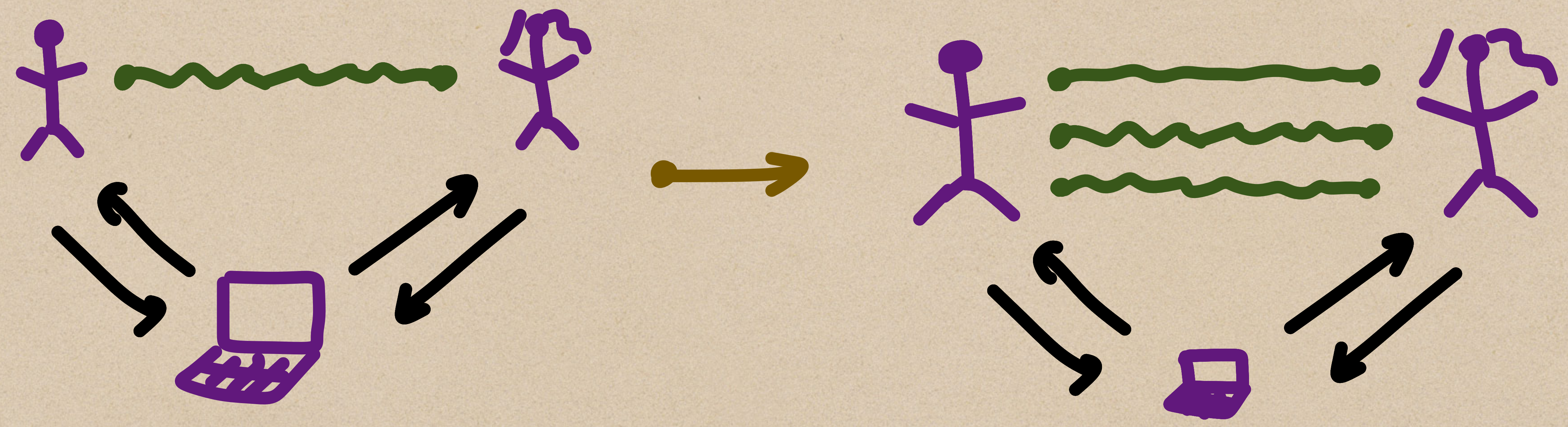
Compression of Nonlocal Games

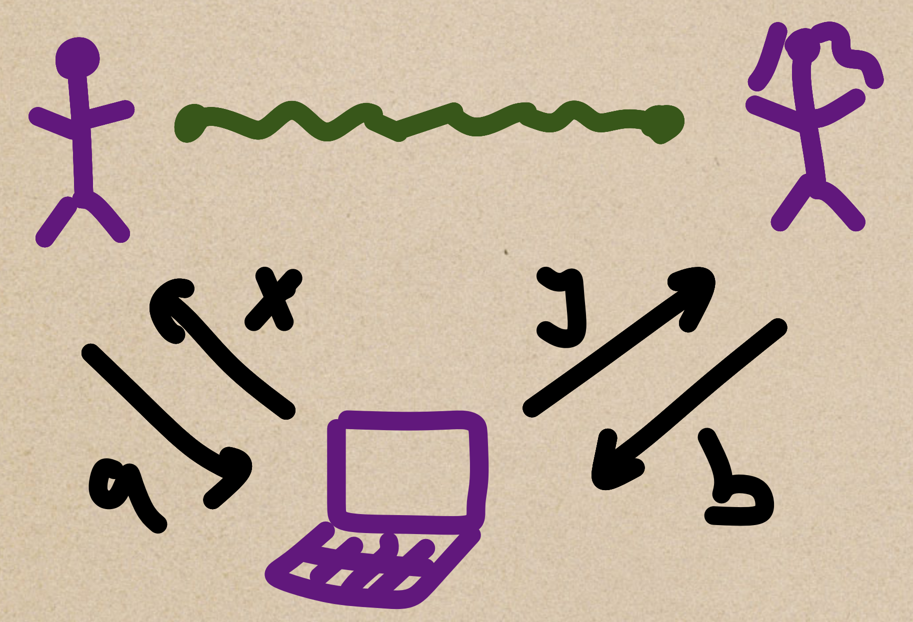


Sajjad Nezhadi

Hamoon Mousavi

Henry Yuen

Nonlocal Games



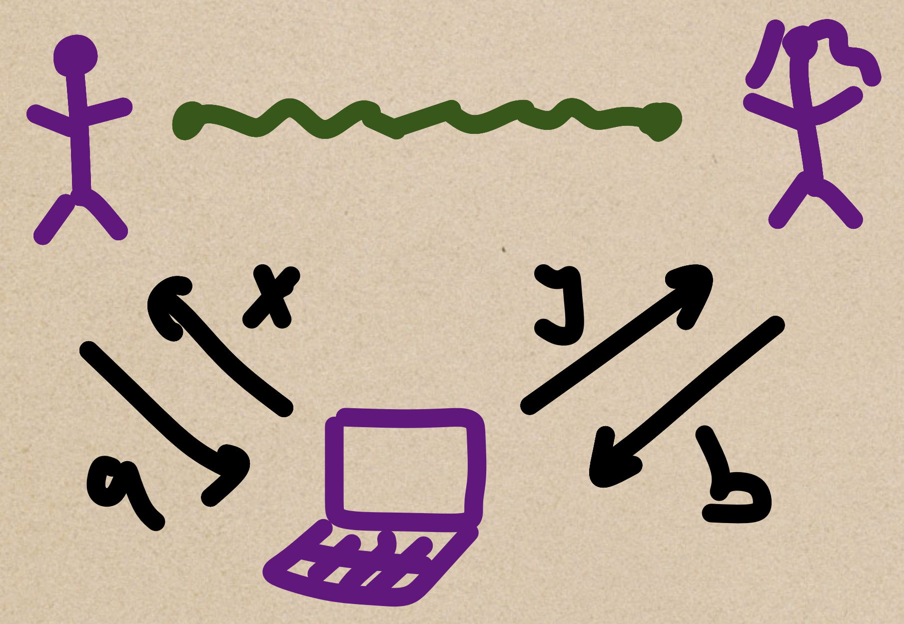
$G = (Q, A, D)$

$x, y \in Q$ Sampled questions

$a, b \in A$ Possible responses

$D(x, y, a, b)$ win condition

Nonlocal Games



$G = (Q, A, D)$

$x, y \in Q$ sampled questions

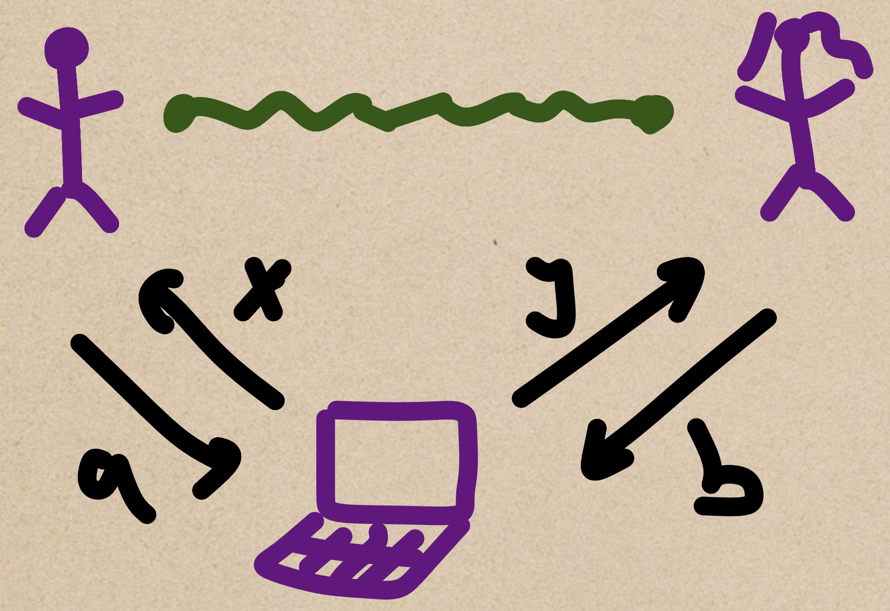
$a, b \in A$ possible responses

$D(x, y, a, b)$ win condition

$\omega(G)$ = max win probability over classical / non-entangled strategies

$\omega^*(G)$ = max win probability using entangled strategies

Nonlocal Games



$G = (Q, A, D)$

$x, y \in Q$ Sampled questions

$a, b \in A$ Possible responses

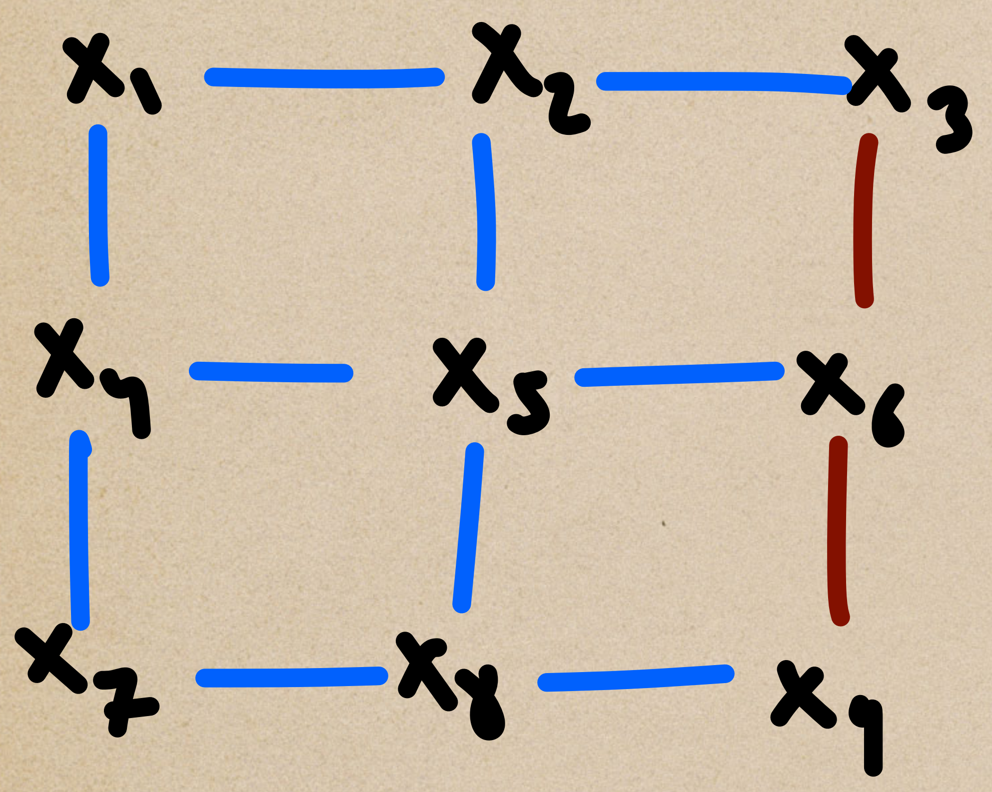
$D(x, y, a, b)$ win condition

$\omega(G)$ = max win probability over classical / non-entangled strategies

$\omega^*(G)$ = max win probability using entangled strategies

- Nonlocal games model interactive proofs with multiple provers
- Used for experimental proofs of quantumness.
- Widly used in Q cryptography

