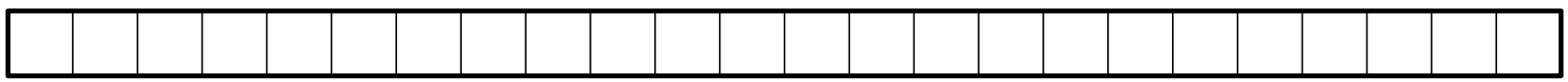
Monochromatic corners and Number-On-Forehead complexity

Julien Duron
(University of Warsaw, Supported by ERC BUKA)

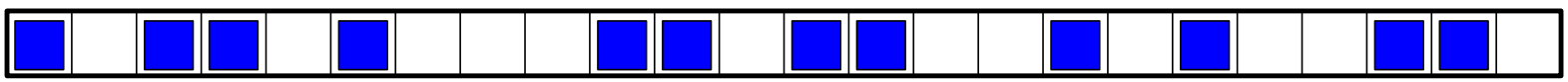
Roth's theorem

$[N]$



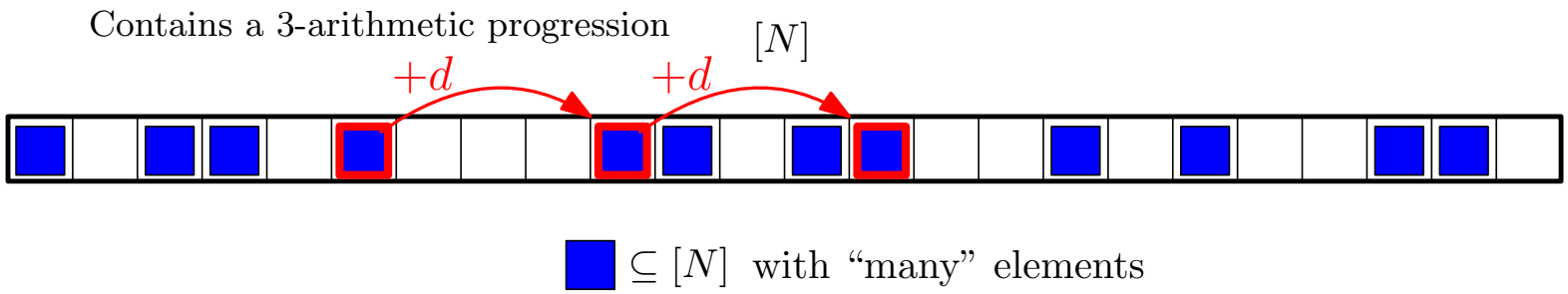
Roth's theorem

$[N]$



$\subseteq [N]$ with "many" elements

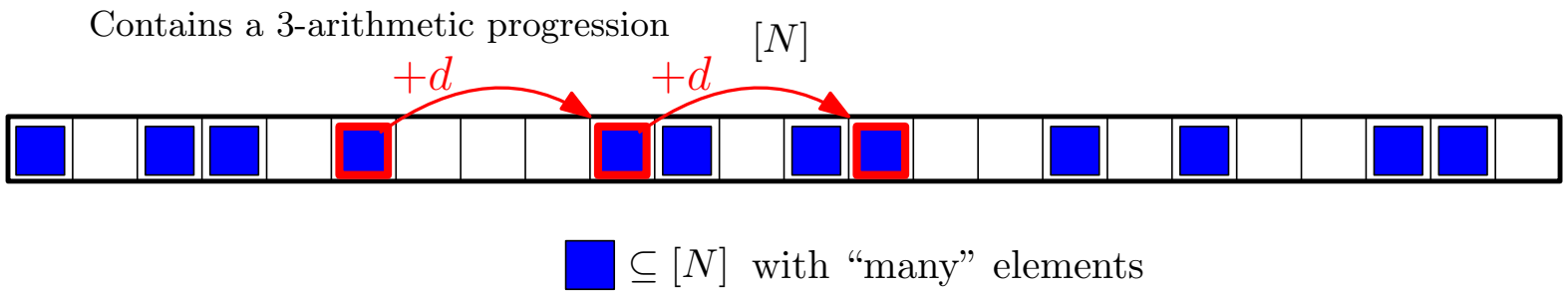
Roth's theorem



Roth's theorem

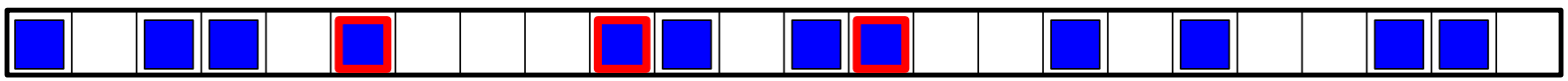
k-Arithmetic progression

$x, x + d, x + 2d, \ldots, x + (k - 1) \cdot d$ for some $x, d \in \mathbb{N}^+$.

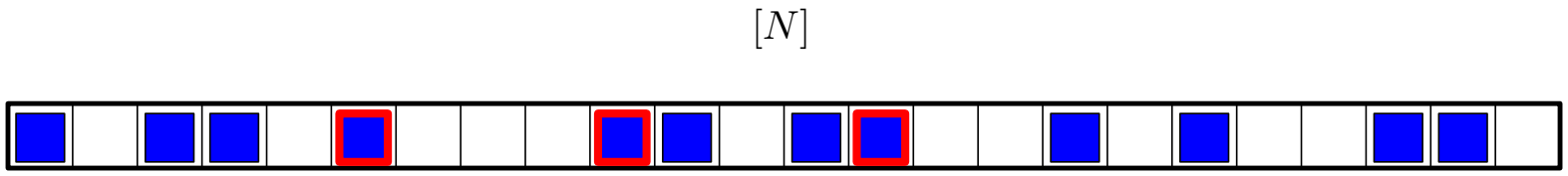


Roth's theorem

$[N]$



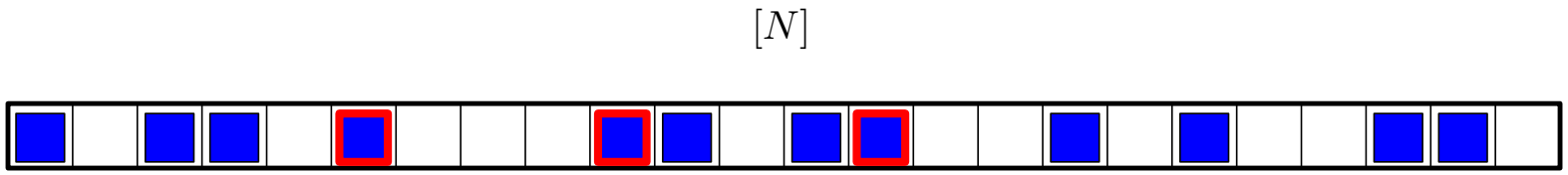
Roth's theorem



Density

The *density* of S in T is $|S|/|T|$.

Roth's theorem



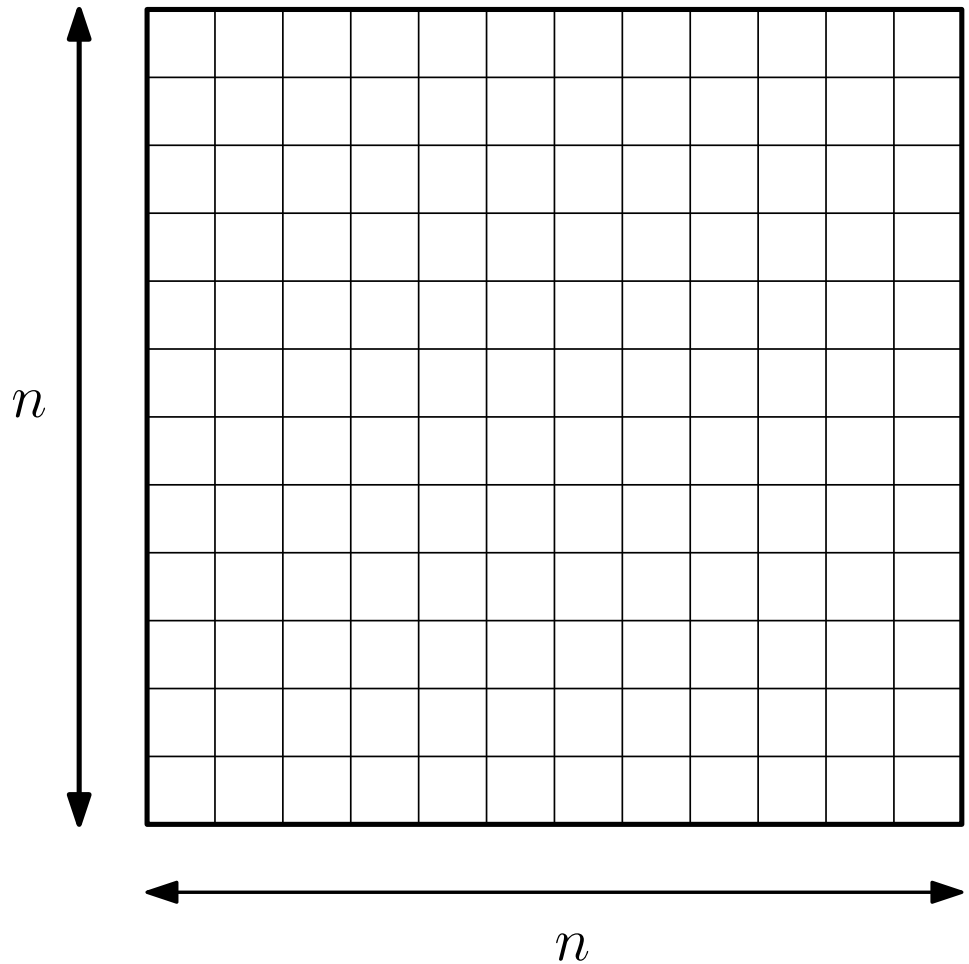
Density

The *density* of S in T is $|S|/|T|$.

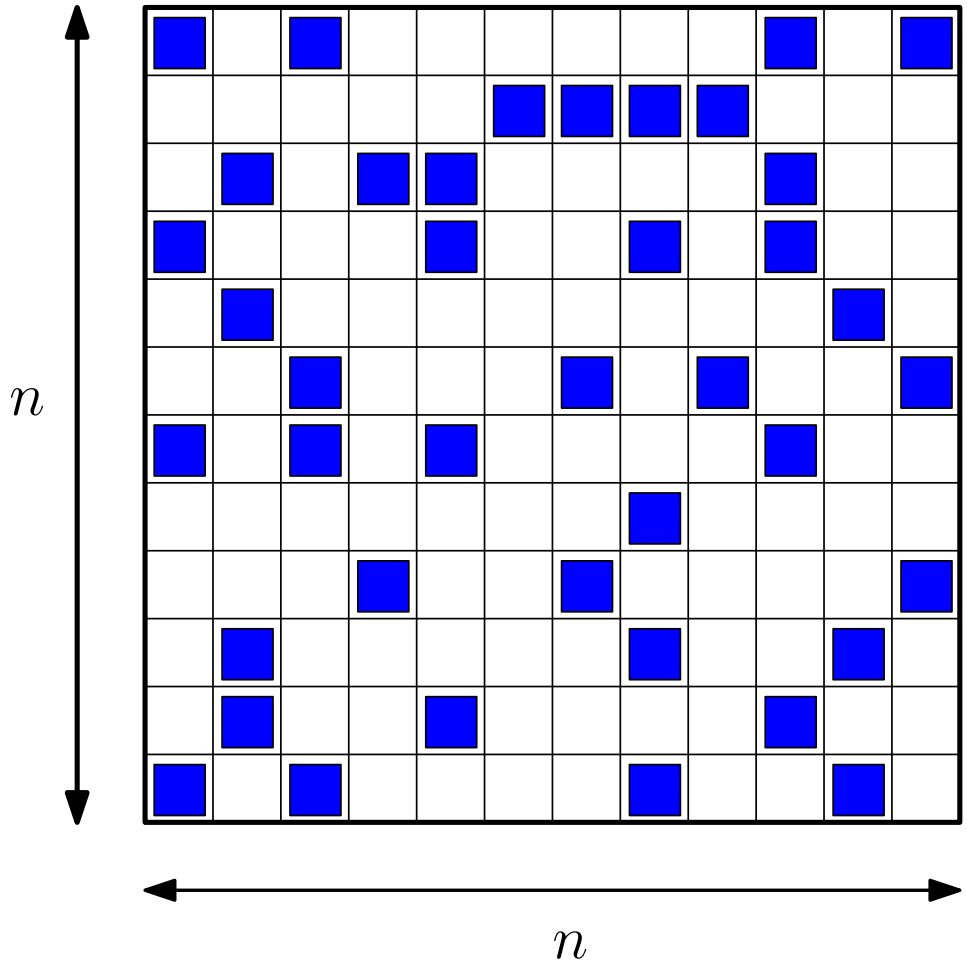
Roth's theorem, 1953

$\forall \epsilon > 0$, there is an N such that
Any $S \subset [N]$ with density $\geqslant \epsilon$ has a 3-arithmetic sequence.

