

Single-Query Exact Discrimination of Phase-Modified Permutation Oracles

Owen Root

oroot@gradcenter.cuny.edu

Hunter College

Research Article

Keywords: oracle discrimination, quantum query model, phase-modified permutation oracle, exact quantum algorithm, unitary discrimination

Posted Date: October 14th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-9181229/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Single-Query Exact Discrimination of Phase-Modified Permutation Oracles

Owen Root¹

¹Department of Physics and Astronomy, CUNY Hunter College, 695
Park Ave, New York, 10065, NY, USA.

Contributing authors: oroot@gradcenter.cuny.edu;

Abstract

I consider a promise problem for an unknown unitary acting on an n -qubit register. The oracle is promised to implement either a fixed permutation of computational basis states or the same permutation accompanied by a conditional sign change determined by a designated input qubit. I show that the two cases can be distinguished exactly with a single query to the oracle and a measurement on only one qubit, and that the query complexity of this task is exactly one. The protocol uses no ancilla qubits and requires only $n + 1$ Hadamard gates in addition to the oracle call. The promise is intrinsically quantum because the two cases differ only through relative phases.

Keywords: oracle discrimination; quantum query model; phase-modified permutation oracle; exact quantum algorithm; unitary discrimination

MSC Classification: 81P68 , 68Q12

1 Introduction

Oracle identification and related black-box problems have played a foundational role in quantum information processing since the early works of Deutsch [1], Deutsch and Jozsa [2], Bernstein and Vazirani [3], and Simon [4]. In different ways, these examples show how superposition and interference can be used to extract global information about an unknown transformation from a small number of oracle calls. They also share a broad architectural feature: an initial Hadamard layer creates a coherent superposition over computational-basis inputs, the oracle imprints structured phase or correlation information, and a final Hadamard transformation converts that

structure into an informative measurement signature. Cleve, Ekert, Macchiavello, and Mosca identified this common pattern explicitly and showed that the canonical oracle algorithms can all be understood as instances of quantum phase estimation [5].

Beyond these canonical oracle algorithms, the broader task of distinguishing quantum operations, and unitary operations in particular, has been studied directly from several perspectives. Acín analyzed the statistical distinguishability of unitary operations and showed that, in general, finitely many uses suffice for perfect discrimination of distinct unitaries [6]. Duan, Feng, and Ying later established general perfect-distinguishability criteria for quantum operations and showed, in particular, that perfect discrimination between unitary operations can be achieved without entanglement between multiple uses of the unknown operation [7, 8]. Collins has also emphasized that standard oracle algorithms may be interpreted as procedures for discriminating among admissible oracle unitaries, including in the Deutsch-Jozsa setting [9]. More recently, the query complexity of unitary-operation discrimination has been studied in a more general framework [10]. In a parallel development, the exact quantum query complexity of Boolean functions has been investigated systematically, and non-trivial separations between exact quantum and classical query complexity have been established for several function families [11, 12]. A broader perspective on the power and limitations of quantum queries is provided by the survey literature on quantum property testing and decision-tree complexity [13, 14].

The present paper considers a different kind of promise within this general black-box setting. Let $\hat{U}$ be an unknown unitary acting on an n -qubit register. It is promised that $\hat{U}$ takes one of two forms: either it permutes the computational-basis states according to a fixed bijection, or it implements the same permutation together with a sign factor determined by a designated input qubit. In contrast with the standard function-oracle settings of Refs. [2–4], the two promised branches here do not correspond to different classical maps on basis labels. Rather, they induce the same permutation of computational-basis states and differ only through relative phases attached to amplitudes.

This distinction is important for how the problem should be interpreted. The present task is most naturally viewed not as a conventional quantum speedup for a classical decision problem, but as an intrinsically quantum oracle-discrimination problem. The promise lives in the phase structure of the unitary action itself. Against the broader literature on unitary and quantum-operation discrimination [6–10], the specific question addressed below is whether this particularly simple phase-modified permutation promise can be resolved with certainty using only a single query to the unknown operator.

