Permutation tests for quantum state identity

arXiv: 2405.09626

Harry Buhrman

Dmitry Grinko

Philip Verduyn Lunel

Jordi Weggemans

QUANTINUUM

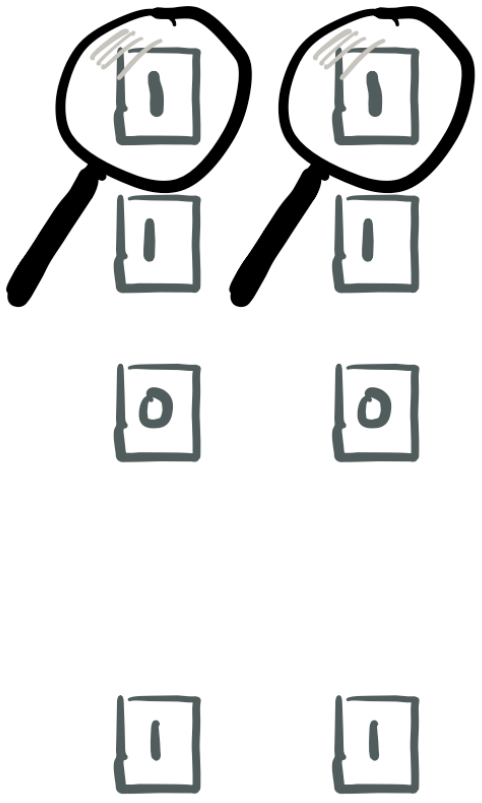
QuSoft
Research Center for Quantum Software