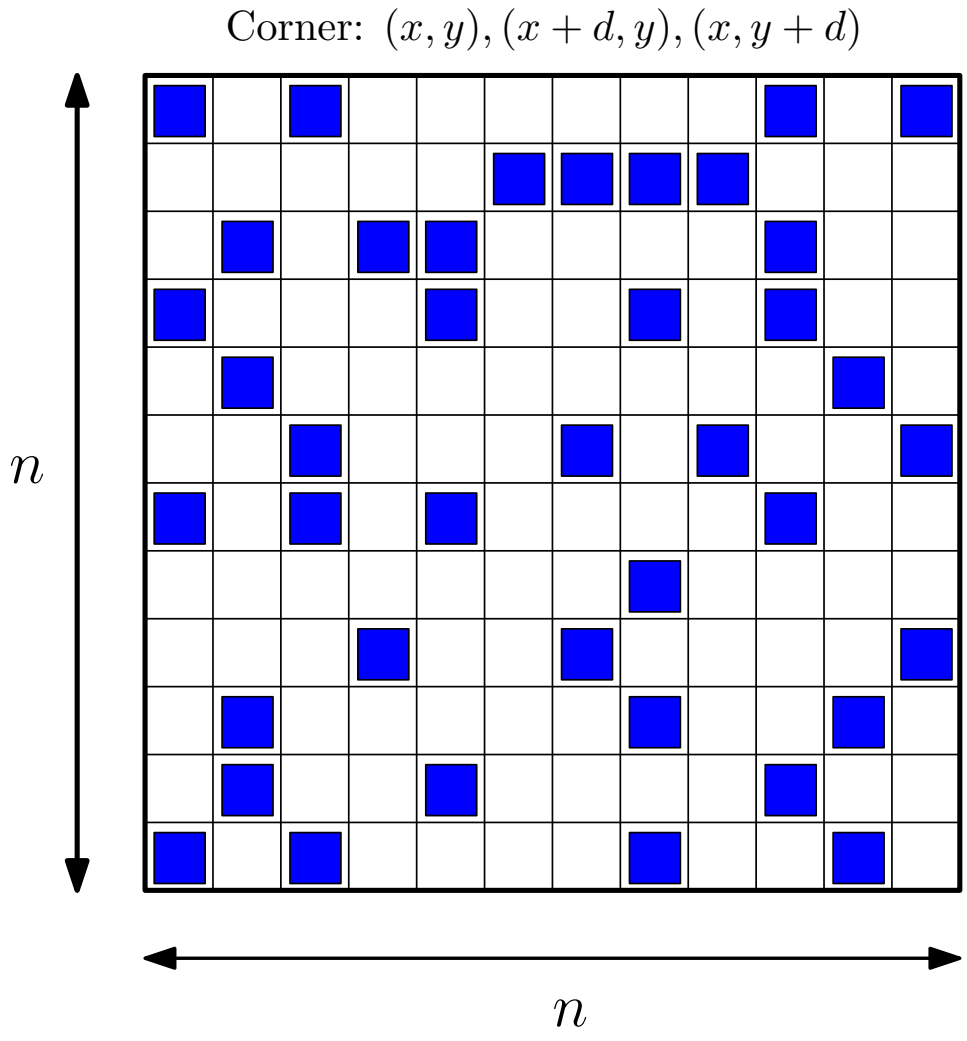
Corners in $[n]^2$: definition



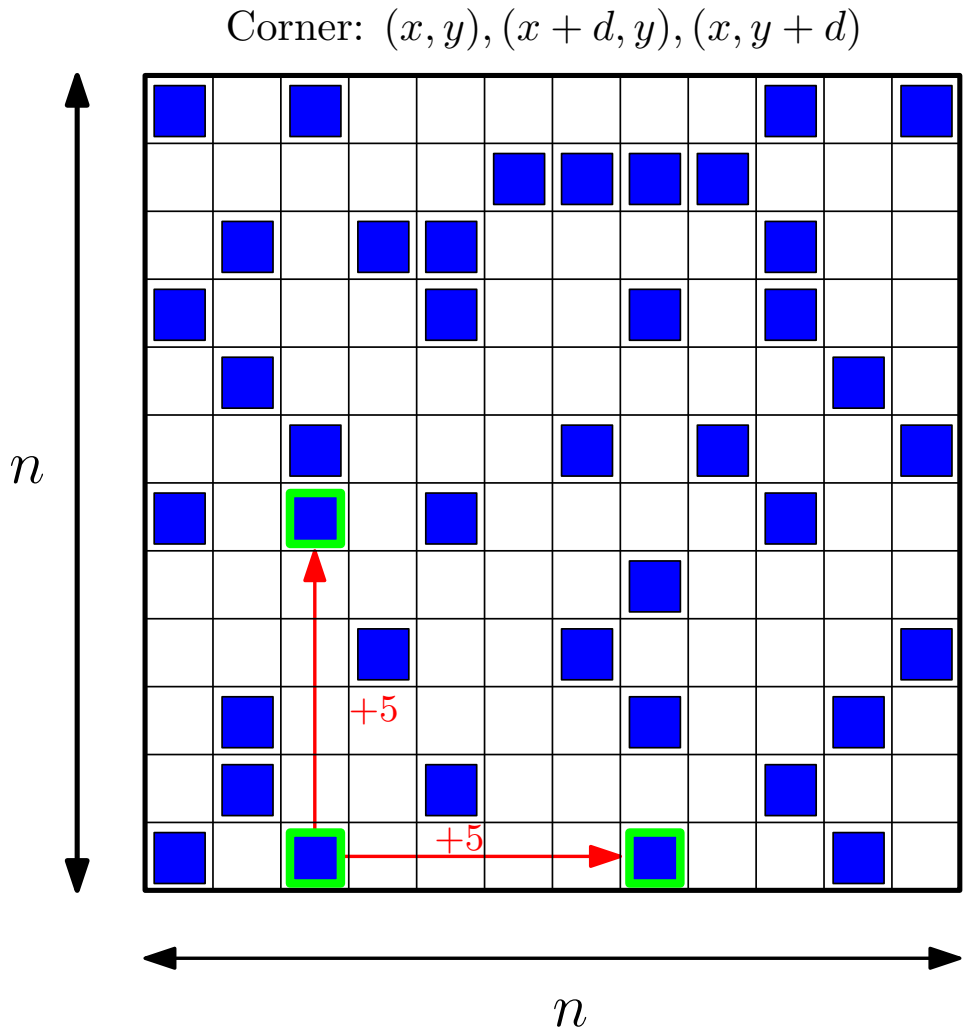
Corners in $[n]^2$: definition



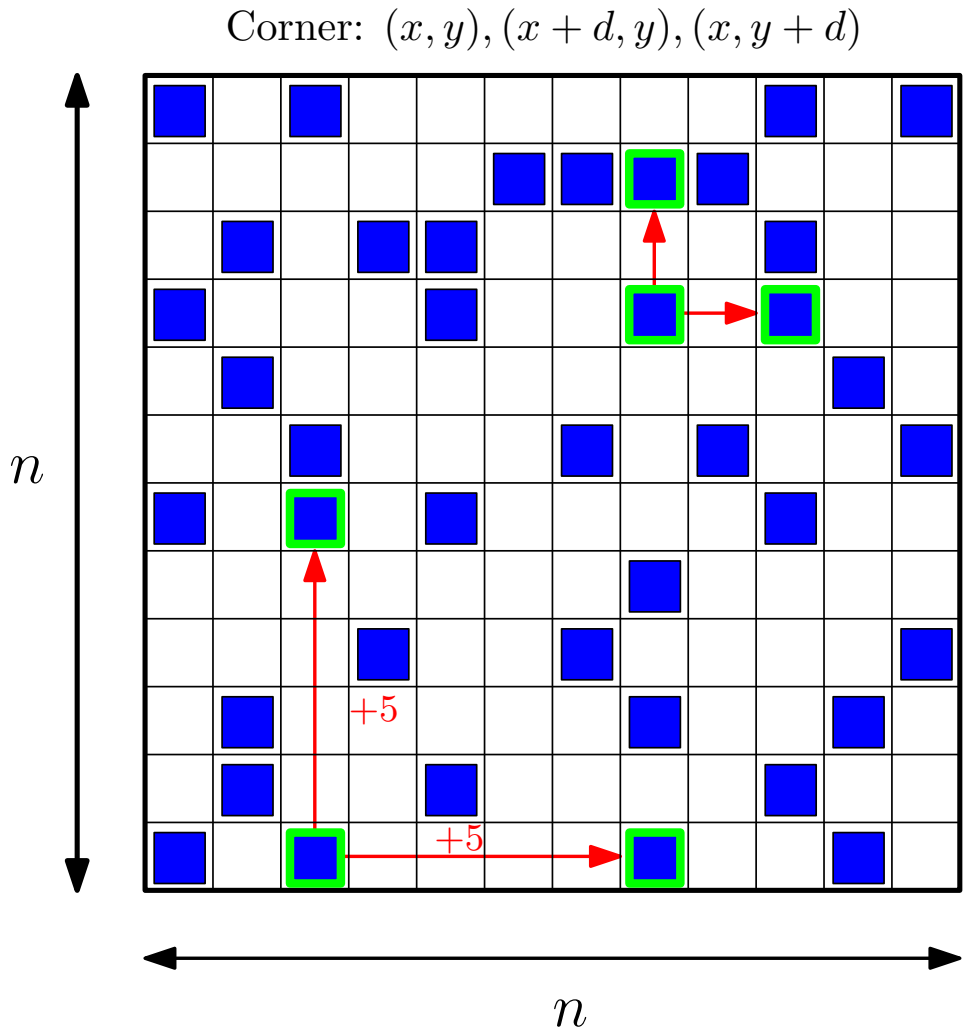
Corners in $[n]^2$: definition



Corners in $[n]^2$: definition



Corners in $[n]^2$: definition

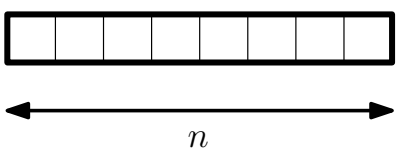


Corners theorem

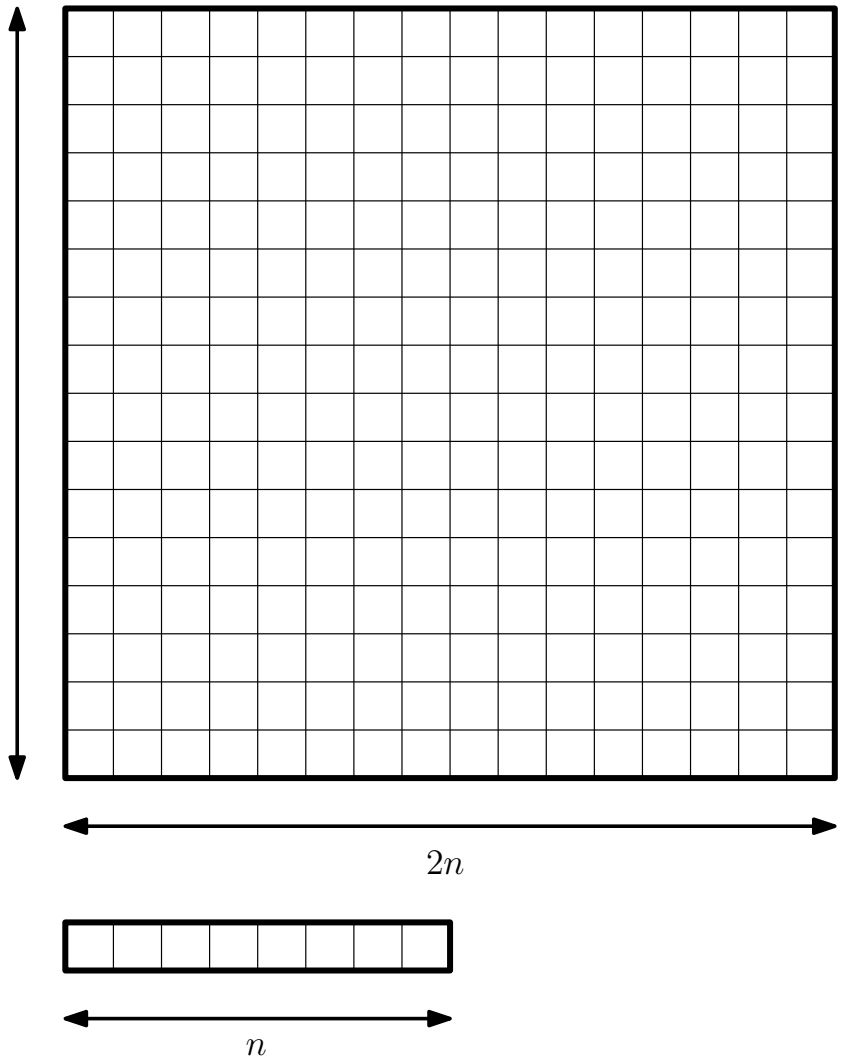
Corners theorem [Ajtai, Szemerédi, 1974]

$\forall \epsilon > 0$, there is an N such that
Any $S \subset [N]^2$ with density $\geqslant \epsilon$ contains a corner.

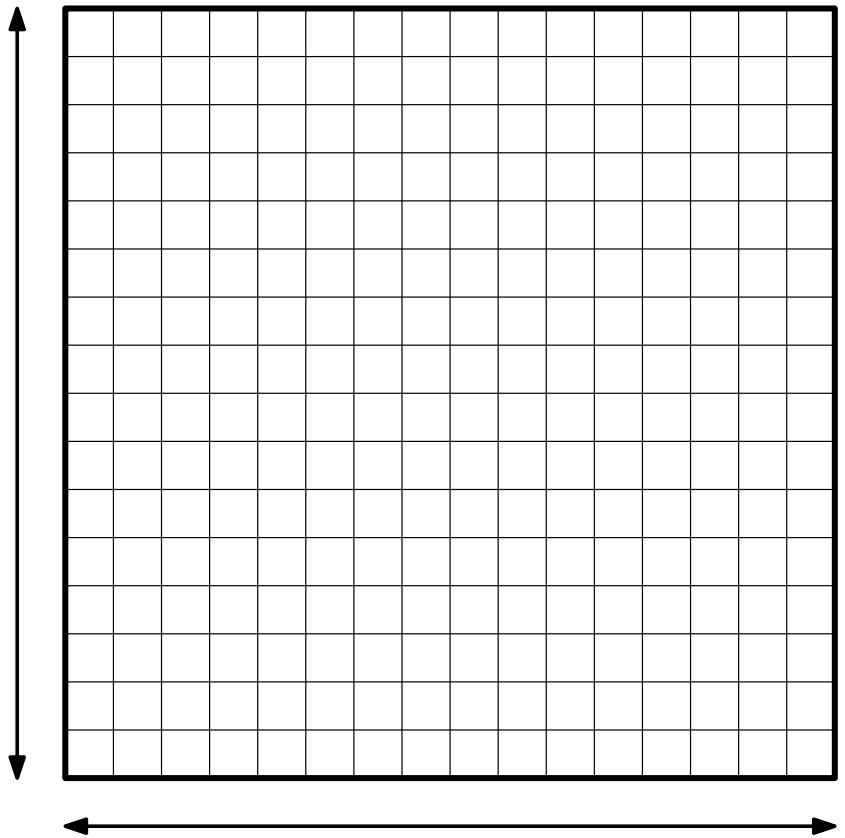
Corner theorem $\Rightarrow$ Roth theorem (folklore)



Corner theorem $\Rightarrow$ Roth theorem (folklore)

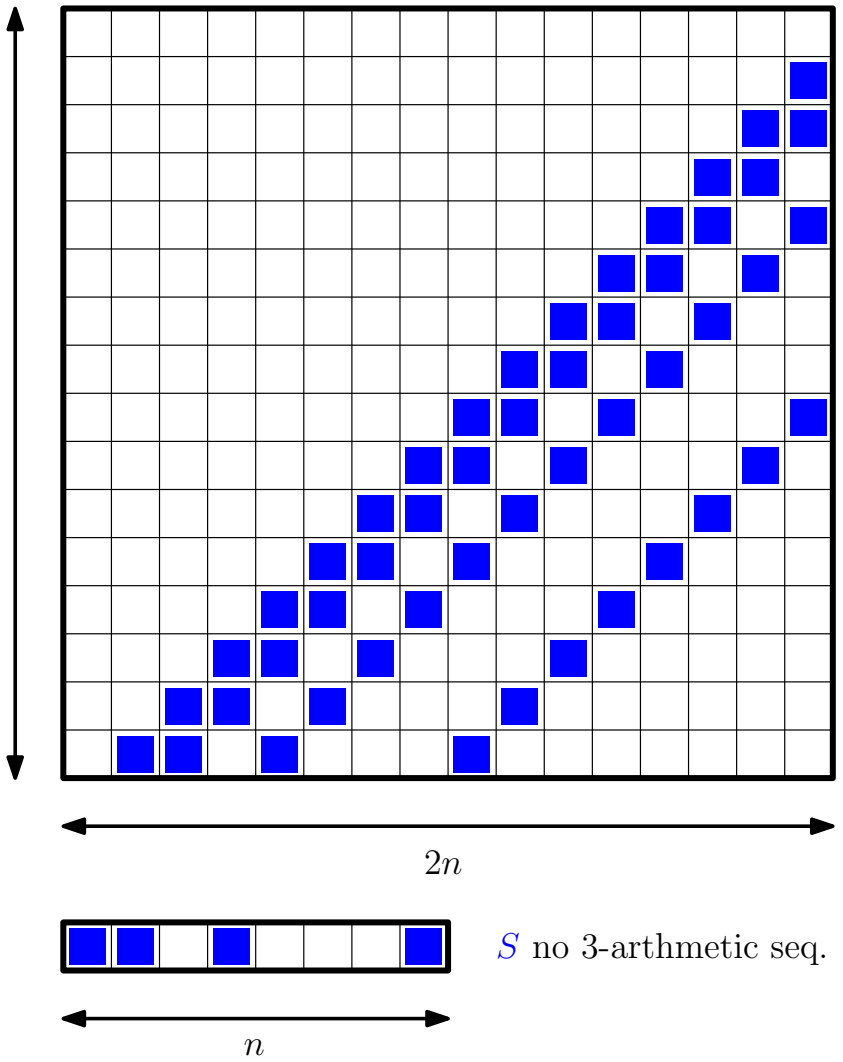


Corner theorem $\Rightarrow$ Roth theorem (folklore)



S no 3-arthmetic seq.

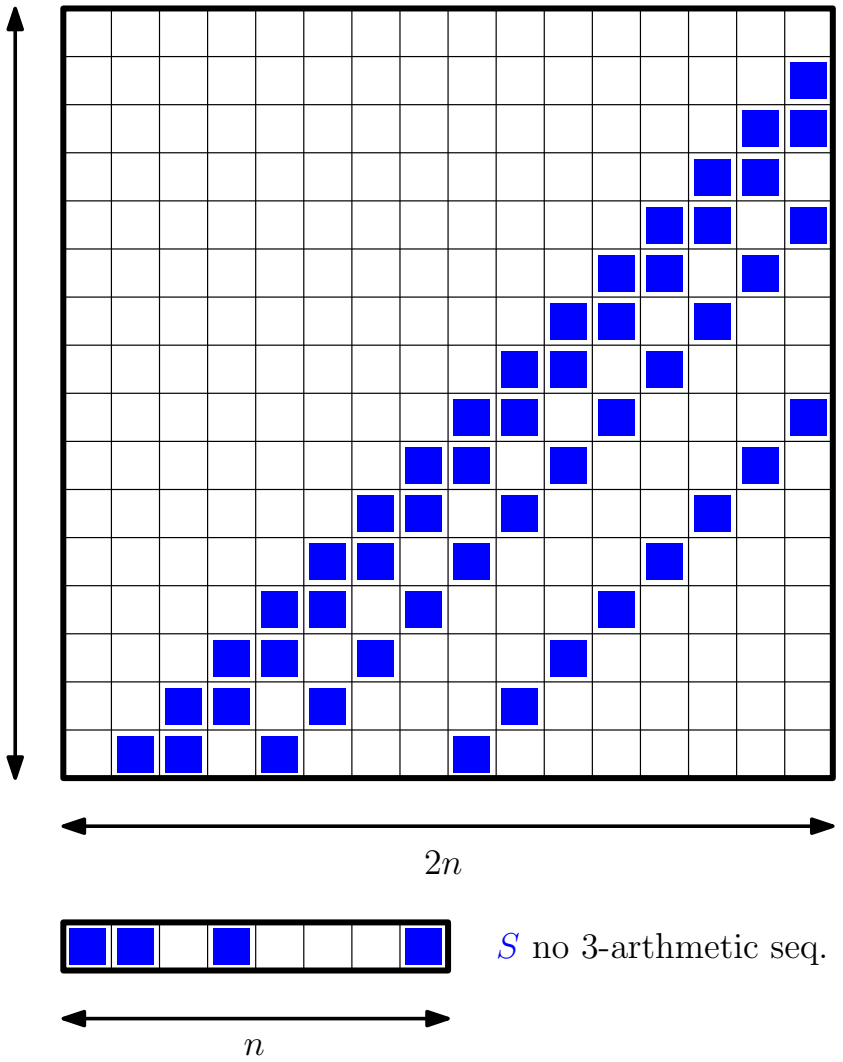
Corner theorem $\Rightarrow$ Roth theorem (folklore)



Build A $(x, y) \in A$ iff $x - y \in S$

S no 3-arthmetic seq.

Corner theorem $\Rightarrow$ Roth theorem (folklore)

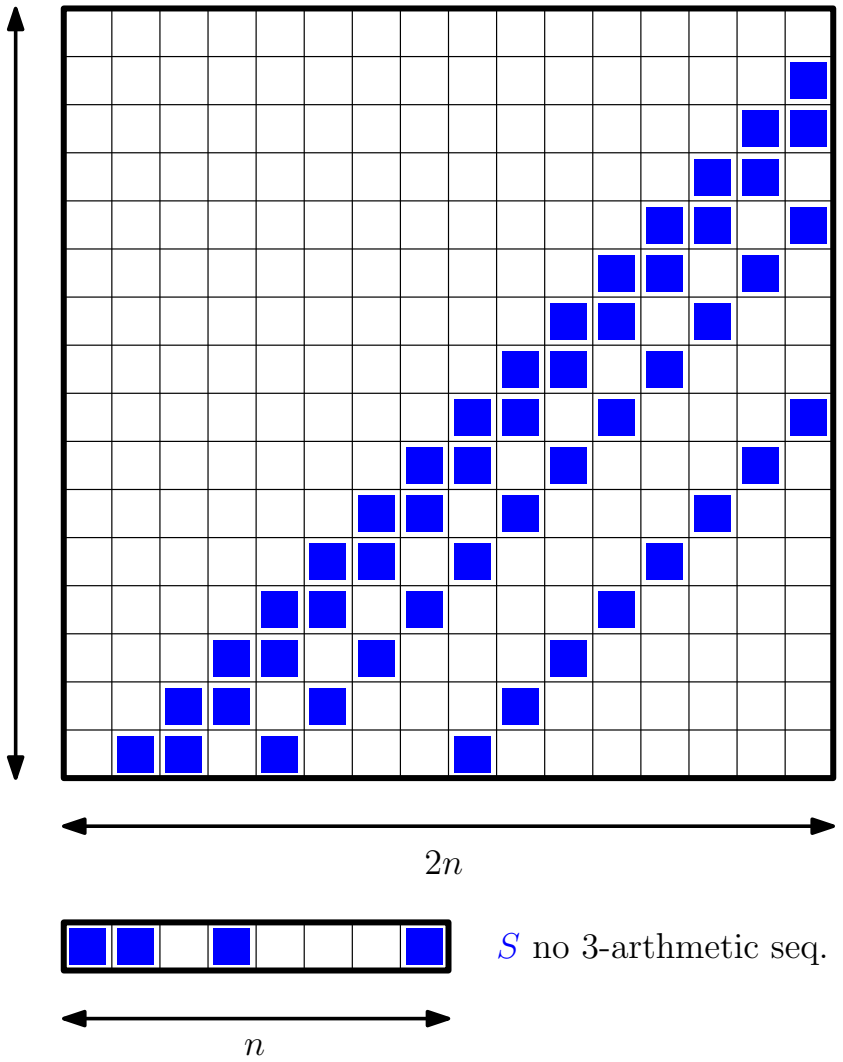


Build A $(x, y) \in A$ iff $x - y \in S$

Density: $|S|/n \cdot 1/4$

S no 3-arthmetic seq.

Corner theorem $\Rightarrow$ Roth theorem (folklore)



Build A $(x, y) \in A$ iff $x - y \in S$

Density: $|S|/n \cdot 1/4$

Corner $\Rightarrow$ 3-arthithmetic seq.

$(x + d, y), (x, y), (x, y + d) \in A$

$\Rightarrow x - y - d, x - y, x + d - y \in S$

S no 3-arthmetic seq.

Szemerédi's theorem

k-Arithmetic progression

Of the form $x, x + d, x + 2d, \ldots, x + (k - 1) \cdot d$ for some $x, d \in \mathbb{N}^+$.

Szemerédi's theorem

k-Arithmetic progression

Of the form $x, x + d, x + 2d, \ldots, x + (k - 1) \cdot d$ for some $x, d \in \mathbb{N}^+$.

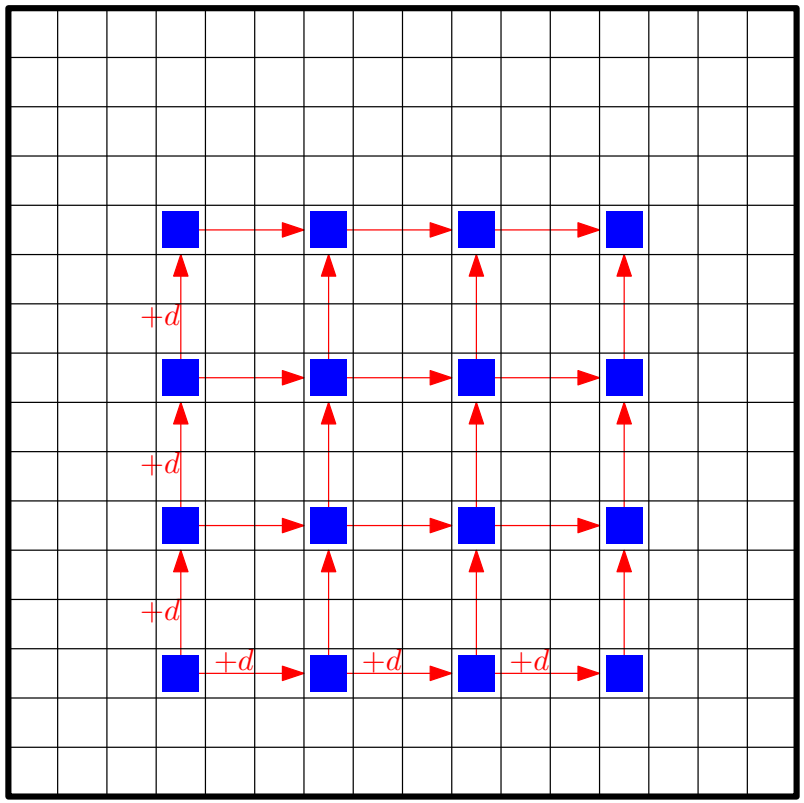
Szemerédi's theorem, 1975

$\forall \epsilon > 0$, $\forall k \in \mathbb{N}^+$, there is a (very large) $N := N(\epsilon, k)$ such that:
$\forall S \subseteq [N]$, density$(S) \geqslant \epsilon \Rightarrow S$ contains a k-arithmetic sequence.

