A GENERALIZATION OF THE DEUTSCH-JOZSA QUANTUM ALGORITHM

Randall R. Holmes and Frederic Texier

Abstract. A quantum algorithm is presented that can be used to distinguish between certain classes of functions on a finite abelian group. The algorithm is patterned after and generalizes one due to Deutsch and Jozsa for distinguishing a constant function from a balanced function on a direct sum of copies of the integers modulo two.

The Deutsch-Jozsa algorithm is a quantum algorithm for distinguishing between two classes of functions with values in $\{0,1\}$ on the set of n-tuples $(a_1,\dots,a_n)$ $(a_i \in \{0,1\})$. One class consists of the constant functions and the other consists of the balanced functions, which, by definition, are those that take on the value 0 for half of the n-tuples and the value 1 for the other half. Using a traditional algorithm for such a determination requires a number of evaluations of the function that grows exponentially with n, while the quantum algorithm requires only two evaluations of the function. The purpose of this note is to present a generalization of this algorithm.

Let $m_1,\dots,m_n$ be positive integers and let $A = \mathbf{Z}_{m_1} \oplus \cdots \oplus \mathbf{Z}_{m_n}$. This is the group of n-tuples $a = (a_1,\dots,a_n)$, $0 \le a_i < m_i$, under the addition given by $a + b = (a_1 + b_1,\dots,a_n + b_n)$, where $a_i + b_i$ is addition modulo m_i. Any finite abelian group is isomorphic to such a direct sum for appropriate n and m_i $(1 \le i \le n)$.

Denote by $\mathcal{F}$ the additive group of all functions $A \to \mathbf{Z}_m$, where m is the least common multiple of $m_1,\dots,m_n$. For $f, g \in \mathcal{F}$, the sum $f+g \in \mathcal{F}$ is defined by $(f+g)(a) = f(a)+g(a)$ (sum modulo m). For $a \in A$, define $\iota_a \in \mathcal{F}$ by

$$\iota_a(b) = a \circ b := \sum_{i=1}^{n} a_i b_i m/m_i \in \mathbf{Z}_m.$$

Note that if $m_1 = m_2 = \cdots = m_n$, then $a \circ b$ is the usual inner product of a and b.

Let ϵ be a primitive mth root of unity, that is, a complex number satisfying $\epsilon^m = 1$ and $\epsilon^k \ne 1$ for all $0 < k < m$. One could take $\epsilon = e^{2\pi\sqrt{-1}/m}$, for instance.

For $f \in \mathcal{F}$, put

$$\varphi(f) = \sum_{a \in A} \epsilon^{f(a)} \in \mathbf{C}.$$

Given a subset P of A, we shall say that $f \in \mathcal{F}$ is *P-based* if $\varphi(\iota_a - f) = 0$ for each $a \in A \backslash P$ (= complement in A of P). Theorems 1 and 3 below provide examples of P-based functions.

The Problem. Let $\{P_1,\dots,P_t\}$ be a partition of A, so that $A = P_1 \cup \cdots \cup P_t$ and $P_i \cap P_j = \emptyset$ for $i \ne j$. Let f be an element of $\mathcal{F}$ and suppose that f is P_k-based for some k. Then this k is

1991 *Mathematics Subject Classification.* 81P68.

uniquely determined (see Remark 1 below); we present a quantum algorithm for its determination. The Deutsch-Jozsa algorithm is recovered as a special case (see Remark 2).

The Algorithm. For each integer i with $1 \leq i \leq n$, let H_i be a Quantum Probability Space (QPS) with basis $\{|j\rangle : j \in \mathbf{Z}_{m_i}\}$. If $m_i = 2$, then H_i is called a *qubit*, and an example of such is the z-spin state space of an electron. In general, H_i might be taken to be the z-spin state space of an appropriate particle, necessarily a fermion if m_i is even and a boson if m_i is odd [3, p. 139].