University of Amsterdam

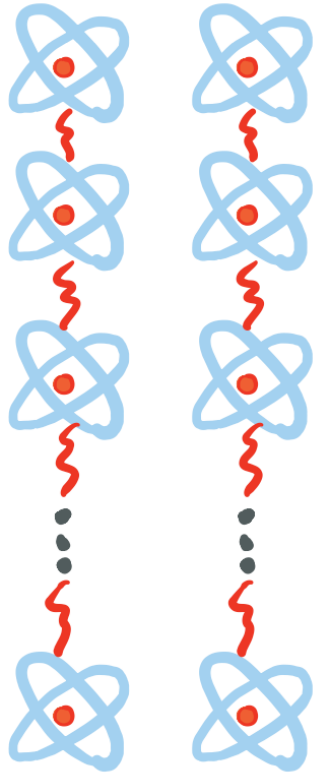
Sorbonne Université

CWI
Centrum Wiskunde & Informatica

Quantum State Identity

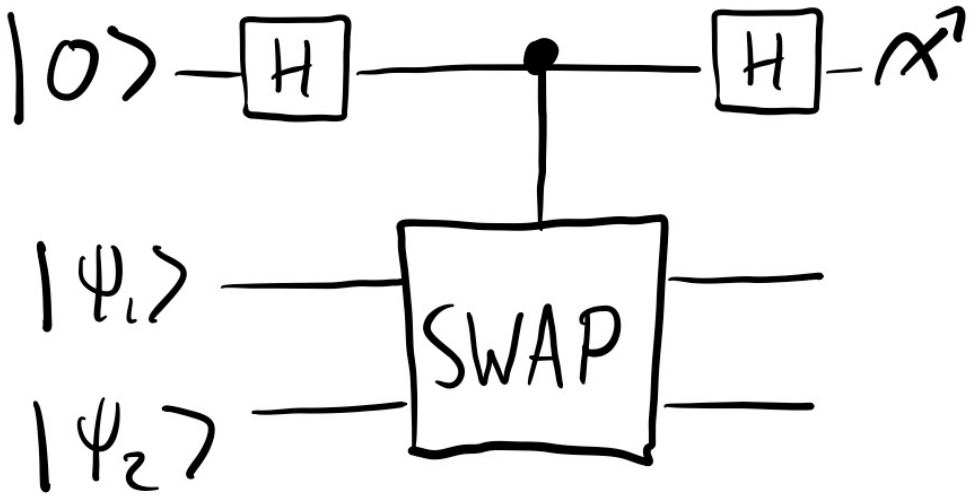


y_1 y_2



$|\psi_1\rangle$ $|\psi_2\rangle$

The SWAP test

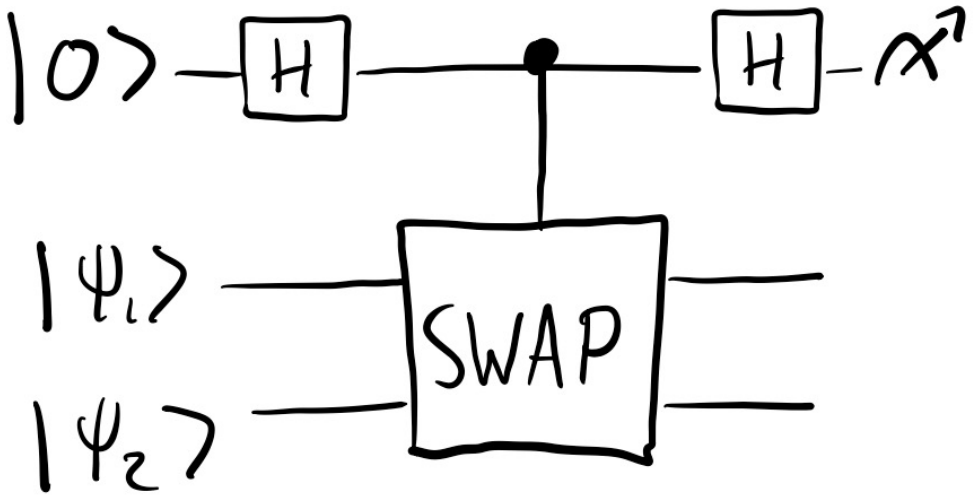


Input	Pr[***measure***$|0\rangle$]
$|\psi\rangle|\psi\rangle$	1
$|\psi\rangle|\psi^{\perp}\rangle$ or $|\psi^{\perp}\rangle|\psi\rangle$	1/2

[Barenco, Berthiaume, Deutsch, Ekert, Jozsa, Macchiavello '97]
[Buhrman, Cleve, Watrous, de Wolf '01]

Optimal test under perfect completeness requirement [Kobayashi, Matsumoto, Yamakami '01]

The SWAP test



$|0\rangle|\psi_1\rangle|\psi_2\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|\psi_1\rangle|\psi_2\rangle + |1\rangle|\psi_1\rangle|\psi_2\rangle) \rightarrow$
$\frac{1}{\sqrt{2}}(|0\rangle|\psi_1\rangle|\psi_2\rangle + |1\rangle|\psi_2\rangle|\psi_1\rangle)$

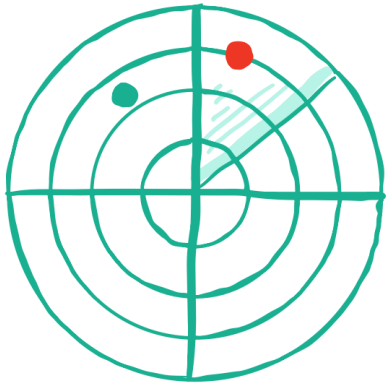
After the final Hadamard we get:
$\frac{1}{2}(|0\rangle(|\psi_1\rangle|\psi_2\rangle + |\psi_2\rangle|\psi_1\rangle)+|1\rangle(|\psi_1\rangle|\psi_2\rangle - |\psi_2\rangle|\psi_1\rangle)$

If the states $|\psi_1\rangle, |\psi_2\rangle$ are equal we always measure 0
Let 0 outcome correspond to answering `=‘, wrong on the non equal inputs if we measure 0

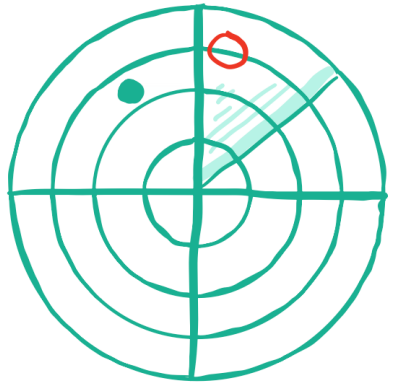
How about n input states?