Multi-dimensional Szemerédi's theorem

The k a-dimensional grid

$$\{\overline{x} + (k_1 d, k_2 d, \ldots, k_a d) \ : \ k_i \in [k]\}$$



Multi-dimensional Szemerédi's theorem

Multidim theorem [Furstenberg, Katznelson, 1985]

$\forall \epsilon > 0$, $\forall k \in \mathbb{N}^+$, there is a (very large) $N := N(\epsilon, k) \in \mathbb{N}$ such that $\forall S \subseteq [N]^d$, density$(S) \geqslant \epsilon \Rightarrow S$ contains a k d-Grid.

The question

Szemerédi's theorem

$\forall \epsilon > 0, \forall k \in \mathbb{N}^+$, there is a (very large) $N := N(\epsilon, k) \in \mathbb{N}$ such that $\forall S \subseteq [N]$, density$(S) \geqslant \epsilon \Rightarrow S$ contains some pattern.

The question

Szemerédi's theorem

$\forall \epsilon > 0, \forall k \in \mathbb{N}^+$, there is a (very large) $N := N(\epsilon, k) \in \mathbb{N}$ such that $\forall S \subseteq [N]$, density$(S) \geqslant \epsilon \Rightarrow S$ contains some pattern.

Question

When $N \to \infty$, how small needs $\epsilon := \epsilon(N)$ to be to avoid:

- 3-arithmetic progressions?
- Corners?
- General d-dimensional grids?

What is known about corners?

Theorem [Behrend, 1946]

There is a corner-free set of density $2^{-2.879\sqrt{\log N}}$.

What is known about corners?

Theorem [Behrend, 1946]

There is a corner-free set of density $2^{-2.879\sqrt{\log N}}$.

Lower bound and link with NOF protocols [Alon, Shraibman, 2021]

There is a corner-free set of density $2^{-2.4022\sqrt{\log N}}$.

What is known about corners?

Theorem [Behrend, 1946]

There is a corner-free set of density $2^{-2.879\sqrt{\log N}}$.

Lower bound and link with NOF protocols [Alon, Shraibman, 2021]

There is a corner-free set of density $2^{-2.4022\sqrt{\log N}}$.

Best Lower bound [Green, 2021]

There is a corner-free set of density $2^{-1.822\sqrt{\log N}}$.

What is known about corners?

Best Lower bound [Green, 2021]

There is a corner-free set of density $2^{-1.822\sqrt{\log N}}$.

What is known about corners?

Best Lower bound [Green, 2021]

There is a corner-free set of density $2^{-1.822\sqrt{\log N}}$.

Theorem [Shkredov, 2006]

There is no corner-free set of density $1/(\log\log N)^c$.

What is known about corners?

Best Lower bound [Green, 2021]

There is a corner-free set of density $2^{-1.822\sqrt{\log N}}$.

Theorem [Shkredov, 2006]

There is no corner-free set of density $1/(\log\log N)^c$.

Best upper bound [Jaber, Liu, Lovett, Ostuni, Sawhney, 2025]

There is no corner-free set of density $2^{-(\log N)^{1/600}}$.

Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

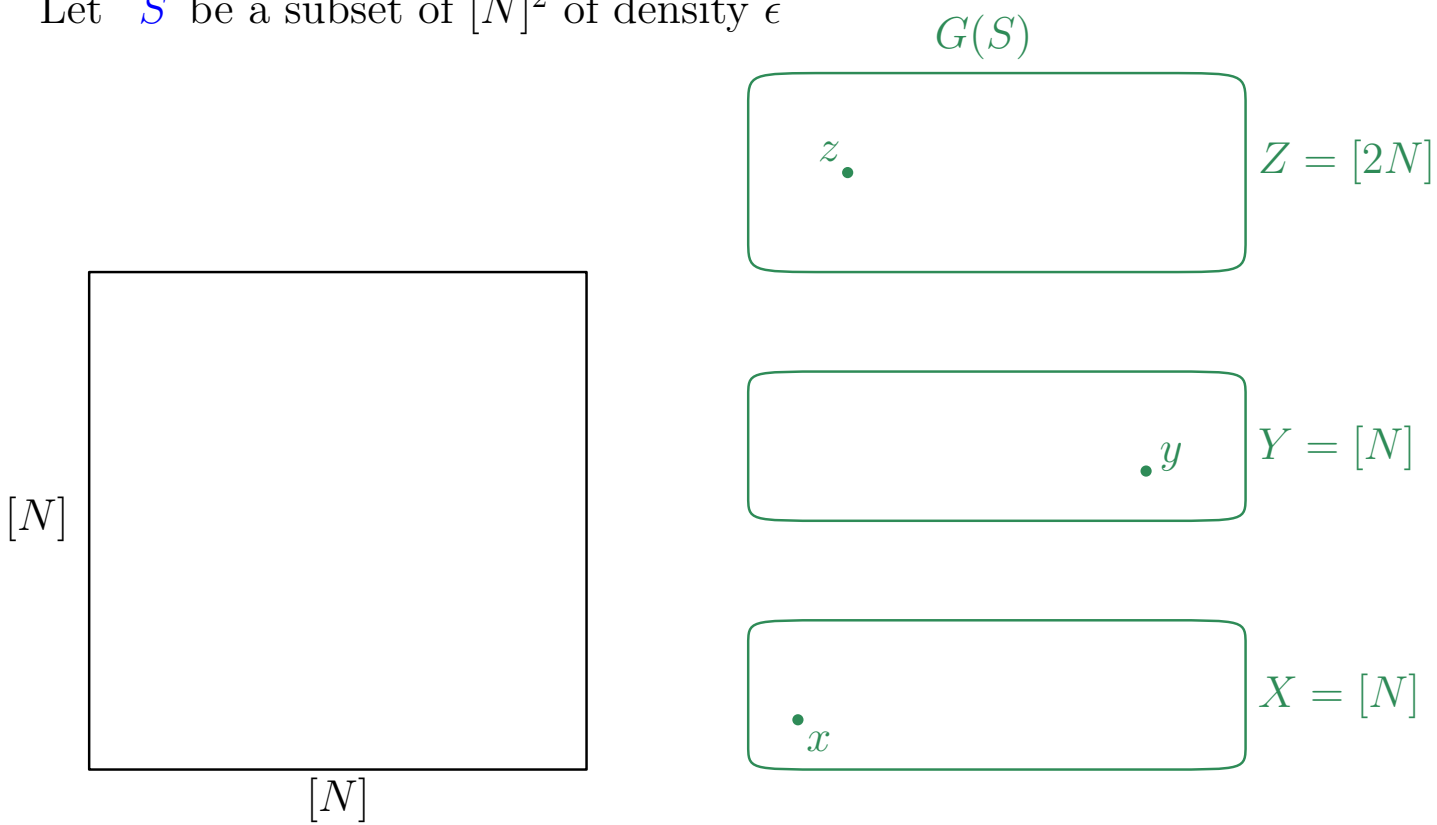
Let S be a subset of $[N]^2$ of density ϵ

Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ

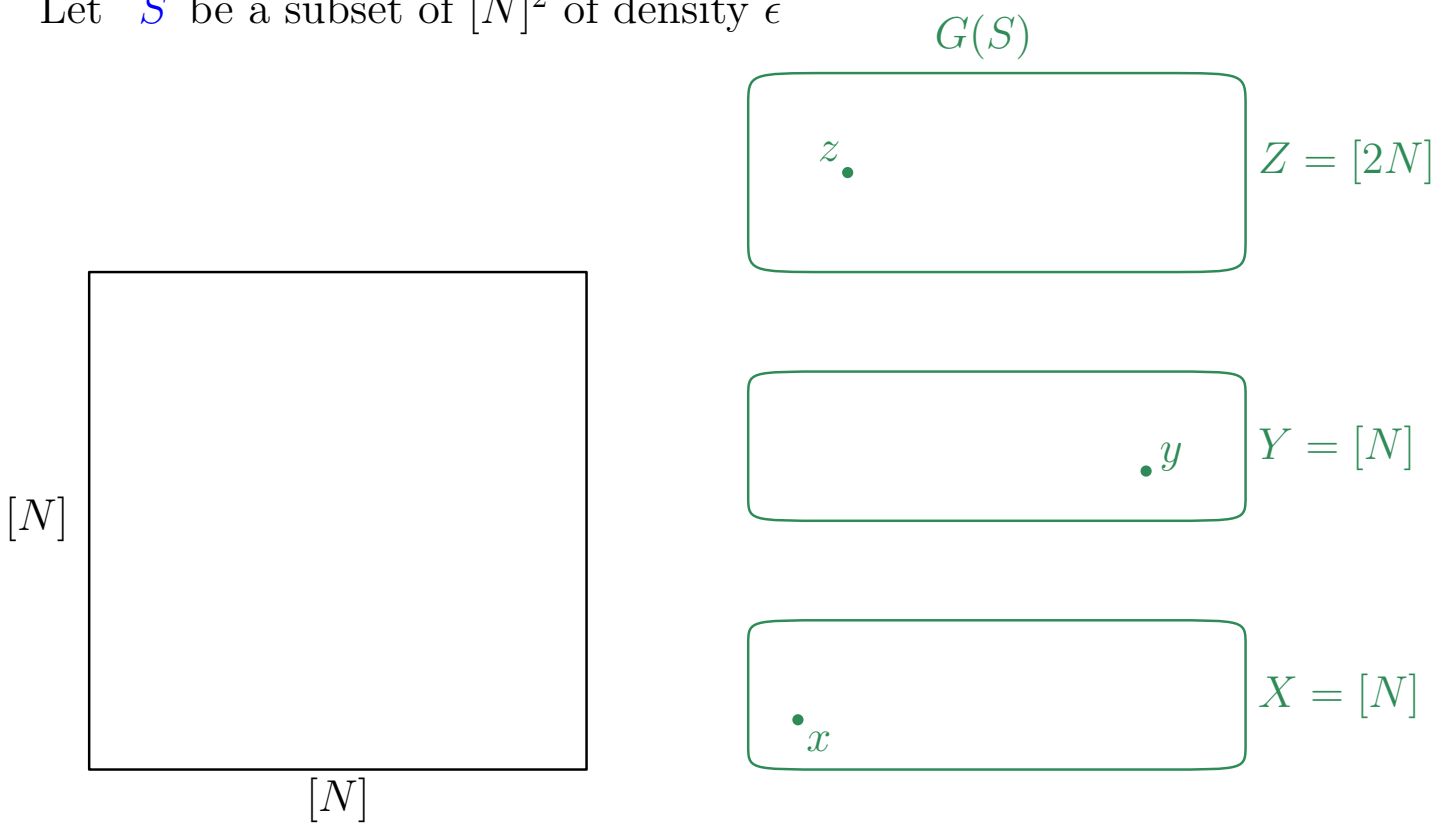


Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ

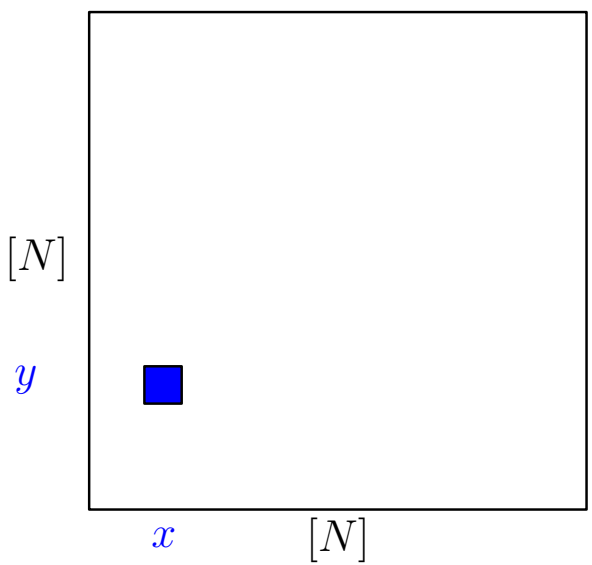


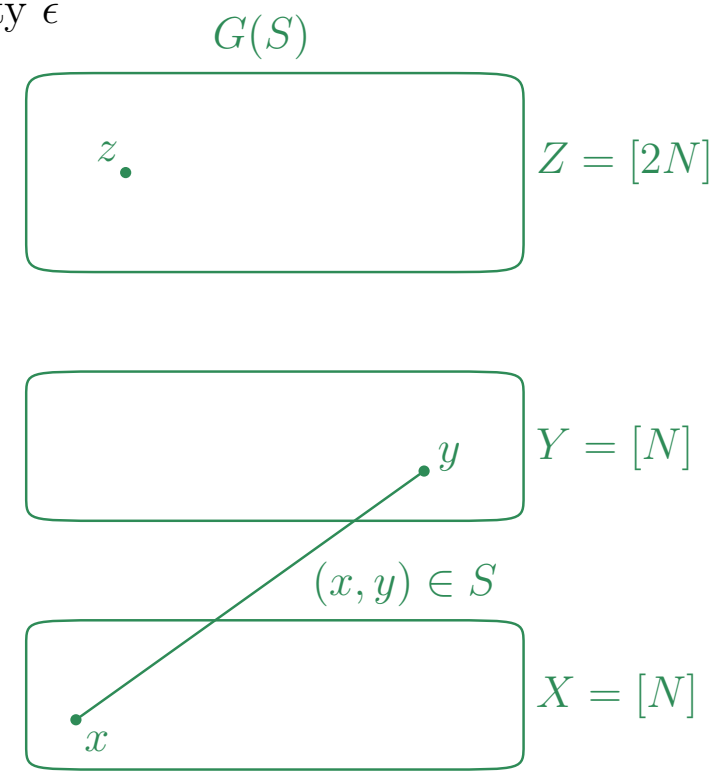
Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ



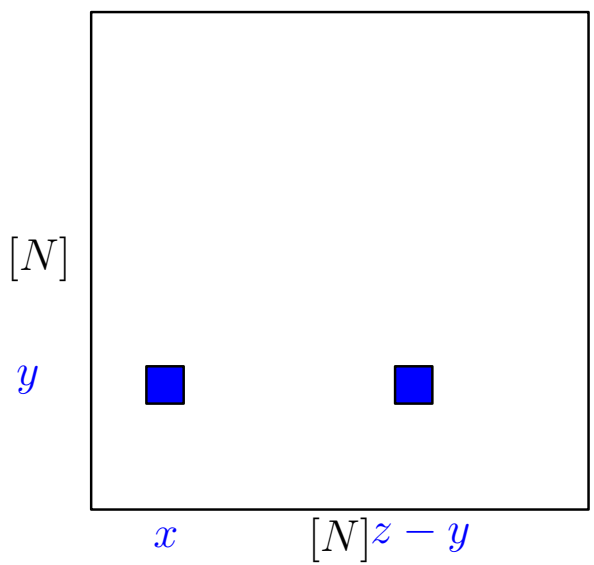


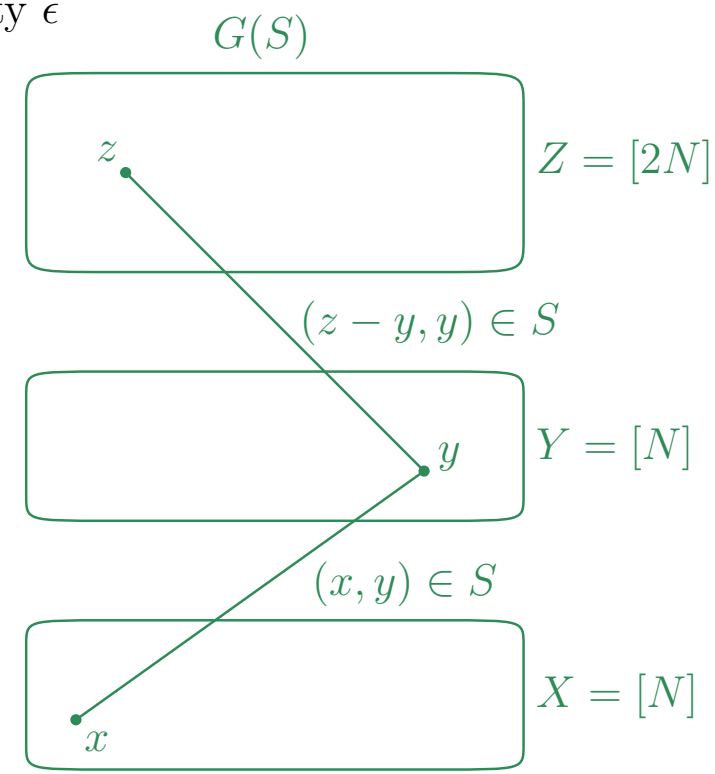
Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ



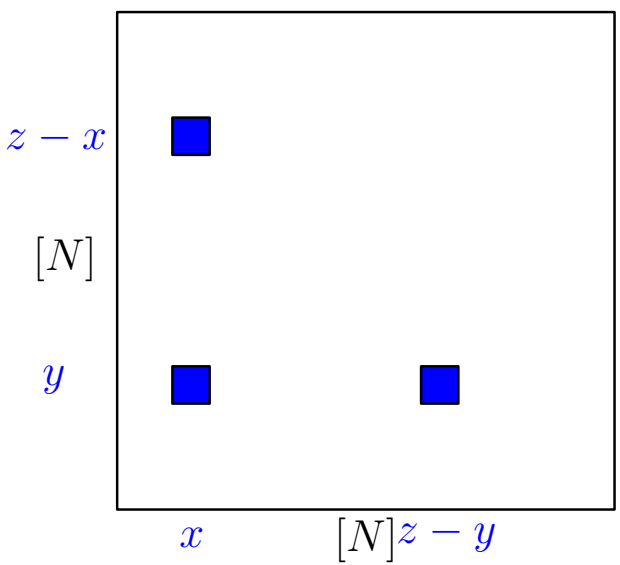


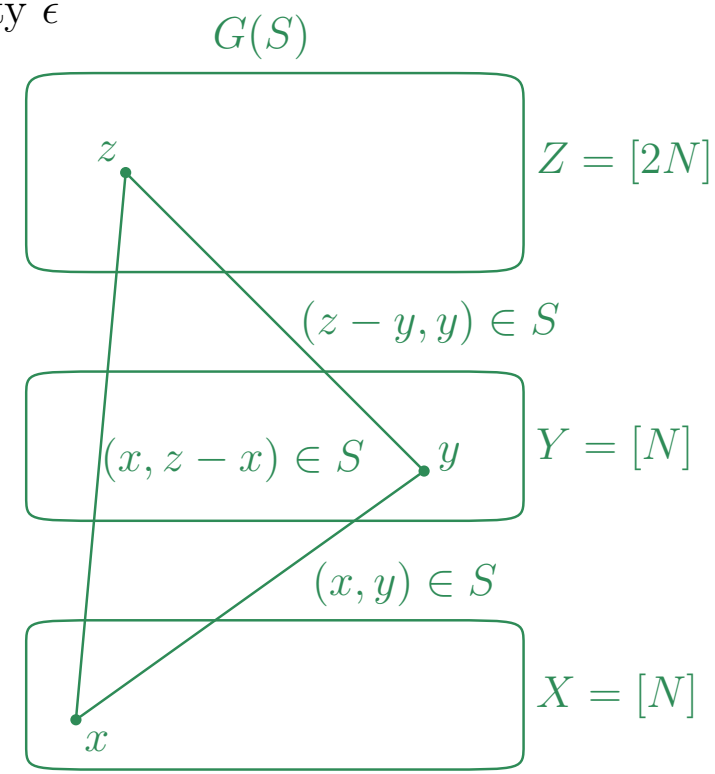
Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ





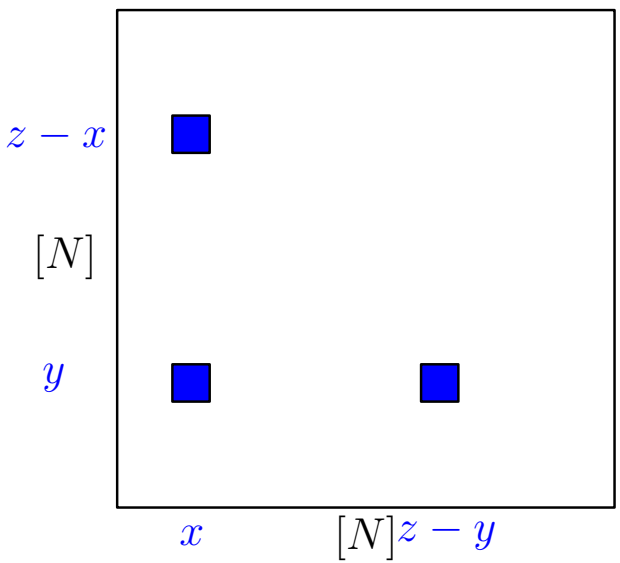
Triangle removal lemma $\Rightarrow$ corners theorem