Magic Square Game

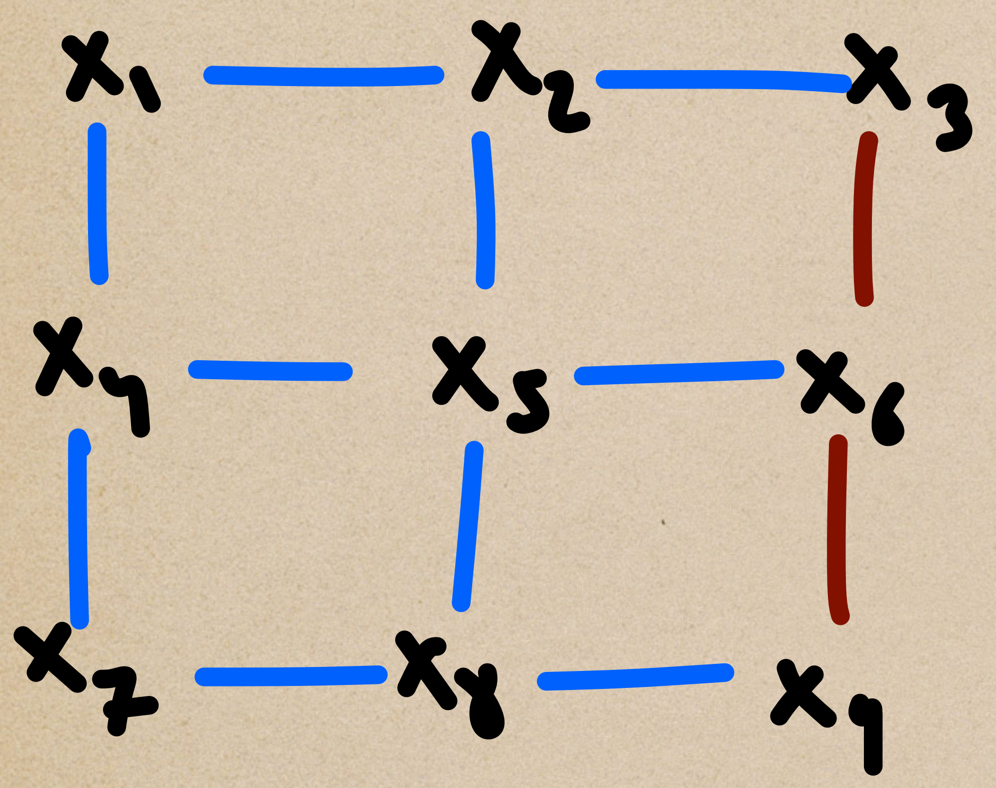


$$Q_A = \left\{ \begin{array}{ll} x_1 + x_2 + x_3 = 0 & x_1 + x_4 + x_7 = 0 \\ x_4 + x_5 + x_6 = 0 & x_2 + x_5 + x_8 = 0 \\ x_7 + x_8 + x_9 = 0 & x_3 + x_6 + x_9 = 1 \end{array} \right\}$$

$$Q_B = \{ x_1, \dots, x_9 \}$$

$$A = \{0, 1\}$$

Magic Square Game



$$Q_A = \left\{ \begin{array}{ll} x_1 x_2 x_3 = 1 & x_1 x_4 x_7 = 1 \\ x_4 x_5 x_6 = 1 & x_2 x_5 x_8 = 1 \\ x_7 x_8 x_9 = 1 & x_3 x_6 x_9 = -1 \end{array} \right\}$$

$$Q_B = \{ x_1, \dots, x_9 \}$$

$$A = \{+1, -1\}$$

$\omega(MS) = \frac{17}{18}$ $\longleftarrow$ The equations are not simultaniously satisfiable

$\omega^*(MS) = 1$ $\longleftarrow$ The equatins have an operator solution

Complexity of $\omega^*(G)$

Alternatively, how powerful are entangled multiprover interactive protocols?

How hard is it to decide if $\omega^*(G) = 1$ given a nonlocal game G?

Complexity of $\omega^*(G)$

Alternatively, how powerfull are entangled multiprover interactive protocols?

How hard is it to decide if $\omega^*(G) = 1$ given a nonlocal game G?

The promise problem $\omega^*(G)=1$ or $\omega^*(G) \leq 1/2$ was shown to be equivalent to the halting problem in the $MIP^*=RE$ paper of JNVWY

Complexity of $\omega^*(G)$

Alternatively, how powerful are entangled multiprover interactive protocols?

How hard is it to decide if $\omega^*(G) = 1$ given a nonlocal game G?

The promise problem $\omega^*(G)=1$ or $\omega^*(G) \leq 1/2$ was shown to be equivalent to the halting problem in the $MIP^*=RE$ paper of JNVWY

We showed exactly deciding if $\omega^*(G)=1$ is even more undecidable and equivalent to the universal halting problem.

Complexity of $\omega^*(G)$

Alternatively, how powerful are entangled multiprover interactive protocols?

How hard is it to decide if $\omega^*(G) = 1$ given a nonlocal game G?

The promise problem $\omega^*(G)=1$ or $\omega^*(G) \leq 1/2$ was shown to be equivalent to the halting problem in the $MIP^* = RE$ paper of JNVWY

We showed exactly deciding if $\omega^*(G) = 1$ is even more undecidable and equivalent to the universal halting problem.

Both these results use a technique known as iterated compression.

Computability Recap

Halting Problem: Decide if $T(x)$ Halts for a fixed x.

RE-complete

Computability Recap

Halting Problem: Decide if T(x) Halts for a fixed x.

RE-complete

Non Halting Problem: Decide if T(x) runs indefinitley for fixed x.

coRE-complete

Computability Recap

Halting Problem: Decide if $T(x)$ Halts for a fixed x.

RE-complete

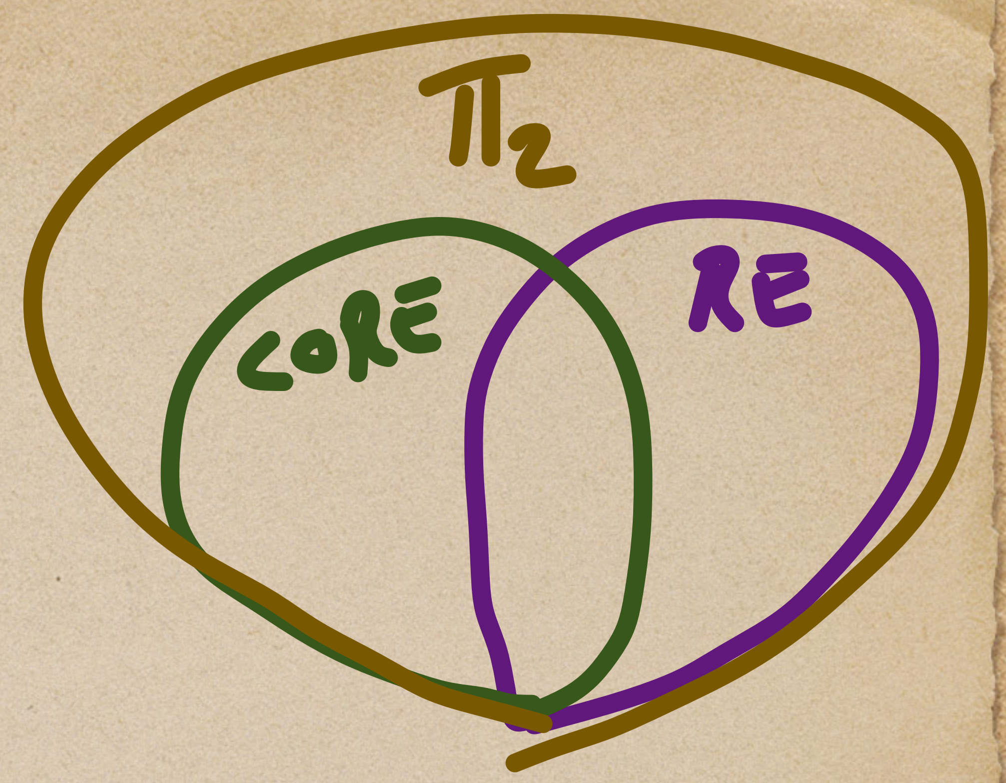
Non Halting Problem: Decide if $T(x)$ runs indefinitley for fixed x.

coRE-complete

Universal Halting Problem: Decide if $T(x)$ Halts for <u>every</u> input x.

Π_2 - Complete

Computability Recap



Halting Problem: Decide if T(x) Halts for a fixed x.

↑ RE-complete

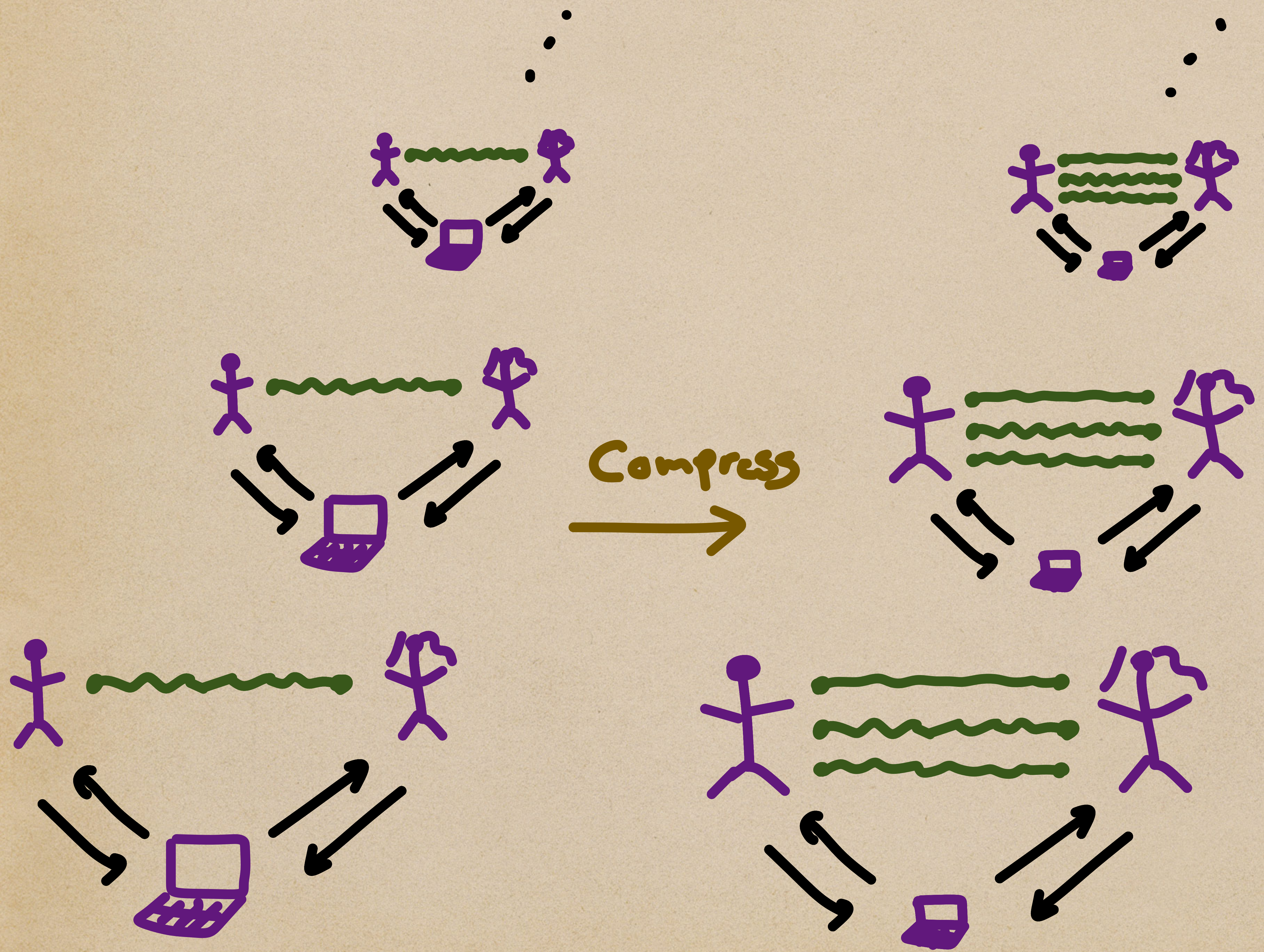
Non Halting Problem: Decide if T(x) runs indefinitley for fixed x.

