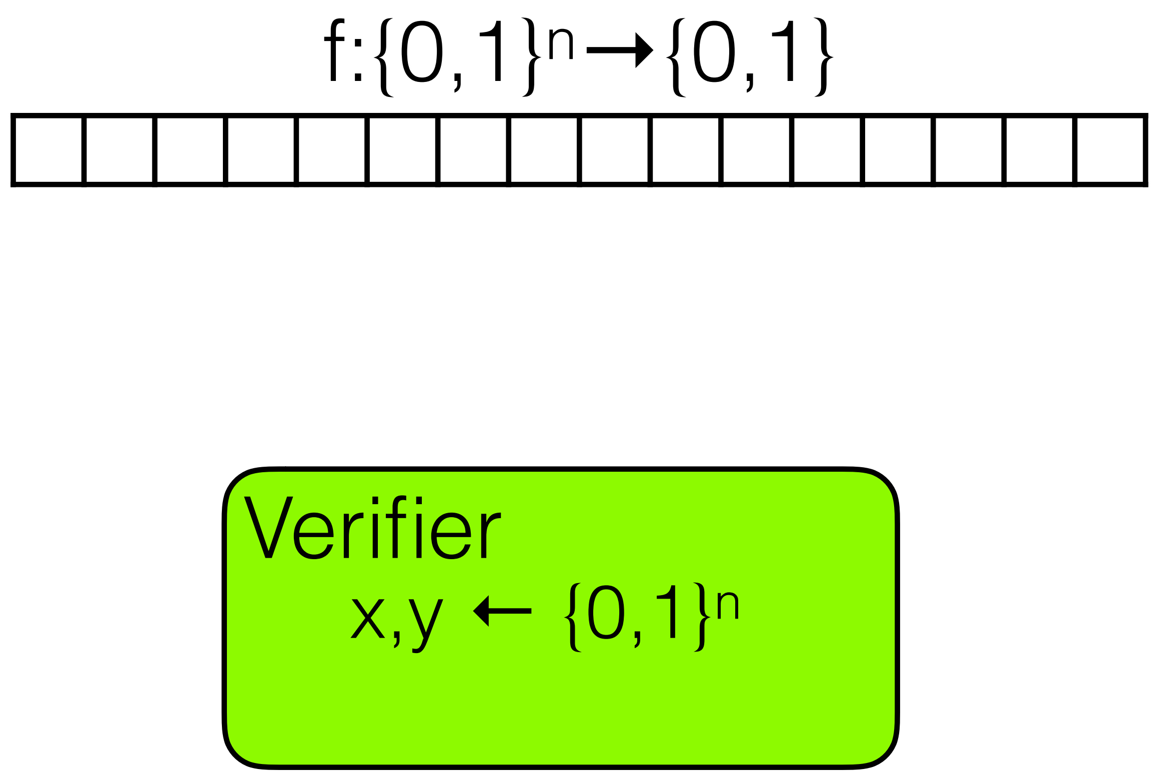
Linearity Testing

Given oracle access to $f:\{0,1\}^n \rightarrow \{0,1\}$ decide if:

(1) f is linear, **or**

(2) f is far from all linear functions.

A simple and natural test:



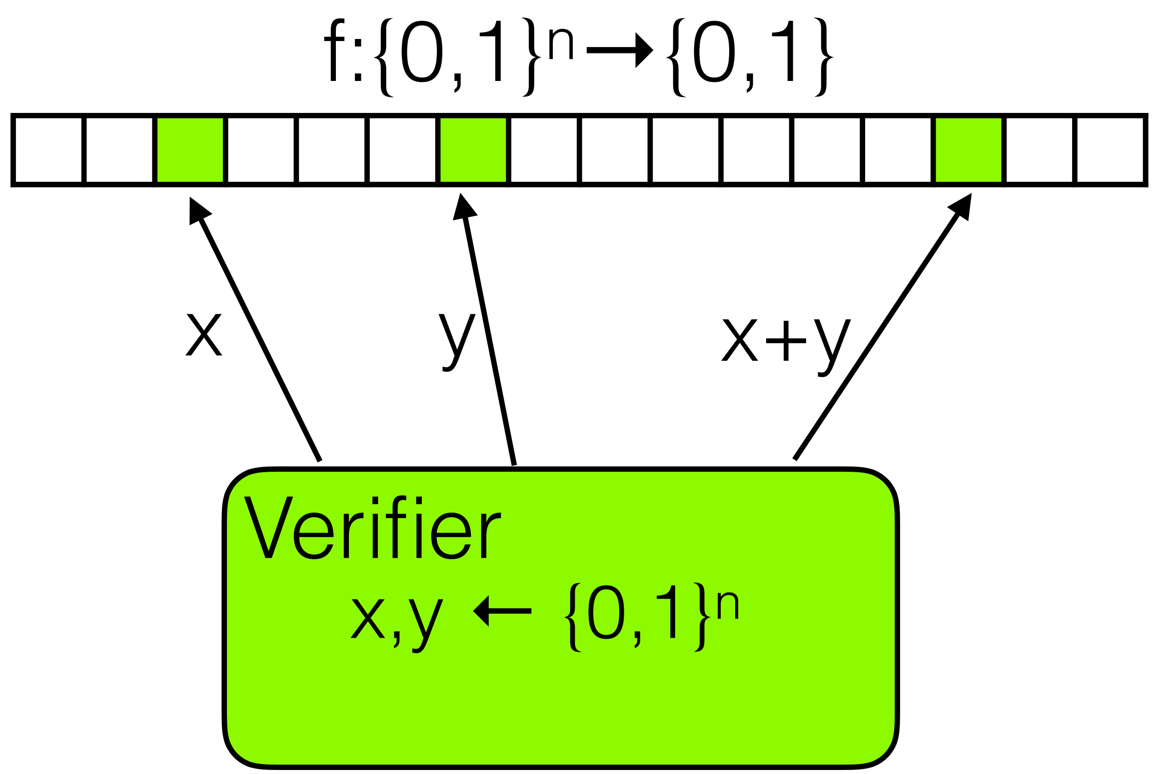
Linearity Testing

Given oracle access to $f:\{0,1\}^n \rightarrow \{0,1\}$ decide if:

(1) f is linear, **or**

(2) f is far from all linear functions.

A simple and natural test:



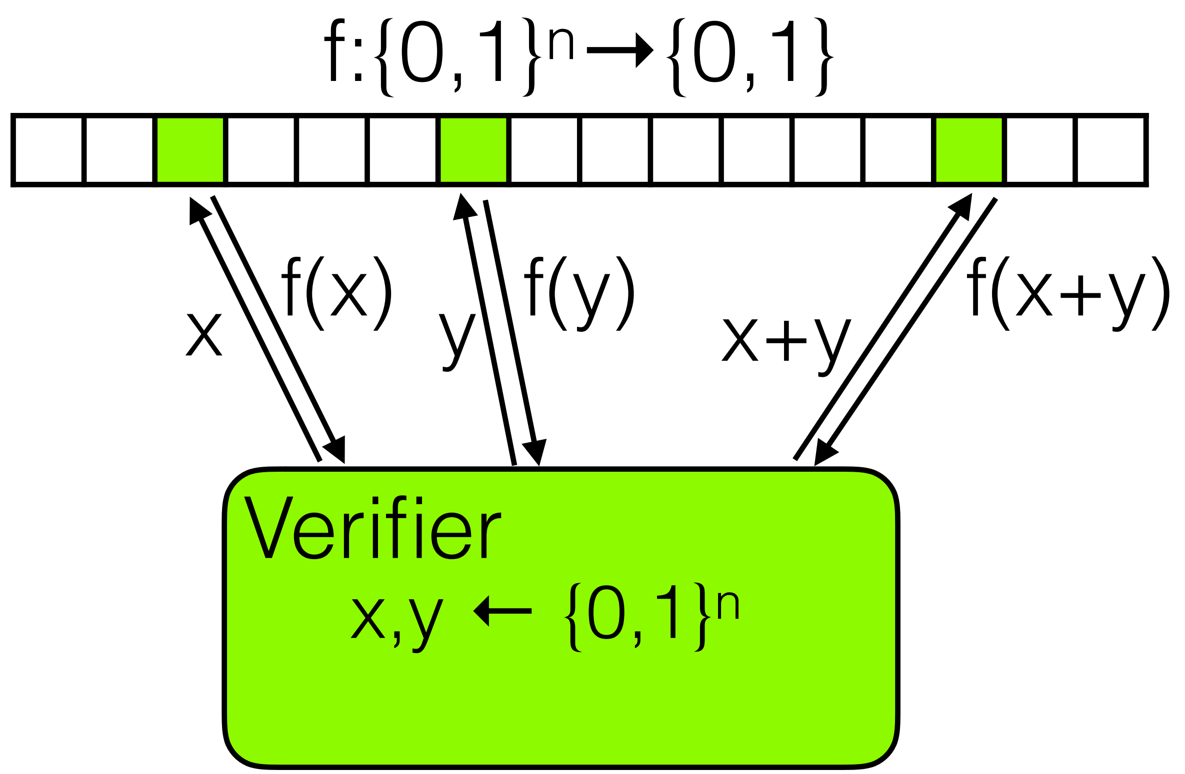
Linearity Testing

Given oracle access to $f:\{0,1\}^n \to \{0,1\}$ decide if:

(1) f is linear, **or**

(2) f is far from all linear functions.

A simple and natural test:



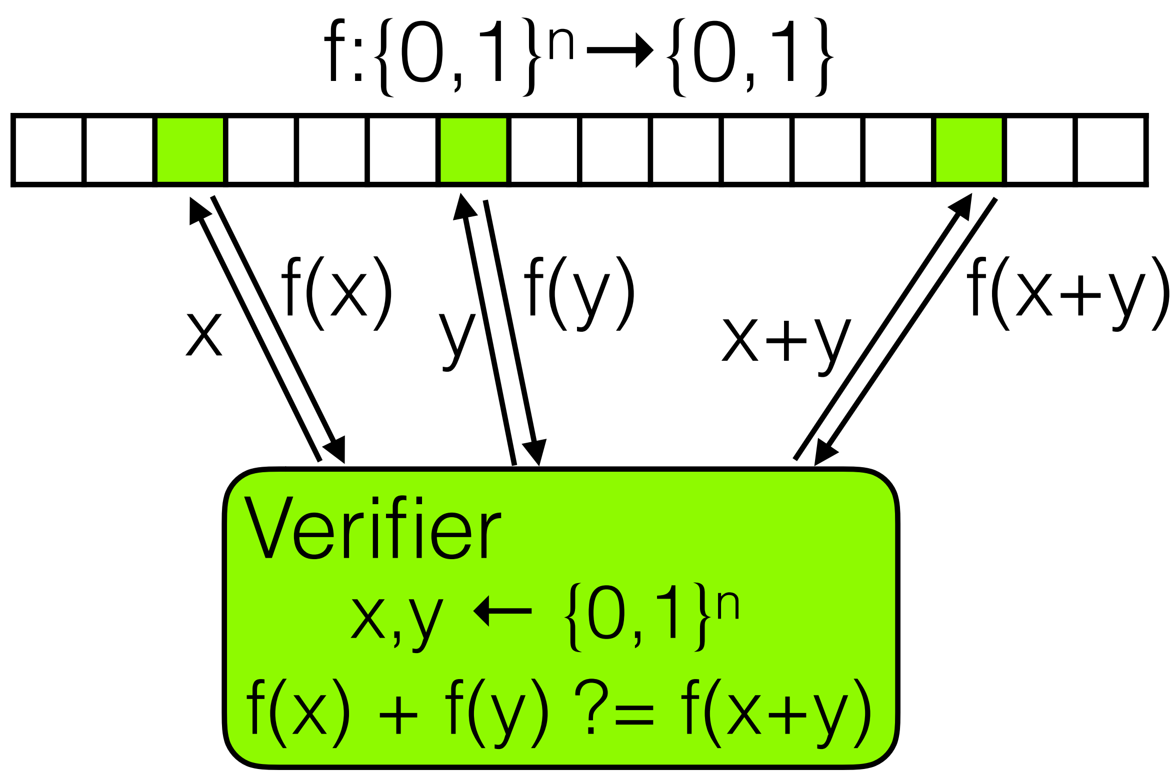
Linearity Testing

Given oracle access to $f:\{0,1\}^n \to \{0,1\}$ decide if:

(1) f is linear, **or**

(2) f is far from all linear functions.

A simple and natural test:



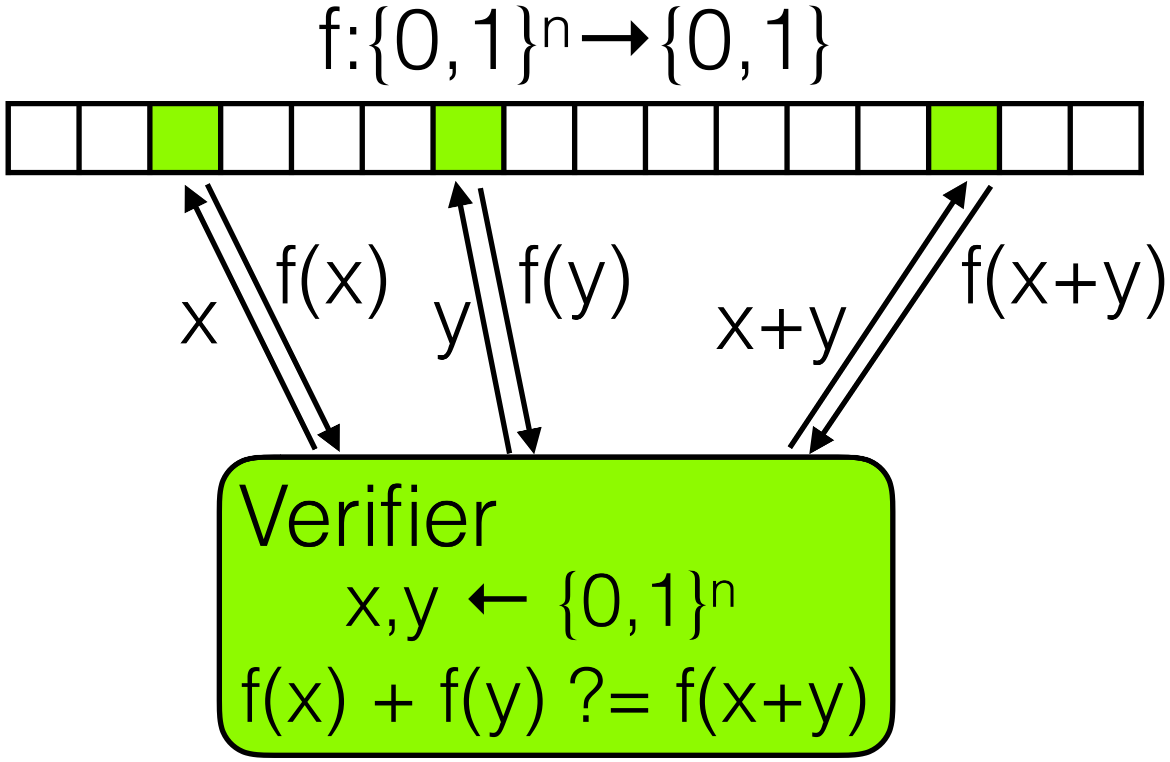
Linearity Testing

Given oracle access to $f:\{0,1\}^n \rightarrow \{0,1\}$ decide if:

(1) f is linear, **or**

(2) f is far from all linear functions.

A simple and natural test:



The test works:

$\Pr_{x,y}[\text{f passes}] \geq 1 - \varepsilon \rightarrow \Delta(f, \text{LIN}) \leq \varepsilon$ [BLR93, BCHKS96]

What are non-signaling strategies?

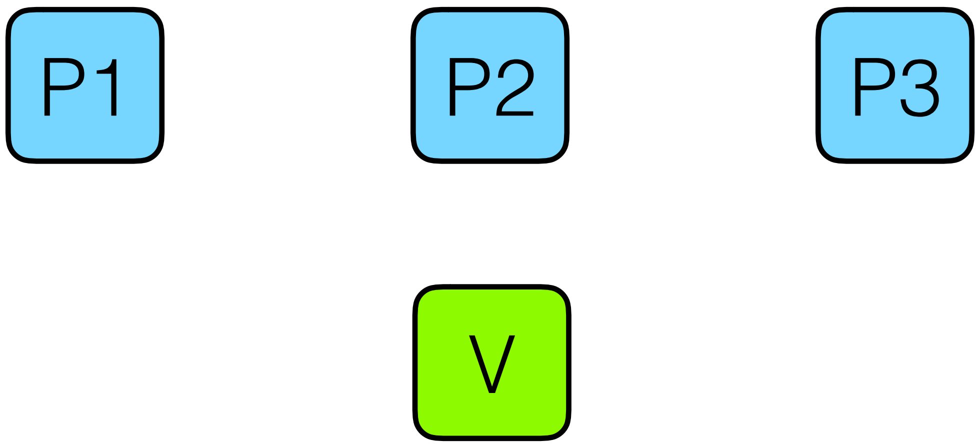
Non-Signaling Strategies

Non-Signaling Strategies

Multiplayer games:

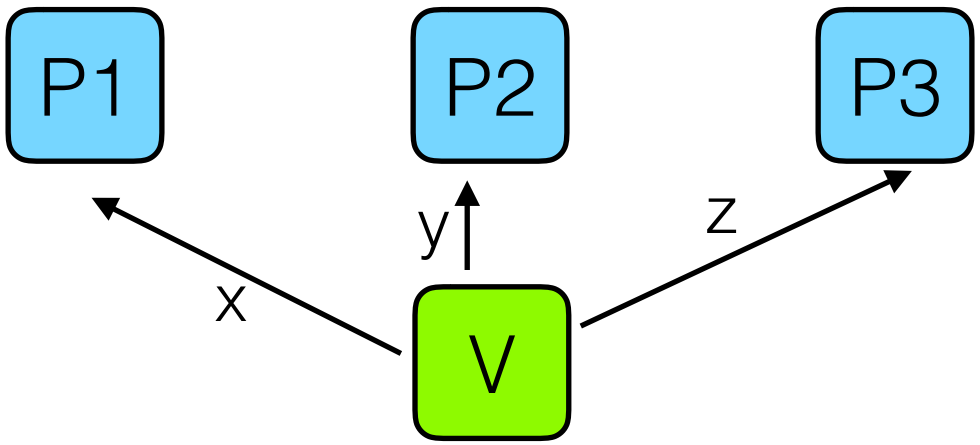
Non-Signaling Strategies

Multiplayer games:



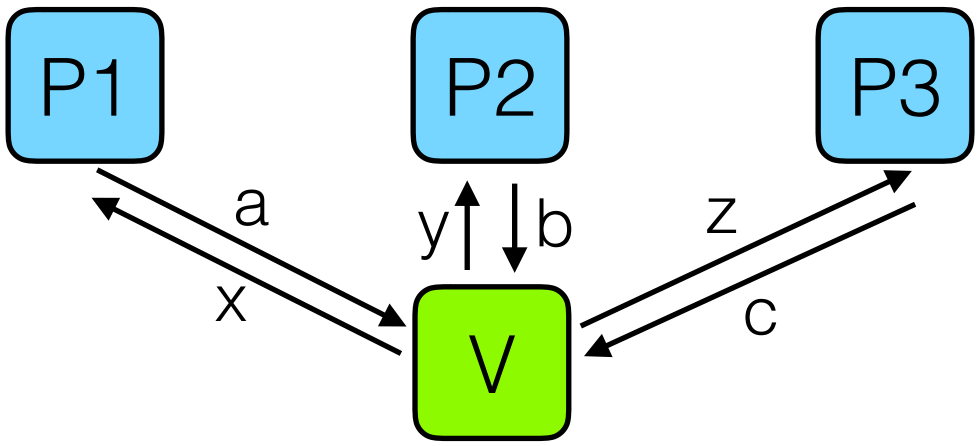
Non-Signaling Strategies

Multiplayer games:



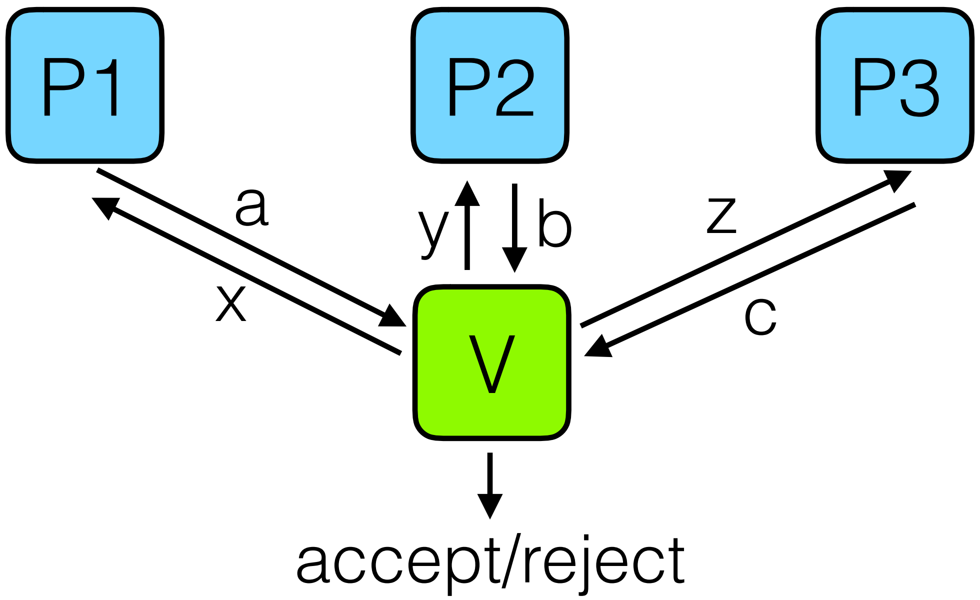
Non-Signaling Strategies

Multiplayer games:



Non-Signaling Strategies

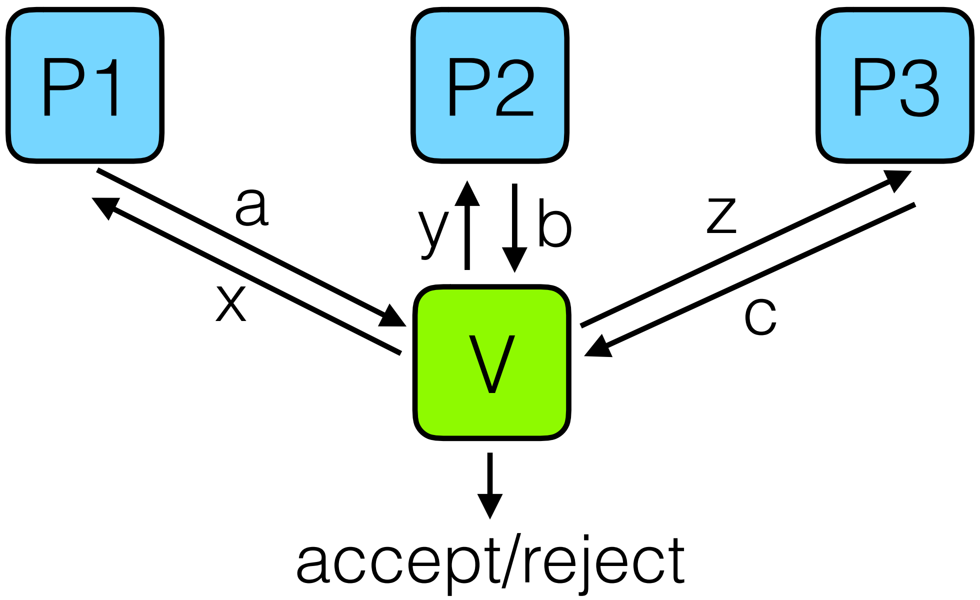
Multiplayer games:



Non-Signaling Strategies

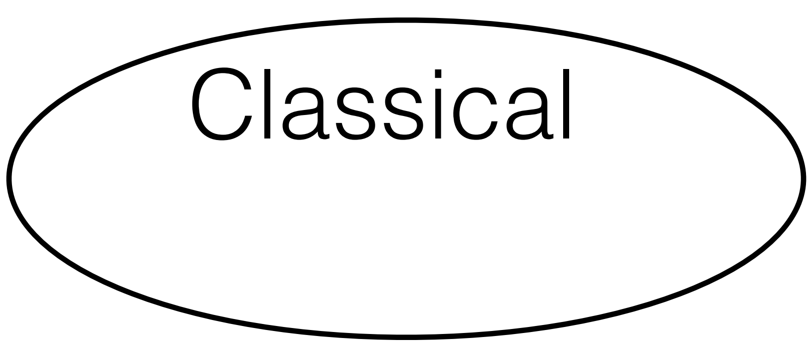
Classes of players:

Multiplayer games:

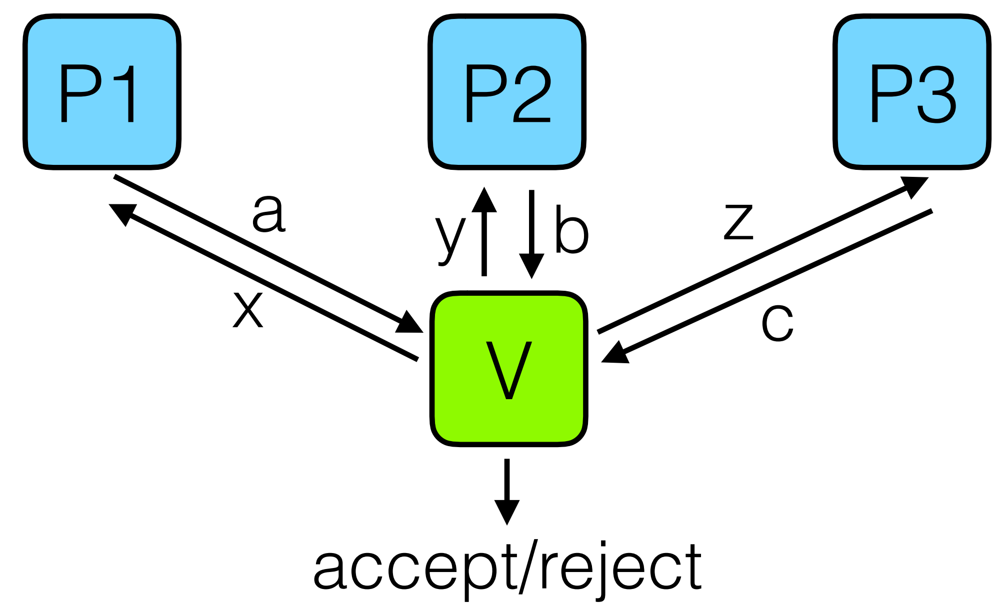


Non-Signaling Strategies

Classes of players:



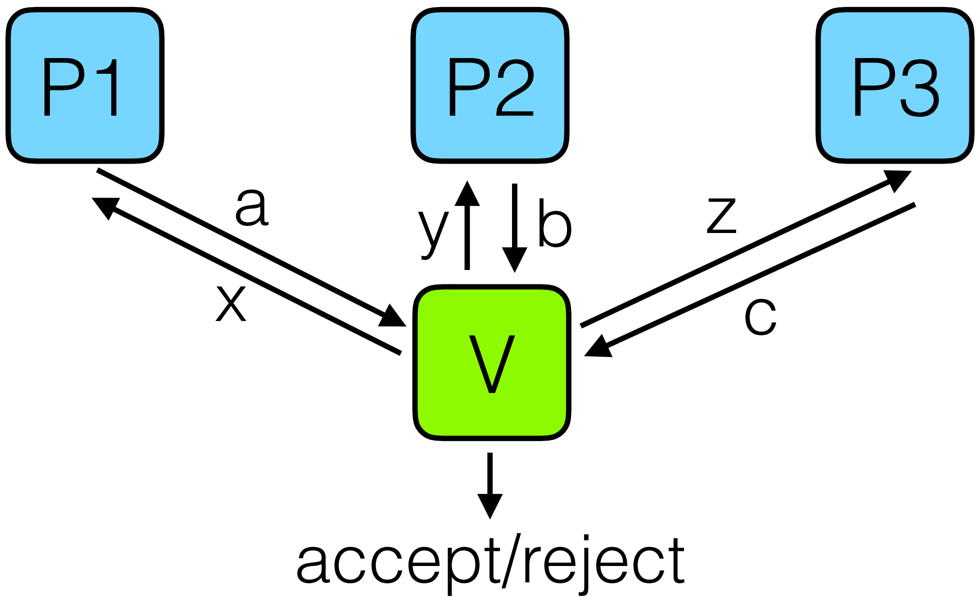
Multiplayer games:



