On the Query Complexity of Perfect Gate Discrimination

Giulio Chiribella[1], Giacomo Mauro D'Ariano[2], and Martin Roetteler[3]

1 **Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University**
Beijing, 100084, China
gchiribella@mail.tsinghua.edu.cn
2 **QUIT group, Dipartimento di Fisica "A. Volta", INFN Sezione di Pavia, via Bassi 6, 27100 Pavia, Italy**
3 **NEC Laboratories America Princeton, New Jersey, USA**

Abstract

We investigate the problem of finding the minimum number of queries needed to perfectly identify an unknown quantum gate within a finite set of alternatives, considering both deterministic strategies. For unambiguous gate discrimination, where errors are not tolerated but inconclusive outcomes are allowed, we prove that parallel strategies are sufficient to identify the unknown gate with minimum number of queries and we use this fact to provide upper and lower bounds on the query complexity. In addition, we introduce the notion of generalized t-designs, which includes unitary t-designs and group representations as special cases. For gates forming a generalized t-design we prove that there is no difference between perfect probabilistic and perfect deterministic gate discrimination. Hence, evaluating of the query complexity of perfect discrimination is reduced to the easier problem of evaluating the query complexity of unambiguous discrimination.

1998 ACM Subject Classification J.2 Physical sciences and engineering

Keywords and phrases quantum gate identification, unambiguous discrimination, minimum error discrimination, query complexity

Digital Object Identifier 10.4230/LIPIcs.TQC.2013.178

1 Introduction

Identifying an unknown unitary evolution is a fundamental problem in quantum theory [1, 2, 3, 4, 5, 6, 7, 8, 9], with a wide range of applications in quantum information and computation. In quantum computation, the problem is known as oracle identification [10, 11, 12, 13, 14] and is the core of paradigmatic quantum algorithms such as Grover's [15] and Bernstein-Vazirani's [16]. In addition, identifying an unknown unitary gate has applications in the alignment of reference frames via quantum communication [17, 18, 19, 20, 21, 22], in the design of quantum communication protocols that work in the absence of shared reference frames [23, 24, 25], and in the design of quantum machines that learn to execute a desired operation from a training set of examples [26]. For all these applications, the crucial step is to find efficient strategies that discriminate among a set of unknown gates with minimum number of queries to the black box uses.

A striking feature of gate discrimination is that any two distinct unitaries can be perfectly distinguished from one another in a finite number of queries, either using entanglement [1, 2] or using a sequential strategy where different queries are called at different time steps [5].

8th Conference on Theory of Quantum Computation, Communication and Cryptography.
Editors: Simone Severini and Fernando Brandao; pp. 178–191

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Clearly, this feature implies that an unknown gate in a finite set $(U_x)_{x\in\mathsf{X}}$ can be perfectly identified in a finite number of queries, e.g. by running $|\mathsf{X}|-1$ pairwise tests each of which eliminates one wrong alternative. However, in terms of efficiency the pairwise approach leaves large room for improvements: For example, when the unitaries $(U_x)_{x\in\mathsf{X}}$ are mutually orthogonal, one can identify the black box in a single query using an ancilla, following the lines of the dense coding protocol [27]. In general, finding the minimum number of queries needed for perfect discrimination is a hard problem: for example, solving it would automatically give a general solution for query complexity of oracle identification. One way to approach the problem is to consider the less demanding task of *unambiguous gate discrimination* [3, 4, 6, 7, 28], where the unknown gate is identified without errors but one allows for an inconclusive result. General conditions for unambiguous discrimination were given in Refs. [4, 7, 28] under the assumption that the available queries are used in parallel. However, the case of general strategies and the quantification of the resources required for unambiguous gate discrimination have remained largely unaddressed up to now.

In this paper we prove that parallel strategies are sufficient for unambiguous gate discrimination: if the unambiguous discrimination can be achieved in N queries, then it can be achieved by calling the N queries in parallel (in general, using ancillas). Furthermore, we show that for suitable sets of gates, called *generalized t-designs*, there is no difference between the performances of deterministic strategies using the queries in parallel and the performances of general probabilistic strategies allowing for inconclusive outcomes and sequential queries. Clearly, this implies that, if unambiguous discrimination is possible in N queries, then also perfect discrimination must be possible in N queries. This result reduces the query complexity of perfect discrimination to the query complexity of unambiguous discrimination, which is simpler to evaluate. The reduction to unambiguous discrimination has a fairly large range of applications, including in particular the case when the set of gates is the representation of a finite group. Particular examples are the group of all Boolean oracles [10], the groups of linear [16] and quadratic [29] Boolean functions, the group of permutations [19], and the group of all oracles corresponding to functions from a given finite set to another [7]. Based on the reductions to parallel strategies, we provide lower and upper bounds on the query complexity of perfect/unambiguous discrimination and on the size of the ancilla systems needed by the discrimination strategy. The bounds are general and can often be improved in specific cases. Nevertheless, they suffice to show that unambiguous discrimination of the gates $(U_x)_{x\in\mathsf{X}}$ is always possible with no more than $|\mathsf{X}|-1$ queries. Since $|\mathsf{X}|-1$ is the minimum number of queries that would be needed by the method of pairwise elimination, our result shows that a joint discrimination strategy typically offers an advantage over pairwise elimination. Finally, we discuss the extension of our result to ancilla-unassisted discrimination strategies, where the prohibition to use ancillas implies an overhead in the number of queries needed to achieve perfect/unambiguous discrimination.

2 Results

Unambiguous gate discrimination. We show that unambiguous gate discrimination can be parallelized: if the gates in a given set can be distinguished unambiguously with N queries, then they can be distinguished unambiguously by applying the queries in parallel, possibly using ancillas. Denoting by $N_{\min}$ the minimum number of queries needed to unambiguously identify a gate in $\mathsf{U}:=(U_x)_{x\in\mathsf{X}}$, we prove the bounds

$$|\mathsf{U}|^{\frac{1}{d^2-1}}-1\leq N_{\min}\leq|\mathsf{U}|-\dim(\mathsf{U})+1, \tag{1}$$

where d is the dimension of the Hilbert space where the gates act and $\dim(\mathsf{U})$ is the number of linearly independent operators in U.

In addition, we prove a basic fact about unambiguous state discrimination of pure states, namely that the states in a generic set $\{|\psi_x\rangle\}_{x\in\mathsf{X}}$ can be unambiguously discriminated using N identical input copies whenever N satisfies

$$N > \frac{\log(|\mathsf{X}|-1)}{\log\left(F^{-\frac{1}{2}}\right)} \qquad F := \max_{x,y\in\mathsf{X},x\neq y} |\langle\psi_x|\psi_y\rangle|^2. \tag{2}$$

Applying this result in the case of gate discrimination then gives the upper bound

$$N_{\min} \leq \left\lfloor \frac{\log(|\mathsf{U}|-1)}{\log\left(F_{\mathsf{U}}^{-1/2}\right)} \right\rfloor + 1, \tag{3}$$

where F_{U} is the *minimax fidelity* $F_{\mathsf{U}} := \min_{|\Psi\rangle\in\mathcal{H}\otimes\mathcal{H},\|\Psi\|=1} \max_{x,y\in\mathsf{X},x\neq y} \left|\langle\Psi|(U_x^\dagger U_y\otimes I)|\Psi\rangle\right|^2$. Of course, every upper bound on F_{U} results in a corresponding upper bound for $N_{\min}$. All the upper bounds in Eqs. (1) and (3) are achieved for particular sets of gates. However, in specific cases they can often be improved.

