London Mathematical Society ISSN 1461–1570

EXTENDING THE PROMISE OF THE DEUTSCH–JOZSA–HØYER ALGORITHM FOR FINITE GROUPS

MICHAEL BATTY, ANDREW J. DUNCAN AND SAMUEL L. BRAUNSTEIN

Abstract

Høyer has given a generalisation of the Deutsch–Jozsa algorithm which uses the Fourier transform on a group G which is (in general) non-Abelian. His algorithm distinguishes between functions which are either perfectly balanced (m-to-one) or constant, with certainty, and using a single quantum query. Here, we show that this algorithm (which we call the Deutsch–Jozsa–Høyer algorithm) can in fact deal with a broader range of promises, which we define in terms of the irreducible representations of G.

1. *Introduction*

Recall that a function $f : \{0, 1\}^n \to \{0, 1\}$ is called *balanced* if $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$. Deutsch's algorithm [5] distinguishes between constant and balanced functions from $\{0, 1\}$ to itself using a single quantum query, whereas classically two queries are required. A function from $\{0, 1\}$ to itself is always either balanced or constant. However, to generalise to functions $\{0, 1\}^n \to \{0, 1\}$, Deutsch and Jozsa [6] realised that we must restrict the class of functions being considered. They showed that we can distinguish between constant and balanced functions $\{0, 1\}^n \to \{0, 1\}$, again in a single query, but if we are given a function $\{0, 1\}^n \to \{0, 1\}$ which is neither constant nor balanced, then we cannot deduce anything from the output of the quantum circuit. Thus, we must be *promised* that the function is either constant or balanced; then we can use the circuit to deduce something.

It was first realised by Høyer that the mathematics underlying the Deutsch–Jozsa algorithm is group-theoretic in nature. In [12], he remarks that if we replace the discrete Fourier transform on $\mathbb{Z}_2^n$ employed in the Deutsch–Jozsa algorithm by the Fourier transform on an arbitrary finite group, then we can distinguish between constant and perfectly balanced functions. In this paper we show that the range of functions that can be distinguished is broader than this, provided that we make corresponding promises. These promises are representation-theoretic in nature, further reflecting the role played by finite groups in the Deutsch–Jozsa circuit.

The definitions of the types of functions that we consider seem at first sight somewhat technical, and perhaps unnatural. However, given a map $f : X \to H$, where H is a finite group, we associate an element r of the integral group ring $\mathbb{Z}H$ to f in such a way that the promise on the function becomes a promise on the element r: namely, that r lies in one of two subsets of $\mathbb{Z}H$ which have natural and straightforward descriptions (see Section 4).

In the case of functions $f : X \to A$ where A is an Abelian group, our promises can be described in terms of a polynomial P_f associated to f. In fact, as we show in Section 4, our

This research was supported by EPSRC MathFIT grant number GR/87406. The third author currently holds a Royal Society Wolfson Research Merit Award.
Received 9 December 2004, revised 22 August 2005; *published* 30 January 2006.
2000 Mathematics Subject Classification 68Q05, 81P68, 81R99

representation-theoretic promise is equivalent to the promise that P_f is either monomial or divisible by the nth cyclotomic polynomial, where $n = |A|$ (see Appendix B). If n has at most 2 distinct prime divisors, then this gives rise to a further characterisation of the promise on f in terms of certain subgroups of A.

The paper is structured as follows. In Sections 2 and 3 we describe quantum oracles for group multiplication and give a definition of the quantum Fourier transform, convenient for our purposes. In Section 4 we define our representation-theoretic versions of constant and balanced functions, characterise these types of function in terms of the integral group ring, discuss the case where the codomain is Abelian, and give examples where the codomain is non-Abelian. Section 5 explains how the Deutsch–Jozsa circuit is used to distinguish between constant and balanced functions, of this kind. Section 6 lists various other algorithms which are special cases of our algorithm. Appendix A gives a brief introduction to group representation theory and the 'Weyl trick'. Appendix B covers the number theory used in Section 4.

2. *A quantum oracle for group multiplication*

The following definition generalises the notion of a qubit.

DEFINITION 2.1. Let X be a finite set. A *qu$X$* is a complex vector space spanned by $\{|x\rangle \mid x \in X\}$.

