Quantum Computation **(CMU 15-859BB, Fall 2015)**

Lecture 21: HSP via the Pretty Good Measurement

November 18, 2015

Lecturer: John Wright *Scribe: Joshua Brakensiek*

1 The Average-Case Model

Recall from Lecture 20 the following problem. Given the mixed state

$$\sigma = \begin{cases} \sigma_1 & \text{with probability } p_1 \\ \sigma_2 & \text{with probability } p_2 \\ & \vdots \\ \sigma_m & \text{with probability } p_m \end{cases}$$

our goal is to correctly identify which of the m states σ is in as often as possible. To do this, we use a POVM

$$E_1 + \cdots + E_m = I,$$

where $E_1, \ldots, E_m$ are positive semi-definite matrices. Upon measuring σ with our POVM, if we yield that measurement $|i\rangle$, then we output "σ_i." For this specific POVM, the success probability is

$$\mathbf{Pr}[\text{success}] = \sum_{i=1}^{m} p_i \cdot \operatorname{tr}(E_i \sigma_i).$$

Since our success probability dependents on the probabilities $p_1, \ldots, p_n$, we call this problem the *Average-Case Model*.

We desire to select the optimal POVM $(E_1, \ldots, E_m)$ so that our probability of success is maximized. Since it is difficult in general to compute the optimal POVM, we use an accurate, elegant approximation, the Pretty Good Measurement (PGM). To compute analyze the success probability of the PGM, we need to understand the *fidelity* of a pair of mixed states.

Definition 1.1. The *fidelity* of two mixed states ρ and σ is

$$F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1,$$

in which $\sqrt{\rho}$ is the matrix with the same eigenvectors as ρ but with square roots of the eigenvalues of ρ (recall that ρ and σ have nonnegative eigenvalues, so this makes sense) and $\|M\|_1$ is the sum of the absolute values of the eigenvalues of M.

Informally, F is a measure of the similarity between two mixed states. In particular, it has the following two useful properties

- $0 \leq F(\rho, \sigma) \leq 1$, and $F(\rho, \sigma) = 1$ if and only if $\rho = \sigma$.
- $1 - F \leq d_{\text{tr}}(\rho, \sigma) \leq \sqrt{1 - F^2}$, in which $d_{\text{tr}}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$.

Note that the later fact implies that if σ and ρ are 'close' (that is, $F(\sigma, \rho) \sim 1$), then $d_{\text{tr}}(\rho, \sigma) \sim 0$. We then have the following bound of the error probability of the PGM. This result was first proved in a weaker for by [BK02] and was later proved in the following form by [AM14].

Theorem 1.2.

$$\mathbf{Pr}[\textit{PGM errs on } \sigma] \leq \frac{1}{2} \sum_{i \neq j} \sqrt{p_i p_j} F(\sigma_i, \sigma_j).$$

Note that if the σ_i's are pairwise similar, the pairwise fidelities will be quite large, implying a poor bound on the error probability of the PGM. This makes intuitive sense since it is much more difficult to distinguish a collection of objects when they look quite similar. Thus, this theorem is most useful when the pairwise fidelities are small. This theorem implies the following corollary.

Corollary 1.3.

$$\mathbf{Pr}[\textit{PGM errs on } \sigma] \leq m \left(\max_{i \neq j} F(\sigma_i, \sigma_j) \right).$$

Proof. Define $F := \max_{i \neq j} F(\sigma_i, \sigma_j)$. Then, from Theorem 1.2

$$\begin{aligned}
\mathbf{Pr}[\text{PGM errs}] &\leq \sum_{i \neq j} \sqrt{p_i p_j} F \\
&\leq F \sum_{i,j} \sqrt{p_i p_j} \\
&= F \left(\sum_{i=1}^{m} \sqrt{p_i} \right)^2 \\
&\leq F \left(\sum_{i=1}^{m} 1 \right) \left(\sum_{i=1}^{m} p_i \right) \quad \text{(Cauchy-Schwarz inequality)} \\
&= mF.
\end{aligned}$$

□

$$\begin{array}{rc}
 & \text{Adv. strategies:} \\
 & \begin{array}{cccc} \sigma_1 & \sigma_2 & \dots & \sigma_m \\ \downarrow & \downarrow & & \downarrow \end{array} \\
\begin{array}{r} \text{Ph. strategies: } \mathcal{E}_j \to \\ \mathcal{E}_k \to \\ \\ \end{array} & \left(\begin{array}{cccc} & \square & & \\ & & & \\ & & & \end{array}\right)
\end{array}$$

Figure 1: A matrix representation of the strategies of the Physicist and the Adversary in the 2-player zero-sum game. Each column represents the mixed state the Adversary may pick and each row represents a POVM the Physicist may pick. Note that this matrix cannot exist ‘in reality’ since there are infinitely many POVMs the Physicist can pick from.