The answer is affirmative. A layer of Hadamard gates applied to all qubits, one call to $\hat{U}$, a final Hadamard gate on the designated qubit, and a single-qubit measurement suffice. No ancilla register is required. The resulting protocol is exact and uses only one oracle call. In that sense, the construction may be viewed as a particularly simple addition to the broader family of Hadamard-interference-based quantum algorithms: the same basic architecture that underlies several canonical oracle problems also suffices here, even though the promise is encoded purely in relative phase and not in distinct classical output strings.

The derivation below is written in a fully explicit form so that the mechanism of the protocol is transparent at the level of amplitudes. After the derivation, I comment briefly on the resource content of the construction, its relation to exact oracle discrimination, and its connection to this broader Hadamard-based architectural motif.

2 Exact discrimination protocol

Let us label the two possible operators $\hat{U} = \hat{U}_1$ and $\hat{U} = \hat{U}_2$, respectively. The result established below may be summarized as follows: for the two oracle classes defined in Eqs. (2) and (3), the circuit in Fig. 1 distinguishes the two possibilities with certainty using a single query to $\hat{U}$ and a final measurement of qubit L .

(Step 1) Consider the system in a general input state

$$|\Psi\rangle = |i\rangle = \bigotimes_{l=1}^n |x_{il}\rangle = |x_{i1}, x_{i2}, \dots, x_{in}\rangle, \quad (1)$$

where $i = 0, 1, 2, \dots, 2^n - 1$ labels the states, $l = 1, 2, \dots, n$ labels the qubits, and $|x_{il}\rangle$ is the state of the l -th qubit in the total state i . Note that $|\Psi\rangle$ denotes the state vector of the system at a given step and that $\bigotimes$ denotes repeated tensor products. The effects of $\hat{U}_1$ and $\hat{U}_2$ can be expressed generally as

$$\hat{U}_1|i\rangle = |k\rangle, \quad (2)$$

$$\hat{U}_2|i\rangle = f(x_{iL})|k\rangle, \quad (3)$$

where $f(x_{iL})$ is a function that is equal to 1 if the state of a particular qubit, the L -th qubit, $|x_{iL}\rangle$ is in the $|0\rangle$ state and equal to -1 if $|x_{iL}\rangle$ is in the $|1\rangle$ state. For example, if $n = 2, L = 1$, and the mapping from $|i\rangle \rightarrow |j\rangle$ is the identity mapping, $\hat{U}_1|01\rangle = |01\rangle$ but $\hat{U}_2|01\rangle = -|01\rangle$. Alternatively, $\hat{U}_1|00\rangle = |00\rangle$ and $\hat{U}_2|00\rangle = |00\rangle$.

(Step 2) We then apply a Hadamard gate to each qubit in the system,

$$\hat{H}^{\otimes n}|\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{i \cdot j} |j\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{i \cdot j} |x_{j1}, x_{j2}, \dots, x_{jn}\rangle, \quad (4)$$

where $i \cdot j$ is the bitwise dot product of the (binary) i and j states.

Now we consider the different possibilities for the action of $\hat{U}$ on the system.

(Step 3) If $\hat{U} = \hat{U}_1$ then

$$\hat{U}|\Psi\rangle = \hat{U}_1|\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{i \cdot j(k)} |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{i \cdot j(k)} |x_{k1}, x_{k2}, \dots, x_{kn}\rangle, \quad (5)$$

where I have written the bitwise dot product as $i \cdot j(k)$ to emphasize that the sign of each k term is dependent upon the state of the qubits in the j state that each k state is mapped from and not the state of the qubits in the k state itself.

