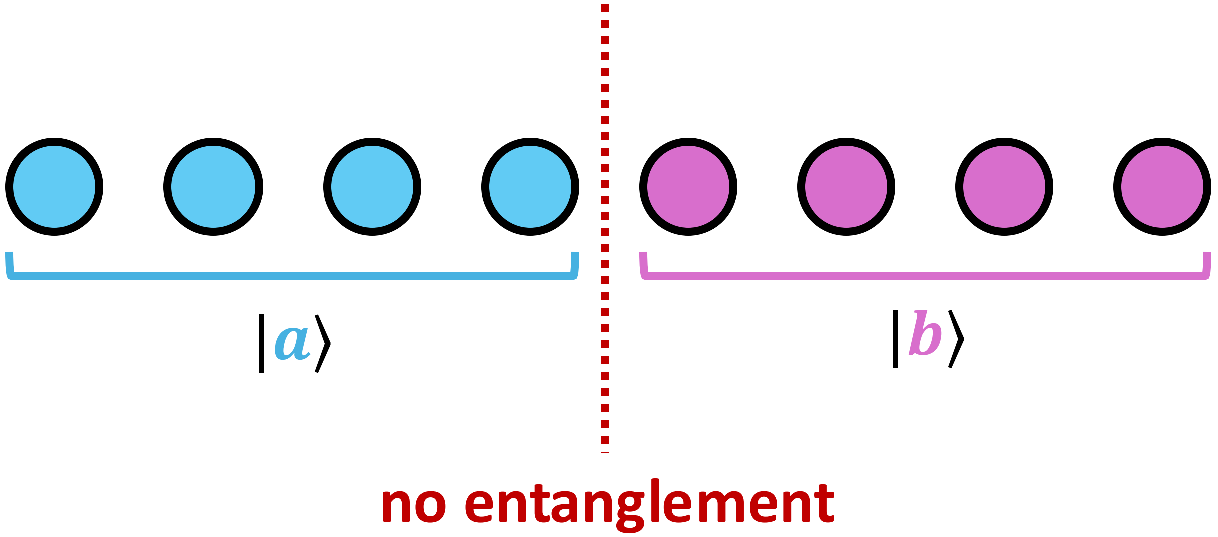
The state hidden subgroup problem
and an efficient algorithm for locating unentanglement

Adam Bouland
Stanford

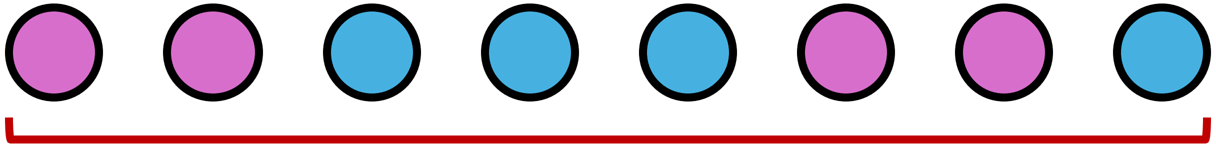
Tudor Giurgică-Tiron
Stanford → U Maryland

John Wright
UC Berkeley

A puzzle



A puzzle



$|\psi\rangle$

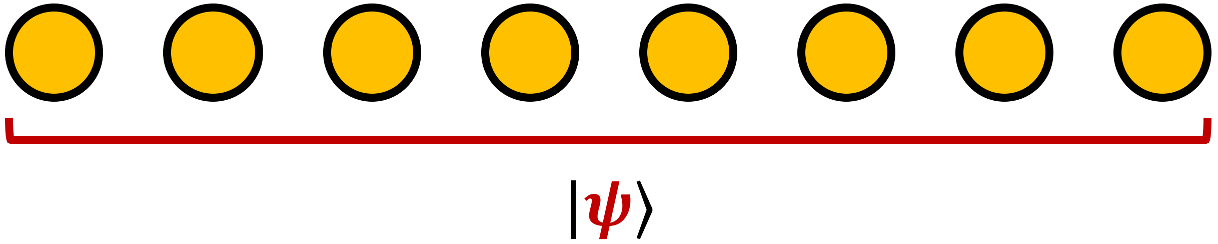
Def: S = the set of blue vertices $\subseteq \{1, \ldots, 8\}$

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

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



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

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

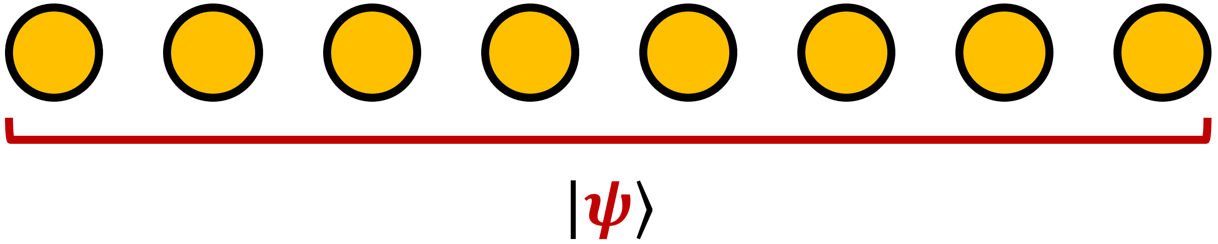
Note: $|\psi\rangle$ is unentangled across the S, T cut

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



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 $\mathrm{poly}(n)$ 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?