Non-Signaling Strategies

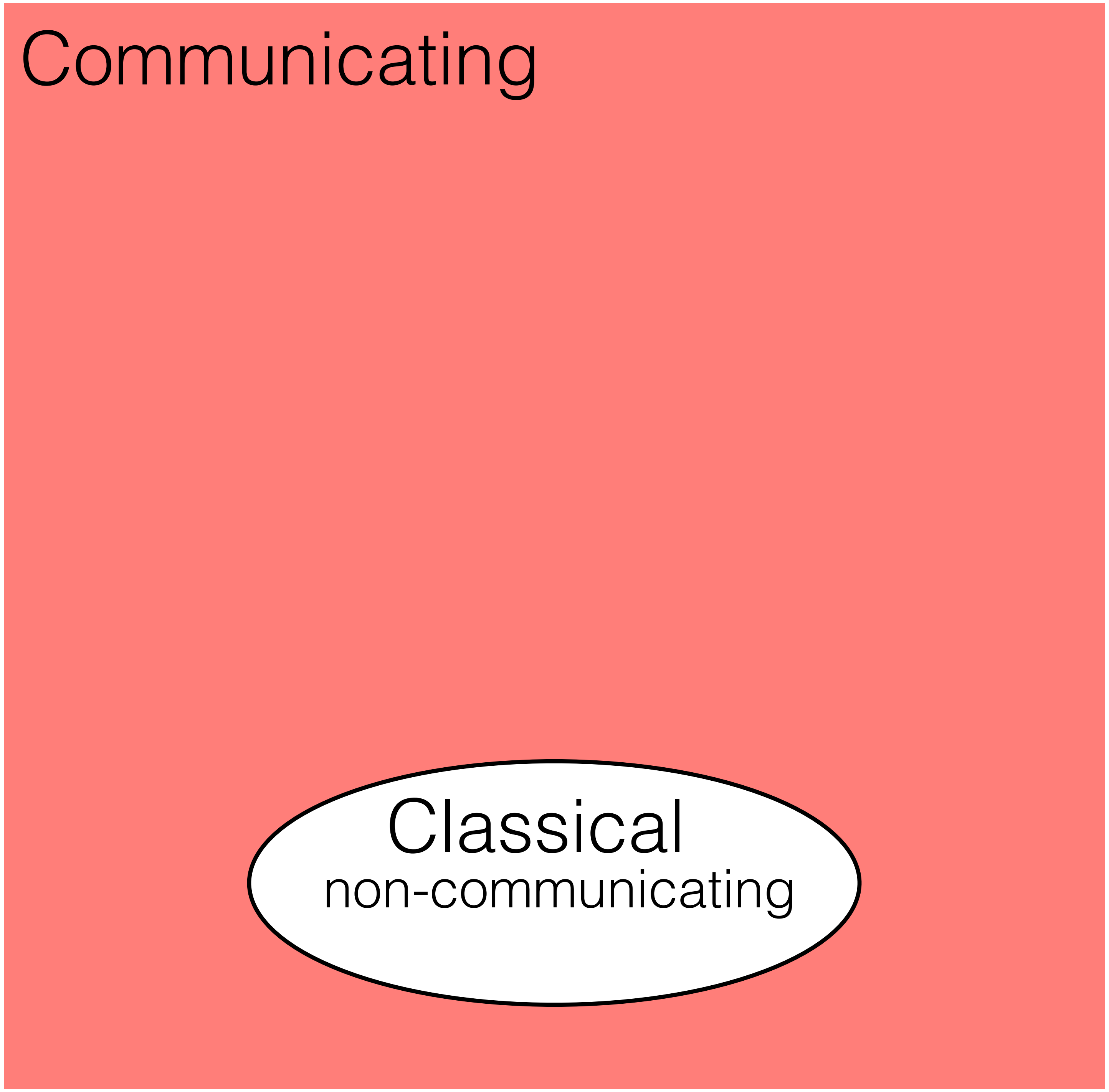
Classes of players:

Multiplayer games:

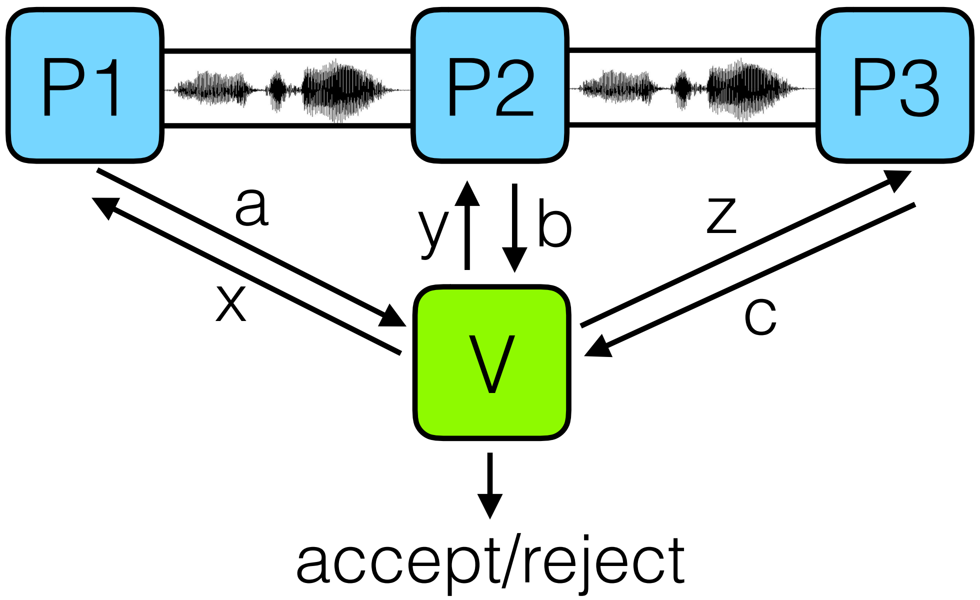


Non-Signaling Strategies

Classes of players:

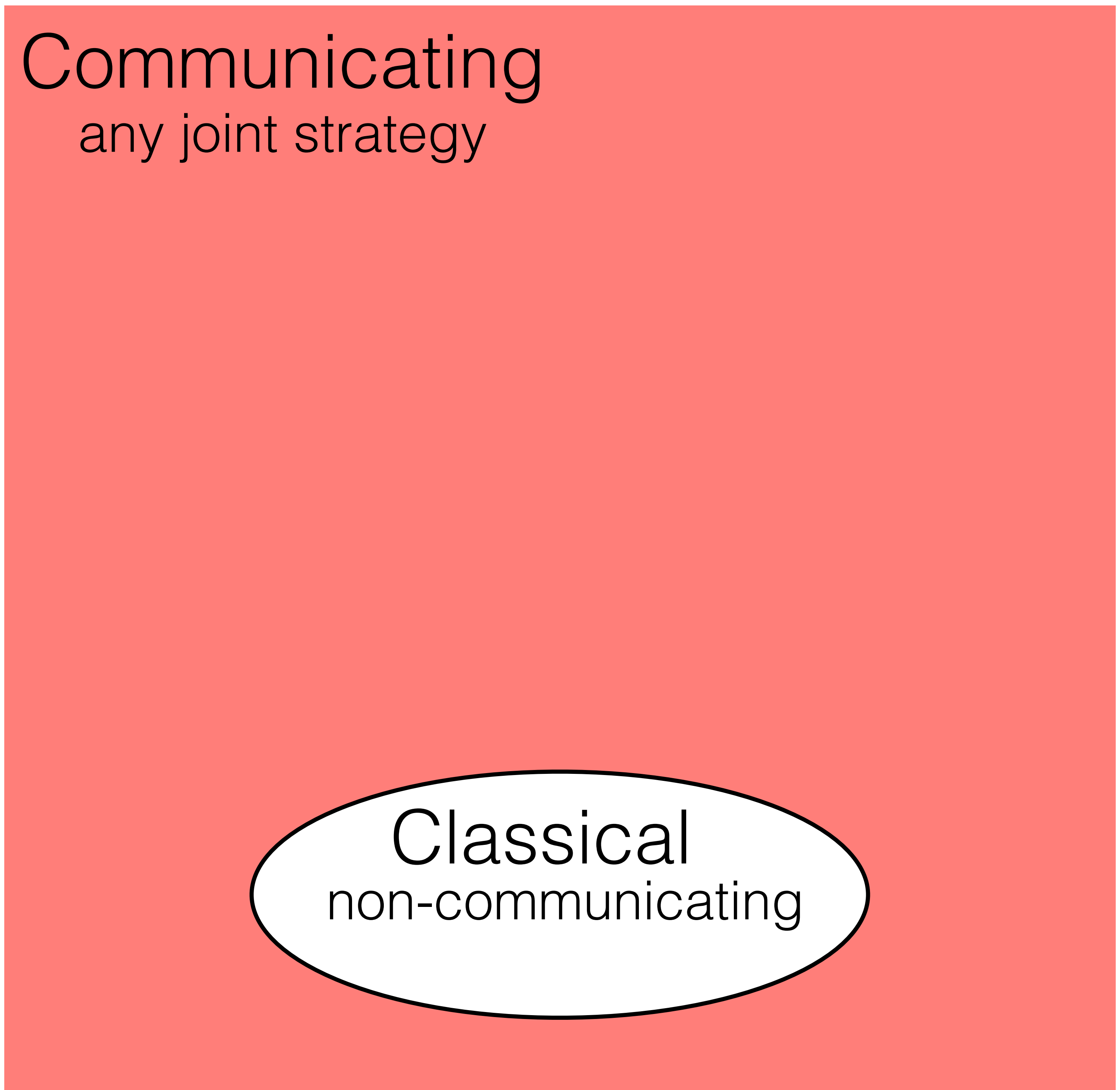


Multiplayer games:

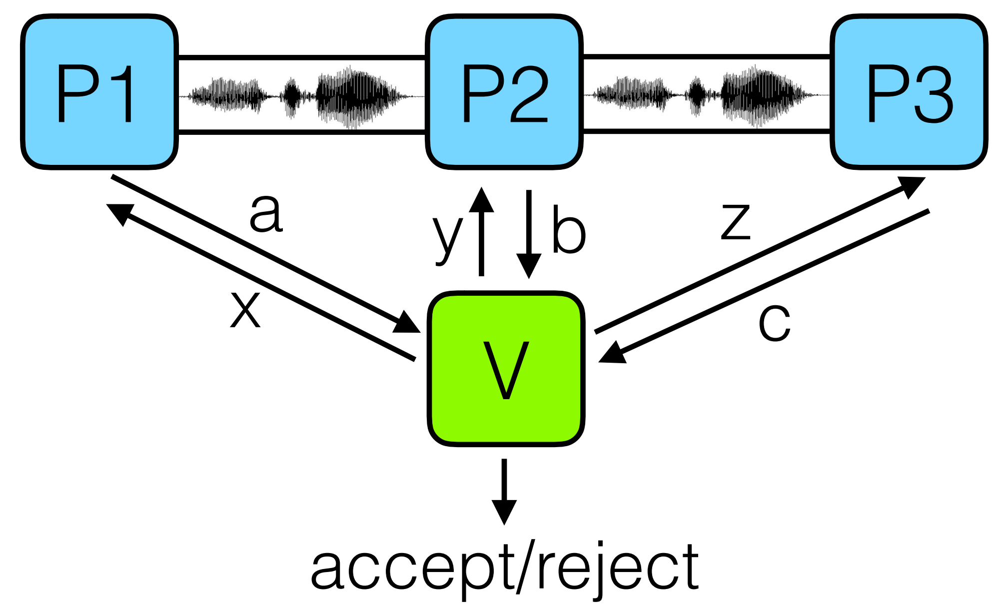


Non-Signaling Strategies

Classes of players:

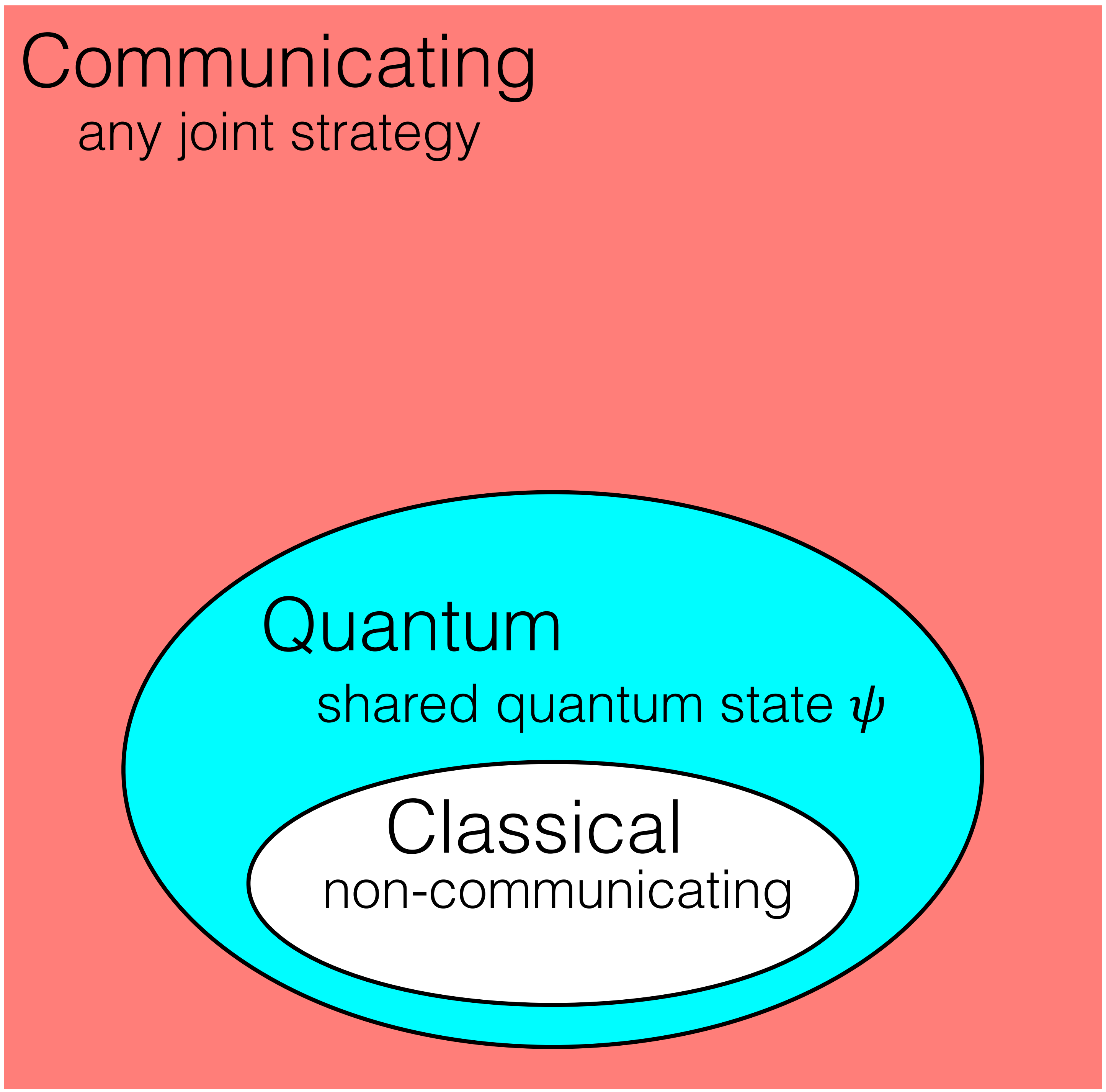


Multiplayer games:

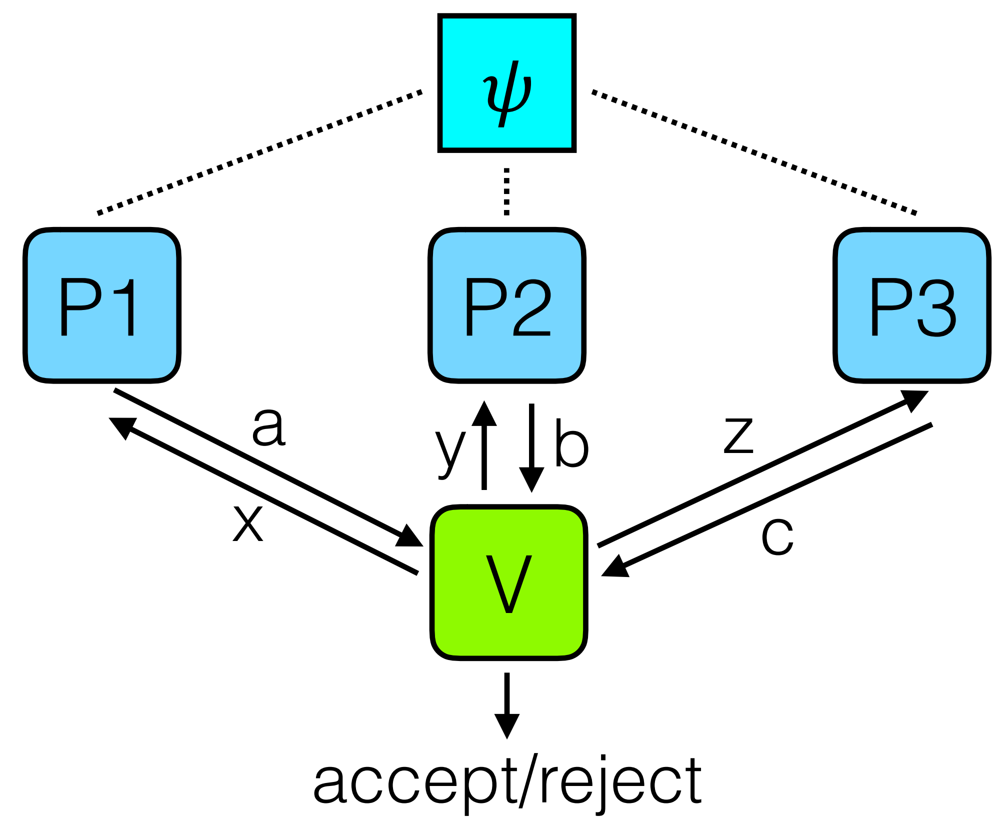


Non-Signaling Strategies

Classes of players:

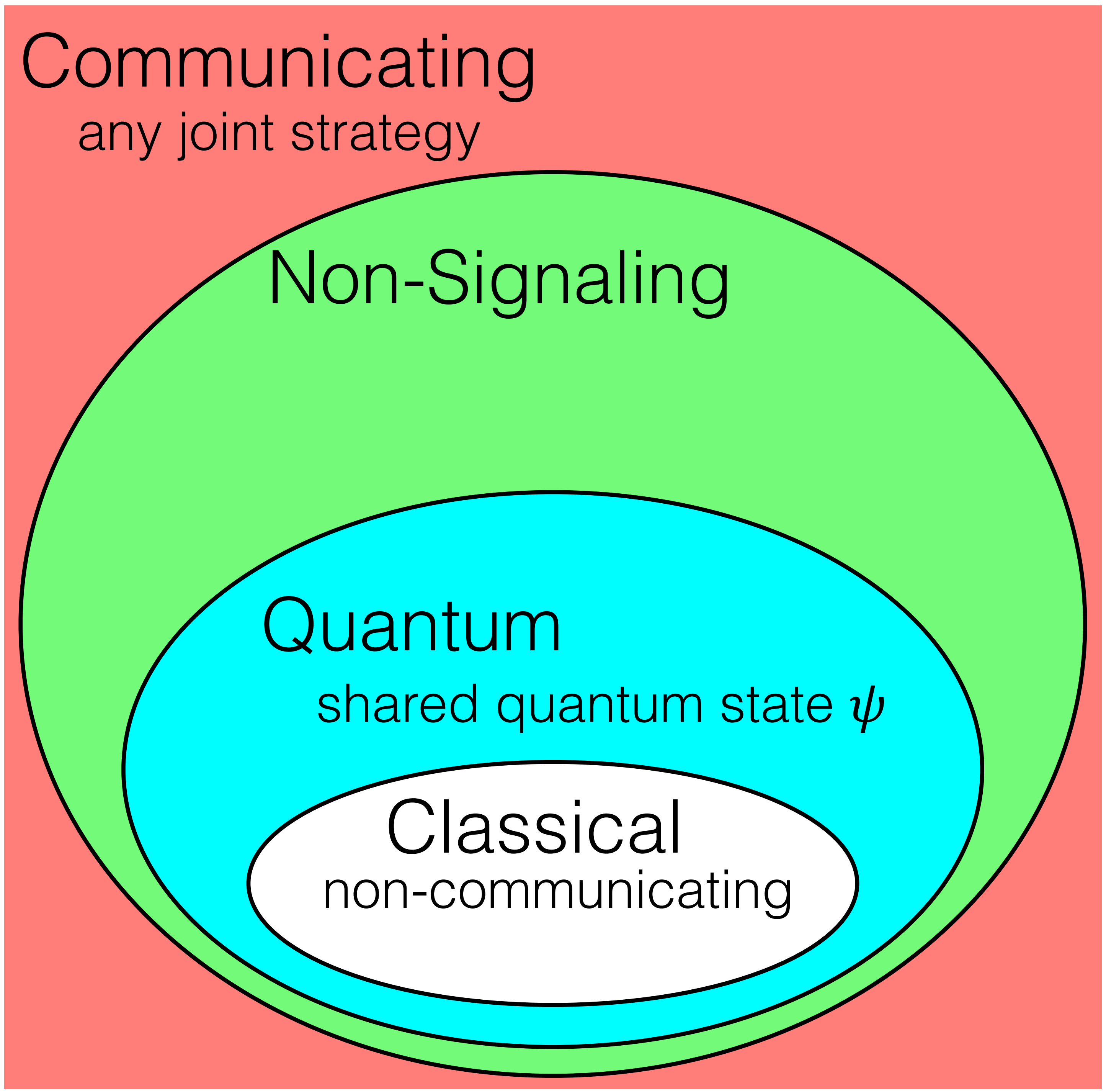


Multiplayer games:

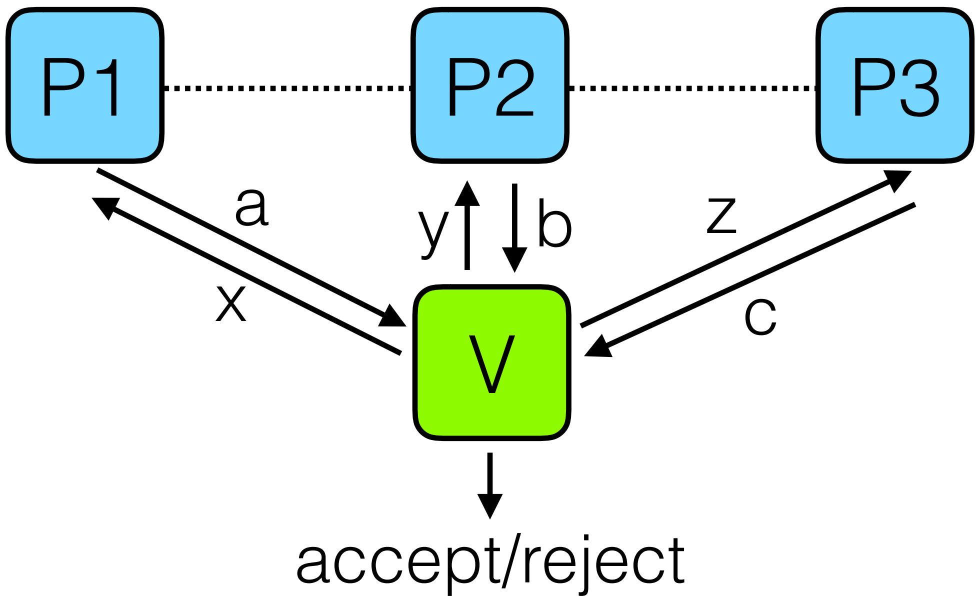


Non-Signaling Strategies

Classes of players:

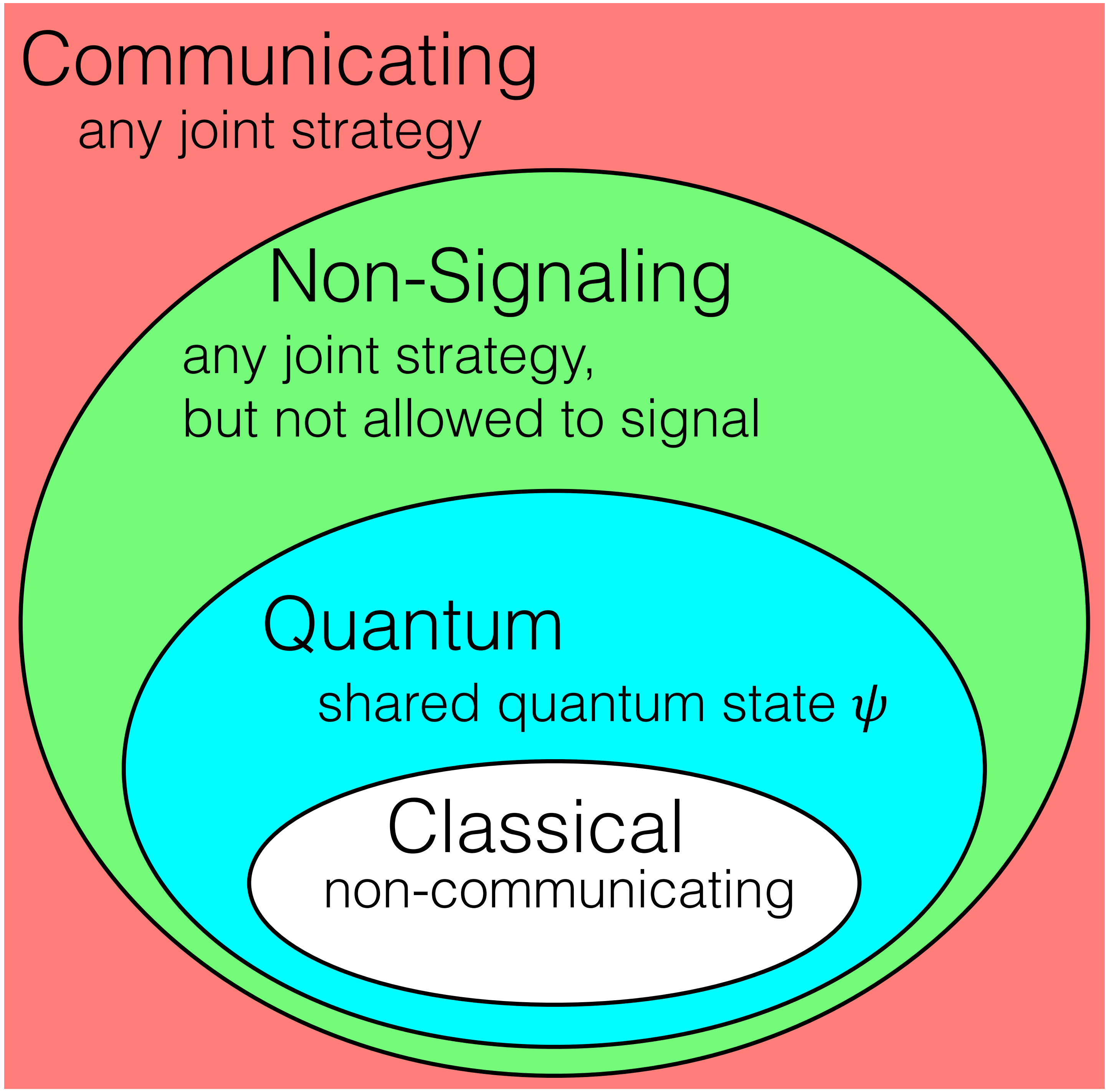


Multiplayer games:

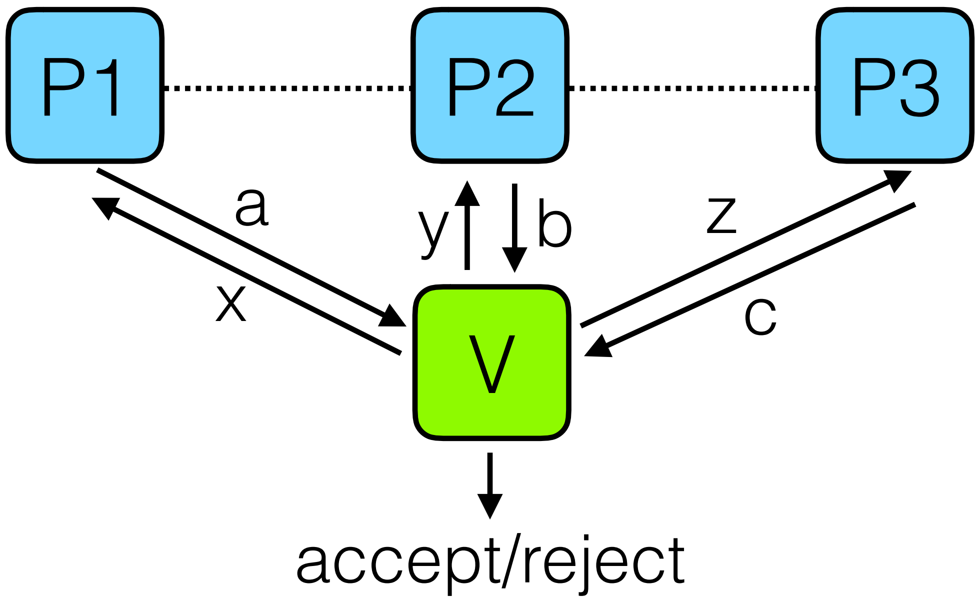


Non-Signaling Strategies

Classes of players:



Multiplayer games:



Why non-signaling?

