A Generalization of the Deutsch-Jozsa Algorithm to Multi-Valued Quantum Logic

Yale Fan
The Catlin Gabel School
8825 SW Barnes Road
Portland, OR 97225-6599, USA
yalefan@gmail.com

Abstract

We generalize the binary Deutsch-Jozsa algorithm to n-valued logic using the quantum Fourier transform. Our algorithm is not only able to distinguish between constant and balanced Boolean functions in a single query, but can also find closed expressions for classes of affine functions in quantum oracles, accurate to a constant term.

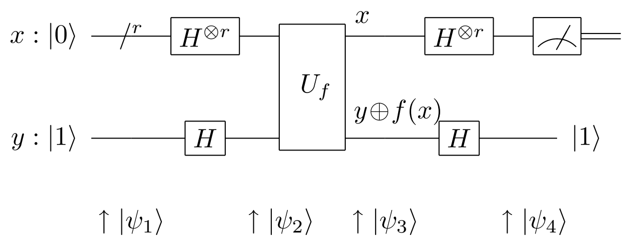

Figure 1. The Deutsch-Jozsa circuit

1 Introduction

The original binary Deutsch-Jozsa algorithm [1] considers a Boolean function of the form $f : \{0,1\}^r \to \{0,1\}$ implemented in a black box circuit, or oracle, U_f. Input states are put in a quantum superposition as query (x) and answer (y) registers so that their state vectors are expressed in terms of the dual basis [3]

$$|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ and } |1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The oracle is defined by its action on the registers $U_f|xy\rangle = |x\rangle|y \oplus f(x)\rangle$, where the $|x\rangle$ register is the tensor product of input states $|x_1\rangle \cdots |x_r\rangle$. When it is promised that the function in question is either constant (returning a fixed value) or balanced (returning outputs equally among 0 and 1), the algorithm decides deterministically which type it is with a single oracle query as opposed to the $2^{r-1}+1$ required classically. The corresponding circuit is shown below ($/^r$ denotes r wires in parallel).

In this paper, we prove an extension of the Deutsch-Jozsa algorithm to arbitrary radices of multi-valued quantum logic. We denote addition over the additive group $\mathbf{Z}_n$ by the operator $\oplus$ and the Kronecker tensor product by $\otimes$.

The Hadamard transform is a special case of the quantum Fourier transform (QFT) in Hilbert space H_n. The well-known Chrestenson gate for ternary quantum computing is also equivalent to the Fourier transform over $\mathbf{Z}_3$. Cereceda [2] has generalized the Deutsch algorithm using two qudits for d-dimensional quantum systems where $d = 2^k$. However, placing no restrictions on the number of computational basis states n leads to a far more versatile characterization of the Deutsch-Jozsa algorithm. The Fourier matrix of order n over the primitive n^{th} roots of unity $\omega^k = e^{i2\pi k/n}$ is given in Figure 2.

$$\mathcal{F}_n = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ 1 & \omega^3 & \omega^6 & \cdots & \omega^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{pmatrix}$$

Figure 2. The QFT as a matrix

Definition 1 *The action of the quantum Fourier transform is described by* $QFT_n : |j\rangle \to \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{i2\pi jk/n}|k\rangle$ *for* $j \in \mathbf{Z}_n$ [3]. *For ease of computation, the QFT can be expressed* *as*

$$\mathcal{F}_n = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} e^{i2\pi jk/n} |j\rangle\langle k|$$

The n-ary quantum Fourier transform gives n normalized rotations of a vector, producing superpositions that differ only in phase. This leads to a redefinition of the dual basis for H_n as

$$\{|0'\rangle, |1'\rangle, \ldots, |n-1'\rangle\} =$$

$$\left\{ \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} |x\rangle, \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} \omega^{x} |x\rangle, \ldots, \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} \omega^{(n-1)x} |x\rangle \right\}$$

2 The *n*-ary Deutsch-Jozsa Algorithm and Affine Functions

We will implement the QFT as a generalization of the Hadamard transform in the multi-valued equivalent of the Deutsch-Jozsa algorithm. First, we cover some extensions by definition.