↑ coRE-complete

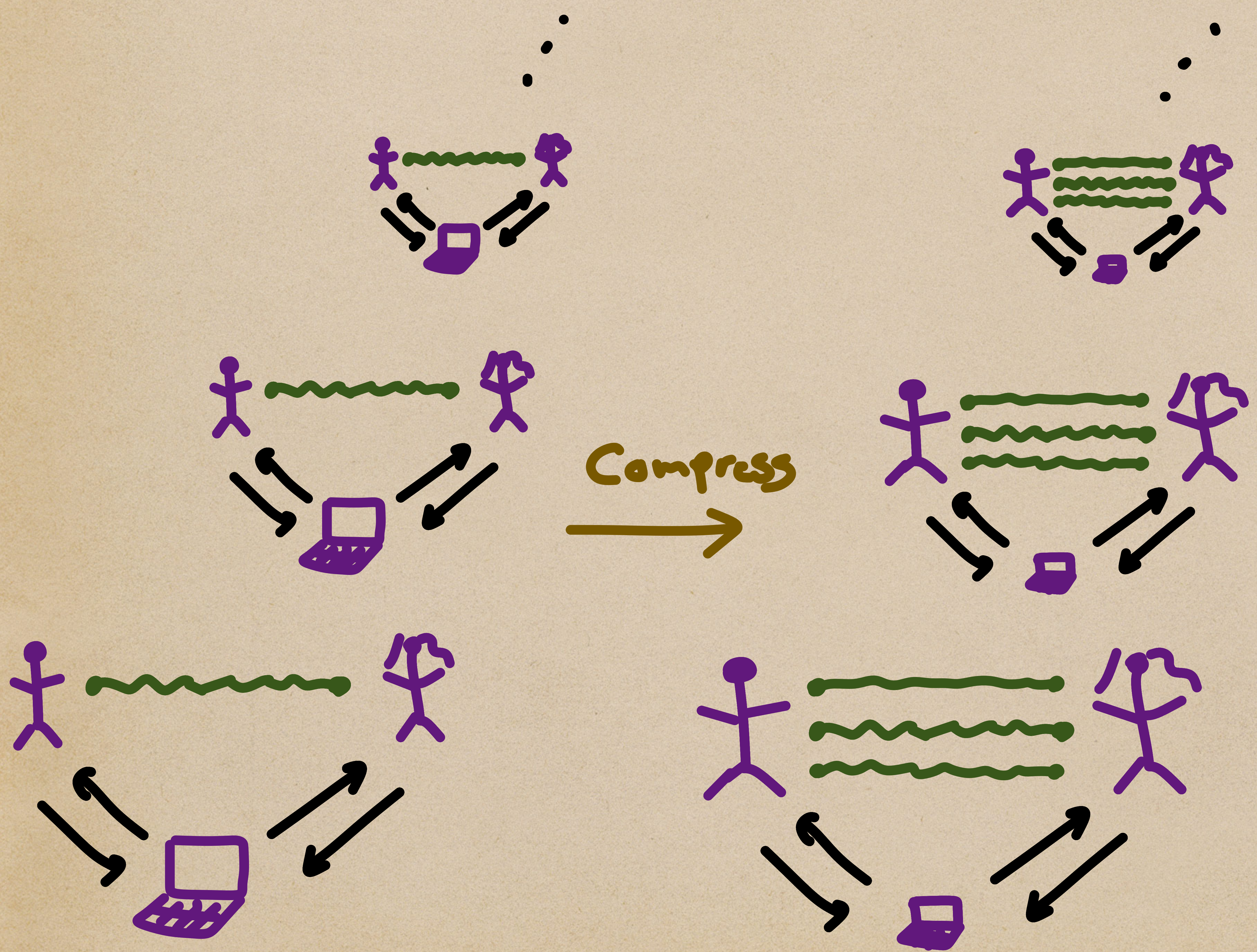
Universal Halting Problem: Decide if T(x) Halts for <u>every</u> input x.

↑ Π_2 - Complete

Compression

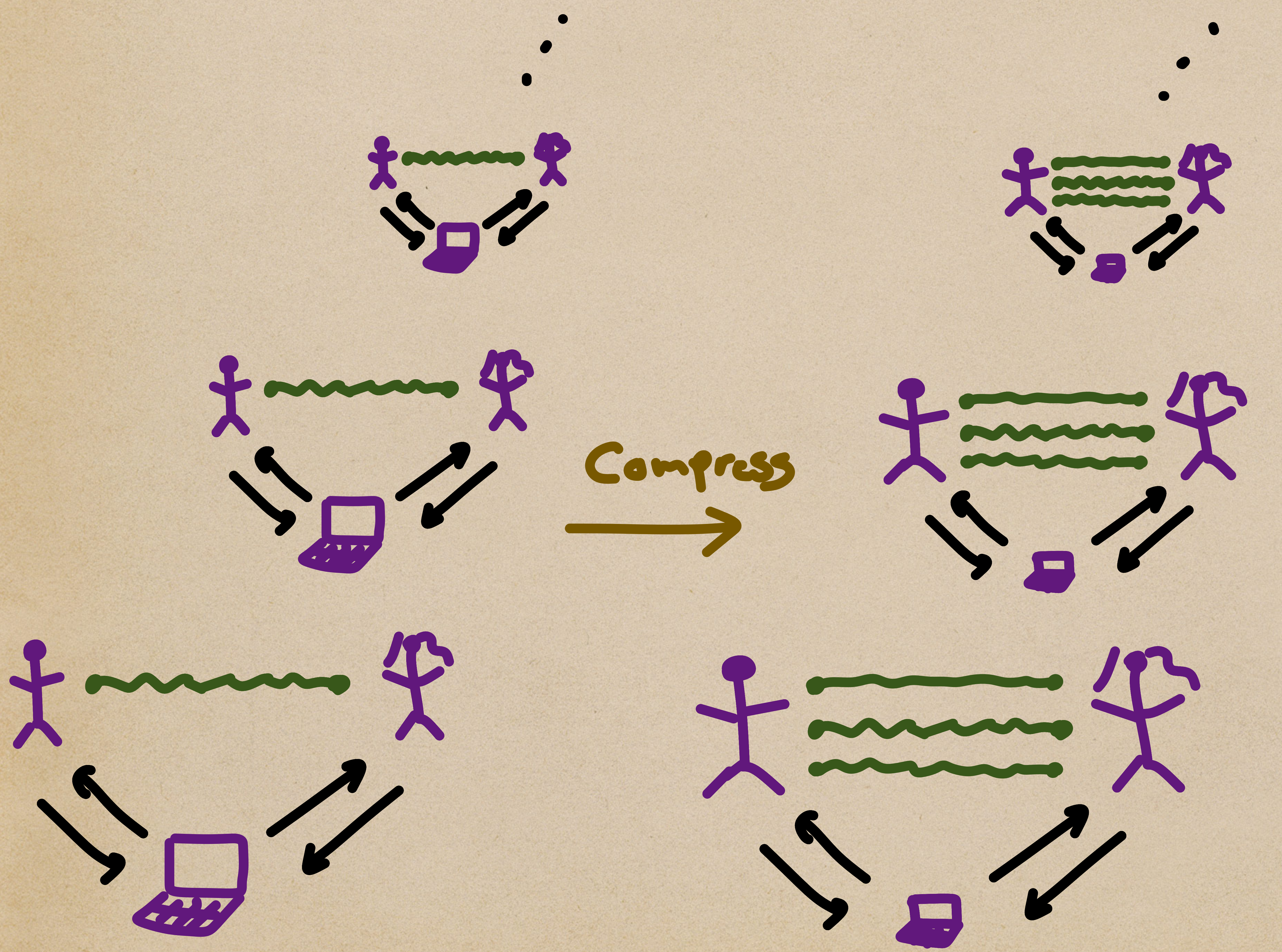


Compression



	$\{G_n\}$	$\longrightarrow$	$\{G_n'\}$
# Questions	N	$\longrightarrow$	$\mathrm{Log}(N)$
# Responses	N	$\longrightarrow$	$\log(N)$
Verifier Runtime	$\mathrm{poly}(n)$	$\longrightarrow$	$\mathrm{polylog}(N)$

Compression

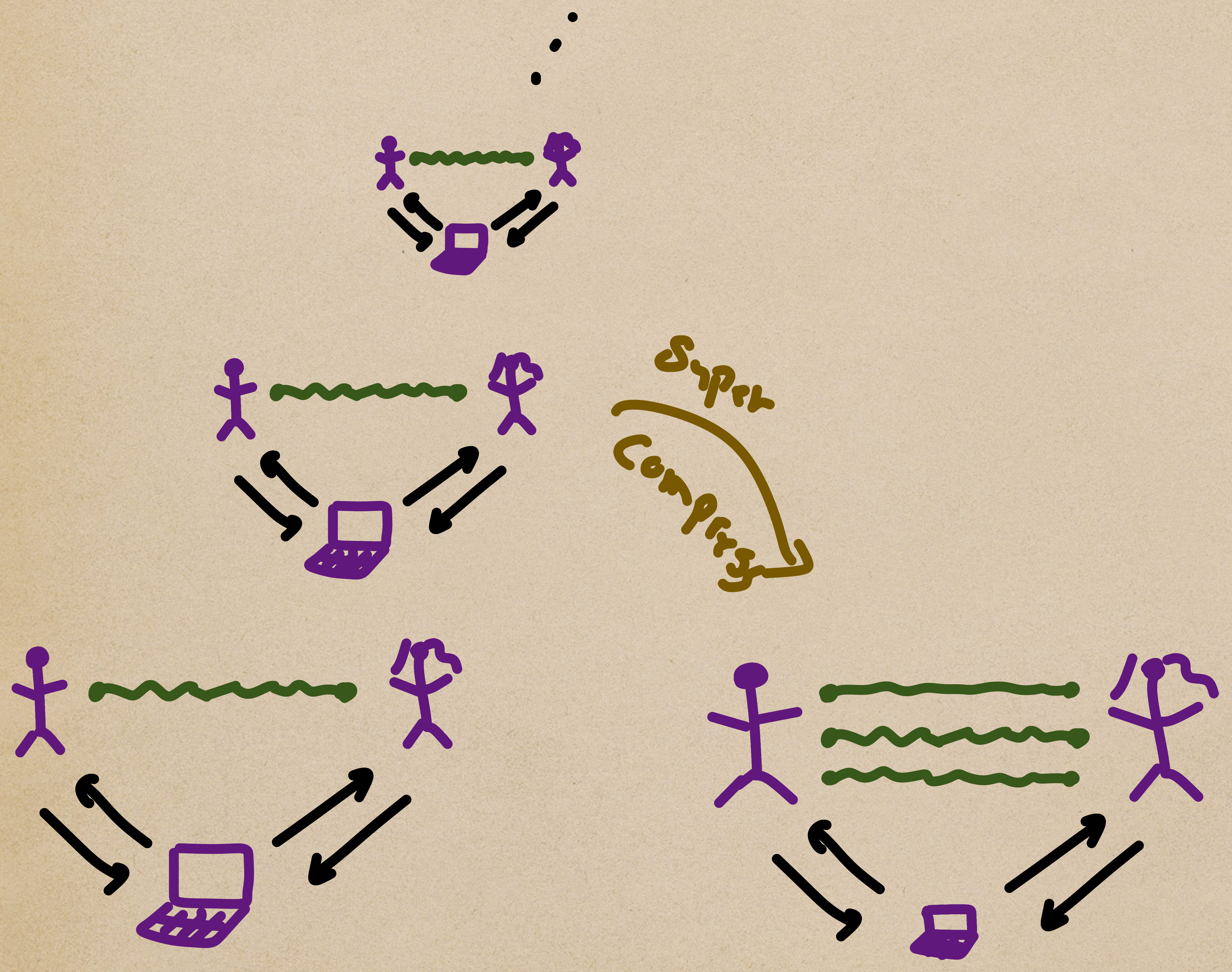


	$\{G_n\}$	$\longrightarrow \{G'_n\}$
# Questions	N	$\longrightarrow \log(N)$
# Responses	N	$\longrightarrow \log(N)$
Verifier Runtime	$\mathrm{poly}(n)$	$\longrightarrow \mathrm{polylog}(N)$

Related quantum values.

