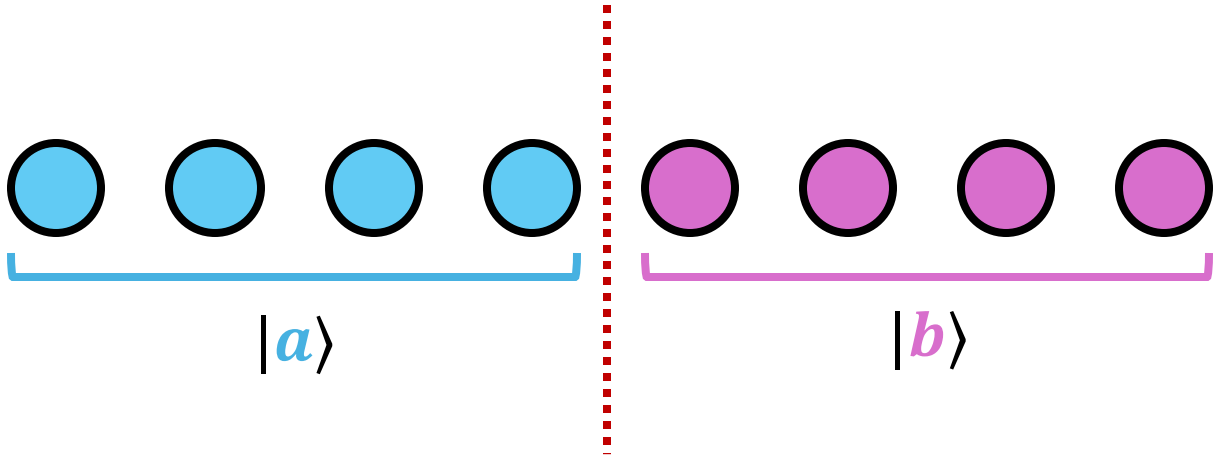
The state hidden subgroup problem
and an efficient algorithm for locating unentanglement

Adam Bouland
Stanford

Tudor Giurgică-Tiron
Stanford → U Maryland

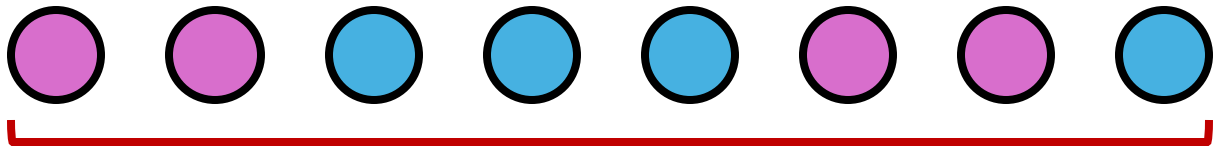
John Wright
UC Berkeley

A puzzle



no entanglement

A puzzle



$|\psi\rangle$

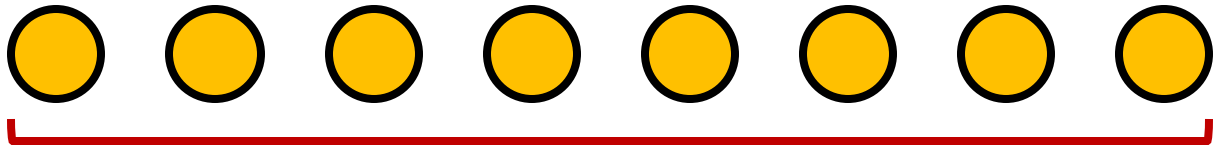
Def: S = the set of blue vertices $\subseteq \{1, \dots, 8\}$

T = the set of purple vertices $\subseteq \{1, \dots, 8\}$

Note: $|\psi\rangle$ is unentangled across the S, T cut

i.e. it is a product state $|\psi\rangle = |a\rangle_S \otimes |b\rangle_T$

A puzzle



$|\psi\rangle$

Def: S = the set of **blue** vertices $\subseteq \{1, \dots, 8\}$

T = the set of **purple** vertices $\subseteq \{1, \dots, 8\}$

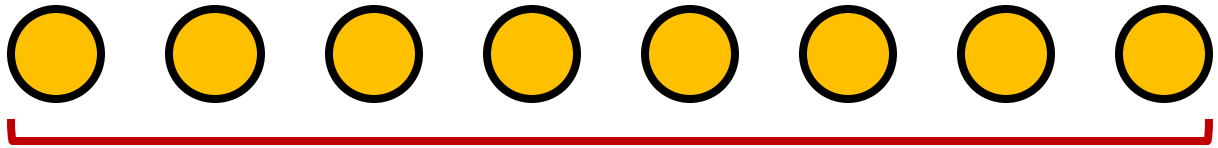
Note: $|\psi\rangle$ is unentangled across the S, T cut

i.e. it is a product state $|\psi\rangle = |a\rangle_S \otimes |b\rangle_T$

The hidden cut problem

Given copies of n-qubit $|\psi\rangle$, find S (or T).

A puzzle



$|\psi\rangle$

The hidden cut problem

Given copies of n-qubit $|\psi\rangle$, find S (or T).

Can solve via full state tomography. Requires $\Omega(2^n)$ copies.

Today's Q: Is this possible with $\mathbf{poly}(n)$ copies?

Easier Q: Suppose you have a guess for S and T.

How to tell if $|\psi\rangle$ is a product state across S and T?