(Step 4) Now we apply a Hadamard gate to just qubit L and leave the rest of the system alone,

$$\hat{H}_L|\Psi\rangle = \frac{1}{\sqrt{2^n}} \left\{ \frac{1}{\sqrt{2}} (|0\rangle_L + |1\rangle_L) \left(\langle 0|_L \sum_{k=0}^{2^n-1} (-1)^{i \cdot j(k)} |x_{k1}, \dots, x_{kn}\rangle \right) + \frac{1}{\sqrt{2}} (|0\rangle_L - |1\rangle_L) \left(\langle 1|_L \sum_{k=0}^{2^n-1} (-1)^{i \cdot j(k)} |x_{k1}, \dots, x_{kn}\rangle \right) \right\}, \quad (6)$$

where the subscript L on a bra or ket denotes that to be just the state of the L -th qubit, or more compactly as

$$\hat{H}_L|\Psi\rangle = \frac{1}{\sqrt{2^n}} \left(\frac{1}{\sqrt{2}} (|0\rangle_L + |1\rangle_L) a_1 + \frac{1}{\sqrt{2}} (|0\rangle_L - |1\rangle_L) b_1 \right), \quad (7)$$

Notice that the signs of the terms in a_1 and b_1 depend upon the initial state of the L -th qubit, $|x_{iL}\rangle$. If $|x_{iL}\rangle = |0\rangle$ then $(-1)^{i \cdot j(k)}$ is the same for each term in a_1 and b_1 , that is $a_1 = b_1$, while if $|x_{iL}\rangle = |1\rangle$ then $(-1)^{i \cdot j(k)}$ gives the k -th term in b_1 the opposite sign as the k -th term in a_1 , that is $a_1 = -b_1$. This follows from states with $|x_{jL}\rangle = |1\rangle$ picking up a factor of -1 in Step 2.

Then, if $|x_{iL}\rangle = |0\rangle$, then the $|1\rangle_L$ terms cancel, leaving

$$|\Psi\rangle = \frac{1}{\sqrt{2^n}} \left(\frac{1}{\sqrt{2}} 2|0\rangle_L a_1 \right) = \frac{1}{\sqrt{2^{n-1}}} |0\rangle_L a_1. \quad (8)$$

But if $|x_{iL}\rangle = |1\rangle$, the $|0\rangle_L$ terms cancel leaving

$$|\Psi\rangle = \frac{1}{\sqrt{2^{n-1}}} |1\rangle_L a_1. \quad (9)$$

Therefore, (Step 5) if $\hat{U} = \hat{U}_1$, following this procedure, we will always find the L -th qubit in its initial state.

Now consider the case that $\hat{U} = \hat{U}_2$. Step 3 is then

$$\hat{U}|\Psi\rangle = \hat{U}_2|\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{i \cdot j(k)} f(x_{j(k)L}) |x_{k1}, x_{k2}, \dots, x_{kn}\rangle, \quad (10)$$

where I have written the argument of f as $x_{j(k)L}$ to emphasize that the value of f for each k term is dependent upon the state of the L -th qubit in the j state that each k state is mapped from and not the state of the L -th qubit in the k state itself.

Step 4 is now

$$\hat{H}_L|\Psi\rangle = \frac{1}{\sqrt{2^n}} \left\{ \frac{1}{\sqrt{2}} (|0\rangle_L + |1\rangle_L) \left(\langle 0|_L \sum_{k=0}^{2^n-1} (-1)^{i \cdot j(k)} f(x_{j(k)L}) |x_{k1}, \dots, x_{kn}\rangle \right) + \frac{1}{\sqrt{2}} (|0\rangle_L - |1\rangle_L) \left(\langle 1|_L \sum_{k=0}^{2^n-1} (-1)^{i \cdot j(k)} f(x_{j(k)L}) |x_{k1}, \dots, x_{kn}\rangle \right) \right\}, \quad (11)$$