2 The Worst-Case Model

Now, we consider the *Worst-Case Model*. In this case, we are provided with some $\sigma \in \{\sigma_1, \dots, \sigma_m\}$ and we would like to identify the σ_i which σ is with minimal worst-case error probability. For a specific POVM $(E_1, \dots, E_m)$, we defined the probability of success in this model to be

$$\begin{aligned} \mathbf{Pr}[\text{success}] &= \min_i \mathbf{Pr}[\text{guess ``}\sigma_i\text{'' : } \sigma = \sigma_i] \\ &= \min_i \operatorname{tr}(E_i \sigma_i). \end{aligned}$$

Using Corollary 1.3, we can prove the following. This result is due to [HW12].

Corollary 2.1. *There exists a measurement with worst-case success probability at least*

$$1 - m \cdot \max_{i \neq j} F(\sigma_i, \sigma_j).$$

Proof. The prove this result using a 2-player zero-sum game. This game consists of two players a Physicist and an Adversary.

- The Physicist is given $\sigma \in \{\sigma_1, \dots, \sigma_m\}$. His set of strategies are possible POVMs $\mathcal{E} = (E_1, \dots, E_m)$. Her goal is to *maximize* the worst-case success probability.
- The Adversary possible strategies are to pick $\sigma_i \in \{\sigma_1, \dots, \sigma_m\}$. His goal is to minimize the worst-case success probability.

See Figure 1 for a visualization of these strategies. As is typical in zero-sum game, the Physicist and the Adversary do not have to settle on a single strategy. Instead, they can pick a probability distribution of strategies. Let $\mathcal{D}$ be the Physicists probability distribution of POVMs and let $\mathcal{P}$ be the Adversaries probability distribution of states. Both decide on their strategies simultaneously and independent of the other one. For a particular choice $(\mathcal{D}, \mathcal{P})$ we assign a *score* to be

$$\text{score} = \mathop{\mathbf{E}}_{\mathcal{E}\sim\mathcal{D}} \mathop{\mathbf{E}}_{\sigma_i\sim\mathcal{P}} \mathbf{Pr}[\mathcal{E} \text{ succeeds on } \sigma_i].$$

The inner expected value is equal to the average case success probability of $\mathcal{E}$ on the distribution $\mathcal{P}$.

For the Physicist, this capability of selecting a distribution of $\mathcal{D}$ is redundant.

Fact 2.2. *For any distribution $\mathcal{D}$ of POVMs, there exists a POVM $\widetilde{\mathcal{E}} = (\widetilde{E_1}, \ldots, \widetilde{E_m})$ such that for all mixed states σ*

$$\mathop{\mathbf{E}}_{(E_1,\ldots,E_m)\sim\mathcal{D}}[\operatorname{tr}(E_i\sigma)] = \operatorname{tr}(\widetilde{E_i}\sigma).$$

That is, $\widetilde{\mathcal{E}}$ is "equivalent" to $\mathcal{D}$.

Proof. For all $j \in \{1, \ldots, m\}$, let

$$\widetilde{E_i} = \mathop{\mathbf{E}}_{(E_1,\ldots,E_m)\sim\mathcal{D}}[E_i],$$

where the expected value of a random matrix consists of the expected value of each entry. We have that $\widetilde{\mathcal{E}} = (\widetilde{E1i}, \ldots, \widetilde{E_m})$ is a POVM because the expected value of a distribution of positive semidefinite matrices is also positive semidefinite and

$$\begin{aligned} \sum_{i=1}^{m} \widetilde{E_i} &= \sum_{i=1}^{m} \mathop{\mathbf{E}}_{(E_1,\ldots,E_m)\sim\mathcal{D}}[E_i] \\ &= \mathop{\mathbf{E}}_{(E_1,\ldots,E_m)\sim\mathcal{D}}\left[\sum_{i=1}^{m} E_i\right] \\ &= \mathop{\mathbf{E}}_{(E_1,\ldots,E_m)\sim\mathcal{D}}[I] = I. \end{aligned}$$