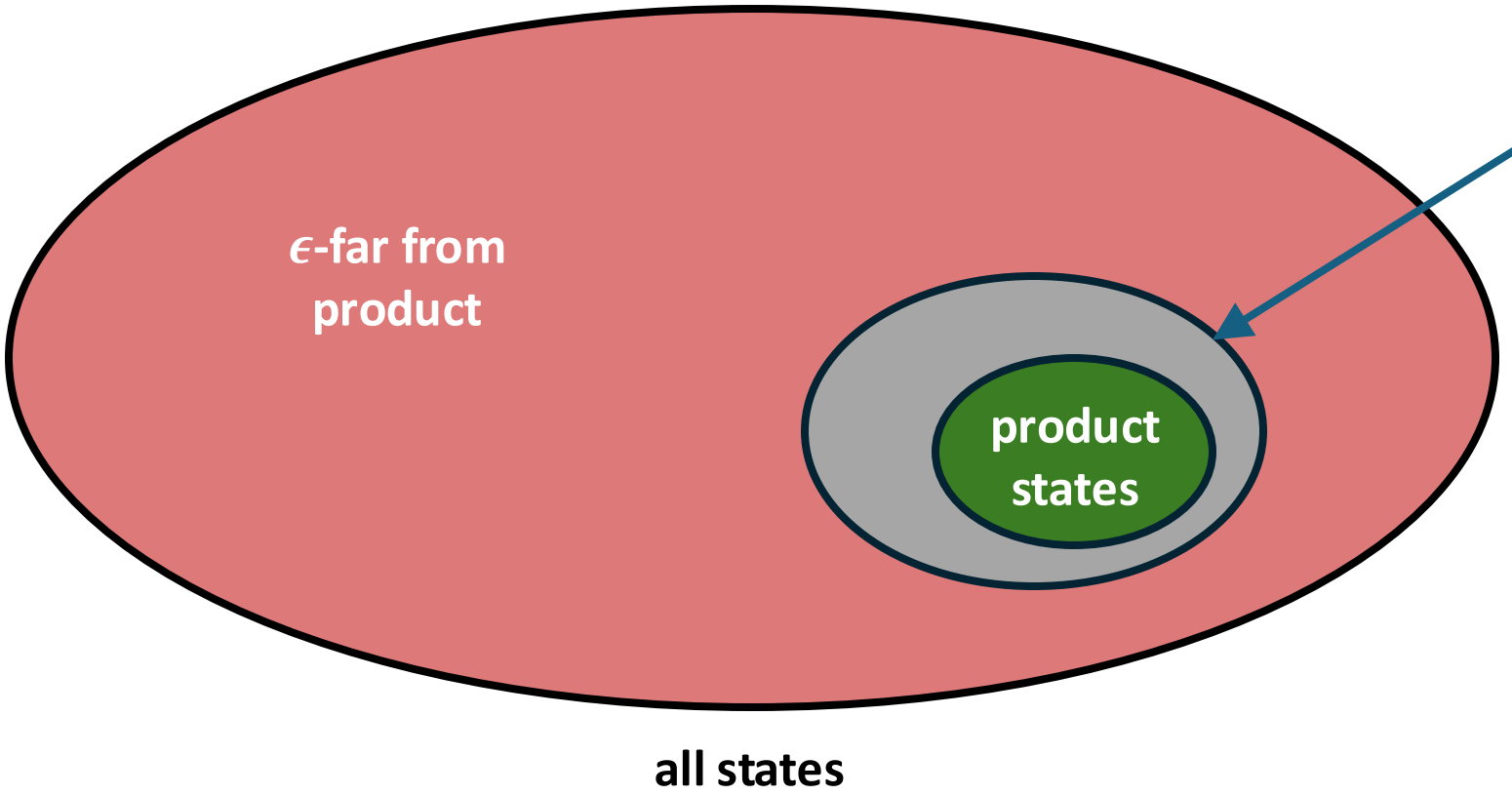
This is called **product testing**.

Product testing

Input: A bipartite quantum state $|\psi_{AB}\rangle$ on two registers A and B

Output:
- "**Product**" if $|\psi_{AB}\rangle$ is a **product state**: $|\psi_{AB}\rangle = |a_A\rangle \otimes |b_B\rangle$
- "**Entangled**" if $|\psi_{AB}\rangle$ is **ϵ-far from product**:

$$\mathrm{D}_{\mathrm{tr}}(|\psi\rangle\langle\psi|, |v\rangle\langle v|) \geq \epsilon \text{ for every product state } |v\rangle$$



Not **product**!

Not **ϵ-far from product** either.

Too close to tell!

Don't care what alg does here.

Product testing

Input: A bipartite quantum state $|\psi_{AB}\rangle$ on two registers A and B

Output:
- "**Product**" if $|\psi_{AB}\rangle$ is a **product state**: $|\psi_{AB}\rangle = |a_A\rangle \otimes |b_B\rangle$
- "**Entangled**" if $|\psi_{AB}\rangle$ is **ϵ-far from product**:

$$\mathrm{D}_{\mathrm{tr}}(|\psi\rangle\langle\psi|, |v\rangle\langle v|) \geq \epsilon \text{ for every product state } |v\rangle$$

Fact:

There is an algorithm called the **SWAP test** with the following guarantees:

- $|\psi_{AB}\rangle$ is a **product state**: ⇒ **SWAP test** always outputs "**product**"
- $|\psi_{AB}\rangle$ is **ϵ-far from product** : ⇒ **SWAP test** outputs "**entangled**" w/prob $\geq \epsilon^2/2$

Furthermore, the **SWAP test** uses only 2 copies of $|\psi_{AB}\rangle$.

$\therefore n = \mathrm{O}(1/\epsilon^2)$ copies of suffice for product testing (w/ success prob **99%**)

The SWAP Test

Def: Given integer d, $\mathbf{SWAP}$ is the unitary acting on $\mathbb{C}^d \otimes \mathbb{C}^d$ as follows:

$$\mathbf{SWAP} \cdot |i\rangle \otimes |j\rangle = |j\rangle \otimes |i\rangle, \qquad \text{for all } i, j \in [d].$$

By linearity, $\mathbf{SWAP} \cdot |u\rangle \otimes |v\rangle = |v\rangle \otimes |u\rangle$ for all $|u\rangle, |v\rangle \in \mathbb{C}^d$.