Put $H' = H_1 \otimes \cdots \otimes H_n$. We shall require an additional QPS H_{n+1} with basis $\{|z\rangle : z \in \mathbf{Z}_m\}$ for the storage of images $f(a)$. The vector space $H := H' \otimes H_{n+1}$ has (standard) basis $\{|a\rangle|z\rangle : a \in A, z \in \mathbf{Z}_m\}$, where $|a\rangle|z\rangle := |a_1\rangle \otimes \cdots \otimes |a_n\rangle \otimes |z\rangle$.

If we view H_i as the vector space of m_i-dimensional column vectors over $\mathbf{C}$ by identifying $|j\rangle$ with the column vector having a one in the $(j+1)$st position and zeros elsewhere, then the operator $R_i : H_i \to H_i$ given by

$$R_i(|k\rangle) = m_i^{-1/2} \sum_{j=0}^{m_i-1} \epsilon^{kjm/m_i}|j\rangle$$

($k \in \mathbf{Z}_{m_i}$) has matrix representation $m_i^{-1/2}\left[\epsilon^{kjm/m_i}\right]_{jk}$. Since $[\epsilon^{kjm/m_i}]_{jk}$ is the character table of $\mathbf{Z}_{m_i}$, it follows from the orthogonality relations [1, p. 20] of irreducible characters (or by direct computation) that R_i is unitary and thus so is the (generalized) Hadamard operator $R = R_1 \otimes \cdots \otimes R_n : H' \to H'$. We have

$$R(|b\rangle) = |A|^{-1/2} \sum_{a \in A} \epsilon^{b \circ a}|a\rangle$$

($b \in A$).

For $f \in \mathcal{F}$, we define $U_f : H \to H$ by

$$U_f(|a\rangle|z\rangle) = |a\rangle|z + f(a)\rangle$$

($a \in A$, $z \in \mathbf{Z}_m$). Since U_f permutes the standard basis vectors, it is clearly unitary. We remark that in the special case $n = 1$, $m_1 = 2$, $f =$ identity map on $\mathbf{Z}_2$, the operator U_f is precisely the "controlled-not" gate for which possible physical implementations have been suggested (see [1] for instance).

Finally, take as generalization of the z-spin operator σ_z the unitary operator $\sigma : H_{n+1} \to H_{n+1}$ given by $\sigma(|z\rangle) = \epsilon^z|z\rangle$ ($z \in \mathbf{Z}_m$), which has matrix representation $\mathrm{diag}(1, \epsilon, \epsilon^2, \ldots, \epsilon^{m-1})$.

We now proceed just as in the Deutsch-Jozsa algorithm. We initialize our system to the state $|0\rangle|0\rangle$ and then apply unitary operators as follows:

$$\begin{aligned}
|0\rangle|0\rangle &\overset{R\otimes 1}{\longmapsto} |A|^{-1/2} \sum_{a \in A} |a\rangle|0\rangle \\
&\overset{U_{-f}}{\longmapsto} |A|^{-1/2} \sum_{a \in A} |a\rangle|-f(a)\rangle \\
&\overset{1\otimes\sigma}{\longmapsto} |A|^{-1/2} \sum_{a \in A} |a\rangle\epsilon^{-f(a)}|-f(a)\rangle \\
&\overset{U_f}{\longmapsto} |A|^{-1/2} \sum_{a \in A} |a\rangle\epsilon^{-f(a)}|0\rangle \\
&\overset{R\otimes 1}{\longmapsto} |A|^{-1} \sum_{b \in A} |b\rangle|0\rangle \sum_{a \in A} \epsilon^{a \circ b}\epsilon^{-f(a)}.
\end{aligned}$$

Since $\sum_{a\in A}\epsilon^{a\circ b}\epsilon^{-f(a)} = \varphi(\iota_b - f)$, and since $\varphi(\iota_b - f) = 0$ for each $b \in A\backslash P_k$ (f is P_k-based), this last expression equals

$$|A|^{-1}\sum_{b\in P_k}|b\rangle|0\rangle\varphi(\iota_b - f).$$

It follows that a measurement at this point will produce a state $|b\rangle$ for some $b \in P_k$, and hence k will be determined.

Remark 1. If $f \in \mathcal{F}$ is P_k-based, then, although it is not obvious from the definition, it follows from the algorithm that f is not P_j-based for any $j \neq k$.