Since trace and matrix multiplication are linear operators, we have that for all σ

$$\begin{aligned} \operatorname{tr}(\widetilde{E_i}\sigma) &= \operatorname{tr}(\mathop{\mathbf{E}}_{(E_1,\ldots,E_m)\sim\mathcal{D}}[E_i]\sigma) \\ &= \mathop{\mathbf{E}}_{(E_1,\ldots,E_m)\sim\mathcal{D}}[\operatorname{tr}(E_i\sigma)], \end{aligned}$$

as desired. □

If the Adversary's choice of $\mathcal{P}$ is fixed, what POVM should the Physicist chose? She should choose the Pretty Good Measurement! Let $\mathcal{E}$ be the PGM for distribution $\mathcal{P}$ of mixed states. From Corollary 1.3, we have that the score will be

$$\mathbf{Pr}[\mathcal{E} \text{ succeeds on } \mathcal{P}] \geq 1 - m \max_{i\neq j} F(\sigma_i, \sigma_j). \tag{1}$$

Since the choice of $\mathcal{P}$ was fixed, the Adversary can pick the $\mathcal{P}$ which minimized this score. Thus, we have shown that

$$1 - m \max_{i \neq j} F(\sigma_i, \sigma_j) \leq \min_{\mathcal{P}} \max_{\mathcal{E}} \operatorname{score}(\mathcal{E}, \mathcal{P}).$$

By the mini-max theorem for 2-player games [VNM44], we then have that

$$1 - m \max_{i \neq j} F(\sigma_i, \sigma_j) \leq \max_{\mathcal{E}} \min_{\mathcal{P}} \operatorname{score}(\mathcal{E}, \mathcal{P}).$$

Hence, there exists a POVM $\mathcal{E}$ which succeeds with probability at least the RHS of (1) for *any* $\mathcal{P}$. In particular, consider the distributions $\mathcal{P}_i$, $i \in \{1, \dots, m\}$, which always outputs σ_i. The worst-case success probability of $\mathcal{E}$ is equal to the minimum of the success probabilities of $\mathcal{E}$ on the $\mathcal{P}_i$'s. Thus, the worst-case success probability is bounded from below by the RHS of (1), as desired. □

3 Application of PGM to HSP

We now use the Pretty Good Measurement to devise a polylogarithmic quantum query algorithm for the Hidden Subgroup Problem. Recall the following details of the HSP.

- Let G be a group. You are given quantum query access to $f : G \to [M]$, where $f(g_1) = f(g_2)$ if and only if $g_1 H = g_2 H$, where H is an unspecified subgroup of G.
- We had constructed a quantum circuit which, after a partial measurement, produces the state
$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle.$$
where $g \in G$ is chosen uniformly at random. In fact, this is equivalent to the mixed state
$$\rho_H = \frac{1}{|G|} \sum_{g \in G} |gH\rangle\langle gH|.$$
- The HSP problem is then, given ρ_H, determine H.

Previously, we had seen that numerous important problems can be reduced to HSP, including factoring, graph isomorphism, and the shortest vector problem. Now, we show that each of these problems has a polylogarithmic quantum query algorithm. This result was originally proved by [EHK04].

Theorem 3.1. *There is a query-efficient algorithm ($q = \operatorname{polylog} |G|$ queries) for the HSP on any group G.*

Proof. We can reduce this problem to worst-case discrimination of the states $\{\rho_H\}_{H\leq G}$. If H is our hidden subgroup, we can create the mixed state ρ_H using only one oracle query. We would like to pick a POVM to discriminate among these mixed states using the Pretty Good Measurement. In order to use Corollary 2.1 to bound the worst-case error probability, we need to determine the following two quantities.

- The number of subgroups of G, which we denote by m.
- The maximum fidelity of pairs of mixed states: $\max\limits_{H\neq H'} F(\rho_H, \rho_{H'})$.

We now bound both of these quantities. Proofs of these facts are relegated to the end of the notes.

Fact 3.2.

$$m \leq 2^{\log^2 |G|}.$$

That is, m is *quasipolynomial* in the size of G.

Fact 3.3.

$$\max_{H\neq H'} F(\rho_H, \rho_{H'}) \leq \sqrt{\frac{3}{4}} < .9.$$

Applying Corollary 2.1, we obtain that success probability is at least $1 - 2^{\log^2 |G|} \cdot .9$, which is less than zero when G is not the trivial group! It makes sense though that this attempt failed because we have only queried our oracle once.