Perfect gate discrimination. We introduce the notion of generalized unitary t-designs, which enables a joint treatment of group representations and unitary t-designs [30, 31, 32, 33]. When the unitary gates form a generalized t-design, we show that probabilistic strategies using $N \leq t$ queres cannot improve the performances of discrimination of parallel deterministic strategies. Precisely, the maximum probability of correct discrimination with $N \leq t$ queries (conditional to the occurrence of conclusive outcomes) is given by

$$p_N = \frac{\dim \mathsf{U}_N}{|\mathsf{U}|} \qquad \mathsf{U}_N := (U_x^{\otimes N})_{x\in\mathsf{X}} \tag{4}$$

and can be achieved by a deterministic strategy that uses the N queries in parallel. As a corollary, for a generalized $|\mathsf{U}|$-design U there is no difference between perfect and unambiguous discrimination: whenever unambiguous discrimination is possible, the probability of the inconclusive result can be reduced to zero. Thanks to this reduction, Eqs. (1) and (3) become bounds on the query complexity of perfect gate discrimination.

3 General gate discrimination strategies

Let $\mathcal{H} \simeq \mathbb{C}^d, d < \infty$ be a finite dimensional Hilbert space, let $\mathsf{Lin}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$, and let $\mathsf{U} = (U_x)_{x\in\mathsf{X}} \subset \mathsf{Lin}(\mathcal{H})$ be a finite set of unitary matrices. All throughout the paper we will require that two unitaries U_x and U_y corresponding to distinct labels $x \neq y$ be statistically distinguishable, that is

$$\forall x, y \in \mathsf{X}, x \neq y \quad \exists|\psi\rangle \in \mathcal{H} : \quad U_x|\psi\rangle\langle\psi|U_x^\dagger \neq U_y|\psi\rangle\langle\psi|U_y^\dagger. \tag{5}$$

▶ **Definition 1.** If Eq. (5) holds, we say that the mapping $U : x \in \mathsf{X} \mapsto U_x \in \mathsf{Lin}(\mathcal{H})$ is a *projectively faithful representation* of the set X.

Suppose that we are given a black box implementing one of the unitaries in U. In order to identify the action of the black box with N queries, we will consider without loss of generality *pure* strategies: the most general pure strategy consists in

1. preparing a pure input state $|\Psi\rangle \in \mathcal{H}\otimes\mathcal{H}_A$, where A is a suitable ancillary system

2. evolving it through a quantum circuit that uses N queries to the unknown gate U_x, interspersed with known unitary gates $(U_n)_{n=1}^N \subset \mathsf{Lin}(\mathcal{H}\otimes\mathcal{H}_A)$, thus obtaining the output state
$$|\Psi_x\rangle := \left[\prod_{n=1}^{N} U_n(U\otimes I_A)\right] |\Psi\rangle \tag{6}$$
3. performing a measurement on the output state $|\Psi_x\rangle$ with measurement outcomes in the set $\mathsf{Y} = \mathsf{X}\cup\{?\}$. The outcome set Y includes an inconclusive outcome $y =?$ corresponding to the case when the experimenter abstains from producing a guess [3].

Denote by p_x the prior probability of U_x and by $p_N(y|x)$ the conditional probability of the measurement outcome y given that the gate is U_x and that N queries are used. Conditionally to the occurrence of conclusive outcomes, the probability of correct gate identification with N queries is
$$p_N := \frac{\sum_{x\in\mathsf{X}} p_N(x|x)\ p_x}{\sum_{x,y\in\mathsf{X}} p_N(y|x)\ p_x}. \tag{7}$$

We will now spell out three different notions of perfect gate discrimination, in increasing order of strength:

▶ **Definition 2.** Denote by p_N^{max} rhe maximum of p_N over all probabilistic discrimination protocols using N queries (with no constraints on the probability of abstention). A discrimination strategy achieves

- *perfect probabilistic discrimination* iff $p_N^{max} = 1$
- *unambiguous discrimination* iff $p_N^{max} = 1$ and $p(x|x) > 0$ for every $x \in \mathsf{X}$ such that $p_x > 0$
- *perfect deterministic discrimination* iff $p_N^{max} = 1$ and $p_? := \sum_{x\in\mathsf{X}} p(?|x)p_x = 0$.

Clearly, perfect deterministic discrimination implies unambiguous discrimination, which in turn implies perfect probabilistic discrimination. The latter two types of discrimination can be characterized in terms of linear independence:

▶ **Theorem 3.** *The unitaries $(U_x)_{x\in\mathsf{X}}$ can be discriminated in N queries*

1. *in a perfect probabilistic way if and only if there exists $x_0 \in \mathsf{X}$ such that $U_{x_0}^{\otimes N} \notin \mathrm{Span}(U_x^{\otimes N})_{x\in\mathsf{X},x\neq x_0}$*
2. *in an unambiguous way if and only if the unitaries $(U_x^{\otimes N})_{x\in\mathsf{X}}$ are linearly independent.*

Proof. We first prove necessity. The condition for perfect probabilistic discrimination is equivalent to the existence of at least one $x_0 \in \mathsf{X}$ such that $p_N(x_0|x) = 0 \quad \forall x \neq x_0$, which in turn is equivalent to the condition that the output state $|\Psi_{x_0}\rangle$ in Eq. (6) is linearly independent from the states $(|\Psi_x\rangle)_{x\in\mathsf{X},x\neq x_0}$. Since the function $U_x^{\otimes N} \mapsto |\Psi_x\rangle$ is linear, the condition $U_{x_0}^{\otimes N} \notin \mathrm{Span}(U_x^{\otimes N})_{x\in\mathsf{X},x\neq x_0}$ is necessary for perfect probabilistic discrimination. Similarly, the condition for unambiguous discrimination is equivalent to requirement that $p_N(x_0|x) = 0 \quad \forall x, x_0 \in \mathsf{X}, x \neq x_0$, which in turn is equivalent to the requirement that the output states $\{|\Psi_x\rangle\}_{x\in\mathsf{X}}$ are linearly independent. Independence of the states $\{|\Psi_x\rangle\}_{x\in\mathsf{X}}$ implies independence of the unitaries $(U_x^{\otimes N})_{x\in\mathsf{X}}$. Both conditions are also sufficient, because the linear function $U_x^{\otimes N} \mapsto \{|\Phi_x\rangle^{\otimes N}\}_{x\in\mathsf{X}}$ defined by $|\Phi_x\rangle := (U_x\otimes I)|\Phi\rangle$, $|\Phi\rangle := \sum_{n=1}^d |n\rangle|n\rangle/\sqrt{d}$ is invertible, and therefore preserves linear independence. Note that the states $|\Phi_x\rangle$ can be obtained from a parallel strategy where N pairs of systems are prepared in the state $|\Phi\rangle^{\otimes N}$ and the unitary U_x is applied on the first system of each pair. ◀

