WEIZMANN INSTITUTE OF SCIENCE

Funded by the European Union

European Research Council
Established by the European Commission

Real-Valued Somewhat-Pseudorandom Unitaries

Zvika Brakerski, **Nir Magrafta**

https://arxiv.org/abs/2403.16704

Quantum Pseudorandomness

JLS 2018

Quantum Pseudorandomness

JLS 2018

Pseudo**R**andom **S**tate (PRS)

- A keyed family $\{\varphi_k\}_k$ of states
- Efficiently generatable
- Computationally indistinguishable from Haar random state:

$$\left| \Pr_{k \leftarrow \mathcal{K}} \left[\mathscr{A}\left(\left| \varphi_k \right\rangle^{\otimes m} \right) = 1 \right] - \Pr_{\psi \leftarrow Haar} \left[\mathscr{A}\left(\left| \psi \right\rangle^{\otimes m} \right) = 1 \right] \right| \leq negl$$

Quantum Pseudorandomness

JLS 2018

Pseudo**R**andom **S**tate (PRS)

- A keyed family $\{\varphi_k\}_k$ of states
- Efficiently generatable
- Computationally indistinguishable from Haar random state:

$$\left| \Pr_{k \leftarrow \mathscr{K}} \left[\mathscr{A}\left(\left| \varphi_k \right\rangle^{\otimes m} \right) = 1 \right] - \Pr_{\psi \leftarrow Haar} \left[\mathscr{A}\left(\left| \psi \right\rangle^{\otimes m} \right) = 1 \right] \right| \leq negl$$

Pseudo**R**andom **U**nitary (PRU)

- A keyed family $\{U_k\}_k$ of unitaries
- Efficiently generatable given k
- Computationally indistinguishable from Haar random unitary:

$$\left| \Pr_{k \leftarrow \mathscr{K}} \left[\mathscr{A}^{U_k}\left(1^\kappa \right) = 1 \right] - \Pr_{U \leftarrow Haar} \left[\mathscr{A}^{U}\left(1^\kappa \right) = 1 \right] \right| \leq negl$$

Why Pseudorandom Unitaries?

Why Pseudorandom Unitaries?

- Imply many other quantum cryptographic objects
- Quantum pseudorandomness is weaker than OWF (relative to an oracle) [Kre21, KQST23]

Why Pseudorandom Unitaries?

- Imply many other quantum cryptographic objects
- Quantum pseudorandomness is weaker than OWF (relative to an oracle) [Kre21, KQST23]
- Benchmarking quantum devices
- Quantum supremacy demonstrations
- Efficient estimation of observables

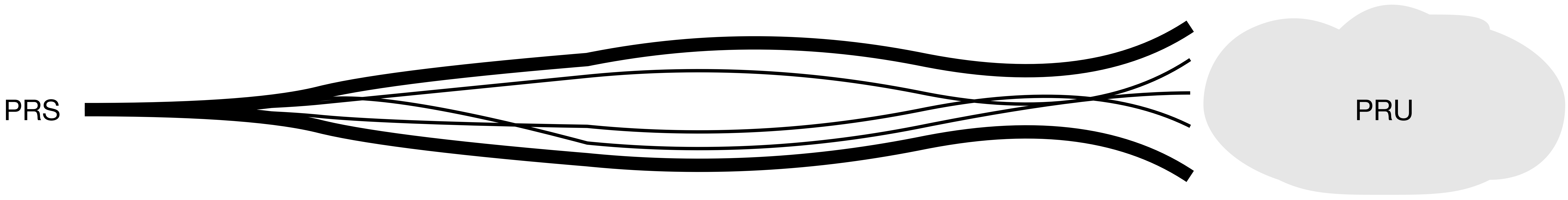
Why Pseudorandom Unitaries?

- Imply many other quantum cryptographic objects
- Quantum pseudorandomness is weaker than OWF (relative to an oracle) [Kre21, KQST23]
- Benchmarking quantum devices
- Quantum supremacy demonstrations
- Efficient estimation of observables
- Quantum learning

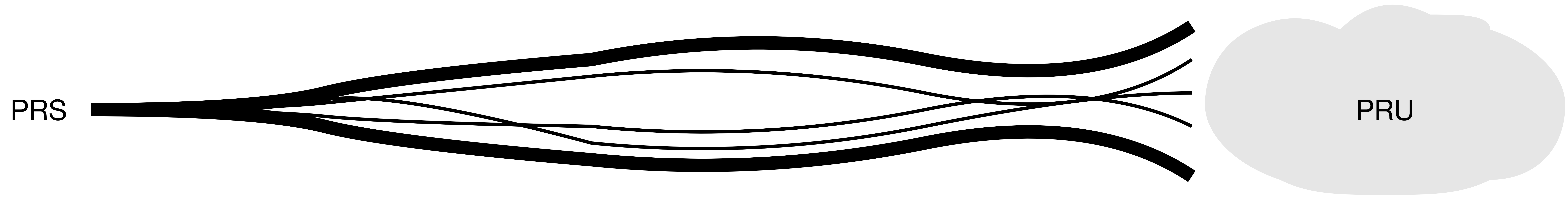
Why Pseudorandom Unitaries?

- Imply many other quantum cryptographic objects
- Quantum pseudorandomness is weaker than OWF (relative to an oracle) [Kre21, KQST23]
- Benchmarking quantum devices
- Quantum supremacy demonstrations
- Efficient estimation of observables
- Quantum learning
- Quantum chaos, quantum gravity

A Plethora of Pseudorandom Objects

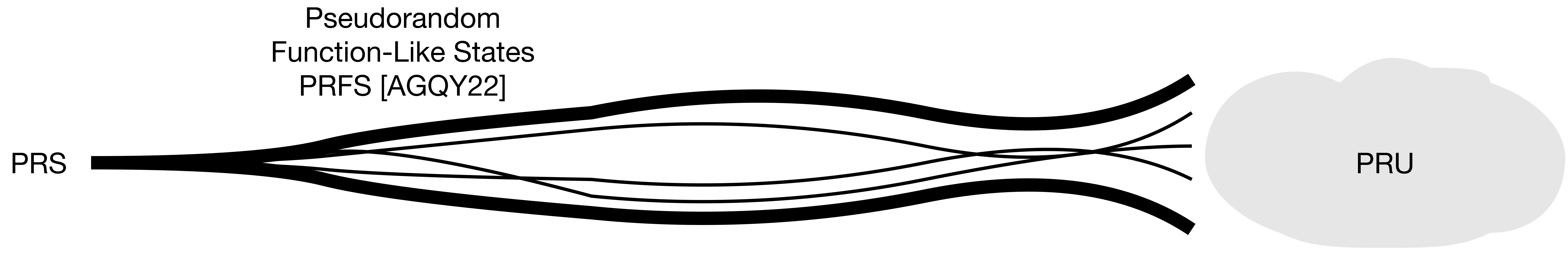


A Plethora of Pseudorandom Objects



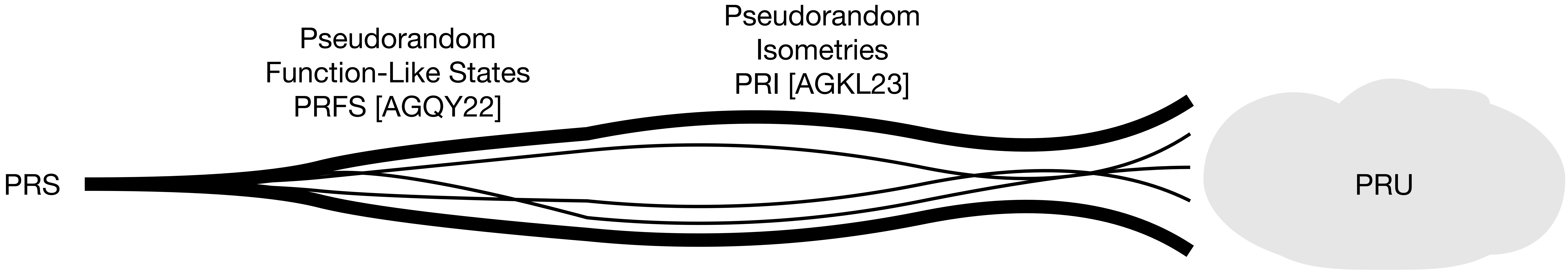
- More complex then states
- Output is harder to model than states
- Variable input

A Plethora of Pseudorandom Objects



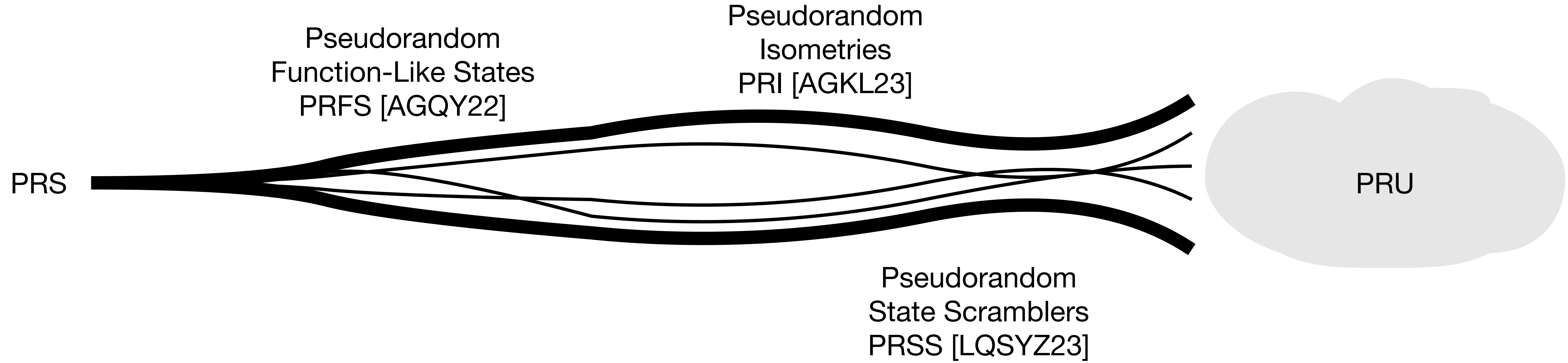
- More complex then states
- Output is harder to model than states
- Variable input

A Plethora of Pseudorandom Objects



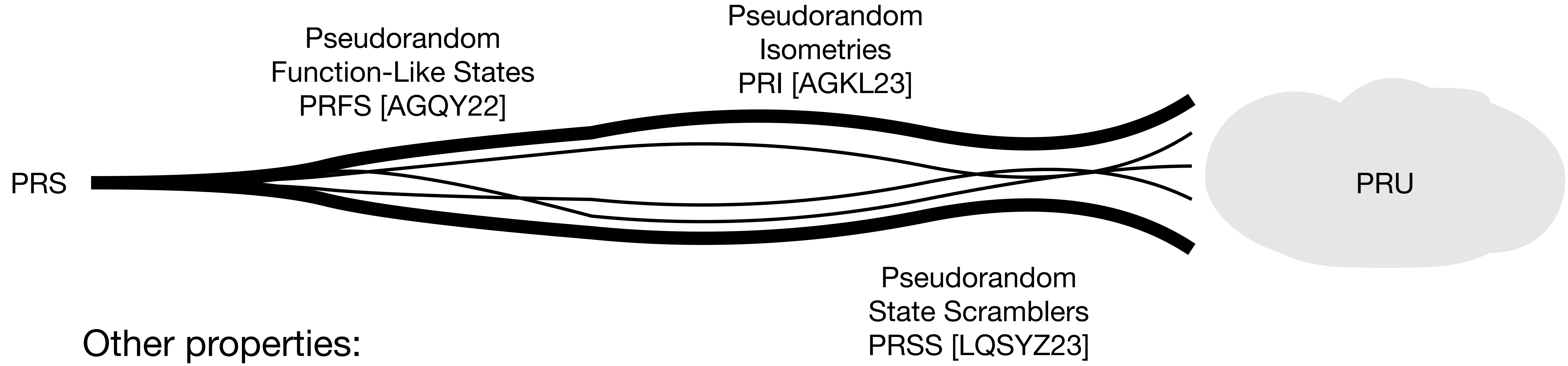
- More complex then states
- Output is harder to model than states
- Variable input

A Plethora of Pseudorandom Objects



- More complex then states
- Output is harder to model than states
- Variable input

A Plethora of Pseudorandom Objects



Other properties:

- Binary ± phase [BS19], Subset PRS [GB23, JMW23]
- Scalable PRS [BS20]
- PRS with pseudo-entanglement [ABFGVZZ22]

Our results:
Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary

Our results:
Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary

Efficient Generation

Our results:
Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary

Efficient Generation

$\forall k \in \{0,1\}^{\kappa(n)}$, U_k is an efficiently generatable QPT algorithm implementing a unitary on n qubits.

Our results:
Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary

Efficient Generation

$\forall k \in \{0,1\}^{\kappa(n)}$, U_k is an efficiently generatable QPT algorithm implementing a unitary on n qubits.

Indistinguishability

Our results:
Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary

Efficient Generation

$\forall k \in \{0,1\}^{\kappa(n)}$, U_k is an efficiently generatable QPT algorithm implementing a unitary on n qubits.

Indistinguishability

Let $s(n), t(n)$ be polynomials in the number of qubits n, and let $\left\{ \left|\psi^1\right\rangle, \ldots, \left|\psi^s\right\rangle \right\}$ be orthogonal states.

Our results:
Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary

Efficient Generation

$\forall k \in \{0,1\}^{\kappa(n)}$, U_k is an efficiently generatable QPT algorithm implementing a unitary on n qubits.

Indistinguishability

Let $s(n), t(n)$ be polynomials in the number of qubits n, and let $\left\{ \left|\psi^1\right\rangle, \ldots, \left|\psi^s\right\rangle \right\}$ be orthogonal states.

Then any n.u. QPT distinguisher $\mathscr{A}$ that makes a query of the form $\rho_{in} = \bigotimes_{j\in[s]} \left(\left|\psi^j\right\rangle\left\langle\psi^j\right| \right)^{\otimes t}$

to the st-tensor of the unitary, it holds that:

Our results:
Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary

Efficient Generation

$\forall k \in \{0,1\}^{\kappa(n)}$, U_k is an efficiently generatable QPT algorithm implementing a unitary on n qubits.