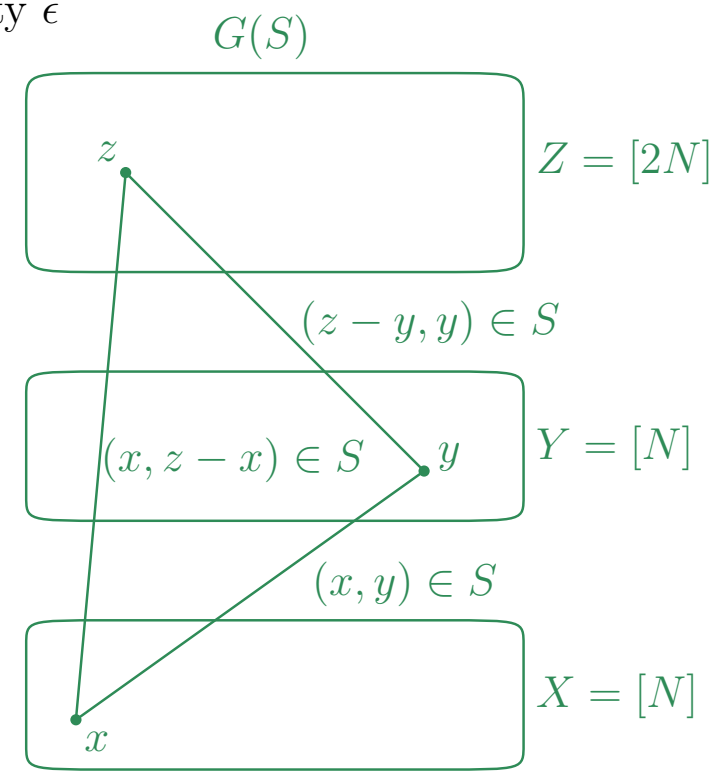
Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ

Triangle $\Leftrightarrow$ (possibly trivial) corner





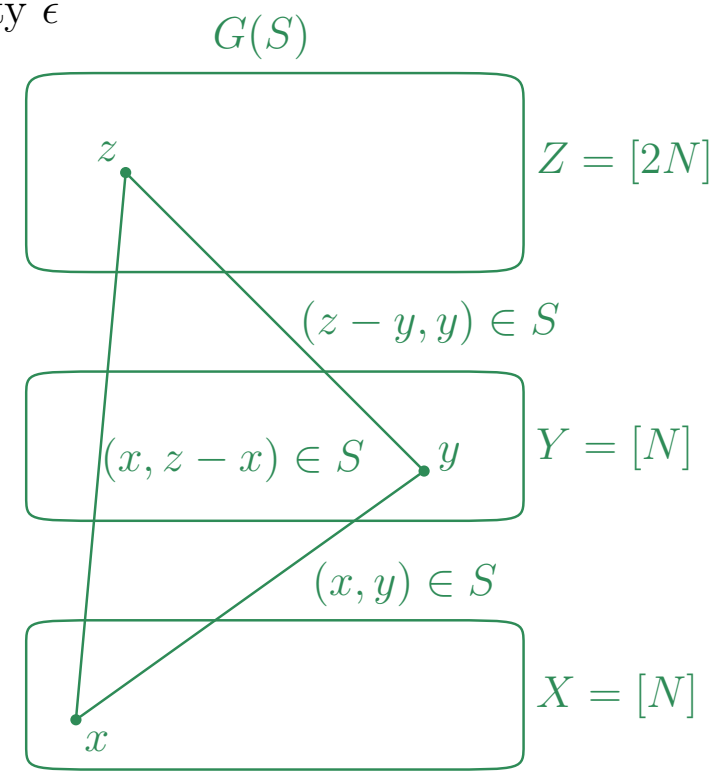
Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ

Triangle $\Leftrightarrow$ (possibly trivial) corner



Triangle removal lemma $\Rightarrow$ corners theorem

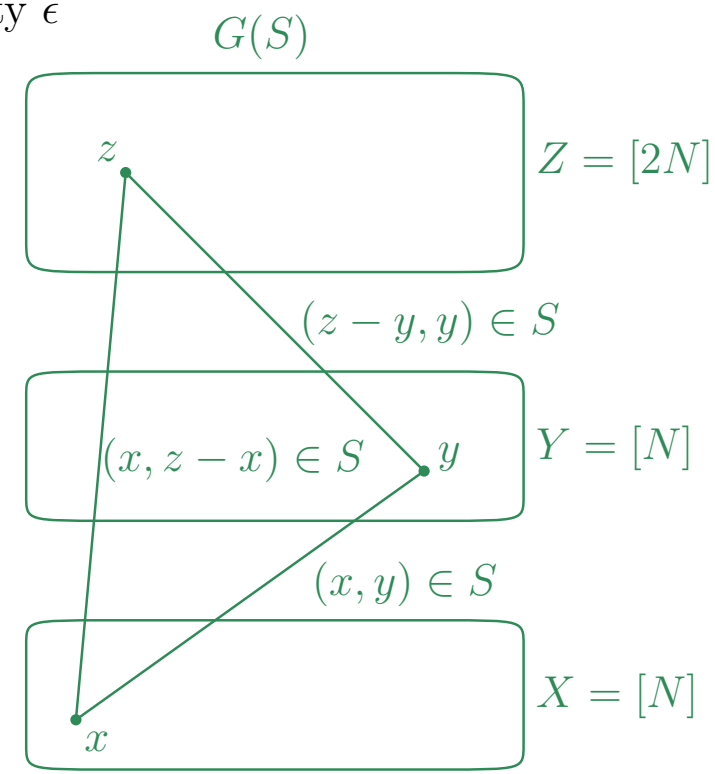
Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ

Triangle $\Leftrightarrow$ (possibly trivial) corner

Trivial corner $(x, y), (x, y), (x, y)$
$\Leftrightarrow$ Triangle $(x, y, x + y)$



Triangle removal lemma $\Rightarrow$ corners theorem

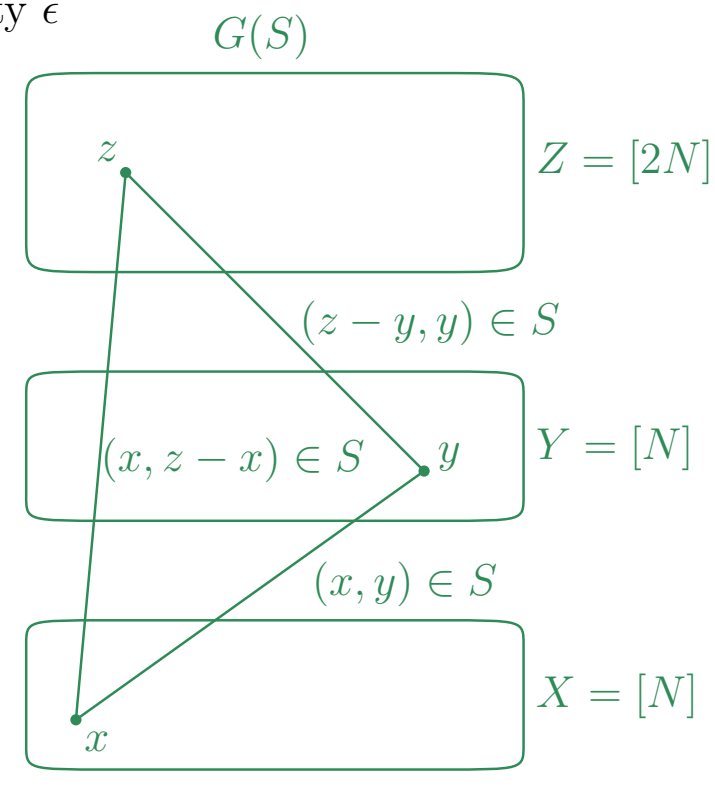
Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ

Triangle $\Leftrightarrow$ (possibly trivial) corner

Trivial corner $(x, y), (x, y), (x, y)$
$\Leftrightarrow$ Triangle $(x, y, x + y)$
$\rightarrow N^2$ edge-disjoint triangle



Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ

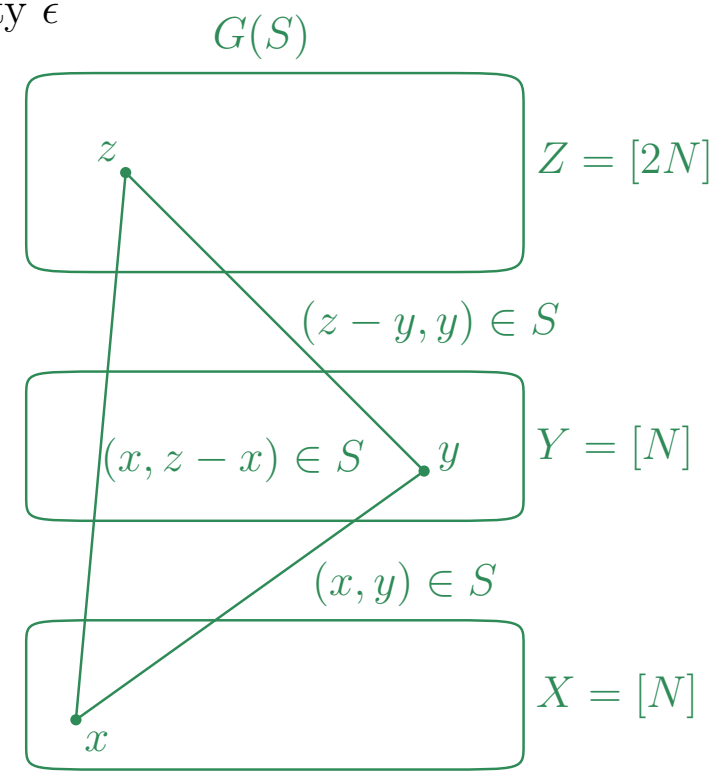
Triangle $\Leftrightarrow$ (possibly trivial) corner

Trivial corner $(x, y), (x, y), (x, y)$

$\Leftrightarrow$ Triangle $(x, y, x + y)$

$\rightarrow N^2$ edge-disjoint triangle

$\rightarrow \delta N^3$ triangles



Triangle removal lemma $\Rightarrow$ corners theorem

Triangle removal lemma [Ruzsa, Szemerédi 1978]

For any $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$ such that:
If one cannot erase **all** triangles of G by deleting ϵn^2 edges,
Then G contains δn^3 triangles.

Let S be a subset of $[N]^2$ of density ϵ

Triangle $\Leftrightarrow$ (possibly trivial) corner

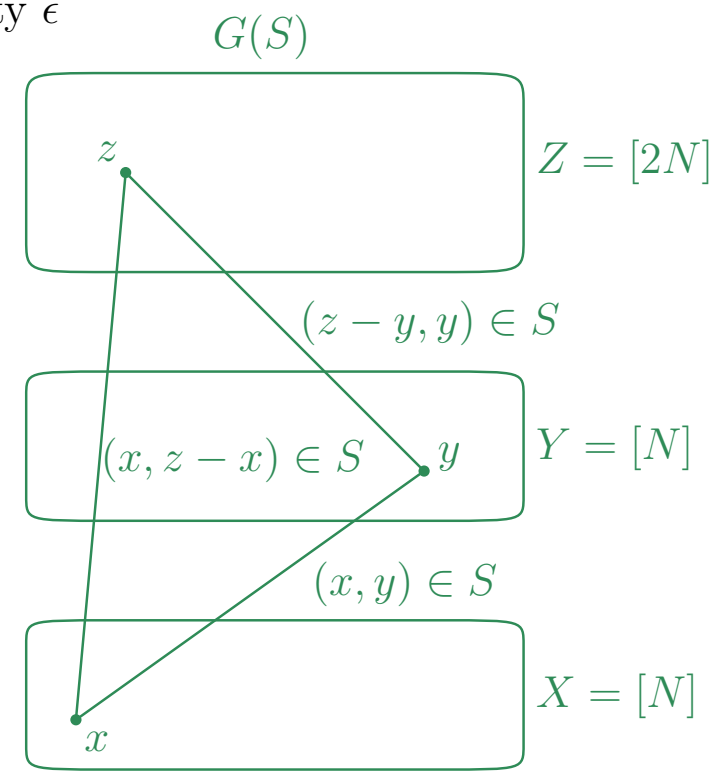
Trivial corner $(x, y), (x, y), (x, y)$

$\Leftrightarrow$ Triangle $(x, y, x + y)$

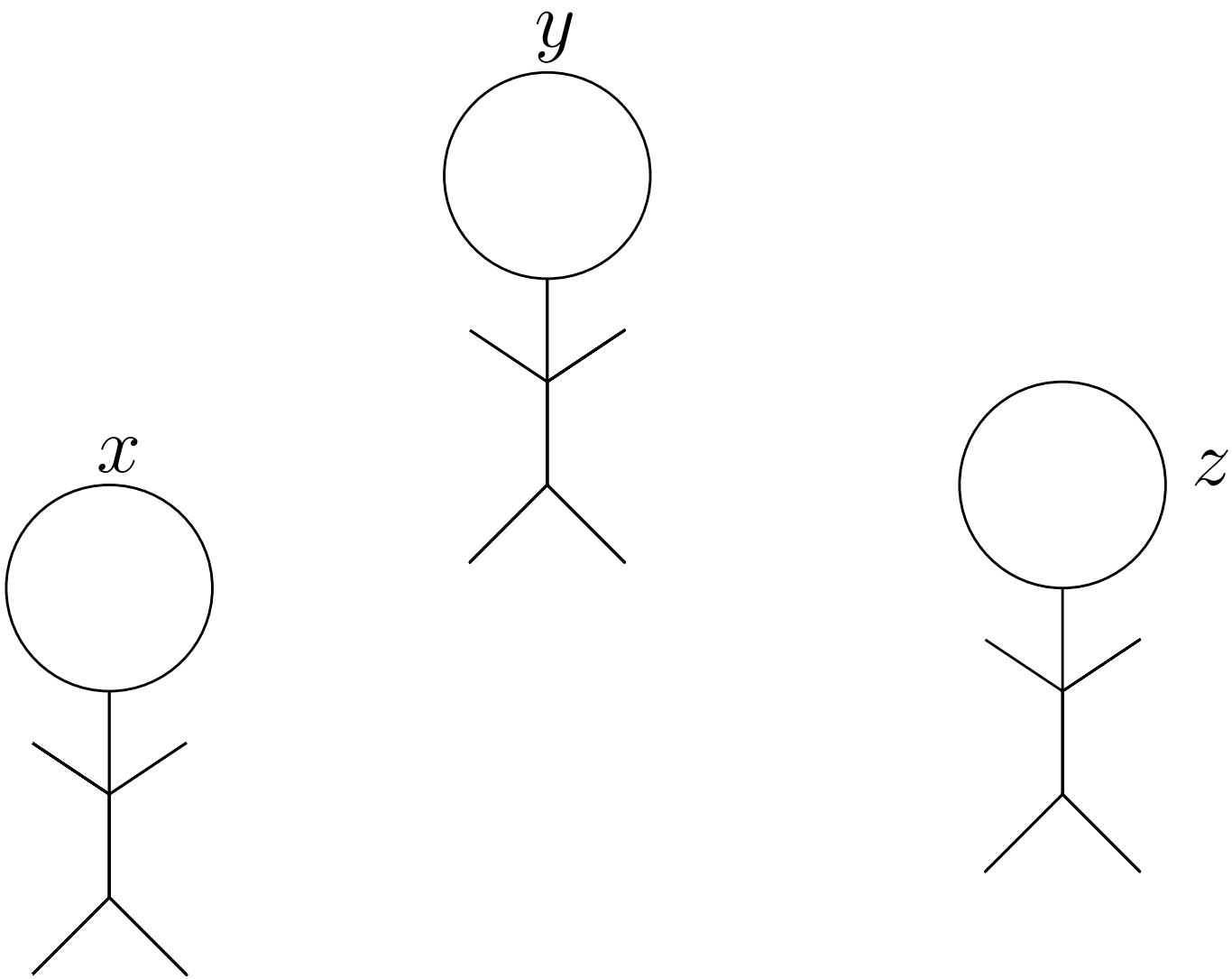
$\rightarrow N^2$ edge-disjoint triangle

$\rightarrow \delta N^3$ triangles

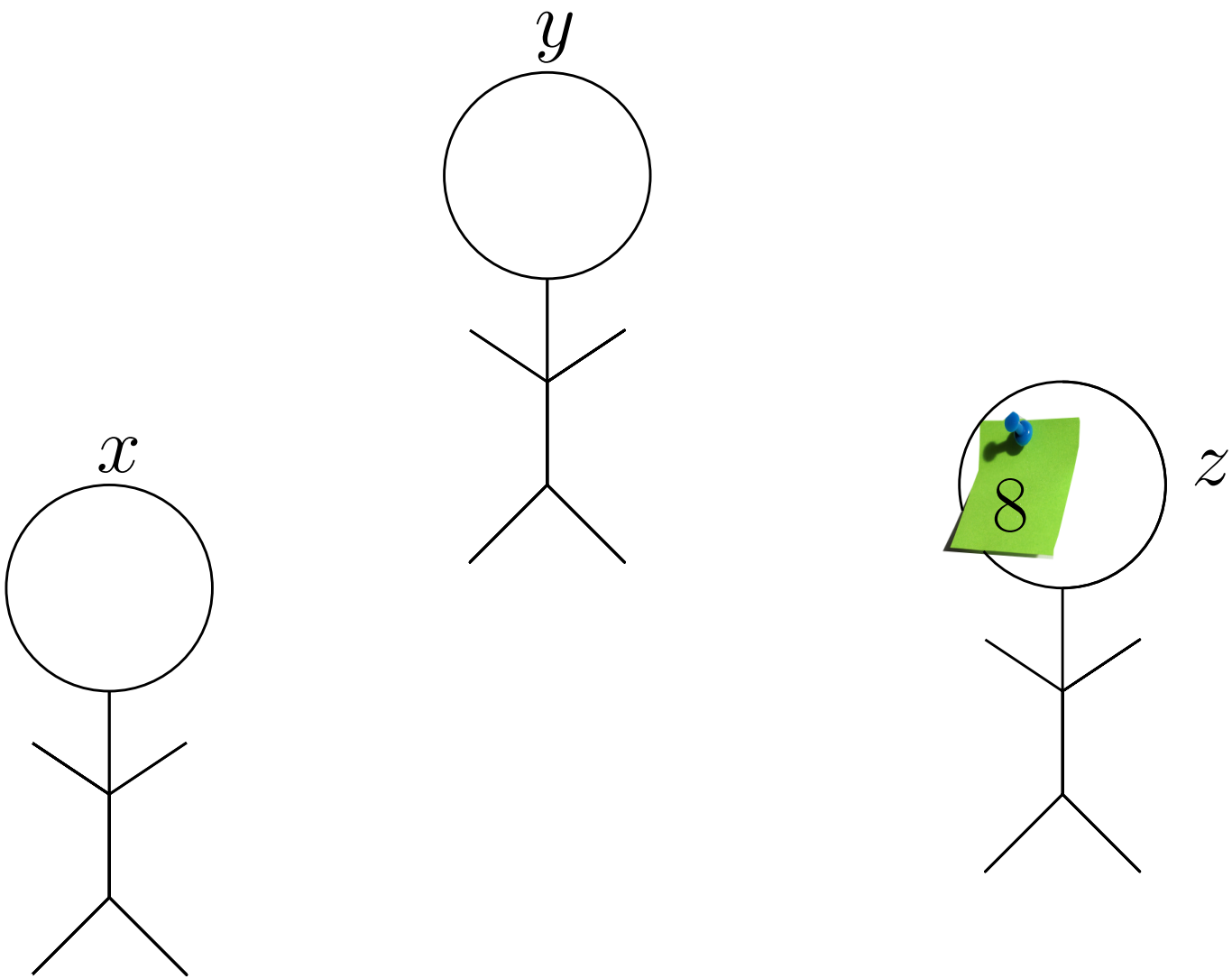
$\rightarrow \delta N^3 - N^2$ non-trivial corners