Suppose $|\psi_{AB}\rangle$ is a **product state**. So $|\psi_{AB}\rangle = |a_A\rangle \otimes |b_B\rangle$.

Then $\mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle \otimes |\psi_{A'B'}\rangle$

$$= \mathbf{SWAP}_{AA'} \cdot |a_A\rangle \otimes |b_B\rangle \otimes |a_{A'}\rangle \otimes |b_{B'}\rangle = |a_A\rangle \otimes |b_B\rangle \otimes |a_{A'}\rangle \otimes |b_{B'}\rangle$$

$$= |\psi_{AB}\rangle \otimes |\psi_{A'B'}\rangle$$

swaps!

The SWAP Test

Def: Given integer d, $\mathbf{SWAP}$ is the unitary acting on $\mathbb{C}^d \otimes \mathbb{C}^d$ as follows:

$$\mathbf{SWAP} \cdot |i\rangle \otimes |j\rangle = |j\rangle \otimes |i\rangle, \qquad \text{for all } i, j \in [d].$$

By linearity, $\mathbf{SWAP} \cdot |u\rangle \otimes |v\rangle = |v\rangle \otimes |u\rangle$ for all $|u\rangle, |v\rangle \in \mathbb{C}^d$.

Suppose $|\psi_{AB}\rangle$ is a **product state**. So $|\psi_{AB}\rangle = |a_A\rangle \otimes |b_B\rangle$.

Then $\mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle \otimes |\psi_{A'B'}\rangle$

$$= \mathbf{SWAP}_{AA'} \cdot |a_A\rangle \otimes |b_B\rangle \otimes |a_{A'}\rangle \otimes |b_{B'}\rangle = |a_A\rangle \otimes |b_B\rangle \otimes |a_{A'}\rangle \otimes |b_{B'}\rangle$$
$$= |\psi_{AB}\rangle \otimes |\psi_{A'B'}\rangle$$

$$\therefore \mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle^{\otimes 2} = |\psi_{AB}\rangle^{\otimes 2}$$

Fact: Suppose $|\psi_{AB}\rangle$ is **ϵ-far from product**. Then

$$|\langle\psi_{AB}|^{\otimes 2} \cdot \mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle^{\otimes 2}| \leq 1 - \epsilon^2.$$

The SWAP Test

Summary:

- If $|\psi_{AB}\rangle$ is a **product state**, then $\mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle^{\otimes 2} = |\psi_{AB}\rangle^{\otimes 2}$.
- If $|\psi_{AB}\rangle$ is **ϵ-far from product**,

$$|\langle\psi_{AB}|^{\otimes 2} \cdot \mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle^{\otimes 2}| \leq \mathbf{1 - \epsilon^2}.$$

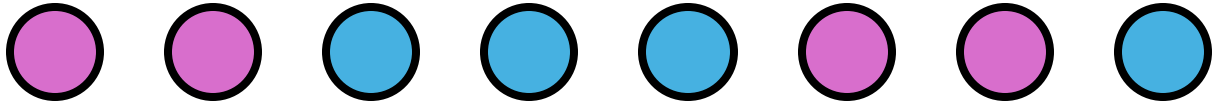
The SWAP test uses two copies of $|\psi_{AB}\rangle$
to check if $\mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle^{\otimes 2} = |\psi_{AB}\rangle^{\otimes 2}$.

If $|\psi_{AB}\rangle$ is a **product state**, the check always passes,
and it always outputs "**product**"

If $|\psi_{AB}\rangle$ is **ϵ-far from product**, the check fails with probability $\epsilon^2/2$,
in which case it outputs "**entangled**"

The hidden cut problem

Input: An n-qubit quantum state $|\psi\rangle$ with a **unique** hidden cut (S, T).



$$|\psi\rangle = |a\rangle_S \otimes |b\rangle_T$$

"**Unique**" means:

- $|a\rangle_S$ and $|b\rangle_T$ are both ϵ-far from product
- $|\psi\rangle$ is ϵ-far from product across any other (S', T') cut

Output: S or T

[Harrow, Lin, Montanaro 2016] studied the **decision** version of this problem.

They gave a $\mathbf{O}(n/\epsilon^2)$ copy algorithm which distinguishes:

- (**Hidden cut**) $|\psi\rangle$ has a hidden cut (S, T).
- (**Genuine multipartite entanglement**)

  $|\psi\rangle$ is ϵ-far from product across any (S, T) cut

computationally **inefficient**

[Montanaro, Jones 2024] $\Omega(n/\log(n))$ copies are required for **decision** version

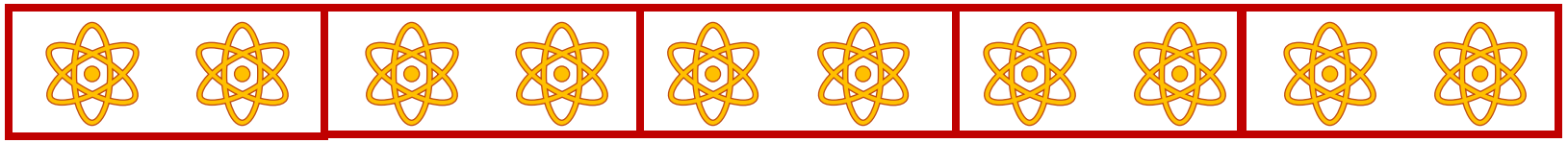
An inefficient alg for the hidden cut problem

We already saw how to test if $|\psi\rangle$ is product across (S, T) using the $\mathbf{SWAP}$ test.