The equivalence between unambiguous gate discrimination and linear independence of the unitaries was observed in Ref. [7] in the case of a single query (and hence of N parallel queries, which can be treated as a single query to the product box $U_x^{\otimes N}$). Theorem 3 extends the existing characterization to arbitrary discrimination strategies, possibly consisting of multiple time steps. As a consequence of this extension, unambiguous discrimination and perfect probabilistic discrimination can be parallelized:

▶ **Corollary 4.** *If the gates $(U_x)_{x\in\mathsf{X}}$ can be distinguished unambiguously (respectively, in a perfect probabilistic fashion) with N queries, then they can be distinguished unambiguously (respectively, in a perfect probabilistic fashion) using the N queries in parallel.*

We refer to the minimum number N_{min} needed to unambiguously identify a gate in $(U_x)_{x\in\mathsf{X}}$ as the *query complexity of unambiguous gate discrimination* for the gate set $\mathsf{U} := (U_x)_{x\in\mathsf{X}}$. Corollary 4 allows us to conclude that the query complexity of perfect probabilistic/unambiguous discrimination does not change if one restricts to parallel strategies. However, general sequential strategies can help in reducing the probability of the inconclusive result.

4 General bounds on the query complexity of unambiguous gate discrimination

The possibility of parallelizing unambiguous gate discrimination, established by theorem 3, leads immediately to general lower and upper bounds on the query complexity. There bounds do not assume any structure of the set of unitaries U, and can typically be improved when more information about U is available.

4.1 Lower bound

▶ **Theorem 5** (Dimensional bound)**.** *The gates in $\mathsf{U} = (U_x)_{x\in\mathsf{X}}$ can be unambiguously discriminated using N queries only if*

$$|\mathsf{U}| \leq \begin{pmatrix} d^2+N-1 \\ d^2-1 \end{pmatrix}, \tag{8}$$

which implies $N_{\min} > |\mathsf{U}|^{\frac{1}{d^2-1}} - 1$.

Proof. By theorem 3, unambiguous discrimination is possible only if $\dim(U_x^{\otimes N})_{x\in\mathsf{X}} = |\mathsf{U}|$. On the other hand, $\dim(U_x^{\otimes N})_{x\in\mathsf{X}} \leq \dim \mathsf{A}_{N,+}$, where $\mathsf{A}_{N,+} := \mathrm{Span}\left\{A^{\otimes N} \mid A \in \mathsf{Lin}(\mathcal{H})\right\}$. Since $\mathsf{A}_{N,+}$ is the symmetric subspace of the N-fold tensor product of $\mathsf{Lin}(\mathcal{H})$, and the dimension of the latter is d^2, the dimension of $\mathsf{A}_{N,+}$ is $\dim \mathsf{A}_{N,+} = \begin{pmatrix} d^2+N-1 \\ d^2-1 \end{pmatrix}$. ◀

If we do not impose any structure on the set of unitaries $\mathsf{U} = (U_x)_{x\in\mathsf{X}}$, then the bound of Eq. (8) is the best we can hope for. Indeed, for any fixed Hilbert space dimension d and for every number N we can always find a set of unitaries U such that the minimum number of queries needed to unambiguously identify a gate in U is exactly N.

▶ **Example 6.** The bound of Eq. (8) can be saturated choosing $(U_x^{\otimes N})_{x\in\mathsf{X}}$ to be a basis for $A_{N,+}$. This is possible thanks to the Schur-Weyl duality [34], which implies that the unitaries $(U^{\otimes N})_{U\in U(d)}$ are a spanning set for $A_{N,+}$.

4.2 Upper bounds

An upper bound on the query complexity can be obtained by observing that the dimension of $\mathrm{Span}(U_x^{\otimes N})_{x\in\mathsf{X}}$ grows at least linearly with N, a fact that can be proved using an earlier result by Chefles [35]:

▶ **Theorem 7** (Linear bound). *The query complexity of unambiguous discrimination of the gates in* U *is upper bounded by*

$$N_{\min} \leq |\mathsf{U}| + 1 - \dim(\mathsf{U}). \tag{9}$$

Proof. Let $\mathsf{S} = (v_x)_{x\in\mathsf{X}}$ be a finite set of vectors in a vector space V, with the property that every two distinct vectors in S are linearly independent. Under this hypothesis, Chefles proved that $\dim \mathrm{Span}(v_x^{\otimes N+1}) \geq \dim \mathrm{Span}(v_x^{\otimes N}) + 1$ [35]. Applying the result to the set $\mathsf{U}_N := (U_x^{\otimes N})_{x\in\mathsf{X}}$ gives $\dim(\mathsf{U}_N) \geq \dim(\mathsf{U}) + N - 1$. Hence, for the unitaries in U_N are linearly independent for $N = |\mathsf{U}| - \dim(\mathsf{U}) + 1$. ◀

In general, the bound of Eq. (9) can be achieved: for every fixed Hilbert space dimension d and for every fixed cardinality $|\mathsf{U}|$ we can find a set of unitaries such that $N_{\min} = |\mathsf{U}| - \dim(\mathsf{U}) + 1$. This can be seen in the following

▶ **Example 8.** Consider the discrete phase shifts

$$U_x := \omega^x\ |1\rangle\langle 1| + (I - |1\rangle\langle 1|) \qquad \omega := e^{\frac{2\pi i}{|\mathsf{X}|}},$$

with $x = 1, \ldots, |\mathsf{X}|$. In this case the number of linearly independent unitaries in $(U_x^{\otimes N})_{x\in\mathsf{X}}$ is exactly equal to $N + 1$, as it can be seen from the fact that the unitaries $(U_x^{\otimes N})_{x\in\mathsf{X}}$ are in bijective correspondence with the vectors of their eigenvalues, given by $(v_x)_{x\in\mathsf{X}} \subset \mathbb{C}^{N+1}$ where $v_x := (1, \omega, \omega^2, \ldots, \omega^N)^T$. Since the number of linearly independent unitaries in $(U_x^{\otimes N})_{x\in\mathsf{X}}$ is $N + 1$, the minimum number needed for unambiguous discrimination is exactly $N_{\min} = |\mathsf{X}| - 1 = |\mathsf{U}| - \dim(U) + 1$.

Another example where the bound of Eq. (7) gives the exact value is is the example of the so-called "shift-and-multiply" gates:

▶ **Example 9** (Shift-and-multiply gates). Theorem 7 provides a tight bound for the "shift-and-multiply" representation of the group $\mathbf{G} = \mathbb{Z}_d \times \mathbb{Z}_d$, defined by

$$U_{pq} = S^p M^q \qquad (p, q) \in \mathbb{Z}_d \times \mathbb{Z}_d\ , \tag{10}$$

where $S = \sum_{k=1}^d |(k+1) \mathrm{mod}\ d\rangle\langle k|$ and $M = \sum_{k=1}^d e^{(2\pi i k)/d} |k\rangle\langle k|$. In this case, the unitaries $(U_{pq})_{(p,q)\in\mathbb{Z}_d\times\mathbb{Z}_d}$ are linearly independent, and therefore the bound gives $N_{\min} = 1$. Note that, in fact, the unitaries are orthogonal in the Hilbert-Schmidt product, and, therefore, an unknown unitary U_{pq} can be identified perfectly and deterministically, as in the dense coding protocol [27].