Indistinguishability

Let $s(n), t(n)$ be polynomials in the number of qubits n, and let $\left\{ \left|\psi^1\right\rangle, \ldots, \left|\psi^s\right\rangle \right\}$ be orthogonal states.

Then any n.u. QPT distinguisher $\mathscr{A}$ that makes a query of the form $\rho_{in} = \bigotimes_{j\in[s]} \left(\left|\psi^j\right\rangle\left\langle\psi^j\right| \right)^{\otimes t}$

to the st-tensor of the unitary, it holds that:

$$\left| \Pr_{k\leftarrow\{0,1\}^\kappa} \left[\mathscr{A}\left((U_k^{\otimes st})\rho_{in}(U_k^{\dagger\otimes st}) \right) = 1\right] - \Pr_{U\leftarrow Haar_n} \left[\mathscr{A}\left((U^{\otimes st})\rho_{in}(U^{\dagger\otimes st}) \right) = 1\right] \right| \leq negl(n)$$

Our results:
Non-Adaptive Orthogonal-Inputs Pseudorandom Unitary

Efficient Generation

$\forall k \in \{0,1\}^{\kappa(n)}$, U_k is an efficiently generatable QPT algorithm implementing a unitary on n qubits.

Indistinguishability

Let $s(n), t(n)$ be polynomials in the number of qubits n, and let $\left\{ \left|\psi^1\right\rangle, \ldots, \left|\psi^s\right\rangle \right\}$ be orthogonal states.

Then any n.u. QPT distinguisher $\mathscr{A}$ that makes a query of the form $\rho_{in} = \bigotimes_{j\in[s]} \left(\left|\psi^j\right\rangle\left\langle\psi^j\right| \right)^{\otimes t}$

to the st-tensor of the unitary, it holds that:

$$\left| \Pr_{k\leftarrow\{0,1\}^\kappa}\left[\mathscr{A}\left((U_k^{\otimes st})\rho_{in}(U_k^{\dagger^{\otimes st}})\right) = 1\right] - \Pr_{U\leftarrow Haar_n}\left[\mathscr{A}\left((U^{\otimes st})\rho_{in}(U^{\dagger^{\otimes st}})\right) = 1\right] \right| \leq negl(n)$$

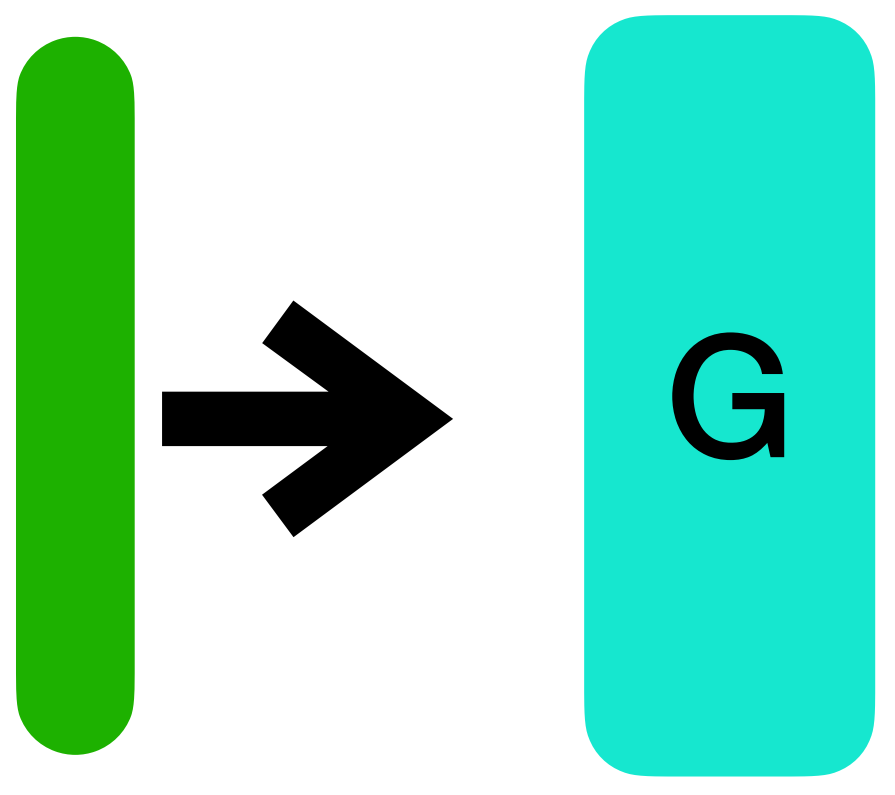
We construct a family of **real valued** unitaries $\{U_k\}_k$ which satisfy this definition

Intuition for the construction

Intuition for the construction

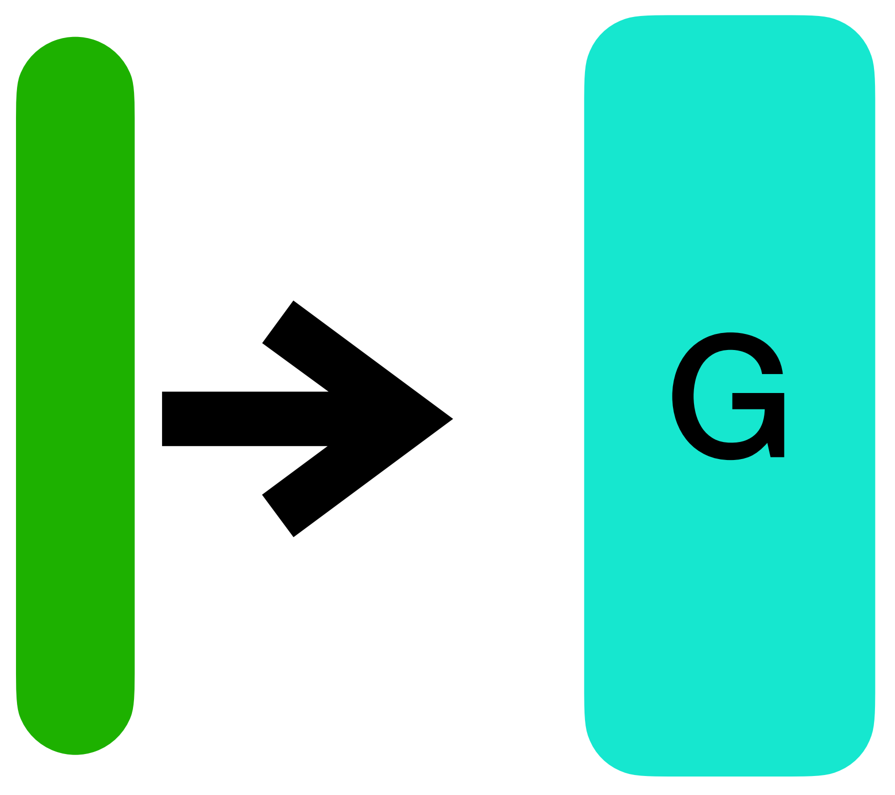
Intuition for the construction

- Randomize the phase



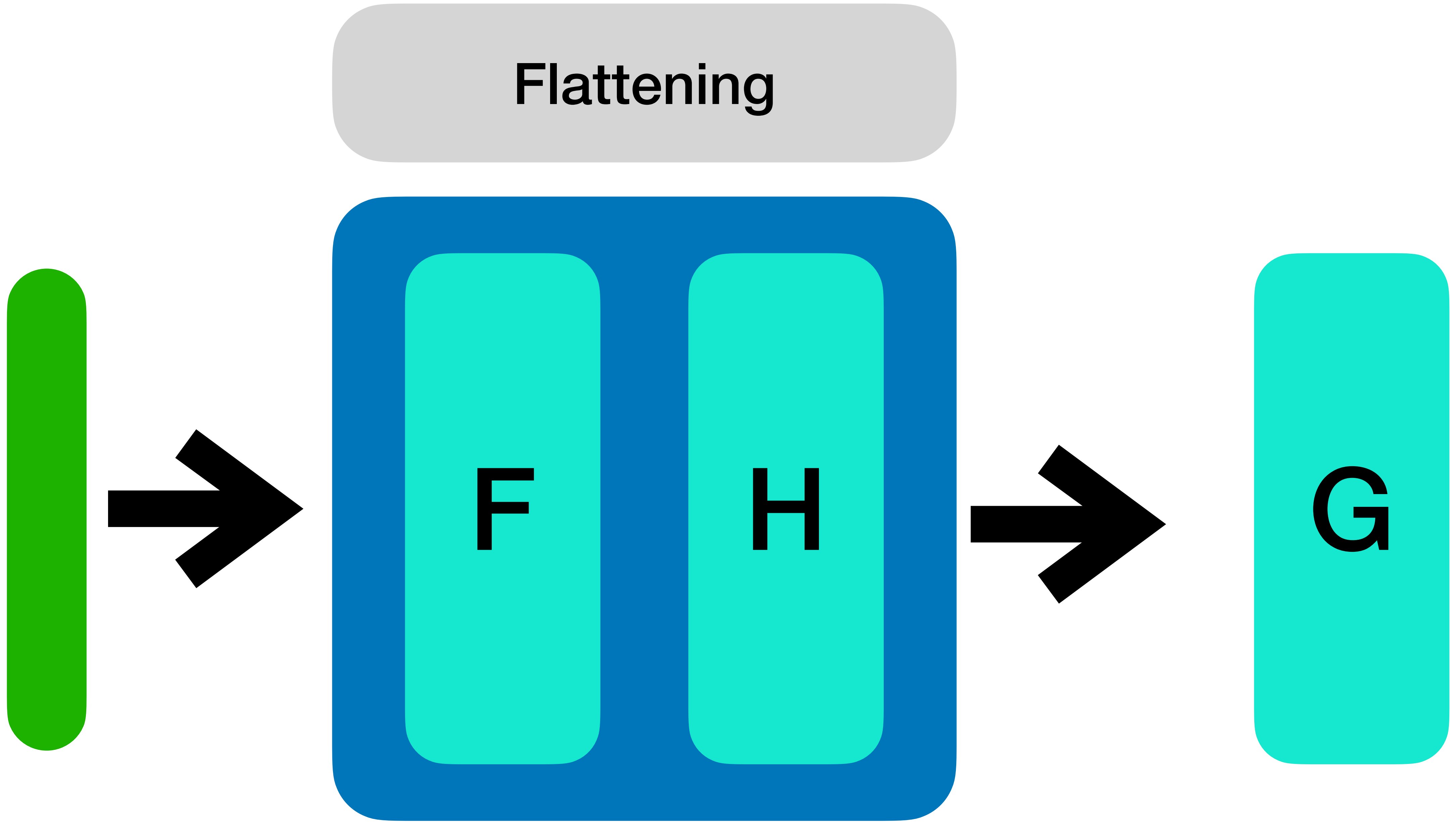
Intuition for the construction

- Randomize the phase
- Control over amplitudes?



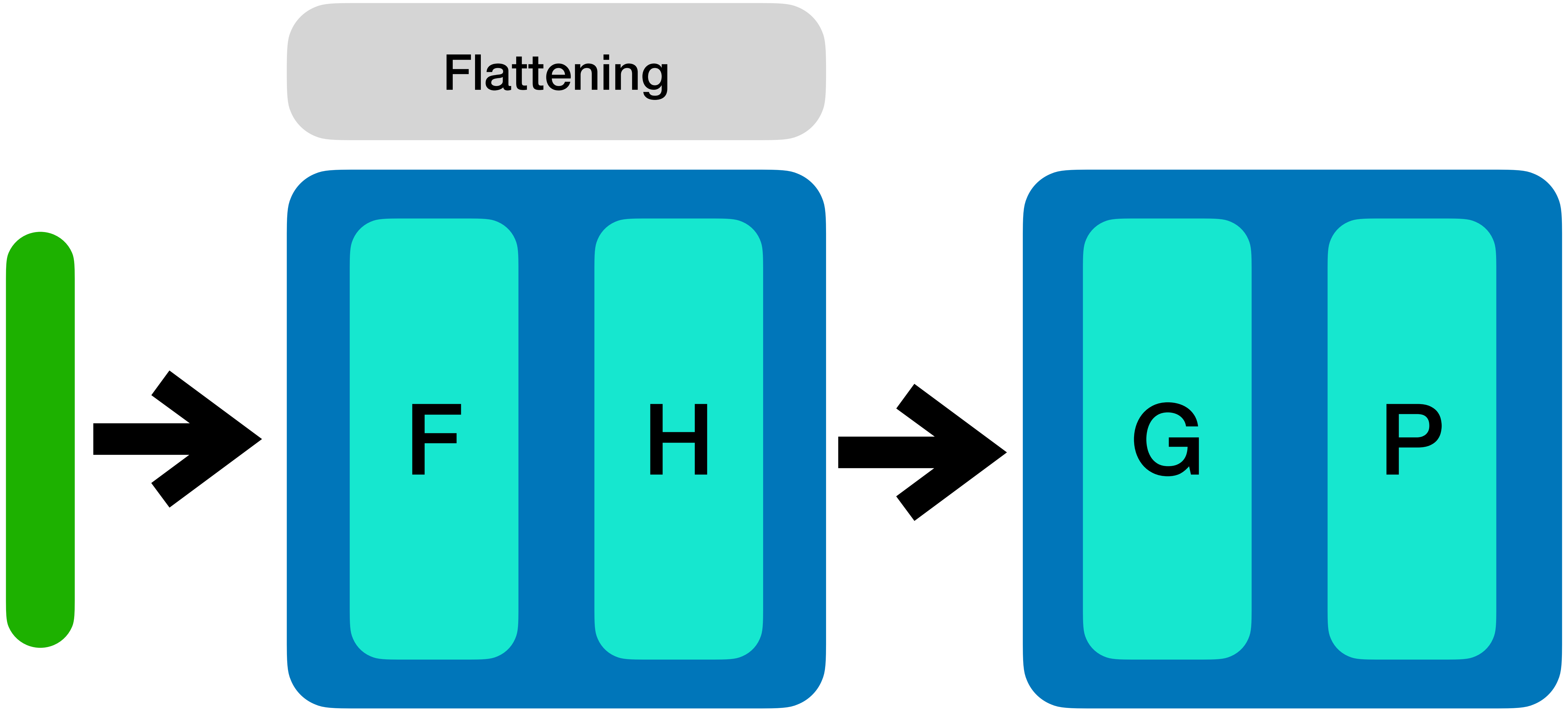
Intuition for the construction

- Randomize the phase
- Control over amplitudes?
  - Get a flat state (no one amplitude is too large)