Types of errors

Type I / false positive / soundness error



Type II / false negative / completeness error



Positive case = all n states are identitical

Average success probability = $p_I \Pr[\textit{success in I}] + p_{II} \Pr[\textit{success in II}]$

We want to maximize this success probability

Perfect completeness means we are always correct on the positive case

Quantum State Identity

Input: n unknown states $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle$ each of local dimension d, pairwise orthogonal or identical

Promise: We have that either

i. All $|\psi_i\rangle$ are identical

ii. We have one of the promises for each of the following problems:

$\mathbf{QSI}_{\mathbf{n}}^{\mathbf{p}}$: there exists an $i, j \in [n]$ such that $|\psi_i\rangle, |\psi_j\rangle$, are pairwise orthogonal

$\widetilde{\mathbf{QSI}}_{\boldsymbol{\mu}}^{\boldsymbol{p}}$: One is given some $\mu \vdash n$ with $\mu_2 > 0$ such that $|\psi_{\sigma(1)}\rangle|\psi_{\sigma(2)}\rangle \dots |\psi_{\sigma(n)}\rangle = U^{\otimes n}|1^{\mu_1}2^{\mu_2} \dots d^{\mu_d}\rangle$ for unknown U and unknown permutation σ

$\mathbf{QSI}_{\mu}^{\mathbf{p}}$: One is given some $\mu \vdash n$ with $\mu_2 > 0$ such that $|\psi_1\rangle|\psi_2\rangle \dots |\psi_n\rangle = U^{\otimes n}|1^{\mu_1}2^{\mu_2} \dots d^{\mu_d}\rangle$ for unknown d-dimensional unitary U

In all problems, case (i) happens with probability p.

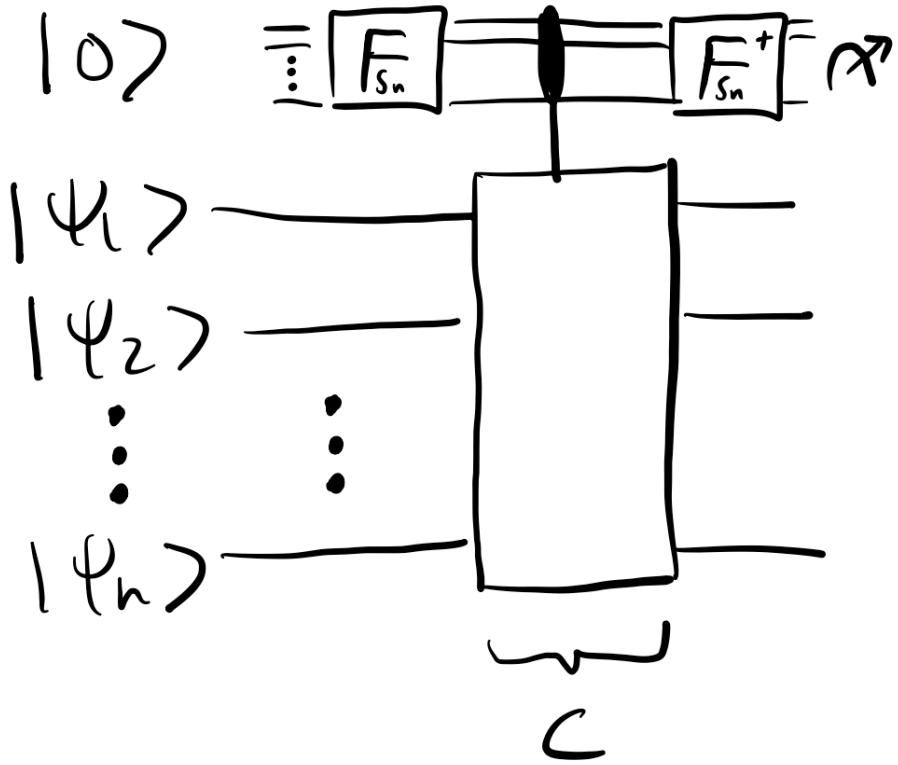
Output: Return "equal" in case (i) and "unequal" in case (ii)

The Permutation Test

[Kada, Nishimura, Yamakami '08]