The key to achieving a nontrivial success probability is to perform this coset sampling $n \approx \text{polylog}\,|G|$ times in parallel. If H is our hidden subgroup, we can then produce that mixed state $\rho_H \otimes \rho_H \otimes \cdots \otimes \rho_H = \rho_H^{\otimes n}$ using only n quantum queries. Thus, we have turned the problem into worst-case mixed state discrimination of the set $\{\rho_H^{\otimes n}\}_{H\leq G}$. Intuitively, this repetition should help us since if ρ_H and $\rho_{H'}$ have some differences, then $\rho_H^{\otimes n}$ and $\rho_{H'}^{\otimes n}$ should amplify those differences. We formalize this intuition with the following fact.

Fact 3.4. *For all mixed states $\rho, \sigma \in \mathbb{C}^{d\times d}$,*

$$F(\rho^{\otimes n}, \sigma^{\otimes n}) = F(\rho, \sigma)^n.$$

From Facts 3.3 and 3.4 we have that

$$\max_{H\neq H'} F(\rho_H^{\otimes n}, \rho_{H'}^{\otimes n}) < .9^n.$$

Therefore, by Corollary 2.1,

$$\begin{aligned}\mathbf{Pr}[\mathit{success}] &\geq 1 - 2^{\log^2 |G|} \cdot (.9)^n \\ &\geq \frac{1}{2} \text{ when } n = \Theta(\log^2 |G|).\end{aligned}$$

Since our algorithm has the number of queries q equal to n, our algorithm uses polylogarithmically many queries, as desired. □

Remark 3.5. Our use of n tensored copies of the mixed state ρ_H is *not* equivalent to performing the PGM on the single mixed state n times. The correlations the PGM exploited were crucial in obtaining a polylogarithmic number of queries.

Now we provide proofs of the unproven facts.

Proof of Fact 3.2. Let H be an arbitrary subgroup of G and let $\{h_1, \ldots, h_k\}$ be a set of generators of H for which k is minimal. We claim that $k \leq \log_2 |G|$ for all k. To see this, consider the sequence of groups

$$H_0 = \{e\}, H_1 = \text{span}\{h_1\}, H_2 = \text{span}\{h_1, h_2\}, \ldots, H_k = \text{span}\{h_1, \ldots, h_k\} = H.$$

For all $i \in \{0, \ldots, k-1\}$, we have that H_i is a strict subgroup of H_{i+1}. Otherwise, if $H_i = H_{i+1}$, h_{i+1} could be removed from the generators of H, violating minimality of k. Thus, by Lagrange's theorem, $|H_{i+1}|$ is a multiple of $|H_i|$ but must be strictly larger than $|H_i|$. Thus, $|H_{i+1}| \geq 2|H_i|$ for all $i \in \{0, \ldots, k-1\}$. Since $|H_0| = 1$, we have that $|H| = |H_k| \geq 2^k$, implying that $|G| \geq 2^k$, or $\log_2 |G| \geq k$, as desired.

Thus, every subgroup of G can be specified by at most $\log_2 |G|$ generators. In fact, by padding the generating set with copies of the identity element, every subgroup of G can be specified by exactly $\lfloor \log_2 |G| \rfloor$ generators. Since there are $|G|$ choices for each generator, there are at most

$$m \leq |G|^{\lfloor \log_2 |G| \rfloor} \leq 2^{\log^2 |G|}$$

subgroups. □

Remark 3.6. The bound obtained is essentially tight up to constant factors in the exponent. For example, consider the Cartesian product of n copies of the cyclic group $\mathbb{Z}_2$.

Proof of Fact 3.3. Consider any pair $H \neq H'$ of subgroups. To upper bound the fidelity of ρ_H, $\rho_{H'}$, how similar they are, it suffices to lower bound how different they are, their trace distance. Recall that

$$d_{\text{tr}}(\rho_H, \rho_{H'}) \leq \sqrt{1 - F(\rho_H, \rho_{H'})^2}$$

which is equivalent to

$$F(\rho_H, \rho_{H'}) \leq \sqrt{1 - d_{\text{tr}}(\rho_H, \rho_{H'})^2}.$$

Thus, to upper bound the fidelity by $\sqrt{3/4}$, it suffices to lower bound the trace distance by $1/2$. To bound the trace distance, we use a result from Lecture 17 on distinguishing two mixed states in the average-case model. Specifically, consider

$$\rho = \begin{cases} \rho_H & \text{with probability } 1/2 \\ \rho_{H'} & \text{with probability } 1/2 \end{cases}.$$

We showed that the optimal success probability of distinguishing these two states is equal to

$$\frac{1}{2} + \frac{1}{2} d_{\text{tr}}(\rho_H, \rho_{H'}).$$

Thus, to lower bound the trace distance by 1/2, it suffices to give an algorithm which distinguishes the two states with probability at least 3/4.