- $w^*(G'_n) \geq \frac{1}{2} + \frac{1}{2} w^*(G_n)$
- $w^*(G_n) < 1 \Rightarrow w^*(G'_n) < 1$

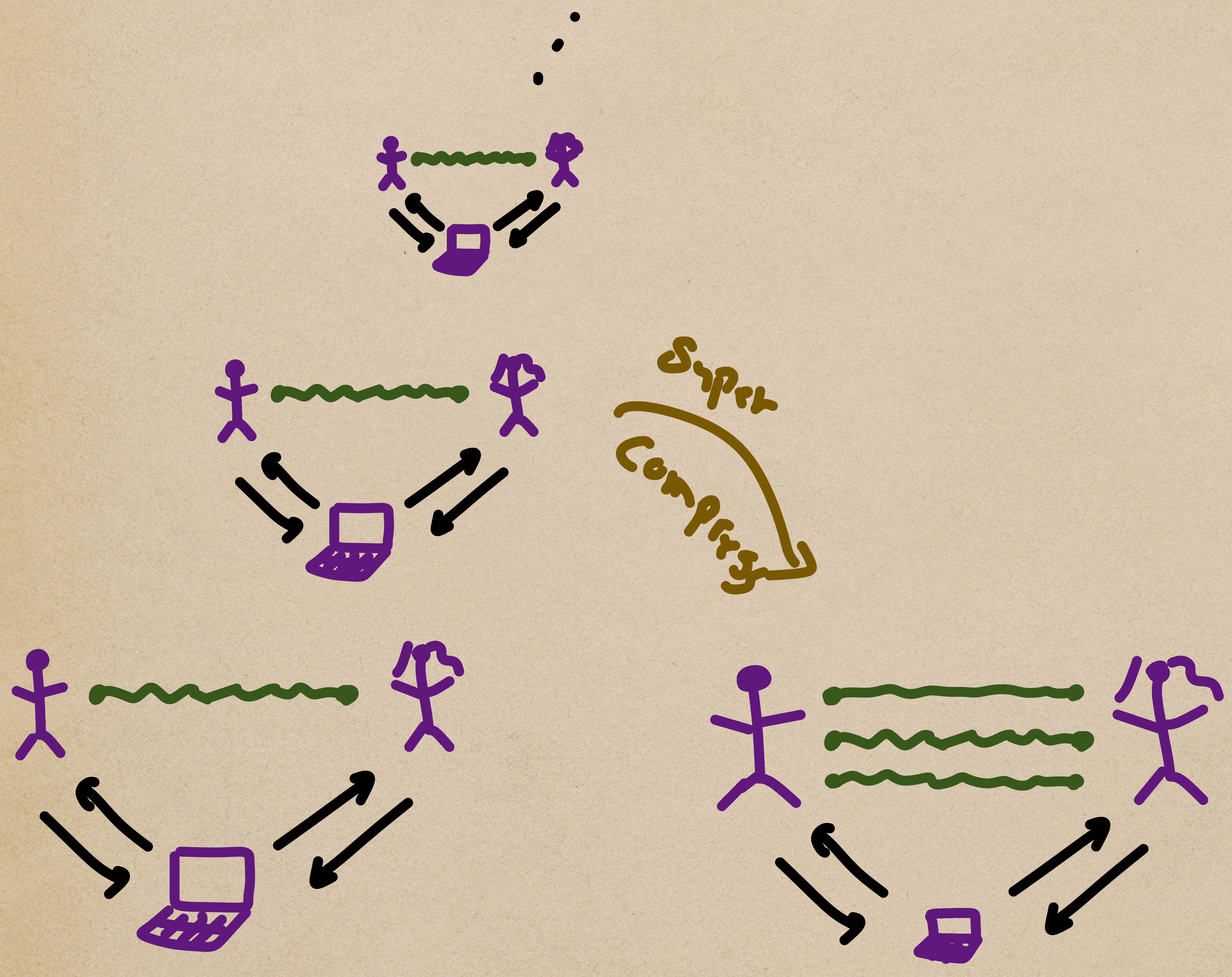
Super Compression



$$\forall n.\ w^*(G_n) = 1 \iff w^*(G^{\text{Super}}) = 1$$

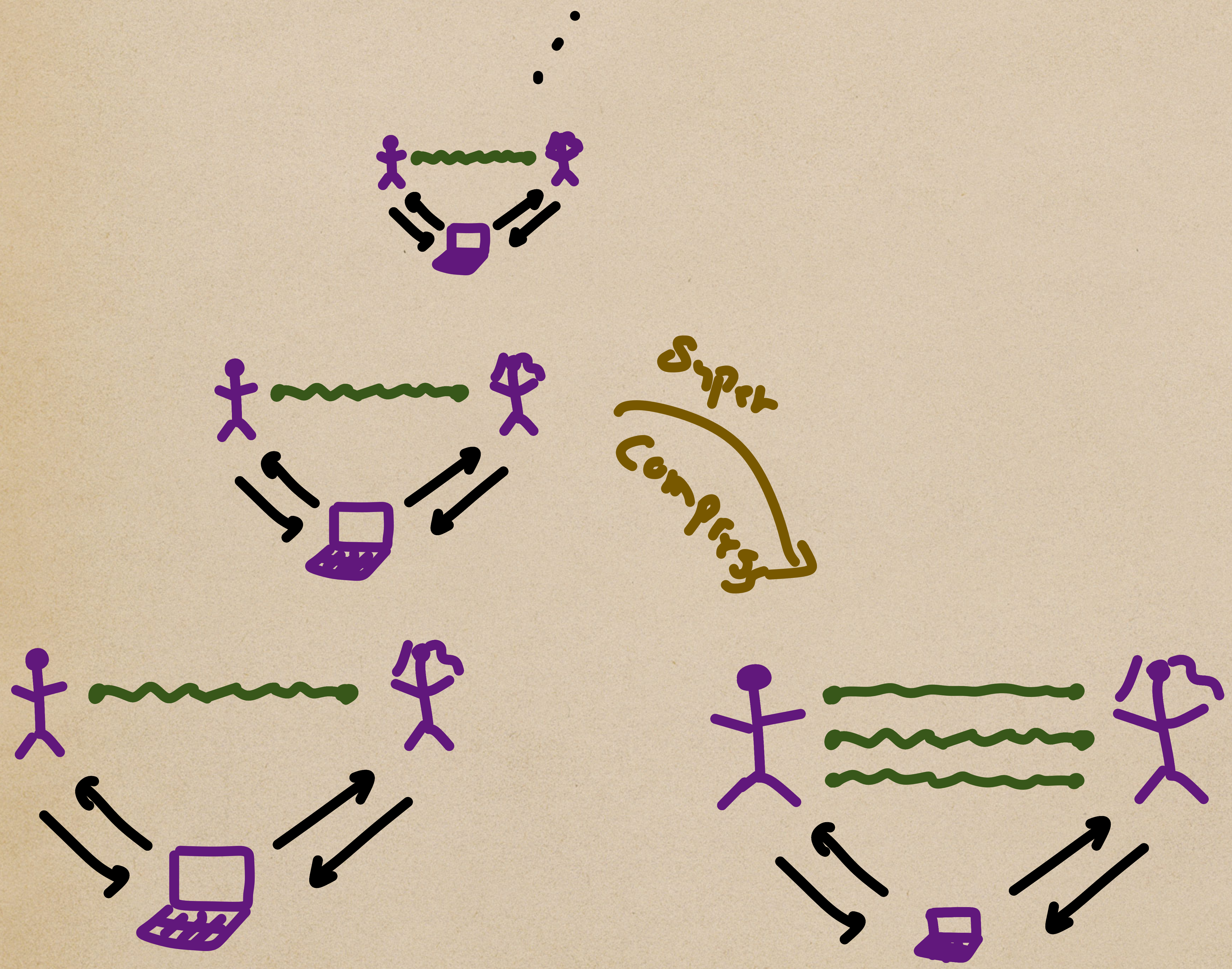
Super Compression

Reduction from Non Halting.



$$\forall n.\ w^*(G_n) = 1 \iff w^*(G^{Super}) = 1$$

Super Compression



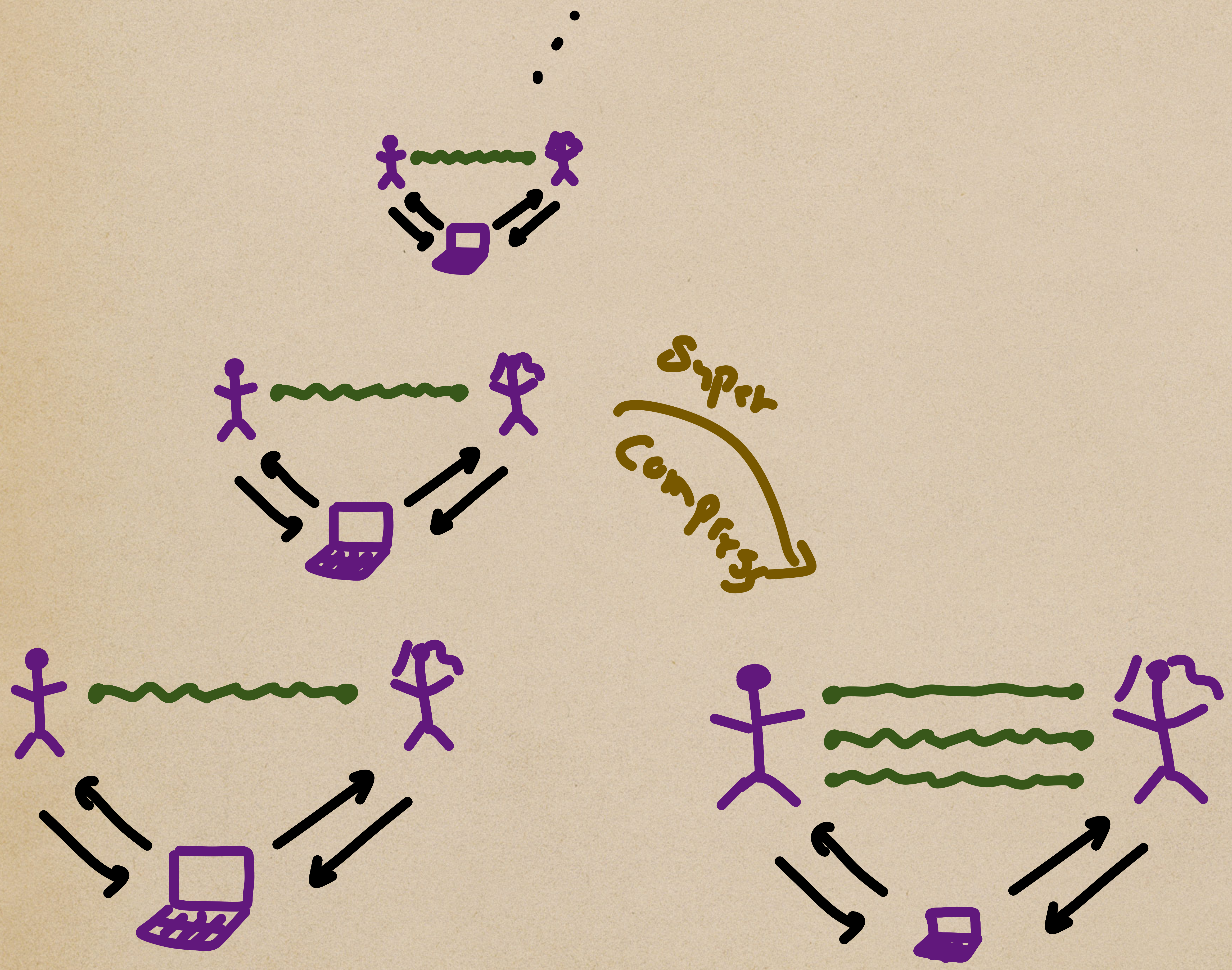
$$\forall n.\ w^*(G_n) = 1 \iff w^*(G^{Super}) = 1$$

Reduction from NonHalting.