For example, a qubit is a qu$\{0, 1\}$.

Suppose that G is a finite group and X is a finite set. Write $\mathrm{Sym}(X)$ for the group of permutations of X. Suppose that we are also given a function (not necessarily a homomorphism) $\theta : G \to \mathrm{Sym}(X)$. Define a map $\phi : G \times X \to G \times X$ by the rule $\phi : (g, x) \mapsto (g, [\theta(g)](x))$. If $\phi(g, x) = \phi(h, y)$, then $g = h$ and $[\theta(g)](x) = [\theta(g)](y)$, in which case $x = y$, as $\theta(g)$ is a permutation; that is, ϕ is an injection, and as $G \times X$ is finite, it is a bijection. Now suppose that we have a quantum system $\mathbb{C}^{G\times X} \cong \mathbb{C}^G \otimes \mathbb{C}^X$ comprising two quantum registers, a qu$G$ and a qu$X$. Then there is a unitary map U which permutes the basis states of this system:

$$U : |g, x\rangle \mapsto |g, [\theta(g)](x)\rangle.$$

In particular, consider the following case. Suppose that X is a group H and $f : G \to H$ is a function (not necessarily a homomorphism). Define $[\theta(g)]h = f(g)h$. Then

$$U : |g, x\rangle \mapsto |g, f(g)h\rangle,$$

and we say that U is the *H-multiplication oracle* for the function $f : G \to H$. For example, suppose that $G \cong (Z_2)^n$ and $H \cong (Z_2)^m$. Then we recover the usual exclusive-OR oracle

$$U : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle.$$

3. *Representations and non-Abelian Fourier transforms*

3.1. *Irreducible representations and the quantum Fourier transform*

The quantum Fourier transform is an essential subroutine in nearly all the quantum algorithms developed to date. First we define the transform, and then we briefly discuss its implementation. Recall that every finite group G has only finitely many irreducible representations (see Appendix A). By application of the 'Weyl trick' (Appendix A), we may

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

convert any finite-dimensional representation ρ of G into an equivalent unitary representation ρ', and if ρ is irreducible, then so is its unitarization ρ' (since it is equivalent to ρ). Let the (unitarized) irreducible representations of the finite group G be $\rho^1, \ldots, \rho^r$ (from now on, we will omit the primes). Then these representations are used to define the quantum Fourier transform on G. It is well known that $\sum_{j=1}^{r} (\dim \rho^j)^2 = |G|$ (see, for example, [8]). Let

$$R = \{(i, j, k) \mid 1 \leqslant i, j \leqslant \dim \rho^k, 1 \leqslant k \leqslant r\}.$$

Then $|R| = |G|$ and we may specify a (non-canonical) bijection $\beta : G \to R$. Writing ε_G for the identity element of G, suppose also that $\beta(\varepsilon_G) = (1, 1, 1)$ and that ρ^1 is the trivial representation. (This will aid calculations later.) Note that every matrix entry $\rho^k_{i,j}$ of an irreducible representation ρ^k is a function from G to $\mathbb{C}$, since the matrices in the representation vary over G. For ease of notation, write $\beta(g) = (i_g, j_g, k_g)$, and then write ρ^g for the function from G to $\mathbb{C}$ defined by

$$\rho^g(g') = \rho^{k_g}_{i_g, j_g}(g') \qquad \text{for all } g' \in G,$$

the (i_g, j_g)th matrix entry of the k_gth irreducible representation. Also, write $\dim(g)$ for $\dim(\rho^{k_g})$. Then the Schur orthogonality relations (see [21, p. 251, Theorem 1. (1), (2)]) tell us that

$$\langle \rho^{g_1}, \rho^{g_2} \rangle =^{\text{defn}} \sum_{g' \in G} \rho^{g_1}(g') \overline{\rho^{g_2}(g')} = \begin{cases} \dfrac{|G|}{\dim(g)} & \text{if } g_1 = g_2 = g, \\ 0 & \text{otherwise,} \end{cases}$$

which is to say that $\{\rho^g\}_{g \in G}$ is an orthogonal basis for $L^2(G)$, the inner product space of the functions $f : G \to \mathbb{C}$ under pointwise addition, scalar multiplication and the above inner product. If we define $\tau^g_G = \rho^g . \sqrt{(\dim g)/|G|}$, then