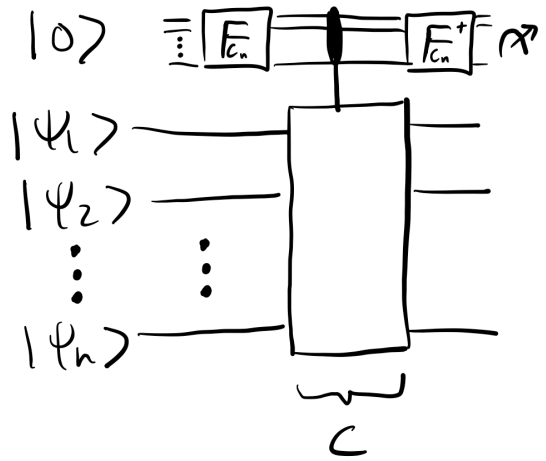
$C: |\sigma\rangle|\psi_1\rangle|\psi_2\rangle \dots |\psi_n\rangle \mapsto |\sigma\rangle|\psi_{\sigma^{-1}(1)}\rangle|\psi_{\sigma^{-1}(2)}\rangle \dots |\psi_{\sigma^{-1}(n)}\rangle$

- Optimal for arbitrary n under the perfect completeness requirement [KNY08]
- Uses QFT on $n \log n$ qubits
- So far optimality was unknown if we relax the perfect completeness requirement



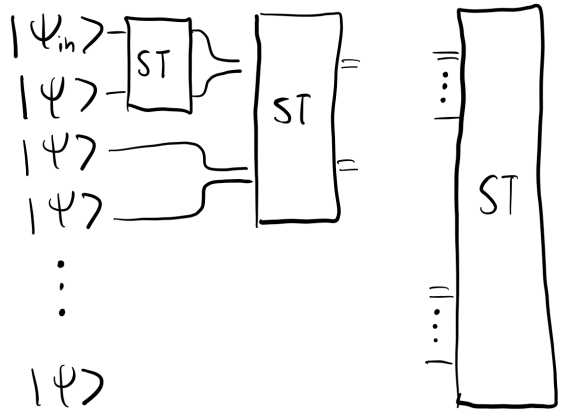
Reducing circuit complexity

Circle test [KNY08]: only cyclic shifts



- Optimal for prime n under perfect completeness requirement
- Achieves $O(1/n)$ error for arbitrary n
- Uses QFT on $\log n$ qubits

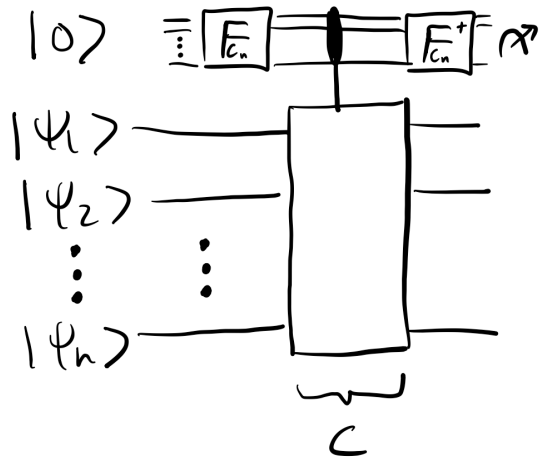
[CDMKJ18]:Iterated SWAP test



- Optimal for arbitrary n when only the first state can be different
- $O(n)$ SWAP tests, no QFT

Reducing circuit complexity

Circle test [KNY08]: only cyclic shifts



- Behaves bad if the input is alternating orthogonal (|01010101⟩), because we create less possible permutations
- Relatively good when inputs are bunched (|00001111⟩)

- Intuitively we want to maximize the number of permutations

Some questions

1) What if one relaxes the perfect completeness requirement? [KNY08]

2) Can one find even simpler approximations based solely on SWAP-tests? [KNY08]

3) What is the underlying mathematical structure that allows one to achieve (near-)optimal performance with simpler tests?

4) What about about performance beyond the worst-case inputs?

The punchline

- There exists an optimal test for QSI for all priors and types of allowed errors: for all ''sensible'' priors, this is in fact the permutation test.

- Key structure is input symmetry, exploit using group theory and representation theory

Permutation groups

Permutation group is a **subgroup** of the symmetric group S_n

Group elements: permutations of the set $\{1,2, \ldots n\}$
Operation: composition of permutations

- S_n has all $n!$ possible permutations
- Cyclic group $C_n \subset S_n$, contains n permutations

Representation theory: represent algebraic objects (such as groups) as linear operators with matrix multiplication preserving the original algebraic operations

The optimal test

Theorem. For all $p \geq p^*$ and for any $\mu \vdash n$ the permutation test is optimal for all quantum state identity problems, achieves perfect completeness and has soundness

$$1 - \frac{1}{\binom{n}{\mu}},$$

where $\binom{n}{\mu} := \frac{n!}{\mu_1! \ldots \mu_n!}$ is a multinomial coefficient and $p^* := \frac{1}{1+\binom{n}{\mu}}$

For all $p < p^*$, the optimal test is to always output "unequal".