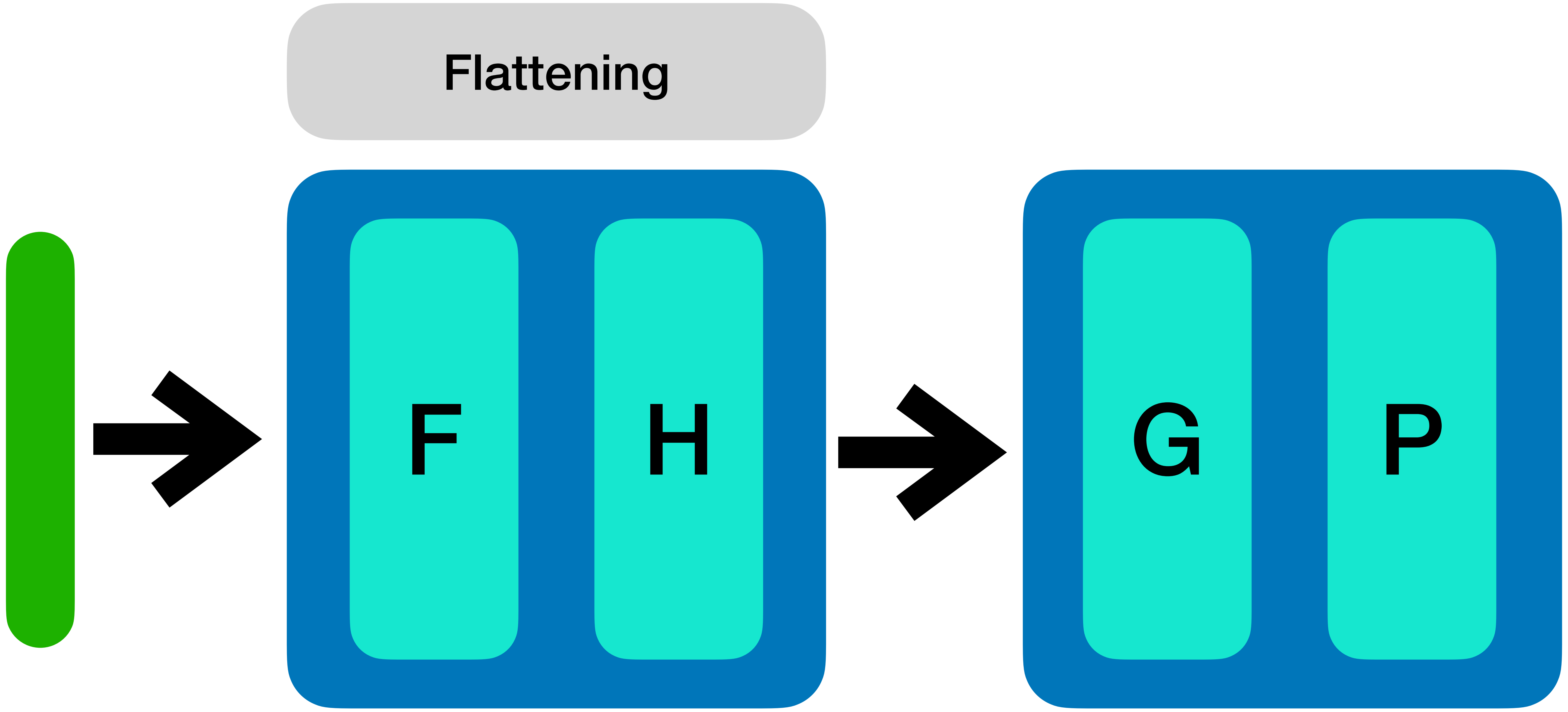
Intuition for the construction

- Randomize the phase
- Control over amplitudes?
    - Get a flat state (no one amplitude is too large)
    - Symmetrize the amplitude



Intuition for the construction

- Randomize the phase
- Control over amplitudes?
  - Get a flat state (no one amplitude is too large)
  - Symmetrize the amplitude
- Flatness follows from concentration bounds



Proof Overview

Proof Overview

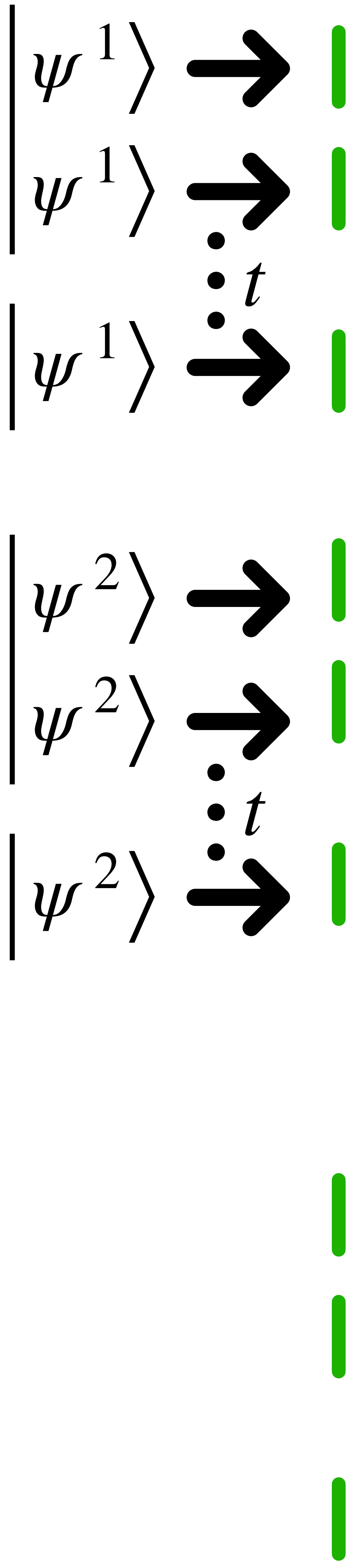
$$\rho_{in} = \bigotimes_{j \in [s]} \left(\left| \psi^j \right\rangle \left\langle \psi^j \right| \right)^{\otimes t}$$

Proof Overview

$$\rho_{in} = \bigotimes_{j \in [s]} \left(\left| \psi^j \right\rangle \left\langle \psi^j \right| \right)^{\otimes t}$$

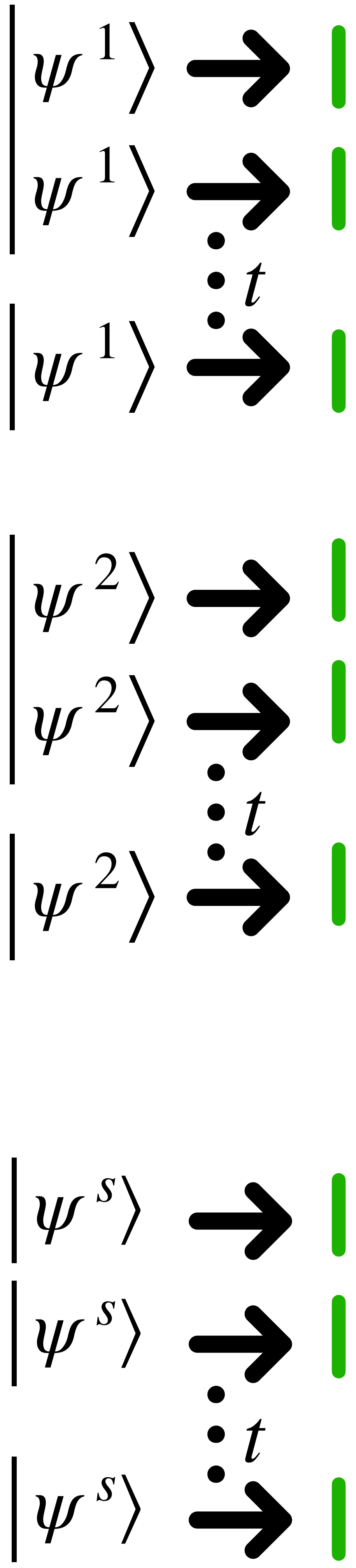
Proof Overview

$$\rho_{in} = \bigotimes_{j\in[s]} \left(\left| \psi^j \right\rangle \left\langle \psi^j \right| \right)^{\otimes t}$$



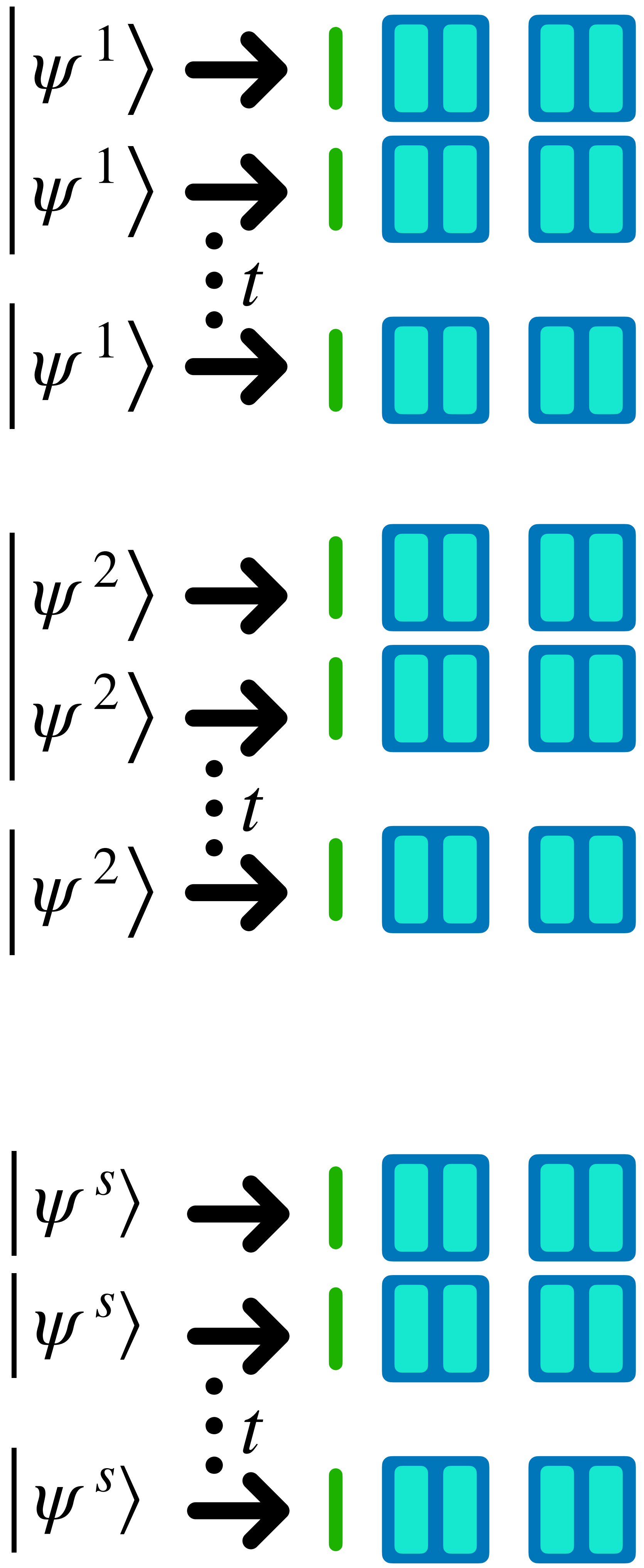
Proof Overview

$$\rho_{in} = \bigotimes_{j \in [s]} \left(\left| \psi^j \right\rangle \left\langle \psi^j \right| \right)^{\otimes t}$$



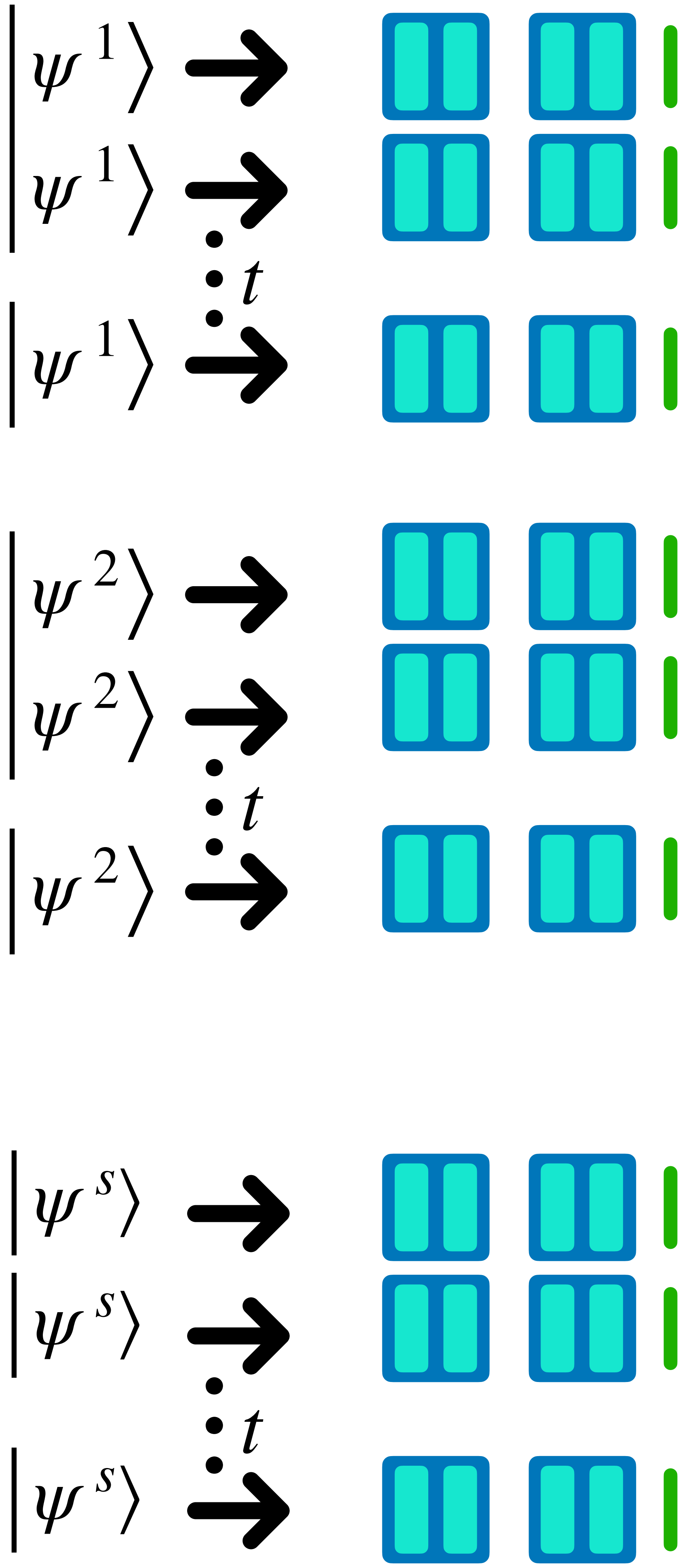
Proof Overview

$$\rho_{in} = \bigotimes_{j\in[s]} \left(|\psi^j\rangle \langle\psi^j| \right)^{\otimes t}$$



