The General Quantum Duality of Mapping and Distinguishing for Representations of Groups

John Bostanci[1] and Barak Nehoran[2]

[1]Columbia University, New York, NY, USA
[2]Princeton University, Princeton, NJ, USA

Tentative Working Abstract

Aaronson, Atia, and Susskind [AAS20] showed that the ability to efficiently map between two quantum states $|\psi\rangle$ and $|\phi\rangle$ is computationally equivalent to that of distinguishing between their two superpositions $\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$ and $\frac{1}{\sqrt{2}}(|\psi\rangle - |\phi\rangle)$. We argue that this is in fact a manifestation of a wider principle in quantum computation wherein the ability to map between quantum states in one basis is equivalent to that of distinguishing states in a complementary basis. In its most general form, it states that for any given group, the ability to implement a unitary representation of the group is computationally equivalent to the ability to perform a handling measurement on the subspaces of its irreducible representations. As an application of this duality, we generalize Zhandry's quantum money construction from Abelian group actions [Zha24] to non-Abelian groups. We also give the first plain model candidate construction of quantum states that are efficiently clonable but not efficiently telegraphable, a problem left open by [NZ23].

1 Preliminaries

Definition 1.1. *A* coherent trapdoor measurement *[[Barak: tentative name]] on a basis* $\{|\psi_i\rangle\}_{i\in[k]}$ *is an isometry of the form*

$$U : |\psi_i\rangle |0\rangle \mapsto |\phi\rangle |i\rangle$$

for any state $|\phi\rangle$ *which does not depend on* i*, and which may not be efficiently constructable.*

This transforms the information encoded in this basis into the standard basis, and allows inverting if we have the trapdoor state $|\phi\rangle$.

If the trapdoor state is efficiently constructable, this is equivalent to the special case of a change of basis $V : |\psi_i\rangle \mapsto |i\rangle$ which maps directly into the standard basis. However, when $|\phi\rangle$ is not efficiently constructible, this allows performing V only in one direction unless we also have access to $|\phi\rangle$.

Remark 1.2. *Compare this with a projective measurement, which can be written as*

$$W : |\psi_i\rangle |0\rangle \mapsto |\psi_i\rangle |i\rangle$$

A coherent trapdoor measurement is stronger than a projective measurement. That is, given a coherent trapdoor measurement , U, we can perform a projective measurement by applying U, copying the i register to an ancilla, and then applying $U^\dagger$. However, there is no general way to "uncompute" the first register in the projective measurement in order to make it a coherent trapdoor measurement .

2 Duality Theorem

Theorem 2.1. *Let G be a finite group with an efficient quantum Fourier transform. Let $\mathcal{F} : G \to \mathrm{U}(\mathcal{H})$ be a unitary representation of G. Then the following are equivalent:*

1. *There exists a quantum circuit of size s that implements the representation $\mathcal{F}$. That is, given g, the circuit implements the unitary $\mathcal{F}(g)$.*

2. *There exists a quantum circuit of size s' that implements a coarse projective measurement onto the subspaces given by the decomposition of $\mathcal{F}$ into its irreducible representations, and a coherent trapdoor measurement within each irreducible representation.*

Remark 2.2. *In the special case in which the group is Abelian, all the irreducible representations are 1-dimensional, and the second item above simplifies to a full projective measurement in the Fourier basis.*

Remark 2.3. *The duality theorem of [AAS20] is the special case in which $G \cong \mathbb{Z}_2$.*

Proof of Theorem 2.1.

1 ⇒ 2: Suppose that Item 1 is true. That is, we have a circuit of size s that implements the representation $\mathcal{F}$. Let $\varrho : G \to U(\mathcal{H})$ be an irrep of G of dimension d_ϱ, and let $V_1^\varrho, \ldots, V_m^\varrho$ be the copies of the irrep in $\mathcal{F}$ (the subspaces on which $\mathcal{F}$ acts as ϱ). For each subspace V_i^ϱ, take some basis for the subspace and let $|\psi_{ij}^\varrho\rangle$ be the jth basis state.

Suppose we have a basis state $|\psi_{ij}^\varrho\rangle$ that we want to measure.