Why non-signaling?

One can study **nsMIPs** (MIPs sound against ns strategies)

Why non-signaling?

One can study **nsMIPs** (MIPs sound against ns strategies)

(1) applications to cryptography

Why non-signaling?

One can study **nsMIPs** (MIPs sound against ns strategies)

(1) applications to cryptography

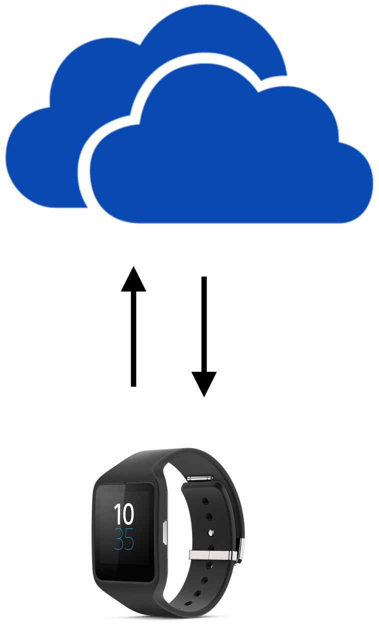
nsMIP + crypto

Why non-signaling?

One can study **nsMIPs** (MIPs sound against ns strategies)

(1) applications to cryptography

nsMIP + crypto → [KRR13] → 1 round delegation of computation from LWE

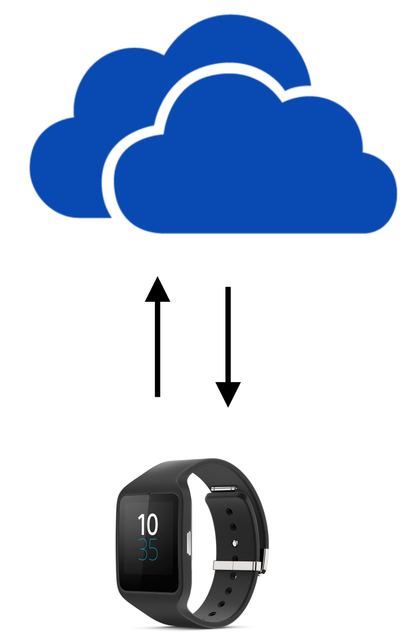


Why non-signaling?

One can study **nsMIPs** (MIPs sound against ns strategies)

(1) applications to cryptography

nsMIP + crypto —[KRR13]→ 1 round delegation of computation from LWE



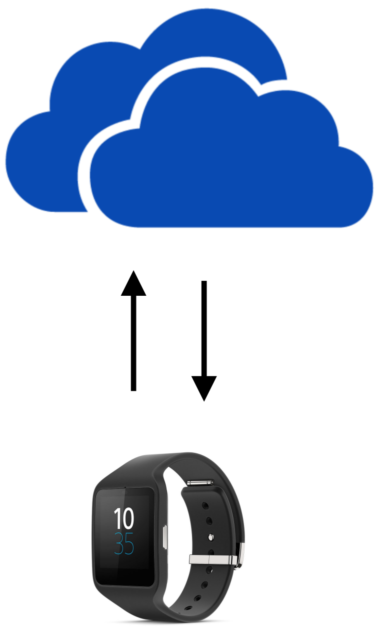
(2) applications to complexity

Why non-signaling?

One can study **nsMIPs** (MIPs sound against ns strategies)

(1) applications to cryptography

nsMIP + crypto → [KRR13] 1 round delegation of computation from LWE



(2) applications to complexity

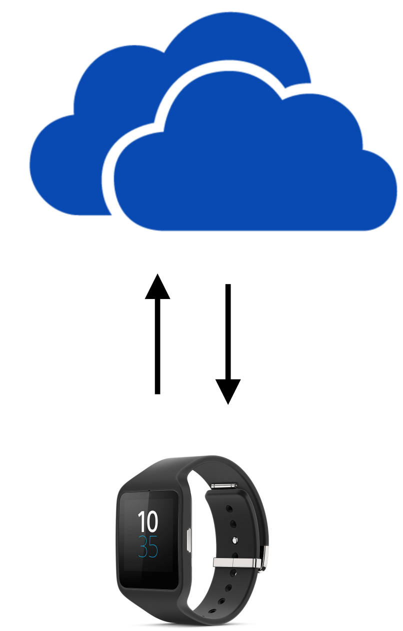
nsMIP

Why non-signaling?

One can study **nsMIPs** (MIPs sound against ns strategies)

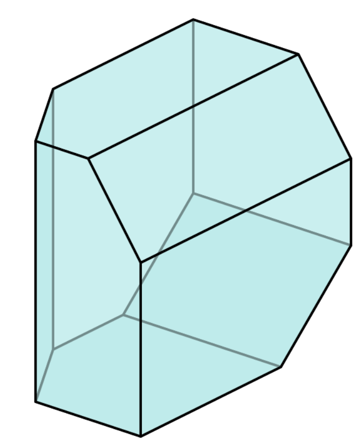
(1) applications to cryptography

nsMIP + crypto —[KRR13]→ 1 round delegation of computation from LWE



(2) applications to complexity

nsMIP —[KRR14]→ hardness of approximation for LPs in bounded space

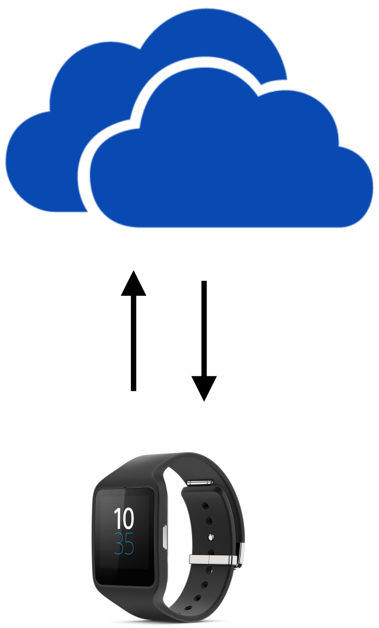


Why non-signaling?

One can study **nsMIPs** (MIPs sound against ns strategies)

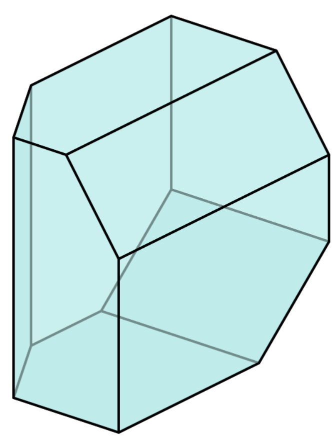
(1) applications to cryptography

nsMIP + crypto → [KRR13] → 1 round delegation of computation from LWE



(2) applications to complexity

nsMIP → [KRR14] → hardness of approximation for LPs in bounded space



BUT: current nsMIP constructions appear *sub-optimal*

State of Affairs

State of Affairs

Standard MIPs

PCP Theorem:
[AS98] [ALMSS98]

$$\mathsf{NEXP} = \mathsf{MIP}\left[\begin{array}{rl} \text{randomness} = & \text{poly} \\ \text{num players} = & \mathrm{O}(1) \end{array}\right]$$

State of Affairs

Standard MIPs

PCP Theorem:
[AS98] [ALMSS98]

$$\mathsf{NEXP} = \mathsf{MIP}\left[\begin{array}{rl} \text{randomness} = & \text{poly} \\ \text{num players} = & \mathrm{O}(1) \end{array}\right]$$

Non-signaling MIPs

[KRR13]:

$$\mathsf{EXP} = \mathsf{nsMIP}\left[\begin{array}{rl} \text{randomness} = & \text{poly} \\ \text{num players} = & \text{poly} \end{array}\right]$$

State of Affairs

Standard MIPs

PCP Theorem:
[AS98] [ALMSS98]

$$\mathsf{NEXP} = \mathsf{MIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & O(1) \end{bmatrix}$$

Non-signaling MIPs

[KRR13]:

$$\mathsf{EXP} = \mathsf{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & \text{poly} \end{bmatrix}$$

[Ito10]:

$$\mathsf{PSPACE} = \mathsf{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & 2 \end{bmatrix}$$

State of Affairs

Standard MIPs

PCP Theorem:
[AS98] [ALMSS98]

$$\mathsf{NEXP} = \mathsf{MIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & O(1) \end{bmatrix}$$

Non-signaling MIPs

[KRR13]:

$$\mathsf{EXP} = \mathsf{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & \text{poly} \end{bmatrix}$$

[Ito10]:

$$\mathsf{PSPACE} = \mathsf{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & 2 \end{bmatrix}$$

State of Affairs

Standard MIPs

PCP Theorem: [AS98] [ALMSS98]

$$\mathsf{NEXP} = \mathsf{MIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & O(1) \end{bmatrix}$$

Non-signaling MIPs

[KRR13]:

$$\mathsf{EXP} = \mathsf{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & \text{poly} \end{bmatrix}$$

[Ito10]:

$$\mathsf{PSPACE} = \mathsf{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & 2 \end{bmatrix}$$

Fundamental question:

Is there a nsPCP Theorem?

State of Affairs

Standard MIPs

PCP Theorem: [AS98] [ALMSS98]

$$\text{NEXP} = \text{MIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & O(1) \end{bmatrix}$$

Non-signaling MIPs

[KRR13]:

$$\text{EXP} = \text{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & \text{poly} \end{bmatrix}$$

[Ito10]:

$$\text{PSPACE} = \text{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & 2 \end{bmatrix}$$

Fundamental question:

Is there a nsPCP Theorem?

Namely, does $\text{EXP} = \text{nsMIP}\begin{bmatrix} \text{randomness} = & \text{poly} \\ \text{num players} = & O(1) \end{bmatrix}$?

Why non-signaling linearity testing?

Why non-signaling linearity testing?

In classical setting,

Property Testing + Modularity/ Abstraction → More efficient PCPs

Why non-signaling linearity testing?

In classical setting,

Property Testing + Modularity/Abstraction → More efficient PCPs

And also in the quantum setting! [IV12] [Vid13] [NV18]

Why non-signaling linearity testing?

In classical setting,

Property Testing + Modularity/ Abstraction → More efficient PCPs

And also in the quantum setting! [IV12] [Vid13] [NV18]

In non-signaling setting,

No property testing results are known!

Why non-signaling linearity testing?

In classical setting,

Property Testing + Modularity/ Abstraction → More efficient PCPs

And also in the quantum setting! [IV12] [Vid13] [NV18]

In non-signaling setting,

No property testing results are known!

We start with linearity testing

Why non-signaling linearity testing?

In classical setting,

Property Testing + Modularity/Abstraction → More efficient PCPs

And also in the quantum setting! [IV12] [Vid13] [NV18]

In non-signaling setting,

No property testing results are known!

We start with linearity testing

Best-understood case in classical setting

Non-Signaling Functions

Non-Signaling Functions

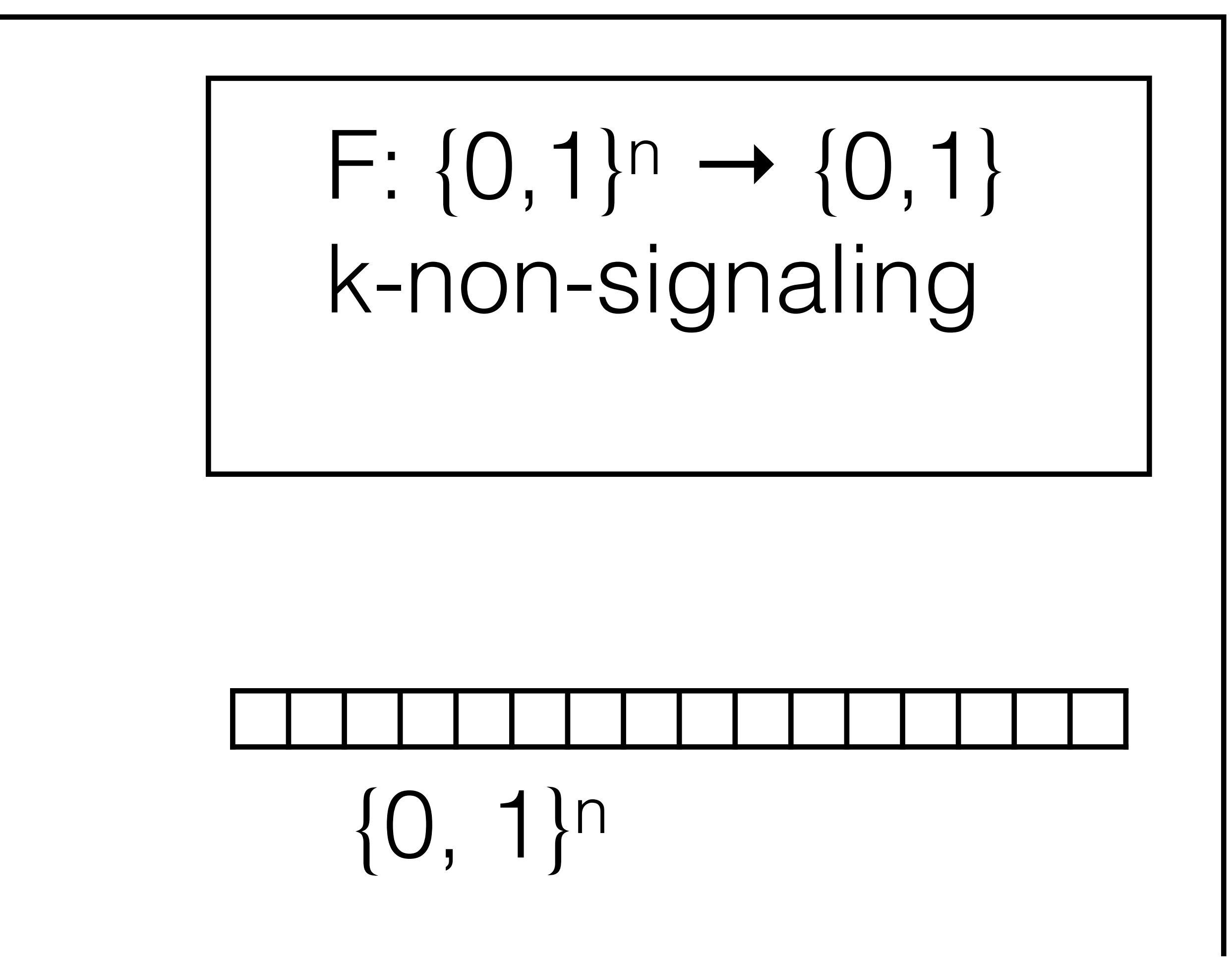
Definition:

A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall\, S \subseteq \{0, 1\}^n$, $|S| \leq k$

Non-Signaling Functions

Definition:

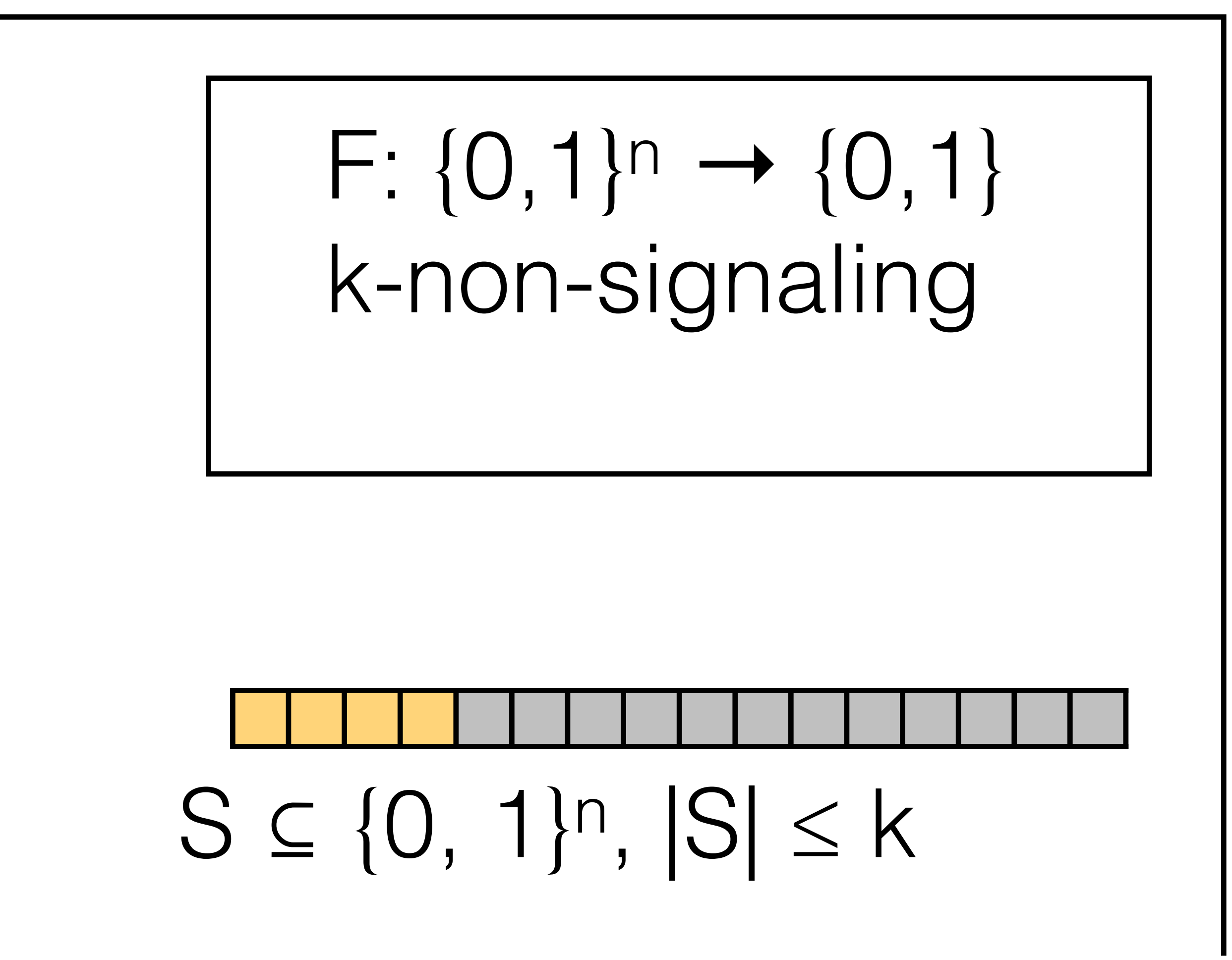
A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall\, S \subseteq \{0, 1\}^n$, $|S| \leq k$



Non-Signaling Functions

Definition:

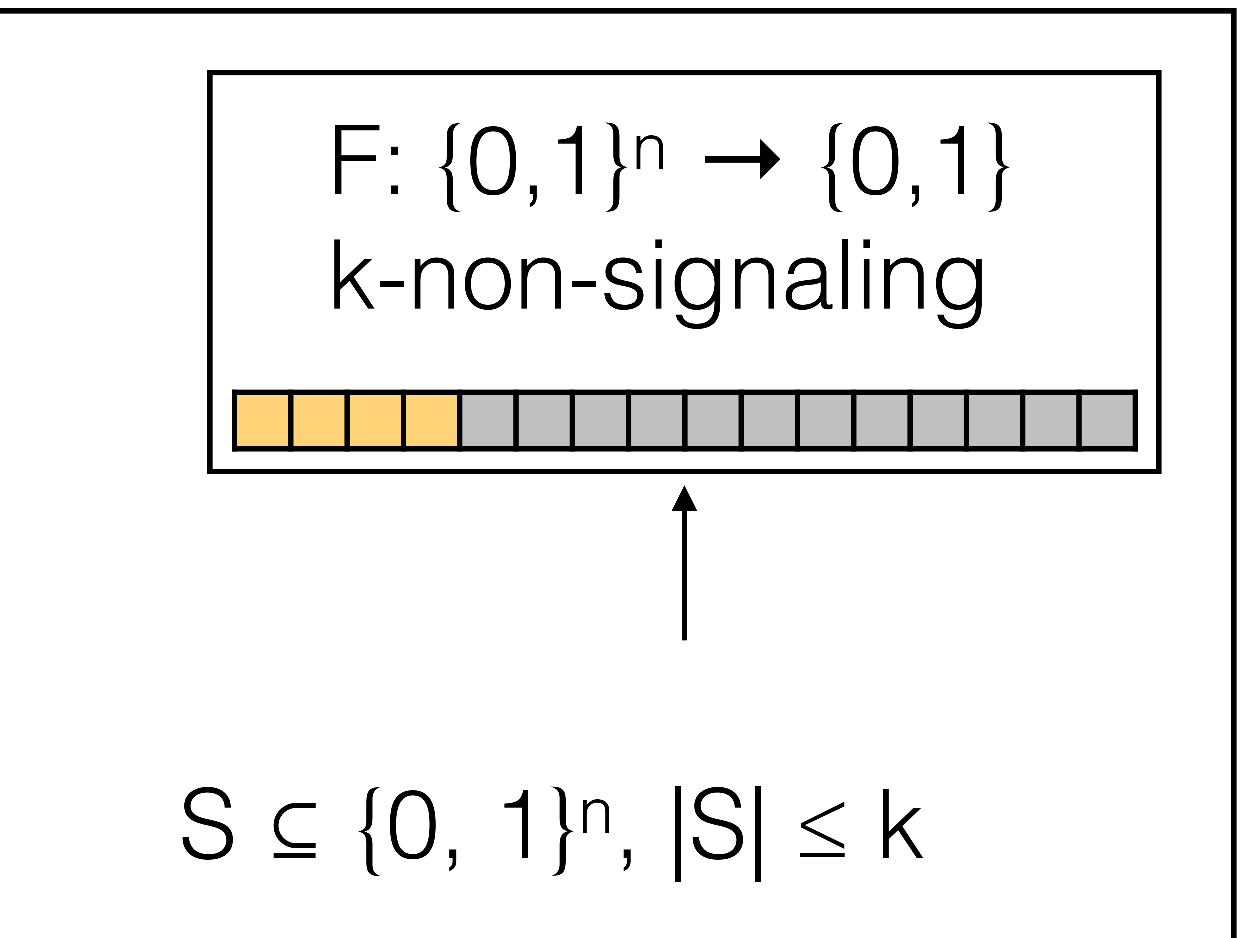
A k-non-signaling function F: $\{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions f: $S \rightarrow \{0,1\}$, $\forall S \subseteq \{0,1\}^n$, $|S| \leq k$



Non-Signaling Functions

Definition:

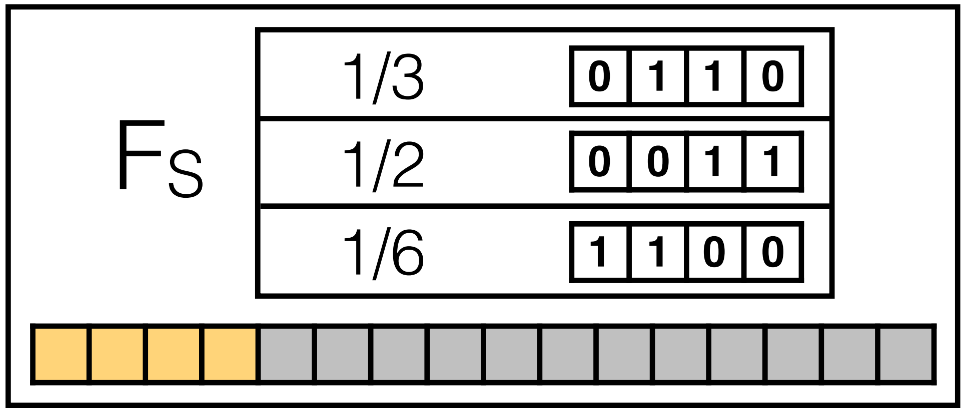
A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall\, S \subseteq \{0, 1\}^n$, $|S| \leq k$



Non-Signaling Functions

Definition:

A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall S \subseteq \{0, 1\}^n$, $|S| \leq k$

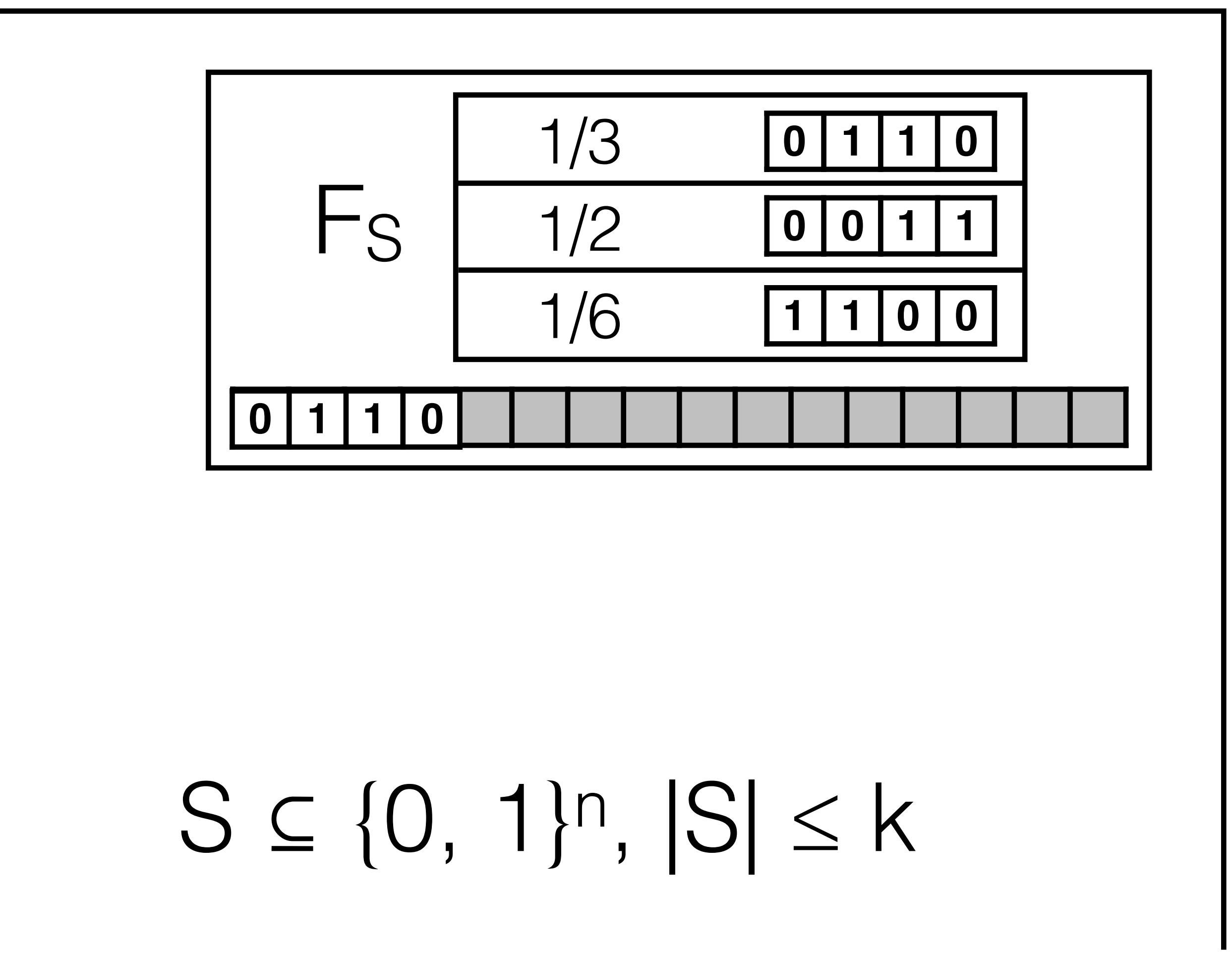


$S \subseteq \{0, 1\}^n$, $|S| \leq k$

Non-Signaling Functions

Definition:

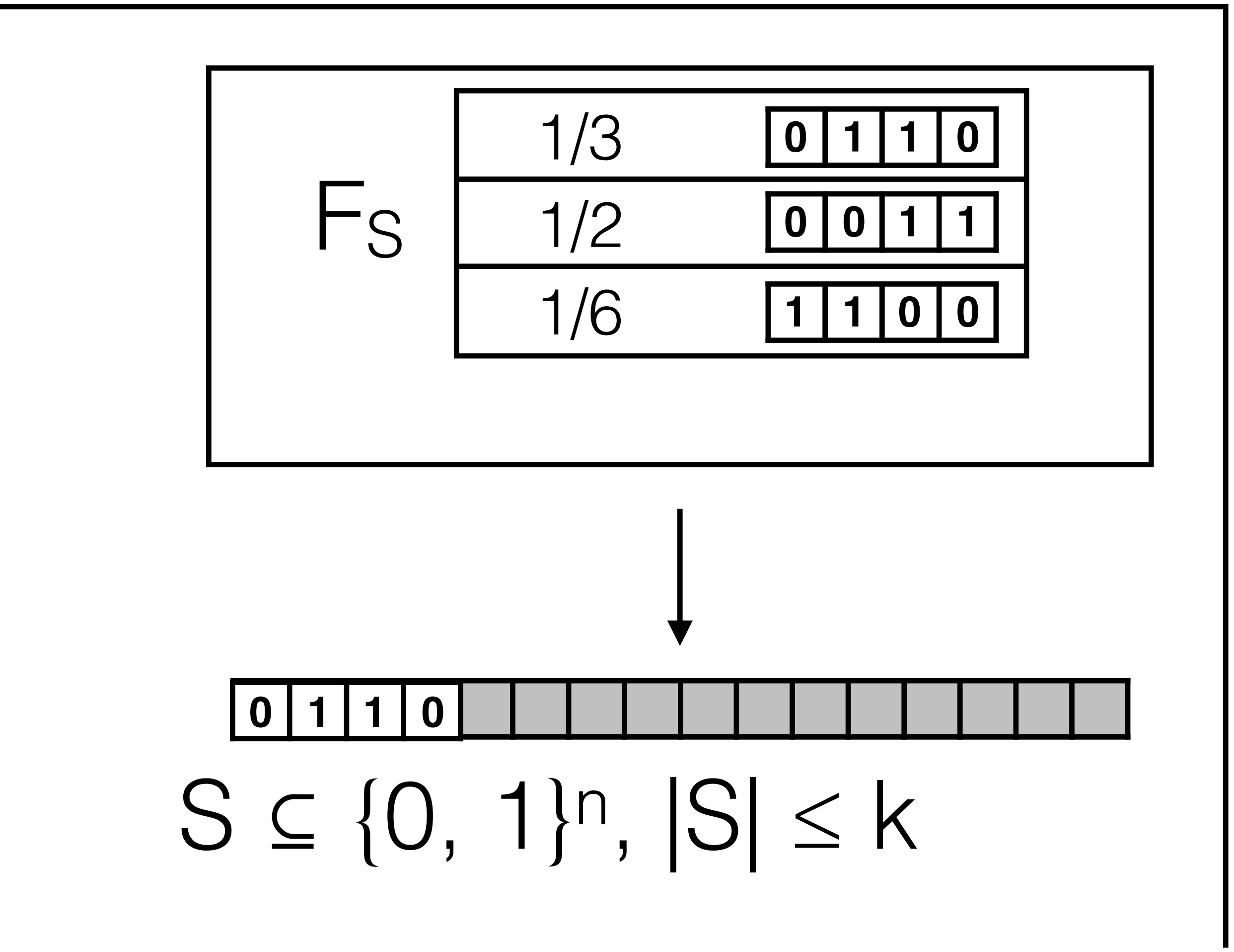
A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall S \subseteq \{0, 1\}^n$, $|S| \leq k$



Non-Signaling Functions

Definition:

A k-non-signaling function $F: \{0,1\}^n \to \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \to \{0,1\}$, $\forall\, S \subseteq \{0, 1\}^n$, $|S| \leq k$



Non-Signaling Functions

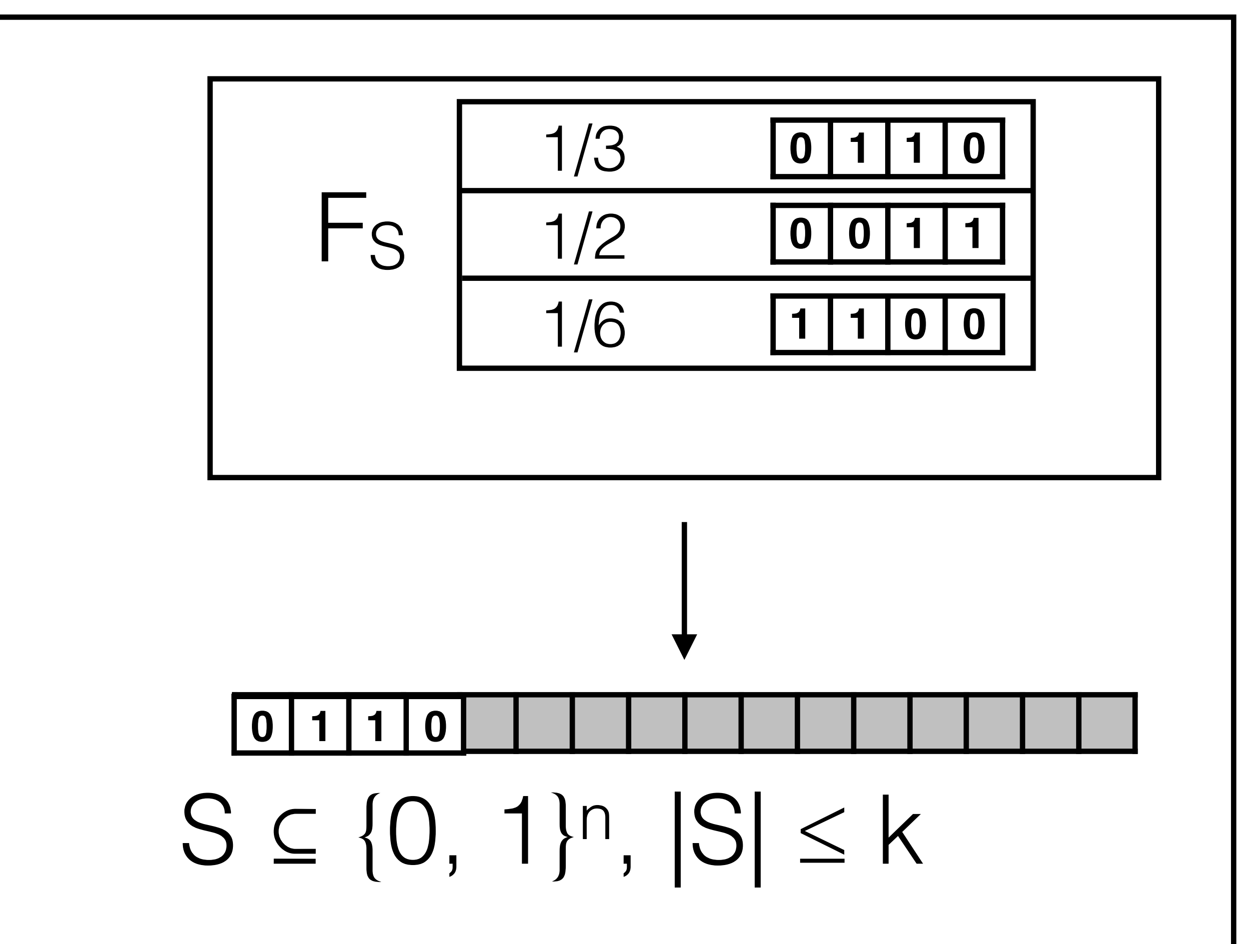
Definition:

A k-non-signaling function $F: \{0,1\}^n \to \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \to \{0,1\}$, $\forall S \subseteq \{0, 1\}^n, |S| \leq k$ that satisfies the **non-signaling property:**

$$\forall S, T \subseteq \{0, 1\}^n, |S|, |T| \leq k$$

$$F_S|_{S \cap T} \equiv F_T|_{S \cap T}$$

(the marginal distributions are equal)



Non-Signaling Functions

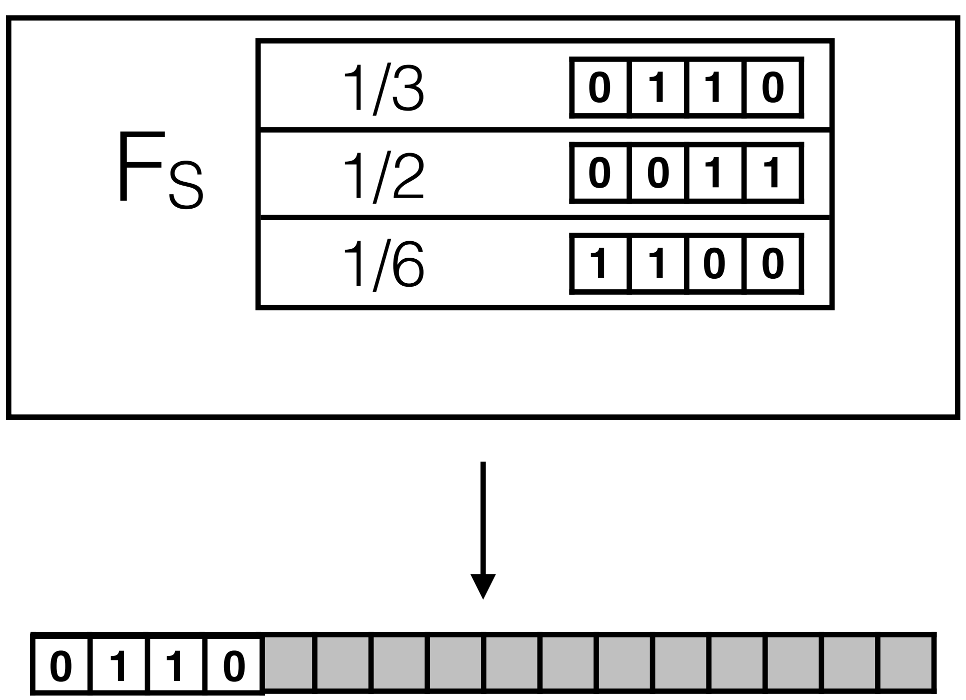
Definition:

A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall S \subseteq \{0, 1\}^n, |S| \leq k$ that satisfies the **non-signaling property:**

$$\forall S, T \subseteq \{0, 1\}^n, |S|, |T| \leq k$$

$$F_S|_{S \cap T} \equiv F_T|_{S \cap T}$$

(the marginal distributions are equal)



$S \subseteq \{0, 1\}^n, |S| \leq k$

1/3	0 1 1 0
1/2	0 0 1 1
1/6	1 1 0 0

F_S

1/3	1 0 0 1
1/2	1 1 1 1
1/6	0 0 0 0

F_T

Non-Signaling Functions

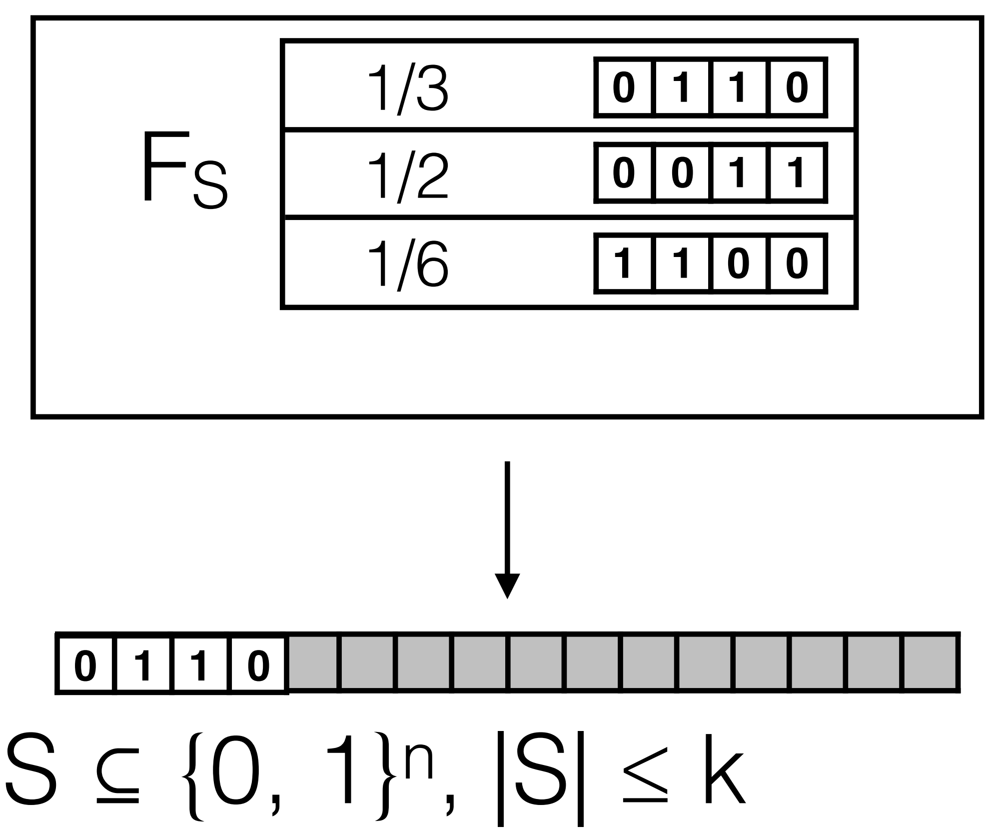
Definition:

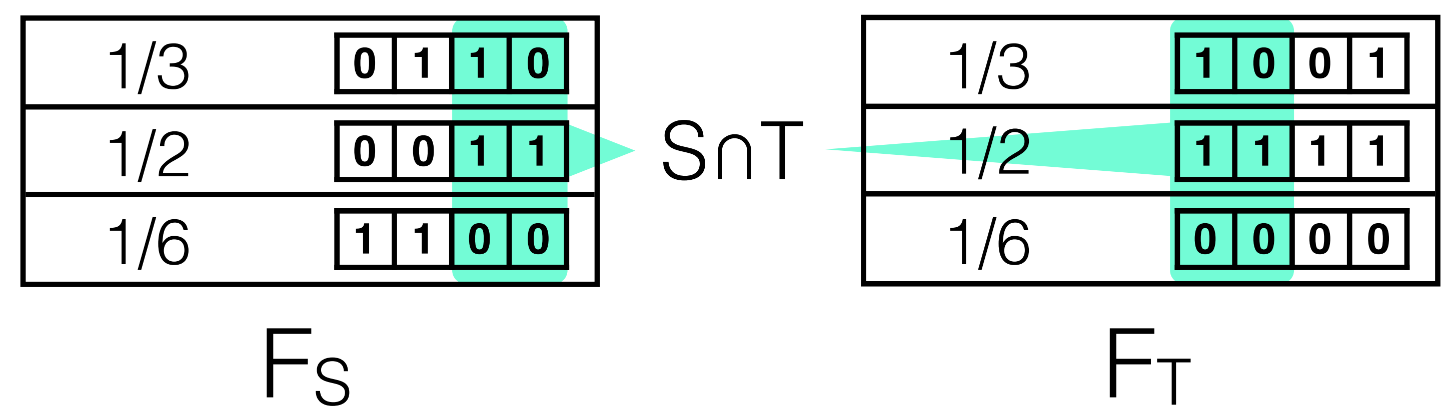
A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall S \subseteq \{0,1\}^n, |S| \leq k$ that satisfies the **non-signaling property:**

$$\forall S, T \subseteq \{0,1\}^n, |S|, |T| \leq k$$

$$F_S|_{S \cap T} \equiv F_T|_{S \cap T}$$

(the marginal distributions are equal)





Non-Signaling Functions

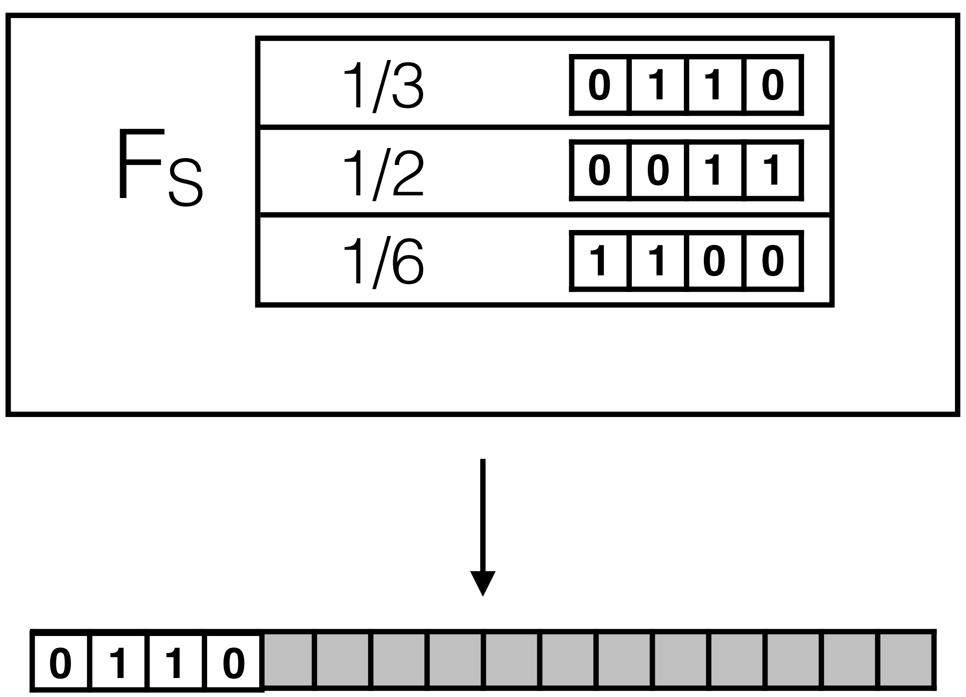
Definition:

A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall\, S \subseteq \{0, 1\}^n$, $|S| \leq k$ that satisfies the **non-signaling property:**

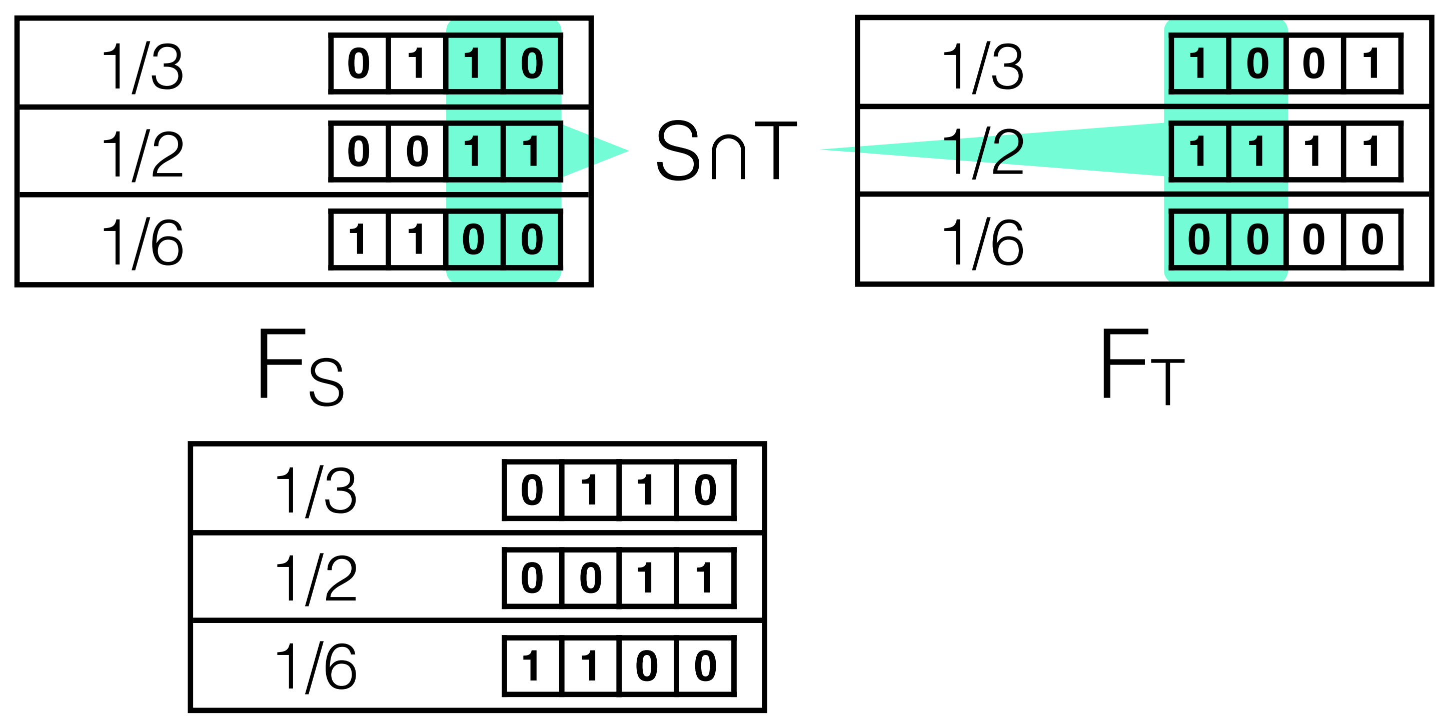
$$\forall\, S, T \subseteq \{0, 1\}^n,\ |S|, |T| \leq k$$

$$F_S|_{S \cap T} \equiv F_T|_{S \cap T}$$

(the marginal distributions are equal)



$S \subseteq \{0, 1\}^n$, $|S| \leq k$



Non-Signaling Functions

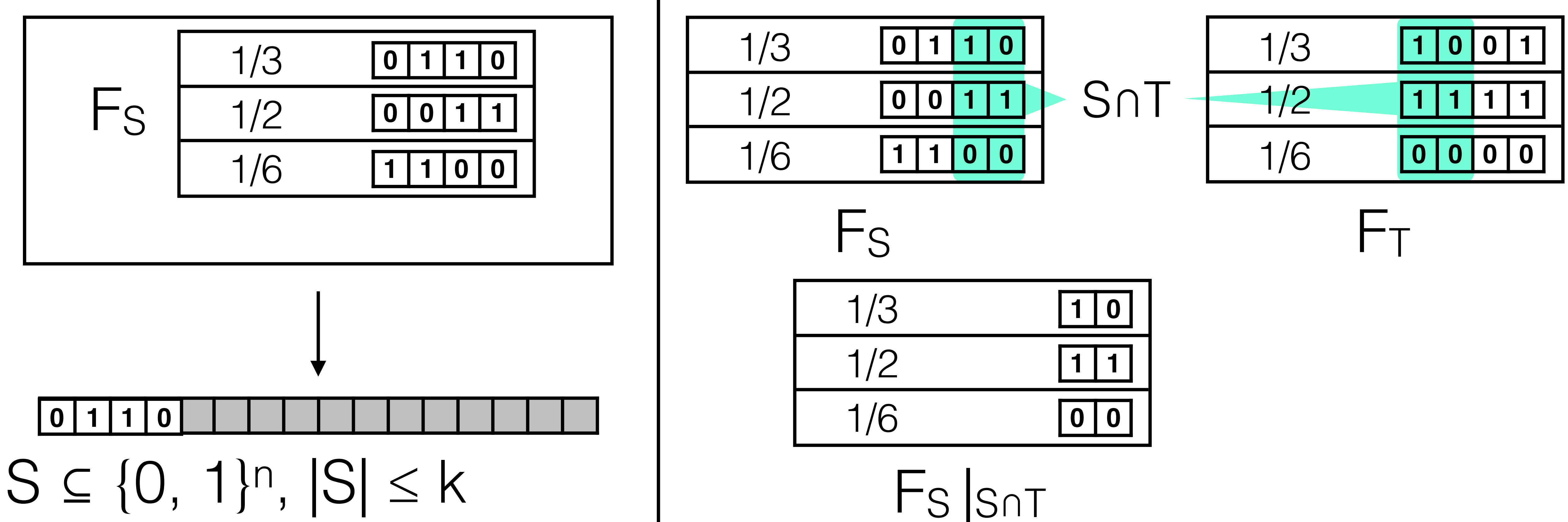
Definition:

A k-non-signaling function F: $\{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions f: $S \rightarrow \{0,1\}$, $\forall\, S \subseteq \{0, 1\}^n$, $|S| \leq k$ that satisfies the **non-signaling property:**

$$\forall\, S, T \subseteq \{0, 1\}^n, |S|, |T| \leq k$$

$$F_S|_{S\cap T} \equiv F_T|_{S\cap T}$$

(the marginal distributions are equal)



Non-Signaling Functions

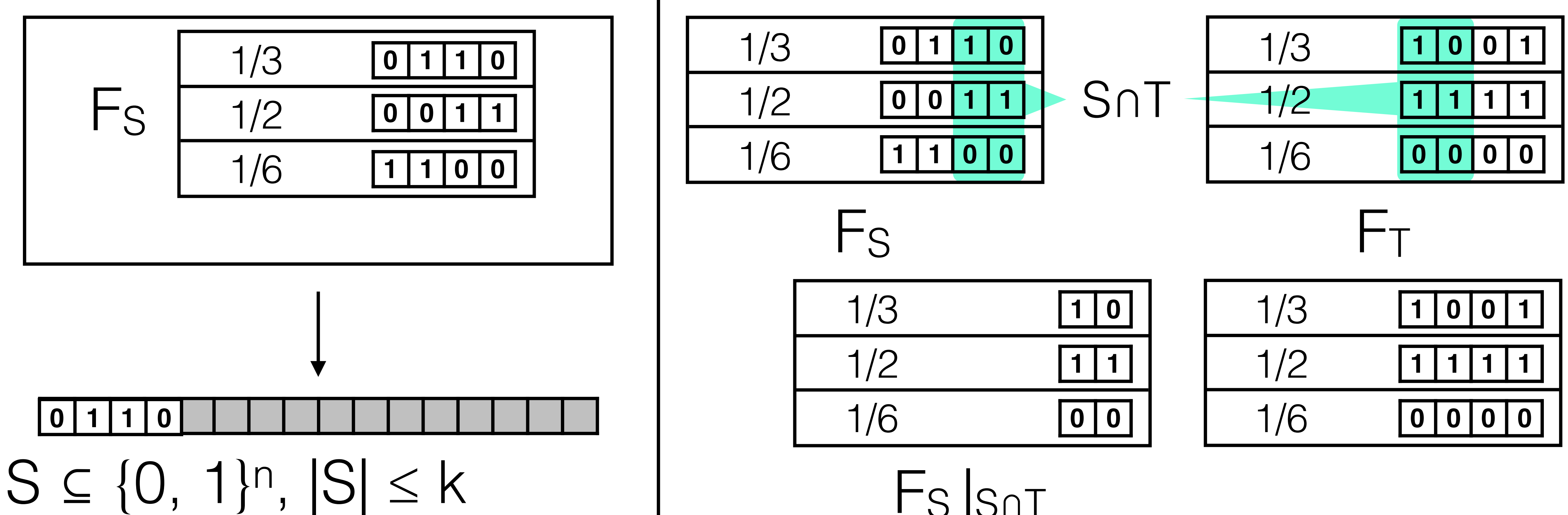
Definition:

A k-non-signaling function F: $\{0,1\}^n \to \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions f: $S \to \{0,1\}$, $\forall\, S \subseteq \{0, 1\}^n$, $|S| \leq k$ that satisfies the **non-signaling property:**

$$\forall\, S, T \subseteq \{0, 1\}^n,\ |S|, |T| \leq k$$

$$F_S|_{S\cap T} \equiv F_T|_{S\cap T}$$

(the marginal distributions are equal)