Definition 2 *An r-qudit multi-valued function of the form $f : \{0, 1, \ldots, n-1\}^r \to \{0, 1, \ldots, n-1\}$ is constant when $f(x) = f(y)\ \forall x, y \in \{0, 1, \ldots, n-1\}^r$ and is balanced when an equal number of the n^r domain values, namely n^{r-1}, is mapped to each of the n elements in the codomain.*

In multi-valued logic, there are n constant functions mapping each element in $\mathbf{Z}_n$ to a fixed element and $n!$ balanced permutative (bijective) mappings of single-qudit inputs. For functions on r qudits, there are accordingly $n^r!/n^{r-1}!^n$ balanced (surjective) mappings.

Theorem 1 *All affine functions defined as $f(x_1, \ldots, x_r) = A_0 \oplus A_1 x_1 \oplus \cdots \oplus A_r x_r$ with $A_0, \ldots, A_r \in \mathbf{Z}_n$ are either constant or balanced functions of r qudits.*

Proof. Those affine functions for which all coefficients $A_{i \neq 0} = 0$ are constant. For affine functions with at least one nonzero coefficient of x_i, each element in the domain $\{0, 1, \ldots, n-1\}^r = \{0, 1, \ldots, n^r - 1\}$ is reducible modulo n to a unique element m of $\mathbf{Z}_n$ because the domain is equivalent to the set $\{m, n-m, 2n-m, \ldots, n^r - n + m\}$ of size n^{r-1}, all of whose members are congruent to m modulo n for every $m \in \{0, 1, \ldots, n-1\}$, a set of size n. Since $f(p) = f(q)$ if $p \equiv q \pmod{n}$, every element in the codomain $\{0, 1, \ldots, n-1\}$ is assigned to exactly n^{r-1} different elements in the domain. Such affine functions satisfy the definition of a balanced function.

The proof of the n-ary Deutsch-Jozsa algorithm will be aided by a trivial lemma:

Lemma 1 *Primitive n^{th} roots of unity satisfy $\sum_{k=0}^{n-1} \omega^{\alpha k} = 0$ for nonzero integers α.*

Proof. Consider the polynomial $z^n - 1 = 0$, of which ω^α is a root. 1 being a real root for all integers n, this can be factorized as $(z-1)(z^{n-1} + z^{n-2} + \cdots + 1) = 0$. Therefore, $\sum_{k=0}^{n-1} z^k = 0$ for $z = \omega^\alpha$ where $z \neq \omega^0 = 1$.

This leads to our main result.

Theorem 2 *The n-ary Deutsch-Jozsa algorithm applied to multi-valued functions of r qudits can both distinguish between constant and balanced functions with a single oracle query and determine a closed expression for an affine function in U_f, excepting the constant term, as follows:*

1. The constant term A_0 is preserved in the phase of the x-register at output (ω^{-A_0}), which is lost during measurement.

2. The coefficients $A_1, \ldots, A_r$ are determined by the state of the x-register at output, $|A_1, \ldots, A_r\rangle$.

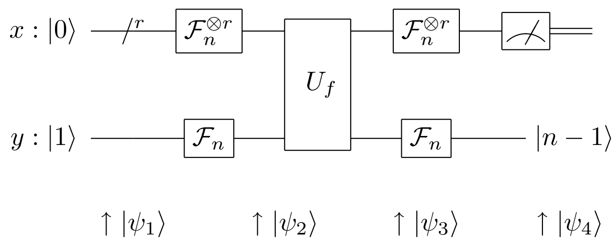

Figure 3. Circuit for the n-ary Deutsch-Jozsa algorithm

In practice, the y-register would not be measured, but we follow through with the calculations for it to demonstrate that its state at the output is constant, regardless of the function in the oracle. The x- and y-registers are written separately as factors of the entire tensored state of the circuit at each step $|\psi_i\rangle$.