$$\langle \tau^{g_1}, \tau^{g_2} \rangle = \begin{cases} 1 & \text{if } g_1 = g_2, \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

so $\{\tau^g_G\}_{g \in G}$ is an ortho*normal* basis. Note that in particular we have

$$\tau^{\varepsilon_G}_G = \frac{1}{\sqrt{|G|}}. \tag{2}$$

We define the *quantum Fourier transform on* G (with respect to the bijection β which is suppressed in the notation) to be the unitary map $\mathcal{F}_G : \mathbb{C}^G \to \mathbb{C}^G$ defined for all $g \in G$ by

$$\mathcal{F}_G |g\rangle = \sum_{g' \in G} \tau^g_G(g') |g'\rangle.$$

The conjugate transpose of $\mathcal{F}_G$ is given by

$$\mathcal{F}^\dagger_G |g\rangle = \sum_{g' \in G} \overline{\tau^{g'}_G(g)} |g'\rangle.$$

That is, the matrix of $\mathcal{F}_G$ is given by $(\mathcal{F}_G)_{g,g'} = \tau^g_G(g')$, and the matrix of $\mathcal{F}^\dagger_G$ is given by

$$(\mathcal{F}^\dagger_G)_{g,g'} = \overline{\tau^{g'}_G(g)}.$$

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

We have

$$\begin{aligned}\mathcal{F}_G^\dagger \mathcal{F}_G |g\rangle &= \mathcal{F}_G^\dagger \sum_{g' \in G} \tau_G^g(g')|g'\rangle \\ &= \sum_{g',g'' \in G} \tau_G^g(g')\overline{\tau_G^{g''}(g')}|g''\rangle \\ &= \sum_{g'' \in G} \delta_{g,g''}|g''\rangle \qquad \text{(by (1))} \\ &= |g\rangle.\end{aligned}$$

This further implies that

$$\mathcal{F}_G \mathcal{F}_G^\dagger = I, \tag{3}$$

since if $AB = I$ for any square (finite-dimensional) matrices A and B of the same size, then it follows that we also have $BA = I$. Thus $\mathcal{F}_G$ is unitary.

The quantum Fourier transform can be efficiently implemented in the case where G is a finitely generated Abelian group using the classical 'Fast Fourier Transform' [**20, 4**]. Note that by an 'efficient algorithm' is meant one which runs in time polynomial in $\log(|G|)$. It is still unknown whether or not there is an efficient algorithm for the quantum Fourier transform over an arbitrary finite group, although such algorithms exist in many cases [**1, 11, 15, 7, 19, 18**]. In [**16**], Moore, Rockmore and Russell survey and extend the results cited above, describing efficient algorithms for the quantum Fourier transform in several classes of groups including: the symmetric groups S_n; wreath products $K \wr S_n$, where $|K|$ is bounded by a polynomial in n; metacyclic groups (a group G is metacyclic if it has a cyclic normal subgroup K such that G/K is cyclic); and metabelian groups (a group G is metabelian if it has an Abelian normal subgroup K such that G/K is Abelian). In particular, all the groups in the examples of Section 4.2 below are covered by these classes.

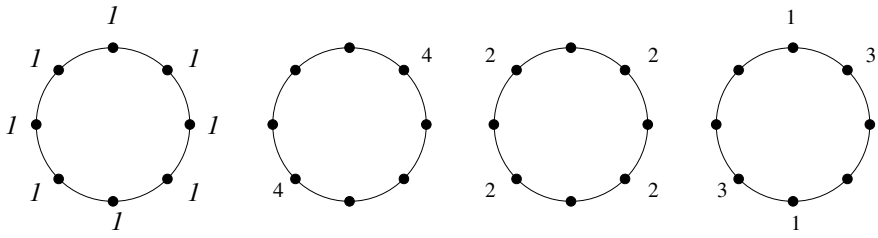
4. *Generalisations of constant and balanced functions*

Let X be a finite set, let H be a finite group, and let $f : X \to H$ be a function. We assume the notation from the previous section for representations of finite groups. When we wish to apply the quantum Fourier transform to the set X, we regard it as the cyclic group $\mathbb{Z}_n$, where $|X| = n$.