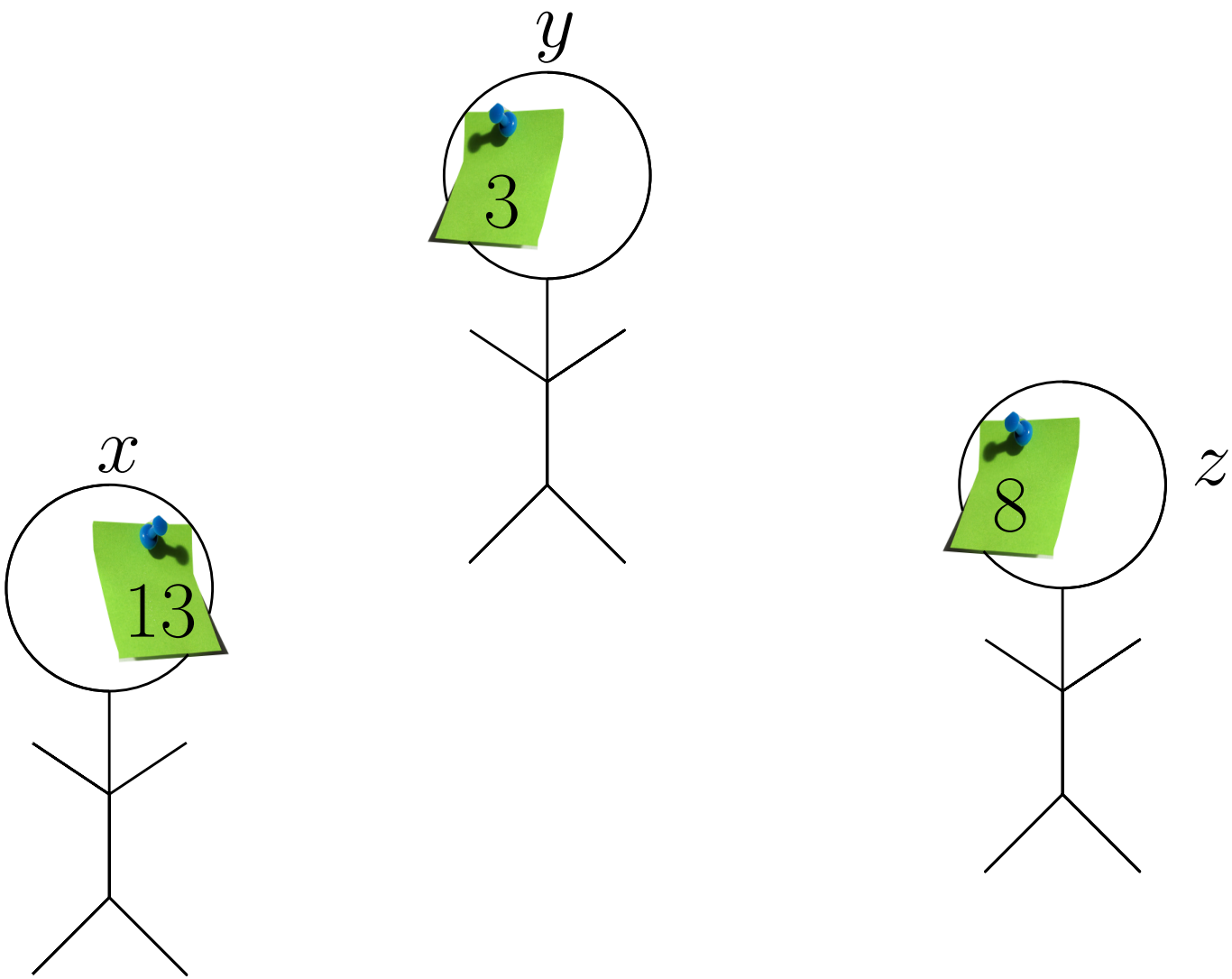
The 3-NOF protocol



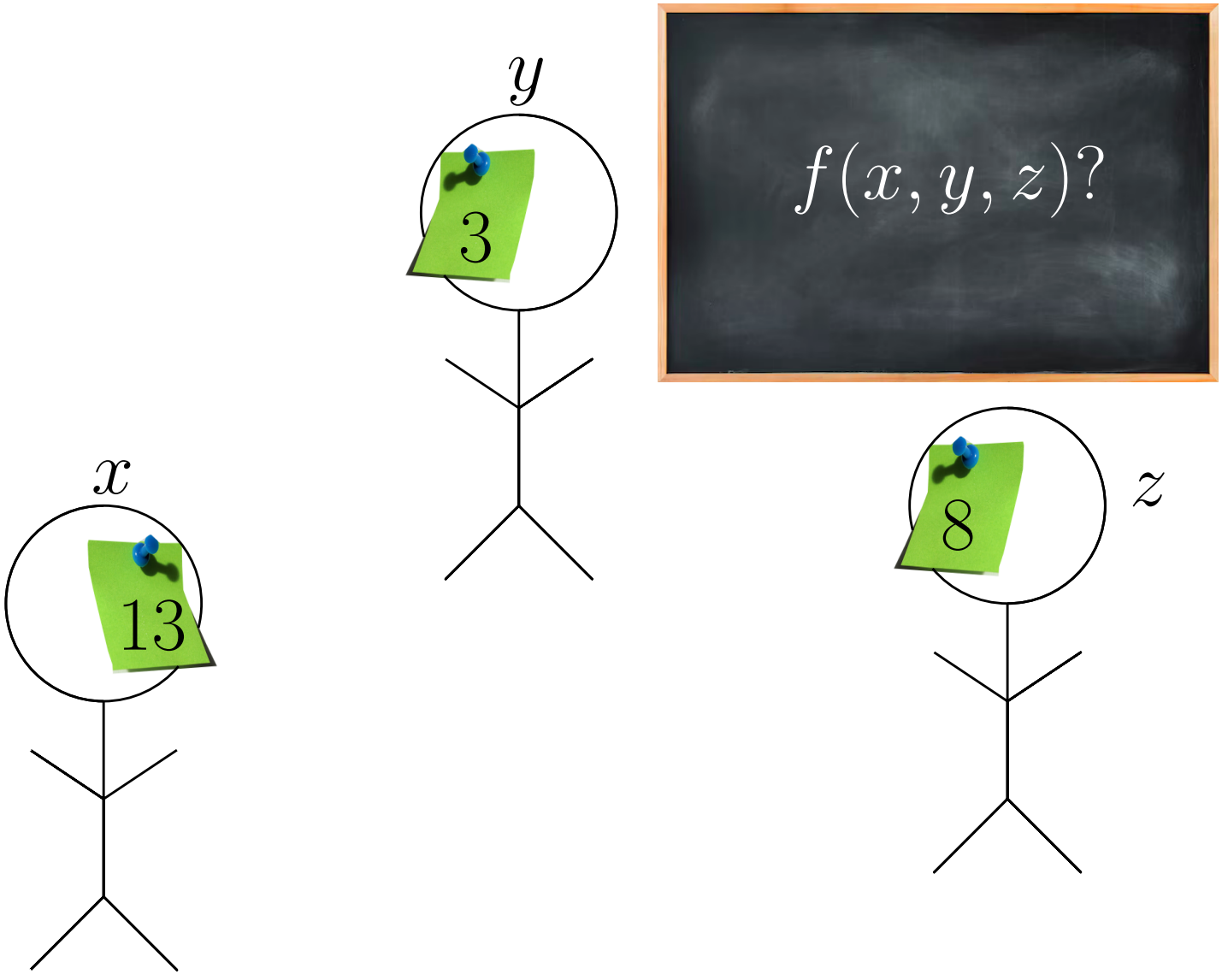
The 3-NOF protocol



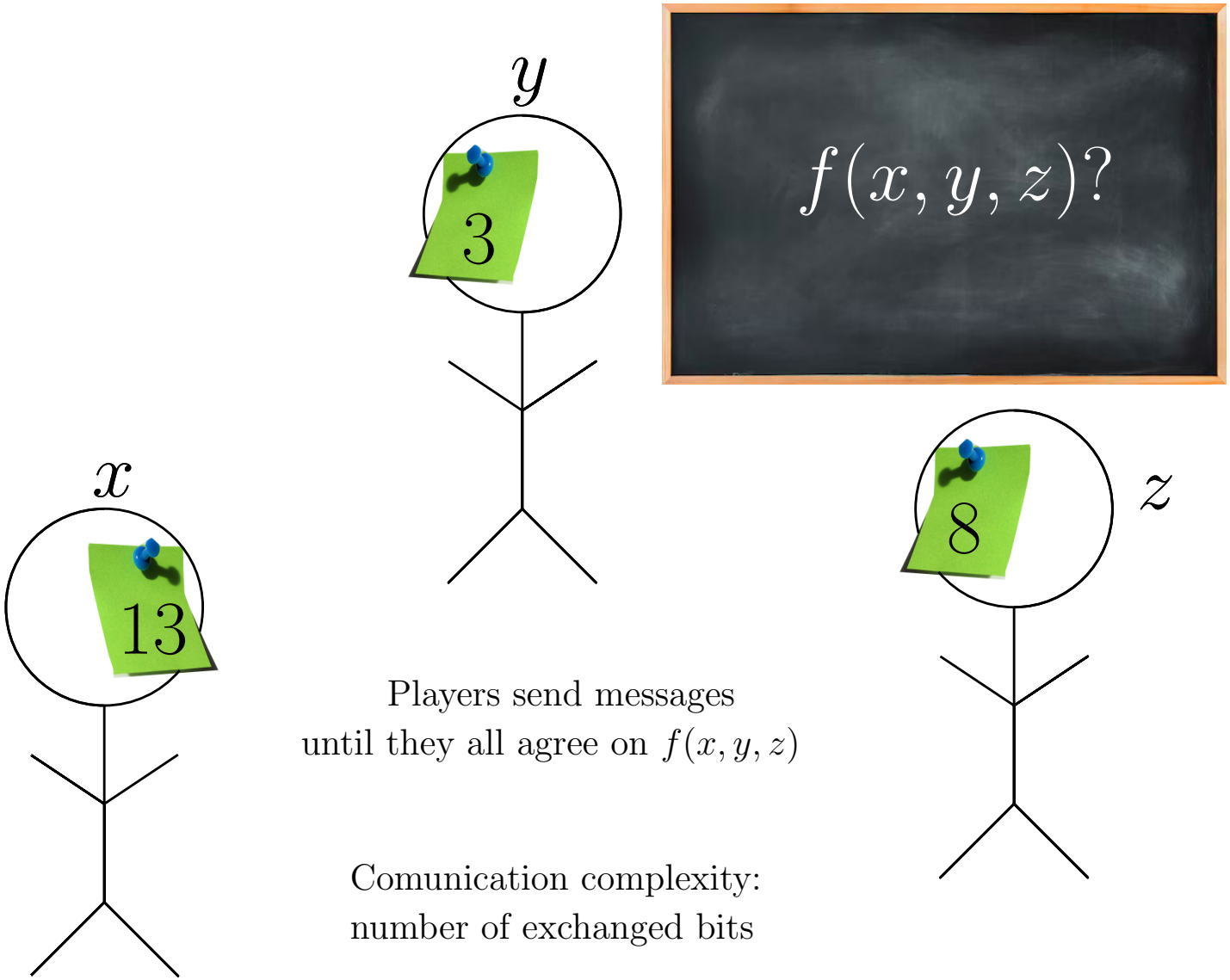
The 3-NOF protocol



The 3-NOF protocol



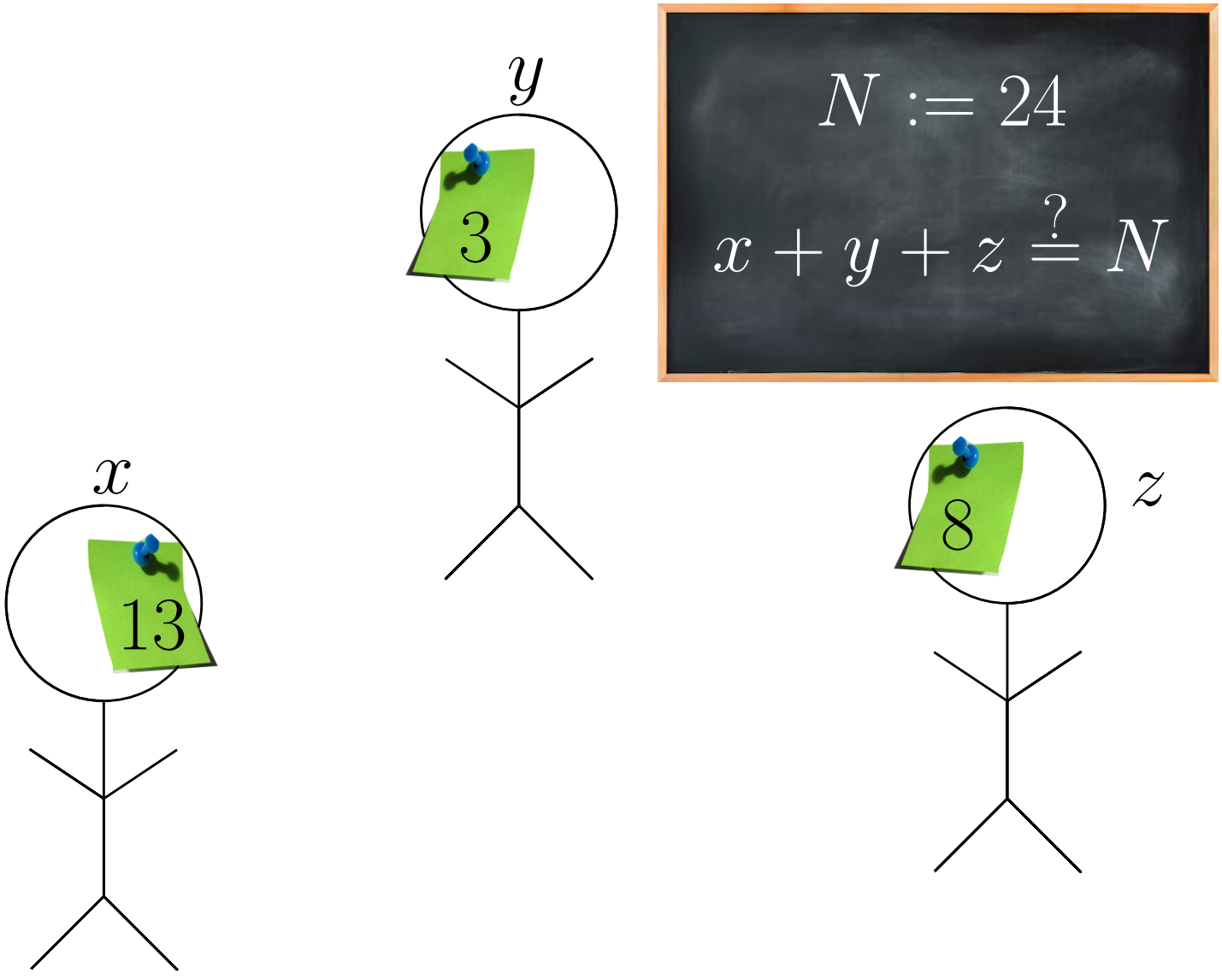
The 3-NOF protocol



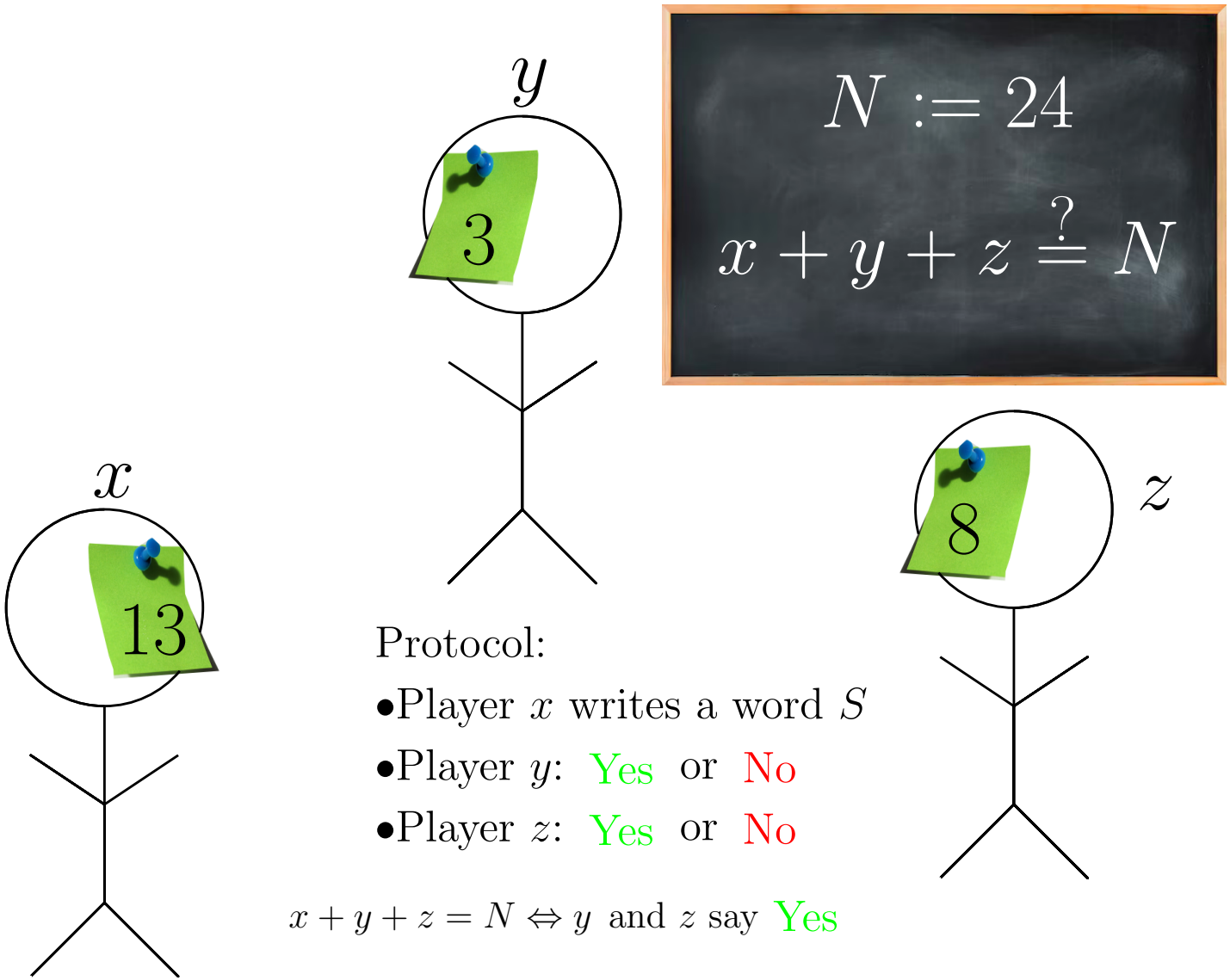
Players send messages
until they all agree on $f(x, y, z)$