So why not do it for (S_1, T_1), then (S_2, T_2), then (S_3, T_3), …?

Testing for the (S, T) cut:

$2t$ copies of $|\psi\rangle$:



…

- (S, T) is the hidden cut ⇒ all $\mathbf{SWAP}$ tests output "**product**"
- (S, T) is **not** the hidden cut ⇒ each $\mathbf{SWAP}$ tests output "**product**" w/prob $\leq 1 - \epsilon^2$

$\therefore$ all $\mathbf{SWAP}$ tests output "**product**" w/prob $\leq (1-\epsilon^2)^t$

$\leq O(1/2^n)$ if $t = O(n/\epsilon^2)$

Def: $\Pi_{S,T}$ = projector onto all-**products** outcome, $\bar{\Pi}_{S,T} = I - \Pi_{S,T}$

$\mathrm{tr}(\Pi_{S,T} \cdot |\psi\rangle\langle\psi|^{\otimes 2t}) = 1$ if (S, T) is hidden cut, $\leq O(1/2^n)$ if not

An inefficient alg for the hidden cut problem

Input: $2t = O(n/\epsilon^2)$ copies of n-qubit $|\psi\rangle$.

1. For all nontrivial cuts (S, T):
2. Measure $|\psi\rangle^{\otimes 2t}$ with $\{\Pi_{S,T}, \overline{\Pi}_{S,T}\}$.
3. If observe $\Pi_{S,T}$ outcome, output "S".

exponential runtime

Pf of correctness:

Each measurement errs with probability $\leq O(1/2^n)$.

Only 2^n total measurements.

So can set error probability to **0.01**.

(But wait? Doesn't each measurement disturb the state?)

(Yes! But analysis still works using **Gao's quantum union bound**.) □

similar to [Harrow, Lin, Montanaro 2016]'s algorithm for decision version

This problem seems to **require** exponentially time
(how else to search over all subsets?)

Suggests the possibility of an information-computation gap.

Potentially useful for … crypto … ?

Pseudorandom state length expansion: (applications?)

$|a\rangle, |b\rangle$ pseudorandom $\xrightarrow{\textbf{scramble}}$ $|\psi\rangle = |a\rangle_S \otimes |b\rangle_T$ also pseudorandom?

Not if you can find **S**!

I like this because it's a natural info theory problem.

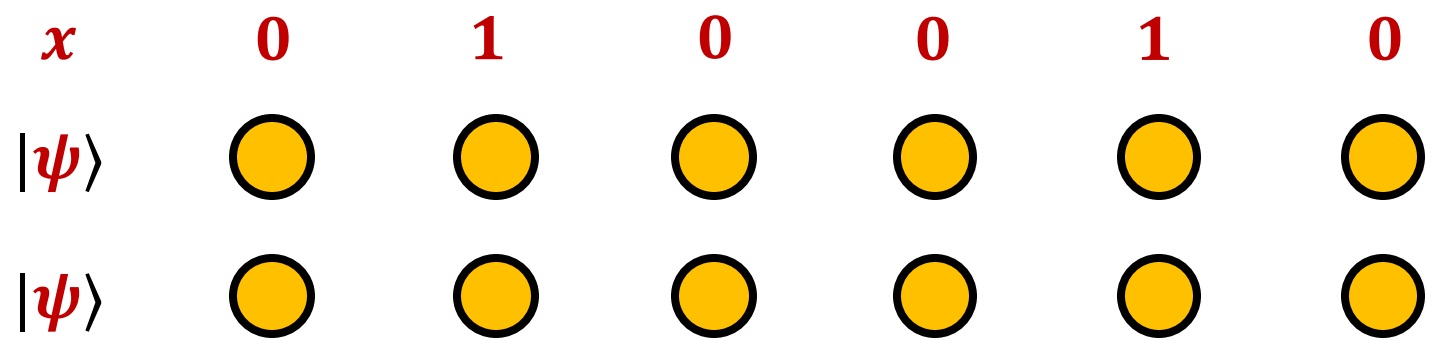
Main result

There is an **efficient** algorithm for the hidden cut problem which uses $\mathbf{O}(\boldsymbol{n}/\boldsymbol{\epsilon}^{\mathbf{2}})$ copies and runs in time $\mathbf{poly}(\boldsymbol{n}, \mathbf{1}/\boldsymbol{\epsilon}^{\mathbf{2}})$.

Algorithm inspired by **Hidden Subgroup Problem** (HSP)

We define a state analogue of HSP called **StateHSP**

Key idea



Properties:

- Let (S, T) be the hidden cut. Then $x \in H = \{0^n, 1_S, 1_T, 1^n\}$ = subgroup of Z_2^n

$$\mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2} = |\psi\rangle^{\otimes 2} \text{ for } x = 0^n,\ 1_S,\ 1_T,\ 1_S + 1_T = 1^n$$

- For any $x \notin H$, $|\langle\psi|^{\otimes 2} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}| \leq 1 - \epsilon^2$.
- $\mathbf{SWAP}_x \cdot \mathbf{SWAP}_y = \mathbf{SWAP}_{x+y}$ ($\mathbf{SWAP}_x$ is a representation of Z_2^n)

Simon's problem

Given: Oracle access to a function $f:\{0,1\}^n \to \{\mathbf{Red}, \mathbf{Green}, \mathbf{Blue}, \dots\}$

which "hides" a secret string $\boldsymbol{s} \in \{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{n}}$:

- $\boldsymbol{f(x) = f(x+s)}$ for all $\boldsymbol{x} \in \{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{n}}$
- $\boldsymbol{f(x) \neq f(x+z)}$ whenever $\boldsymbol{z \neq s}$

Goal: find $\boldsymbol{s}$.