G_n Verifier runs $T(x)$ for n steps and automatically makes players win if does not Halt.

O/w. makes players lose

Super Compression



$$\forall n.\ \omega^*(G_n) = 1 \iff \omega^*(G^{super}) = 1$$

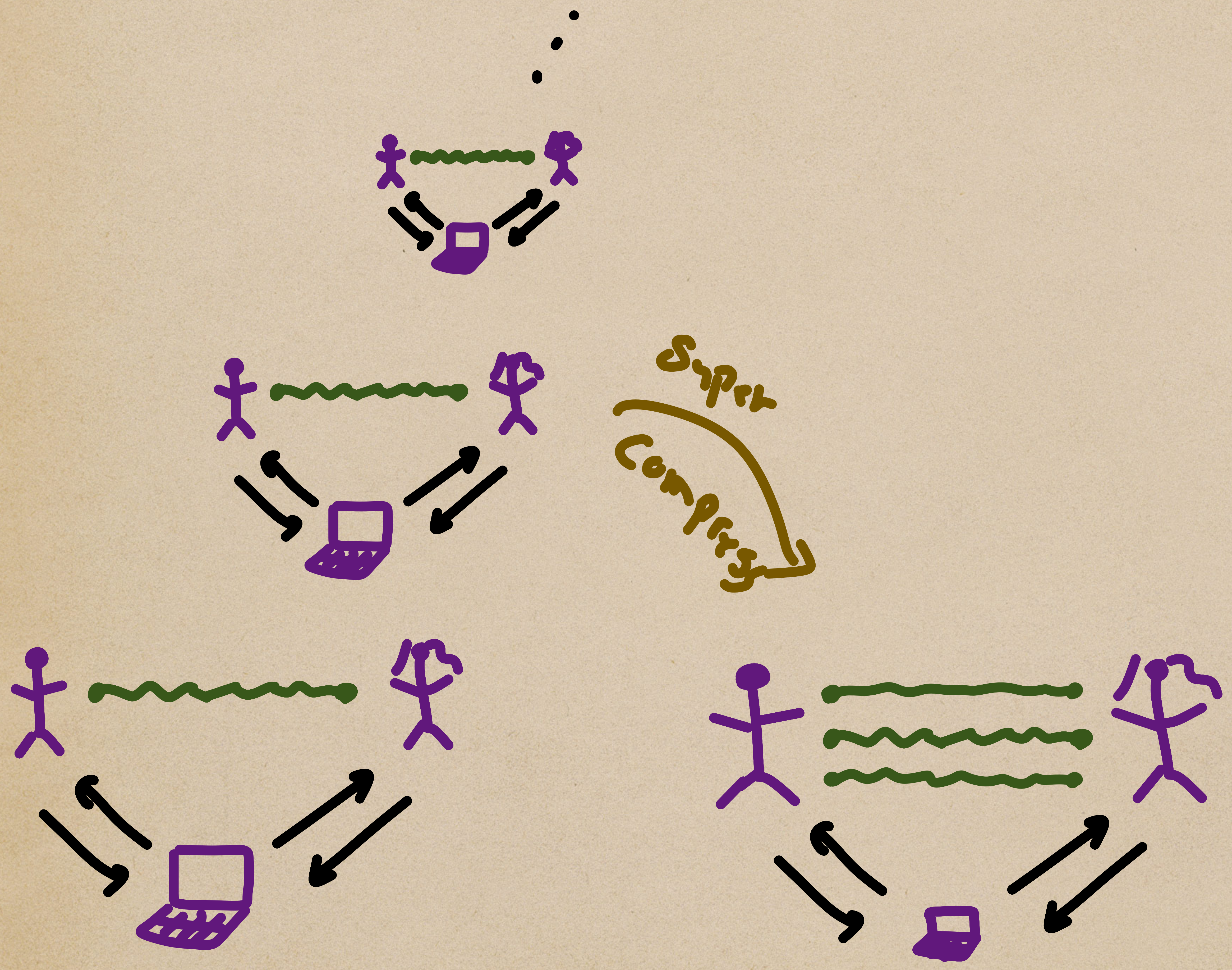
Reduction from Non Halting.

G_n Verifier runs $T(x)$ for n Steps and automatically makes players win if does not Halt.

O/w. makes players lose

$T(x)$ runs forever $\iff \omega^*(G_n) = 1\ \forall n.$

Super Compression



Reduction from NonHalting.

G_n Verifier runs $T(x)$ for n Steps and automatically makes players win if does not Halt.

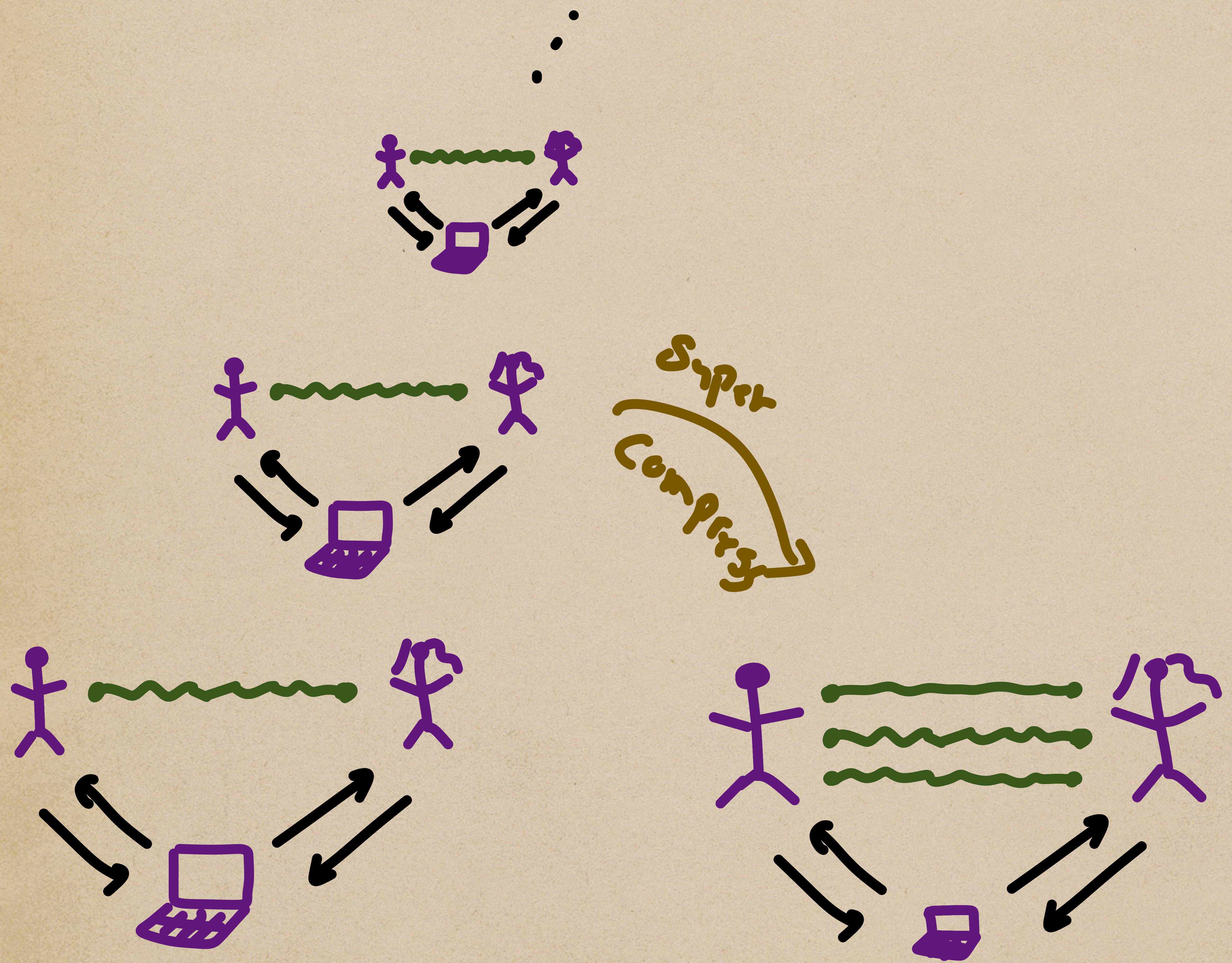
O/w. makes players lose

$T(x)$ runs forever $\iff w^*(G_n)=1 \ \forall n.$

Super Compress $\{G_n\}$ to $G^\#$

$$\forall n.\ w^*(G_n)=1 \iff w^*(G^{\text{Super}})=1$$

Super Compression



$\forall n.\ w^*(G_n) = 1 \iff w^*(G^{\text{Super}}) = 1$

Reduction from Non Halting.

G_n Verifier runs $T(x)$ for n Steps and automatically makes players win if does not Halt.

O/w. makes players lose

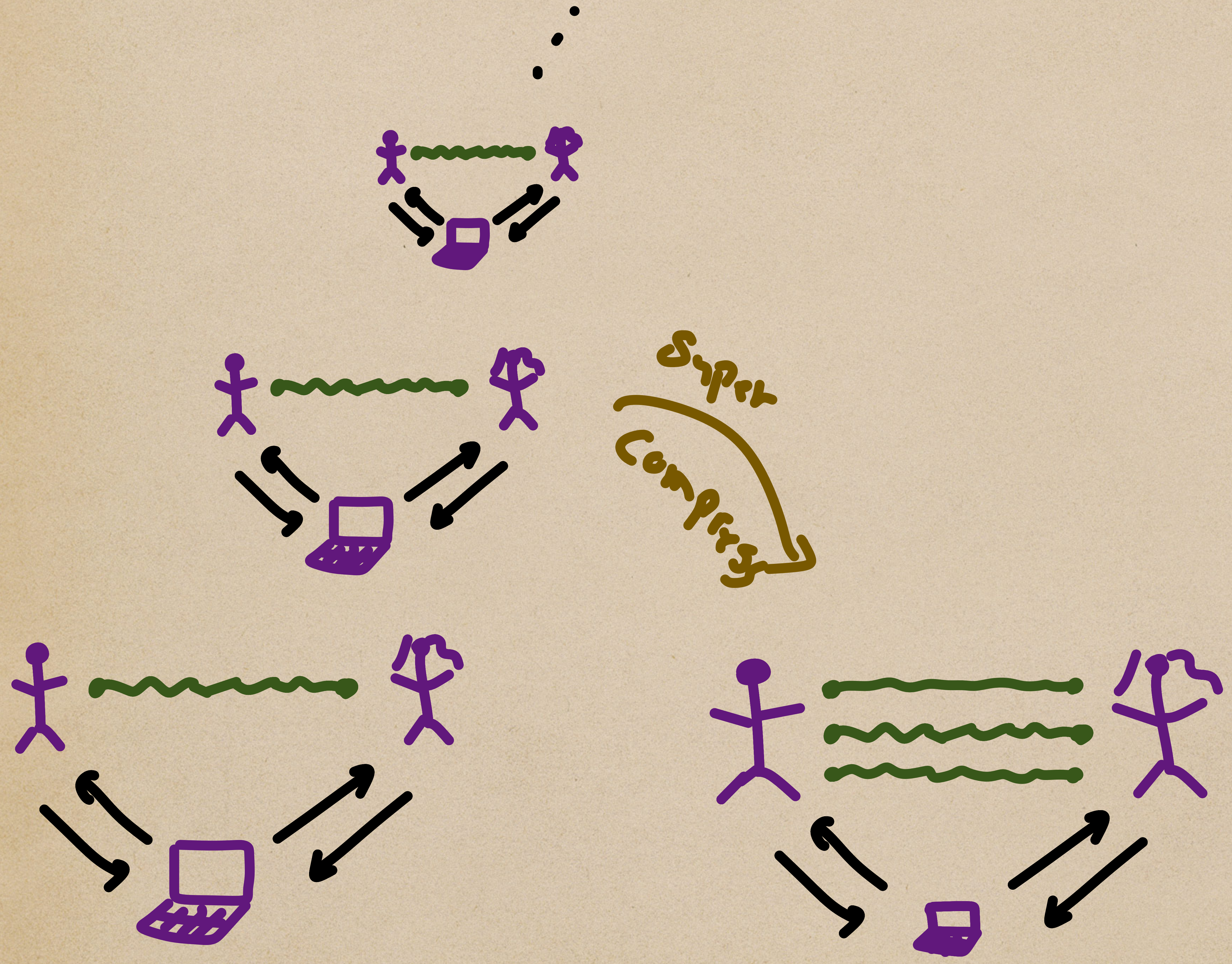
$T(x)$ runs forever $\iff w^*(G_n) = 1\ \forall n.$

Super Compress $\{G_n\}$ to $G^\#$

Then $T(x)$ runs forever $\iff w^*(G^\#) = 1$!