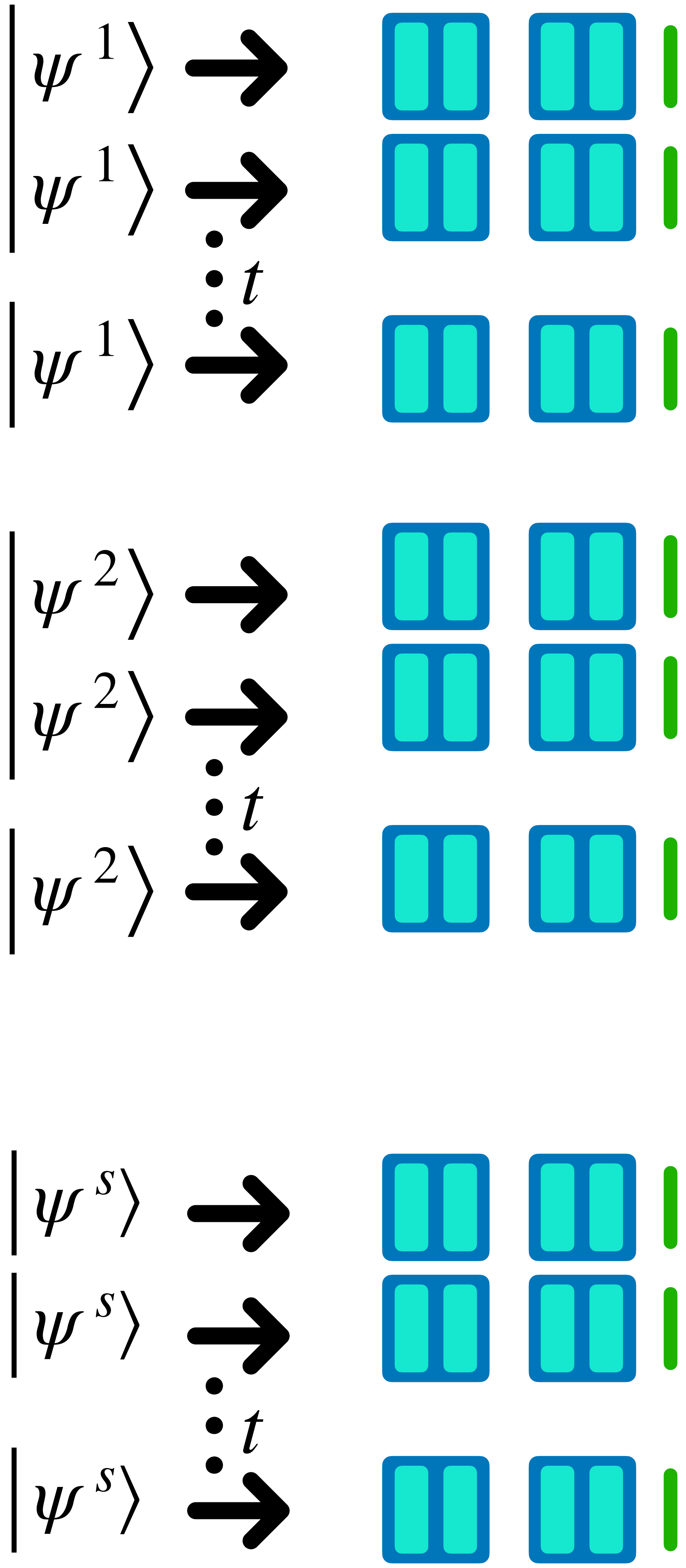
Proof Overview

$$\rho_{in} = \bigotimes_{j \in [s]} \left(\left| \psi^j \right\rangle \left\langle \psi^j \right| \right)^{\otimes t}$$



Proof Overview

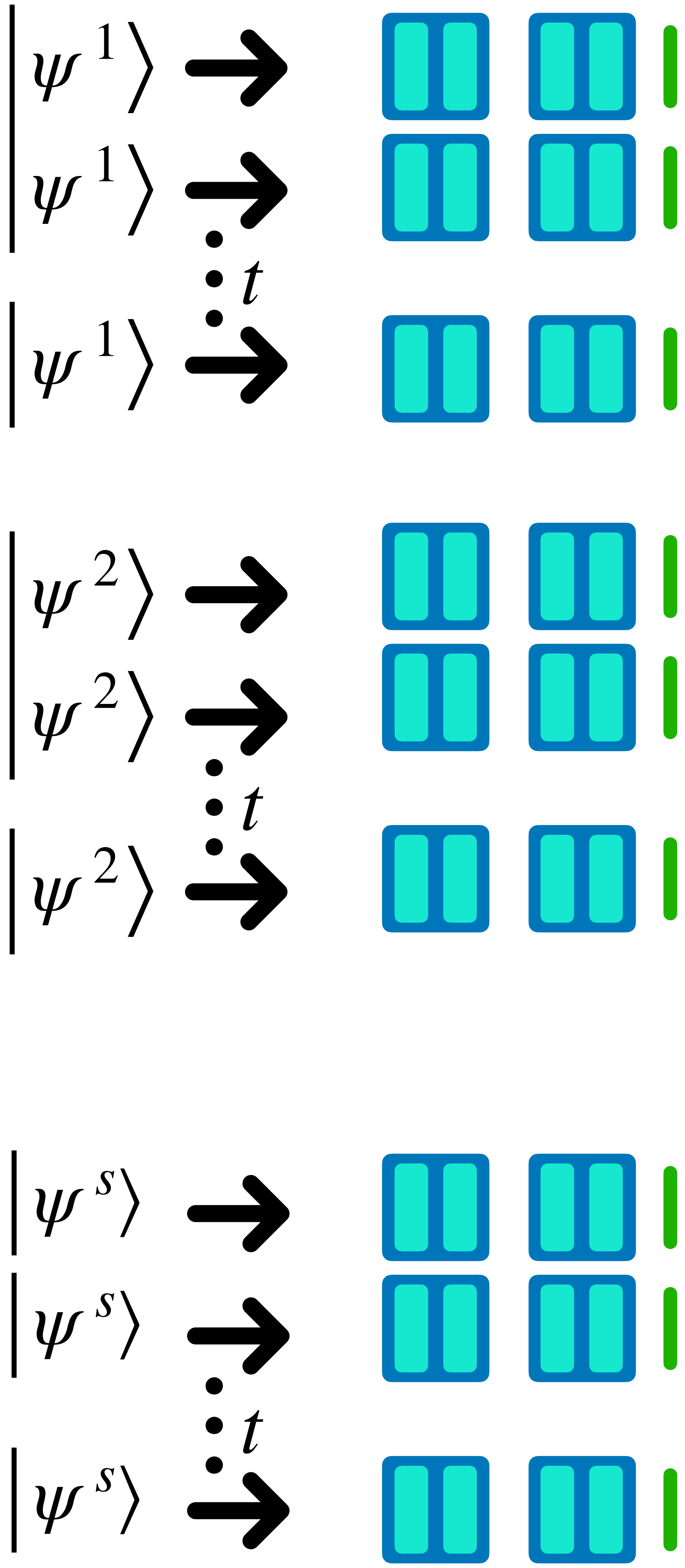
$$\rho_{in} = \bigotimes_{j\in[s]} \left(\left|\psi^j\right\rangle \left\langle \psi^j \right| \right)^{\otimes t}$$



$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s} \left|\vec{z}\right\rangle \left\langle \sigma(\vec{z}) \right|$$

Proof Overview

$$\rho_{in} = \bigotimes_{j \in [s]} \left(|\psi^j\rangle \langle \psi^j| \right)^{\otimes t}$$

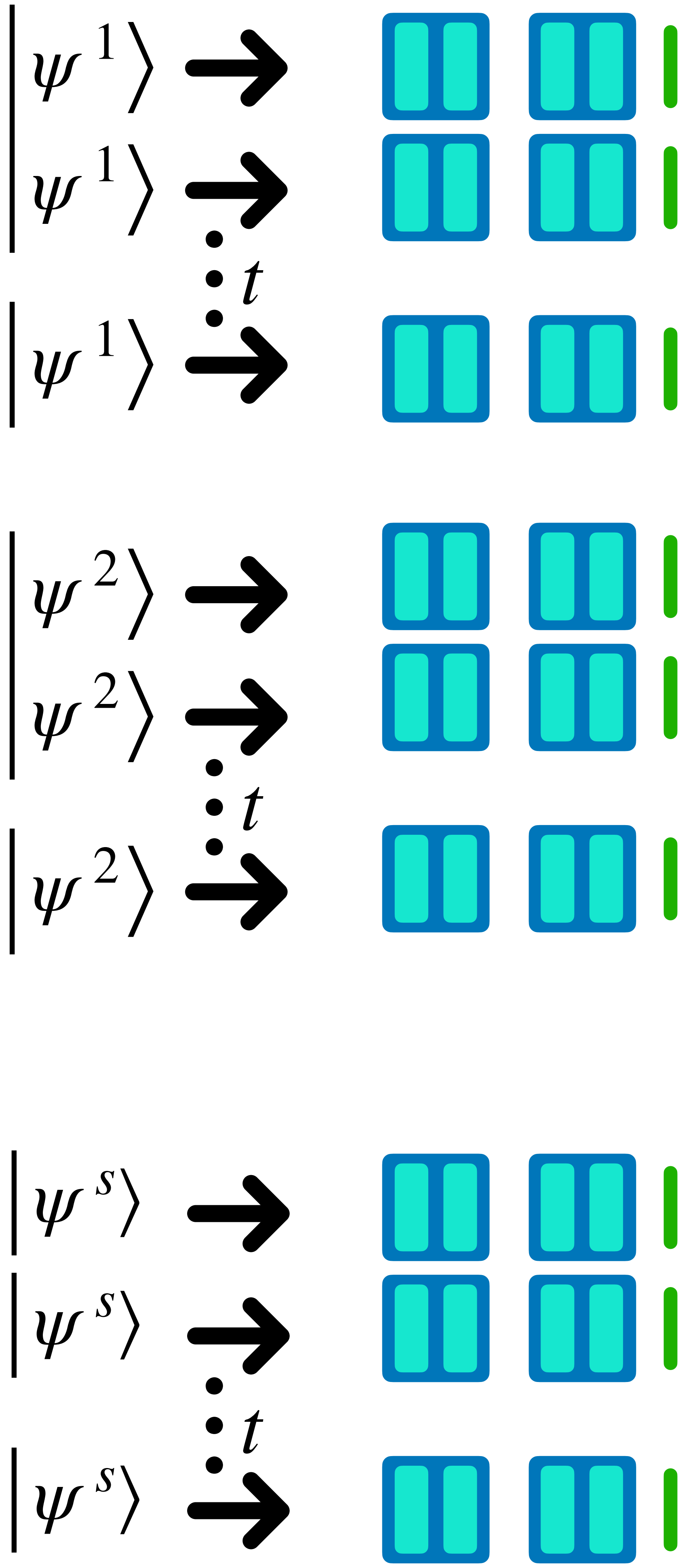


$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z} \in U_{st}\ ,\ \sigma \in S_t^s} |\vec{z}\rangle \langle \sigma(\vec{z})|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \in \{0,1\}^n \ \mathit{for}\ i \neq j$$

Proof Overview

$$\rho_{in} = \bigotimes_{j \in [s]} \left(\left| \psi^j \right\rangle \left\langle \psi^j \right| \right)^{\otimes t}$$