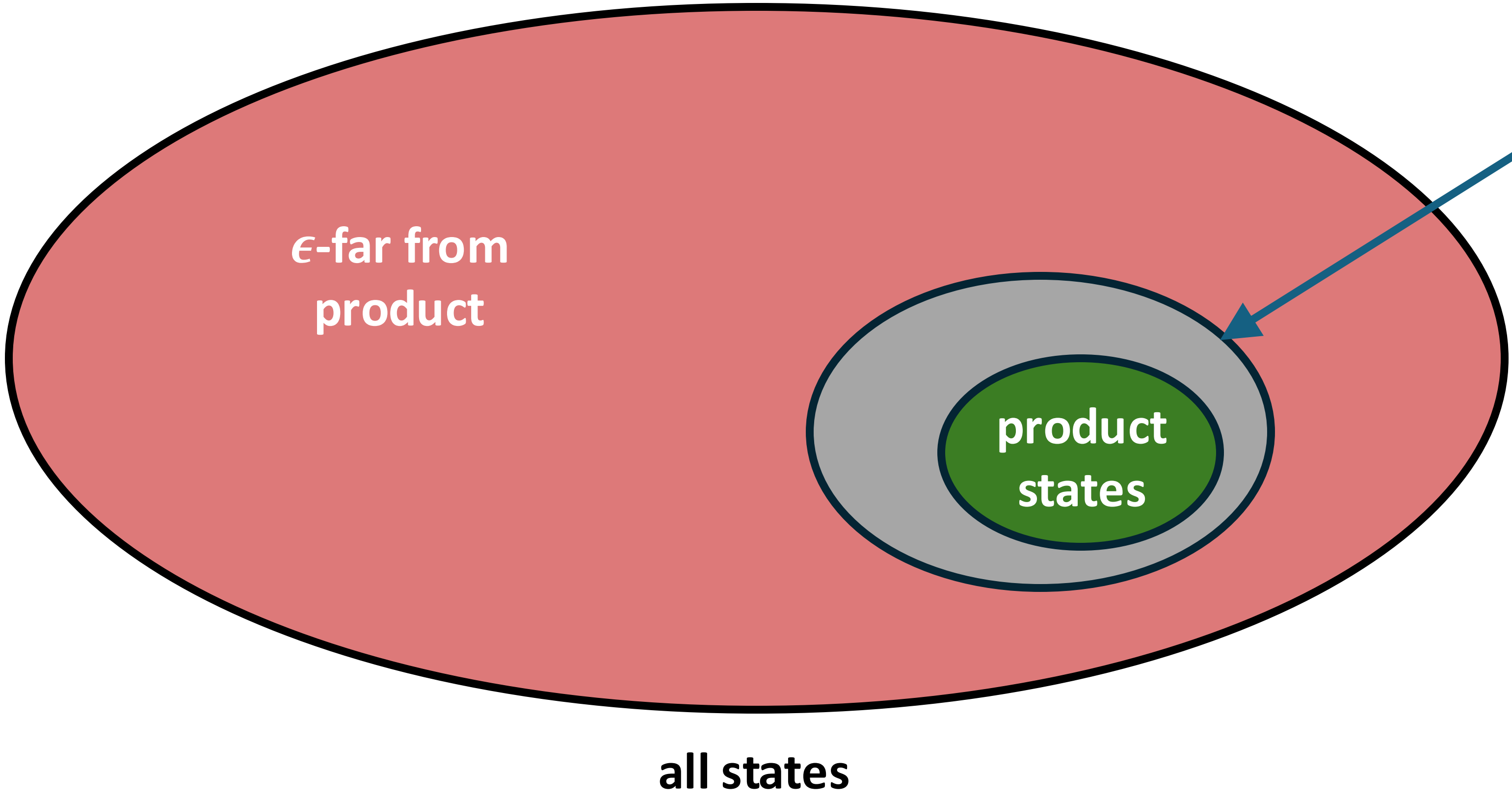
This is called **product testing**.