We have an object ($\boldsymbol{f}$)

It is invariant when shifted by an element of $\boldsymbol{H} = \{\boldsymbol{0^n}, \boldsymbol{s}\}$

It gets completely changed when shifted by any other $\mathbf{z}$

Our goal is to identify $\boldsymbol{H}$

Similar to the hidden cut problem!

Simon's problem

Given: Oracle access to a function $f:\{0,1\}^n \to \{\mathbf{Red}, \mathbf{Green}, \mathbf{Blue}, \dots\}$ which "hides" a secret string $\boldsymbol{s} \in \{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{n}}$:

- $f(\boldsymbol{x}) = f(\boldsymbol{x}+\boldsymbol{s})$ for all $\boldsymbol{x} \in \{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{n}}$
- $f(\boldsymbol{x}) \neq f(\boldsymbol{x}+z)$ whenever $\boldsymbol{z} \neq \boldsymbol{s}$

Goal: find $\boldsymbol{s}$.

Alg:

1. Prepare the unif. superpos. $\sum_{\boldsymbol{x}\in\{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{n}}} |\boldsymbol{x}\rangle$
2. Query $\boldsymbol{f}$, giving the state $\sum_{\boldsymbol{x}\in\{\boldsymbol{0},\boldsymbol{1}\}^{\boldsymbol{n}}} |\boldsymbol{x}\rangle \otimes |\boldsymbol{f(x)}\rangle$
3. FT the first register and measure, yielding a uniform $\boldsymbol{y} \in \boldsymbol{H}^{\perp}$
4. Repeat until $\boldsymbol{H}$ has been identified.

Algorithm for hidden cut

Given: copies of $|\psi\rangle$, find $H = \{0^n, 1_S, 1_T, 1^n\}$

1. Prepare the state $\sum_{x\in\{0,1\}^n} |x\rangle \otimes |\psi\rangle^{\otimes 2}$
2. Apply $\mathbf{SWAP}$, yielding $\sum_{x\in\{0,1\}^n} |x\rangle \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$
3. FT the first register and measure, yielding $y \in H^\perp$
4. Repeat until H has been identified.

One problem: y is probably not a uniform element of $H^\perp$.

- For any $x \notin H$, $|\langle\psi|^{\otimes 2} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}| \leq 1 - \epsilon^2$. ← **nonzero**

Can **amplify** this closer to 0 by using more copies. Everything works out ☺.

Algorithm for hidden cut

2. Apply $\mathbf{SWAP}$, yielding $\sum_{x\in\{0,1\}^n} |x\rangle \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$

3. FT the first register and measure, yielding $y \in H^\perp$

$$\sum_{x\in\{0,1\}^n} |x\rangle \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2} \xrightarrow{\text{FT}} \sum_{x\in\{0,1\}^n} \left(\sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle \right) \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$$

$$= \sum_{y\in\{0,1\}^n} |y\rangle \otimes \boxed{\sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}} \quad (*)$$

Suppose $y \notin H^\perp$. Then $h \cdot y = 1 \pmod 2$ for some $h \in H$. So coeff on y:

$$(*) = \frac{1}{2} \cdot \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2} + \frac{1}{2} \cdot \sum_{x\in\{0,1\}^n} \boxed{(-1)^{(x+h)\cdot y}} \cdot \mathbf{SWAP}_{x+h} \cdot |\psi\rangle^{\otimes 2}$$

$$(-1)^{(x+h)\cdot y} = (-1)^{x\cdot y + h\cdot y} = -(-1)^{x\cdot y}$$

Algorithm for hidden cut

2. Apply $\mathbf{SWAP}$, yielding $\sum_{x\in\{0,1\}^n} |x\rangle \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$

3. FT the first register and measure, yielding $y \in H^{\perp}$

$$\sum_{x\in\{0,1\}^n} |x\rangle \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2} \xrightarrow{\text{FT}} \sum_{x\in\{0,1\}^n} \left(\sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle \right) \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$$

$$= \sum_{y\in\{0,1\}^n} |y\rangle \otimes \boxed{\sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}} \quad (*)$$

Suppose $y \notin H^{\perp}$. Then $h \cdot y = 1 \pmod 2$ for some $h \in H$. So coeff on y:

$$(*) = \frac{1}{2} \cdot \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2} - \frac{1}{2} \cdot \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \cdot \mathbf{SWAP}_{x+h} \cdot |\psi\rangle^{\otimes 2}$$

$$\mathbf{SWAP}_{x+h} \cdot |\psi\rangle^{\otimes 2} = \mathbf{SWAP}_x \cdot \mathbf{SWAP}_h \cdot |\psi\rangle^{\otimes 2} = \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$$

Algorithm for hidden cut

2. Apply $\mathbf{SWAP}$, yielding $\sum_{x\in\{0,1\}^n} |x\rangle \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$

3. FT the first register and measure, yielding $y \in H^{\perp}$

$$\sum_{x\in\{0,1\}^n} |x\rangle \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2} \xrightarrow{\text{FT}} \sum_{x\in\{0,1\}^n} \left(\sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle \right) \otimes \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$$

$$= \sum_{y\in\{0,1\}^n} |y\rangle \otimes \boxed{\sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}} \quad (*)$$

Suppose $y \notin H^{\perp}$. Then $h \cdot y = 1 \pmod 2$ for some $h \in H$. So coeff on y:

$$(*) = \frac{1}{2} \cdot \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2} - \frac{1}{2} \cdot \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y} \cdot \mathbf{SWAP}_x \cdot |\psi\rangle^{\otimes 2}$$

$$= \mathbf{0}!$$

□

Simon's problem is a special case of the HSP over $\boldsymbol{Z_2^n}$.