We now construct a POVM which succeeds with probability at least 3/4. In lecture 20, a key motivation for the PGM is that close-to-optimal POVMs often use a family of PSD matrices quite similar to the mixed states they are trying to distinguish. We strive for something similar (but easier to reason about in our construction). Assume without loss of generality that $|H| \geq |H'|$. Let $\Pi_H = \frac{|G|}{|H|}\rho_H$. We then have our POVM be $(\Pi_H, I - \Pi_H)$, where the first matrix corresponds to measuring 'ρ_H' and the latter matrix corresponds to measuring '$\rho_{H'}$.' We now need to show that we have constructed a valid POVM and that the success probability is at least 3/4.

To establish that $(\Pi_H, I-\Pi_H)$ is a valid POVM, it suffices to show that Π_H is a projection matrix. The simplest way to reason about Π_H is to note that is equals

$$\frac{1}{|H|}\sum_{g\in G}|gH\rangle\langle gH| = \frac{|H|}{|H|}\sum_{C\text{: }H\text{-coset of }G}|C\rangle\langle C|$$

since each H-coset has $|H|$ elements. Note that the set of H-coset states are orthonormal since each element of G appears in exactly one coset. Hence, we have that Π_H is then a projection matrix. Thus, $I - \Pi_H$ is also a projection matrix, so we have a valid POVM.

Next, we bound the success probability of this particular POVM. This success probability equals

$$\begin{aligned}\mathbf{Pr}[\text{success}] &= \frac{1}{2}\operatorname{tr}(\Pi_H\rho_H) + \frac{1}{2}\operatorname{tr}((I-\Pi_H)\rho_{H'}) \\ &= \frac{1}{2}\operatorname{tr}(\rho_H)\ (\Pi_H \text{ is a projection onto the nontrivial eigenvectors of } \rho_H) \\ &\quad + \frac{1}{2}\operatorname{tr}(\rho_{H'}) - \frac{1}{2}\operatorname{tr}(\Pi_H\rho_{H'}) \\ &= 1 - \frac{|G|}{2|H|}\operatorname{tr}(\rho_H\rho_{H'}).\end{aligned}$$

Now, observe that

$$\begin{aligned}\frac{|G|}{2|H|}\operatorname{tr}(\rho_H\rho_{H'}) &= \frac{|G|}{2|H|}\operatorname{tr}\left[\left(\frac{1}{|G|}\sum_{g\in G}|gH\rangle\langle gH|\right)\left(\frac{1}{|G|}\sum_{g\in G}|gH'\rangle\langle gH'|\right)\right] \\ &= \frac{1}{2|G||H|}\sum_{g,g'\in G}\operatorname{tr}(|gH\rangle\langle gH|g'H'\rangle\langle g'H'|) \\ &= \frac{1}{2|G||H|}\sum_{g,g'\in G}\operatorname{tr}(\langle gH|g'H'\rangle\langle g'H'|gH\rangle) \\ &= \frac{1}{2|G||H|}\sum_{g,g'\in G}|\langle gH|g'H'\rangle|^2\end{aligned}$$

Since we defined $|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle$, it is easy to see that $\langle gH | g'H' \rangle = \frac{|gH \cap g'H'|}{\sqrt{HH'}}$. Thus, we have that

$$\begin{aligned}
\frac{|G|}{2|H|} \operatorname{tr}(\rho_H \rho_{H'}) &= \frac{1}{2|G||H|^2|H'|} \sum_{g,g' \in G} |gH \cap g'H'|^2 \\
&= \frac{1}{2|G||H|} \sum_{C:H\text{-coset}} \sum_{C':H'\text{-coset}} |C \cap C'|^2 \\
&= \frac{1}{2|G||H|} \sum_{C:H\text{-coset}} \sum_{C':H'\text{-coset}} \sum_{g \in C \cap C', g' \in C \cap C'} 1 \\
&= \frac{1}{2|G||H|} \sum_{g,g' \in G} \mathbf{1}[\exists\ H\text{-coset } C \text{ and } H'\text{-coset } C' \text{ such that } g, g' \in C \cap C'] \\
&= \frac{1}{2|G||H|} \sum_{g \in G} \sum_{g' \in G} \mathbf{1}[g'g^{-1} \in H \cap H'] \\
&= \frac{1}{2|G||H|} \sum_{g \in G} |H \cap H'| \\
&= \frac{|H \cap H'|}{2|H|}.
\end{aligned}$$