First, we consider the case in which the function $f(x)$ hidden in the oracle is constant:

$$|\psi_1\rangle = |0\rangle^{\otimes r} |1\rangle$$

$$\xrightarrow{\mathcal{F}_n^{\otimes r+1}} |\psi_2\rangle = \frac{1}{\sqrt{n^r}} \sum_{x=0}^{n^r-1} |x\rangle \otimes \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} e^{i2\pi y/n} |y\rangle$$

$$\xrightarrow{U_f} |\psi_3\rangle = \frac{1}{\sqrt{n^r}} \sum_{x=0}^{n^r-1} |x\rangle \otimes \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} e^{i2\pi y/n} |y \oplus f(x)\rangle$$

At this point, we can transfer the action of U_f from the basis states themselves onto their phases by observing that if a basis vector $|j \oplus k\rangle$ is appended with the phase ϕ^j, then $|j\rangle$ itself must have phase ϕ^{j-k} by definition. This yields:

$$|\psi_3\rangle = \frac{1}{\sqrt{n^r}} \sum_{x=0}^{n^r-1} |x\rangle \otimes \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} e^{i2\pi[y-f(x)]/n} |y\rangle$$
$$= \frac{1}{\sqrt{n^r}} e^{-i2\pi f(x)/n} \sum_{x=0}^{n^r-1} |x\rangle \otimes \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} e^{i2\pi y/n} |y\rangle$$

Because we assume our function to be constant, $e^{-i2\pi f(x)/n}$ can be regarded as a global phase factor. Subsequently, the QFT on the x-register can be computed explicitly:

$$\mathcal{F}_n{}^{\otimes r} = \frac{1}{\sqrt{n}} \sum_{j=0}^{n^r-1} \sum_{k=0}^{n^r-1} e^{i2\pi jk/n} |j\rangle\langle k|, \text{ giving}$$

$$\xrightarrow{\mathcal{F}_n^{\otimes r+1}} |\psi_4\rangle =$$
$$\frac{1}{n^r} e^{-i2\pi f(x)/n} \sum_{j=0}^{n^r-1} \sum_{k=0}^{n^r-1} \sum_{x=0}^{n^r-1} e^{i2\pi jk/n} |j\rangle\langle k|x\rangle \otimes$$
$$\frac{1}{n} \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} \sum_{y=0}^{n-1} e^{i2\pi(jk \oplus y)/n} |j\rangle\langle k|y\rangle$$

In the standard basis, $\langle k|z\rangle = 0$ when $k \neq z$, while $\langle k|z\rangle = 1$ otherwise. We can hence reduce the above to:

$$|\psi_4\rangle = \frac{1}{n^r} e^{-i2\pi f(x)/n} \sum_{j=0}^{n^r-1} \sum_{k=0}^{n^r-1} e^{i2\pi jk/n} |j\rangle \otimes$$
$$\frac{1}{n} \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} e^{i2\pi(j \oplus 1)k/n} |j\rangle$$

By lemma 1, all basis states $|j\rangle$ in the x-register will have null amplitudes for $j \neq 0$. Similarly, all basis states $|j\rangle$ in the y-register will have null amplitudes for $j \neq n-1$. It follows that

$$|\psi_4\rangle = |0\rangle^{\otimes r} |n-1\rangle$$

with a phase factor of $e^{-i2\pi f(x)/n}$ for all constant functions $f(x)$.

The balanced case is similar. After initializing and superposing our states as above, we obtain:

$$|\psi_3\rangle = \frac{1}{\sqrt{n^r}} \sum_{x=0}^{n^r-1} e^{-i2\pi f(x)/n} |x\rangle \otimes \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} e^{i2\pi y/n} |y\rangle$$

In this case, the phase factor $e^{-i2\pi f(x)/n}$ cannot be assumed to be global because its value is dependent upon x. The output of the y-register will be the same as in the constant case, so we need only to proceed with the state of the x-register. After applying the second QFT:

$$|\psi_3\rangle \xrightarrow{\mathcal{F}_n^{\otimes r}} |\psi_4\rangle$$

$$= \frac{1}{n^r} \sum_{j=0}^{n^r-1} \sum_{k=0}^{n^r-1} \sum_{x=0}^{n^r-1} e^{i2\pi jk/n} e^{-i2\pi f(x)/n} |j\rangle\langle k|x\rangle$$
$$= \frac{1}{n^r} \sum_{j=0}^{n^r-1} \sum_{x=0}^{n^r-1} e^{i2\pi[jx-f(x)]/n} |j\rangle$$