Theorem 7 provides an estimate of $N_{\min}$ that is always better than the number of pairwise tests $|\mathsf{U}| - 1$ that would be needed to identify a gate in $(\mathsf{U}_x)_{x\in\mathsf{X}}$ with the method of pairwise eliminations outlined in [1, 2]. Note however that Eq. (9) only ensures *unambiguous* discrimination, while the pairwise elimination method ensures *perfect deterministic* discrimination. In the next Section we will see that the distinction between unambiguous and perfect discrimination disappears when the gates in U form a group representation, or, more generally, a generalized t-design.

Before adding more structure on the set U, we give here a second upper bound that often yields a better estimate than Theorem 7. To state the bound we introduce the *minimax fidelity* of the unitaries U, defined as

$$F_{\mathsf{U}} := \min_{|\Psi\rangle\in\mathcal{H}\otimes\mathcal{H},\||\Psi\|=1} \max_{x,y\in\mathsf{X},x\neq y} \left|\langle\Psi|(U_x^\dagger U_y\otimes I)|\Psi\rangle\right|.$$

The minimax fidelity quantifies the distinguishability of the unitaries $(U_x)_{x\in\mathsf{X}}$ when single-shot ancilla-assisted strategies are used. Clearly, if $F_{\mathsf{U}}=0$, the unitaries can be perfectly distinguished in one shot using a suitable input state. Note also that, under the standing assumption of this paper (projective faithfulness of the mapping $x\mapsto U_x$), F_{U} must be strictly smaller than 1.

▶ **Theorem 10** (Fidelity bound). *The query complexity of unambiguous discrimination of the gates in* U *is upper bounded as*

$$N_{\min} \leq \left\lfloor \frac{\log(|\mathsf{U}|-1)}{\log\left(F_{\mathsf{U}}^{-\frac{1}{2}}\right)} \right\rfloor + 1. \tag{11}$$

The proof is based on a simple observation:

▶ **Lemma 11.** *Let* $(|\psi_x\rangle)_{x\in\mathsf{X}}\in\mathcal{H}$ *be a set of unit vectors such that* $F:=\max_{x,y\in\mathsf{X},x\neq y}|\langle\psi_x|\psi_y\rangle|^2$ *is strictly smaller than one. If* $F^{N/2}<1/(|\mathsf{X}|-1)$*, then the states* $(|\psi_x\rangle^{\otimes N})_{x\in\mathsf{X}}$ *are linearly independent, and, therefore, unambiguously distinguishable.*

Proof. Suppose that $\sum_{y\in\mathsf{X}} c_y|\psi_y\rangle^{\otimes N}=0$. Multiplying by $\langle\psi_x|^{\otimes N}$, taking the modulus, and summing over x we obtain

$$\begin{aligned}\sum_{x\in\mathsf{X}}|c_x| &= \sum_{x\in\mathsf{X}}\left|\sum_{y\in\mathsf{X},y\neq x} c_y\langle\psi_x|\psi_y\rangle^N\right| \\ &\leq \sum_{x\in\mathsf{X}}\sum_{y\in\mathsf{X},y\neq x}|c_y|F^{N/2} \\ &= (|\mathsf{X}|-1)F^{N/2}\left(\sum_{x\in\mathsf{X}}|c_x|\right).\end{aligned}$$

Clearly, if $(|\mathsf{X}|-1)F_{\mathsf{S}}^{N/2}<1$, the only possible solution is $c_x=0\ \forall x\in\mathsf{X}$. Hence, the states $(|\psi_x\rangle^{\otimes N})_{x\in\mathsf{X}}$ are linearly independent. ◀

Proof of theorem 10. Choose the input state $|\Psi\rangle\in\mathcal{H}\otimes\mathcal{H}$ so that $\max_{x,y\in\mathsf{X},x\neq y}|\langle\Psi|(U_x^\dagger U_y\otimes I)|\Psi\rangle|^2=F_{\mathsf{U}}$. For $F_{\mathsf{U}}^{N/2}\leq 1/(|\mathsf{U}|-1)$ the states $(|\Psi_x\rangle^{\otimes N})_{x\in\mathsf{X}}, |\Psi_x\rangle:=(U_x\otimes I)|\Psi\rangle$ are linearly independent. Therefore, also the unitaries $(U_x^{\otimes N})_{x\in\mathsf{X}}$ are linearly independent, i.e. unambiguously distinguishable. ◀

The fidelity bound gives good estimates when F_{U} is close to zero. However, it tends to produce large overheads when F_{U} approaches 1. This phenomenon is illustrated in the following example:

▶ **Example 12** (Permutation gates). Consider the permutations matrices

$$U_\pi=\sum_{k=1}^{d}|\pi(k)\rangle\langle k|, \tag{12}$$

where π is an element of the permutation group S_d. In this case it is clear that the unitary U_π can be perfectly identified with d queries (applying U_π to all the d vectors in the computational basis we can surely identify the permutation $\pi\in S_d$). One the other hand, applying the unitary U_π on a maximally entangled state gives the bound $F_{\mathsf{U}}\geq\left(\frac{d-2}{d}\right)^2$, which inserted in the fidelity bound gives $N_{\min}\leq\log(d!)/\log[d/(d-2)]=O(d^2\log d)$, which is off by a factor $d\log d$ from the actual value.

5 Discrimination of generalized unitary t-designs

Here we impose additional structure on the set of gates $(U_x)_{x\in\mathsf{X}}$. Our analysis includes the case where the set X is a finite group and $x \mapsto U_x$ is a projective representation of X. Also, it will include the case where the unitaries $(U_x)_{x\in\mathsf{X}}$ from a unitary t-design [30, 31, 32, 33]. In order to treat these two cases in a unified way, we introduce the notion of *generalized unitary t-designs*. For the discrimination of generalized unitary t-designs we will show the following properties

1. among all possible discrimination strategies using $N \leq t$ queries, the deterministic strategies using all queries in parallel maximize the probability of correct gate identification
2. for strategies using $N \leq t$ queries, there is no difference between perfect probabilistic, unambiguous, and perfect deterministic discrimination.

5.1 Generalized unitary t-designs: definition and characterization

Let us start from the definition:

▶ **Definition 13** (Generalized unitary t-designs)**.** Let $(U_x)_{x\in\mathsf{X}}$ be a set of unitaries, $(p_x)_{x\in\mathsf{X}}$ be a set of probabilities. We say that the set $(U_x, p_x)_{x\in\mathsf{X}}$ is a *generalized weighted unitary t-design* iff

$$\left(U_y^{\otimes t} \otimes \overline{U}_y^{\otimes t}\right)\left(\sum_{x\in\mathsf{X}} p_x U_x^{\otimes t} \otimes \overline{U}_x^{\otimes t}\right) = \left(\sum_{x\in\mathsf{X}} p_x U_x^{\otimes t} \otimes \overline{U}_x^{\otimes t}\right) \qquad \forall y \in \mathsf{X}. \tag{13}$$

If $p_x = 1/|\mathsf{X}| \quad \forall x \in \mathsf{X}$ we say that $(U_x)_{x\in\mathsf{X}}$ is a *generalized unitary t-design* (or shortly, a *generalized t-design*).