Since $H \neq H'$ and $|H| \geq |H'|$, we have that $H \cap H'$ is a strict subgroup of H. Thus, $|H| \geq 2|H \cap H'|$. This implies that

$$\frac{|G|}{2|H|} \operatorname{tr}(\rho_H \rho_{H'}) \leq \frac{1}{4}.$$

Thus, the probability of success is at least $\frac{3}{4}$, yielding that the trace distance is at least $\frac{1}{2}$, so the fidelity is at most $\sqrt{\frac{3}{4}}$, as desired. □

Proof of Fact 3.4. Recall that $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$, in which $\sqrt{\rho}$ and $\sqrt{\sigma}$ have the same eigenvectors as ρ and σ, respectively, but with the squareroots of the eigenvalues (mixed states are PSD and thus have nonnegative eigenvalues). Now we seek to show that the tensoring and square root operations are commutative.

Claim 3.7. *For all mixed states ρ, $\sqrt{\rho^{\otimes n}} = \sqrt{\rho}^{\otimes n}$.*

Proof. Since the matrices are Hermitian, it suffices to show that both matrices have identical eigenvalues and eigenvectors. Let $|v_i\rangle, i \in \{1, \ldots, d\}$ be the eigenvectors of ρ and let σ_i be the corresponding eigenvalues. The following table summarizes the eigenvectors and eigenvalues of relevant matrices.

matrix	eigenvectors	eigenvalues
ρ	$\lvert v_i\rangle$	λ_i
$\rho^{\otimes n}$	$\lvert v_{i_1}\rangle \otimes \cdots \otimes \lvert v_{i_n}\rangle$	$\lambda_{i_1} \cdots \lambda_{i_n}$
$\sqrt{\rho}$	$\lvert v_i\rangle$	$\sqrt{\lambda_i}$
$\sqrt{\rho}^{\otimes n}$	$\lvert v_{i_1}\rangle \otimes \cdots \otimes \lvert v_{i_n}\rangle$	$\sqrt{\lambda_{i_1}} \cdots \sqrt{\lambda_{i_n}}$
$\sqrt{\rho^{\otimes n}}$	$\lvert v_{i_1}\rangle \otimes \cdots \otimes \lvert v_{i_n}\rangle$	$\sqrt{\lambda_{i_1} \cdots \lambda_{i_n}}$

We can now see that $\sqrt{\rho}^{\otimes n}$ and $\sqrt{\rho^{\otimes n}}$ have identical eigenvectors and eigenvalues. Thus, they are equal, as desired. □

Since we have that the eigenvalues of $\rho^{\otimes n}$ are the products of all n-tuples of eigenvalues of ρ, we have that $\|\rho^{\otimes n}\|_1 = \|\rho\|_1^n$. Applying this fact and the Claim, we have that

$$\begin{aligned} F(\rho^{\otimes n}, \sigma^{\otimes n}) &= \|\sqrt{\rho^{\otimes n}}\sqrt{\sigma^{\otimes n}}\|_1 \\ &= \|\sqrt{\rho}^{\otimes n}\sqrt{\sigma}^{\otimes n}\|_1 \\ &= \|(\sqrt{\rho}\sqrt{\sigma})^{\otimes n}\|_1 \\ &= \|\sqrt{\rho}\sqrt{\sigma}\|_1^n \\ &= F(\rho, \sigma)^n, \end{aligned}$$

as desired. □

References

[AM14] Koenraad MR Audenaert and Milán Mosonyi. Upper bounds on the error probabilities and asymptotic error exponents in quantum multiple state discrimination. *Journal of Mathematical Physics*, 55(10):102201, 2014.

[BK02] Howard Barnum and Emanuel Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *Journal of Mathematical Physics*, 43(5):2097–2106, 2002.

[EHK04] Mark Ettinger, Peter Høyer, and Emanuel Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Information Processing Letters*, 91(1):43–48, 2004.

[HW12] Aram W Harrow and Andreas Winter. How many copies are needed for state discrimination? *Information Theory, IEEE Transactions on*, 58(1):1–2, 2012.

[VNM44] John Von Neumann and Oskar Morgenstern. *Theory of games and economic behavior.* Princeton university press, 1944.