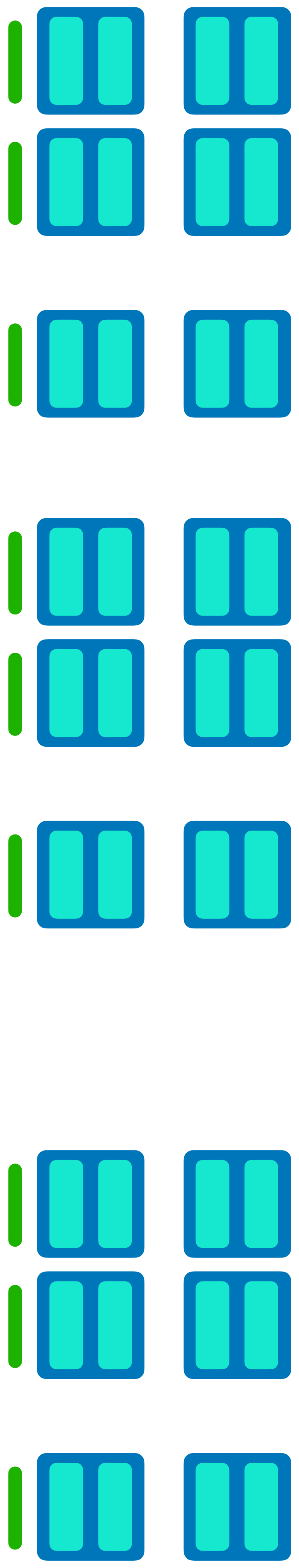


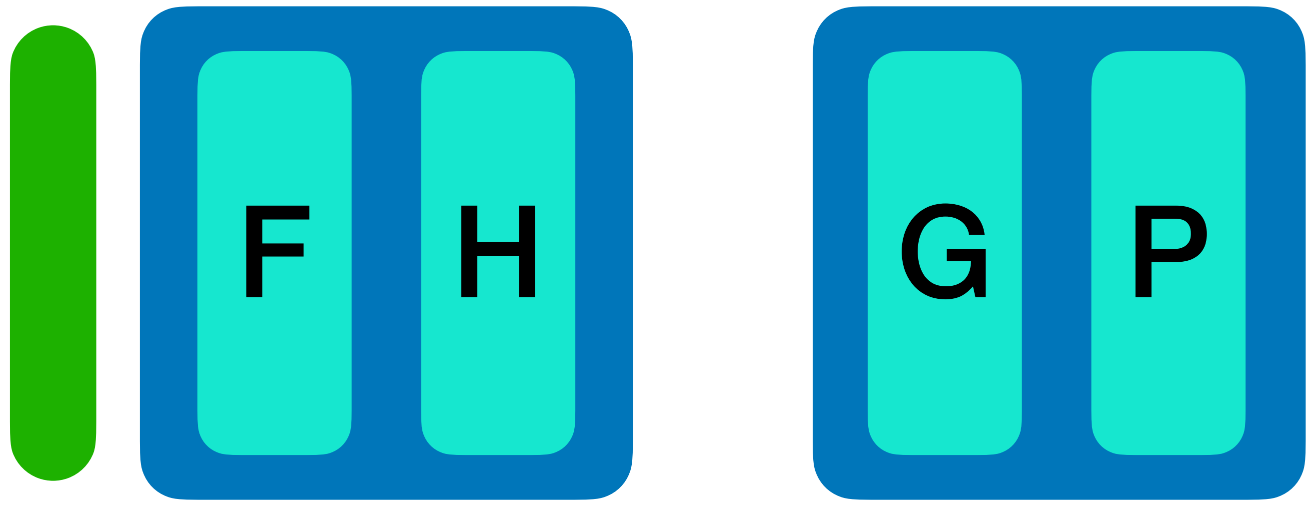
$$\approx \frac{(N - st)!}{N!} \sum_{\vec{z} \in U_{st}\ ,\ \sigma \in S_t^s} \left| \vec{z} \right\rangle \left\langle \sigma(\vec{z}) \right|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \in \{0,1\}^n \ \ for\ i \neq j$$

$$S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$

Proof Overview



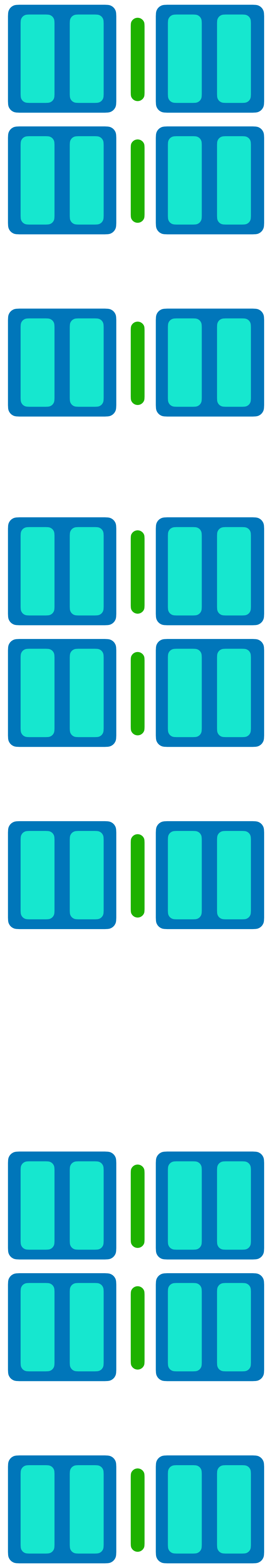


$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z} \in U_{st}\ ,\ \sigma \in S_t^s} \left| \vec{z} \right\rangle \left\langle \sigma(\vec{z}) \right|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$

Proof Overview

1. F, H: Get flat vectors

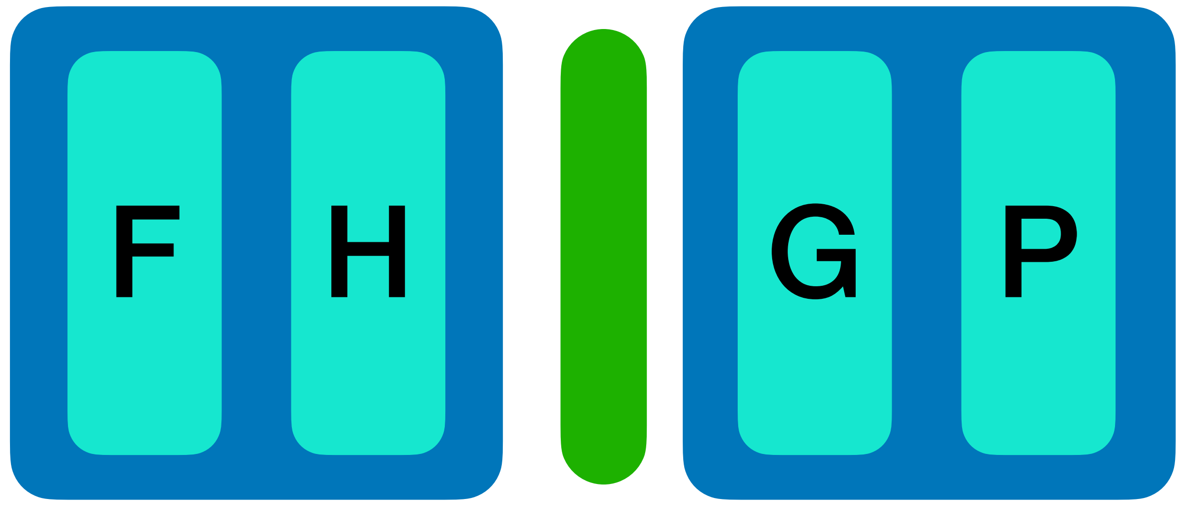


$$\alpha_{\vec{z},\vec{z}'} \left| \vec{z} \right\rangle \left\langle \vec{z}' \right|$$

$$\vec{z}, \overrightarrow{z'} \in (\{0,1\}^n)^{st}$$

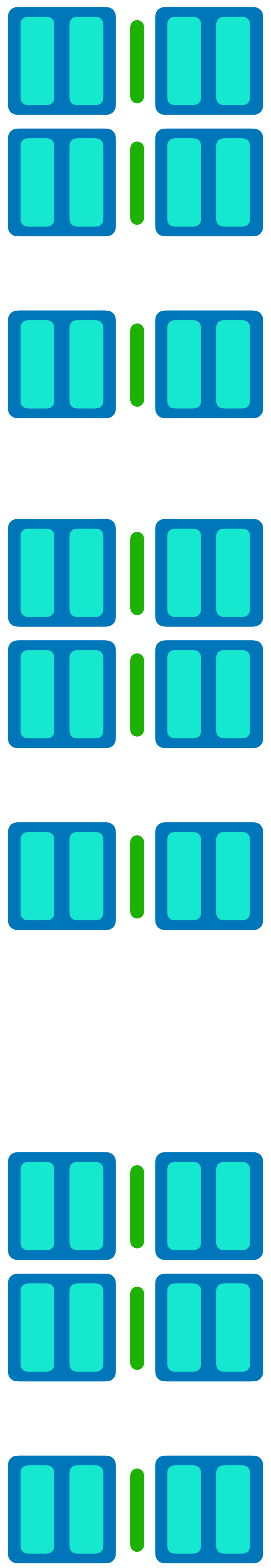
$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z} \in U_{st}\ ,\ \sigma \in S_t^s} \left| \vec{z} \right\rangle \left\langle \sigma(\vec{z}) \right|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$



Proof Overview

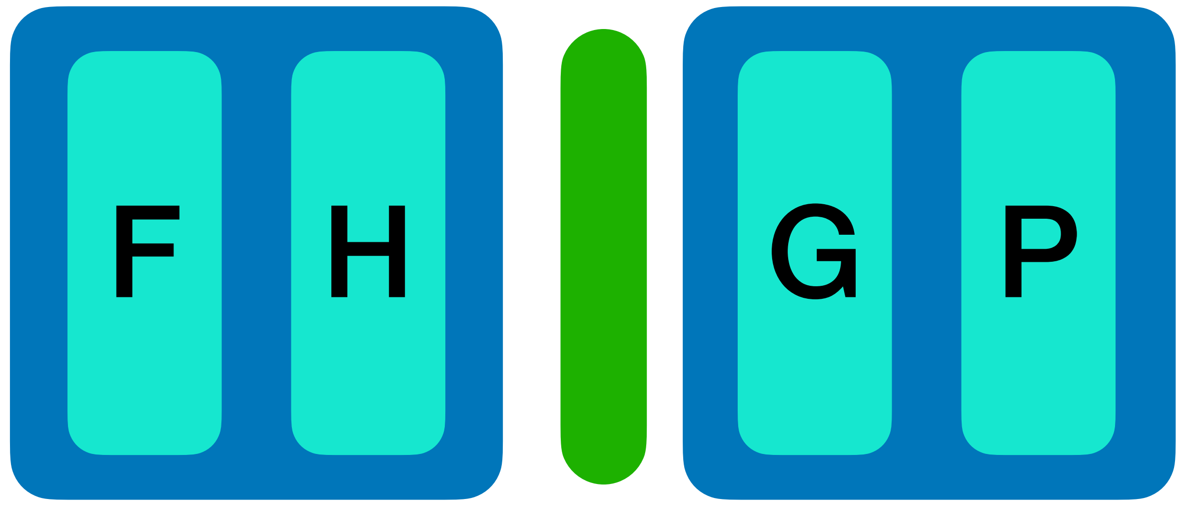
1. F, H: Get flat vectors
2. $\approx$ Unique entries



$\alpha_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$

$\vec{z}, \vec{z'} \in U_{st}$

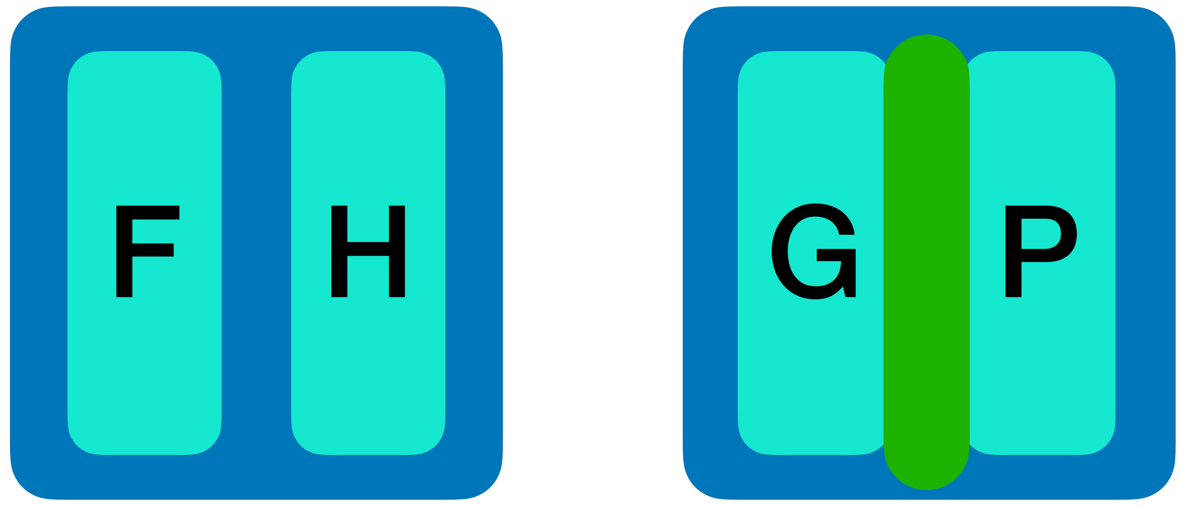
$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s} \left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$$

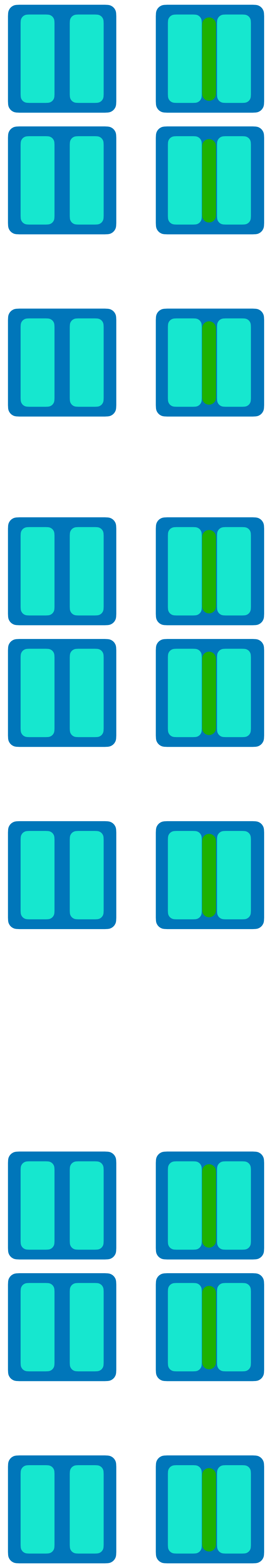


$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$

Proof Overview

1. F, H: Get flat vectors
2. $\approx$ Unique entries
3. G: Remove $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ for $\vec{z}, \vec{z}'$ with different entry histogram





$\alpha_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ $\qquad \vec{z}, \overrightarrow{z'} \in U_{st}$