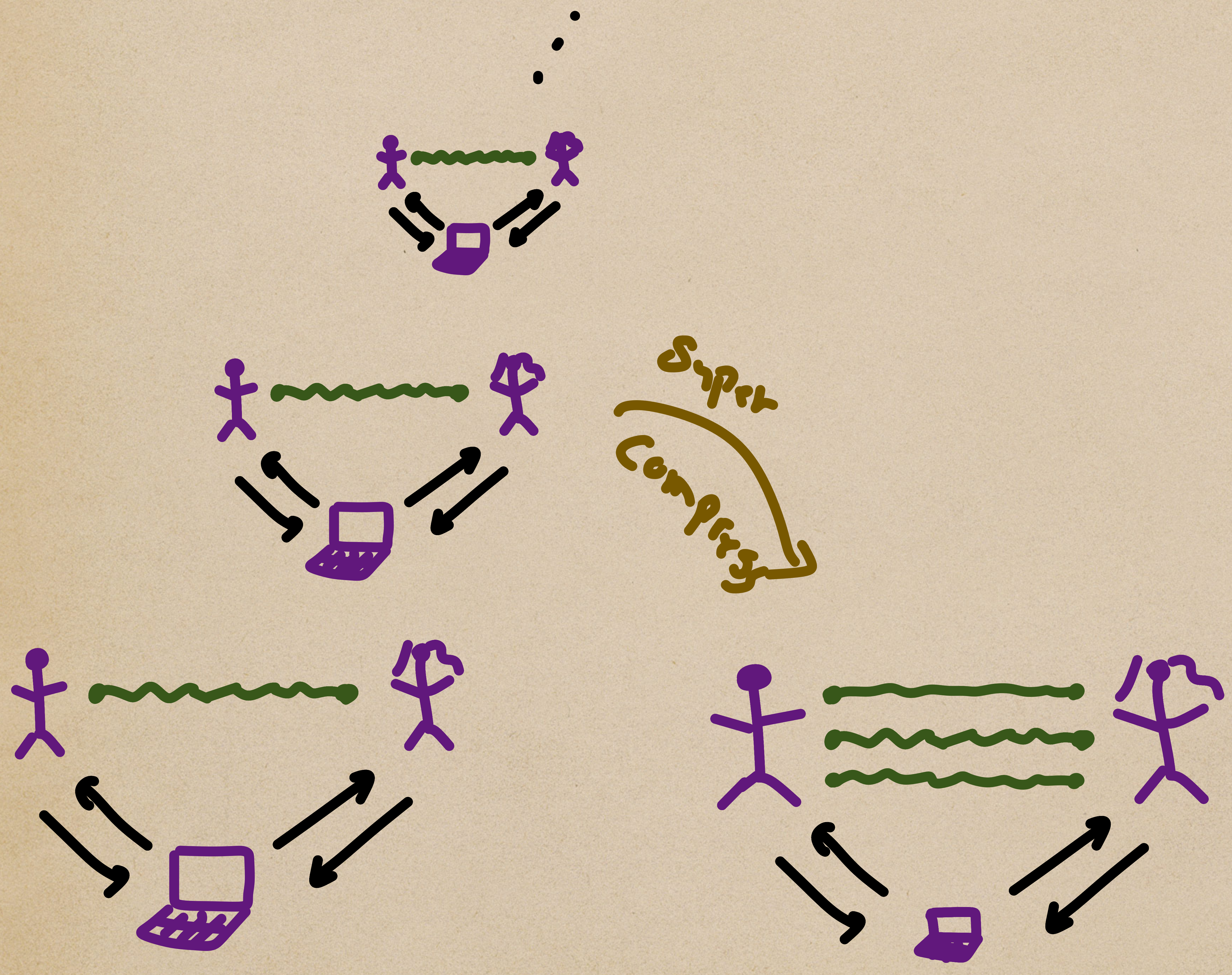
Super Compression

Reduction from Universal Halting.



$$\forall n.\ w^*(G_n) = 1 \iff w^*(G^{Super}) = 1$$

Super Compression



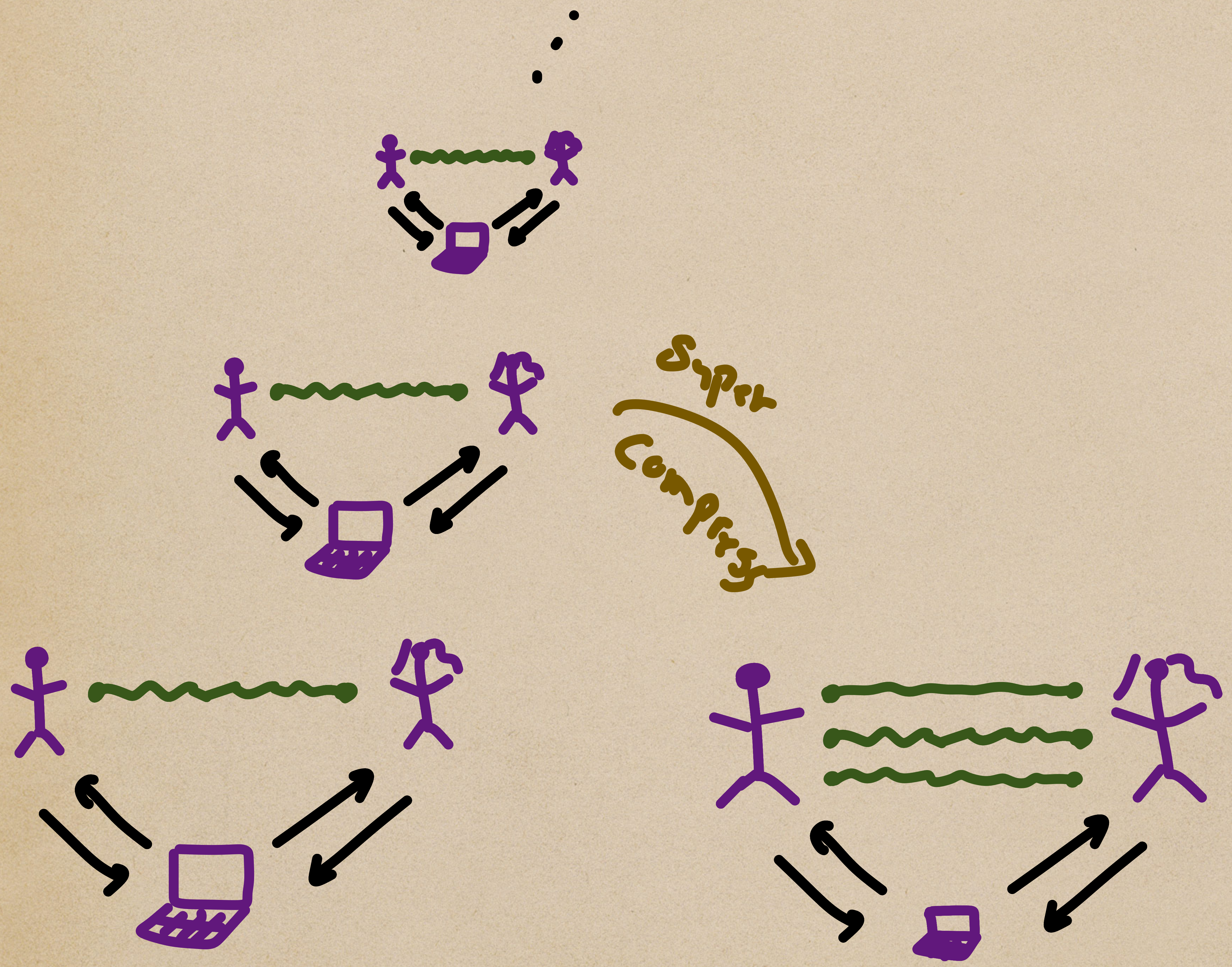
$\forall n.\ w^*(G_n) = 1 \iff w^*(G^{Super}) = 1$

Reduction from Universal Halting.

G_n verifier uses $MIP^* = RE$ reduction to obtain game that decides if $T(Bin(n))$ Halts.

Then proceeds to play according to it.

Super Compression



$$\forall n.\ w^*(G_n) = 1 \iff w^*(G^{Super}) = 1$$

Reduction from Universal Halting.