Non-Signaling Functions

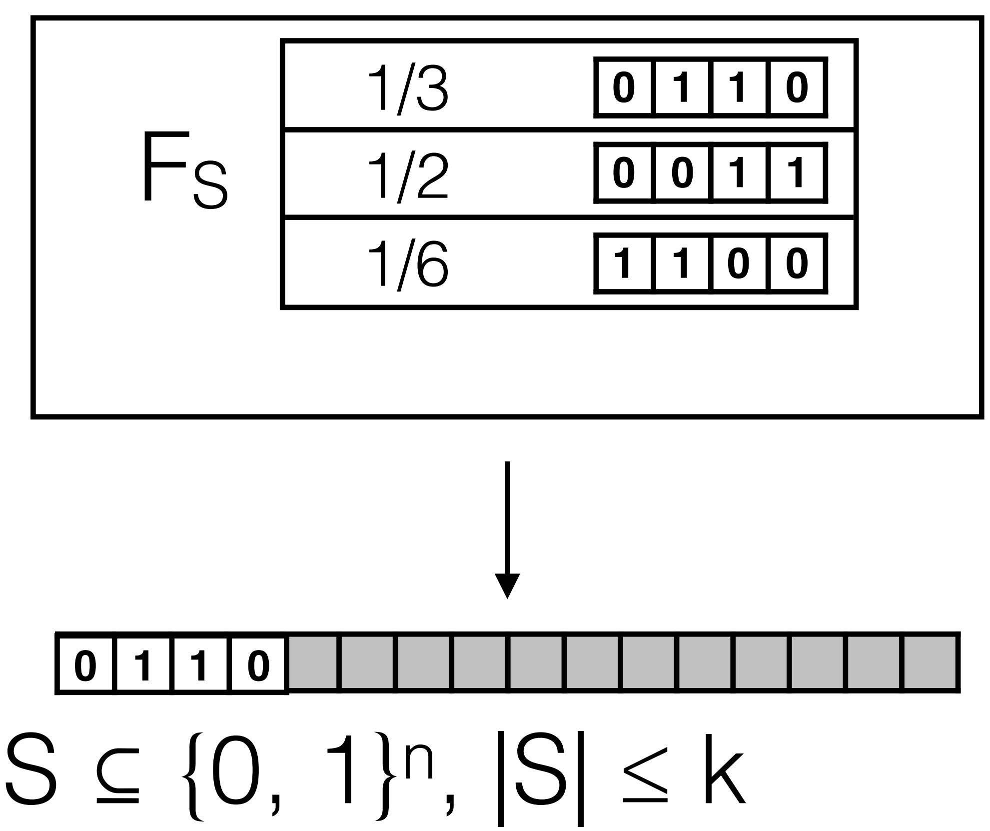
Definition:

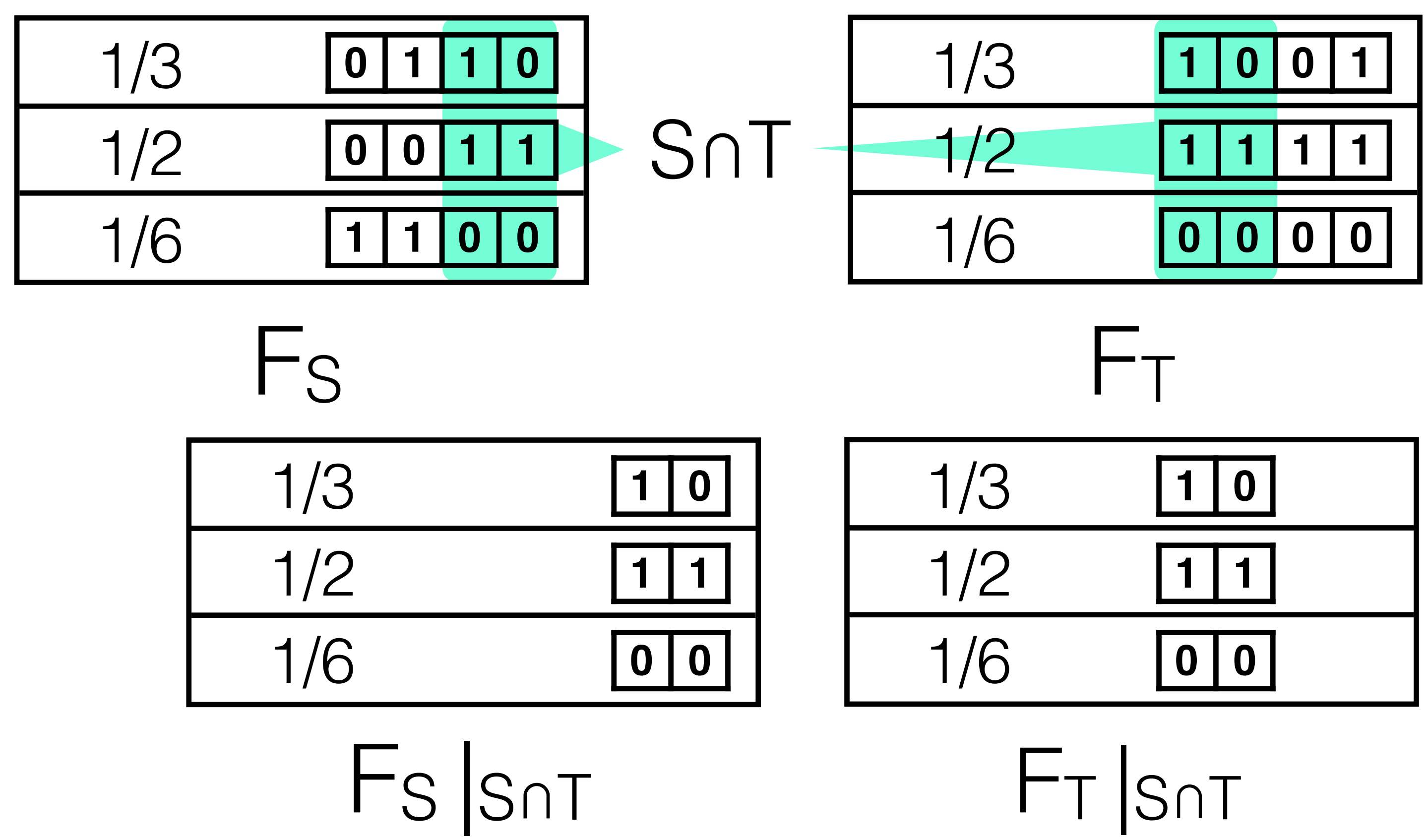
A k-non-signaling function $F: \{0,1\}^n \rightarrow \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions $f: S \rightarrow \{0,1\}$, $\forall\, S \subseteq \{0, 1\}^n$, $|S| \leq k$ that satisfies the **non-signaling property:**

$$\forall\, S, T \subseteq \{0, 1\}^n,\ |S|, |T| \leq k$$

$$F_S|_{S\cap T} \equiv F_T|_{S\cap T}$$

(the marginal distributions are equal)





Non-Signaling Functions

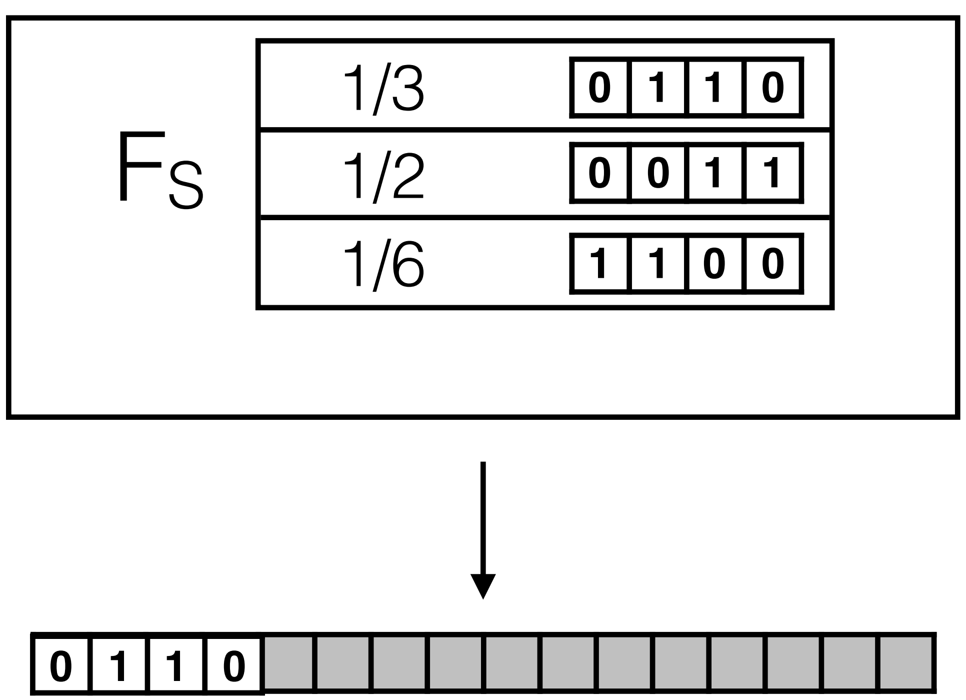
Definition:

A k-non-signaling function F: $\{0,1\}^n \to \{0,1\}$ is a collection of distributions $\{F_S\}_S$ over functions f: $S \to \{0,1\}$, $\forall S \subseteq \{0,1\}^n$, $|S| \leq k$ that satisfies the **non-signaling property:**

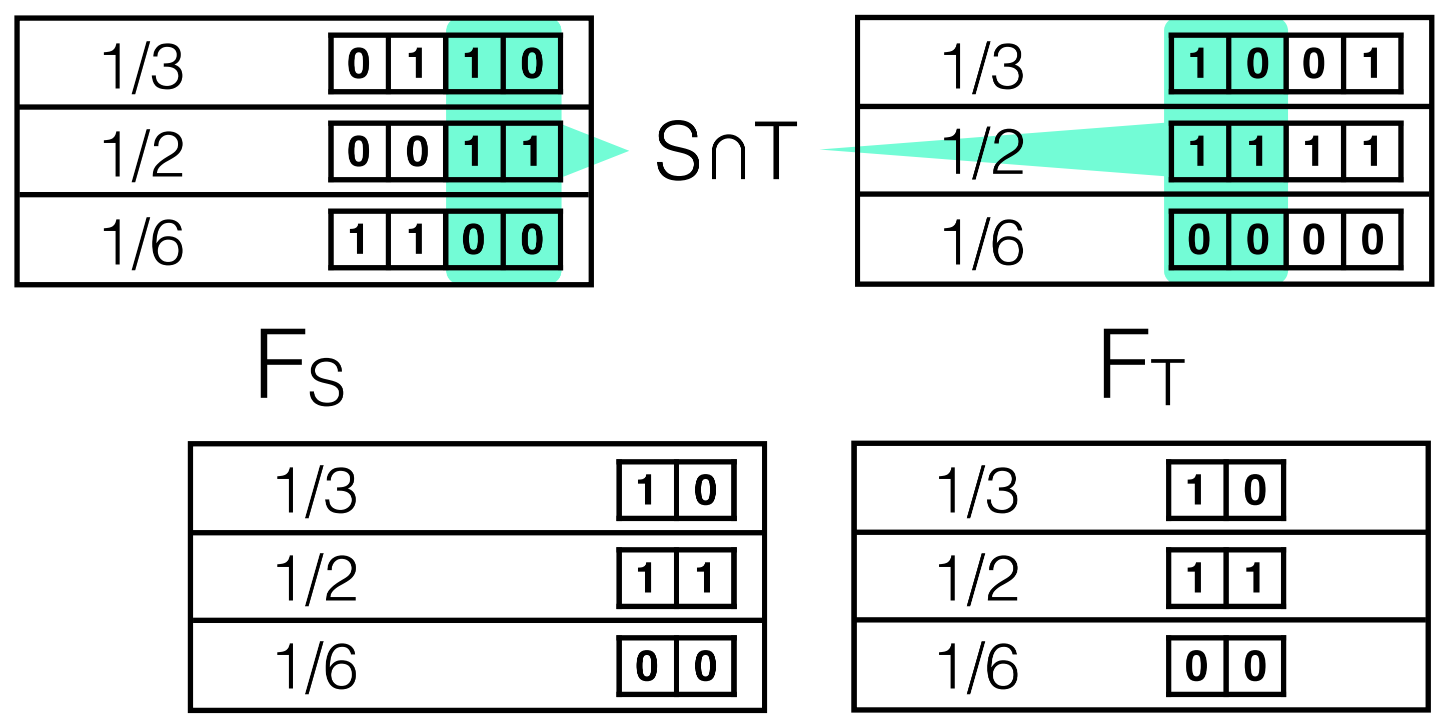
$$\forall S, T \subseteq \{0,1\}^n, |S|, |T| \leq k$$

$$F_S|_{S\cap T} \equiv F_T|_{S\cap T}$$

(the marginal distributions are equal)



$S \subseteq \{0,1\}^n$, $|S| \leq k$



$$F_S|_{S\cap T} \equiv F_T|_{S\cap T}$$

NS Linearity Testing

NS Linearity Testing

Given oracle access to $F:\{0,1\}^n \to \{0,1\}$, k-non-signaling.

NS Linearity Testing

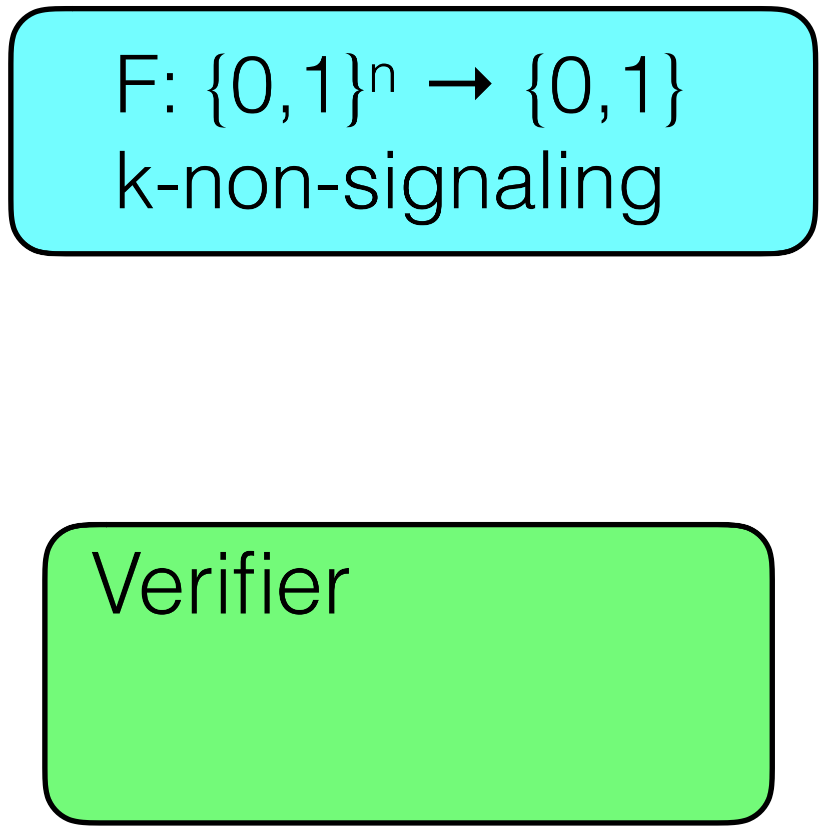
Given oracle access to $F:\{0,1\}^n \rightarrow \{0,1\}$, k-non-signaling.

Run the same test as before:

NS Linearity Testing

Given oracle access to $F:\{0,1\}^n \rightarrow \{0,1\}$, k-non-signaling.

Run the same test as before:



NS Linearity Testing

Given oracle access to $F:\{0,1\}^n \to \{0,1\}$, k-non-signaling.

Run the same test as before:

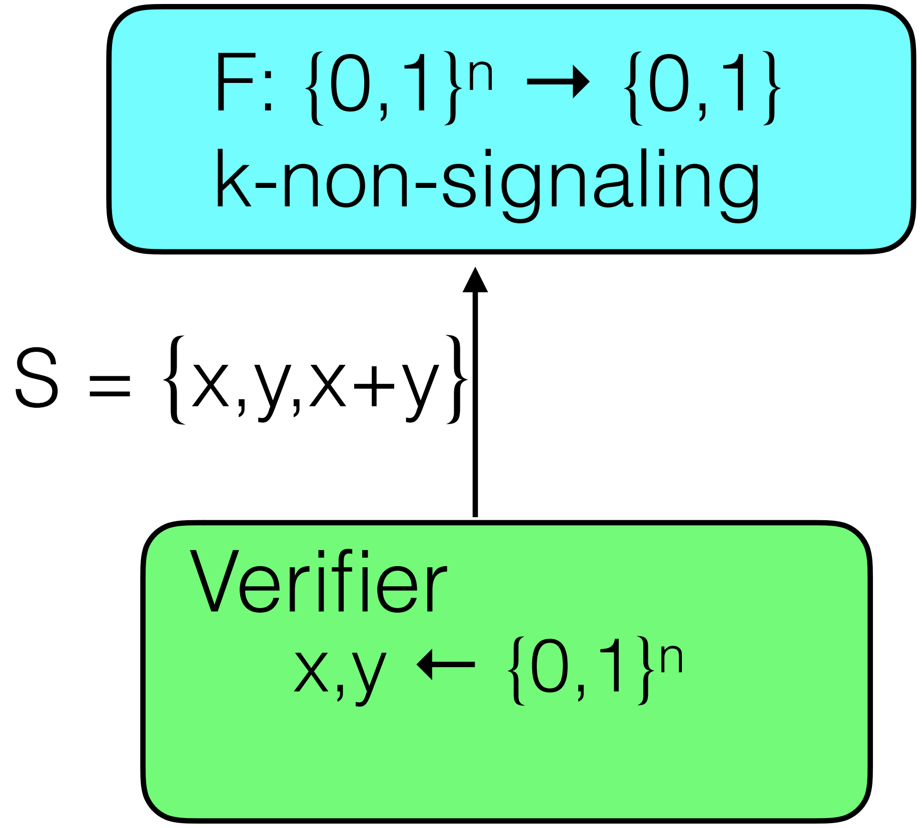
$F: \{0,1\}^n \to \{0,1\}$
k-non-signaling

Verifier
$x,y \leftarrow \{0,1\}^n$

NS Linearity Testing

Given oracle access to $F:\{0,1\}^n \to \{0,1\}$, k-non-signaling.

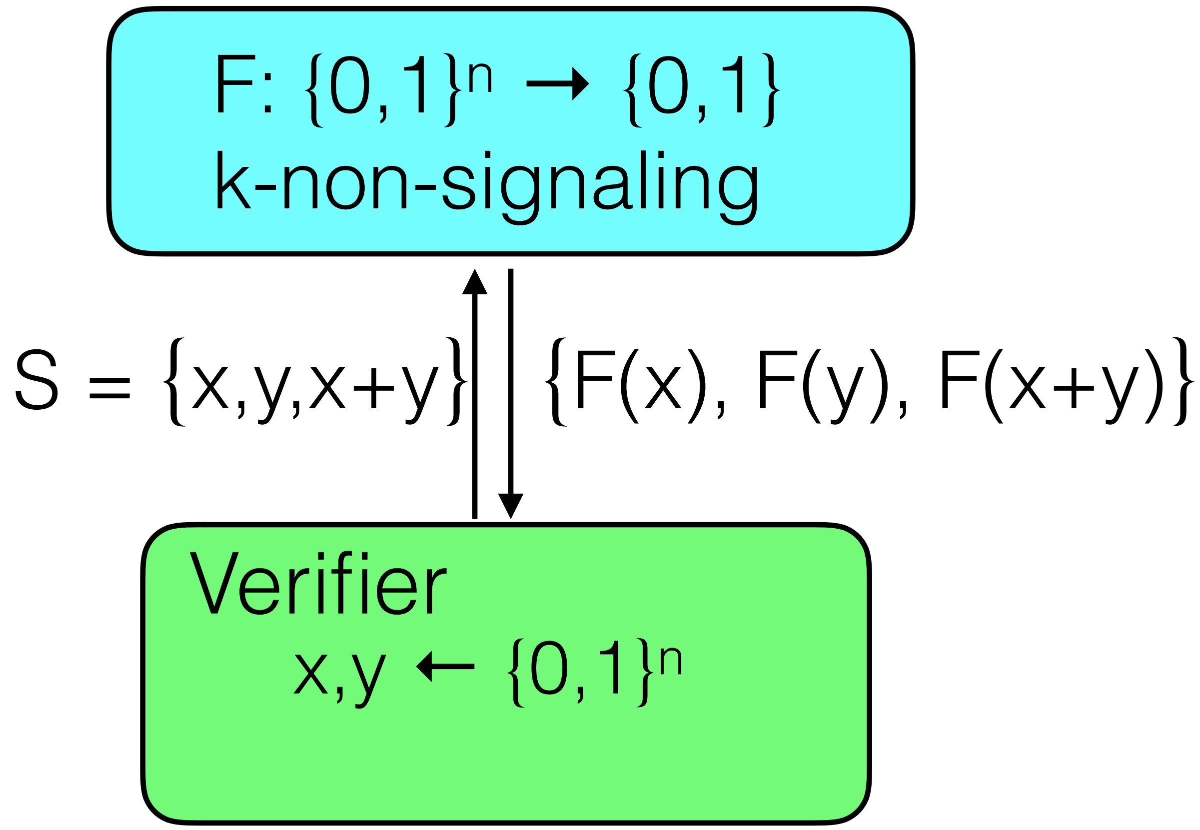
Run the same test as before:



NS Linearity Testing

Given oracle access to F:{0,1}^{n} → {0,1}, k-non-signaling.

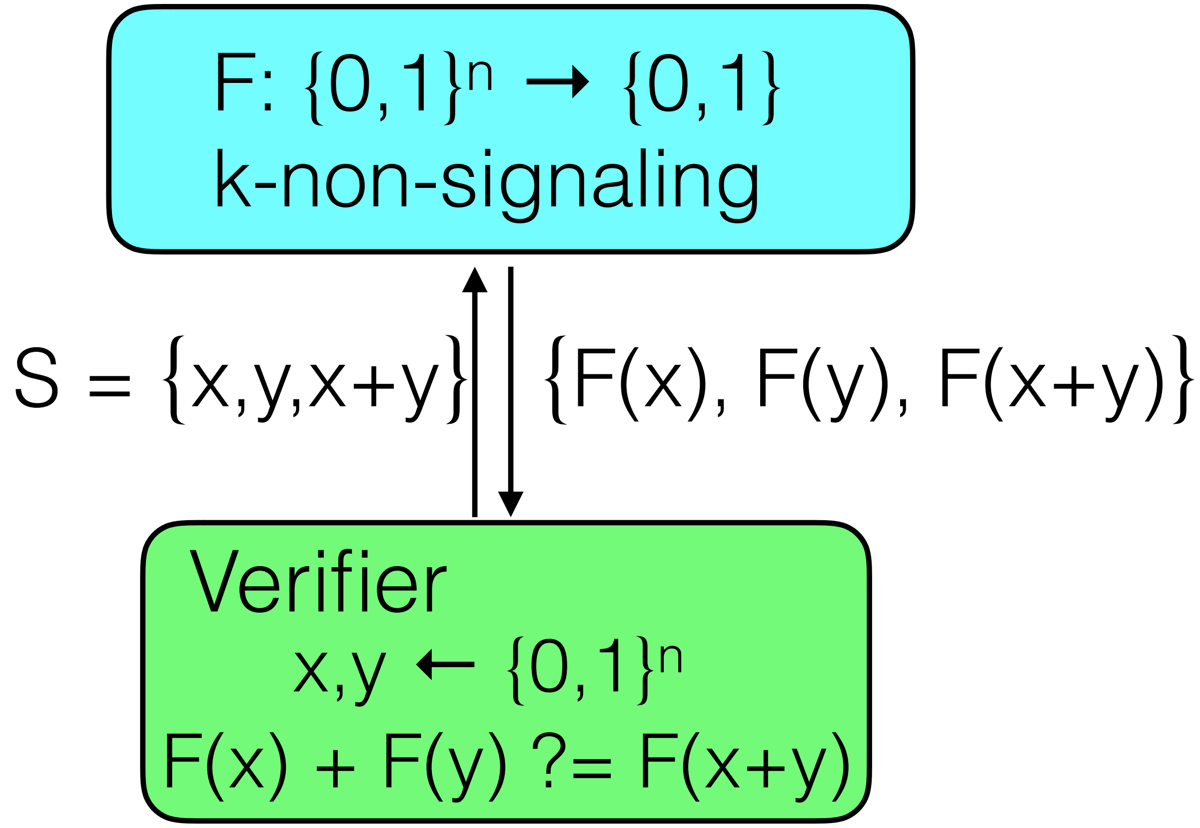
Run the same test as before:



NS Linearity Testing

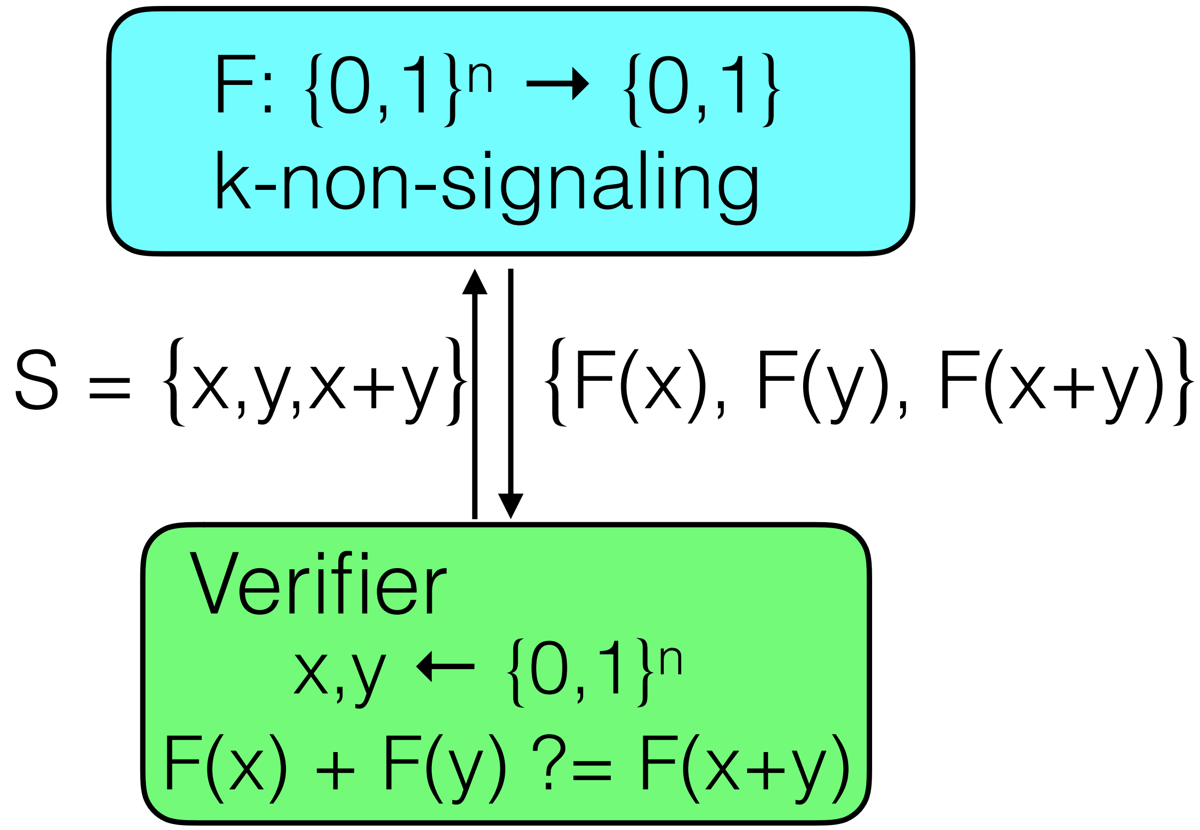
Given oracle access to $F:\{0,1\}^n \rightarrow \{0,1\}$, k-non-signaling.