DEFINITION 4.1. Let ρ^k be an irreducible (unitary) representation of H. Let $n = \dim \rho^k$, and suppose that $i \in \{1, \ldots, n\}$. We say that f is ρ_i^k*-constant* if for each $r \in \{1, \ldots, n\}$ there exists a constant $c_r \in \mathbb{C}$ such that for all $g \in X$ we have $\tau_{i,r}^k(f(g)) = c_r$.

If χ is a linear (one-dimensional) representation of H, then we may simply refer to f being 'χ-constant'. Recall that linear representations coincide with their characters, and that the set of linear representations of H forms a group. In the case of an Abelian group, the irreducible representations are all linear and we denote this group by $\hat{H}$ (see Section 4 below). If H is an Abelian group and $h \in H$, then we adopt the practice of referring to 'h-balanced', meaning χ-balanced, where χ is the character corresponding to h under the canonical isomorphism between H and its group of characters $\hat{H}$. Note that if χ_0 is the trivial character of H, then every function from X to H is χ_0-constant, so we normally only consider χ-constant functions for non-trivial characters χ.

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press



(a) Surjective (b) 2-valued (c) 4-valued, evenly (d) 4-valued, unevenly

Figure 1: 1-balanced functions into $\mathbb{Z}_8$.

Let $H = \mathbb{Z}_n$, and let the set of irreducible characters of H be $\{\chi_k\}_{k\in H}$, where

$$\chi_k(x) = \exp\left(\frac{2\pi ikx}{n}\right), \qquad \text{for } x \in H.$$

Then $f : X \to H$ is k-constant if and only if there exists a complex number $e^{i\theta}$ ($\theta \in \mathbb{R}$) such that for all $s \in X$, $e^{2\pi ikf(s)/n} = e^{i\theta}$.

Example 4.2. Suppose that f is k-constant and that, for simplicity, $\theta = 0$. Then $f(s) = nr/k$ for some integer r, and for all $s \in X$. For example, let $n = 8$. Then f is 1-constant if and only if $f \equiv 0$; f is 2-constant if and only if $f(X) \subset \{0, 4\}$, and f is 4-constant if and only if $f(X) \subset \{0, 2, 4, 6\}$. To say that f is 3-constant, 5-constant or 7-constant means that $f \equiv 0$. To say that f is 6-constant means that $f(s) = 4r/3$, which means that $f(s) \subset \{0, 4\}$, for all $s \in X$.

Definition 4.3. Let ρ^k be an irreducible (unitary) representation of H. Let $n = \dim \rho^k$ and suppose that $i \in \{1, \ldots, n\}$. We say that $f : X \to H$ is ρ^k_i-*balanced* if for all $r \in \{1, \ldots, n\}$ we have $\sum_{g\in X} \tau^k_{i,r}(f(g)) = 0$.

As before, we can refer to f being 'χ-balanced' in the case where χ is a linear representation of H.

The trivial representation χ_0 of H is the map sending every element of H to $1 \in \mathbb{C}$. Therefore f can never be χ_0-balanced, and we usually consider only χ-balanced functions f where χ is non-trivial.

Again, if $f : X \to \mathbb{Z}_n$ then to say that f is k-balanced is to say that $\sum_{s\in X} e^{2\pi ikf(s)/n} = 0$.

Example 4.4. Suppose that $X = H = \mathbb{Z}_n$, $k = 1$ and $n = 8$. One possibility is that f is surjective, but this is not necessarily the case. For example, f could take four values of 1 and four values of 5. In Figures 1(a) and 1(b) we illustrate these possibilities, showing each of the eighth roots of unity labelled with the number of elements of X mapping to it under $\chi_1 \circ f$. Two of the other possibilities are illustrated in Figure 1(c), where f takes values 1, 3, 5 and 7 twice each, and in Figure 1(d), where f takes the values 2 and 6 once each and the values 1 and 5 three times each.

The definitions of ρ^k_i-constant and balanced functions are in a form that is convenient for computation, as we shall see in Section 5. By contrast, the following characterisations of such functions, in terms of the integral group ring of H, emphasise their structural properties.