Note that, by definition, every generalized weighted t-design is also a weighted generalized $(t-1)$-design.

▶ **Example 14** (Unitary t-designs)**.** A unitary t-design is a set of unitaries and probabilities $(U_x, p_x)_{x\in\mathsf{X}}$ such that

$$\sum_{x\in\mathsf{X}} p_x U_x^{\otimes t} \otimes \overline{U}_x^{\otimes t} = \int \mathrm{d}U \; U^{\otimes t} \otimes \bar{U}^{\otimes t},$$

where the integral in the l.h.s. runs over the normalized Haar measure of the group $U(d)$. From the definition is clear that any unitary t-design is an example of generalized unitary t-design.

Generalized t-designs can be characterized as follows:

▶ **Proposition 15.** *A set of unitaries $(U_x, p_x)_{x\in\mathsf{X}}$ is a weighted generalized t-design if and only if there exists a compact group $\mathbf{G}$ such that $\mathsf{X} \subseteq \mathsf{G}$ and*

$$\sum_{x\in\mathsf{X}} p_x \; U_x^{\otimes t} \otimes \overline{U}_x^{\otimes t} = \int \mathrm{d}g \; U_g^{\otimes t} \otimes \overline{U}_g^{\otimes t}, \tag{14}$$

where $\int \mathrm{d}g f(g)$ denotes the integral of f with respect to the normalized Haar measure.

Proof. If the condition in proposition 15 is satisfied, clearly $(U_x, p_x)_{x\in\mathsf{X}}$ is a weighted generalized t-design. Conversely, if $(U_x, p_x)_{x\in\mathsf{X}}$ is a generalized weighted t-design, define $\mathbf{G}$ to be the closure of the group generated by the unitaries $(U_x,)_{x\in\mathsf{X}}$. Since we are in

finite dimensions, $\mathbf{G}$ is a compact group. Clearly, $(U_g^{\otimes t} \otimes \overline{U}_g^{\otimes t})(\sum_{x\in\mathsf{X}} p_x\ U_x^{\otimes t} \otimes \overline{U}_x^{\otimes t}) = (\sum_{x\in\mathsf{X}} p_x\ U_x^{\otimes t} \otimes \overline{U}_x^{\otimes t})$ for every $g \in \mathbf{G}$. Hence,

$$\begin{aligned}(\sum_{x\in\mathsf{X}} p_x\ U_x^{\otimes t} \otimes \overline{U}_x^{\otimes t}) &= \int \mathrm{d}g (U_g^{\otimes t} \otimes \overline{U}_g^{\otimes t}) \left(\sum_{x\in\mathsf{X}} p_x\ U_x^{\otimes t} \otimes \overline{U}_x^{\otimes t}\right) \\ &= \int \mathrm{d}g (U_g^{\otimes t} \otimes \overline{U}_g^{\otimes t}).\end{aligned}$$

◀

Thanks to the above characterization, one can easily transfer properties of compact groups to generalized t-designs. In the next sections we will use this trick to prove strong properties of gate discrimination for generalized t-designs.

5.2 Basic group-theoretic facts

Since generalized t-designs have an underlying group-theoretic structure, it is useful to recall here some basic facts about the representation of compact groups. Let $\mathbf{G}$ be a compact group and let $U : \mathbf{G} \to \mathsf{Lin}(\mathcal{H}),\ g \mapsto U_g$ be a a *unitary projective representation (UPR)* of G with multiplier $\omega : \mathbf{G} \times \mathbf{G} \to \mathbb{C}$ [in short, this means that $U_g U_h = \omega(g,h) U_{gh},\ \forall g, h \in \mathbf{G}$]. Unitary representations correspond to the special case UPRs where $\omega(g,h) = 1\ \forall g, h \in \mathbf{G}$.

With a suitable choice of basis, the Hilbert space can be decomposed as a direct sum of tensor product pairs

$$\mathcal{H} = \bigoplus_{\mu\in\mathsf{Irr}(U)} (\mathcal{R}_\mu \otimes \mathcal{M}_\mu)\,, \tag{15}$$

where the sum runs over the set $\mathsf{Irr}(U)$ of all inequivalent irreducible representations (*irreps*) contained in the decomposition of U (known as *isotypic decomposition*), $\mathcal{R}_\mu$ is a *representation space* of dimension d_μ, carrying the irrep U^μ, and $\mathcal{M}_\mu$ is a *multiplicity space* of dimension m_μ, m_μ being the multiplicity of the irrep U^μ in the decomposition of U. Eq. (15) implies that the representation U can be written in the block diagonal form

$$U = \bigoplus_{\mu\in\mathsf{Irr}(U)} \left(U^\mu \otimes I_{\mathcal{M}_\mu}\right), \tag{16}$$

where $I_{\mathcal{M}_\mu}$ denotes the identity matrix on $\mathcal{M}_\mu$. Note that all the irreps $U^\mu \in \mathsf{Irr}(U)$ must have the same multiplier ω.

Using Eq. (16) and the orthogonality of matrix elements, one can prove that the set of unitaries $\mathsf{U} := (U_g)_{g\in\mathbf{G}}$ satisfies

$$\dim(\mathsf{U}) = \sum_{\mu\in\mathsf{Irr}(U)} d_\mu^2. \tag{17}$$

Due to the importance of linear independence in the gate discrimination problem, this equation will become very useful in the following section.

A representation that plays a key role in gate discrimination is the *regular representation*, which for finite groups is a representation of $\mathbf{G}$ on the Hilbert space $\mathcal{H} = \mathbb{C}^{|\mathbf{G}|}$, equipped with the orthonormal basis $\{|g\rangle \mid g \in \mathbf{G}\}$:

▶ **Definition 16.** The *regular representation with multiplier* ω is the projective representation $U^{reg,\omega} : \mathbf{G} \to \mathsf{Lin}(\mathbb{C}^{|\mathbf{G}|})$ defined by

$$U_g^{reg,\omega}|h\rangle = \omega(g,h)\ |gh\rangle\ , \qquad \forall g, h \in \mathbf{G} \tag{18}$$

The regular decomposition is reducible and its isotypic decomposition is

$$U_g^{reg,\omega} = \bigoplus_{\mu\in \mathrm{Irr}(\mathbf{G},\omega)} \left(U_g^\mu \otimes I_{\mathcal{M}_\mu}\right) \qquad \mathcal{M}_\mu \simeq \mathbb{C}^{d_\mu} \tag{19}$$

where $\mathrm{Irr}(\mathbf{G},\omega)$ denotes the set of all the irreps of $\mathbf{G}$ with multiplier ω [in particular, $\mathrm{Irr}(\mathbf{G},1)$ is the set of all *unitary* irreps of $\mathbf{G}$]. Note that every irrep appears with multiplicity $m_\mu = d_\mu$. Choosing $g = e$ (the identity element in the group) and taking the trace on both sides of Eq. (19) one obtains

$$|\mathbf{G}| = \sum_{\mu\in \mathrm{Irr}(\mathbf{G},\omega)} d_\mu^2 \ , \tag{20}$$

which holds for every possible multiplier ω. Finally, combining Eqs. (17) and (20), one gets the following statement:

▶ **Proposition 17.** *Let $\mathbf{G}$ be a finite group and let $U : \mathbf{G} \to \mathsf{Lin}(\mathcal{H})$ be a UPR with multiplier ω. Then, the unitaries $(U_g)_{g\in\mathbf{G}}$ are linearly independent if and only if the isotypic decomposition of U contains all the irreps in $\mathsf{Irr}(\mathbf{G},\omega)$.*

5.3 Optimal discrimination of generalized unitary t-designs

We start from general result about the maximum probability of correct identification, maximized over over all probabilistic strategies consisting of N queries. Precisely, we show that the maximum success probability can be always achieved with a deterministic parallel strategy:

▶ **Theorem 18** (Optimal probabilistic gate discrimination)**.** *Let $(U_x)_{x\in\mathsf{X}}$ be a set of unitary gates and let $(p_x)_{x\in\mathsf{X}}$ the corresponding prior probabilities. Then, the maximum probability of correct gate identification [defined in Eq. (7)] is*

$$p_N^{\max} = \max_{x\in\mathsf{X}} \ p_x \langle\!\langle U_x|^{\otimes N} \ R_N^{-1} \ |U_x\rangle\!\rangle^{\otimes N}, \tag{21}$$

with $|U_x\rangle\!\rangle := (U_x\otimes I)|I\rangle\!\rangle$, $|I\rangle\!\rangle := \sum_{n=1}^d |n\rangle|n\rangle$, $R_N := \sum_{x\in\mathsf{X}} p_x \ (|U_x\rangle\!\rangle\langle\!\langle U_x|)^{\otimes N}$, and R_N^{-1} denotes the Moore-Penrose inverse of R_N. The maximum probability of correct identification can be achieved applying the N queries in parallel on an entangled state.

Proof. Using the formalism of quantum combs [36, 37, 38], we express the probability $p_N(y|x)$ as $p_N(y|x) = \langle\!\langle U_x|^{\otimes N} \ T_y \ |U_x\rangle\!\rangle^{\otimes N}$ where $(T_y)_{y\in\mathsf{Y}}$ is a collection of positive operators satisfying suitable normalization conditions [38, 36] (the actual form of the conditions is irrelevant here). The probability of correct identification can be bounded as

$$\begin{aligned}
p_N &= \frac{\sum_{x\in\mathsf{X}} p_x \ \langle\!\langle U_x|^{\otimes N} R_N^{-\frac{1}{2}} \ \left(R_N^{\frac{1}{2}} T_x R_N^{\frac{1}{2}}\right) \ R_N^{-\frac{1}{2}} |U_x\rangle\!\rangle^{\otimes N}}{\sum_{y\in\mathsf{X}} \mathrm{Tr}[T_y R_N]} \\
&\le \sum_{x\in\mathsf{X}} p_x \ \mathrm{Tr}[\rho_x \ R_N^{-\frac{1}{2}} (|U_x\rangle\!\rangle\langle\!\langle U_x|)^{\otimes N} R_N^{-\frac{1}{2}}] \qquad \rho_x := \frac{R_N^{\frac{1}{2}} T_x R_N^{\frac{1}{2}}}{\sum_{y\in\mathsf{X}} \mathrm{Tr}[R_N^{\frac{1}{2}} T_y R_N^{\frac{1}{2}}]} \\
&\le \sum_{x\in\mathsf{X}} p_x \ \mathrm{Tr}[\rho_x] \ \|R_N^{-\frac{1}{2}} (|U_x\rangle\!\rangle\langle\!\langle U_x|)^{\otimes N} R_N^{-\frac{1}{2}}\|_\infty \\
&\le \max_{x\in\mathsf{X}} p_x \ \langle\!\langle U_x|^{\otimes N} \ R_N^{-1} \ |U_x\rangle\!\rangle^{\otimes N},
\end{aligned}$$

the last inequality coming from the condition $\sum_{x\in\mathsf{X}} \mathrm{Tr}[\rho_x] = 1$. Defining

$$x_{\max} := \mathrm{argmax}\ p_x\ \langle\!\langle U_x|^{\otimes N}\ R^{-1}\ |U_x\rangle\!\rangle^{\otimes N},$$

the bound can be saturated by applying the N queries of U_x in parallel on the maximally entangled state $|\Phi\rangle^{\otimes N}$,$|\Phi\rangle := |I\rangle\!\rangle/\sqrt{d}$, and by performing the POVM $(P_y)_{y\in\mathsf{Y}}$ defined by $P_{x_{\max}} = R^{-1}(|U_{x_{\max}}\rangle\!\rangle\langle\!\langle U_{x_{\max}}|)^{\otimes N}R^{-1}/\langle\!\langle U_{x_{\max}}|)^{\otimes N}R^{-2}|U_{x_{\max}}\rangle\!\rangle$, $P_? = I - P_{x_{\max}}$, $P_y = 0$ for every $y \neq x_{\max}$. ◀

In the case of generalized weighted t-designs, the following strong property holds:

▶ **Theorem 19** (Optimal gate discrimination for generalized N-designs). *Let $(U_x, p_x)_{x\in\mathsf{X}}$ be a generalized weighted N-design. Then, the maximum of the probability of correct discrimination over all probabilistic strategies consisting of N queries is*

$$p_N^{\max} = \dim(\mathsf{U}_N)\ \max_{x\in\mathsf{X}} p_x \qquad \mathsf{U}_N := (U_x^{\otimes N})_{x\in\mathsf{X}}. \tag{22}$$

For uniform prior $p_x = 1/|\mathsf{U}|$, the maximum probability $p_N^{\max} = \dim(\mathsf{U}_N)/|\mathsf{U}|$ can be achieved by a deterministic strategy that uses the N queries in parallel.