, or more compactly as

$$\hat{H}_L|\Psi\rangle = \frac{1}{\sqrt{2^n}} \left(\frac{1}{\sqrt{2}}(|0\rangle_L + |1\rangle_L)a_2 + \frac{1}{\sqrt{2}}(|0\rangle_L - |1\rangle_L)b_2 \right), \quad (12)$$

Notice that here a_2 and b_2 have an additional contribution to the sign of the k terms, namely the factor $f(x_{j(k)L})$, compared to a_1 and b_1 . This contributes a factor of -1 precisely to every state that also gets a factor of -1 from the L -qubit contribution to $(-1)^{i \cdot j(k)}$. Therefore, once again, there is a balanced situation in the signs of the states in a_2 and b_2 : if $|x_{iL}\rangle = |0\rangle$, then $a_2 = -b_2$, and if $|x_{iL}\rangle = |1\rangle$ then $a_2 = b_2$.

Then, if $|x_{iL}\rangle = |0\rangle$, the $|0\rangle_L$ terms cancel, leaving

$$|\Psi\rangle = \frac{1}{\sqrt{2^{n-1}}} |1\rangle_L a_2. \quad (13)$$

But if $|x_{iL}\rangle = |1\rangle$, the $|1\rangle_L$ terms cancel leaving

$$|\Psi\rangle = \frac{1}{\sqrt{2^{n-1}}} |0\rangle_L a_2. \quad (14)$$

Therefore (Step 5) if $\hat{U} = \hat{U}_2$, following this procedure, we will always find the L -th qubit in the opposite of its initial state.

To summarize, the algorithm is as follows: (1) initialize the system in some known, unentangled state; (2) apply a Hadamard gate to each qubit; (3) act on the system with the unknown operator $\hat{U}$; (4) apply a Hadamard gate to the L -th qubit; (5) measure the L -th qubit. If the L -th qubit is found to be in its initial state, then $\hat{U} = \hat{U}_1$, whereas if it is found flipped from its initial state, then $\hat{U} = \hat{U}_2$. Figure 1 shows an example implementation of the protocol.

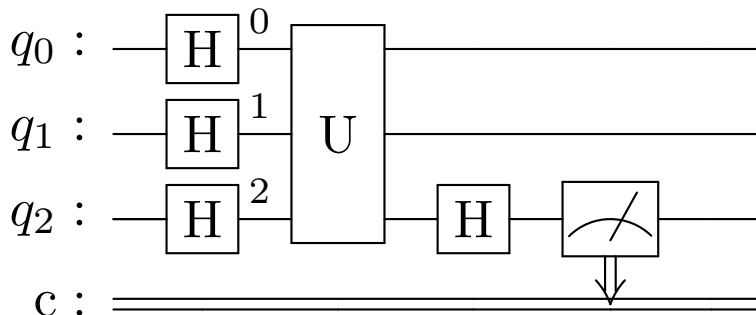


Figure 1: Circuit implementation of the protocol for the case $n = 3$ and $L = 2$.

3 Discussion

Three features of the construction deserve emphasis. First, the protocol is exact. No repetition, postselection, or bounded-error analysis is required. Second, the oracle-query cost is both necessary and sufficient. It is sufficient because the derivation above shows that one query resolves the promise with certainty. It is necessary because, without any query, no information about the oracle is available: the initial state is prepared independently of $\hat{U}$, and any subsequent unitaries and measurements that do not involve $\hat{U}$ are the same regardless of which promised branch is realized, so the measurement statistics are identical in the two cases. The exact query complexity of this discrimination task is therefore exactly one. Third, the discrimination is driven entirely by relative-phase information. The induced permutation of computational-basis labels is identical in the two cases, and all distinguishing power comes from interference generated by the Hadamard layers.