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

Let $\mathbb{Z}H$ denote the integral group ring of H, $\mathbb{Z}H = \bigoplus_{h\in H} \mathbb{Z}h$. If T is a subset of H, then define $\mathbb{Z}T = \sum_{t\in T} \mathbb{Z}t$. As usual, by an H-module we mean a $\mathbb{Z}H$-module. Recall that if ρ is a representation of H of dimension n, then H acts on the right on $\mathbb{C}^n$ by

$$v \cdot h = v\rho(h), \qquad \text{for } v \in \mathbb{C}^n \text{ and } h \in H,$$

where we regard v as a row-vector of length n and $\rho(h)$ as an $n \times n$ matrix over $\mathbb{C}$. This action of H extends by linearity to an action of $\mathbb{Z}H$ on $\mathbb{C}^n$, which is in this way a right H-module. For $v \in \mathbb{C}$, define the *annihilator* of $\langle v\rangle$ (with respect to ρ) to be

$$\mathrm{Ann}(v) = \{r \in \mathbb{Z}H : v \cdot r = 0\}.$$

Then $\mathrm{Ann}(v)$ is a right ideal of $\mathbb{Z}H$. We also define the *stabiliser*, in H, of an element $v \in \mathbb{C}^n$ to be

$$\mathrm{Stab}_H(v) = \{h \in H : v \cdot h = v\}.$$

Since H is finite, we may assume that $H = \{h_1, \ldots, h_d\}$, where $d = |H|$. Given $f : X \to H$, define

$$m_j = |f^{-1}(h_j)|, \qquad j = 1, \ldots, d;$$

so $m_j \geqslant 0$ and $\sum_{j=1}^d m_j = |X|$. We call an element $r = \sum_{j=1}^d a_j h_j$ of $\mathbb{Z}H$ *admissible* if $a_j \geqslant 0$ and $\sum_{j=1}^d a_j = |X|$.

Definition 4.5. Given $f : X \to H$, the element

$$r_f = \sum_{j=1}^{d} m_j h_j \in \mathbb{Z}H$$

is called the *element of $\mathbb{Z}H$ associated to f*.

We denote the ith standard basis element, the row-vector which is zero everywhere except the ith coordinate which is 1, by e_i. Given an irreducible representation ρ of H, we define

$$\tau = \sqrt{\frac{\dim(\rho)}{|H|}}\rho.$$

This is consistent with the definitions of Section 3.1 since, using the notation of that section, we have $\tau_{i_h, j_h} = \tau_H^h$. The first statement of the following theorem is due to S. Linton.

Theorem 4.6. *Let $f : X \to H$ be a map, let ρ be an irreducible representation of H, let r_f be the element of $\mathbb{Z}H$ associated to f, and let $S = \mathrm{Stab}_H(e_i)$. Then*

(i) *f is ρ_i-constant if and only if $r_f \in \mathbb{Z}T$, where T is a coset $T = Sh$ of S in H, with $h \in \mathrm{Im}(f)$; and*

(ii) *f is ρ_i-balanced if and only if $r_f \in \mathrm{Ann}(e_i)$.*

Proof. By definition, f is ρ_i-constant if and only if there exists $c = (c_1, \ldots, c_r) \in \mathbb{C}^n$ such that

$$(\tau_{i,1}(f(g)), \ldots, \tau_{i,n}(f(g)) = c,$$

for all $g \in X$. The left-hand side of the equality above is $e_i\tau(f(g))$, so f is ρ_i-constant if and only if

$$e_i \cdot f(g) = e_i\rho(f(g)) = c',$$

where $c' = \sqrt{|\dim(\rho)|/|H|}c$, for all $g \in X$.

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

Choose $h \in \mathrm{Im}(f)$; so $e_i \cdot h = c'$. If $h' \in H$, then $e_i \cdot h' = c' = e_i \cdot h$ if and only if $h' = sh$, for some $s \in S$. Thus $\{h' \in H : e_i \cdot h' = c'\} = T$, where $T = Sh$. It follows that f is ρ_i-constant if and only if $\mathrm{Im}(f) \in T$; if and only if $r_f \in \mathbb{Z}T$. As h is an arbitrary element of $\mathrm{Im}(f)$, the first statement of the theorem now follows.