Indeed, we recover the SWAP test ($\mathrm{p} = \frac{1}{2}, n = 2, h = 1$):

$$P_{succ}(2,1) = \frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{\binom{2}{1}}\right) = \frac{3}{4}$$

Some conclusions from the Theorem

- Knowing the order does not allow one to achieve a higher success probability
- Relaxing the one-sided error requirement does not increase the average success probability
- The permutation test will perform much better on most inputs than the worst-case instances (those where only one state is different) that have $1/n$ soundness error
    - The number of states that are different makes a big difference in the ability to distinguish between both cases

A 1-page sketch of the proof

Assume that we twirl with respect to the Haar measure.

Write the problem of finding the optimal measurement as an SDP **(P).**

The permutation test is a feasible solution to **(P)** with an objective value f.

We make an educated guess for the solution in the dual SDP **(D),** show that it is feasible with objective value f^* (relies on representation theory and Weingarten calculus).

$f^* = f$, so weak duality implies that the permutation test is optimal for Haar random.

Show that the Haar measure is, in fact, the hardest measure over all inputs

Sketch of the proof for $p = \frac{1}{2}$

$$\rho_{=}^{\mu} := \int U^{\otimes n} |1^n\rangle\langle 1^n| (U^\dagger)^{\otimes n} dU, \quad \rho_{\neq}^{\mu} := \int U^{\otimes n} |1^{\mu_1} 2^{\mu_2} \dots d^{\mu_d}\rangle\langle 1^{\mu_1} 2^{\mu_2} \dots d^{\mu_d}| (U^\dagger)^{\otimes n} dU$$

dU can come from any measure on the unitary group

Primal program (P)

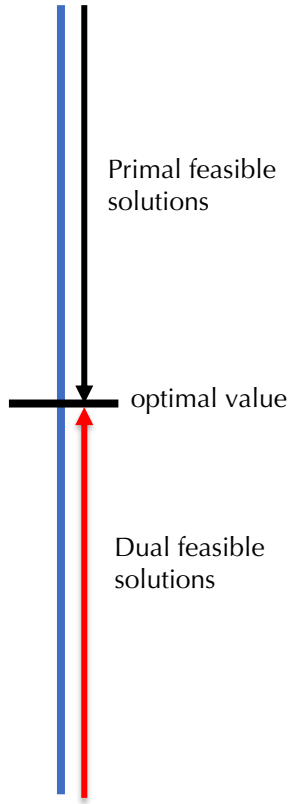
$$\textbf{max} \quad \frac{1}{2}\,\mathrm{Tr}[\Pi_{=}\rho_{=}^{n}] + \frac{1}{2}\mathrm{Tr}[\Pi_{\neq}\rho_{\neq}^{n}]$$

$$\textbf{s.t.} \quad \Pi_{=} + \Pi_{\neq} = \mathbb{I}_{d^n}$$
$$\Pi_{=}, \Pi_{\neq} \succcurlyeq 0$$

Dual program (D)

$$\textbf{min} \quad \mathrm{Tr}[Y]$$

$$\textbf{s.t.} \quad Y - \frac{1}{2}\rho_{=}^{n} \succcurlyeq 0$$
$$Y - \frac{1}{2}\rho_{\neq}^{n} \succcurlyeq 0$$
$$Y \in Herm\left((\mathbb{C}^d)^{\otimes n}\right)$$



Sketch of the proof (iii)

Key lemma: One can write $\rho_{\neq}^{n}$ when using the Haar measure in terms of multinomial coefficients, Kostka numbers and isotypic projectors onto irreps in the tensor representation of the symmetric group

For the symmetric group, all of the above can easily be computed!