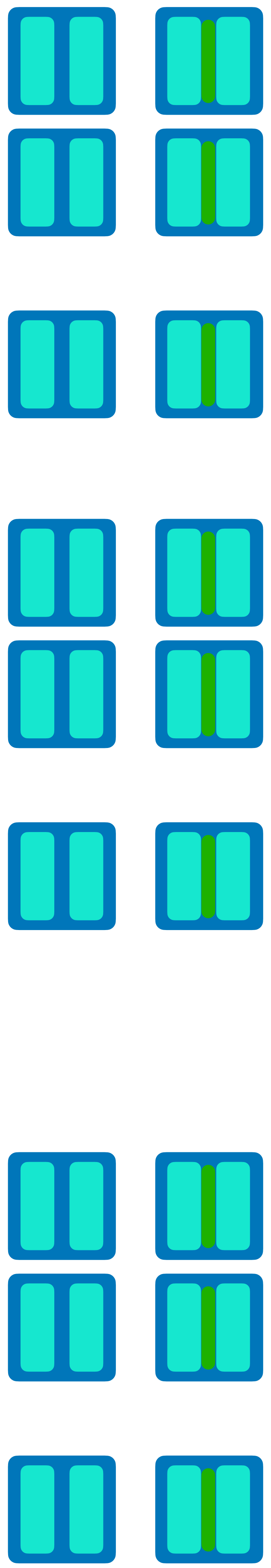
$\alpha_{\vec{z},\vec{z}'} \cdot (-1)^{g(z_1)+\cdots+g(z_{st})+g(z'_1)+\cdots+g(z'_{st})}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$

$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s} \left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$

Proof Overview

1. F, H: Get flat vectors
2. $\approx$ Unique entries
3. G: Remove $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ for $\vec{z}, \vec{z}'$ with different entry histogram



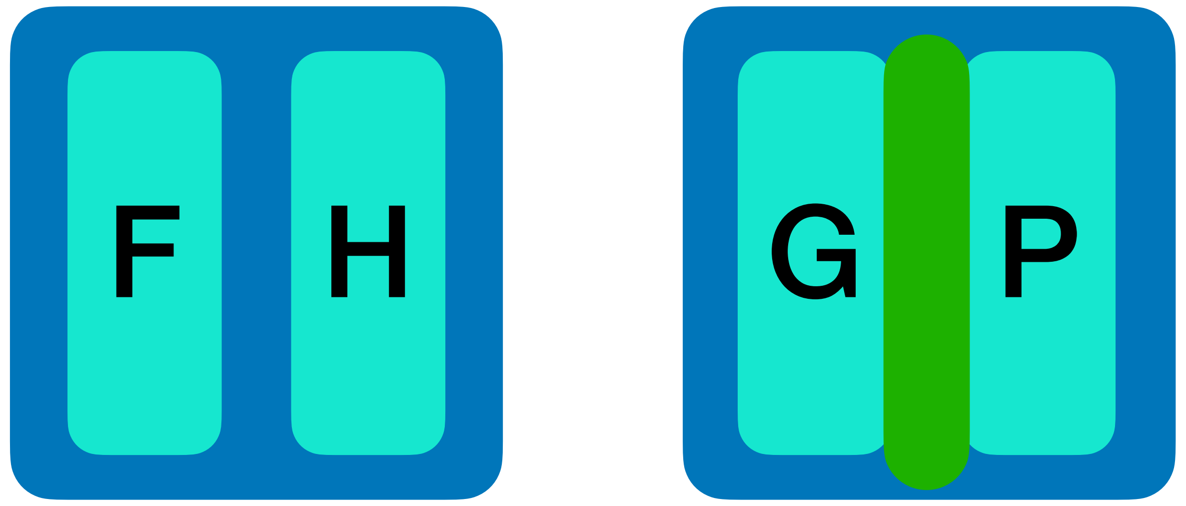
$$\alpha_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right| \qquad \vec{z}, \vec{z'} \in U_{st}$$

$$\alpha_{\vec{z},\vec{z}'} \cdot (-1)^{g(z_1)+\cdots+g(z_{st})+g(z_1')+\cdots+g(z_{st}')}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$$

$$\alpha_{\vec{z},\sigma}\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right| \qquad \sigma \in S_{st}$$

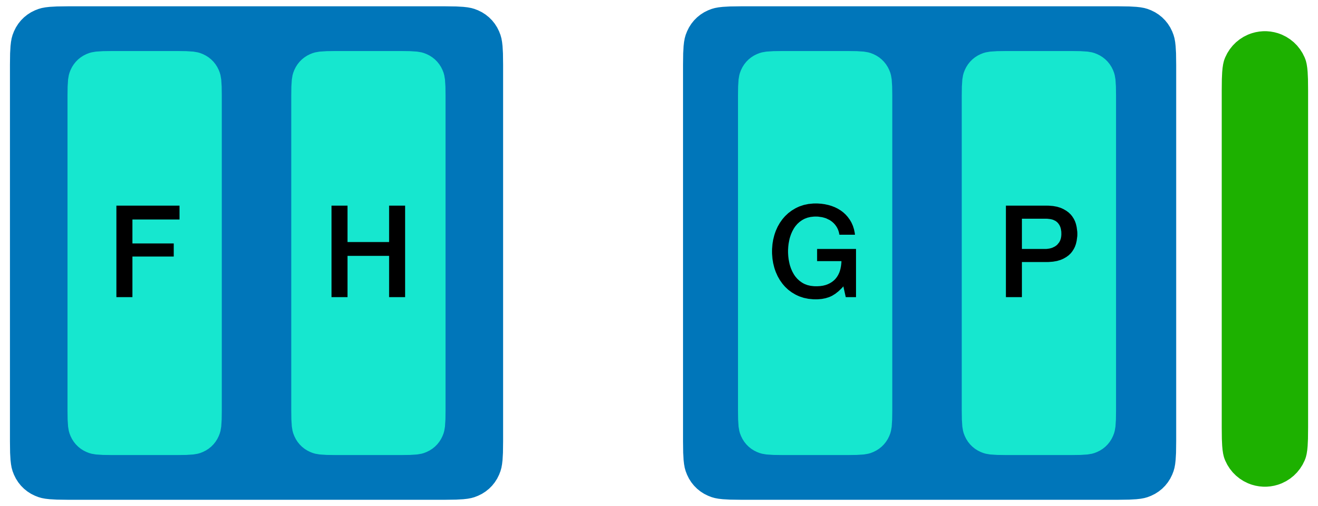
$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s} \left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$$

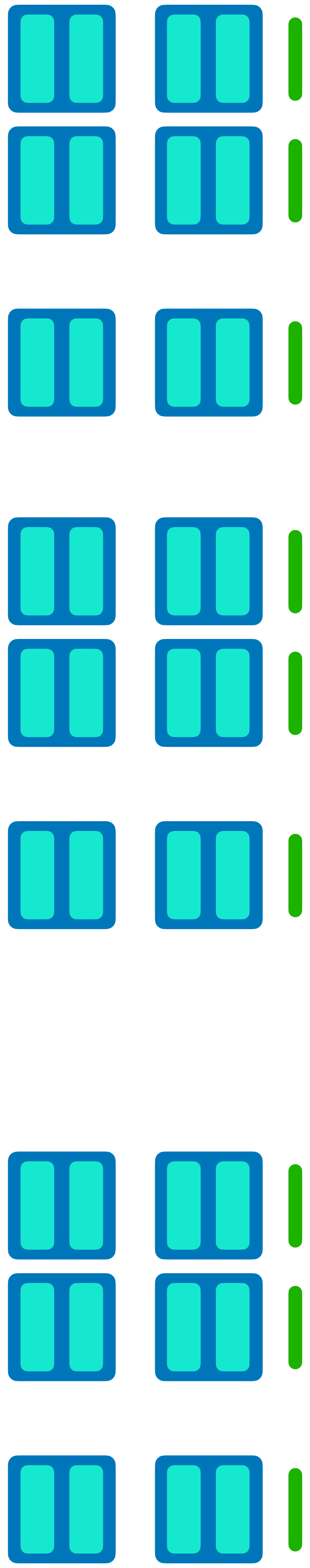
$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$



Proof Overview

1. F, H: Get flat vectors
2. $\approx$ Unique entries
3. G: Remove $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ for $\vec{z}, \vec{z}'$ with different entry histogram
4. P: symmetrizes $\vec{z}$s





$\alpha_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ $\qquad \vec{z}, \overrightarrow{z'} \in U_{st}$

$\alpha_{\vec{z},\vec{z}'} \cdot (-1)^{g(z_1)+\cdots+g(z_{st})+g(z'_1)+\cdots+g(z'_{st})}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$

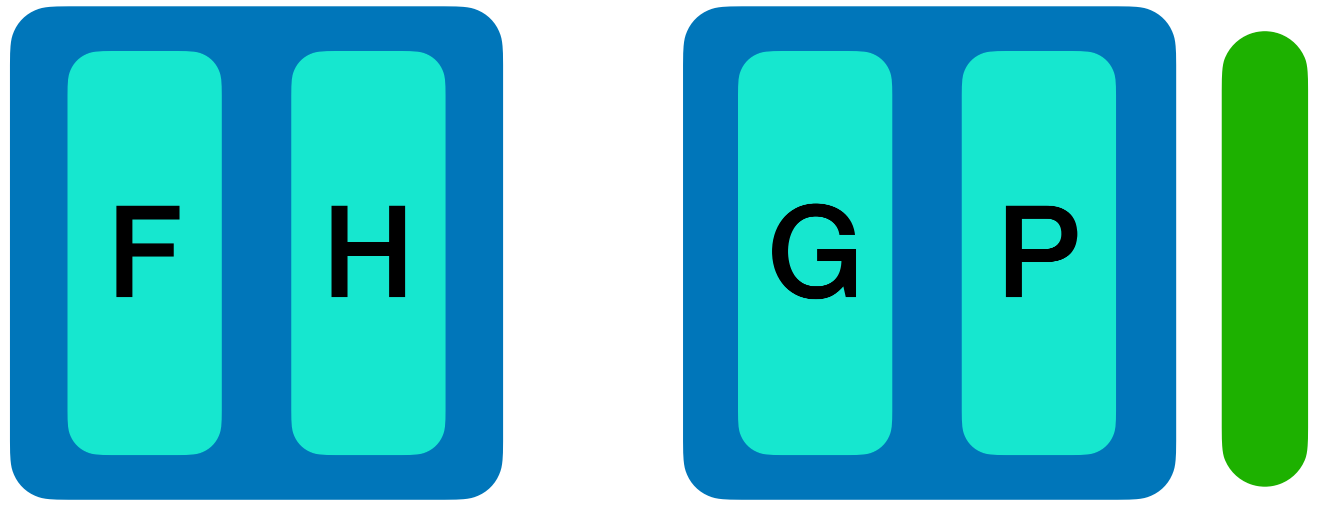
$\alpha_{\vec{z},\sigma}\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$ $\qquad \sigma \in S_{st}$

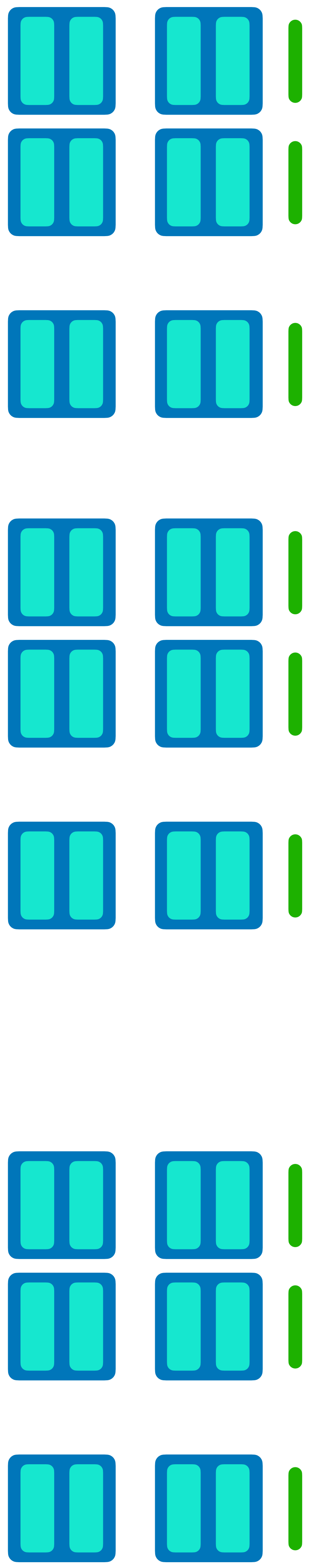
$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s} \left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$

Proof Overview

1. F, H: Get flat vectors
2. $\approx$ Unique entries
3. G: Remove $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ for $\vec{z}, \vec{z}'$ with different entry histogram
4. P: symmetrizes $\vec{z}$s





$\alpha_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ $\qquad \vec{z}, \overrightarrow{z'} \in U_{st}$

$\alpha_{\vec{z},\vec{z}'} \cdot (-1)^{g(z_1)+\cdots+g(z_{st})+g(z_1')+\cdots+g(z_{st}')}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$

$\alpha_{\vec{z},\sigma}\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$ $\qquad \sigma \in S_{st}$