We prepare the state $\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle$ in an ancilla register and then, controlled on that register, apply $\mathcal{F}(g)$ to our state.

$$\begin{aligned}
&\frac{1}{\sqrt{|G|}}\sum_{g\in G}\mathcal{F}(g)\,|\psi_{ij}^\varrho\rangle\otimes|g\rangle\\
&=\frac{1}{\sqrt{|G|}}\sum_{g\in G}\sum_k \varrho(g)_{kj}\,|\psi_{ik}^\varrho\rangle\otimes|g\rangle\\
&=\sum_k|\psi_{ik}^\varrho\rangle\otimes\frac{1}{\sqrt{|G|}}\sum_{g\in G}\varrho(g)_{kj}\,|g\rangle\\
&=\frac{1}{\sqrt{d_\varrho}}\sum_k|\psi_{ik}^\varrho\rangle\otimes|\mathcal{R}_{kj}^\varrho\rangle
\end{aligned}$$

where $|\mathcal{R}_{kj}^\varrho\rangle$ is the jth basis vector of the kth copy of the irrep ϱ in the right regular representation of G.

If we now perform a quantum Fourier transform on the second register, we get

$$\begin{aligned}
&\frac{1}{\sqrt{d_\varrho}}\sum_k|\psi_{ik}^\varrho\rangle\otimes|\varrho,k,j\rangle\\
&=\left(\frac{1}{\sqrt{d_\varrho}}\sum_k|\psi_{ik}^\varrho\rangle\otimes|\varrho,k\rangle\right)|j\rangle
\end{aligned}$$

If we measure the register containing ϱ, we get the label of the irrep containing our state. Note that within subspace V_i^ϱ, this is a coherent trapdoor measurement that extracts out j and leaves behind the trapdoor state $\frac{1}{\sqrt{d_\varrho}}\sum_k|\psi_{ik}^\varrho\rangle\otimes|\varrho,k\rangle$.

2 ⇒ 1: Suppose that Item 2 is true. Then we have a hybrid measurement that projects onto the union of the supbspaces $V_1^\varrho, \ldots, V_m^\varrho$, and a coherent trapdoor measurement that extracts j.

$$\mathcal{M} : |\psi_{ij}^\varrho\rangle \mapsto |\phi_i^\varrho\rangle\otimes|\varrho\rangle\,|j\rangle$$

Let $|\psi\rangle = \sum_{\varrho,i,j}\alpha_{ij}^\varrho\,|\psi_{ij}^\varrho\rangle$ be the state on which we would like to perform $\mathcal{F}(g)$.

We start by applying $\mathcal{M}$ to get

$$\mathcal{M}\,|\psi\rangle = \sum_{\varrho\in\hat{G},i\in[d_\varrho],j\in[d_\varrho]}\alpha_{ij}^\varrho\,|\phi_i^\varrho\rangle\otimes|\varrho\rangle\,|j\rangle$$

Now, controlled on the label containing the irrep label ϱ, apply $\varrho(g)$ to the j register, producing

$$\begin{aligned}
&\sum_{\varrho\in\hat{G},i\in[d_\varrho],j\in[d_\varrho]} \alpha_{ij}^{\varrho} \left|\phi_i^{\varrho}\right\rangle \otimes \left|\varrho\right\rangle \varrho(g) \left|j\right\rangle \\
&= \sum_{\varrho\in\hat{G},i\in[d_\varrho],j\in[d_\varrho]} \alpha_{ij}^{\varrho} \left|\phi_i^{\varrho}\right\rangle \otimes \sum_{k\in[d_\varrho]} \left|\varrho\right\rangle \varrho(g)_{kj} \left|k\right\rangle \\
&= \sum_{\varrho\in\hat{G},i\in[d_\varrho],j\in[d_\varrho]} \alpha_{ij}^{\varrho} \sum_{k\in[d_\varrho]} \varrho(g)_{kj} \left|\phi_i^{\varrho}\right\rangle \otimes \left|\varrho\right\rangle \left|k\right\rangle
\end{aligned}$$

We now perform $\mathcal{M}^\dagger$ to get

$$\begin{aligned}
&\sum_{\varrho\in\hat{G},i\in[d_\varrho],j\in[d_\varrho]} \alpha_{ij}^{\varrho} \sum_{k\in[d_\varrho]} \varrho(g)_{kj} \left|\psi_{ik}^{\varrho}\right\rangle \\
&= \sum_{\varrho\in\hat{G},i\in[d_\varrho],j\in[d_\varrho]} \alpha_{ij}^{\varrho} \ \mathcal{F}(g) \left|\psi_{ij}^{\varrho}\right\rangle \\
&= \mathcal{F}(g) \sum_{\varrho\in\hat{G},i\in[d_\varrho],j\in[d_\varrho]} \alpha_{ij}^{\varrho} \left|\psi_{ij}^{\varrho}\right\rangle \\
&= \mathcal{F}(g) \left|\psi\right\rangle
\end{aligned}$$

We can see that this successfully implements the representation $\mathcal{F}(g)$. □

2.1 Approximate Case

We show that the duality theorem also holds in the approximate case, in which Item 1 and Item 2 hold only approximately, up to some error.