Other HSPs can be defined over more general groups $\boldsymbol{G}$,
with applications to factoring, lattice-based crypto, etc.

Our hidden cut problem can be viewed as a
state version of the HSP over $\boldsymbol{Z_2^n}$.

We define a more general state HSP over arbitrary groups $\boldsymbol{G}$.

We show that certain algorithms for HSP over $\boldsymbol{G}$
will behave similarly for StateHSP over $\boldsymbol{G}$.

State Hidden Subgroup Problem

Let G be a group and $R: G \to U(d)$ be a representation of G.

Given copies of quantum state $|\psi\rangle$ which "**hides**" a subgroup $H \leq G$:

- For all $h \in H$, $R(h) \cdot |\psi\rangle = |\psi\rangle$.
- For all $h \notin H$, $|\langle\psi| \cdot R(h) \cdot |\psi\rangle| \leq 1 - \epsilon$. ← "orthogonality allowance"

Goal: find H using as few copies of $|\psi\rangle$ as possible.

Hidden State Problem:
Special case when $G = Z_2^n$, $R(x) = \mathrm{SWAP}_x$, and states are of the form $|\psi\rangle^{\otimes 2}$.

Quantum state version of the standard HSP problem.

Looks more like standard HSP as the orthogonality allowance $\epsilon \to 1$,

Can "**inflate**" orthogonality allowance: replace $R(g) \to R(g)^{\otimes k}$, $|\psi\rangle \to |\psi\rangle^{\otimes k}$,

then $|\langle\psi|^{\otimes k} \cdot R(h)^{\otimes k} \cdot |\psi\rangle^{\otimes k}| \leq (1 - \epsilon)^k$.

State Hidden Subgroup Problem

Let G be a group and $R: G \to U(d)$ be a representation of G.

Given copies of quantum state $|\psi\rangle$ which "**hides**" a subgroup $H \leq G$:

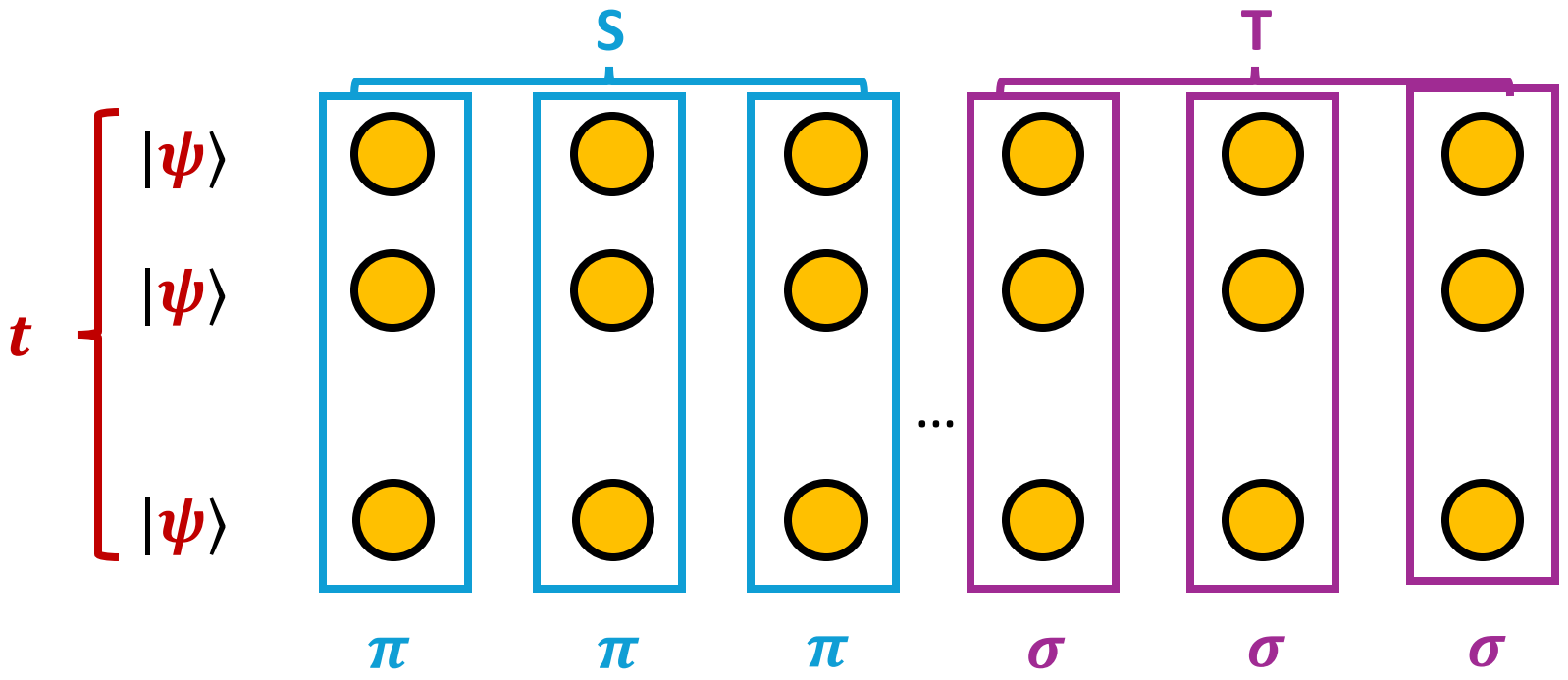
- For all $h \in H$, $R(h) \cdot |\psi\rangle = |\psi\rangle$.
- For all $h \notin H$, $|\langle\psi| \cdot R(h) \cdot |\psi\rangle| \leq 1 - \epsilon$. ← "orthogonality allowance"

Goal: find H using as few copies of $|\psi\rangle$ as possible.