This is not the case for any group G

General Statement: the G-test

Arbitrary subgroup $G \subseteq S_n$

G-test measurement $\Pi_= = \Pi_G$ and $\Pi_{\neq} = \mathbb{I} - \Pi_G$, where Π_G is the projector onto the trivial irrep of G

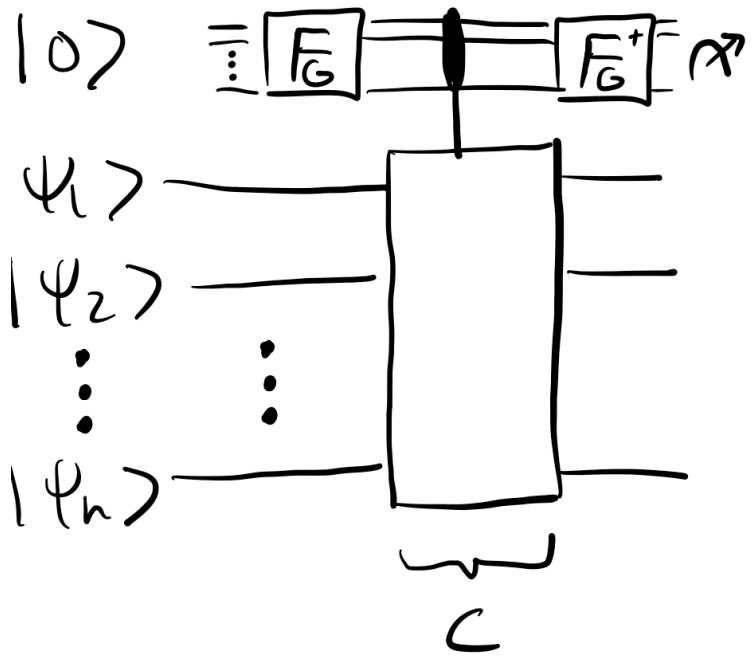
Theorem. The G-test has perfect completeness and soundness

$$1 - \frac{1}{\binom{n}{\mu}} \sum_{\lambda \vdash_d n} K_{\lambda,\mu} r_\lambda^G$$

where

r_λ^G = multiplicity of the trivial irrep of the subgroup $G \subseteq S_n$ inside the irrep λ of the symmetric group S_n.