The function f is ρ_i-balanced if and only if

$$0 = \sum_{g \in X} \tau_{i,r}(f(g)) = \sum_{j=1}^{d} m_j \tau_{i,r}(h_j),$$

for $r = 1, \ldots, n$; that is, if and only if

$$0 = \sum_{j=1}^{d} m_j (\tau_{i,1}(h_j), \ldots, \tau_{i,n}(h_j)) = e_i \sum_{j=1}^{d} m_j \tau(h_j).$$

Since τ and ρ differ only by a constant, this holds if and only if

$$0 = e_i \sum_{j=1}^{d} m_j \rho(h_j) = e_i \cdot \sum_{j=1}^{d} m_j h_j;$$

that is, if and only if $r_f \in \mathrm{Ann}(e_i)$, as required. □

As is clear from the proof above, f is ρ_i-constant if and only if $\mathrm{Im}(f) \subset T$, where T is an appropriate coset of $\mathrm{Stab}_H(e_i)$. Thus we may characterise ρ_i-constant functions without reference to the group ring. However, there does not appear to be such a simple characterisation of ρ_i-balanced functions, for which we need to pass to the group ring. To compare the two, we then need to recast the characterisation of ρ_i-constant in similar terms.

Note that if $X = \{x_1, \ldots, x_n\}$ then, classically, we may compute $f(x_j)$, for $j = 1, \ldots, n/2$, and find that $e_i \cdot f(x_j) = c$, for all such j. If $f(x_{j+1})$ is such that $e_i \cdot f(x_{j+1}) = c$, then f is ρ_i-constant. However, if $e_i \cdot f(x_j) = -c$, for $j = n/2 + 1, \ldots, n$, then f is ρ_i-balanced. Hence we can distinguish, with certainty, between ρ_i-constant and ρ_i-balanced functions, using classical computation, only after making $n/2 + 1$ calls to the oracle for f. Therefore a classical algorithm cannot solve this problem in polynomial time. In Section 5 we show that for the same purpose a quantum algorithm requires only one call to the quantum oracle for f. Thus, as in the case of the standard Deutsch–Jozsa algorithm, quantum computation gives an improvement in speed which seems impressive. However, as the number of admissible elements of $\mathrm{Stab}_H(e_i)$ is much smaller, in general, than the number of admissible elements in $\mathrm{Ann}(e_i)$, by using a classical algorithm we can quickly distinguish between a ρ_i-constant and ρ_i-balanced functions, to within a bounded probability of error. To be more exact: in Section 6 below we observe that the original Deutsch–Jozsa algorithm may be viewed as a special case of our algorithm. In this case we can use a classical algorithm to determine whether f is ρ_i-constant or ρ_i-balanced, with probability of error less than $1/2$, in two calls to the oracle evaluating f (see, for example, [17]); so the problem lies in the complexity class BPP. Hence in general if we accept bounded error computation, then our quantum algorithm gives only a constant-factor improvement over a classical algorithm. However, it should be emphasised the quantum algorithm gives an exact answer, so the more general problems described here lie in complexity class EQP.

4.1. *Finite Abelian groups*

In Section 3 we made use of a bijection $\beta : G \to R$, where R is a set which indexes all the matrix entries of the unitarized irreducible representations of G. In the general case

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

there is no canonical choice of β. In some cases, however, it is clear which bijection to choose, and this lends extra structure to the Fourier transform. One such case is that of an Abelian group A, where every irreducible representation is one-dimensional. In this case the irreducible representations coincide with the characters of A and form a group, denoted $\hat{A}$, of the same order as A. Suppose that $A = \mathbb{Z}_n$ is a cyclic group, under addition mod n, and let the characters of A be ρ^k, where $\rho^k(a) = e^{2\pi i ak/n}$, $k = 0, \ldots, n$. Then $k \mapsto \rho^k$ is an isomorphism between A and $\hat{A}$.