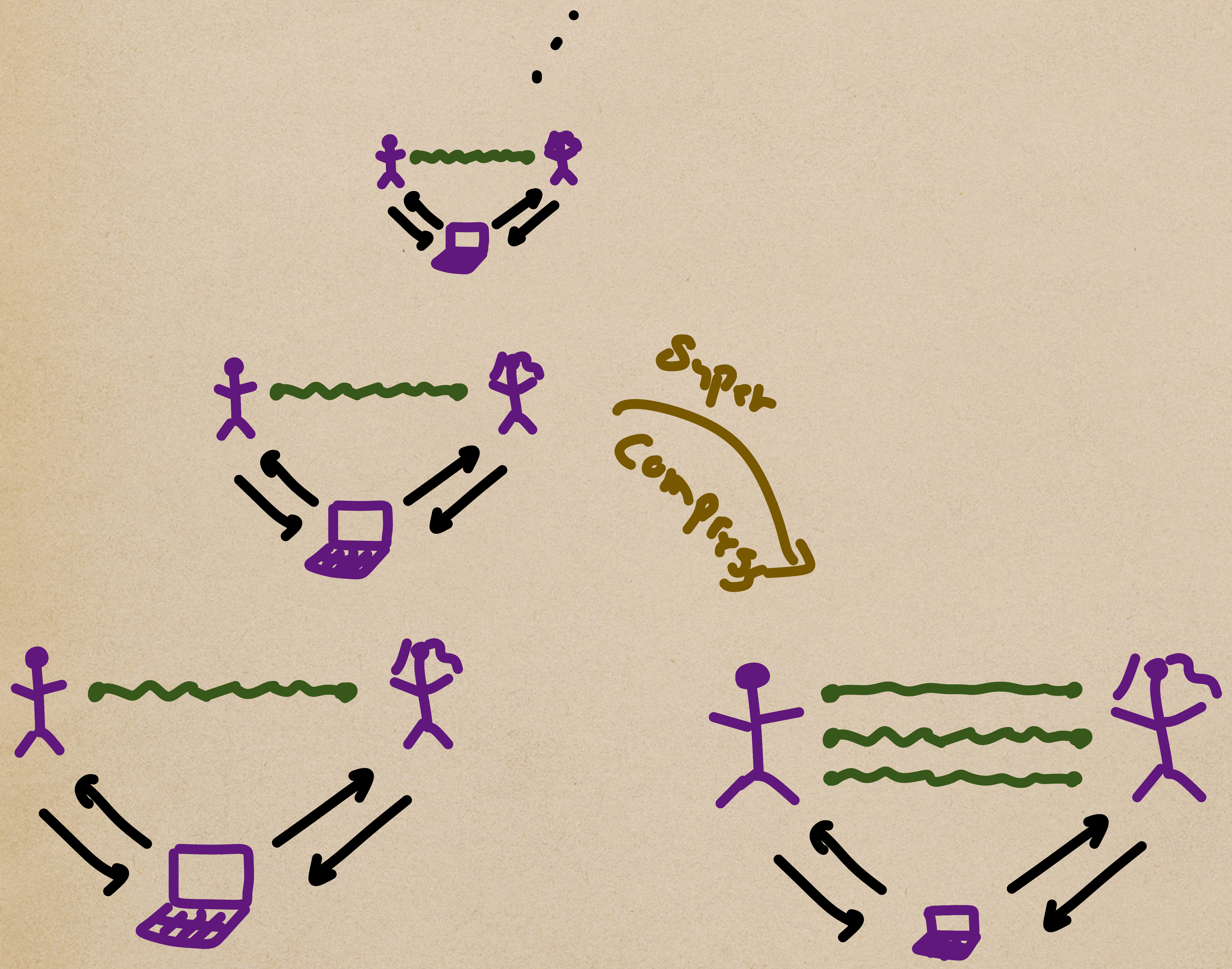
G_n verifier uses $MIP^* = RE$ reduction to obtain game that decides if $T(Bin(n))$ Halts.

Then proceeds to play according to it.

$T(x)$ Halts for every x

$$\iff w^*(G_n) = 1 \ \forall n.$$

Super Compression



$\forall n.\ w^*(G_n) = 1 \iff w^*(G^{Super}) = 1$

Reduction from Universal Halting.

G_n verifier uses $MIP^* = RE$ reduction to obtain game that decides if $T(Bin(n))$ Halts.

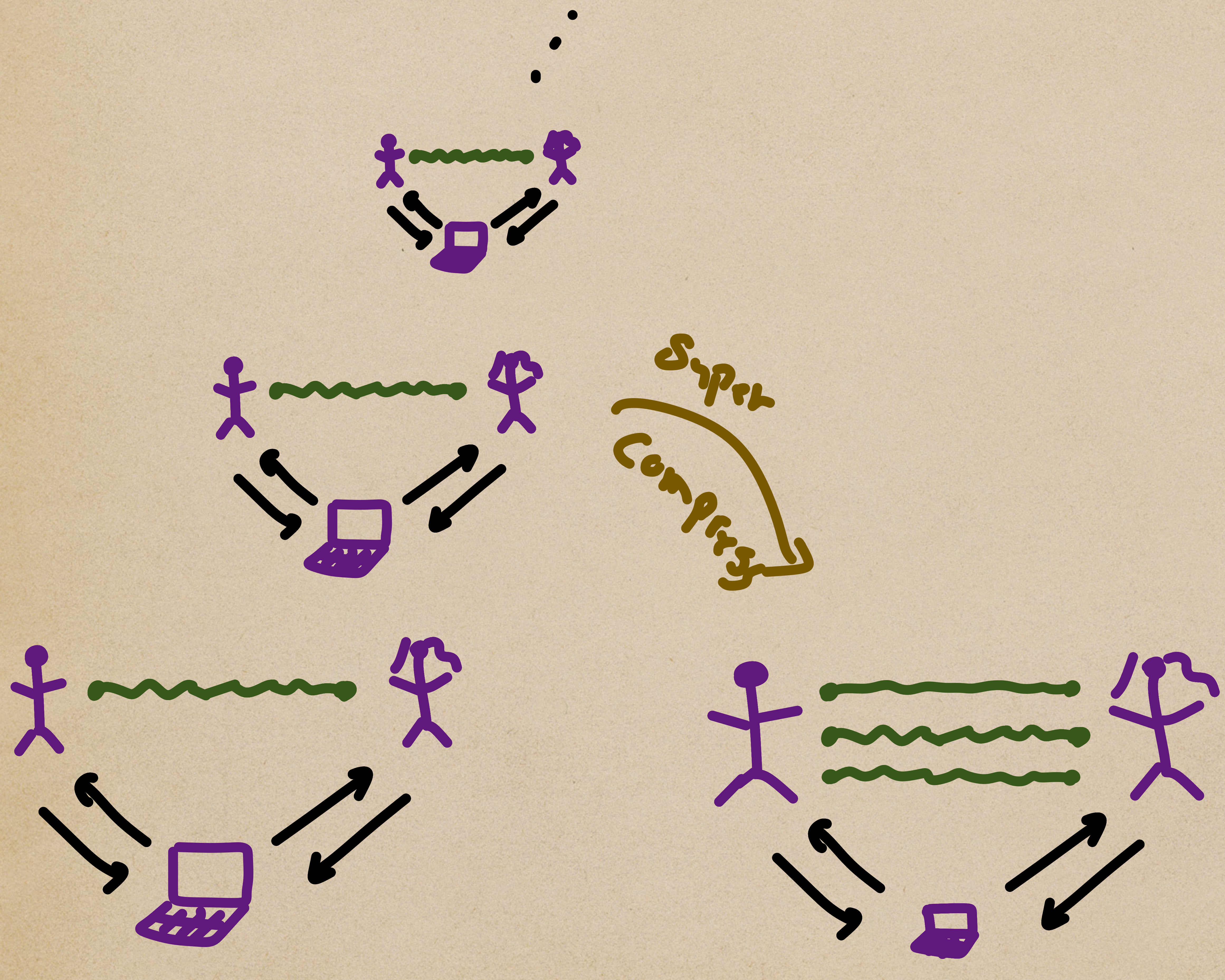
Then proceeds to play according to it.

$T(x)$ Halts for every x

$\iff w^*(G_n) = 1 \ \forall n.$

Super Compress $\{G_n\}$ to $G^{\#}$

Super Compression



$$\forall n.\ w^*(G_n)=1 \iff w^*(G^{Super})=1$$

Reduction from Universal Halting.

G_n verifier uses $MIP^*=RE$ reduction to obtain game that decides if $T(Bin(n))$ Halts.

Then proceeds to play according to it.

$T(X)$ Halts for every X

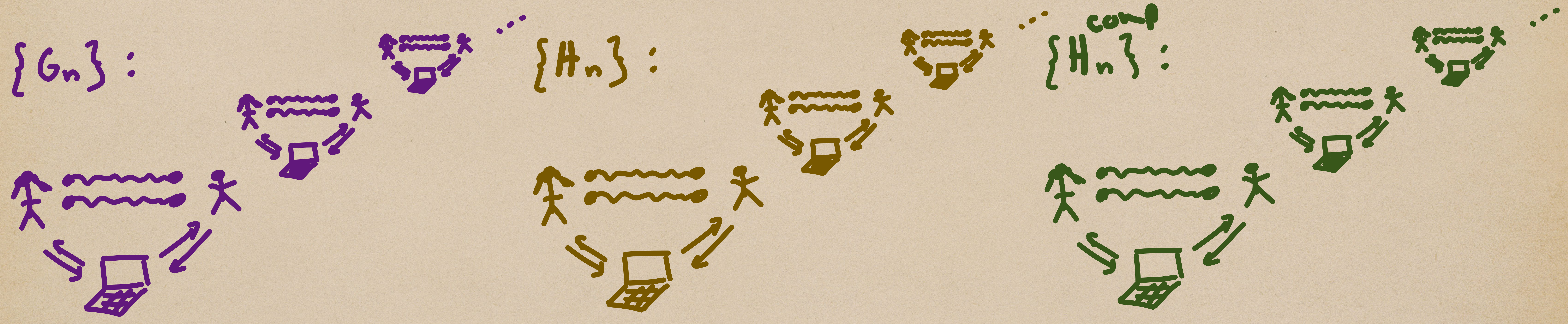
$$\iff w^*(G_n)=1\ \forall n.$$

Super Compress $\{G_n\}$ to $G^\#$

Then $T(x)$ Halts on every X

$$\iff w^*(G^\#)=1$$

Iterated Compression



Iterated Compression

$\{G_n\}$:

$\{H_n\}$:

$\{H_n\}^{comp}$:

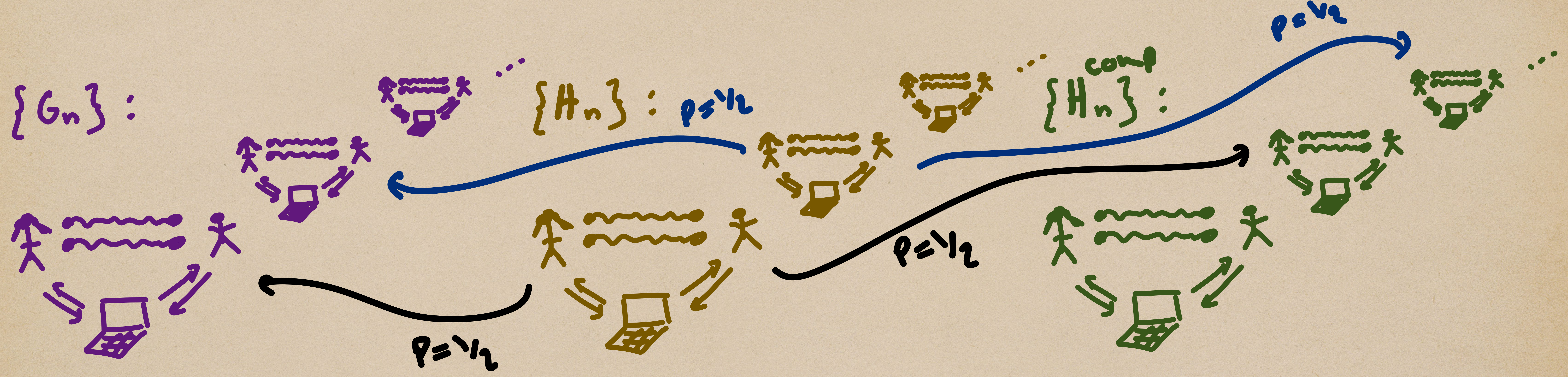
Family we wish to SuperCompress

New family we define such that $G^{\#} = H_1$

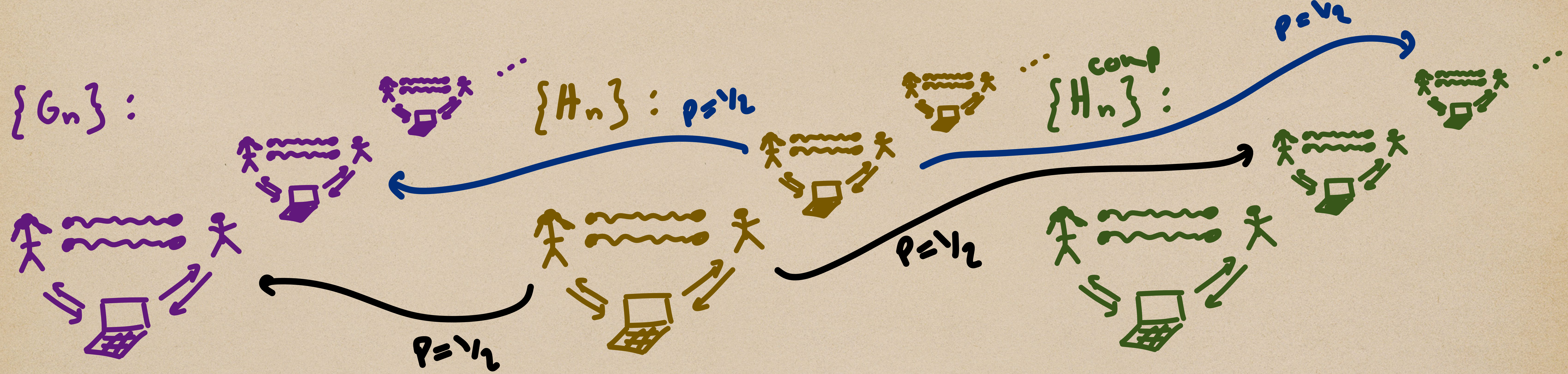
Compression of $\{H_n\}$ family

Iterated Compression

Iterated Compression



Iterated Compression



Claim. $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n.$

Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n.$

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$

Claim: $\omega^*(H_1) = 1 \iff \omega^*(G_n) = 1 \ \forall n.$

If $\omega^*(G_n) = 1 \ \forall n$

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $\omega^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2}\omega^*(H_n)$
- $\omega^*(H_n) < 1 \Rightarrow \omega^*(H_n^{comp}) < 1$