Run the same test as before:



NS Linearity Testing

Given oracle access to $F:\{0,1\}^n \rightarrow \{0,1\}$, k-non-signaling.
Run the same test as before:



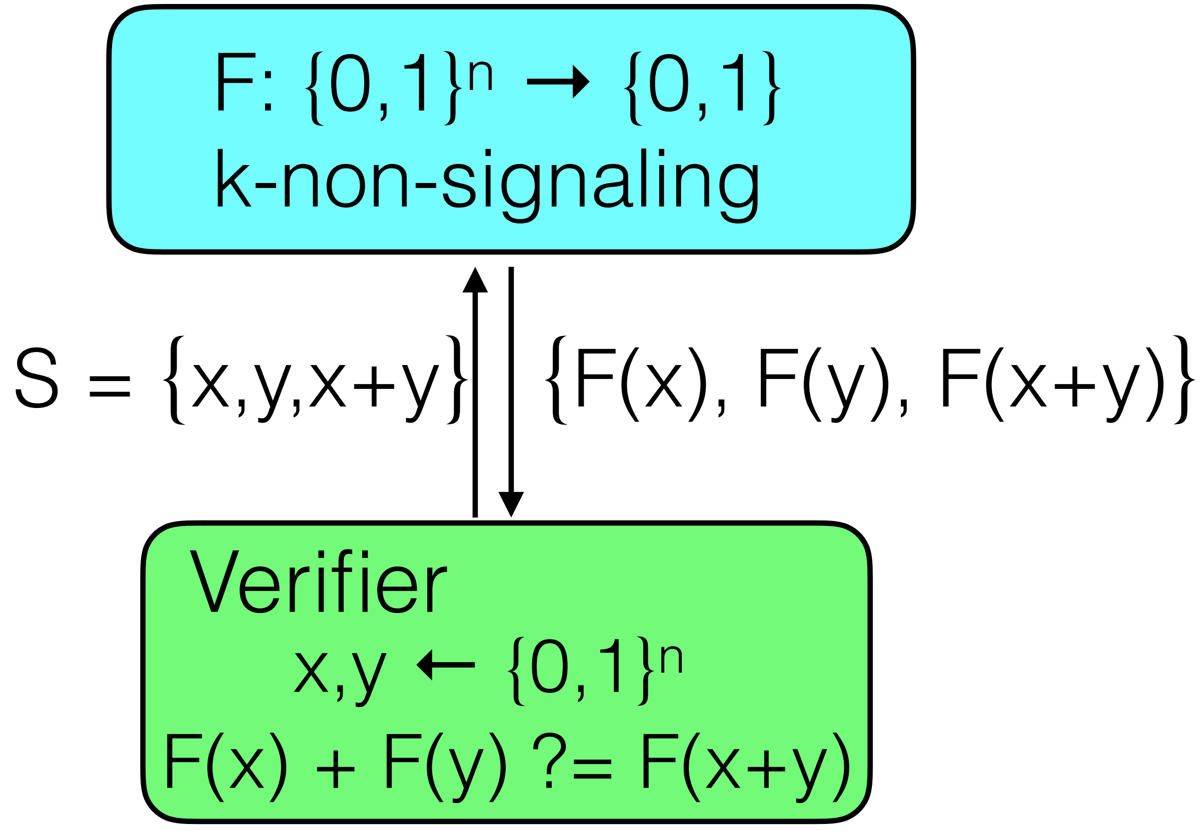
Does the test do anything useful?

$\Pr_{x,y,F}[F \text{ passes}] = 1 \rightarrow$ some global conclusion?

NS Linearity Testing

Given oracle access to $F:\{0,1\}^n \rightarrow \{0,1\}$, k-non-signaling.

Run the same test as before:



Does the test do anything useful?

$\Pr_{x,y,F}$[F passes] = 1 → some global conclusion?

How? NS functions are collections of local distributions.

Let's first understand non-signaling functions

Examples of NS Functions

Examples of NS Functions

- A function:

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

Examples of NS Functions

- A function:

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

- A distribution over functions:

1/2	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
1/6	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
1/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

Examples of NS Functions

- A function:

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

- A distribution over functions:

1/2	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
1/6	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
1/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

- A more interesting example:

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

Examples of NS Functions

- A function:

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

- A distribution over functions:

1/2	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
1/6	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
1/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

- A more interesting example:

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$		
1/2	0	0
1/2	1	1

Examples of NS Functions

- A function:

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

- A distribution over functions:

1/2	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
1/6	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
1/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

- A more interesting example:

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$		
1/2	0	0
1/2	1	1

$F_{\{2,3\}}$		
1/2	0	0
1/2	1	1

Examples of NS Functions

- A function:

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

- A distribution over functions:

1/2	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
1/6	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
1/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

- A more interesting example:

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$		
1/2	0	0
1/2	1	1

$F_{\{2,3\}}$		
1/2	0	0
1/2	1	1

$F_{\{1,3\}}$		
1/2	0	1
1/2	1	0

Examples of NS Functions

- A function:

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

- A distribution over functions:

1/2	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
1/6	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
1/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

- A more interesting example:

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$		
1/2	0	0
1/2	1	1

$F_{\{2,3\}}$		
1/2	0	0
1/2	1	1

$F_{\{1,3\}}$		
1/2	0	1
1/2	1	0

Cannot be explained by a distribution…

Examples of NS Functions

- A function:

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

- A distribution over functions:

1/2	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
1/6	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
1/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

- A more interesting example:

$F: \{1,2,3\} \rightarrow \{0,1\}$, $k = 2$

F_S defined as:

$F_{\{1,2\}}$		
1/2	0	0
1/2	1	1

$F_{\{2,3\}}$		
1/2	0	0
1/2	1	1

$F_{\{1,3\}}$		
1/2	0	1
1/2	1	0

Cannot be explained by a distribution…
But can try anyways!

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$		
1/2	0	0
1/2	1	1

$F_{\{2,3\}}$		
1/2	0	0
1/2	1	1

$F_{\{1,3\}}$		
1/2	0	1
1/2	1	0

Example cont.

$F: \{1,2,3\} \to \{0,1\}$, $k = 2$

F_S defined as:

$F_{\{1,2\}}$		$F_{\{2,3\}}$		$F_{\{1,3\}}$	
1/2	0 0	1/2	0 0	1/2	0 1
1/2	1 1	1/2	1 1	1/2	1 0

Let's try to write it as a distribution anyways.

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$	
1/2	0 0
1/2	1 1

$F_{\{2,3\}}$	
1/2	0 0
1/2	1 1

$F_{\{1,3\}}$	
1/2	0 1
1/2	1 0

Let's try to write it as a distribution anyways.

System of linear eqs:

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$		
1/2	0	0
1/2	1	1

$F_{\{2,3\}}$		
1/2	0	0
1/2	1	1

$F_{\{1,3\}}$		
1/2	0	1
1/2	1	0

Let's try to write it as a distribution anyways.

System of linear eqs:

Variables: q_f for every f: {1,2,3} → {0,1}

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$	
1/2	0 0
1/2	1 1

$F_{\{2,3\}}$	
1/2	0 0
1/2	1 1

$F_{\{1,3\}}$	
1/2	0 1
1/2	1 0

Let's try to write it as a distribution anyways.

System of linear eqs:

- Variables: q_f for every f: {1,2,3} → {0,1}
- Constraints:

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$	
1/2	0 0
1/2	1 1

$F_{\{2,3\}}$	
1/2	0 0
1/2	1 1

$F_{\{1,3\}}$	
1/2	0 1
1/2	1 0

Let's try to write it as a distribution anyways.

System of linear eqs:

- Variables: q_f for every f: {1,2,3} → {0,1}
- Constraints: $1/2 = \Pr[F_{\{1,2\}} = (0,0)] = q_{(0,0,0)} + q_{(0,0,1)}$

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$		$F_{\{2,3\}}$		$F_{\{1,3\}}$	
1/2	0 0	1/2	0 0	1/2	0 1
1/2	1 1	1/2	1 1	1/2	1 0

Let's try to write it as a distribution anyways.

System of linear eqs:

Variables: q_f for every f: {1,2,3} → {0,1}

Constraints: $1/2 = \Pr[F_{\{1,2\}} = (0,0)] = q_{(0,0,0)} + q_{(0,0,1)}$

$1/2 = \Pr[F_{\{1,2\}} = (1,1)] = q_{(1,1,0)} + q_{(1,1,1)}$

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$	
1/2	0 0
1/2	1 1

$F_{\{2,3\}}$	
1/2	0 0
1/2	1 1

$F_{\{1,3\}}$	
1/2	0 1
1/2	1 0

Let's try to write it as a distribution anyways.

System of linear eqs:

Variables: q_f for every f: {1,2,3} → {0,1}

Constraints: $1/2 = \Pr[F_{\{1,2\}} = (0,0)] = q_{(0,0,0)} + q_{(0,0,1)}$

$1/2 = \Pr[F_{\{1,2\}} = (1,1)] = q_{(1,1,0)} + q_{(1,1,1)}$

$0 = \Pr[F_{\{1,2\}} = (0,1)] = q_{(0,1,0)} + q_{(1,0,1)}$

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$	
1/2	0 0
1/2	1 1

$F_{\{2,3\}}$	
1/2	0 0
1/2	1 1

$F_{\{1,3\}}$	
1/2	0 1
1/2	1 0

Let's try to write it as a distribution anyways.

System of linear eqs:

Variables: q_f for every f: {1,2,3} → {0,1}

Constraints:
$$1/2 = \Pr[F_{\{1,2\}} = (0,0)] = q_{(0,0,0)} + q_{(0,0,1)}$$
$$1/2 = \Pr[F_{\{1,2\}} = (1,1)] = q_{(1,1,0)} + q_{(1,1,1)}$$
$$0 = \Pr[F_{\{1,2\}} = (0,1)] = q_{(0,1,0)} + q_{(1,0,1)}$$
$$0 = \Pr[F_{\{1,2\}} = (1,0)] = q_{(1,0,0)} + q_{(1,0,1)}$$

…

Example cont.

$F: \{1,2,3\} \to \{0,1\}$, $k = 2$

F_S defined as:

$F_{\{1,2\}}$		$F_{\{2,3\}}$		$F_{\{1,3\}}$	
1/2	0 0	1/2	0 0	1/2	0 1
1/2	1 1	1/2	1 1	1/2	1 0

Let's try to write it as a distribution anyways.

System of linear eqs:

Variables: q_f for every $f: \{1,2,3\} \to \{0,1\}$

Constraints: $1/2 = \Pr[F_{\{1,2\}} = (0,0)] = q_{(0,0,0)} + q_{(0,0,1)}$

$1/2 = \Pr[F_{\{1,2\}} = (1,1)] = q_{(1,1,0)} + q_{(1,1,1)}$

$0 = \Pr[F_{\{1,2\}} = (0,1)] = q_{(0,1,0)} + q_{(1,0,1)}$

$0 = \Pr[F_{\{1,2\}} = (1,0)] = q_{(1,0,0)} + q_{(1,0,1)}$

…

Fact: system of linear equations has a solution.

Example cont.

F: {1,2,3} → {0,1}, k = 2

F_S defined as:

$F_{\{1,2\}}$	
1/2	0 0
1/2	1 1

$F_{\{2,3\}}$	
1/2	0 0
1/2	1 1

$F_{\{1,3\}}$	
1/2	0 1
1/2	1 0

Let's try to write it as a distribution anyways.

System of linear eqs:

Variables: q_f for every f: {1,2,3} → {0,1}

Constraints: $1/2 = \Pr[F_{\{1,2\}} = (0,0)] = q_{(0,0,0)} + q_{(0,0,1)}$

$1/2 = \Pr[F_{\{1,2\}} = (1,1)] = q_{(1,1,0)} + q_{(1,1,1)}$

$0 = \Pr[F_{\{1,2\}} = (0,1)] = q_{(0,1,0)} + q_{(1,0,1)}$

$0 = \Pr[F_{\{1,2\}} = (1,0)] = q_{(1,0,0)} + q_{(1,0,1)}$

…

Fact: system of linear equations has a solution.

Solution has *negative* entries, but marginals on "queryable sets" are non-negative.

Quasi-Distributions

Quasi-Distributions

A *quasi-distribution* is a distribution, only “probabilities” are allowed to be negative.

Quasi-Distributions

A *quasi-distribution* is a distribution, only “probabilities” are allowed to be negative.

-1/3	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
2/3	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
2/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

Quasi-Distributions

A *quasi-distribution* is a distribution, only “probabilities” are allowed to be negative.

-1/3	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
2/3	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
2/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

A quasi-distribution is *k-local* if every marginal on k points is a (standard) distribution.

Quasi-Distributions

A *quasi-distribution* is a distribution, only “probabilities” are allowed to be negative.

-1/3	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
2/3	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
2/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

A quasi-distribution is *k-local* if every marginal on k points is a (standard) distribution.

Observation:

k-local quasi-distributions → k-non-signaling functions

Quasi-Distributions

A *quasi-distribution* is a distribution, only “probabilities” are allowed to be negative.

-1/3	1	0	1	1	0	0	0	1	1	1	0	0	1	0	1	1
2/3	1	1	0	0	1	1	0	1	1	0	0	1	1	1	0	1
2/3	0	0	1	1	1	1	1	0	0	1	0	1	1	1	1	0

A quasi-distribution is *k-local* if every marginal on k points is a (standard) distribution.

Observation:

k-local quasi-distributions → k-non-signaling functions

Does the reverse direction hold?

Theorem 1

k-local quasi-distributions ⟷ k-non-signaling functions

Theorem 1

k-local quasi-distributions ⟷ k-non-signaling functions

Proof sketch:

⟹ direction: easy

Theorem 1

k-local quasi-distributions ⟷ k-non-signaling functions

Proof sketch:

⟶ direction: easy

⟵ direction:

Theorem 1

k-local quasi-distributions $\Longleftrightarrow$ k-non-signaling functions

Proof sketch:

$\Rightarrow$ direction: easy

$\Leftarrow$ direction: $\forall S \subseteq \{0,1\}^n, |S| \leq k, \text{ and } \vec{b} \in \{0,1\}^S$

$$\Pr[F(S) = \vec{b}] = -1 + \frac{1}{2^{|S|-1}} \sum_{T \subseteq S} \Pr[\sum_{x \in T} F(x) = \sum_{x \in T} b_x]$$

Theorem 1

k-local quasi-distributions ⟷ k-non-signaling functions

Proof sketch:

⟹ direction: easy

⟸ direction: $\forall S \subseteq \{0,1\}^n, |S| \leq k, \text{ and } \vec{b} \in \{0,1\}^S$

$$\Pr[F(S) = \vec{b}] = -1 + \frac{1}{2^{|S|-1}} \sum_{T \subseteq S} \Pr[\sum_{x \in T} F(x) = \sum_{x \in T} b_x]$$

Fourier analysis: Quasi-dist is a *function* Q: funcs → $\mathbb{R}$.

Theorem 1

k-local quasi-distributions ⟷ k-non-signaling functions

Proof sketch:

⟹ direction: easy

⟸ direction: $\forall S \subseteq \{0,1\}^n, |S| \leq k, \text{ and } \vec{b} \in \{0,1\}^S$

$$\Pr[F(S) = \vec{b}] = -1 + \frac{1}{2^{|S|-1}} \sum_{T \subseteq S} \Pr[\sum_{x \in T} F(x) = \sum_{x \in T} b_x]$$

Fourier analysis: Quasi-dist is a *function* Q: funcs → ℝ.

A basis element $\boldsymbol{\chi}_S$ for each
$S \subseteq \{0, 1\}^n$,

Theorem 1

k-local quasi-distributions ⟺ k-non-signaling functions

Proof sketch:

⟹ direction: easy

⟸ direction: $\forall S \subseteq \{0,1\}^n, |S| \leq k, \text{ and } \vec{b} \in \{0,1\}^S$

$$\Pr[F(S) = \vec{b}] = -1 + \frac{1}{2^{|S|-1}} \sum_{T \subseteq S} \Pr[\sum_{x \in T} F(x) = \sum_{x \in T} b_x]$$

Fourier analysis: Quasi-dist is a *function* Q: funcs → $\mathbb{R}$.

A basis element χ_S for each $S \subseteq \{0, 1\}^n$, which determines

$$\Pr[\sum_{x \in S} Q(x) = 0] := \sum_{f : \sum_{x \in S} f(x) = 0} q_f$$

Theorem 1

k-local quasi-distributions ⟺ k-non-signaling functions

Proof sketch:

⟹ direction: easy

⟸ direction: $\forall S \subseteq \{0,1\}^n, |S| \leq k, \text{ and } \vec{b} \in \{0,1\}^S$

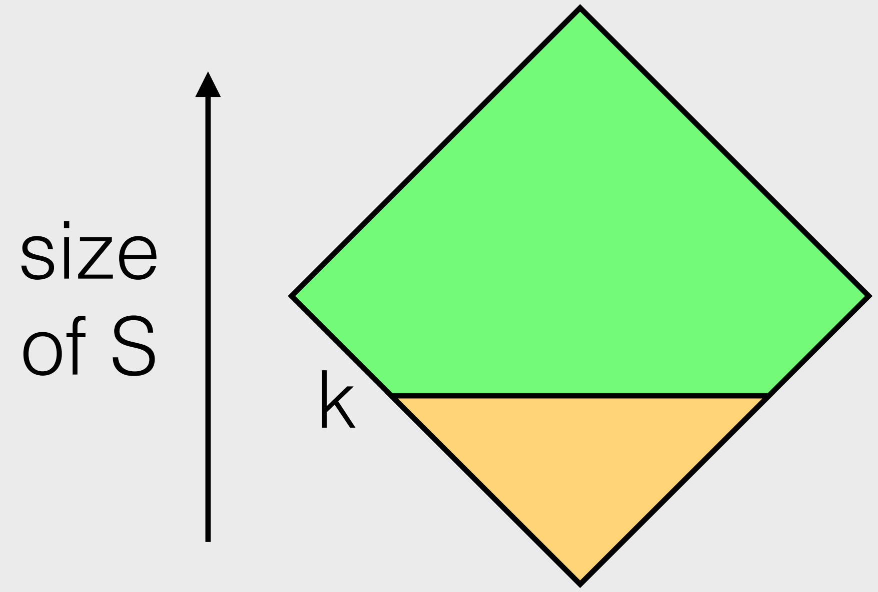
$$\Pr[F(S) = \vec{b}] = -1 + \frac{1}{2^{|S|-1}} \sum_{T \subseteq S} \Pr[\sum_{x \in T} F(x) = \sum_{x \in T} b_x]$$

Fourier analysis: Quasi-dist is a *function* Q: funcs → $\mathbb{R}$.

A basis element $\boldsymbol{\chi}_S$ for each $S \subseteq \{0, 1\}^n$, which determines

$$\Pr[\sum_{x \in S} Q(x) = 0] := \sum_{f : \sum_{x \in S} f(x) = 0} q_f$$

Fourier spectrum of Q



Theorem 1

k-local quasi-distributions ⟷ k-non-signaling functions

Proof sketch:

⟹ direction: easy

⟸ direction: $\forall S \subseteq \{0,1\}^n, |S| \leq k, \text{ and } \vec{b} \in \{0,1\}^S$

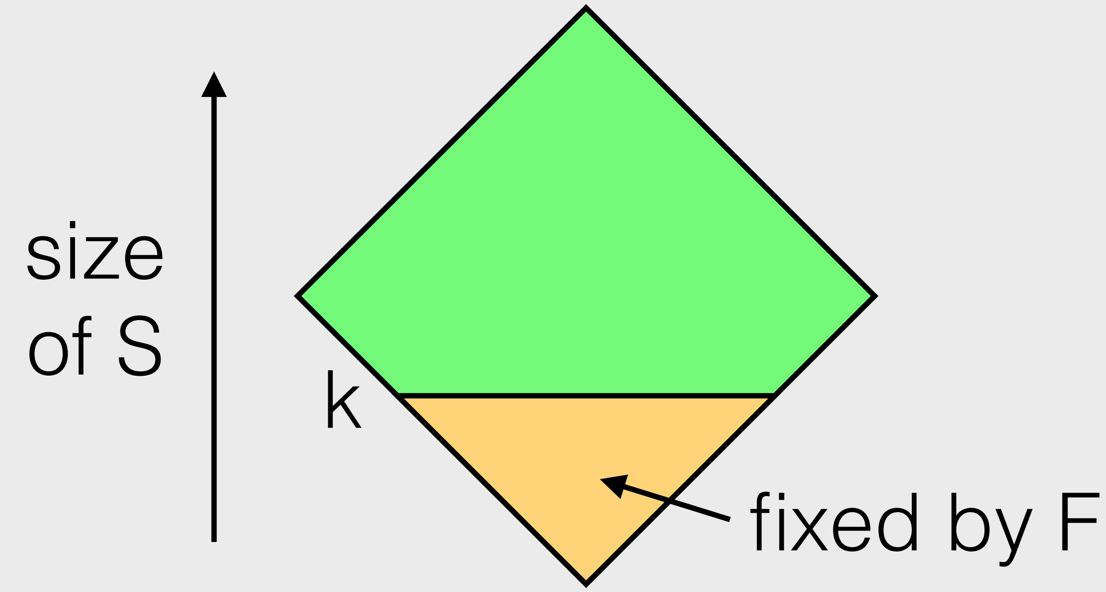
$$\Pr[F(S) = \vec{b}] = -1 + \frac{1}{2^{|S|-1}} \sum_{T \subseteq S} \Pr[\sum_{x \in T} F(x) = \sum_{x \in T} b_x]$$

Fourier analysis: Quasi-dist is a *function* Q: funcs → $\mathbb{R}$.

A basis element χ_S for each $S \subseteq \{0, 1\}^n$, which determines

$$\Pr[\sum_{x \in S} Q(x) = 0] := \sum_{f : \sum_{x \in S} f(x) = 0} q_f$$

Fourier spectrum of Q



Theorem 1

k-local quasi-distributions ⟺ k-non-signaling functions

Proof sketch:

⟹ direction: easy

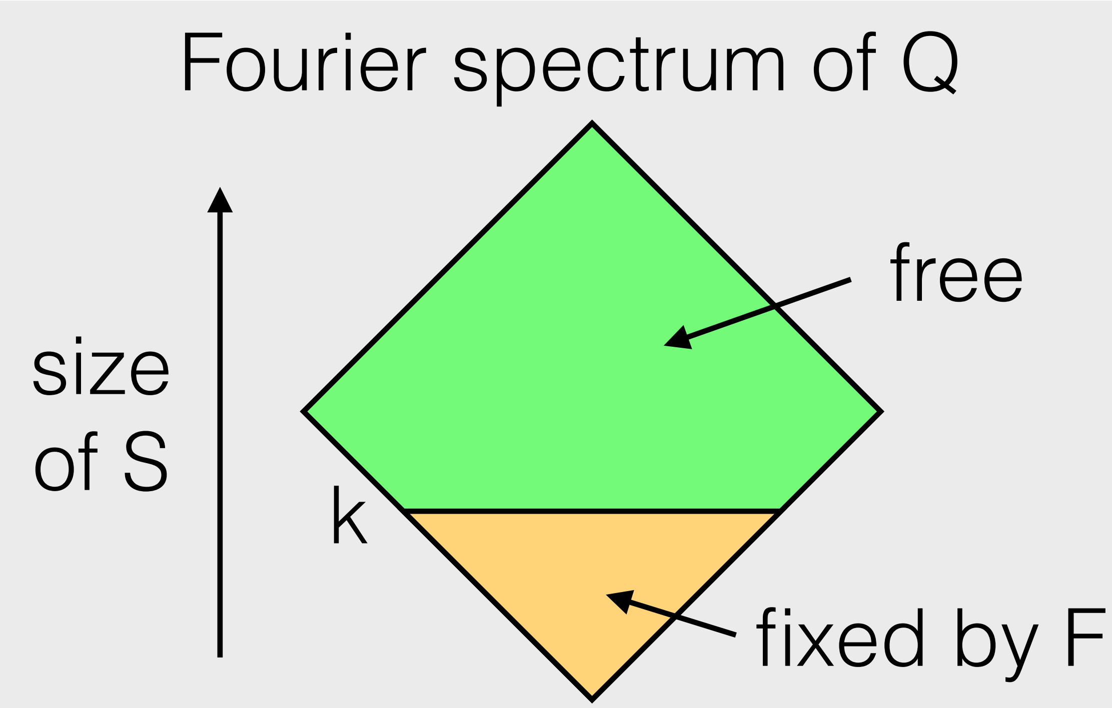
⟸ direction: $\forall S \subseteq \{0,1\}^n, |S| \leq k,$ and $\vec{b} \in \{0,1\}^S$

$$\Pr[F(S) = \vec{b}] = -1 + \frac{1}{2^{|S|-1}} \sum_{T \subseteq S} \Pr[\sum_{x \in T} F(x) = \sum_{x \in T} b_x]$$

Fourier analysis: Quasi-dist is a *function* Q: funcs → ℝ.

A basis element χ_S for each $S \subseteq \{0, 1\}^n$, which determines

$$\Pr[\sum_{x \in S} Q(x) = 0] := \sum_{f : \sum_{x \in S} f(x) = 0} q_f$$



Recall the linearity test:

F: $\{0,1\}^n$ -> $\{0,1\}$
k-non-signaling

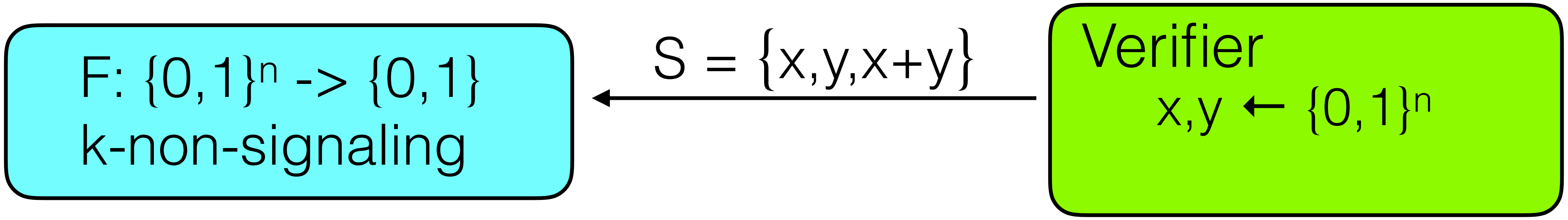
Verifier

Recall the linearity test:

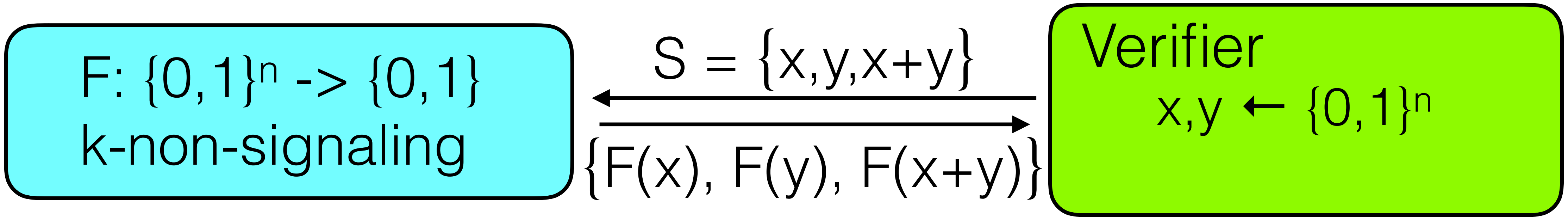
F: $\{0,1\}^n$ -> $\{0,1\}$
k-non-signaling

Verifier
$x,y \leftarrow \{0,1\}^n$

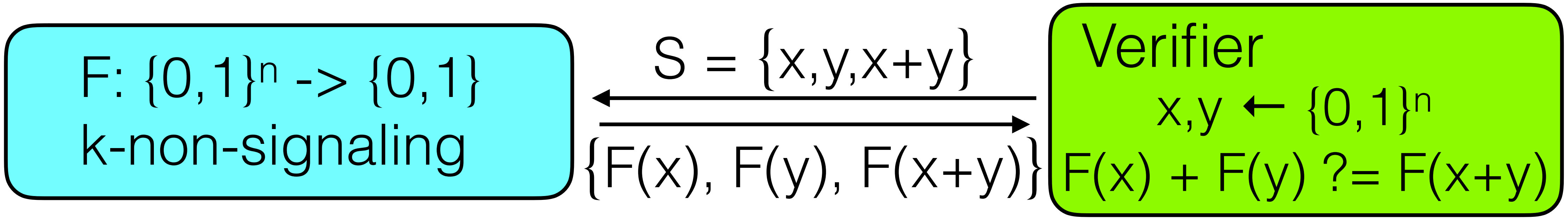
Recall the linearity test:



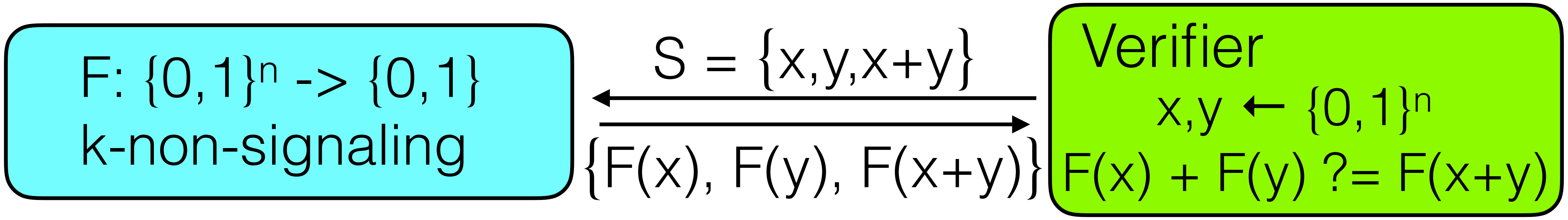
Recall the linearity test:



Recall the linearity test:

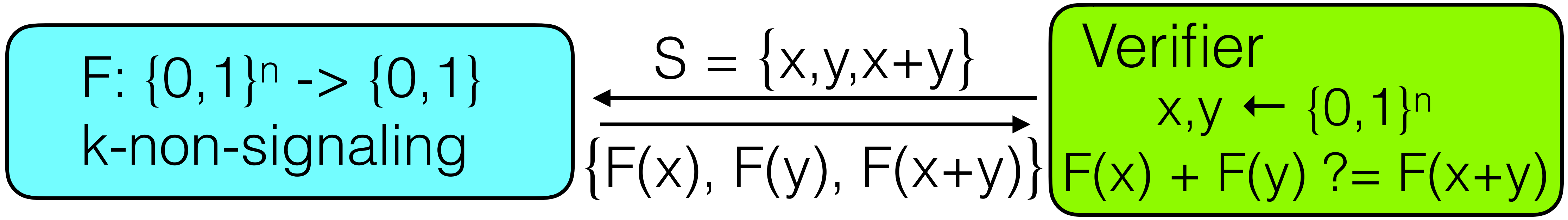


Recall the linearity test:



Observation: F = quasi-dist over LIN → Pr[F passes] = 1

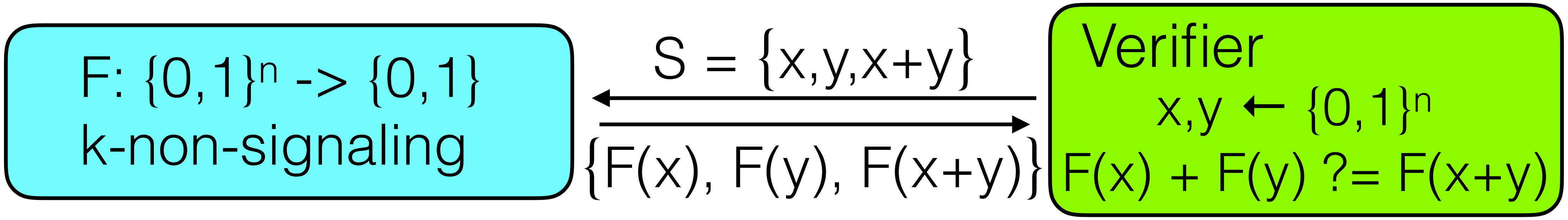
Recall the linearity test:



Observation: F = quasi-dist over LIN → Pr[F passes] = 1

Is the converse true?