This generalises to the case where A is an arbitrary finite Abelian group, say $A = \bigoplus_{j=1}^{k} \mathbb{Z}_{n_j}$, of order $n = \prod n_j$, as follows. Let $m = (m_1, \ldots, m_k) \in A$, and let $\rho^{j,i}$ be the ith character of $\mathbb{Z}_{n_j}$, as above. Then the map

$$m = (m_1, \ldots, m_k) \mapsto \prod_{j=1}^{k} \rho^{j,m_j} = \rho_A^m$$

is an isomorphism between A and $\hat{A}$. So, for fixed m and all $a = (a_1, \ldots, a_k) \in A$, we have

$$\begin{aligned} \tau_A^m(a) &= \frac{1}{\sqrt{n}} \prod_{j=1}^{k} \rho^{j,m_j}(a_j) = \frac{1}{\sqrt{n}} \prod_{j=1}^{k} e^{2\pi i a_j m_j/n_j} \\ &= \frac{1}{\sqrt{n}} \exp\left(2\pi i \sum_{j=1}^{k} \frac{a_j m_j}{n_j}\right). \end{aligned} \tag{4}$$

Now set $k_j = n/n_j$, for $j = 1, \ldots, k$, and define

$$\phi_m : A \to \mathbb{Z}_n \qquad \text{by} \qquad \phi_m(a) = \left(\sum_{j=1}^{k} a_j m_j k_j\right) \bmod n.$$

Then ϕ_m is a well-defined map from A to $\mathbb{Z}_n$ (which is a homomorphism but not, in general, an isomorphism). Define $f_m = \phi_m \circ f$, a map from X to $\mathbb{Z}_n$. From (4), we have

$$\begin{aligned} \tau_A^m(a) &= \frac{1}{\sqrt{n}} \exp\left(\frac{2\pi i}{n} \sum_{j=1}^{k} a_j m_j k_j\right) \\ &= \frac{1}{\sqrt{n}} \exp\left(\frac{2\pi i}{n} \phi_m(a)\right) \\ &= \tau_{\mathbb{Z}_n}^1(\phi_m(a)). \end{aligned}$$

Therefore $\tau_{\mathbb{Z}_n}^1 \circ f_m = \tau_A^m \circ f$ and we have the following lemma.

LEMMA 4.7. *In the notation above, f is m-constant if and only if f_m is 1-constant, and f is m-balanced if and only if f_m is 1-balanced.*

In the light of this lemma, if the codomain of f is Abelian we may always assume that it is cyclic.

We shall now analyse more carefully the condition that $f : X \to H$ is k-constant or k-balanced when H is the finite cyclic group $\mathbb{Z}_n$ and $0 \leqslant k < n$. Let $d = \gcd(k, n)$, and suppose that $k = ud$ and $n = vd$. Let $\langle v \rangle$ be the subgroup of $\mathbb{Z}_n$ generated by v. Then $\mathbb{Z}_v \cong \mathbb{Z}_n/\langle v \rangle$, and there is a canonical homomorphism $\pi : \mathbb{Z}_n \to \mathbb{Z}_v$. Let $\bar{f} = \pi \circ f$, so $\bar{f}(a) = f(a) \bmod v$, for $a \in \mathbb{Z}_n$.

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

PROPOSITION 4.8. *In the notation above, the following conditions are equivalent.*

(i) f *is* k*-constant.*

(ii) $\bar{f}$ *is* u*-constant.*

(iii) $\bar{f}$ *is constant.*

Proof. As was observed following Definition 4.1, f is k-constant if and only if there exists a constant $\theta \in \mathbb{R}$ such that $e^{2\pi i k f(s)/n} = e^{2\pi i \theta/n}$, for all $s \in X$. This is so if and only if $kf(s) \equiv \theta \bmod n$; if and only if $uf(s) \equiv (\theta/d) \bmod v$. As $f(s) \equiv \bar{f}(s) \bmod v$, this shows that (i) and (ii) are equivalent. Now $\bar{f}$ is u-constant if and only if $uf(s) \equiv \theta \bmod v$, for some θ, if and only if $f(s) \equiv u^{-1}\theta \bmod v$, as u and v are coprime. Thus (ii) and (iii) are equivalent. □

COROLLARY 4.9. f *is* k*-constant if and only if* $f(X)$ *is contained within some coset of* $\langle v \rangle$.