Comunication complexity:
number of exchanged bits

One round 3-NOF exactly-*N* protocol



One round 3-NOF exactly-N protocol

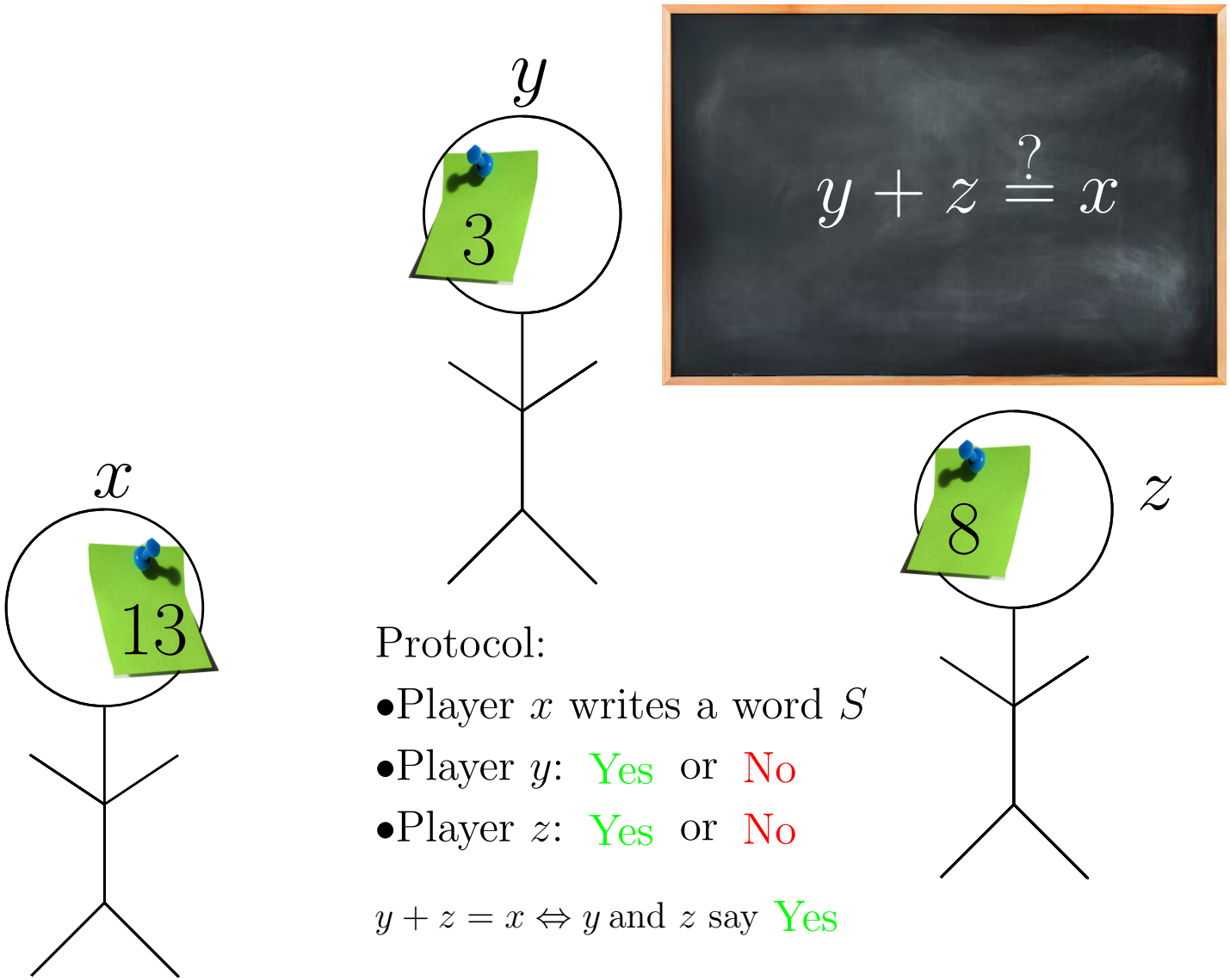


Protocol:

- Player x writes a word S
- Player y: Yes or No
- Player z: Yes or No

$x + y + z = N \Leftrightarrow y$ and z say Yes

One round 3-NOF exactly-N protocol



Protocol:

- Player x writes a word S
- Player y: Yes or No
- Player z: Yes or No

$y + z = x \Leftrightarrow y$ and z say Yes

Good protocol $\Rightarrow$ big corner-free set

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy

Let w a possible message of P_x

Good protocol $\Rightarrow$ big corner-free set

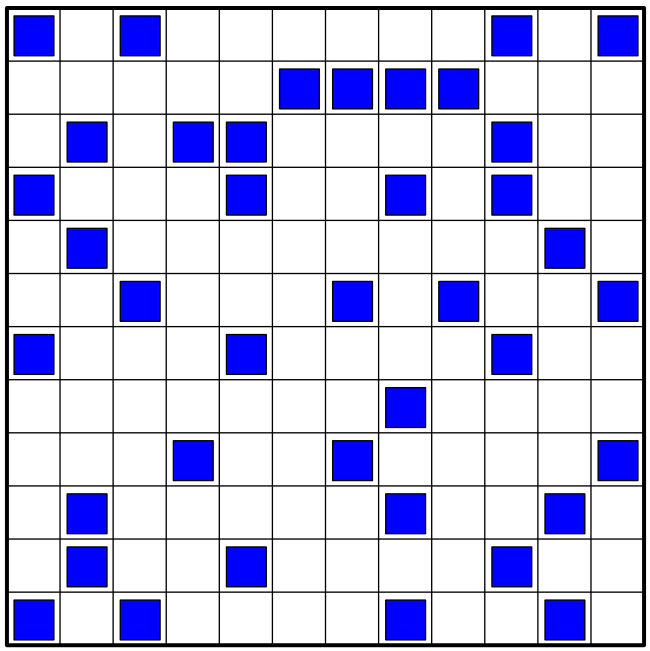
Assume P_x, P_y, P_z obey a good strategy

Let w a possible message of P_x

$S(w) := \{(y,z) \ : \ P_x(y,z) = w\}$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy

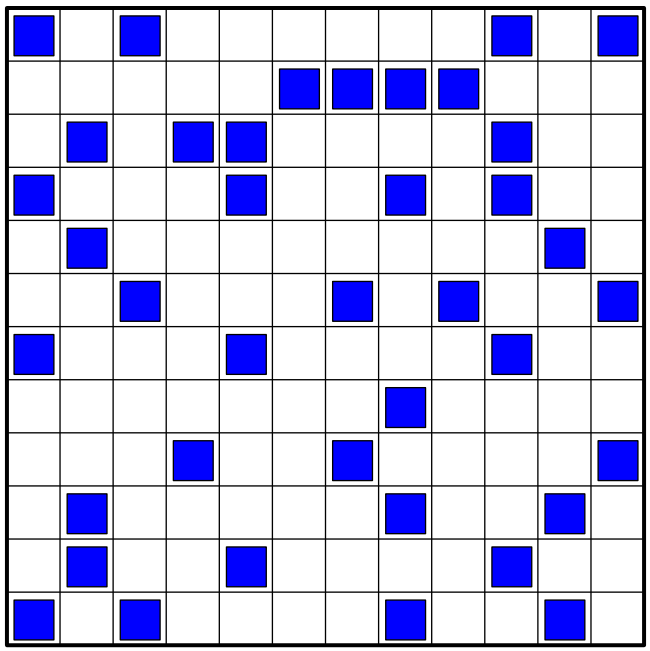


Let w a possible message of P_x

$S(w) := \{(y,z) \ : \ P_x(y,z) = w\}$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



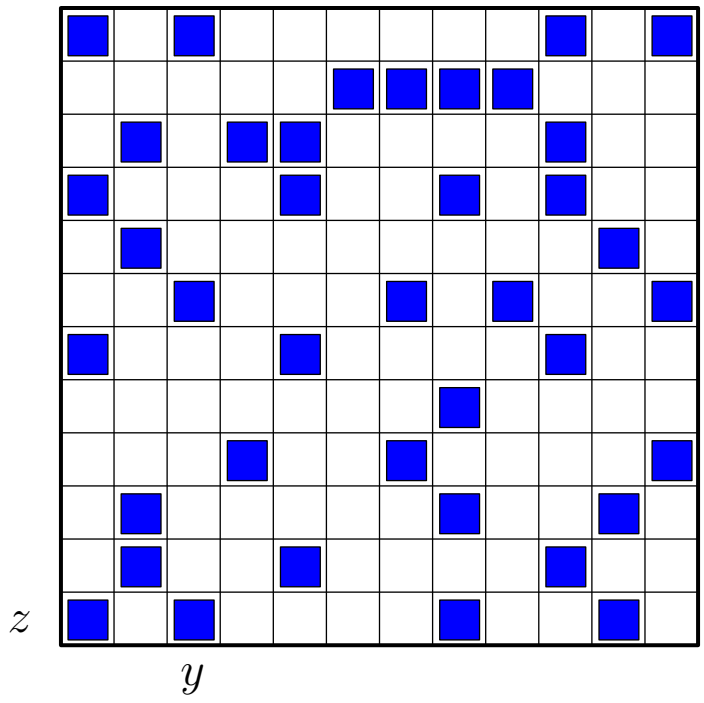
Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

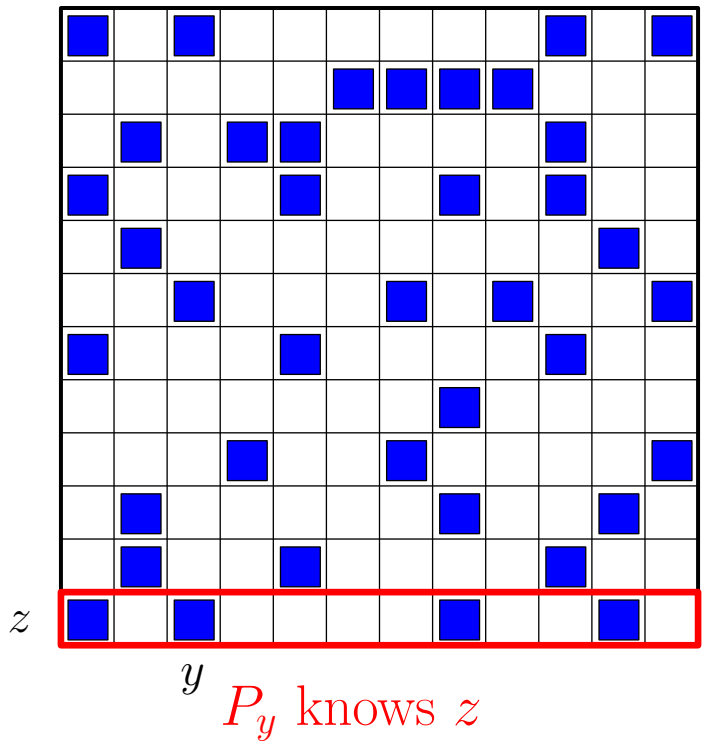
$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

Proof: Let $(y,z) \in S_w$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

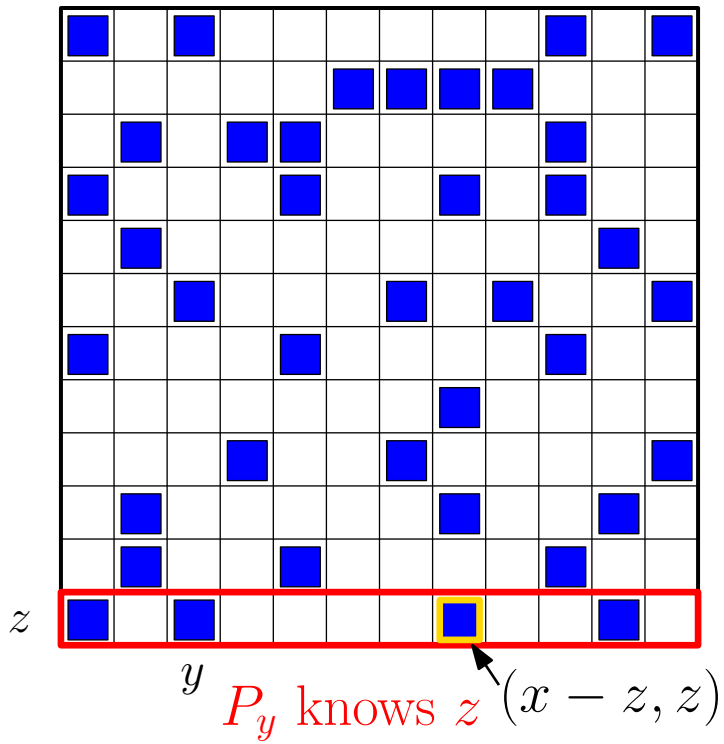
Fact: $S(w)$ is corner-free

Proof: Let $(y,z) \in S_w$

P_y knows: x, z, S_w, $(y,z) \in S_w$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

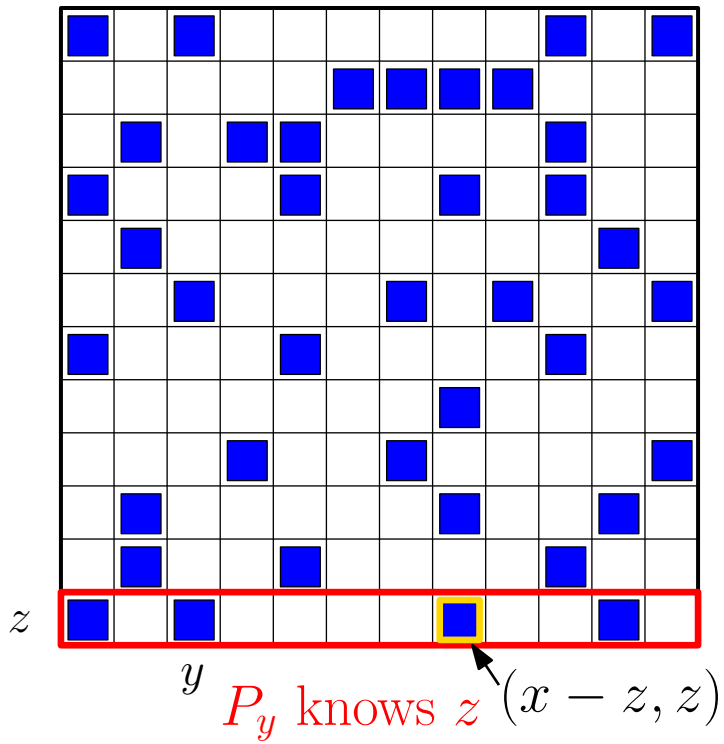
Proof: Let $(y,z) \in S_w$

P_y knows: x, z, S_w, $(y,z) \in S_w$

y says YES when $y = x - z$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

Proof: Let $(y,z) \in S_w$

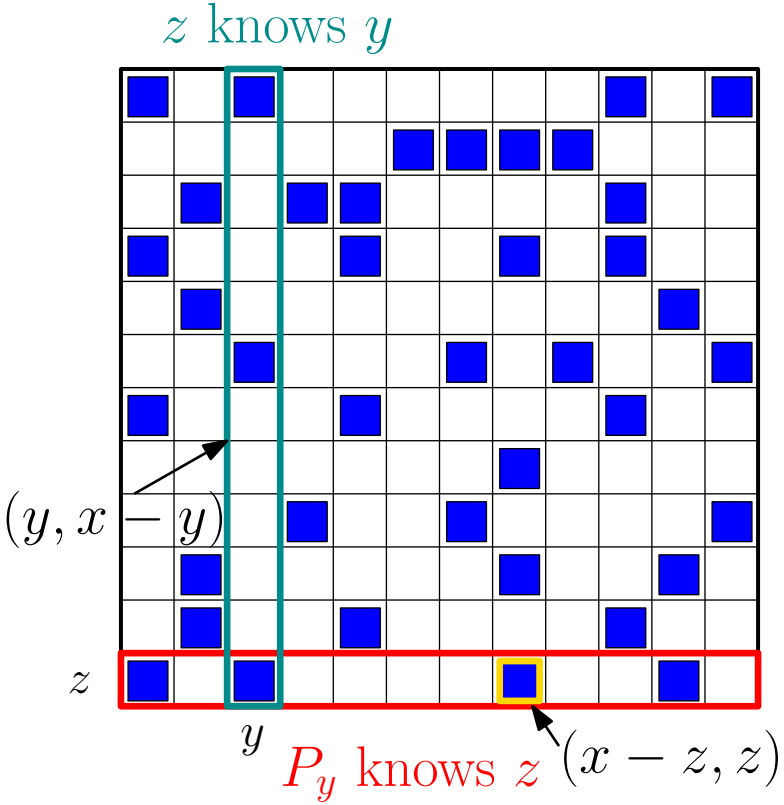
P_y knows: x, z, S_w, $(y,z) \in S_w$

y says YES when $y = x - z$

$\rightarrow$ has to say yes if $(x-z, z) \in S_w$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

Proof: Let $(y,z) \in S_w$

P_y knows: x, z, S_w, $(y,z) \in S_w$

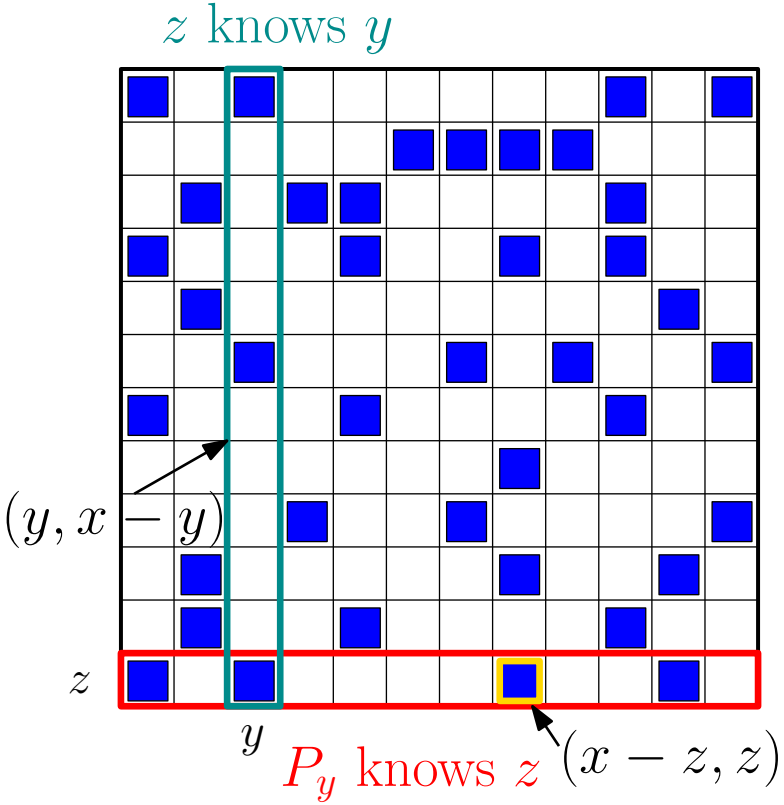
y says YES when $y = x - z$

$\rightarrow$ has to say yes if $(x-z, z) \in S_w$

P_z has to say YES if $(y, x-y) \in S_w$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

Proof: Let $(y,z) \in S_w$

P_y knows: x, z, S_w, $(y,z) \in S_w$

y says YES when $y = x - z$

$\rightarrow$ has to say yes if $(x-z, z) \in S_w$

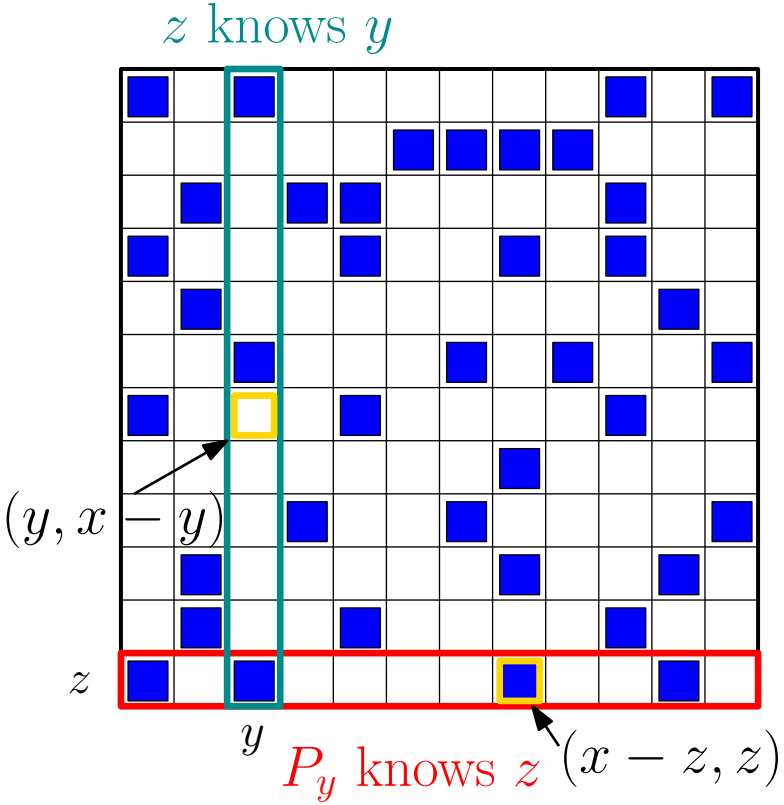
P_z has to say YES if $(y, x-y) \in S_w$

Hence, $\forall x, \forall (y,z) \in S_w$

$(y, x-y), (x-z, z) \in S_w \Rightarrow z = x - y$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