Recall the linearity test:



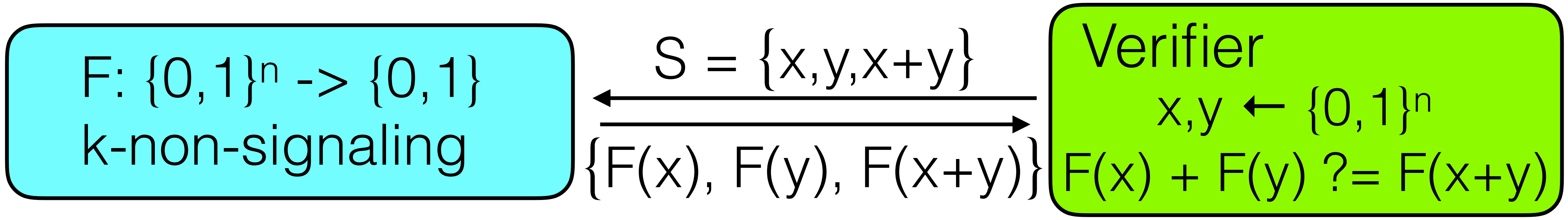
Observation: F = quasi-dist over LIN → Pr[F passes] = 1

Is the converse true?

Theorem 2

Pr[F passes] = 1 ⇔ F is a quasi-dist over LIN

Recall the linearity test:



Observation: F = quasi-dist over LIN → Pr[F passes] = 1

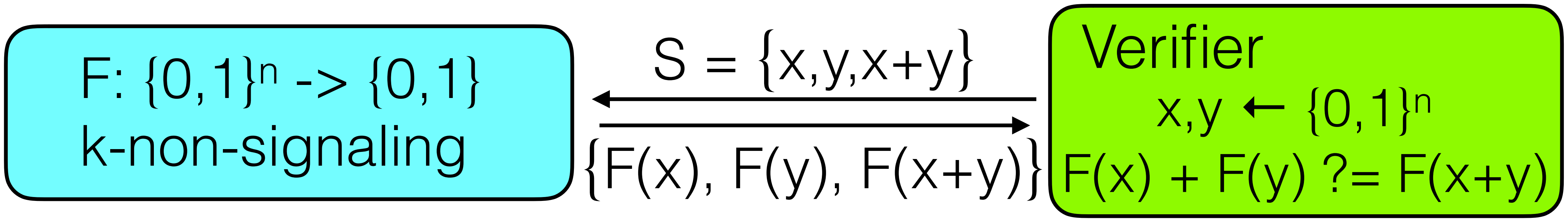
Is the converse true?

Theorem 2

Pr[F passes] = 1 ⇔ F is a quasi-dist over LIN

Proof: characterize Fourier spectrum of quasi-dists over LIN.

Recall the linearity test:



Observation: F = quasi-dist over LIN → Pr[F passes] = 1

Is the converse true?

Theorem 2

Pr[F passes] = 1 ⇔ F is a quasi-dist over LIN

Proof: characterize Fourier spectrum of quasi-dists over LIN.

This is a global conclusion!

Now suppose F passes the linearity test w.p. 1 - ε

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f's

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f's
(this is what happens in the classical case)

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f's
(this is what happens in the classical case)

This is true.

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f's (this is what happens in the classical case)

This is true.

But…

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f's
(this is what happens in the classical case)

This is true.

But… it's true without the hypothesis!

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f's
(this is what happens in the classical case)

This is true.

But… it's true without the hypothesis!

Even for | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | !

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f's
(this is what happens in the classical case)

This is true.

But… it's true without the hypothesis!

Even for | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | !

Let's try again.

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f's
(this is what happens in the classical case)

This is true.

But… it's true without the hypothesis!

Even for

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

!

Let's try again.

Another natural conjecture: F ≈ quasi-dist over linear f's

Now suppose F passes the linearity test w.p. 1 - ε

Natural conjecture: F = quasi-dist over almost linear f’s
(this is what happens in the classical case)

This is true.

But… it’s true without the hypothesis!
Even for | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | !

Let’s try again.

Another natural conjecture: F ≈ quasi-dist over linear f’s

This is the correct answer.

Suppose F passes the linearity test w.p. 1 - ε

Suppose F passes the linearity test w.p. 1 - ε

Goal: show F $\approx$ quasi-dist over linear f's

Suppose F passes the linearity test w.p. $1 - \varepsilon$

Goal: show F $\approx$ quasi-dist over linear f's

$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$

Suppose F passes the linearity test w.p. 1 - ε

Goal: show F ≈ quasi-dist over linear f's

$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$

Bad example: F =

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

Suppose F passes the linearity test w.p. 1 - ε

Goal: show F $\approx$ quasi-dist over linear f's

$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$

Bad example: F = | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Then $\Delta(F, Q)$ is large for all Q!

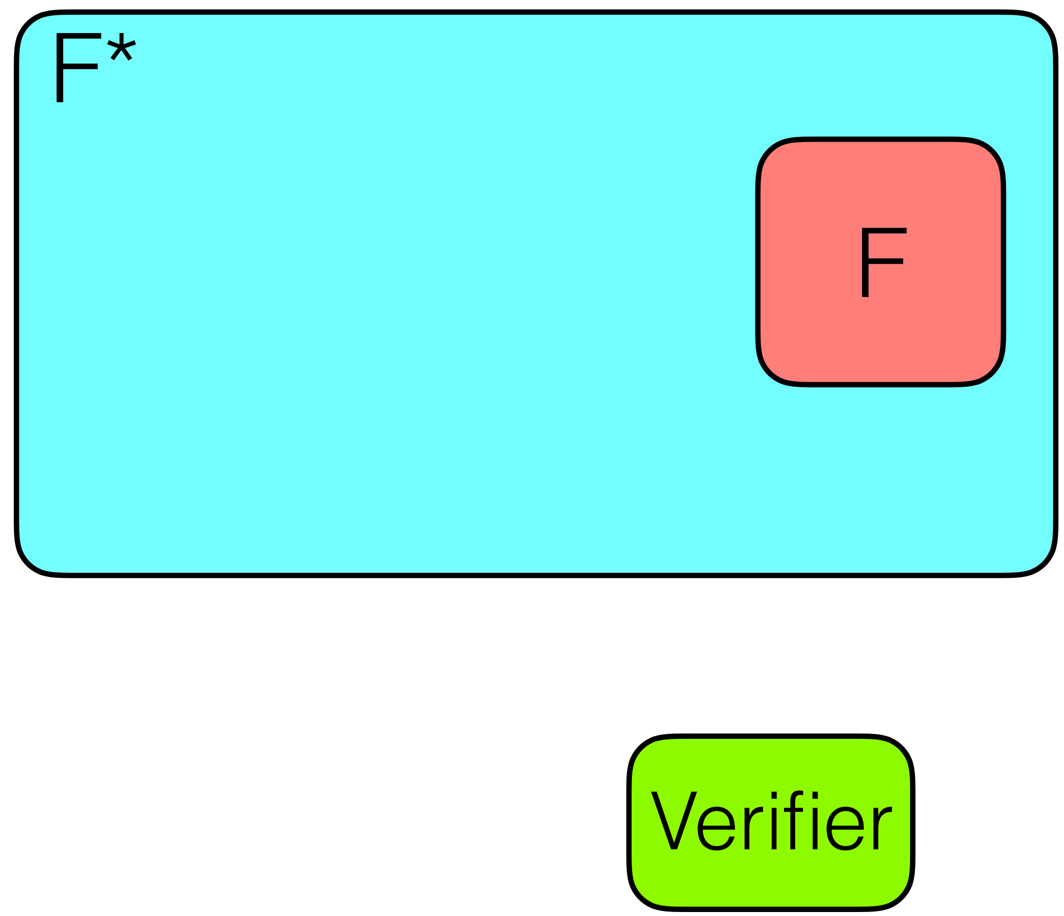
Suppose F passes the linearity test w.p. 1 - ε

Goal: show F $\approx$ quasi-dist over linear f's

$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$

Bad example: F = | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Then $\Delta(F, Q)$ is large for all Q!
Fix: define F*, a "smooth" F
(self-correction)



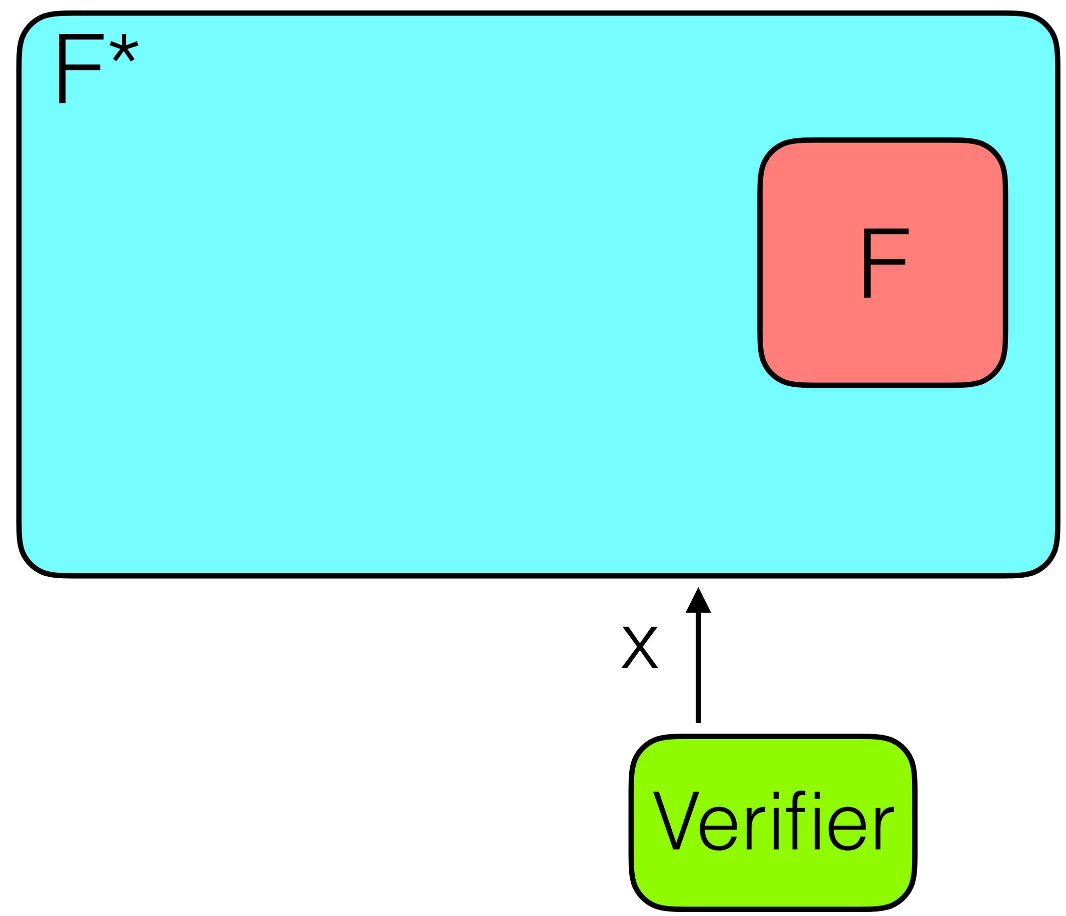
Suppose F passes the linearity test w.p. $1 - \varepsilon$

Goal: show F $\approx$ quasi-dist over linear f's

$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$

Bad example: F = | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Then $\Delta(F, Q)$ is large for all Q!
Fix: define F*, a “smooth” F
(self-correction)



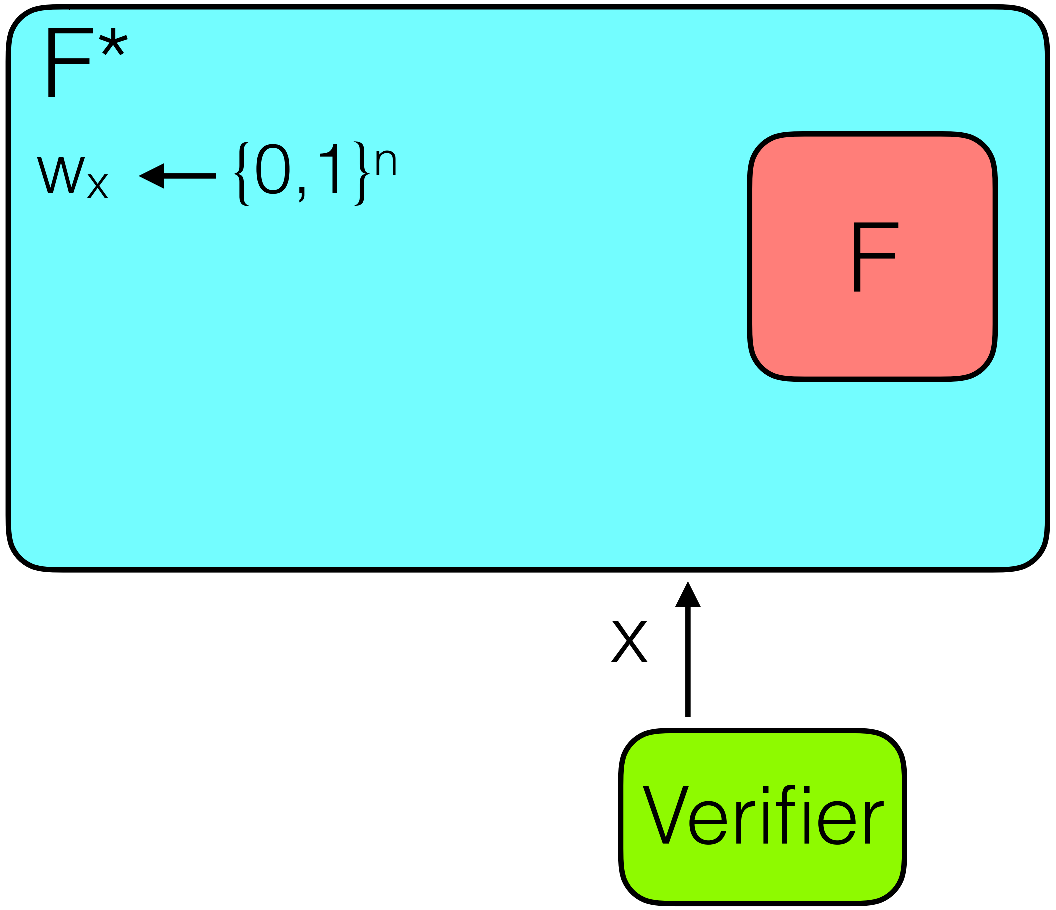
Suppose F passes the linearity test w.p. 1 - ε

Goal: show F ≈ quasi-dist over linear f's

$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$

Bad example: F = | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Then Δ(F, Q) is large for all Q!
Fix: define F*, a "smooth" F
(self-correction)



Suppose F passes the linearity test w.p. $1 - \varepsilon$

Goal: show F $\approx$ quasi-dist over linear f's

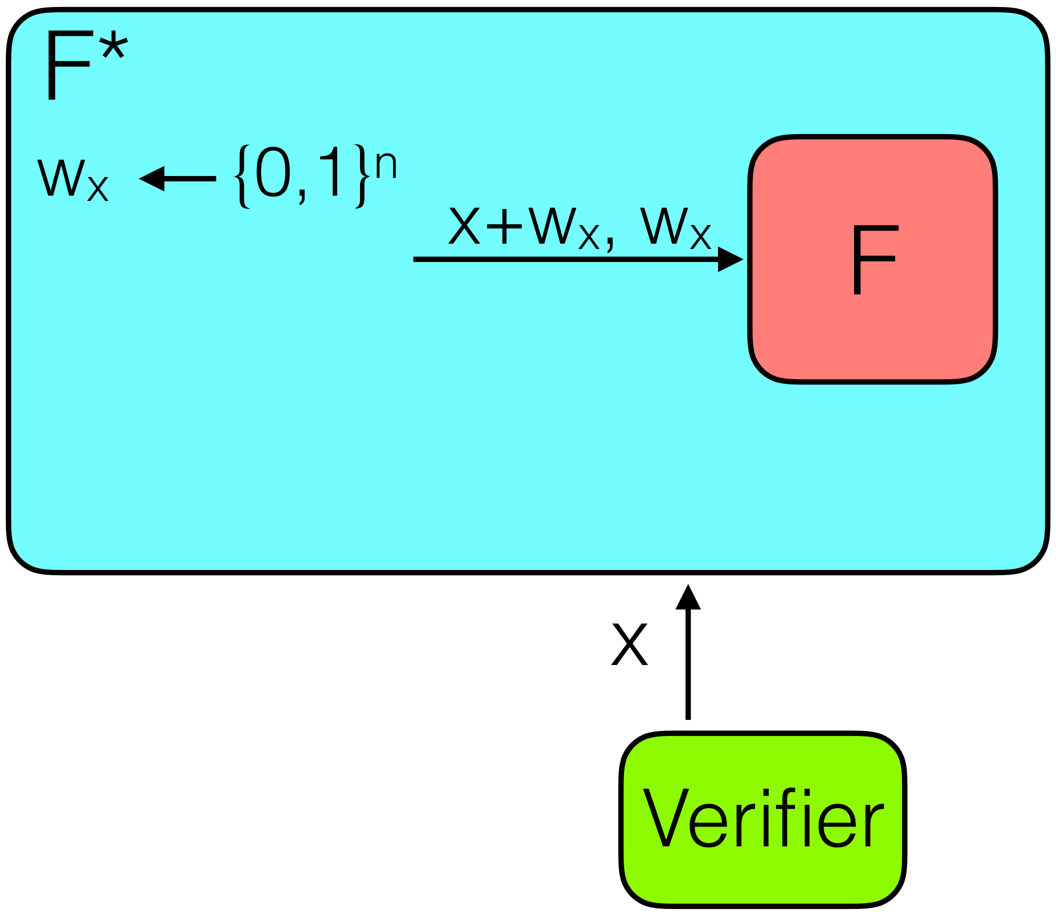
$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$

Bad example: F = | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Then $\Delta(F, Q)$ is large for all Q!

Fix: define F*, a "smooth" F

(self-correction)



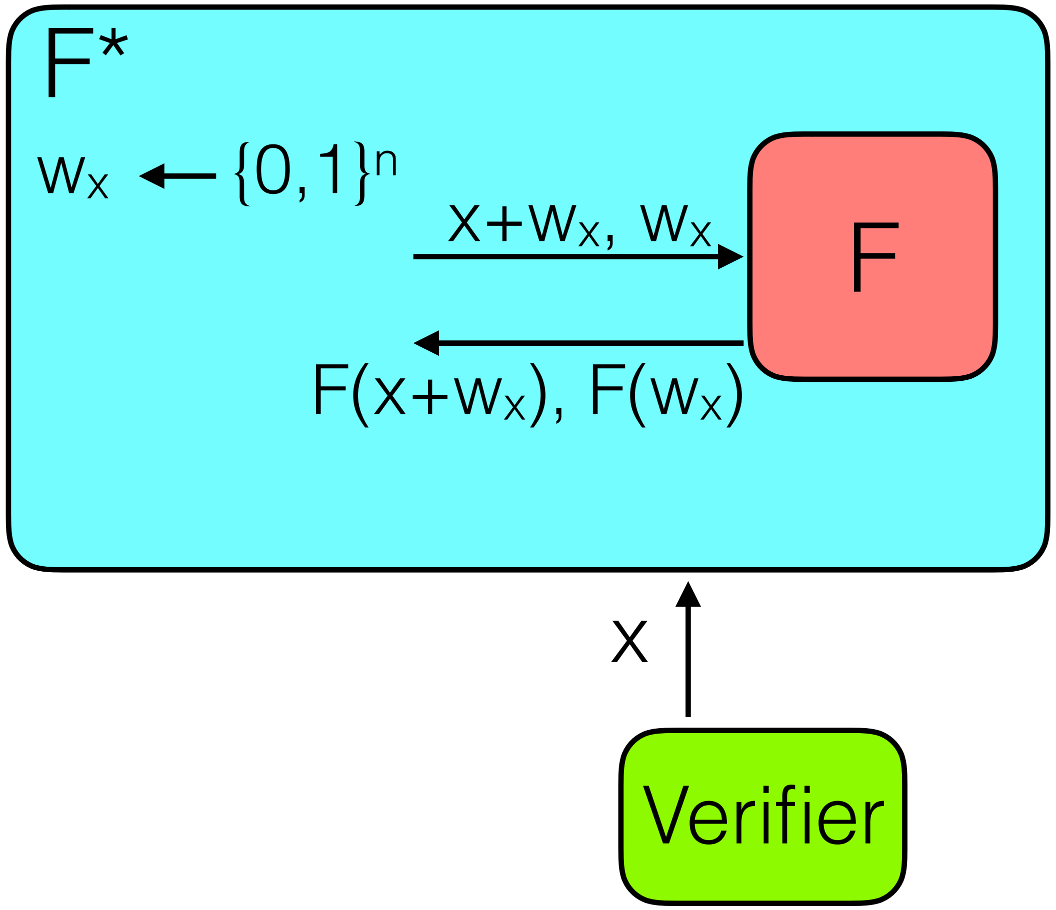
Suppose F passes the linearity test w.p. 1 - ε

Goal: show F ≈ quasi-dist over linear f's

$$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$$

Bad example: F = | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Then Δ(F, Q) is large for all Q!
Fix: define F*, a "smooth" F
(self-correction)



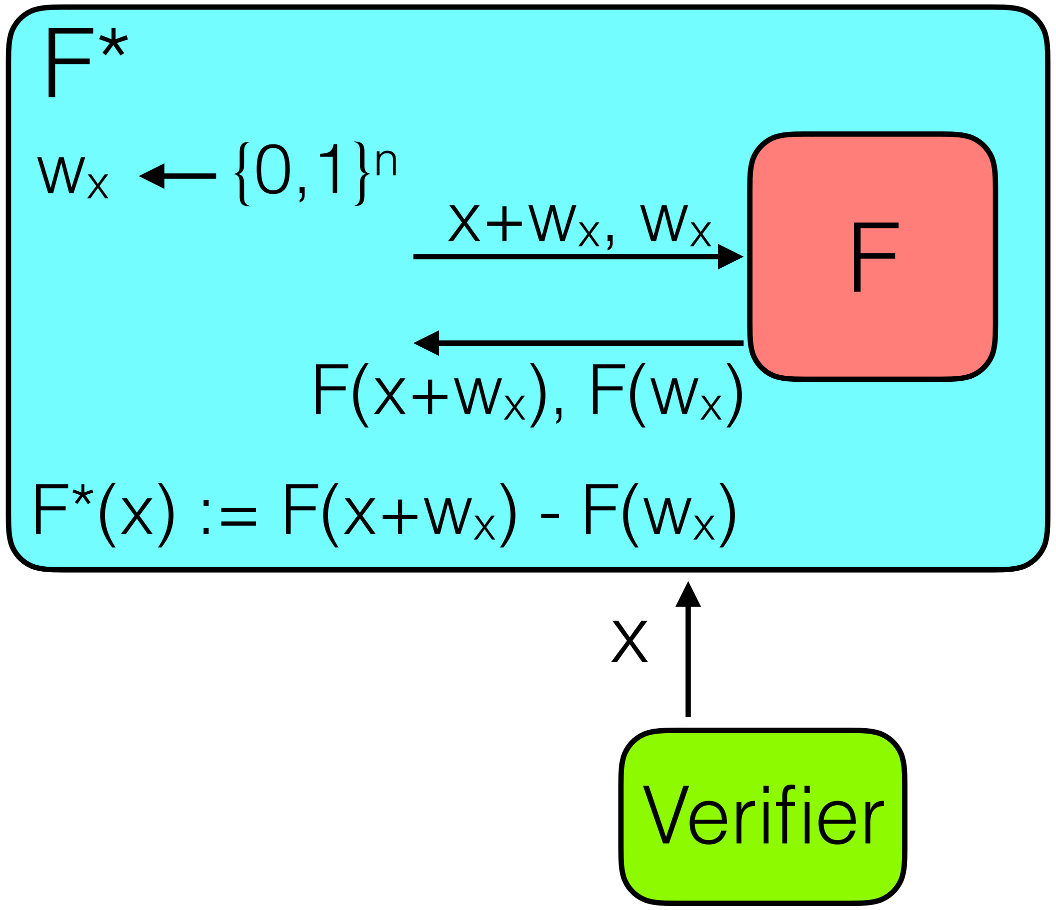
Suppose F passes the linearity test w.p. $1 - \varepsilon$

Goal: show F $\approx$ quasi-dist over linear f's

$$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$$

Bad example: F = | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Then $\Delta(F, Q)$ is large for all Q!
Fix: define F*, a "smooth" F
(self-correction)