Theorem 1. *For a subset P of A and an element a of A, the function $\iota_a \in \mathcal{F}$ is P-based if and only if $a \in P$.*

Proof. Given $a \in A$, the function $\chi_a : A \to \mathbf{C}^\times$ (= group of nonzero complex numbers under multiplication) given by $\chi_a(b) = \epsilon^{a\circ b}$ is easily seen to be a homomorphism and therefore an irreducible character of A. Moreover, $\chi_a \neq \chi_b$ for $a, b \in A$ with $a \neq b$.

Fix $a, b \in A$. We have

$$\varphi(\iota_b - \iota_a) = \sum_{c\in A}\epsilon^{\iota_b(c)-\iota_a(c)} = \sum_{c\in A}\epsilon^{b\circ c}\epsilon^{a\circ(-c)} = \sum_{c\in A}\chi_b(c)\chi_a(-c) = |A|\delta_{ba},$$

where δ_{ba} (= Kronecker delta) is one or zero according as $b = a$ or $b \neq a$, and where the last equality is from an orthogonality relation [1, p. 20].

Let P be a subset of A. If $a \in P$, then $\varphi(\iota_b - \iota_a) = 0$ for every $b \in A\backslash P$, implying that ι_a is P-based. On the other hand, if $a \notin P$, then $\varphi(\iota_a - \iota_a) = |A| \neq 0$, implying that ι_a is not P-based. The result follows. □

It is not obvious that the algorithm presented above generalizes that of Deutsch and Jozsa. We next consider a generalization of the notion of a balanced function and show in Theorem 3 that our algorithm can be used in this setting to obtain a generalization of the Deutsch-Jozsa algorithm that more closely resembles it.

Let f be a function in $\mathcal{F}$ and let B be a subset of A. We say that f is *balanced on B* if $f(B)$ is a coset C of a nontrivial subgroup of $\mathbf{Z}_m$ and the cardinality $|f|_B^{-1}(c)|$ ($c \in C$) does not depend on the choice of c, that is, $f|_B$ takes on each element of C the same number of times. Note that if f is balanced on B then, due to the nontriviality of the subgroup in the definition, f is not constant on B.

Theorem 2. *Let B be a subgroup of A. A homomorphism $f : A \to \mathbf{Z}_m$ is either constant on each coset of B or balanced on each coset of B.*

Proof. Let $f : A \to \mathbf{Z}_m$ be a homomorphism and assume that f is not constant on some coset $a + B$ of B. Then there exist $b_1, b_2 \in B$ such that $f(b_1 - b_2) = f(a + b_1) - f(a + b_2) \neq 0$. This implies that $H := f(B)$ is a nonidentity subgroup of $\mathbf{Z}_m$. Since $\{f|_B^{-1}(h) : h \in H\}$ is precisely the collection of cosets of $K = \ker f|_B$ and since each of these cosets has the same cardinality as K, it follows that $f|_B$ takes on each element of H the same number of times, that is, f is balanced on B. Finally, if $D = d + B$ is an arbitrary coset of B in A, then $f(d+b) = f(d) + f(b)$ for each $b \in B$, so that, by the previous argument, $f|_D$ takes on each element of the coset $f(d) + H$ the same number of times and f is balanced on D as desired. □

Lemma. *If B is a subset of A and f is a function in $\mathcal{F}$ that is balanced on B, then $\sum_{b\in B}\epsilon^{f(b)}=0$.*

Proof. Let H be a nontrivial subgroup of $\mathbf{Z}_m$. Then H is cyclic and is generated by a divisor d of m with $d\neq m$. Let $C=z+H$ be a coset of H. Then $C=\{z+jd : 0\leq j<m/d\}$, so that

$$\sum_{c\in C}\epsilon^c=\sum_{j=0}^{m/d-1}\epsilon^{z+jd}=\epsilon^z\sum_{j=0}^{m/d-1}(e^d)^j=\epsilon^z\cdot\frac{\epsilon^m-1}{\epsilon^d-1}=0,$$

where the next to the last equality is verified by multiplying both sides by ϵ^d-1 and noting the telescoping nature of the resulting sum on the left. The lemma follows. □