Proof: Let $(y,z) \in S_w$

P_y knows: x, z, S_w, $(y,z) \in S_w$

y says YES when $y = x - z$

$\rightarrow$ has to say yes if $(x-z, z) \in S_w$

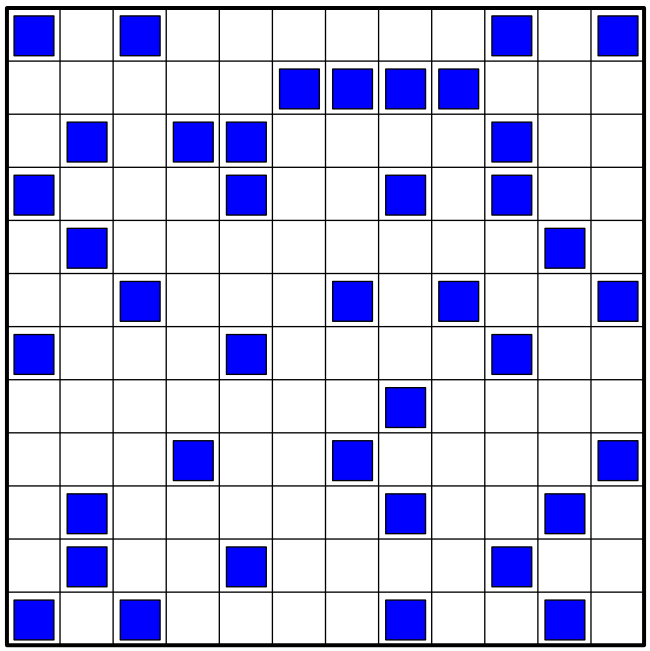
P_z has to say YES if $(y, x-y) \in S_w$

Hence, $\forall x, \forall (y,z) \in S_w$
$(y, x-y), (x-z, z) \in S_w \Rightarrow z = x - y$

$\Rightarrow \forall d, \forall (y,z) \in S_w \neg(y+d, z) \in S_w$
or $\neg(y, z+d) \in S_w$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



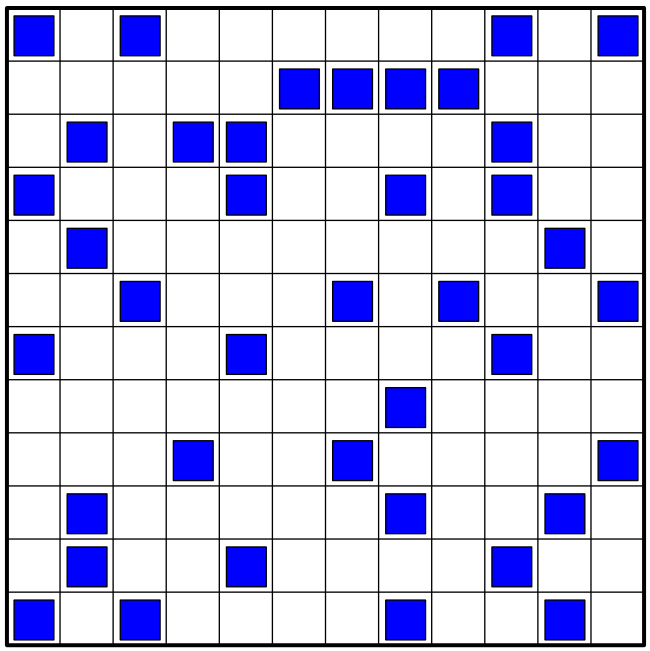
Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

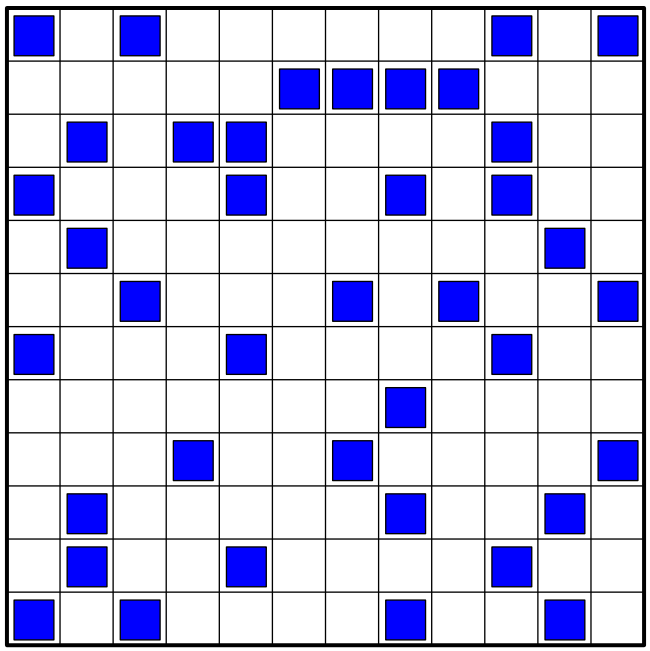
$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

$[n]^2 \subseteq \cup_w S_w$

Good protocol $\Rightarrow$ big corner-free set

Assume P_x, P_y, P_z obey a good strategy



Let w a possible message of P_x

$S(w) := \{(y,z) : P_x(y,z) = w\}$

Fact: $S(w)$ is corner-free

$[n]^2 \subseteq \cup_w S_w$

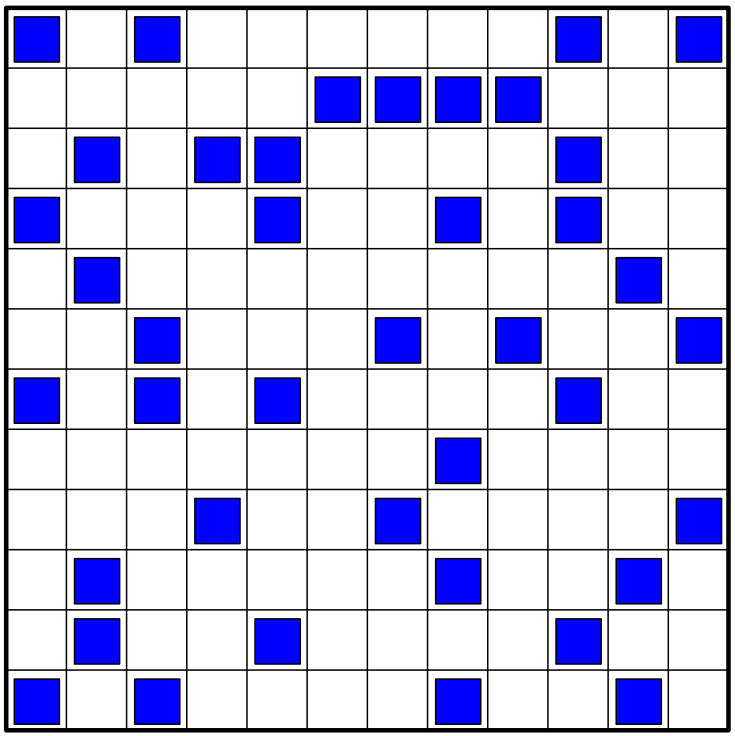
$\exists w,\ \text{density}(S_w) \geq 1/2^{|w|}$

Exists large corner-free sets!

Big corner-free set $\Rightarrow$ good protocol

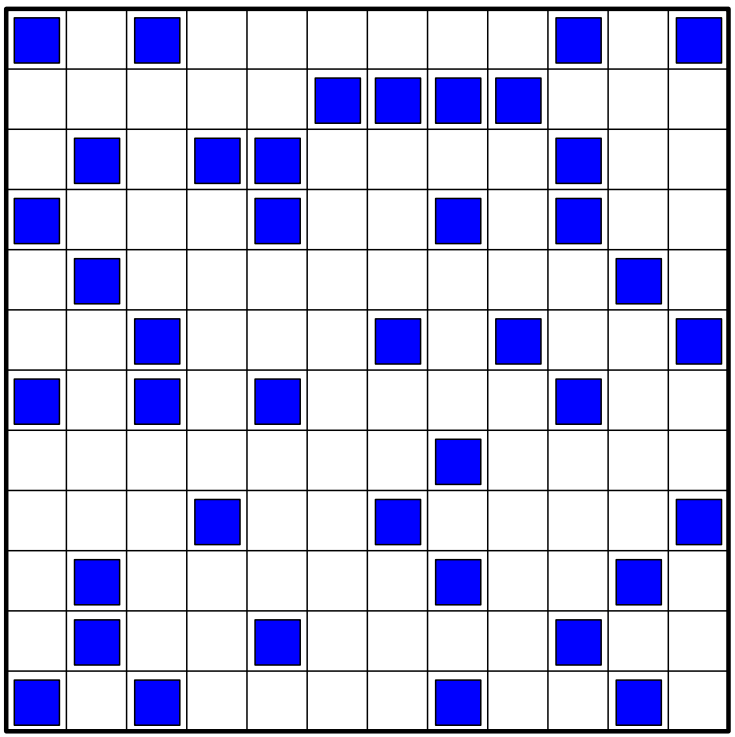
Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



Big corner-free set $\Rightarrow$ good protocol

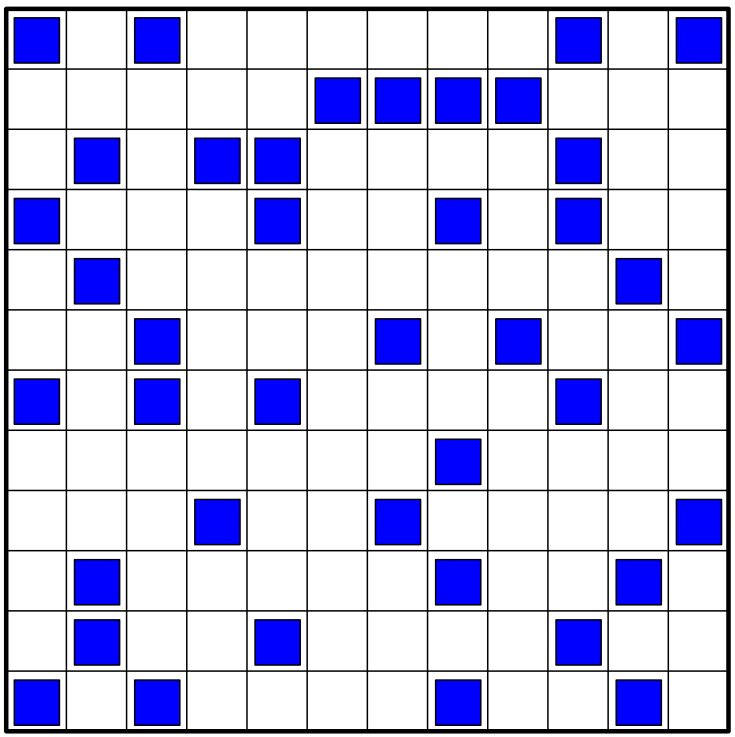
Let S be a corner-free set of size k



Protocol *under* $(y, z) \in S$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k

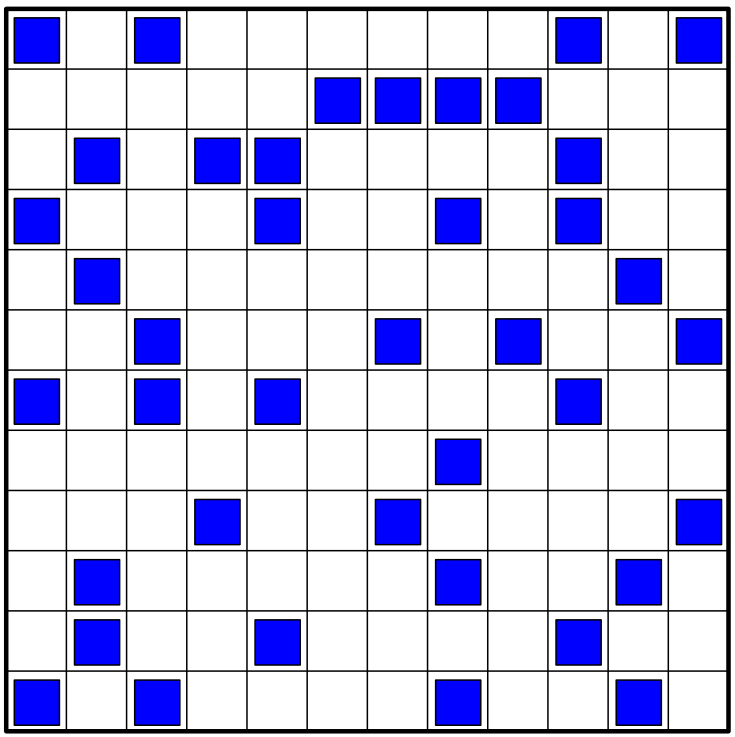


Protocol *under* $(y, z) \in S$

P_x says nothing

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



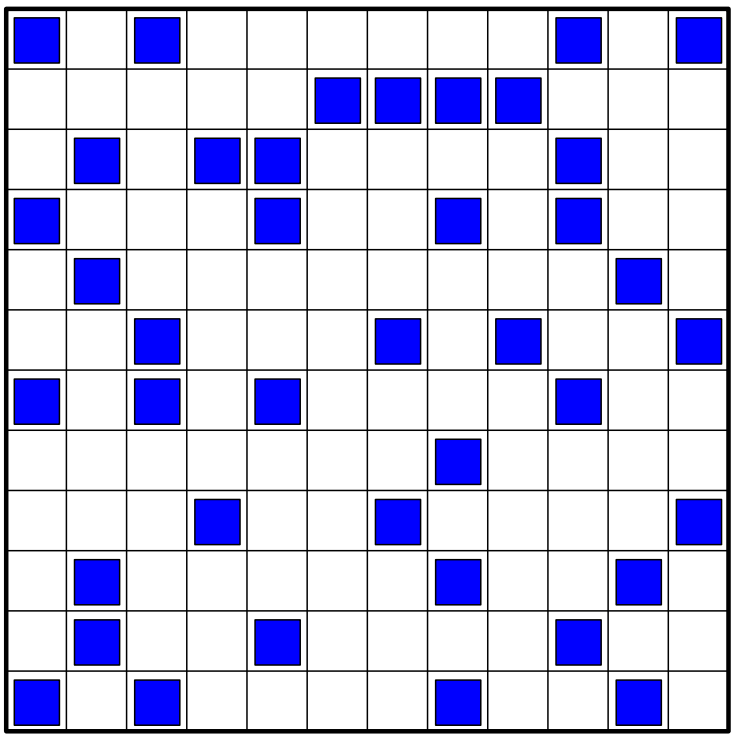
Protocol *under* $(y, z) \in S$

P_x says nothing

P_y says YES if $(z - x, z) \in S$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



Protocol *under* $(y, z) \in S$

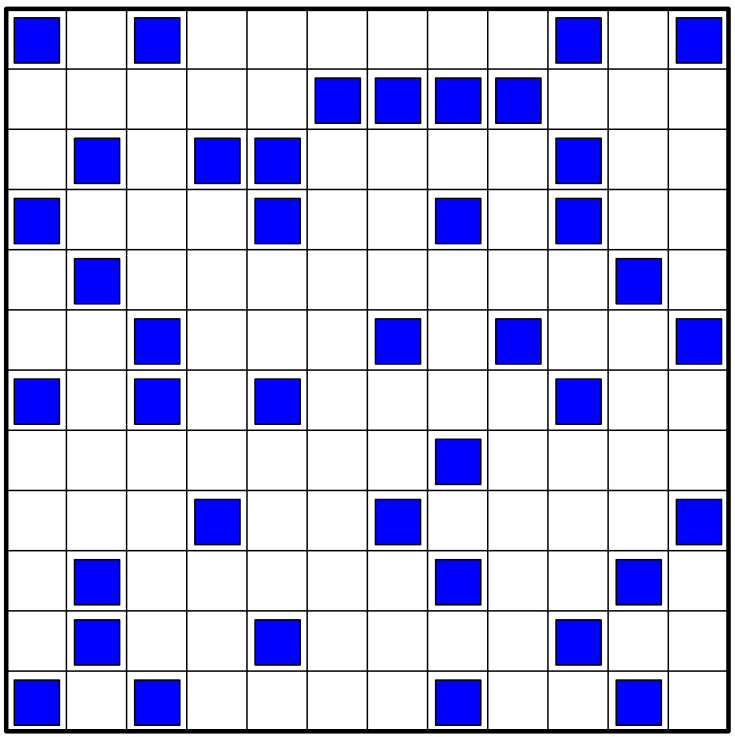
P_x says nothing

P_y says YES if $(z - x, z) \in S$

P_y says YES if $(y, x - y) \in S$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



Protocol *under* $(y, z) \in S$

P_x says nothing

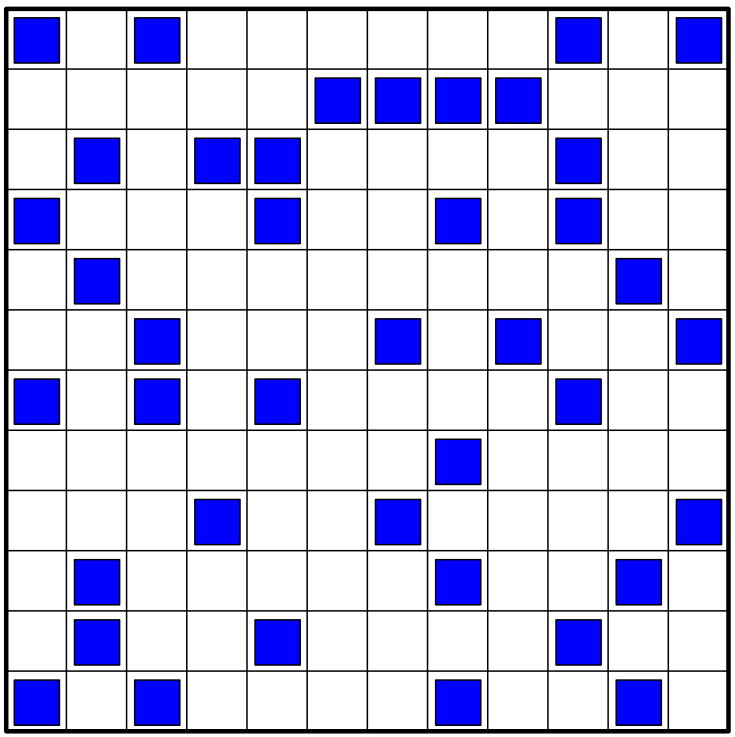
P_y says YES if $(z - x, z) \in S$

P_y says YES if $(y, x - y) \in S$

S corner-free $\Rightarrow$ prot. valid

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k

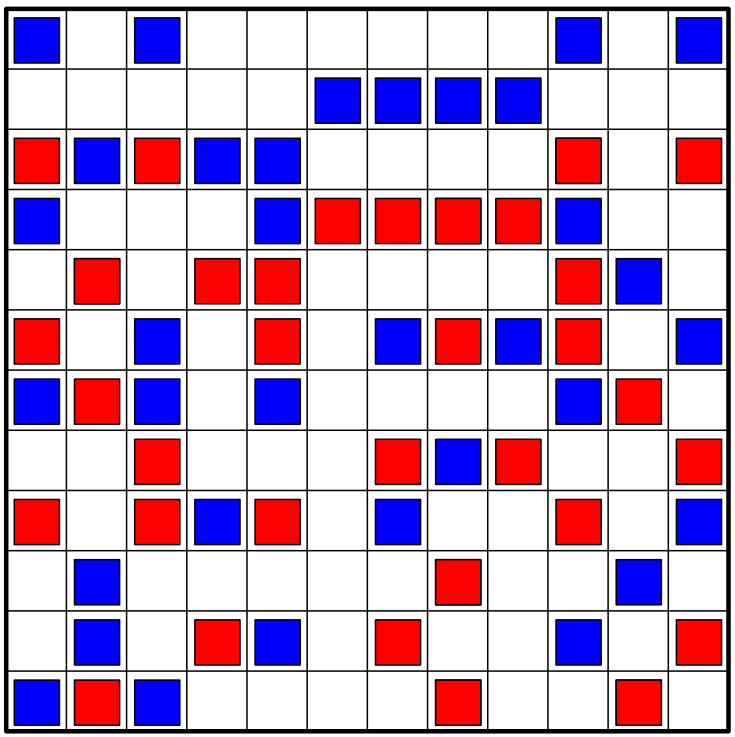


Protocol *under* $(y, z) \in S$

How to generalise?