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**:

$\mathrm{D}_{\mathrm{tr}}(|\psi\rangle\langle\psi|, |v\rangle\langle v|) \geq \epsilon$ 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**: $\Rightarrow$ **SWAP test** always outputs "**product**"
- $|\psi_{AB}\rangle$ is **ϵ-far from product** : $\Rightarrow$ **SWAP test** outputs "**entangled**" w/prob $\geq \epsilon^2/2$

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

$\therefore n = O(1/\epsilon^2)$ 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 $\mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle \otimes |\psi_{A'B'}\rangle$

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

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

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

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

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**,

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

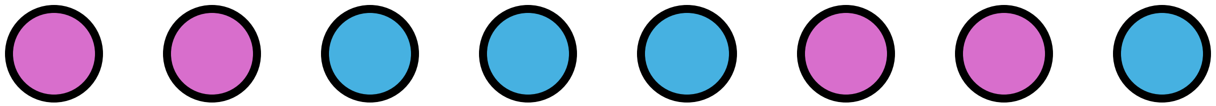
The SWAP test uses two copies of $|\psi_{AB}\rangle$
to check if $\mathbf{SWAP}_{AA'} \cdot |\psi_{AB}\rangle^{\otimes 2} = |\psi_{AB}\rangle^{\otimes 2}$.

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 $\mathrm{O}(n/\epsilon^2)$ 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

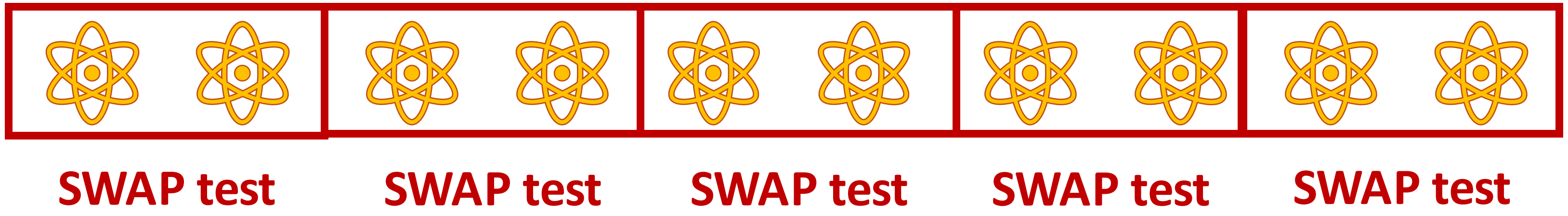
An inefficient alg for the hidden cut problem

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 $\leq \mathbf{1-\epsilon^2}$

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

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

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

$\mathrm{tr}(\Pi_{S,T} \cdot |\psi\rangle\langle\psi|^{\otimes 2t}) = 1$ 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**.) $\square$

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 $\xrightarrow{\text{scramble}}$ $|\psi\rangle = |a\rangle_S \otimes |b\rangle_T$ 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 $\mathbf{O}(\boldsymbol{n}/\boldsymbol{\epsilon}^{2})$ copies and runs in time $\mathbf{poly}(\boldsymbol{n}, \mathbf{1}/\boldsymbol{\epsilon}^{2})$.

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

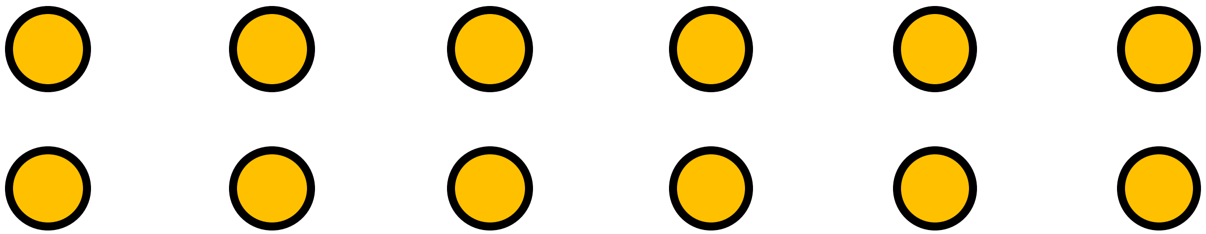
We define a state analogue of HSP called **StateHSP**

Key idea

x $0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad \in \{0,1\}^n$

$|\psi\rangle$

$|\psi\rangle$



$\mathbf{SWAP_x} \quad I \otimes \mathbf{SWAP} \otimes I \otimes I \otimes \mathbf{SWAP} \otimes I \quad \in \{I, \mathbf{SWAP}\}^n$

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

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

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

- $\mathbf{SWAP}_x \cdot \mathbf{SWAP}_y = \mathbf{SWAP}_{x+y} \qquad$ ($\mathbf{SWAP}_x$ is a representation of Z_2^n)

Simon's problem

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

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

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

Goal: find $\boldsymbol{s}$.

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

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

It gets completely changed when shifted by any other **z**

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

Similar to the hidden cut problem!

Simon's problem

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

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

Goal: find $\boldsymbol{s}$.

Alg:

1. Prepare the unif. superpos. $\sum_{\boldsymbol{x} \in \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}} |\boldsymbol{x}\rangle$
2. Query $\boldsymbol{f}$, giving the state $\sum_{\boldsymbol{x} \in \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{n}}} |\boldsymbol{x}\rangle \otimes |\boldsymbol{f}(\boldsymbol{x})\rangle$
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 ☺.

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 $\boldsymbol{G}$.

Final questions

1. Are there applications of the hidden cut problem?

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

3. 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?

Thanks!