3 Applications

3.1 Quantum Money From Non-Abelian Group Actions

We generalize the quantum money / lightning of [Zha24] to general group actions. The following is an informal sketch of the generalization:

3.1.1 The construction

Suppose we have a group G with an efficient quantum Fourier transform for which each irrep ϱ of G has size at most $d_\varrho \leq \sqrt{|G|} \cdot \mathsf{negl}(\log(|G|))$. [[Barak: Would the symmetric group S_n satisfy this?]]

Let $* : G \times X \to X$ be a group action of G on set X, and let $x \in X$ be a starting element in the set.

Minting. We start by preparing the uniform superposition over the group (which can be done by taking the inverse Fourier transform of the trivial irrep label). We then apply the group action in superposition onto the starting element $x \in X$.

$$\frac{1}{\sqrt{|G|}} \sum_{g\in G} \left|g\right\rangle \left|g * x\right\rangle$$

We then perform a Fourier transform on the first register and measure the resulting irrep. We get irrep ϱ with probability $p_\varrho = \frac{d_\varrho^2}{|G|} \leq \mathsf{negl}(\log(|G|))$, and the resulting state is

$$\left|\$_{ij}^{\varrho}\right\rangle = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \varrho\left(g^{-1}\right)_{ij} \left|g * x\right\rangle$$

for some $i, j \in [d_\varrho]$.

Output the irrep label ϱ as the serial number and $|\$^\varrho_{ij}\rangle$ as the quantum money state.

Verification. To verify, do essentially the same process, but starting with the claimed banknote in the second register, rather than $|x\rangle$. Accept if the measurement produces the correct irrep label. If the verified state is valid, the resulting state will be of the form $|\$^\varrho_{ij'}\rangle$ for possibly a different $j' \in [d_\varrho]$, but we can then uncompute to return the original state.

3.1.2 Security

The assumption. We show security under the assumption that the following problem is hard

Inputs:
- A group G, satisfying the requirements above, with a list of generators $a_1, \ldots, a_k$ for the group, with a group action $*$ of G on set X, and a starting element $x \in X$.
- A black box word W_{w^2}, which when given a list of generators $a'_1, \ldots, a'_k \in G$ and $x' \in X$, performs the group action of the square of some word $w(a'_1, \ldots, a'_k)$ on the generators.
- an element $y \in X$

Goal: Accept if $y = w(a_1, \ldots, a_k) * x$ and reject otherwise.

We base security on the assumption that it is computationally hard to decide this problem by making only a single query to the black box.

Remark 3.1. *Note that this problem is information-theoretically possible to solve with just a single query to the black box. In particular, if the discrete logarithm problem on the group action is easy, then it is possible to recover $w(a_1, \ldots, a_k)$ from y. We can then compute $w^2(a_1, \ldots, a_k) * x$ and compare to the the action of the black box. This means in particular that the assumption implies that the discrete logarithm of the group action is computationally hard.*

Main Idea. We follow the format of [Zha24], with two main modifications: First, in the reduction we will need to allow w^2 to commute past g, the summation index which runs over the full group. This is taken for granted in [Zha24] as the group there is always Abelian, but this is not in general possible in the non-Abelian case. We get around this issue by amending the group action to include the list of generators $a_1, \ldots, a_k$ and conjugating them by the summation index as $ga_1g^{-1}, \ldots, ga_kg^{-1}$. Then, for each g, the corresponding word produced by the conjugated generators is the original word, but conjugated by g.

The second issue comes from having multidimensional irreps. This comes into play when performing a swap test on two valid quantum money states. If the valid quantum money states are not unique, but rather come from a larger subspace, then it is not clear how to compare two orthogonal states in the same subspace. To get around this issue, we use the fact that we can perform a coherent trapdoor measurement on the subspace and then run a swap test on the resulting trapdoor states.

References

[AAS20] Scott Aaronson, Yosi Atia, and Leonard Susskind. On the hardness of detecting macroscopic superpositions, 2020.

[GH16] W. T. Gowers and O. Hatami. Inverse and stability theorems for approximate representations of finite groups, 2016.

[NZ23] Barak Nehoran and Mark Zhandry. A computational separation between quantum no-cloning and no-telegraphing. In *ITCS 2024*, 2023.

[Zha24] Mark Zhandry. Quantum money from abelian group actions. In *ITCS 2024*, 2024. https://eprint.iacr.org/2023/1097.