It is now necessary to show that $jx - f(x) =$ some constant C, or $f(x) = jx - C$, for a fixed value of $j \neq 0$ and all x in domain $\{0, 1, \ldots, n^r - 1\}$. This would allow $e^{i2\pi C/n}$, or ω^C, to be the phase factor of some basis state $|j\rangle$ other than $|0\rangle^{\otimes r}$ as in the constant case, with a deterministic probability of measurement. Equivalently, since addition and multiplication are modular, $f(x_1, \ldots, x_r) = -C \oplus j_1 x_1 \oplus \cdots \oplus j_r x_r$ must hold for some $j \in \{1, ..., n^r - 1\}$, j_i representing the i^{th} digit of j. This is the definition of a non-constant affine function, so j exists only when the hidden function in the oracle is affine. The x-register is therefore measured to be:

$$|\psi_4\rangle = e^{i2\pi[jx-f(x)]/n} |j\rangle = \omega^C |j\rangle,$$

$f(x)$ being balanced for $j \neq 0$ and constant otherwise. In consequence, the Deutsch-Jozsa algorithm gives a deterministic output only when $f(x)$ is restricted to being either constant or balanced, *and* affine (we will give an example of the algorithm for a non-affine function below). However, observe that the state $|0\rangle^{\otimes r}$ will have a zero probability of measurement for all balanced functions, whether affine or not, because its amplitude is

$$\frac{1}{n^r} \sum_{x=0}^{n^r-1} e^{i2\pi f(x)/n} \equiv \frac{n^{r-1}}{n^r} \sum_{x=0}^{n-1} e^{i2\pi f(x)/n}$$
$$\equiv \frac{1}{n} \sum_{x=0}^{n-1} e^{i2\pi x/n} = 0$$

by definition 2 and lemma 1. Thus, the algorithm is still deterministic in the sense that it can always distinguish between constant and either affine *or* non-affine balanced functions, although with no fixed output in the latter case.

Finally, the generalized Deutsch-Jozsa algorithm has a useful property that becomes apparent in multi-valued logic; it can not only distinguish between constant and balanced functions, but can determine explicitly the function $f(x_1, \ldots, x_r) = A_0 \oplus A_1 x_1 \oplus \cdots \oplus A_r x_r$ implemented by the oracle excepting the constant term A_0, given that it is affine. As calculated above, the constant term A_0 of such a function is encoded in the phase of the x-register at output ($A_0 = -C$, where the phase is ω^C), while the respective coefficients $A_1, \ldots, A_r$ of x are determined by the basis vector $|j\rangle = |A_1, \ldots, A_r\rangle$. Since the phase of the x-register is lost at measurement, only A_0 cannot be retrieved. We regard affine functions that differ only in the constant term as a "class."

In some variations of the Deutsch-Jozsa algorithm [5], the y-register is unnecessary if the oracle, corresponding to the diagonal operator

$$U_f = \sum_{x=0}^{n^r-1} e^{-i2\pi f(x)/n} |x\rangle\langle x|,$$

directly encodes the action of $f(x)$ into the phase of the x-register. We use this scheme below.

Example 1 (Deutsch-Jozsa for an affine function)

U_f contains the following balanced function defined on two qutrits $|AB\rangle$:

$B \backslash A$	0	1	2
0	1	0	2
1	2	1	0
2	0	2	1

We begin at $|\psi_3\rangle$, after the states have been initialized.

$$|\psi_3\rangle = \frac{1}{3} \begin{pmatrix} \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} \omega^2 \\ \omega \\ 1 \\ 1 \\ \omega^2 \\ \omega \\ \omega \\ 1 \\ \omega^2 \end{pmatrix}$$