Let B be a subgroup of A. Let $\mathcal{F}_B$ be the collection of all functions in $\mathcal{F}$ that are either constant on every coset of B or balanced on every coset of B. Denote by $B^\perp$ the orthogonal complement relative to $\circ$ of B in A:

$$B^\perp=\{a\in A : a\circ b=0 \text{ for all } b\in B\}.$$

Theorem 3. *Let B be a subgroup of A and let f be a function in $\mathcal{F}_B$.*

(1) *f is constant on each coset of B if and only if f is $B^\perp$-based.*
(2) *f is balanced on each coset of B if and only if f is $A\backslash B^\perp$-based.*

Proof. Assume for the moment that we have proved the "only if" part of both statements. Suppose that f is $B^\perp$-based. By Remark 1, f is not $A\backslash B^\perp$-based. Then part (2) says that f is not balanced on some coset of B. Since f is in $\mathcal{F}_B$, we conclude that f is constant on each coset of B. This proves the "if" part of the first statement. The "if" part of the second statement is proved similarly.

Therefore, it remains to prove the "only if" part of each statement.

(1) Assume that f is constant on each coset of B. Let c be an element of $A\backslash B^\perp$. Let $\{a_i+B\}_{1\leq i\leq s}$ be the distinct cosets of B in A. We have

$$\varphi(\iota_c-f)=\sum_{a\in A}\epsilon^{\iota_c(a)-f(a)}=\sum_{i=1}^{s}\sum_{b\in B}\epsilon^{\iota_c(a_i+b)}\epsilon^{-f(a_i+b)}=\sum_{i=1}^{s}\epsilon^{-f(a_i)}\sum_{b\in B}\epsilon^{\iota_c(a_i+b)}.$$

Now c is not in $B^\perp$, so $\iota_c(b)=c\circ b\neq 0$ for some $b\in B$. Since 0 is in B and $\iota_c(0)=0$ it follows that ι_c is not constant on B. Thus, ι_c is balanced on each coset of B by Theorem 2. Using the lemma we now see that the final sum above is zero for each i so that $\varphi(\iota_c-f)=0$ and f is $B^\perp$-based.

(2) Assume that f is balanced on each coset of B. Let d be an element of $B^\perp$. With $\{a_i+B\}_{1\leq i\leq s}$ again the distinct cosets of B in A, we have

$$\begin{aligned}\varphi(\iota_d-f)&=\sum_{a\in A}\epsilon^{\iota_d(a)-f(a)}=\sum_{i=1}^{s}\sum_{b\in B}\epsilon^{\iota_d(a_i+b)}\epsilon^{-f(a_i+b)}\\&=\sum_{i=1}^{s}\epsilon^{d\circ a_i}\sum_{b\in B}\epsilon^{d\circ b}\epsilon^{-f(a_i+b)}=\sum_{i=1}^{s}\epsilon^{d\circ a_i}\sum_{b\in B}\epsilon^{-f(a_i+b)}.\end{aligned}$$

By the lemma, the last sum is zero for each i, so f is $A\backslash B^\perp$-based. □

Remark 2. In the notation of the theorem, $\{B^\perp, A\backslash B^\perp\}$ is a partition of A, so it follows that the algorithm can be used to distinguish between a function that is constant on each coset of B and one that is balanced on each coset of B. This applies in particular to the choice $B=A$. Thus, considering the special case $m_1=m_2=\cdots=m_n=m$, we see that the algorithm can be used to distinguish between a function that is constant (on all of A) and a function that takes on each of the values $0,1,2,\ldots,m-1$ an equal number of times. When $m=2$, this is precisely the situation for the Deutsch-Josza algorithm.

References

1. Isaacs, I. Martin, *Character Theory of Finite Groups*, Dover, 1976.
2. Pittenger, Arthur O., *An Introduction to Quantum Computing Algorithms*, Birkhäuser, 2000.
3. Sudbery, Anthony, *Quantum Mechanics and the Particles of Nature*, Cambridge University Press, 1986.

Department of Mathematics, Auburn University, AL 36849-5310
Department of Physics, Auburn University, AL 36849-5310