Proof. Let $\mathbf{G}$ the compact group such that $\sum_{x\in\mathsf{X}}(U_x\otimes\overline{U}_x)^{\otimes N} = \int \mathrm{d}g\ (U_g\otimes\overline{U}_g)^{\otimes N}$, or equivalently, $\sum_{x\in\mathsf{X}} U_x^{\otimes N} A U_x^{\dagger\otimes N} = \int \mathrm{d}g\ U_g^{\otimes N} A U_g^{\dagger\otimes N}$ for every operator $A \in \mathsf{Lin}(\mathcal{H}^{\otimes N})$. Exploiting the isotypic decomposition of $U^{\otimes N}$, one can write $U_x^{\otimes N} = \bigoplus_{\mu\in\mathsf{Irr}(U)} \left(U_x^\mu \otimes I_{\mathcal{M}_\mu}\right)$ and, therefore, $|U_x\rangle\!\rangle^{\otimes N} = \bigoplus_{\mu\in\mathsf{Irr}(U^{\otimes N})} |U_x^\mu\rangle\!\rangle|I_{\mathcal{M}_\mu}\rangle\!\rangle$. The operator R_N in theorem 18 can be directly computed as

$$\begin{aligned} R_N &= \textstyle\sum_{x\in\mathsf{X}} p_x\ (|U_x\rangle\!\rangle\langle\!\langle U_x|)^{\otimes N} \\ &= \textstyle\int \mathrm{d}g\ (|U_g\rangle\!\rangle\langle\!\langle U_g|)^{\otimes N} \\ &= \textstyle\bigoplus_{\mu\in\mathsf{Irr}(U^{\otimes N})} \frac{m_\mu}{d_\mu}\ \left(I_{\mathcal{R}_\mu}\otimes I_{\mathcal{R}_\mu}\otimes \frac{|I_{\mathcal{M}_\mu}\rangle\!\rangle\langle\!\langle I_{\mathcal{M}_\mu}|}{m_\mu}\right), \end{aligned}$$

so that, computing the inverse, one has $\langle\!\langle U_x|^{\otimes N}\ R_N^{-1}\ |U_x\rangle\!\rangle^{\otimes N} = \sum_{\mu\in\mathsf{Irr}(U^{\otimes N})} d_\mu^2 = \dim(\mathsf{U}^{\otimes N})$ [cf. Eq. (17)]. Inserting this value in Eq. (21) proves Eq. (22). We now prove that for the uniform prior the maximum success probability can be obtained with a deterministic strategy that uses the N queries in parallel. To this purpose, consider the maximum likelihood input state [39, 40]: this is the state in $\mathcal{H}^{\otimes N}\otimes\mathcal{H}_A$ given by

$$|\Phi_{ML}\rangle := \bigoplus_{\mu\in\mathsf{Irr}(U^{\otimes N})} \sqrt{\frac{d_\mu}{\dim(U^{\otimes N})}}\ |I_{\mathcal{R}_\mu}\rangle\!\rangle,$$

where $|I_{\mathcal{R}_\mu}\rangle\!\rangle = \sum_{n=1}^{d_\mu} |\alpha_n^\mu\rangle|\beta_n^\mu\rangle$, $(|\alpha_n^\mu\rangle)_{n=1}^{d_\mu}$ being an orthonormal basis for $\mathcal{R}_\mu$ and $(|\beta_n^\mu\rangle)_{n=1}^{d_\mu}$ being an orthonormal set of vectors in $\mathcal{M}_\mu\otimes\mathcal{H}_A$ [here the dimension of $\mathcal{H}_A$ is chosen in order to satisfy the relation $d_\mu \leq m_\mu d_A, \forall\mu\in\mathsf{Irr}(U^{\otimes N})$]. Applying the N queries in parallel one obtains the output states $|\Phi_{ML,x}\rangle := (U_x^{\otimes N}\otimes I_A)|\Phi_{ML}\rangle$. Optimal discrimination can be achieved deterministically using the square root measurement [41], which in this case has POVM elements $P_x := \frac{\dim(U^{\otimes N})}{|\mathsf{U}|}\ |\Phi_{ML,x}\rangle\langle\Phi_{ML,x}|$. ◀

The general result of theorem 19 is well illustrated by the case of discrete phase shifts:

▶ **Example 20** (Discrete phase shifts). Consider the discrete phase shifts

$$U_k = \sum_{l=0}^{L-1} \omega^{kl}\ P_l \qquad \omega = e^{\frac{2\pi i}{K}}, k \in \{1,\dots K\} \tag{23}$$

where $\{P_l\}_{l=0}^{L-1}$ are orthogonal projectors summing up to the identity in $\mathcal{H}$. The unitaries $\{U_k \mid k = 1, \ldots, K\}$ form a unitary representation of the Abelian group $\mathbf{G} = \mathbb{Z}^K$. Now, the unitary irreps of $\mathbb{Z}^K$ are one-dimensional, and are given by $U_\mu : \mathbb{Z}^d \to \mathbb{C}, k \mapsto \omega^{\mu k}$, with $\mu \in \{0, \ldots, K-1\}$. From Eq. (23) it is then clear that $\mathrm{Irr}(U) = \{0, 1, \ldots L-1\}$ and Eq. (22) gives $p_1^{\max} = L/K$. Similarly, it is clear that $\mathrm{Irr}(U^{\otimes N}) = \{0, 1, \ldots, N(L-1)\}$, and therefore, Eq. (22) gives

$$p_N^{\max} = \frac{NL - N + 1}{K} \qquad N \leq \frac{K-1}{L-1}. \tag{24}$$

The minimum number of queries needed for perfect discrimination is then $N_{\min} = \left\lceil \frac{K-1}{L-1} \right\rceil$.

5.4 Perfect discrimination of generalized unitary t-designs

An immediate consequence of Theorem 19, all possible notions of perfect gate discrimination coincide in the case of generalized unitary t-designs:

▶ **Corollary 21.** *If the unitaries $(U_x)_{x\in\mathsf{X}}$ form a generalized t-design, then the following are equivalent:*

1. *perfect probabilistic discrimination is possible with $N \leq t$ queries*
2. *unambiguous discrimination is possible with $N \leq t$ queries*
3. *perfect deterministic discrimination is possible in $N \leq t$ queries.*

In particular, for a generalized $|\mathsf{U}|$-design there is no difference between the three types of perfect discrimination.

For generalized t-designs the evaluation of the query complexity of perfect discrimination is reduced to the simpler problem of evaluating the query complexity of unambiguous discrimination. In particular, the bounds in Theorems 5, 7, and 10 become automatically bounds on the query complexity of perfect discrimination.

6 Conclusions

We investigated the problem of identifying an unknown unitary gate in a finite set of alternatives, using both deterministic and probabilistic discrimination strategies, and allowing the unknown gate to be queried multiple times and to be be used in parallel or in series in arbitrary quantum circuits. In this scenario, we provided upper and lower bounds on the amount of resources needed to achieve unambiguous and perfect gate identification. Specifically, we gave bounds on the query complexity and the minimum size of the ancillas needed to achieve unambiguous/perfect identification. Most of our results stem from two key observations. The first observation is that unambiguous gate discrimination can be parallelized: if unambiguous discrimination is possible with N queries, then unambiguous gate discrimination must also be possible by applying the N queries in parallel on a suitable entangled state. The second key observation is based on the definition of generalized unitary t-designs, a definition that includes unitary t-designs and group representations as special cases. The remarkable feature of generalized t-designs is that for strategies using $N \leq t$ queries there is no difference between unambiguous and perfect deterministic discrimination. Using this fact, one can reduce the analysis of perfect gate discrimination to the simpler analysis of unambiguous gate discrimination.

Acknowledgments. GC acknowledges support by the National Basic Research Program of China (973) 2011CBA00300 (2011CBA00301), by the 1000 Youth Fellowship Program of China, and by the National Natural Science Foundation of China through Grants 61033001 and 61061130540, and by Perimeter Institute for Theoretical Physics, where part of this work was carried out. Research at Perimeter Institute for Theoretical Physics is supported in part by the Government of Canada through NSERC and by the Province of Ontario through MRI.