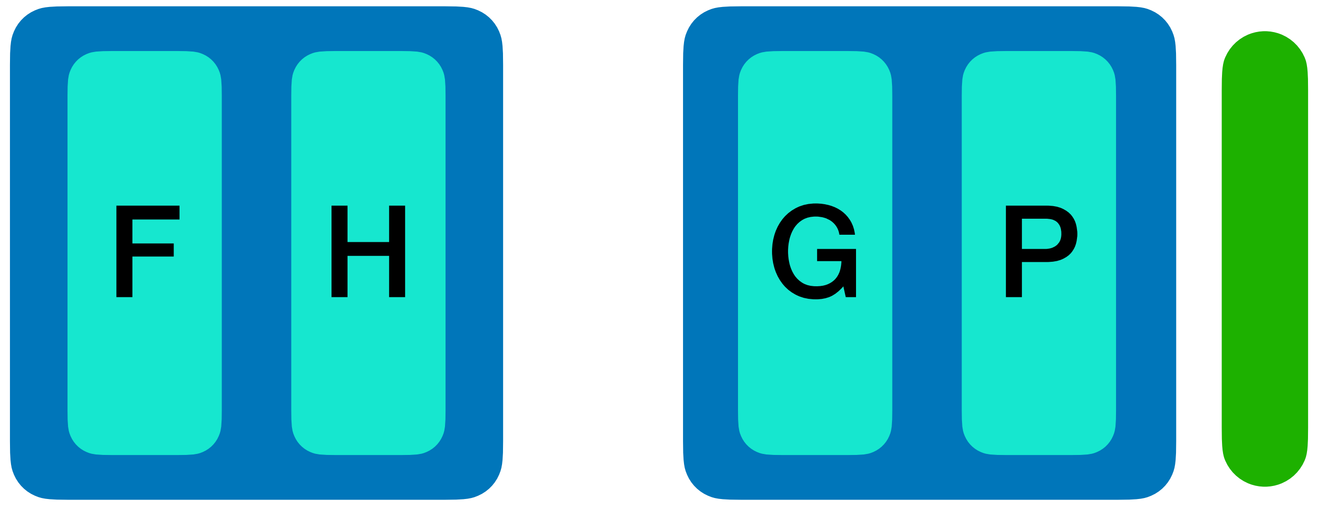
$\nu_\sigma\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$

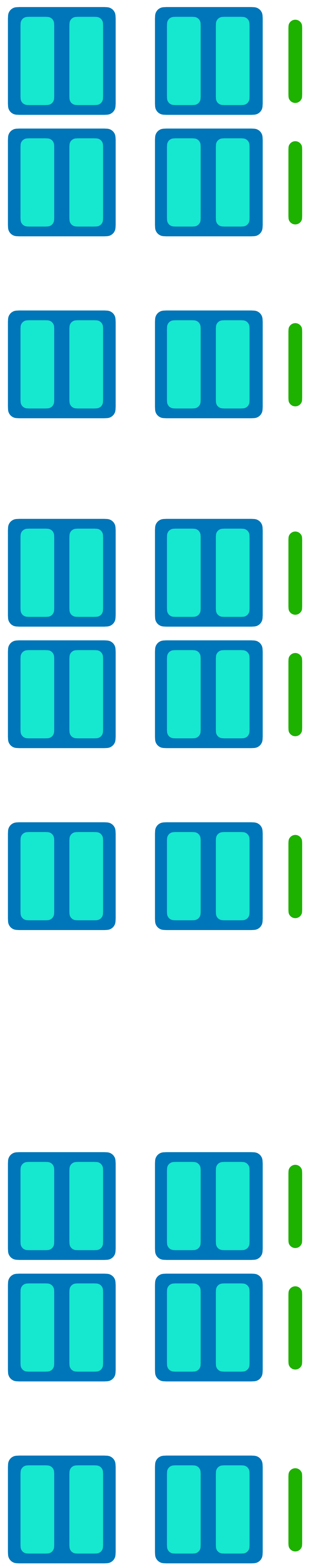
$$\approx \frac{(N-st)!}{N!}\sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s}\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$

Proof Overview

1. F, H: Get flat vectors
2. $\approx$ Unique entries
3. G: Remove $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ for $\vec{z}, \vec{z}'$ with different entry histogram
4. P: symmetrizes $\vec{z}$s





$\alpha_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ $\qquad \vec{z}, \overrightarrow{z'} \in U_{st}$

$\alpha_{\vec{z},\vec{z}'} \cdot (-1)^{g(z_1)+\cdots+g(z_{st})+g(z'_1)+\cdots+g(z'_{st})}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$

$\alpha_{\vec{z},\sigma}\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$ $\qquad \sigma \in S_{st}$

$\nu_\sigma\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$

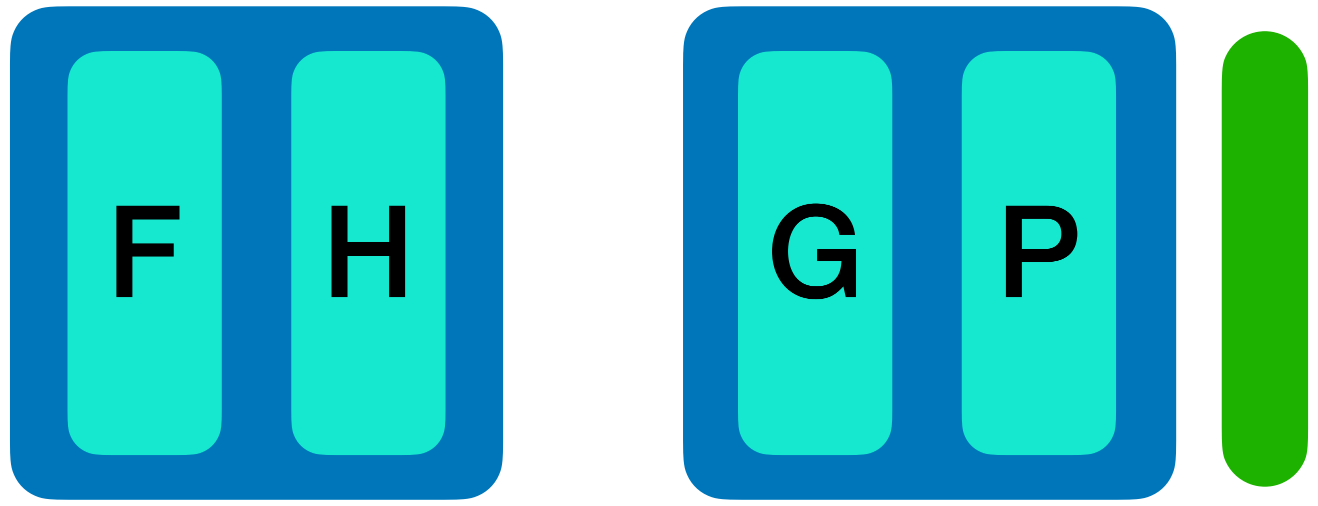
$\nu_\sigma \approx 0,\ \sigma \notin S_t^s$

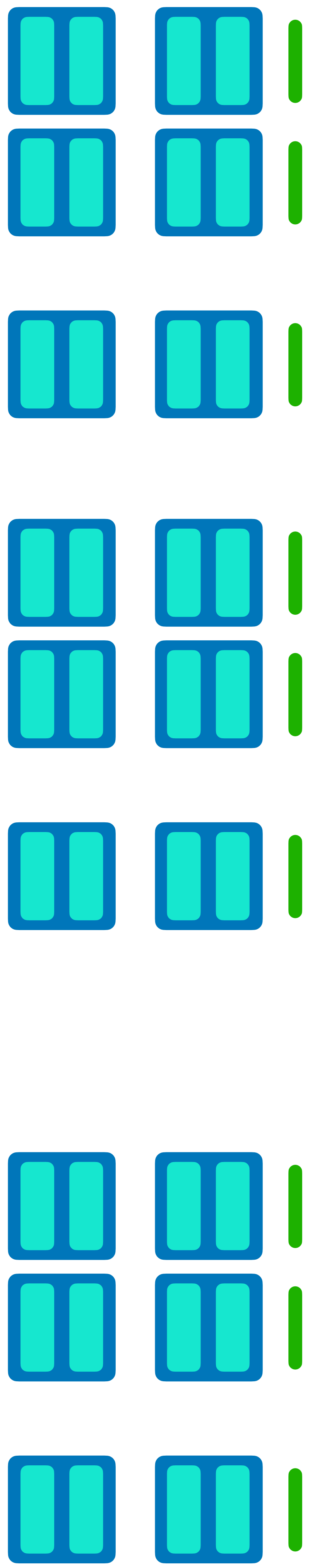
$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s} \left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j\ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$

Proof Overview

1. F, H: Get flat vectors
2. $\approx$ Unique entries
3. G: Remove $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ for $\vec{z}, \vec{z}'$ with different entry histogram
4. P: symmetrizes $\vec{z}$s





$\alpha_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ $\quad \vec{z}, \vec{z'} \in U_{st}$

$\alpha_{\vec{z},\vec{z}'} \cdot (-1)^{g(z_1)+\cdots+g(z_{st})+g(z_1')+\cdots+g(z_{st}')}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$

$\alpha_{\vec{z},\sigma}\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$ $\quad \sigma \in S_{st}$

$\nu_\sigma\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$

$\nu_\sigma \approx 0,\ \sigma \notin S_t^s$

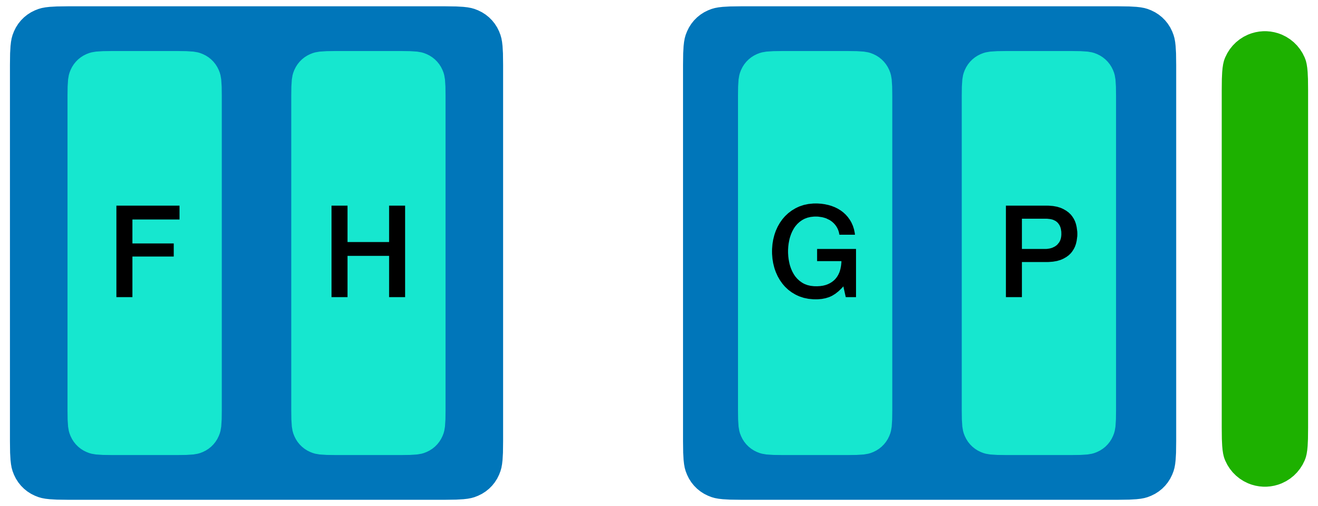
Follows from the inner product of two orthogonal vectors being zero.

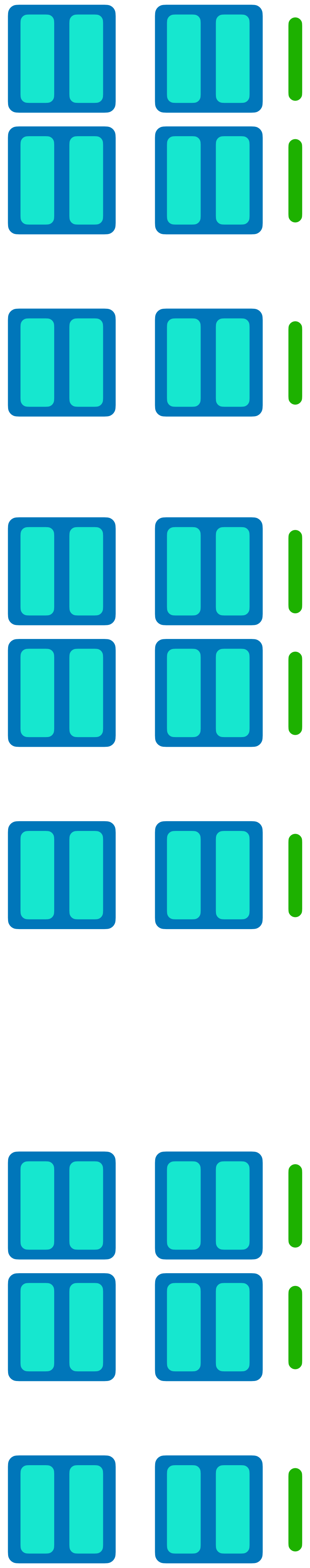
$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s} \left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$$

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$$

Proof Overview

1. F, H: Get flat vectors
2. $\approx$ Unique entries
3. G: Remove $\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ for $\vec{z}, \vec{z}'$ with different entry histogram
4. P: symmetrizes $\vec{z}$s





$\alpha_{\vec{z},\vec{z}'}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$ $\qquad \vec{z}, \vec{z}' \in U_{st}$

$\alpha_{\vec{z},\vec{z}'} \cdot (-1)^{g(z_1)+\cdots+g(z_{st})+g(z_1')+\cdots+g(z_{st}')}\left|\vec{z}\right\rangle\left\langle\vec{z}'\right|$

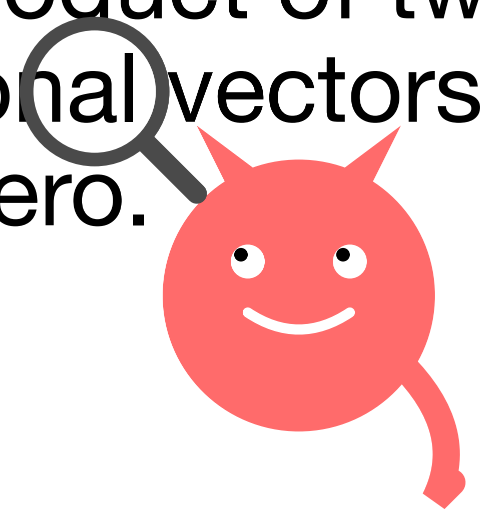
$\alpha_{\vec{z},\sigma}\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$ $\qquad \sigma \in S_{st}$