Suppose F passes the linearity test w.p. $1 - \varepsilon$

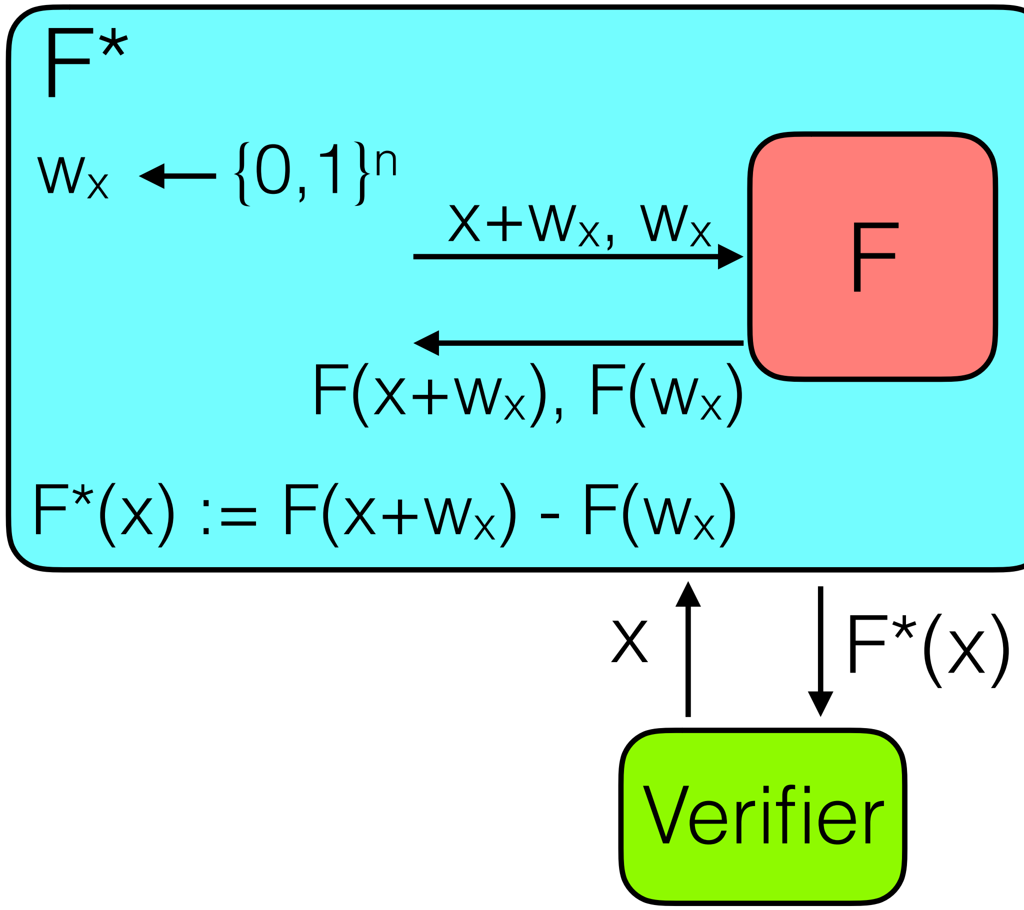
Goal: show F $\approx$ quasi-dist over linear f's

$$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$$

Bad example: F =

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

Then $\Delta(F, Q)$ is large for all Q!
Fix: define F*, a "smooth" F
(self-correction)



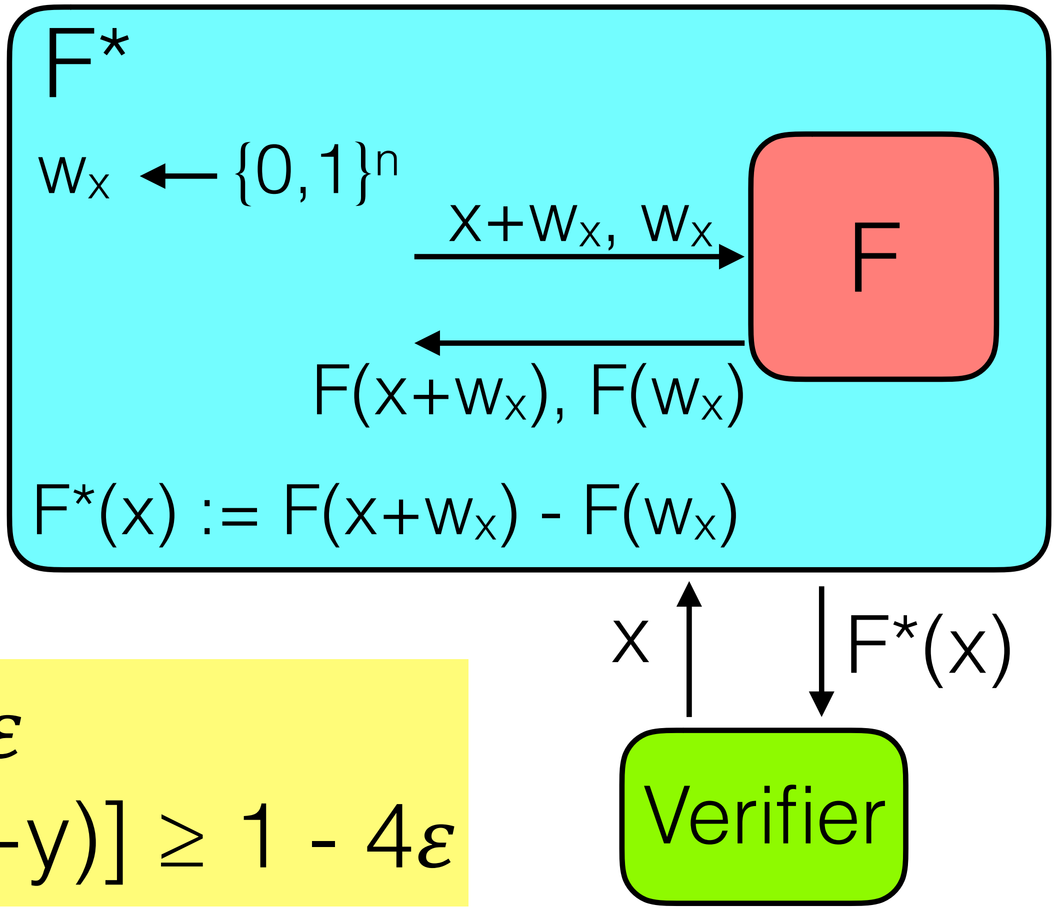
Suppose F passes the linearity test w.p. $1 - \varepsilon$

Goal: show F $\approx$ quasi-dist over linear f's

$\Delta(F, Q) = \max_S \Delta_{TV}(F_S, Q_S)$

Bad example: F = | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Then $\Delta(F, Q)$ is large for all Q!
Fix: define F*, a "smooth" F
(self-correction)



Average to worst case:

If $\Pr_{x,y,F}[F(x) + F(y) = F(x+y)] \geq 1 - \varepsilon$
then $\forall x,y,\ \Pr_{F^*}[F^*(x) + F^*(y) = F^*(x+y)] \geq 1 - 4\varepsilon$

Theorem 3

If Pr[F passes] ≥ 1 - ε then F* is $O_K(\varepsilon)$-close to a quasi-dist over LIN

Theorem 3

If Pr[F passes] ≥ 1 - ε then F* is $O_K(\varepsilon)$-close to a quasi-dist over LIN

Summary:

Theorem 3

If Pr[F passes] $\geq$ 1 - ε then F* is $O_K(\varepsilon)$-close to a quasi-dist over LIN

Summary:

If F passes the linearity test w.h.p, then its self-correction can be well-approximated by a quasi-dist over LIN.

Theorem 3

If Pr[F passes] ≥ 1 - ε then F* is $O_K(\varepsilon)$-close to a quasi-dist over LIN

Summary:

If F passes the linearity test w.h.p, then its self-correction can be well-approximated by a quasi-dist over LIN.

Property testing is possible against non-signaling strategies.

Theorem 3

If Pr[F passes] $\geq$ 1 - ε then F* is $O_K(\varepsilon)$-close to a quasi-dist over LIN

Summary:

If F passes the linearity test w.h.p, then its self-correction can be well-approximated by a quasi-dist over LIN.

Property testing is possible against non-signaling strategies. The above is a sample of what you can prove.

Theorem 3

If Pr[F passes] ≥ 1 - ε then F* is $O_K(\varepsilon)$-close to a quasi-dist over LIN

Summary:

If F passes the linearity test w.h.p, then its self-correction can be well-approximated by a quasi-dist over LIN.

Property testing is possible against non-signaling strategies.
The above is a sample of what you can prove.

Quasi-distributions are essential.

Theorem 3

If Pr[F passes] ≥ 1 - ε then F* is $O_K(\varepsilon)$-close to a quasi-dist over LIN

Summary:

If F passes the linearity test w.h.p, then its self-correction can be well-approximated by a quasi-dist over LIN.

Property testing is possible against non-signaling strategies.
The above is a sample of what you can prove.

Quasi-distributions are essential.
Not just a technique! Can't state results without them.

Thanks!

full version available on ECCC
(TR18-067)

Non-Signaling Players

Non-Signaling Players

Definition:

A k-non-signaling player P is a collection of distributions $\{F_{(x1, \ldots, xk)}\}$ over functions f: [k] → {0,1}, ∀ tuples $(x_1, \ldots, x_k)$ that satisfies the **non-signaling property:**

∀ $(x_1, \ldots, x_k), (y_1, \ldots, y_k)$ where

$S = \{i : x_i = y_i\}$, then

$F_{(x1, \ldots, xk)}|_S \equiv F_{(y1, \ldots, yk)}|_S$

Non-Signaling Players

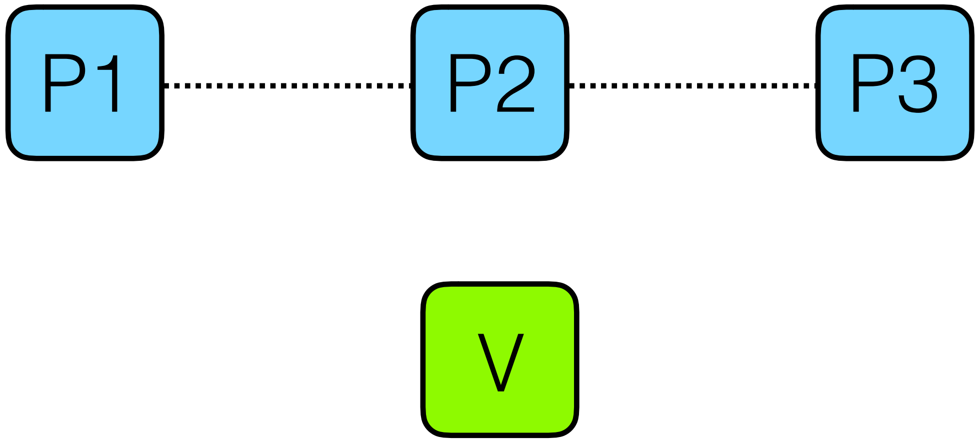
Definition:

A k-non-signaling player P is a collection of distributions $\{F_{(x1, \ldots, xk)}\}$ over functions f: [k] → {0,1}, ∀ tuples $(x_1, \ldots, x_k)$ that satisfies the **non-signaling property:**

∀ $(x_1, \ldots, x_k), (y_1, \ldots, y_k)$ where

$S = \{i : x_i = y_i\}$, then

$F_{(x1, \ldots, xk)}|_S \equiv F_{(y1, \ldots, yk)}|_S$



Non-Signaling Players

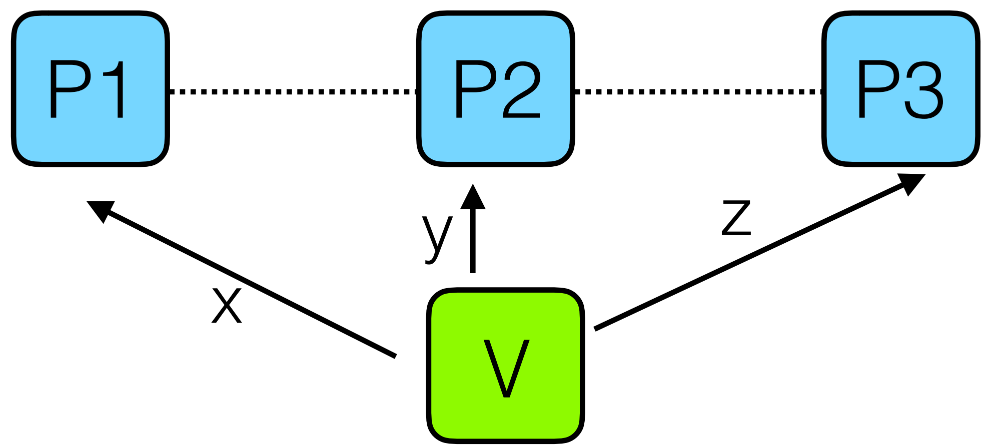
Definition:

A k-non-signaling player P is a collection of distributions $\{F_{(x1, \ldots, xk)}\}$ over functions f: $[k] \to \{0,1\}$, $\forall$ tuples $(x_1, \ldots, x_k)$ that satisfies the **non-signaling property:**

$\forall$ $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k)$ where

$S = \{i : x_i = y_i\}$, then

$F_{(x1, \ldots, xk)} |_S \equiv F_{(y1, \ldots, yk)} |_S$



Non-Signaling Players

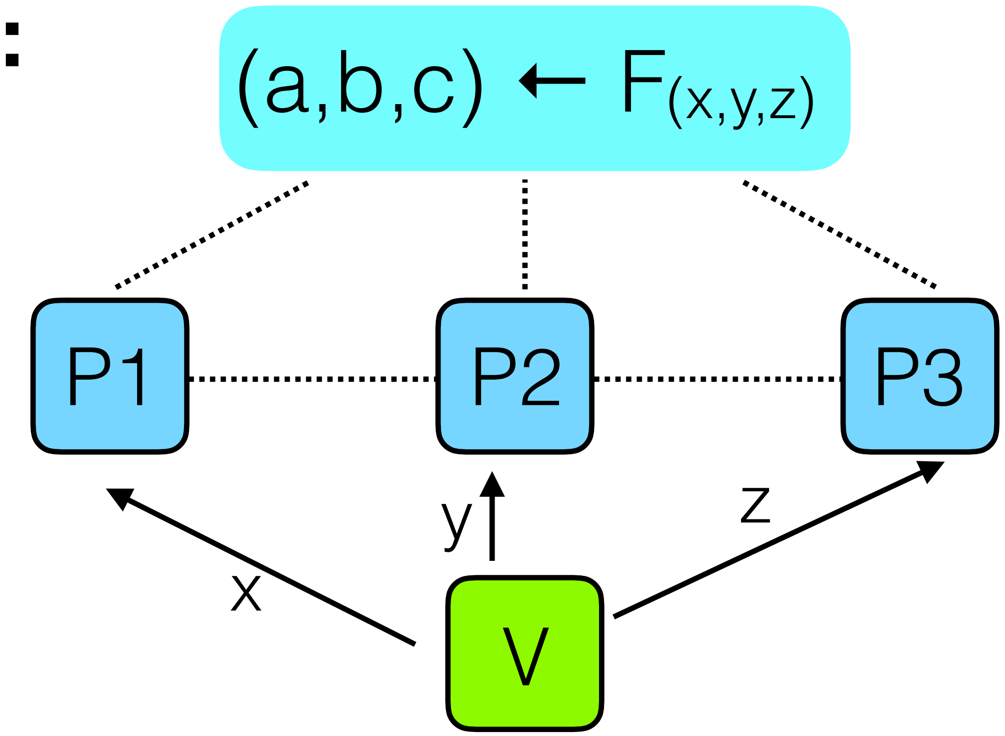
Definition:

A k-non-signaling player P is a collection of distributions $\{F_{(x1, \ldots, xk)}\}$ over functions f: $[k] \to \{0,1\}$, $\forall$ tuples $(x_1, \ldots, x_k)$ that satisfies the **non-signaling property:**

$\forall (x_1, \ldots, x_k), (y_1, \ldots, y_k)$ where

$S = \{i : x_i = y_i\}$, then

$F_{(x1, \ldots, xk)}|_S \equiv F_{(y1, \ldots, yk)}|_S$



Non-Signaling Players

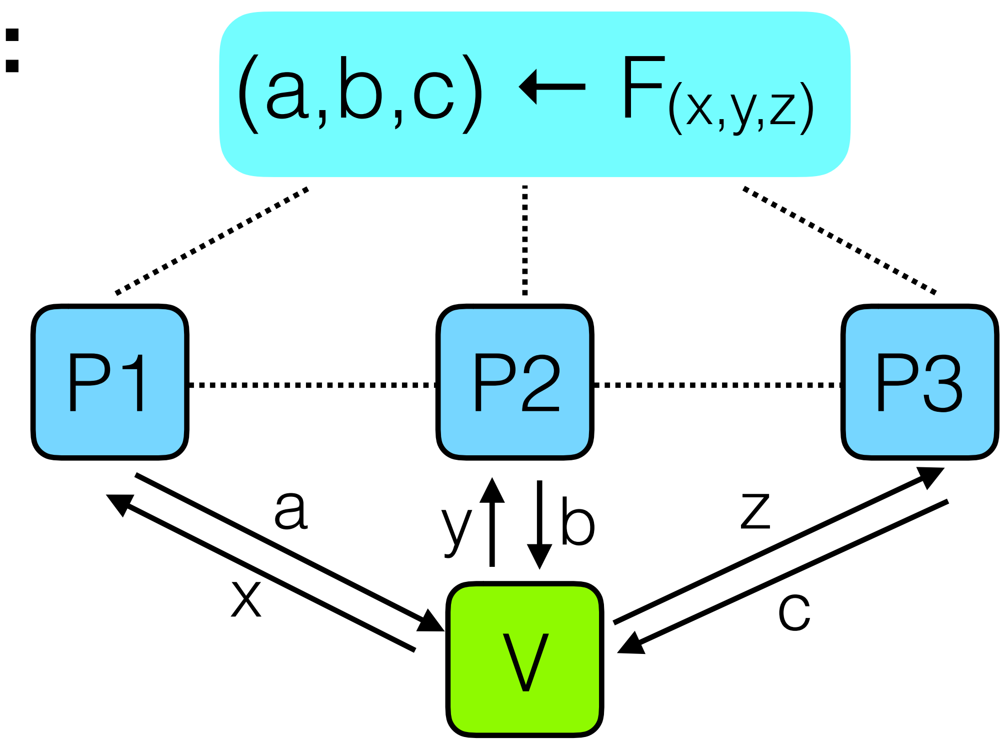
Definition:

A k-non-signaling player P is a collection of distributions $\{F_{(x1,\ \dots,\ xk)}\}$ over functions $f: [k] \to \{0,1\}$, $\forall$ tuples $(x_1, \dots, x_k)$ that satisfies the **non-signaling property:**

$\forall\ (x_1, \dots, x_k), (y_1, \dots, y_k)$ where

$S = \{i : x_i = y_i\}$, then

$F_{(x1,\ \dots,\ xk)}\,|_S \equiv F_{(y1,\ \dots,\ yk)}\,|_S$



Non-Signaling Players

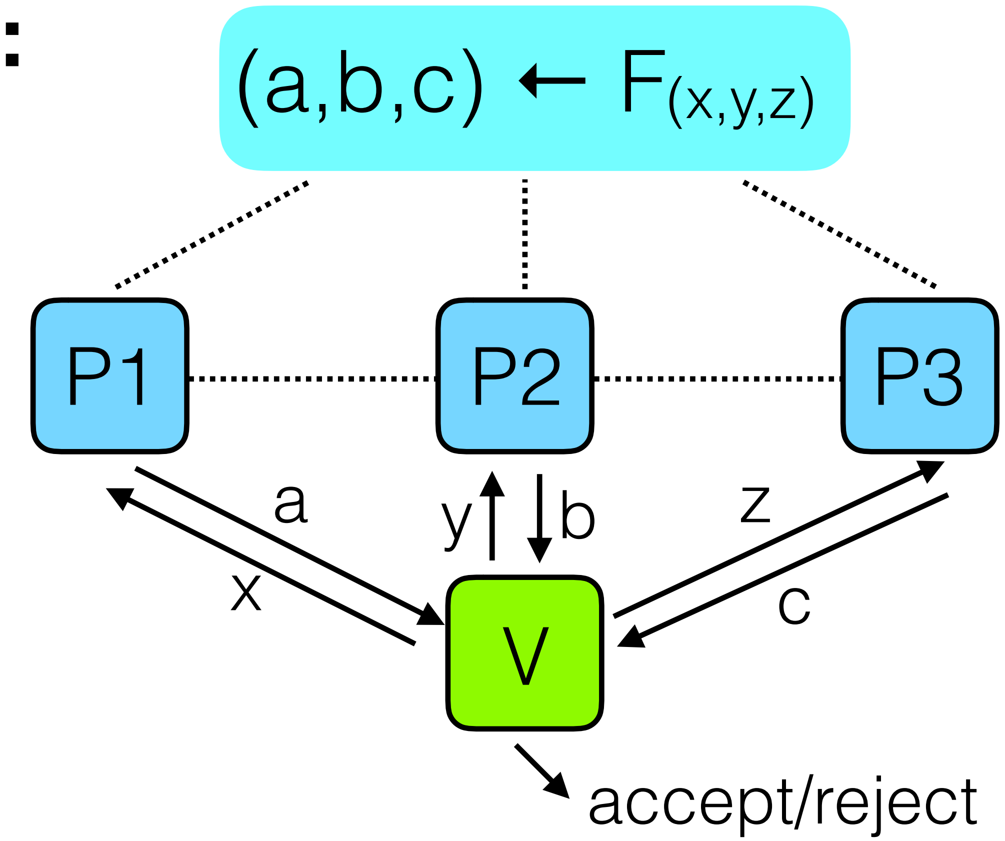
Definition:

A k-non-signaling player P is a collection of distributions $\{F_{(x1, \ldots, xk)}\}$ over functions f: [k] → {0,1}, ∀ tuples $(x_1, \ldots, x_k)$ that satisfies the **non-signaling property:**

∀ $(x_1, \ldots, x_k)$, $(y_1, \ldots, y_k)$ where

$S = \{i : x_i = y_i\}$, then

$F_{(x1, \ldots, xk)}|_S \equiv F_{(y1, \ldots, yk)}|_S$



Non-Signaling Players

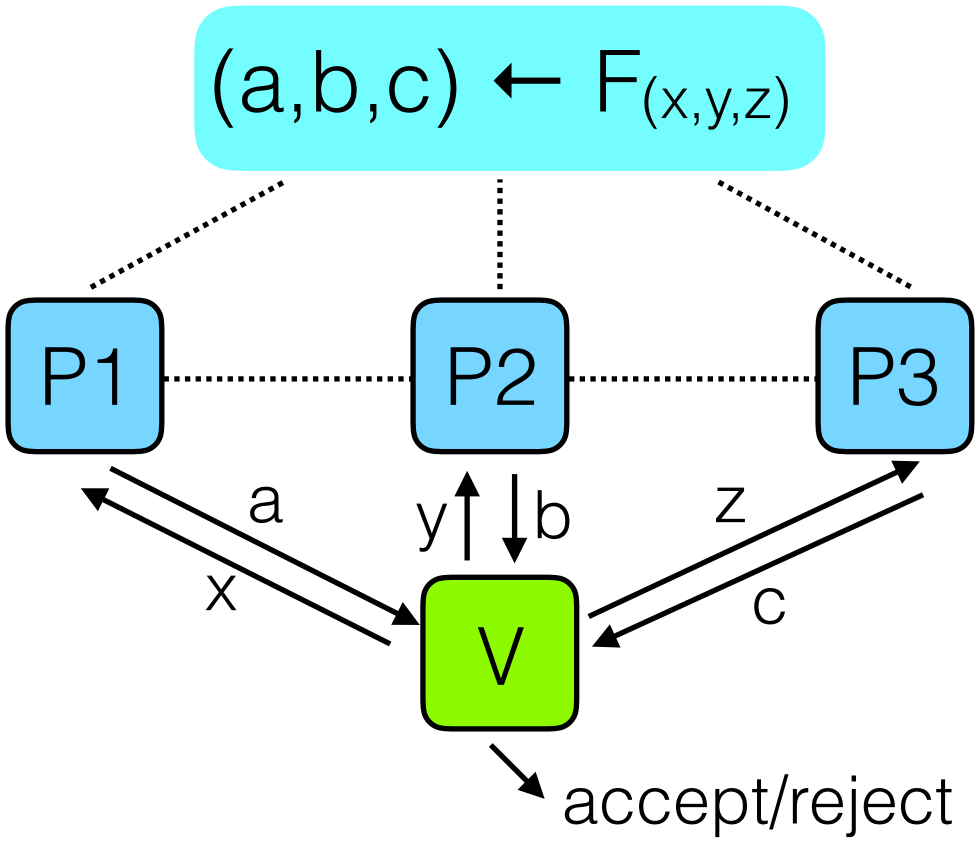
Definition:

A k-non-signaling player P is a collection of distributions $\{F_{(x1, \ldots, xk)}\}$ over functions f: $[k] \rightarrow \{0,1\}$, $\forall$ tuples $(x_1, \ldots, x_k)$ that satisfies the **non-signaling property:**

$\forall (x_1, \ldots, x_k), (y_1, \ldots, y_k)$ where

$S = \{i : x_i = y_i\}$, then

$F_{(x1, \ldots, xk)} |_S \equiv F_{(y1, \ldots, yk)} |_S$



Analogues of all three theorems hold for ns players

Non-Signaling Players

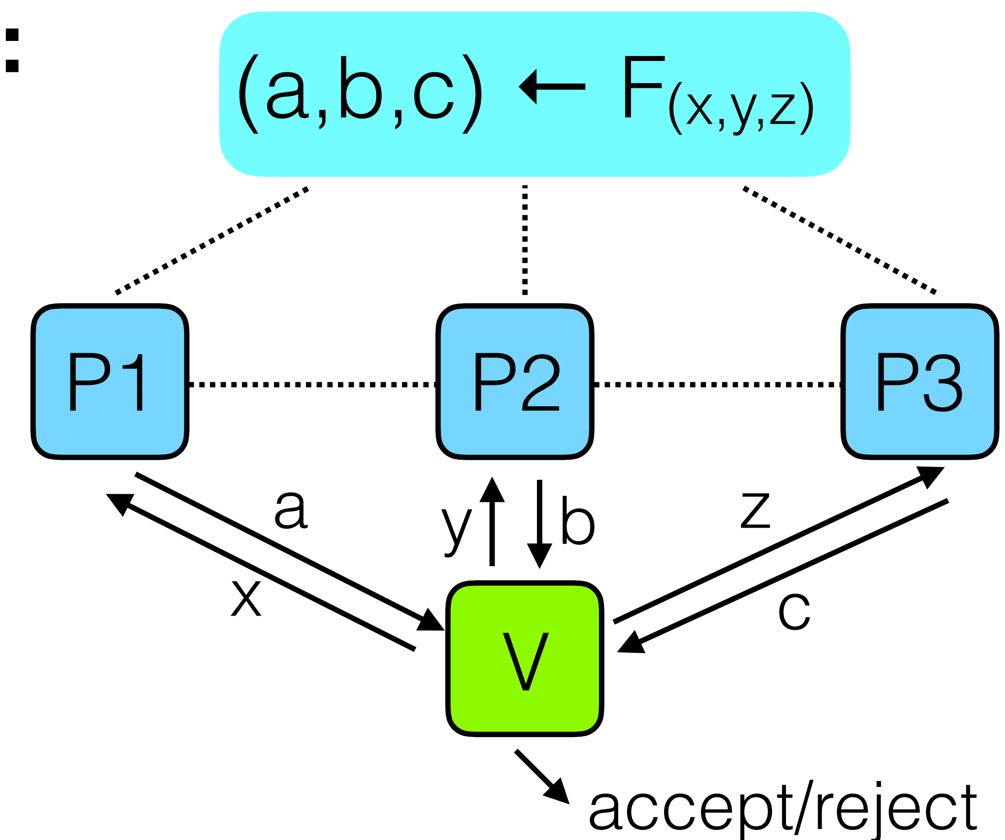
Definition:

A k-non-signaling player P is a collection of distributions $\{F_{(x1, \ldots, xk)}\}$ over functions f: $[k] \to \{0,1\}$, $\forall$ tuples $(x_1, \ldots, x_k)$ that satisfies the **non-signaling property:**

$\forall (x_1, \ldots, x_k), (y_1, \ldots, y_k)$ where

$S = \{i : x_i = y_i\}$, then

$F_{(x1, \ldots, xk)}|_S \equiv F_{(y1, \ldots, yk)}|_S$



Analogues of all three theorems hold for ns players

Theorem 1 for players

k-non-signaling players ⟷ local quasi-distributions over k-tuples of f's