This resource profile is worth comparing with the broader literature. General results on unitary and quantum-operation discrimination show that perfect discrimination is often achievable after finitely many uses of the unknown operation, and that the required resources can be analyzed in terms of distinguishability criteria and query complexity [6–8, 10]. By contrast, the present promise family admits deterministic identification with a single use of the unknown unitary and without ancilla assistance. The point is not that the protocol establishes a new general criterion, but that it provides an explicit and especially transparent one-query instance within that broader landscape.

This also clarifies the sense in which the problem is intrinsically quantum. The promise does not encode two different classical functions on basis labels. Instead, it distinguishes two unitary transformations whose action differs only in phase structure. The example therefore sits more naturally within exact oracle discrimination and restricted unitary characterization than within the standard paradigm of quantum-over-classical query separation.

At the same time, the protocol is deliberately elementary. It isolates a simple mechanism by which a phase modification correlated with a designated input qubit can be converted into a deterministic measurement signature on a single output qubit. In that respect, the construction may serve as a useful toy model for broader questions involving phase-modified permutations, exact oracle discrimination, or restricted forms of unitary certification.

It is natural to ask how far this mechanism extends. In the present setting, the phase modification is a ± 1 sign determined by a single designated qubit. One immediate generalization would be to allow the sign to depend on multiple input qubits; for instance, $\hat{U}_2|i\rangle = (-1)^{g(x_{i1}, \dots, x_{in})}|k\rangle$ for some Boolean function g . In such a setting, the Hadamard recombination on a single qubit would generally not suffice to extract g exactly, and one expects that the number of required Hadamard recombination steps and measured qubits would depend on the structure of g . In particular, the case $g(x_{i1}, \dots, x_{in}) = x_{iL}$ treated here is special precisely because the phase depends on a single bit, allowing a single final Hadamard gate on qubit L to convert the phase information into a deterministic outcome. A further direction concerns the replacement of the ± 1 phase by a general phase $e^{i\theta}$; in that case exact discrimination in a single

query would generally not be achievable, and one would instead need to consider the tradeoff between the number of queries and the precision of the phase estimate, connecting the problem to the broader framework of quantum phase estimation [5]. These extensions would connect the present construction to the more general landscape of exact quantum query complexity [11, 12] and quantum property testing [14].

It is also natural to view the protocol from the perspective of circuit architecture. Canonical oracle algorithms such as those of Deutsch [1], Deutsch and Jozsa [2], Bernstein and Vazirani [3], and Simon [4] all exploit, in different forms, the combination of an initial Hadamard spreading, a non-Hadamard oracle action, and a final Hadamard recombination that converts otherwise hidden phase structure into an accessible measurement outcome. As noted by Cleve et al. [5], this common pattern can be understood as instances of quantum phase estimation, and related discrimination-based analyses of oracle algorithms have also been developed explicitly [9, 10]. The present example adds another exact instance to that broader pattern. Here the architecture succeeds even though the two candidate operators induce the same permutation on computational-basis labels and differ only by a correlated sign structure. A systematic characterization of what classes of promise problems are naturally solvable within such Hadamard-interference-based schemes remains an interesting direction for further work.

4 Conclusion

I have shown that a phase-modified permutation oracle can be distinguished exactly from the corresponding unmodified permutation oracle with a single query, no ancilla qubits, and a measurement on only one qubit. The protocol uses an initial Hadamard layer on all qubits and a final Hadamard gate on the designated qubit, converting the relative-phase promise into a deterministic readout of whether the measured qubit is preserved or flipped.

The contribution is modest but clean. It provides an explicit one-query example of exact discrimination in a setting where the two candidate unitaries differ only through relative phases and not through their induced permutation of computational-basis labels. This should be read against the broader literature on unitary and quantum-operation discrimination [6–10], the main value of the example is its simplicity: the promise is narrow, but within that narrow setting the mechanism is completely explicit and the resource count is immediate.