$\nu_\sigma\left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$

$\nu_\sigma \approx 0,\ \sigma \notin S_t^s$

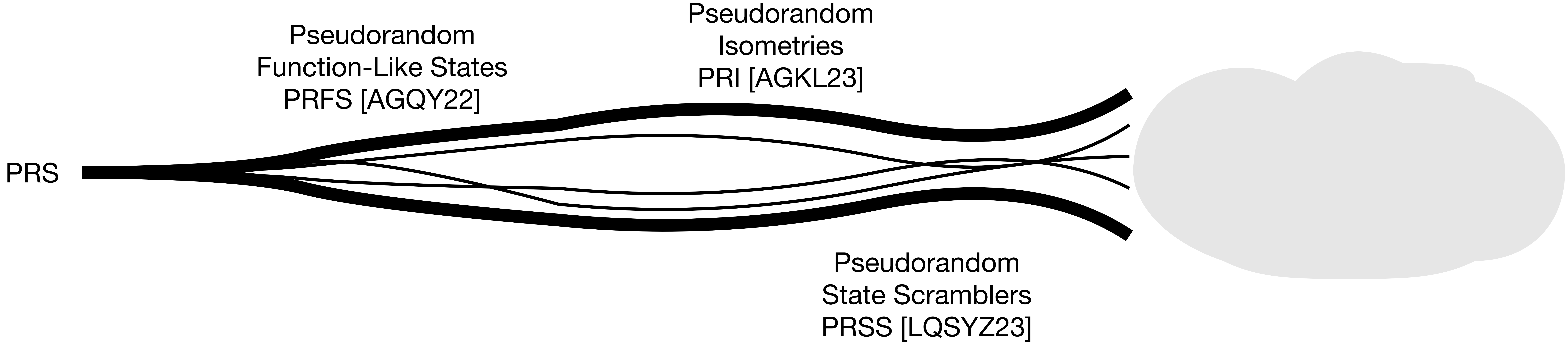
Follows from the inner product of two orthogonal vectors being zero.

$$\approx \frac{(N-st)!}{N!} \sum_{\vec{z}\in U_{st}\ ,\ \sigma\in S_t^s} \left|\vec{z}\right\rangle\left\langle\sigma(\vec{z})\right|$$

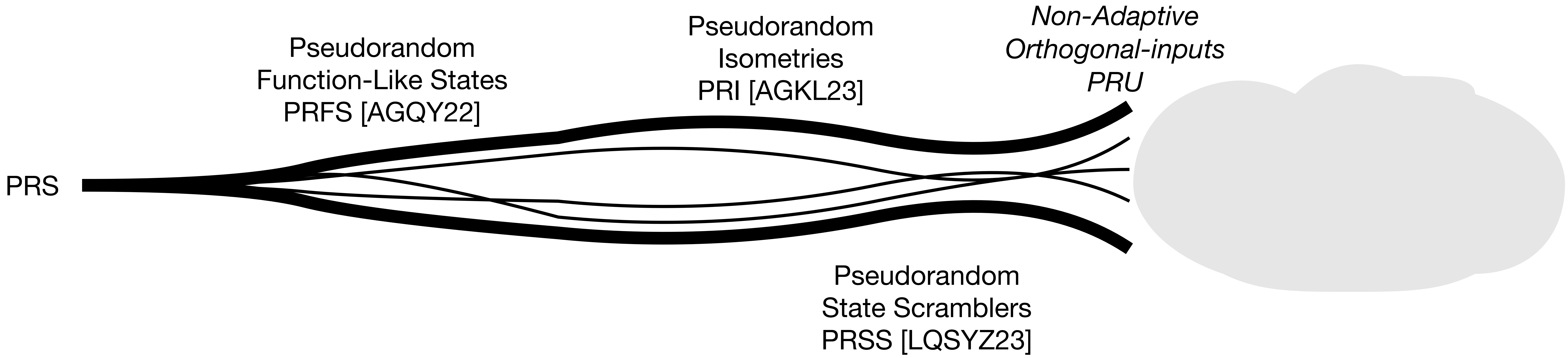


$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{st} \end{bmatrix}, z_i \neq z_j \ for\ i \neq j \qquad S_t^s = \underbrace{S_t \times \cdots \times S_t}_{s\ times}$

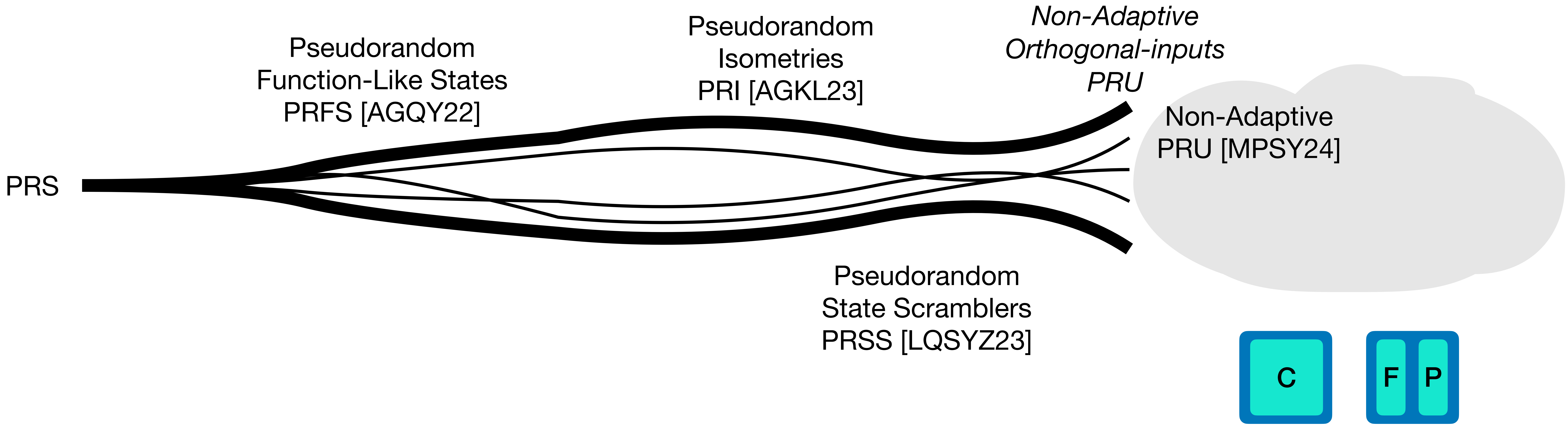
A Plethora of Pseudorandom Objects



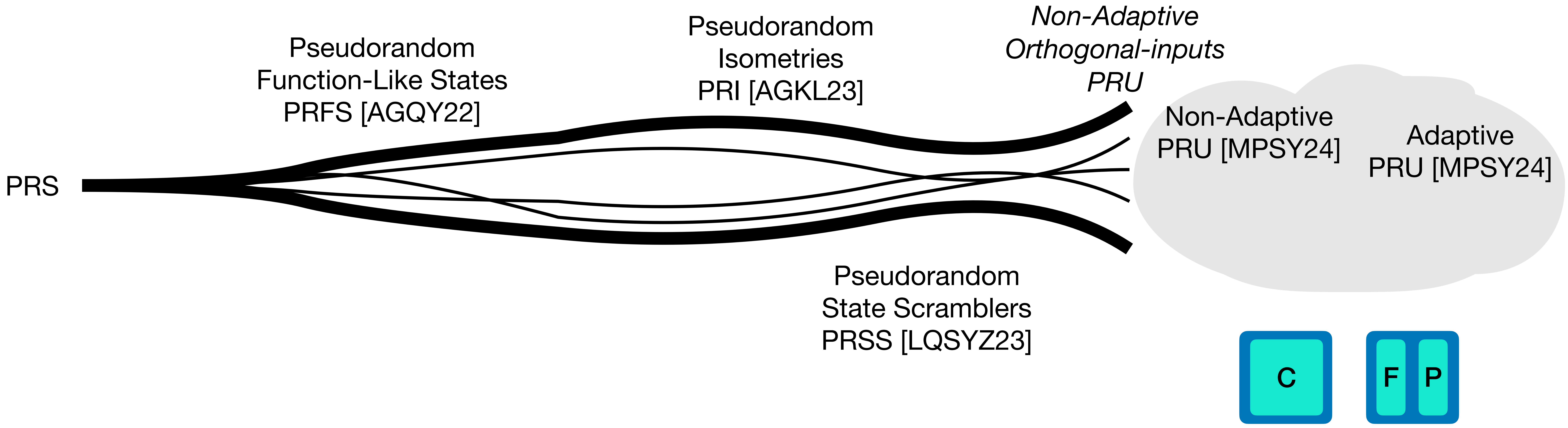
A Plethora of Pseudorandom Objects



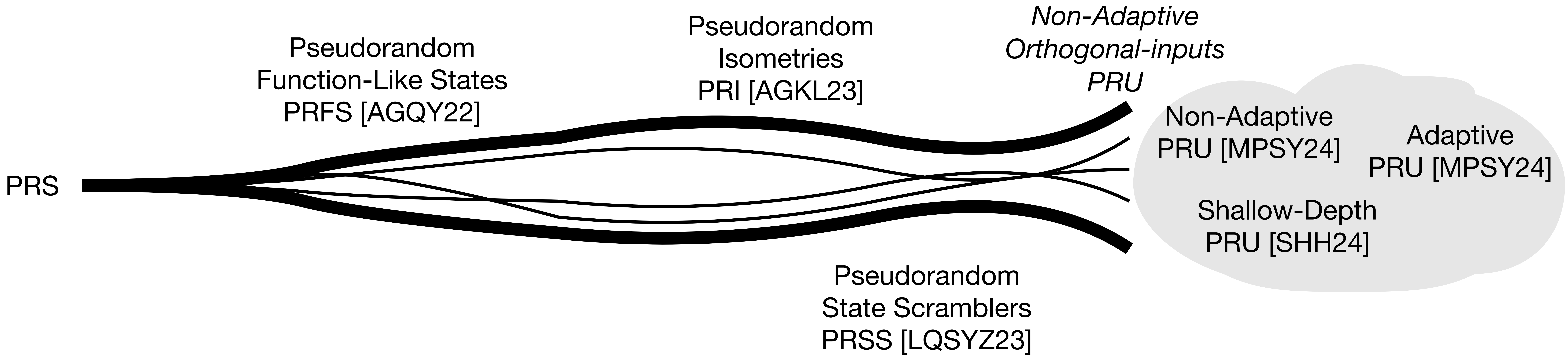
A Plethora of Pseudorandom Objects



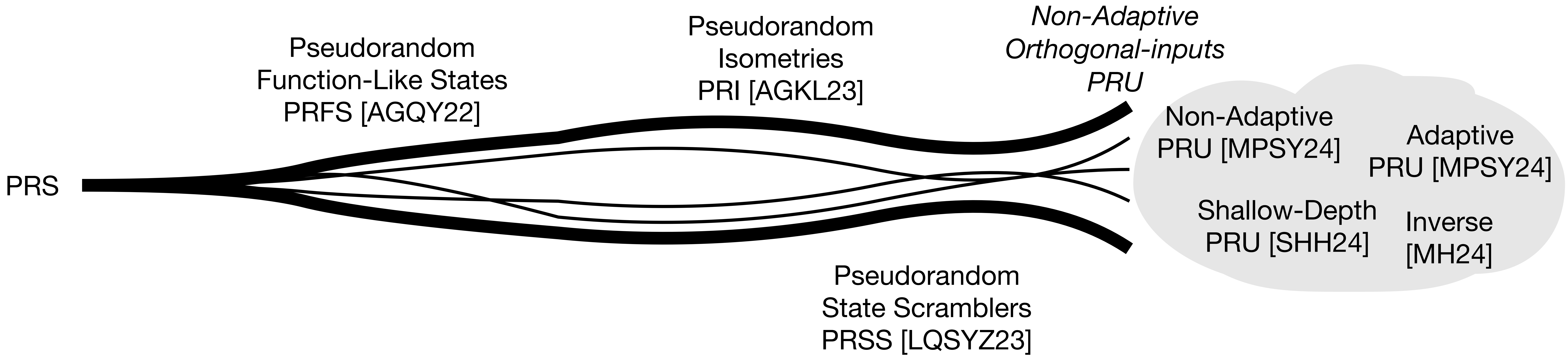
A Plethora of Pseudorandom Objects



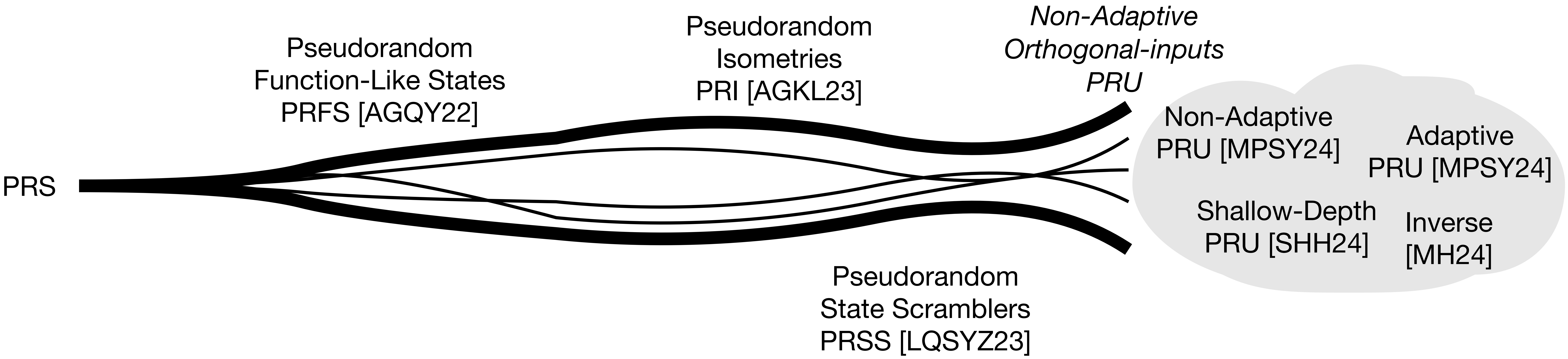
A Plethora of Pseudorandom Objects



A Plethora of Pseudorandom Objects



A Plethora of Pseudorandom Objects



Pseudorandom unitaries are neither real nor sparse nor noise-robust [HBK23]

Future Directions

- Can we prove security for *tensor-product* inputs?
- In what cases is the security definition sufficient, and what does it imply on the need for an imaginary part?