$K_{\lambda,\mu}$ = Kostka number



Examples

$G = S_n$ — the permutation test ✓

$G = C_n$ — the cycle test ✓

While the following are not known

For $n = 2^m : G = C_2 \wr \cdots \wr C_2$ — the iterated SWAP tree test

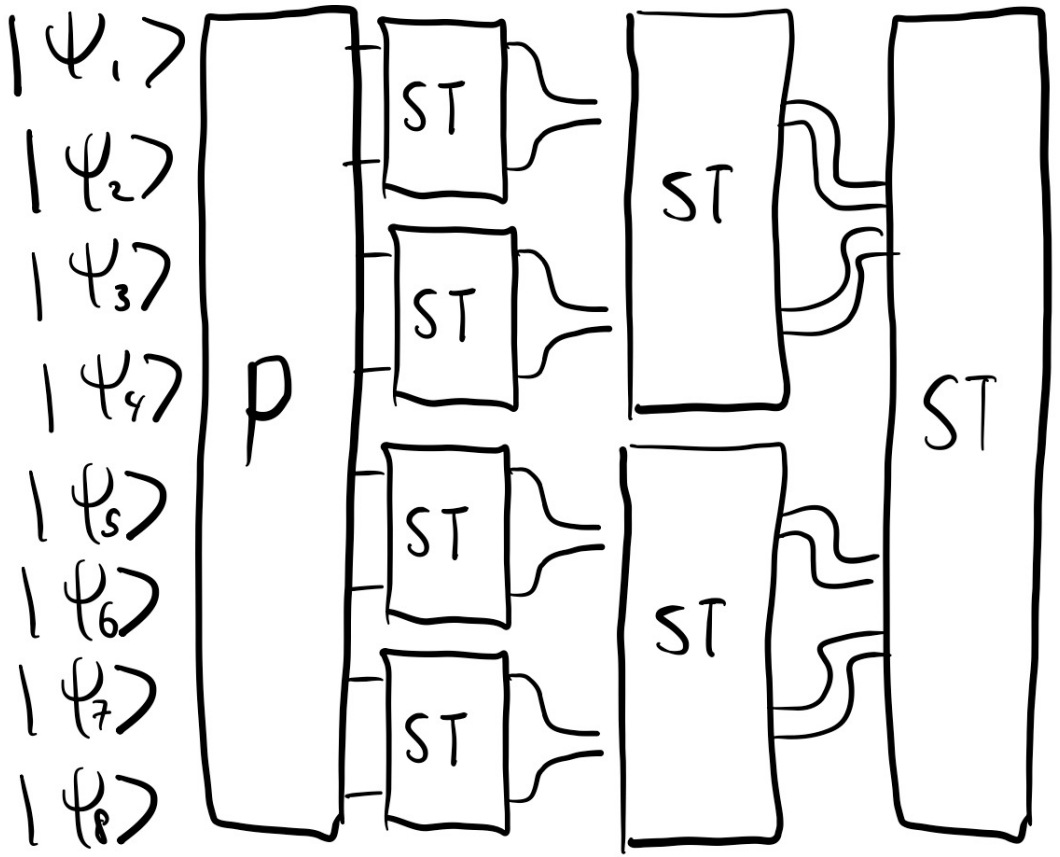
m

The Iterated SWAP Tree

- Uses $n - 1$ SWAP tests
- Only need one ST to measure orthogonal
- Perfect completeness and soundness lower bounded by some recurrence relation which is $1 - 1/n$ on the hardest input for the permutation test (only one state different)
- ”Hardware-friendly” when using **optics-based qc**? [CDM+18]

(Partly) resolves an open question by [KNY08]

How to analyze performance on certain inputs?



Conclusion

- When you know little about your input and have the resources use the Permutation test!
- If you have fewer resources, use restricted G-tests such as the Circle or Iterated Swap Tree
- If you have few resources *and* know more about the input distribution analyze what works best for the case

Open problems

What about an approximate version of QSI?

Can we analyze G-tests for a specific $G \subset S_n$?

Can we find an exact expression for the performance of the Iterated SWAP Tree?

Can we use similar techniques to solve the problem of reconstructing μ

References

[BBD+97] Adriano Barenco, Andre Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of quantum computations by symmetrization. SIAM Journal on Computing, 26(5):1541–1557, 1997.

[BCdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. Physical Review Letters, 87(16), October 2001.

[KMY01] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum certificate verification: Single versus multiple quantum certificates. arXiv preprint quant-ph/0110006, 2001.

[BLW23] Zachary P. Bradshaw, Margarite L. LaBorde, Mark M. Wilde. Cycle Index Polynomials and Generalized Quantum Separability Tests. Proceedings of the Royal Society A, vol. 479, no. 2274, page 20220733 June 2023

[KNY08] Masaru Kada, Harumichi Nishimura, and Tomoyuki Yamakami. The efficiency of quantum identity testing of multiple states. Journal of Physics A: Mathematical and Theoretical, 41(39):395309, 2008

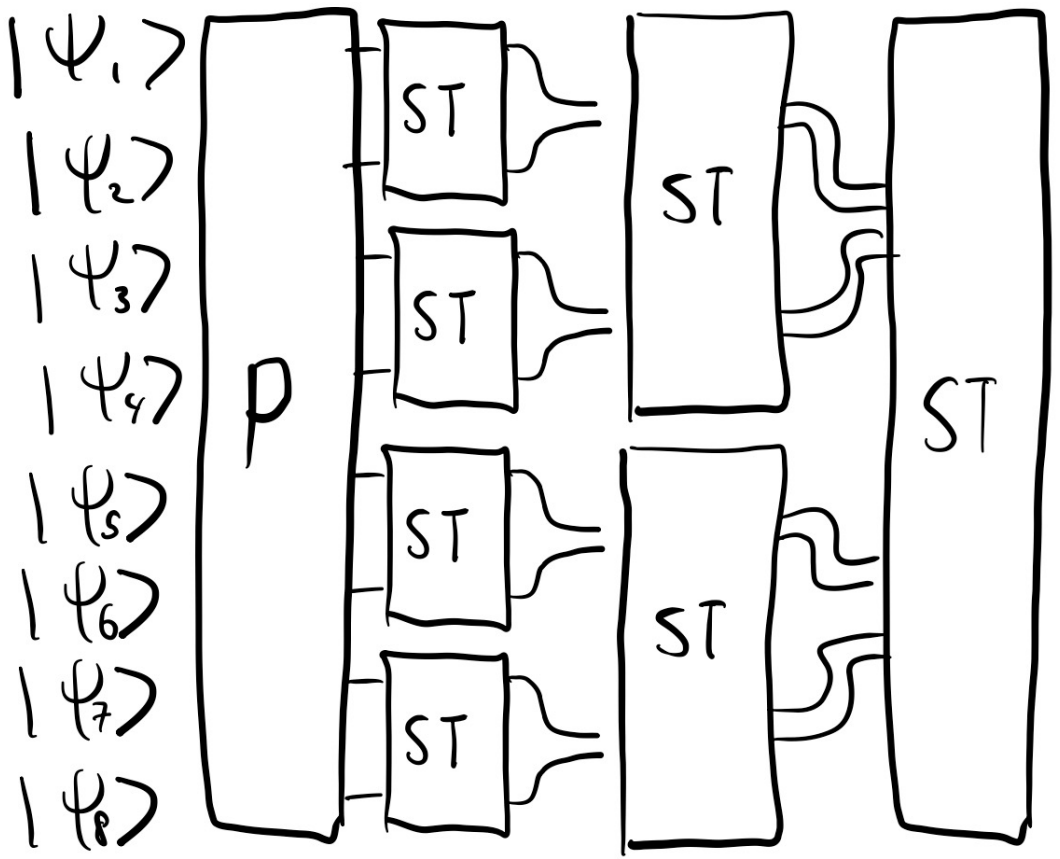
[CDM+18] Ulysse Chabaud, Eleni Diamanti, Damian Markham, Elham Kashefi, and Antoine Joux. Optimal quantum-programmable pro jective measurement with linear optics. Phys. Rev. A, 98:062318, Dec 2018.