Some facts transfer over directly from normal HSP:

- Normal HSP Fourier sampling algorithms transfer to the state HSP setting
  (e.g. hidden cut alg is just $G = Z_2^n$ Fourier sampling alg)
- Can information theoretically solve state HSP with $O(|G|/\epsilon^2)$copies of $|\psi\rangle$
- Some HSPs still seem computationally difficult (the **symmetric group**) ☹

On the symmetric group…



Consider the parent group $G = S_t^{\times n} = S_t \times S_t \times \cdots \times S_t$.

Then $|\psi\rangle^{\otimes t}$ "hides" the subgroup $H = \{(\pi^{\times S}, \sigma^{\times T}), \pi, \sigma \in S_t\}$.

Could try: set t large, do Fourier sampling over $G = S_t^{\times n}$.

We show this is **hard**, for same reason that symmetric group HSP is **hard**.

Past State HSPs

Standard HSP

Let G be a group and $f: G \to \mathbf{Outputs}$ be a function "hiding" a subgroup $H \leq G$:

- For all $g \in G, h \in H,\ f(g) = f(gh)$
- For all $g \in G, h \notin H,\ f(g) \neq f(gh)$

Standard HSP approach begins by preparing the state $|\psi\rangle = \sum_{g \in G} |g\rangle \otimes |f(g)\rangle$

Let $R(\cdot)$ be the **right regular representation** of G,

$$R(h) \cdot |g\rangle = |gh^{-1}\rangle$$

$$R(h) \cdot |\psi\rangle = \sum_{g \in G} |gh^{-1}\rangle \otimes |f(g)\rangle = \sum_{g \in G} |g'\rangle \otimes |f(g'h)\rangle = \begin{cases} |\psi\rangle & \text{if } h \in H \\ \perp |\psi\rangle & \text{if } h \notin H \end{cases}$$

$gh^{-1} = g'$ $\quad f(g) = g'h$

$$= \begin{cases} g' & \text{if } h \in H \\ \neq g' & \text{if } h \notin H \end{cases}$$

Past State HSPs

Standard HSP

Let G be a group and $f: G \to \mathbf{Outputs}$ be a function "hiding" a subgroup $H \leq G$:

- For all $g \in G, h \in H,\ f(g) = f(gh)$
- For all $g \in G, h \notin H,\ f(g) \neq f(gh)$

Standard HSP approach begins by preparing the state $|\psi\rangle = \sum_{g \in G} |g\rangle \otimes |f(g)\rangle$

Let $R(\cdot)$ be the **right regular representation** of G,

$$R(h) \cdot |g\rangle = |gh^{-1}\rangle$$

$$R(h) \cdot |\psi\rangle = \sum_{g \in G} |gh^{-1}\rangle \otimes |f(g)\rangle = \sum_{g \in G} |g'\rangle \otimes |f(g'h)\rangle = \begin{cases} |\psi\rangle & \text{if } h \in H \\ \perp |\psi\rangle & \text{if } h \notin H \end{cases}$$

Standard HSP = state HSP with orthogonality allowance $\epsilon = 1$.

Past State HSPs

Standard HSP

Standard HSP = state HSP with orthogonality allowance $\epsilon = 1$.

State isomorphism [LG17]

Given copies of n-qubit $|\psi\rangle$ and permutation $\pi \cdot |\psi\rangle$, find π.

Stabilizer states

Let G = n-qubit Paulis. A **stabilizer state** is a state $|\psi\rangle$ s.t.

$$P \cdot |\psi\rangle = |\psi\rangle, \qquad \text{for all } P \in H,$$

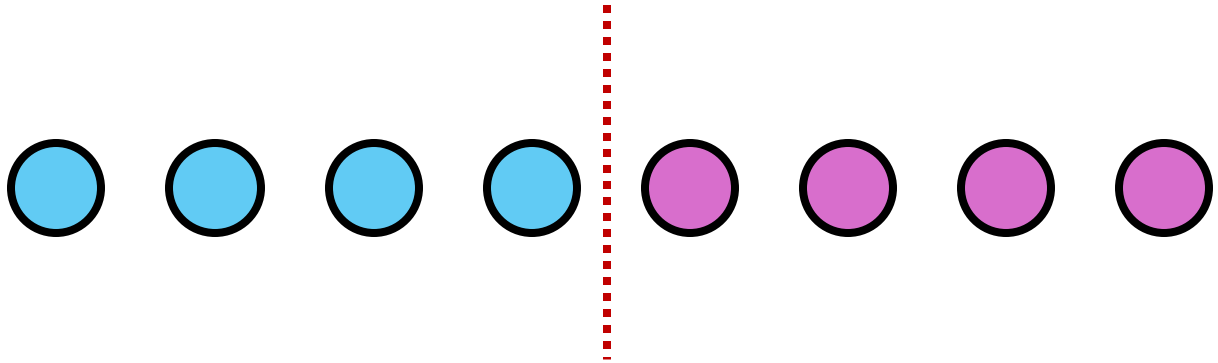
where H = size 2^n commuting subgroup of G.

Goal: given copies of $|\psi\rangle$, **test** if $|\psi\rangle$ is a stabilizer state, or **learn** H.

Lots of work on this problem! Solved via **Bell difference sampling**.

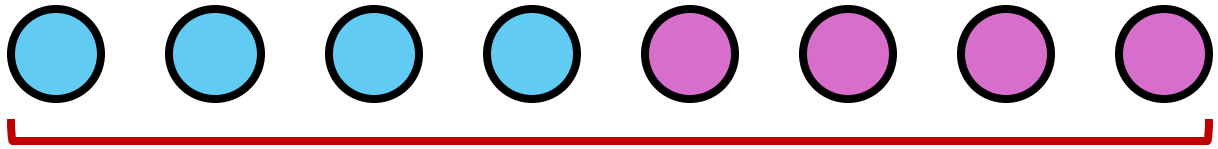
[HIC]: simplify our analysis, only measures 2 copies at a time.