Lemma 1 is used for simplification ($1 + \omega + \omega^2 = 0$):

$$\mathcal{F}_n^{\otimes 2} |\psi_3\rangle =$$

$$\frac{1}{9} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \end{pmatrix} \begin{pmatrix} \omega^2 \\ \omega \\ 1 \\ 1 \\ \omega^2 \\ \omega \\ \omega \\ 1 \\ \omega^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \omega^2 \\ 0 \end{pmatrix}$$

$$\Rightarrow |\psi_4\rangle = \omega^2 |21\rangle,$$

from which we derive a closed expression for the affine function $f(x_1, x_2) = A_0 \oplus A_1 x_1 \oplus A_2 x_2$ in U_f, save for the constant term, by taking $\{2, 1\}$ as the respective coefficients A_1 and A_2 (although theoretically, A_0 should be $(-2) \bmod 3 = 1$):

$$f(x_1, x_2) = \text{(Constant)} \oplus 2x_1 \oplus x_2$$

Example 2 (Deutsch-Jozsa for a non-affine function)

U_f contains the following balanced function defined on two qutrits $|AB\rangle$:

$B \backslash A$	0	1	2
0	0	1	2
1	2	0	0
2	1	2	1

Again beginning at $|\psi_3\rangle$:

$$|\psi_3\rangle = \frac{1}{3} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \omega^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{3} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \omega^2 \\ 1 \\ \omega \\ \omega \\ 1 \\ \omega^2 \end{pmatrix}$$

$$\Rightarrow \mathcal{F}_n^{\otimes 2} |\psi_3\rangle =$$

$$\frac{1}{9} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & 1 & 1 & \omega & \omega & \omega & \omega^2 & \omega^2 & \omega^2 \\ 1 & \omega & \omega^2 & \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ 1 & \omega^2 & \omega & \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega & \omega & \omega \\ 1 & \omega & \omega^2 & \omega^2 & 1 & \omega & \omega & \omega^2 & 1 \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 & \omega & 1 & \omega^2 \end{pmatrix} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \\ \omega^2 \\ 1 \\ \omega \\ \omega \\ 1 \\ \omega^2 \end{pmatrix} = \begin{pmatrix} 0 \\ \omega/3 \\ (1+\omega^2)/3 \\ 0 \\ 1/3 \\ 2/3 \\ 0 \\ \omega^2/3 \\ (1+\omega)/3 \end{pmatrix}$$

$$\Rightarrow |\psi_4\rangle = \frac{\omega}{3}|01\rangle + \frac{1+\omega^2}{3}|02\rangle + \frac{1}{3}|11\rangle + \frac{2}{3}|12\rangle + \frac{\omega^2}{3}|21\rangle + \frac{1+\omega}{3}|22\rangle$$

The basis state $|12\rangle$ hence has a $4/9$ probability of measurement, with all others having $1/9$ probability. To determine that this balanced function is non-affine, enough measurements of the x-register are required so as to obtain different states. Furthermore, observe that if the function is not affine, there is still a relatively high probability of measuring the output state of the algorithm that would be associated with a similar affine function. For example, compare the Marquand chart of the non-affine function in U_f above with that of the affine function $f(x_1, x_2) = x_1 \oplus 2x_2$ associated with the output state $|12\rangle$:

$x_2 \backslash x_1$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

Because an affine multi-valued function in our context is defined in terms of the modulo-additive operator $\oplus$, any arbitrary function is affine iff it satisfies the *cyclic group property* (this is easy to determine when the outputs are plotted in a Marquand chart as above, which requires that rows and columns be successive cyclic shifts of each other), and the state after U_f is factorable - e.g., entanglement does not occur in the Deutsch-Jozsa circuit.

Our extended Deutsch-Jozsa algorithm requires only one measurement to deterministically distinguish an expression for an affine function of radix n and r inputs up to the accuracy of a constant, given that it is affine.

3 Conclusion

Although the original Deutsch-Jozsa algorithm is mainly of theoretical interest, its multi-valued extension could potentially find application in image processing to distinguish between maps of texture images encoded by affine functions in a Marquand chart, with the number of colors corresponding to the size of the radix.