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



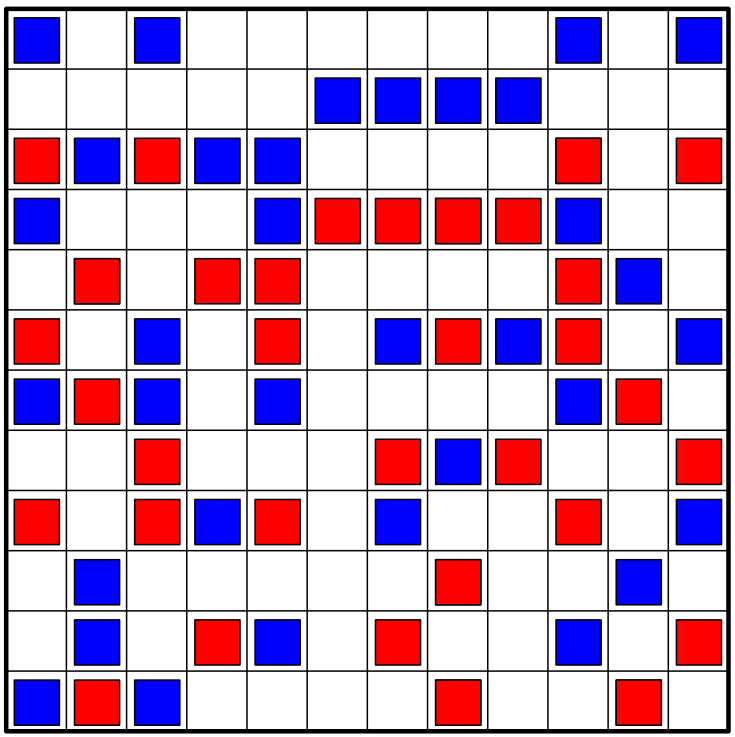
Protocol *under* $(y, z) \in S$

How to generalise?

Shift S! here $S' = S - (0, 2)$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



Protocol *under* $(y, z) \in S$

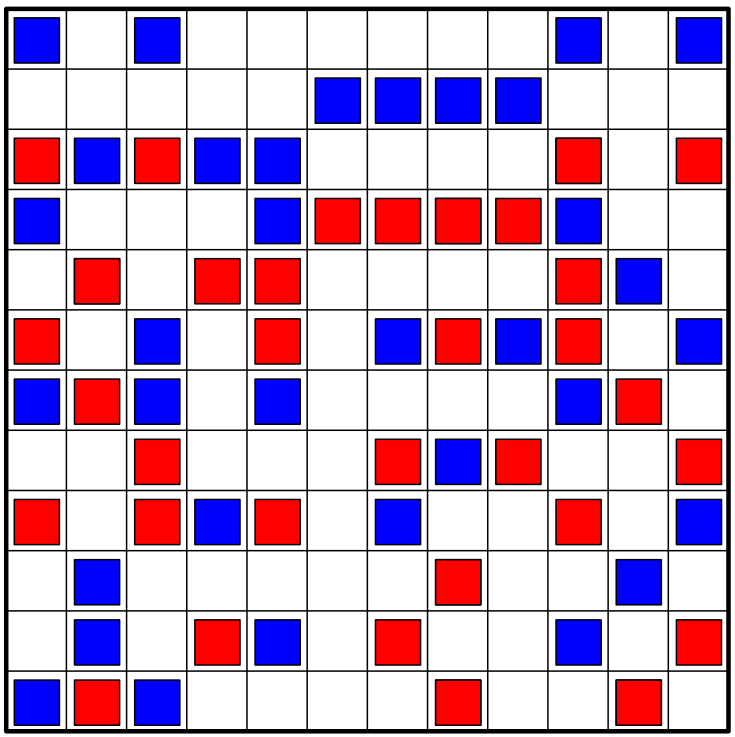
How to generalise?

Shift S! here $S' = S - (0, 2)$

Let A a set of vectors
Such that $[n]^2 \in \cup_{v \in A} S + v$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



Protocol *under* $(y, z) \in S$

How to generalise?

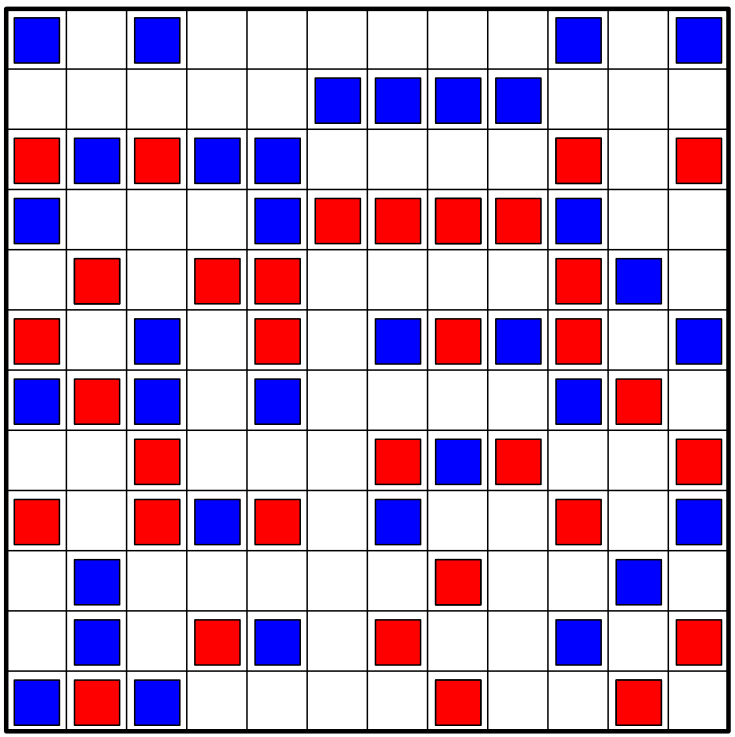
Shift S! here $S' = S - (0, 2)$

Let A a set of vectors
Such that $[n]^2 \in \cup_{v \in A} S + v$

New protocol:

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



Protocol *under* $(y, z) \in S$

How to generalise?

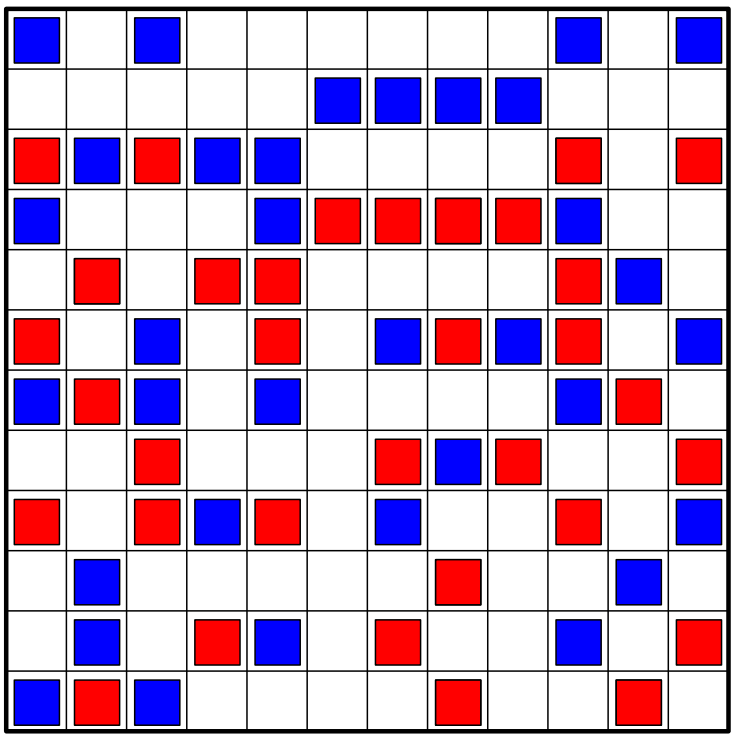
Shift S! here $S' = S - (0, 2)$

Let A a set of vectors
Such that $[n]^2 \in \cup_{v \in A} S + v$

New protocol:
P_x says the shift we play in
P_y and P_z play in the shift

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k



Protocol *under* $(y, z) \in S$

How to generalise?

Shift S! here $S' = S - (0, 2)$

Let A a set of vectors
Such that $[n]^2 \in \cup_{v \in A} S + v$

New protocol:
P_x says the shift we play in
P_y and P_z play in the shift

Complexity:
$\log(\#$ shifts to cover $[n]^2)$
$= \log |A|$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k

Goal: cover $[n]^2$ with minimum number of shifts of S

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k

Goal: cover $[n]^2$ with minimum number of shifts of S

set-cover **input:** set of sets $\mathcal{S} \in 2^X$
output: min number of sets of $\mathcal{S}$ covering X

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k

Goal: cover $[n]^2$ with minimum number of shifts of S

set-cover **input:** set of sets $\mathcal{S} \in 2^X$
output: min number of sets of $\mathcal{S}$ covering X

set-cover*: min $\sum_{S \in \mathcal{S}} \omega(S)$ under the conditions:

$\forall S\ \omega(S) \geq 0 \wedge \forall x \in X \sum_{x \in S} \omega(S) \geq 1$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k

Goal: cover $[n]^2$ with minimum number of shifts of S

set-cover **input:** set of sets $\mathcal{S} \in 2^X$
output: min number of sets of $\mathcal{S}$ covering X

set-cover*: min $\sum_{S \in \mathcal{S}} \omega(S)$ under the conditions:

$$\forall S\ \omega(S) \geq 0 \wedge \forall x \in X \sum_{x \in S} \omega(S) \geq 1$$

Theorem[Lovász, 1975]: set-cover $< O(\log |X| \cdot \text{set-cover}^*)$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k

Goal: cover $[n]^2$ with minimum number of shifts of S

set-cover **input:** set of sets $\mathcal{S} \in 2^X$
output: min number of sets of $\mathcal{S}$ covering X

set-cover*: min $\Sigma_{S \in \mathcal{S}}\, \omega(S)$ under the conditions:

$\forall S\ \omega(S) \geq 0 \wedge \forall x \in X\, \Sigma_{x \in S}\, \omega(S) \geq 1$

Theorem[Lovász, 1975]: set-cover $< O(\log |X| \cdot$set-cover $^*)$

Apply with: $\mathcal{S} :=$ all shifts of S $\quad X := [n]^2$

set-cover$^* \leq n^2/k$ by taking $\omega(S + v) = 1/k$

Big corner-free set $\Rightarrow$ good protocol

Let S be a corner-free set of size k

Goal: cover $[n]^2$ with minimum number of shifts of S

set-cover **input:** set of sets $\mathcal{S} \in 2^X$
output: min number of sets of $\mathcal{S}$ covering X

set-cover*: min $\Sigma_{S \in \mathcal{S}}\, \omega(S)$ under the conditions:

$\forall S\ \omega(S) \geq 0 \wedge \forall x \in X\, \Sigma_{x \in S}\, \omega(S) \geq 1$

Theorem[Lovász, 1975]: set-cover $< O(\log |X| \cdot$set-cover $^*)$

Apply with: $\mathcal{S} :=$ all shifts of S $\quad X := [n]^2$

set-cover*$\leq n^2/k$ by taking $\omega(S + v) = 1/k$

$\rightarrow$ set-cover $\leq O(n^2/k \log n)$

$\rightarrow$ protocol complexity $O(\log(n/k))$

Summary

Theorem

If a one round NOF equal protocol with $\leqslant b$-bits exists,
then there is a corner-free set of density $1/2^b$.

Theorem

If a corner-free set of density $1/2^b$ exists,
then a one round NOF equal protocol with $\leqslant O(\log(1/2^b)) = O(b)$-bits exists.

Theorem[Alon, Shraibman, '20]

There is a NOF equal protocol on $\leqslant \theta(\sqrt{\log n})$-bits.

A simple protocol on $[\mathbb{Z}_{2q}^d]^2$ instead of $[n]^2$

A simple protocol on $[\mathbb{Z}_{2q}^d]^2$ instead of $[n]^2$

We work with vectors $\overline{x} := (x_1, \ldots, x_d) \in \mathbb{N}^d \quad x_i \leq 2q$

$\overline{y} := (y_1, \ldots, y_d) \quad y_i \leq q$

$\overline{z} := (z_1, \ldots, z_d) \quad z_i \leq q$

A simple protocol on $[\mathbb{Z}_{2q}^d]^2$ instead of $[n]^2$

We work with vectors $\overline{x} := (x_1, \ldots, x_d) \in \mathbb{N}^d \quad x_i \leq 2q$

$\overline{y} := (y_1, \ldots, y_d) \quad y_i \leq q$

$\overline{z} := (z_1, \ldots, z_d) \quad z_i \leq q$

P_x, P_y and P_z want to decide if $\overline{y} + \overline{z} = \overline{x}$

A simple protocol on $[\mathbb{Z}_{2q}^d]^2$ instead of $[n]^2$

We work with vectors $\overline{x} := (x_1, \ldots, x_d) \in \mathbb{N}^d \quad x_i \leq 2q$

$\overline{y} := (y_1, \ldots, y_d) \quad y_i \leq q$

$\overline{z} := (z_1, \ldots, z_d) \quad z_i \leq q$

P_x, P_y and P_z want to decide if $\overline{y} + \overline{z} = \overline{x}$

P_x sends $||\overline{z} - \overline{y}||_2^2$ in $\log(dq^2)$ bits

A simple protocol on $[\mathbb{Z}_{2q}^d]^2$ instead of $[n]^2$

We work with vectors $\overline{x} := (x_1, \ldots, x_d) \in \mathbb{N}^d \quad x_i \leq 2q$

$\overline{y} := (y_1, \ldots, y_d) \quad y_i \leq q$

$\overline{z} := (z_1, \ldots, z_d) \quad z_i \leq q$

P_x, P_y and P_z want to decide if $\overline{y} + \overline{z} = \overline{x}$

P_x sends $||\overline{z} - \overline{y}||_2^2$ in $\log(dq^2)$ bits

P_y says YES if $||2\overline{z} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2$

A simple protocol on $[\mathbb{Z}_{2q}^d]^2$ instead of $[n]^2$

We work with vectors $\overline{x} := (x_1, \ldots, x_d) \in \mathbb{N}^d \quad x_i \leq 2q$

$\overline{y} := (y_1, \ldots, y_d) \quad y_i \leq q$

$\overline{z} := (z_1, \ldots, z_d) \quad z_i \leq q$

P_x, P_y and P_z want to decide if $\overline{y} + \overline{z} = \overline{x}$

P_x sends $||\overline{z} - \overline{y}||_2^2$ in $\log(dq^2)$ bits

P_y says YES if $||2\overline{z} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2$

P_z says YES if $||2\overline{y} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2$

A simple protocol on $[\mathbb{Z}_{2q}^d]^2$ instead of $[n]^2$

We work with vectors $\overline{x} := (x_1, \ldots, x_d) \in \mathbb{N}^d \quad x_i \leq 2q$

$\overline{y} := (y_1, \ldots, y_d) \quad y_i \leq q$

$\overline{z} := (z_1, \ldots, z_d) \quad z_i \leq q$

P_x, P_y and P_z want to decide if $\overline{y} + \overline{z} = \overline{x}$

P_x sends $||\overline{z} - \overline{y}||_2^2$ in $\log(dq^2)$ bits

P_y says YES if $||2\overline{z} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2$

P_z says YES if $||2\overline{y} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2$

Fact: $||2\overline{z} - \overline{x}||_2^2 = ||2\overline{y} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2 \Rightarrow \overline{y} + \overline{z} = \overline{x}$

A simple protocol on $[\mathbb{Z}_{2q}^d]^2$ instead of $[n]^2$

We work with vectors $\overline{x} := (x_1, \ldots, x_d) \in \mathbb{N}^d$ $\quad x_i \leq 2q$

$\overline{y} := (y_1, \ldots, y_d) \quad y_i \leq q$

$\overline{z} := (z_1, \ldots, z_d) \quad z_i \leq q$

P_x, P_y and P_z want to decide if $\overline{y} + \overline{z} = \overline{x}$

P_x sends $||\overline{z} - \overline{y}||_2^2$ in $\log(dq^2)$ bits $\quad << \log|\text{space}| = d \log q$

P_y says YES if $||2\overline{z} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2$

P_z says YES if $||2\overline{y} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2$

Fact: $||2\overline{z} - \overline{x}||_2^2 = ||2\overline{y} - \overline{x}||_2^2 = ||\overline{z} - \overline{y}||_2^2 \Rightarrow \overline{y} + \overline{z} = \overline{x}$

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

For $a \in [n]$ let $\overline{a_q} \in \mathbb{Z}^d$ the vector of its q-ary decomposition

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

For $a \in [n]$ let $\overline{a_q} \in \mathbb{Z}^d$ the vector of its q-ary decomposition

$C_q(a, b) \in \{0, 1\}^d :=$ carry vector of $a + b$ in base q

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

For $a \in [n]$ let $\overline{a_q} \in \mathbb{Z}^d$ the vector of its q-ary decomposition

$C_q(a, b) \in \{0, 1\}^d :=$ carry vector of $a + b$ in base q

Example: $C_2(1011_2, 1101_2) = 1001$

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

For $a \in [n]$ let $\overline{a_q} \in \mathbb{Z}^d$ the vector of its q-ary decomposition

$C_q(a,b) \in \{0,1\}^d :=$ carry vector of $a+b$ in base q

Example: $C_2(1011_2, 1101_2) = 1001$

Fact: There is a (simple) f such that:

$$\forall a, b, \overline{a_q} + \overline{b_q} + f(C_q(a,b)) = \overline{(a+b)_q}$$

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

For $a \in [n]$ let $\overline{a_q} \in \mathbb{Z}^d$ the vector of its q-ary decomposition

$C_q(a,b) \in \{0,1\}^d :=$ carry vector of $a+b$ in base q

Example: $C_2(1011_2, 1101_2) = 1001$

Fact: There is a (simple) f such that:

$$\forall a, b, \overline{a_q} + \overline{b_q} + f(C_q(a,b)) = \overline{(a+b)_q}$$

Knowing $C_q(a,b)$ reduces to the $\mathbb{Z}_{2q}^d$ case!

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

For $a \in [n]$ let $\overline{a_q} \in \mathbb{Z}^d$ the vector of its q-ary decomposition

$C_q(a,b) \in \{0,1\}^d :=$ carry vector of $a+b$ in base q

Example: $C_2(1011_2, 1101_2) = 1001$

Fact: There is a (simple) f such that:

$$\forall a, b, \overline{a_q} + \overline{b_q} + f(C_q(a,b)) = \overline{(a+b)_q}$$

Knowing $C_q(a,b)$ reduces to the $\mathbb{Z}_{2q}^d$ case!

Protocol: P_x writes $C_q(y,z)$ and $||\overline{z_q} - \overline{y_q}||_2^2$

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

For $a \in [n]$ let $\overline{a_q} \in \mathbb{Z}^d$ the vector of its q-ary decomposition

$C_q(a,b) \in \{0,1\}^d :=$ carry vector of $a+b$ in base q

Example: $C_2(1011_2, 1101_2) = 1001$

Fact: There is a (simple) f such that:
$$\forall a, b, \overline{a_q} + \overline{b_q} + f(C_q(a,b)) = \overline{(a+b)_q}$$

Knowing $C_q(a,b)$ reduces to the $\mathbb{Z}_{2q}^d$ case!

Protocol: P_x writes $C_q(y,z)$ and $||\overline{z_q} - \overline{y_q}||_2^2$
P_y and P_z can play in $\mathbb{Z}_{2q}^d$!

Complexity $d + 2\log dq$

From $\mathbb{Z}_q^d$ to $\mathbb{N}$

We cannot use the same trick: $||n||_2^2$ is too big

For $a \in [n]$ let $\overline{a_q} \in \mathbb{Z}^d$ the vector of its q-ary decomposition

$C_q(a,b) \in \{0,1\}^d :=$ carry vector of $a+b$ in base q

Example: $C_2(1011_2, 1101_2) = 1001$

Fact: There is a (simple) f such that:
$$\forall a, b, \overline{a_q} + \overline{b_q} + f(C_q(a,b)) = \overline{(a+b)_q}$$

Knowing $C_q(a,b)$ reduces to the $\mathbb{Z}_{2q}^d$ case!

Protocol: P_x writes $C_q(y,z)$ and $||\overline{z_q} - \overline{y_q}||_2^2$
P_y and P_z can play in $\mathbb{Z}_{2q}^d$!

Complexity $d + 2\log dq = \theta(\sqrt{\log n})$ for good d, q

Theorem[Alon, Shraibman, '20]

There is a NOF equal protocol on $\leqslant \theta(\sqrt{\log n})$-bits.

Theorem[Alon, Shraibman, '20]

There is a NOF equal protocol on $\leqslant \theta(\sqrt{\log n})$-bits.

Thank you!