It also contributes a further example to the broader family of quantum algorithms whose essential mechanism is the combination of Hadamard spreading, non-Hadamard operator action, and Hadamard recombination [5]. As discussed above, natural extensions include phase modifications depending on multiple input qubits, general (non-binary) phase factors, and a systematic study of which promise structures within permutation oracles admit exact single-query discrimination. These directions would connect the present construction more closely to the broader frameworks of exact quantum query complexity [11, 12] and quantum property testing [13, 14].

Declarations

Funding

This work was supported by the NASA MIRO CUNY program at Hunter College.

References

- [1] Deutsch, D.: Quantum theory, the church–turing principle and the universal quantum computer. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences **400**(1818), 97–117 (1985) <https://doi.org/10.1098/rspa.1985.0070> <https://royalsocietypublishing.org/rspa/article-pdf/400/1818/97/65933/rspa.1985.0070.pdf>
- [2] Deutsch, D., Jozsa, R.: Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences **439**(1907), 553–558 (1992) <https://doi.org/10.1098/rspa.1992.0167> <https://royalsocietypublishing.org/rspa/article-pdf/439/1907/553/68698/rspa.1992.0167.pdf>
- [3] Bernstein, E., Vazirani, U.: Quantum complexity theory. In: Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing. STOC '93, pp. 11–20. Association for Computing Machinery, New York, NY, USA (1993). <https://doi.org/10.1145/167088.167097> . <https://doi.org/10.1145/167088.167097>
- [4] Simon, D.R.: On the power of quantum computation. SIAM Journal on Computing **26**(5), 1474–1483 (1997) <https://doi.org/10.1137/S0097539796298637> <https://doi.org/10.1137/S0097539796298637>
- [5] Cleve, R., Ekert, A., Macchiavello, C., Mosca, M.: Quantum algorithms revisited. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences **454**(1969), 339–354 (1998) <https://doi.org/10.1098/rspa.1998.0164>
- [6] Acín, A.: Statistical distinguishability between unitary operations. Physical Review Letters **87**(17), 177901 (2001) <https://doi.org/10.1103/PhysRevLett.87.177901>
- [7] Duan, R., Feng, Y., Ying, M.: Entanglement is not necessary for perfect discrimination between unitary operations. Physical Review Letters **98**(10), 100503 (2007) <https://doi.org/10.1103/PhysRevLett.98.100503>
- [8] Duan, R., Feng, Y., Ying, M.: Perfect distinguishability of quantum operations. Physical Review Letters **103**(21), 210501 (2009) <https://doi.org/10.1103/PhysRevLett.103.210501>

- [9] Collins, D.: Discrimination of unitary transformations in the deutsch-jozsa algorithm: Implications for thermal-equilibrium-ensemble implementations. *Physical Review A* **81**(5), 052323 (2010) <https://doi.org/10.1103/PhysRevA.81.052323>
- [10] Huang, X., Li, L.: Query complexity of unitary operation discrimination. *Physica A: Statistical Mechanics and its Applications* **604**, 127863 (2022) <https://doi.org/10.1016/j.physa.2022.127863>
- [11] Montanaro, A., Jozsa, R., Mitchison, G.: On exact quantum query complexity. *Algorithmica* **71**(4), 775–796 (2015) <https://doi.org/10.1007/s00453-013-9826-8>
- [12] Beals, R., Buhrman, H., Cleve, R., Mosca, M., Wolf, R.: Quantum lower bounds by polynomials. *Journal of the ACM* **48**(4), 778–797 (2001) <https://doi.org/10.1145/502090.502097>
- [13] Buhrman, H., Wolf, R.: Complexity measures and decision tree complexity: A survey. *Theoretical Computer Science* **288**(1), 21–43 (2002) [https://doi.org/10.1016/S0304-3975\(01\)00144-X](https://doi.org/10.1016/S0304-3975(01)00144-X)
- [14] Montanaro, A., Wolf, R.: A survey of quantum property testing. *Theory of Computing* **7**, 1–81 (2016). ToC Library, Graduate Surveys 7