Acknowledgements

The author gratefully acknowledges Professor Marek Perkowski of Portland State University Department of Electrical and Computer Engineering for his guidance and Jacob Biamonte of D-Wave Systems, as well as the members of the Portland Quantum Logic Group for their support.

Appendix

For radices higher than 2 in which U_f is merely $r+1$ wires in parallel (implementing the constant function $f : \{0,1\}^r \rightarrow 0$), the initialized state $|0\rangle^{\otimes r}|1\rangle$ is mapped to a different output $|0\rangle^{\otimes r}|n-1\rangle$. Practically, this makes no difference because the output of the y-register is discarded. However, theorem 3 makes clear why this is so.

Theorem 3 *Four iterations of the QFT gives an identity mapping (the binary Hadamard gate is a special case that is also self-inverse).*

Proof. Let $[\mathcal{F}_n]_{pq}$ denote the p,q entry in $\mathcal{F}_n$. Row p and column q of $\mathcal{F}_n$ are given by

$$\langle p| = \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\omega^{k(p-1)}\langle k| \text{ and } |q\rangle = \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}\omega^{k(q-1)}|k\rangle,$$

respectively. $[\mathcal{F}_n^2]_{pq} = \langle p|q\rangle = \frac{1}{n}\sum_{k=0}^{n-1}\omega^{k(p+q-2)}$; $p+q-2$ is some integer α that is nonzero when $(p+q) \bmod n \neq 2$, so by lemma 1, $[\mathcal{F}_n^2]_{pq} = 1$ if $(p+q) \bmod n = 2$ and $[\mathcal{F}_n^2]_{pq} = 0$ otherwise. By definition, all such indices $p, q \in \{1, 2, \ldots, n\}$ for which $[\mathcal{F}_n^2]_{pq} = 1$ satisfy $p+q = C_0 n + 2$ for some $C_0 \in \mathbf{Z}_n$. C_0 is further restricted to $\{0,1\}$ because any larger values of $C_0 n + 2$ exceed the maximum value of $p+q$, or $2n$. Therefore, either $p+q = 2$ or $p+q = n+2$, giving the solution sets

$$p = q = 1 \text{ or } \{p, q\} = \{n-m+1, m+1\}$$

for $m \in \{1, 2, \ldots, n-1\}$, which correspond to the permutation matrix

$$\mathcal{F}_n^2 = \sum_{m=0}^{n-1}|n-m\rangle\langle m|, \; |n\rangle \text{ taken modulo to mean } |0\rangle$$

Thus, (z^* denoting the complex conjugate)

$$\begin{aligned}
\mathcal{F}_n^3 &= \frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1}\sum_{m=0}^{n-1} e^{i2\pi jk/n}|n-m\rangle\langle m|j\rangle\langle k| \\
&= \frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} e^{i2\pi jk/n}|n-j\rangle\langle k| \\
&= \frac{1}{\sqrt{n}}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} (e^{i2\pi jk/n})^*|j\rangle\langle k| \\
&= \mathcal{F}_n^\dagger
\end{aligned}$$

by our previous arguments, and given that $\mathcal{F}_n$ is unitary,

$$\mathcal{F}_n^4 = \mathcal{F}_n\mathcal{F}_n^\dagger = I_n$$

is immediate. This is a property that the QFT shares with the continuous Fourier transform.

References

[1] Deutsch, D. and Jozsa, R. (1992). *Rapid solutions of problems by quantum computation*. Proc. Roy. Soc. Lond. A 439, 553-558.

[2] Cereceda, J. L. (2004). *Generalization of the Deutsch algorithm using two qudits*. Available at quant-ph/0407253.

[3] Jozsa, R. (1997). *Quantum algorithms and the Fourier transform*. Proc. Roy. Soc. Lond. A 454, 323-337.

[4] Perkowski, M. (2005). Lecture notes. Available at http://web.cecs.pdx.edu/~mperkows/seminar.html.

[5] Gruska, J. (1999). *Quantum computing*. Berkshire, UK: McGraw-Hill.

[6] Perry, R. T. (2006). *The temple of quantum computing, version 1.1*. Available at http://www.toqc.com/.