A harder puzzle



Schmidt rank ≤ 2

A harder puzzle



$|\psi\rangle$

Def: **S** = the set of **blue** vertices $\subseteq \{1, \dots, 8\}$

T = the set of **purple** vertices $\subseteq \{1, \dots, 8\}$

Q: Can you find **S** and **T**?

Easier Q: Suppose you have a guess for **S** and **T**.

How to tell if $|\psi\rangle$ is rank 2 across **S** and **T**?

Rank testing

Input: A bipartite quantum state $|\psi_{AB}\rangle$ on two registers A and B

Output:
- "Rank r" if $|\psi_{AB}\rangle$ has Schmidt rank at most r
- "Not rank r" if $|\psi_{AB}\rangle$ is ϵ-far Schmidt rank r

Thm [OW15]

There is an algorithm called the **Rank tester** with the following guarantees:

- $|\psi_{AB}\rangle$ is a rank r: $\Rightarrow$ **Rank tester** always outputs "rank r"
- $|\psi_{AB}\rangle$ is ϵ-far from rank r : $\Rightarrow$ **Rank tester** outputs "not rank r" w/prob $\geq 99\%$

Furthermore, the **Rank tester** uses $t = O(r^2/\epsilon^2)$ copies of $|\psi_{AB}\rangle$.

Rank tester is natural generalization of the **SWAP test**.

Alg:
1. Trace out the B registers, giving copies of $\psi_A^{\otimes t}$
2. Measure $\psi_A^{\otimes t}$ with **weak Schur sampling**. Receive Young diagram λ.
3. Output "rank r" if λ has at most r rows. Otherwise, "not rank r".

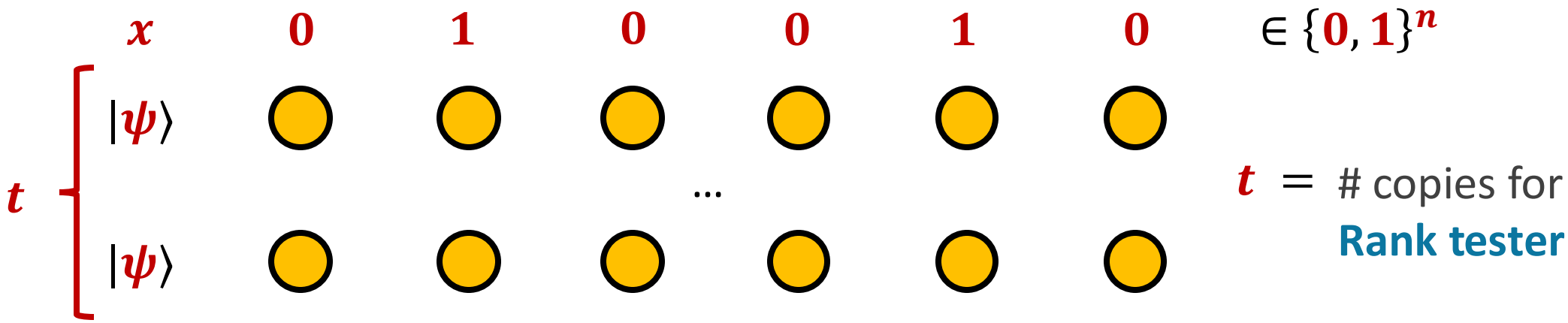
Hidden rank 2 cut

Rank tester + **Gao's quantum union bound**

⇒ Can find hidden rank 2 cut with $O(n/\epsilon^2)$ copies of n-qudit $|\psi\rangle$ inefficiently.

Q: can we do this efficiently?

Idea:



Let $X \subseteq [n]$ be the subset indicated by x.

Let $\{\Pi_x, \bar{\Pi}_x\}$, be the measurement the **Rank tester** uses on $\psi_X^{\otimes t}$.

So $\Pi_x \cdot |\psi\rangle^{\otimes t} = |\psi\rangle^{\otimes t}$ if $x = S, T$.

Set $R_x = \Pi_x - \bar{\Pi}_x$ to turn these into unitaries. **Sad fact:** $R_x R_y \neq R_{x+y}$. ☹

Hence, these do **not** form a representation of Z_2^n. Can't use StateHSP framework!

Hidden rank 2 cut

Rank tester + **Gao's quantum union bound**

⇒ Ca

Q: ca

Idea:

We don't know how to solve this problem!

Information theoretically **easy**.

Could be computationally **easy** or computationally **hard**.

Let X

Let {

So $\boldsymbol{\Pi}_x \cdot |\psi\rangle^{\otimes t} = |\psi\rangle^{\otimes t}$ if $x = S, T$.

Set $Z_x = \boldsymbol{\Pi}_x - \overline{\boldsymbol{\Pi}}_x$ to turn these into unitaries. **Sad fact:** $Z_x Z_y \neq Z_{x+y}$.

Hence, these do **not** form a representation of Z_2^n. Can't use StateHSP framework!

Final questions

1. Are there applications of the hidden cut problem?

2. More generally, are there more applications of HSP to state problems?

3. Can [Montanaro, Jones 2024] $\Omega(n/\log(n))$ copy lower bound be improved?

4. Testing if a pure state is entangled is **easy**: use the $\mathbf{SWAP}$ test.

   How many copies are needed to test if a **mixed** state is entangled?

   Easier: How many copies are needed to test if a **mixed** state is **PPT**?

Thanks!