Thank you for listening!

The Iterated SWAP Tree

How to analyze performance on certain inputs?

- Can compute the relevant quantities from the G-test to get analytical expression
- No direct method to compute these quantities however
- We propose a different way to compute its performance based on bounding the number of `clicks' when the inputs are orthogonal

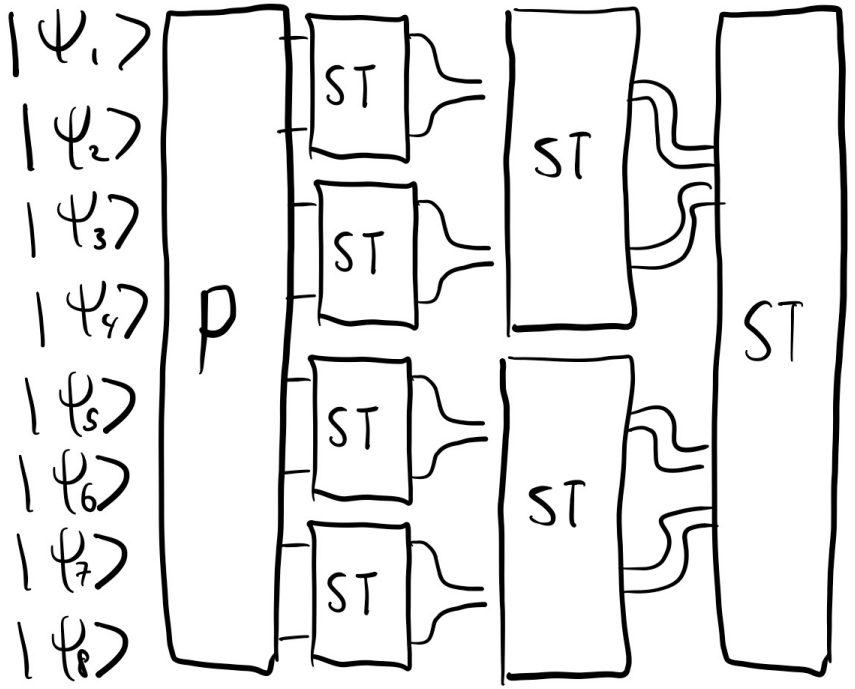


Recursive Upper Bound

Theorem. The soundness probability of the IST for $n = 2^m$ and $h \in [n]$, with the promise that $\mu = (n-h, h)$ is

$$P_s^{IST}(n,h) \geq 1 - \frac{\gamma(h, \log_2(n))}{\binom{n}{h}},$$

where $\gamma(h,m) = \sum_{k=0}^{\lfloor \frac{h}{2} \rfloor} \gamma(k, m-1)\gamma(h-k, m-1)$,
$\gamma(0,m) = \gamma(1,m) = 1 \; for \; all \; m \geq 0$ **and** $\gamma(h,0) = 0$



Idea to lower bound the number of clicks is to compare the number of orthogonal states in two blocks.

- If this is different add 1 to counter, then look at the next blocks.

Note that this does not count *all* cases