<u>Claim</u>: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n.$

If $w^*(G_n) = 1 \ \forall n$

$\Rightarrow w^*(H_n) = \frac{1}{2} + \frac{1}{2} w^*(H_{n+1}^{comp})$ [Def. H_n]

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$

Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n.$

If $w^*(G_n) = 1 \ \forall n$

$\Rightarrow w^*(H_n) = \frac{1}{2} + \frac{1}{2} w^*(H_{n+1}^{comp})$ [Def. H_n]

$\Rightarrow w^*(H_n) \geq 3/4 + 1/4\, w^*(H_{n+1})$ [Comp]

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$

Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n.$

If $w^*(G_n) = 1 \ \forall n$

$\Rightarrow w^*(H_n) = \frac{1}{2} + \frac{1}{2} w^*(H_{n+1}^{comp})$ [Def. H_n]

$\Rightarrow w^*(H_n) \geq 3/4 + 1/4\, w^*(H_{n+1})$ [Comp]

$\vdots$

$\Rightarrow w^*(H_1) \geq 1 - \lim_{n \to \infty} \frac{1}{4^n}\left(1 + w^*(H_n)\right)$

$= 1!$

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$

<u>Claim</u>: $\omega^*(H_1) = 1 \iff \omega^*(G_n) = 1 \ \forall n.$

If $\omega^*(G_k) < 1$ for some k.

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $\omega^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2}\omega^*(H_n)$
- $\omega^*(H_n) < 1 \Rightarrow \omega^*(H_n^{comp}) < 1$

Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n.$

If $w^*(G_k) < 1$ for some k.

$$\Rightarrow w^*(H_k) = \frac{1}{2} w^*(H_{k+1}^{comp}) + \frac{1}{2} w^*(G_k) \quad [\text{Def. } H_n]$$

$$< \underline{1}$$

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$

Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n.$

If $w^*(G_k) < 1$ for some k.

$$\Rightarrow w^*(H_k) = \underbrace{\tfrac{1}{2} w^*(H_{k+1}^{comp}) + \tfrac{1}{2} w^*(G_k)}_{<1} \quad [\text{Def. } H_n]$$

$$\Rightarrow w^*(H_k^{comp}) < 1 \quad [\text{Comp}]$$

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$

Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \;\; \forall n.$

If $w^*(G_k) < 1$ for some k.

$$\Rightarrow w^*(H_k) = \frac{1}{2} w^*(H_{k+1}^{comp}) + \frac{1}{2} w^*(G_k) \quad [\text{Def. } H_n]$$

$$< 1$$

$$\Rightarrow w^*(H_k^{comp}) < 1 \quad [\text{Comp}]$$

$$\Rightarrow w^*(H_{k-1}) < 1 \quad [\text{Def. } H_n]$$

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H_{n+1}^{comp}

Compression:

- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$

Claim: $w^*(H_1) = 1 \iff w^*(G_n) = 1 \ \forall n.$

If $w^*(G_k) < 1$ for some k.

$$\Rightarrow w^*(H_k) = \frac{1}{2} w^*(H^{comp}_{k+1}) + \frac{1}{2} w^*(G_k) \quad [\text{Def. } H_n]$$

$$< \underline{1}$$

$$\Rightarrow w^*(H^{comp}_k) < 1 \quad [\text{Comp}]$$

$$\Rightarrow w^*(H_{k-1}) < 1 \quad [\text{Def. } H_n]$$

$$\vdots$$

$$\Rightarrow w^*(H_1) < 1!$$

H_n:

- $p = 1/2$ play G_n
- $p = 1/2$ play H^{comp}_{n+1}

Compression:

- $w^*(H_n^{comp}) \geq \frac{1}{2} + \frac{1}{2} w^*(H_n)$
- $w^*(H_n) < 1 \Rightarrow w^*(H_n^{comp}) < 1$

Recap

We have used Compression to map a family of games $\{G_n\}$ to a single game $G^\#$ so that $w^*(G^\#)=1 \iff w^*(G_n)=1 \ \forall n.$

Using this Supercompression map we immediately get a reduction from nonHalting to deciding $w^*(G)=1$.

And using $MIP^*=RE$ we can improve this to a reduction from Universal Halting.

How to Compress

Answer Reduction

Question Reduction

How to Compress

Answer Reduction

Deligate deciding if the players won to the players and ask them for a short proof that they won instead [Think PCP]

Question Reduction

How to Compress

Answer Reduction

Deligate deciding if the players won to the players and ask them for a short proof that they won instead [Think PCP]

Question Reduction

Ask the players to sample their own questions.

To verify the questions were sampled honestly play a game with appropriate rigidity properties [Think randomness expansion]

How to Compress

Answer Reduction

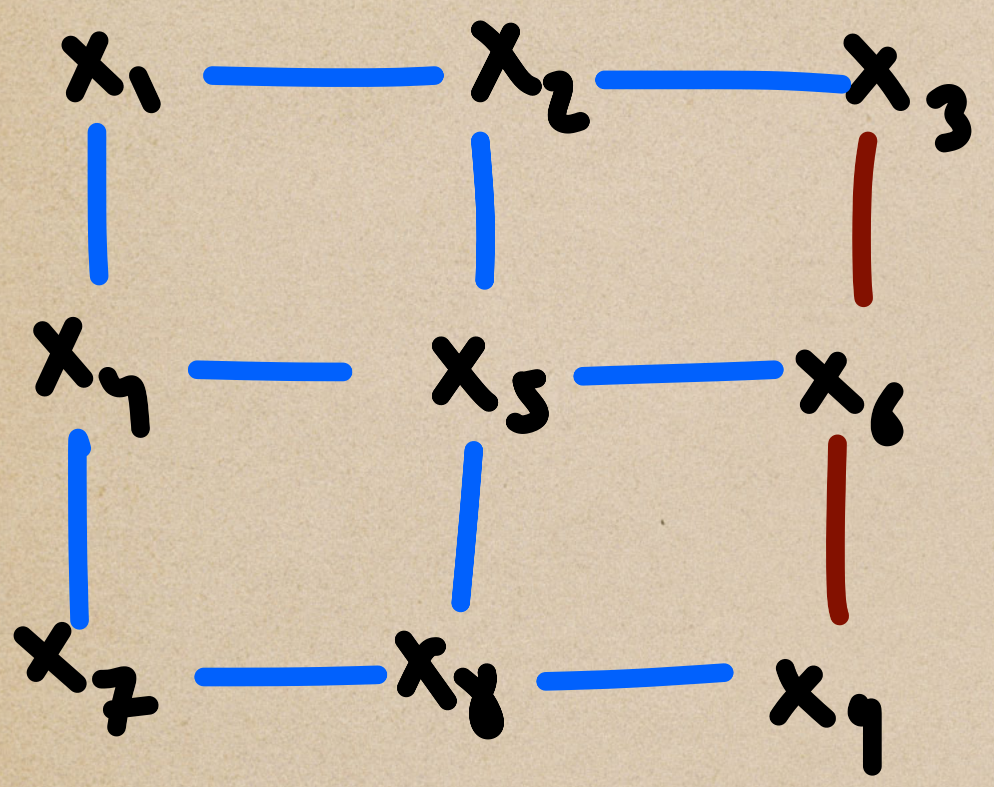
Deligate deciding if the players won to the players and ask them for a short proof that they won instead [Think PCP]

Question Reduction ← Quantum enters

Ask the players to sample their own questions.

To verify the questions were sampled honestly play a game with appropriate rigidity properties [Think randomness expansion]

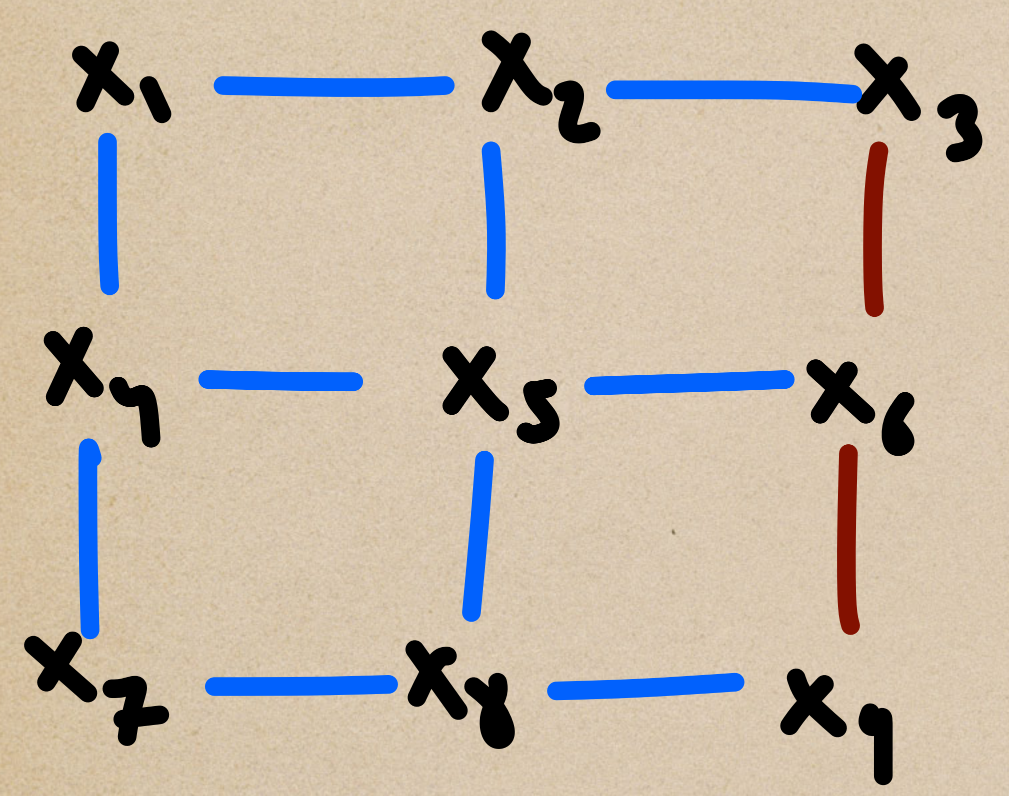
Rigidity



Any quantum strategy wining the MS game must be sharing two EPR entangled states and measuring them in a particular bases.

Generating two uniformly sampled bits.

Rigidity



Any quantum strategy wining the MS game must be sharing two EPR entangled states and measuring them in a particular bases. Generating two uniformly sampled bits.

We want a similar phenomena which is more efficient i.e. bits sampled as questions exponentially smaller than bits forced to be generated as responses.

Thank you