References

1 A. Acín, *Statistical Distinguishability between Unitary Operations*, Phys. Rev. Lett. **87**, 177901 (2001).

2 G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, *Using Entanglement Improves the Precision of Quantum Measurements*, Phys. Rev. Lett. **87**, 270404 (2001).

3 J. A. Bergou, U. Herzog, and M. Hillery, *Quantum Filtering and Discrimination between Sets of Boolean Functions*, Phys. Rev. Lett. **90**, 257901 (2003).

4 A. Chefles and M. Sasaki, *Retrodiction of Generalized Measurement Outcomes* Phys. Rev. A **67**, 032112 (2003).

5 R. Duan, Y. Feng, and M. Ying, *Entanglement is Not Necessary for Perfect Discrimination between Unitary Operations*, Phys. Rev. Lett. **98**, 100503 (2007).

6 J. A. Bergou and M. Hillery, *Quantum State Filtering Applied to the Discrimination of Boolean Functions*, Phys. Rev. A **72**, 012302 (2005).

7 A. Chefles, A. Kitagawa, M. Takeoka, M. Sasaki, and J. Twamley *Unambiguous Discrimination among Oracle Operators*, J. Phys. A: Math. Theor. **40**. 10183 (2007).

8 G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Memory Effects in Quantum Channel Discrimination*, Phys. Rev. Lett. **101** 180501 (2008).

9 R. Duan, Y. Feng, and M. Ying, *Perfect Distinguishability of Quantum Operations*, Phys. Rev. Lett. **103**, 210501 (2009).

10 A. Ambainis, *Quantum Lower Bounds by Quantum Arguments*, Journal of Computer and System Science **64**, 750 (2002).

11 W. van Dam 1998 *Quantum Oracle Interrogation: Getting All Information For Almost Half the Price*, Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science (FOCS) **362** (1998).

12 E. Fahri, J. Goldstone, S. Gutman, and M. Sipser, *Bound on the Number of Functions That Can Be Distinguished With k Quantum Queries*, Phys. Rev. A **60**, 4331 (1999).

13 A. Ambainis, K. Iwama, A. Kawachi, H. Masuda, R. H. Putra, and S. Yamashita, *Quantum Identification of Boolean Oracles*, Proceedings of STACS 2004, Lecture Notes in Computer Science **2996**, 105 (2004).

14 A. Ambainis, K. Iwama, A. Kawachi, R. Raymond, and S. Yamashita, *Improved Algorithms for Quantum Identification of Boolean Oracles*, Lecture Notes in Computer Science **4059**, 105 (2006).

15 L. Grover, *Quantum Mechanics Helps in Searching for a Needle in a Haystack*, Phys. Rev. Lett. **79**, 325 (1997).

16 E. Bernstein and U. Vazirani, *Quantum Complexity Theory*, Proceedings of the 25th Annual ACM Symposium on the Theory of Computing, 11 (1993).

17 G. Chiribella, G. M. D'Ariano, P. Perinotti P, and M. F. Sacchi, *Efficient Use of Quantum Resources for the Transmission of a Reference Frame*, Phys. Rev. Lett. **93**, 180503 (2004).

18 E. Bagan, M. Baig, and R. Muñz-Tapia, *Quantum Reverse Engineering and Reference-Frame Alignment Without Nonlocal Correlations*, Phys. Rev. A **70**, 030301(R) (2004).

19 J. von Korff and J. Kempe, *Quantum Advantage in Transmitting a Permutation*, Phys. Rev. Lett. **93** 260502 (2004).

20 D. Collins, L. Diosi, G. Gisin, S. Massar, and S. Popescu, *Quantum Gloves: Quantum States That Encode As Much As Possible Chirality and Nothing Else*, Phys. Rev. A **72**. 022304 (2005).

21 A. Hayashi, T. Hashimoto, and M. Horibe, *Extended Quantum Color Coding*, Phys. Rev. A **71** 012326 (2005).

22 G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Optimal Covariant Quantum Newtorks*, AIP Conf. Proc. **1110**, 47 (2008).

23 S. D. Bartlett, T. Rudolph, R. W. Spekkens, and P. S. Turner, *Quantum Communication Using a Bounded-Size Quantum Reference Frame*, New J. Phys. **11** 063013 (2009).

24 G. Chiribella, V. Giovannetti, L. Maccone, and P. Perinotti, *Teleportation Transfers Only Speakable Quantum Information*, Phys. Rev. A **86** 010304(R) (2012).

25 M. Skotiniotis, B. Kraus, and W. Dür, *Efficient Quantum Communication Under Collective Noise*, Quantum Information and Computation **13**. 0290 (2013).

26 A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. Perinotti, *Optimal Quantum Learning of a Unitary Transformation*, Phys. Rev. A **81** 032324 (2010).

27 C. H. Bennett and S. J. Wiesner, *Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States*, Phys. Rev. Lett. **69** 2881 (1992).

28 G. Wang and M. Ying, *Unambiguous Discrimination Among Quantum Operations*, Phys. Rev. A **73**, 042301 (2006).

29 M. Rötteler, *Quantum Algorithms to Solve the Hidden Shift Problem for Quadratics and for Functions of Large Gowers Norm*, Letc. Notes Comp. Science, **5734,** 993 (2009).

30 C. Dankert, R. Cleve, J. Emerson, and E. Livine, *Exact and Approximate Unitary 2 - Designs and their Application to Fidelity Estimation*, Physical Review A **80**, 012304 (2009).

31 D. Gross, K. Audenaert, and J. Eisert, *Evenly Distributed Unitaries: On the Structure of Unitary Designs*, J. Math. Phys. **48**, 052104 (2007).

32 A. J. Scott, *Optimizing Quantum Process Tomography with Unitary 2-Designs*, J. Phys. A **41**, 055308 (2008).

33 A. Roy and A. J. Scott, *Unitary Designs and Codes*, Des. Codes Cryptogr. **53**, 13 (2009).

34 R. W. Goodman and N. Wallach, *Representations and invariants of the classical groups*, Cambridge University Press (2003).

35 A. Chefles, *Quantum operations, state transformations and probabilities*, Phys. Rev. A **65**, 052314 (2002).

36 G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Quantum Circuits Architecture*, Phys. Rev. Lett. **101**, 060401 (2008).

37 G. Chiribella, G. M. D'Ariano and P. Perinotti, *Theoretical Framework for Quantum Networks*, Phys. Rev. A **80**, 022339 (2009).

38 G. Gutoski and J. Watrous, *Toward a General Theory of Quantum Games*, Proceedings of the 39th ACM Symposium on the Theory of Computation (STOC) **39**, 565 (2007).

39 G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, *Covariant Quantum Measurements That Maximize The Likelihood*, Phys. Rev. A **70**, 062105 (2004).

40 G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi, *Maximum Likelohood Estimation of an Unknown Group Transformation*, Int. J. Quantum Inf. **4**, 453 (2006).

41 P. Hausladen and W. K. Wootters, *A 'Pretty Good' Measurement for Distinguishing Quantum States*, J. Mod. Opt. **41**, 2385 (1994).