Proof. f is k-constant if and only if $\bar{f}$ is constant, from Proposition 4.8(iii), and the result follows. □

COROLLARY 4.10. *If* p *is a prime number, then for all* $k \in \{1, \ldots, p-1\}$*, a function* $f : \mathbb{Z}_p \to \mathbb{Z}_p$ *is* k*-constant if and only if it is constant.*

Proof. This follows directly from the equivalence of Proposition 4.8(ii) and (iii). □

PROPOSITION 4.11. *In the notation above, the following conditions are equivalent.*

(i) f *is* k*-balanced*

(ii) $\bar{f}$ *is* u*-balanced.*

(iii) $\bar{f}$ *is* 1*-balanced.*

Proof. Conditions (i) and (ii) are equivalent because

$$\sum_{s \in X} e^{2\pi i k f(s)/n} = \sum_{s \in X} e^{2\pi i u f(s)/v} = \sum_{s \in X} e^{2\pi i u \bar{f}(s)/v}.$$

To see the equivalence of (ii) and (iii) note that, because $\gcd(u, v) = 1$,

$$\{0, \ldots, v-1\} =_{\mathbb{Z}_v} \{0, u, 2u, \ldots, (v-1)u\};$$

that is, $0, u, \ldots, (v-1)u$ is a complete set of residues for $\mathbb{Z}_v$. Therefore $\sum_{s \in X} e^{2\pi i u f(s)/v} = \sum_{s \in X} e^{2\pi i f(s)/v}$. □

Given n and k as above, replacing the function $f : X \to \mathbb{Z}_n$ with the function $\bar{f} : X \to \mathbb{Z}_v$, it follows from Propositions 4.8 and 4.11 that we reduce the problem of distinguishing between k-constant and k-balanced to that of distinguishing between constant and 1-balanced. Therefore we now restrict to functions $f : X \to \mathbb{Z}_n$, which are either constant or 1-balanced.

Corollary 4.9 gives a characterisation of k-constant functions in terms of the subgroup $\langle v \rangle$ of $\mathbb{Z}_n$ but, despite the similarities between Propositions 4.8 and 4.11, we have no analogous characterisation of k-balanced functions. In order to find such a characterisation it is convenient to recast Definition 4.5 in terms of polynomials over $\mathbb{Z}$, since in this special case we obtain a polynomial of one variable. As before, given $f : X \to \mathbb{Z}_n$, we may define the integer $p_t = |f^{-1}(t)|$, for $t = 0, \ldots, n-1$, and now define the polynomial

$$P_f(x) = \sum_{t=0}^{n-1} p_t x^t.$$

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

(Regarding x as the generator of $\mathbb{Z}_n$, we may identify P_f with the element r_f of the integral group ring of $\mathbb{Z}_n$.) Observe that

(a) the degree of P_f is at most $n-1$,

(b) all the coefficients p_t of are non-negative, and

(c) $\sum_{t=0}^{n-1} p_t = |X|$.

Let $\omega = e^{2\pi i/n}$; then f is 1-balanced if and only if

$$0 = \sum_{s\in X} \omega^{f(s)} = \sum_{t=0}^{n-1} p_t \omega^t = P_f(w).$$

The minimum polynomial of ω over $\mathbb{Q}$ is Φ_n, the nth cyclotomic polynomial (see Appendix B for further details). Therefore f is 1-balanced if and only if $\Phi_n | P_f$. On the other hand, f is constant if and only if P_f is a monomial (that is, has the form $p_t x^t$, for some t). Conversely, given a polynomial P satisfying (a), (b) and (c), we may define a function $f : X \to \mathbb{Z}_n$, by choosing a partition of X into (at most) n subsets $X_0, \ldots, X_{n-1}$, such that X_i has size p_i, and defining $f(g) = t$, if and only if $g \in X_t$. Then f is constant if and only if P is monomial, and is 1-balanced if and only if P is divisible by Φ_n. If we regard the oracle for f as an oracle that determines the polynomial P_f, then the promise that f is constant or 1-balanced is equivalent to the promise that P_f is monomial of divisible by Φ_n. The problem of distinguishing between constant or 1-balanced functions is therefore equivalent to the problem of distinguishing between (hidden) polynomials which are either monomial or divisible by Φ_n.

Example 4.12. Consider the functions $f : \mathbb{Z}_n \to \mathbb{Z}_n$ of Example 4.4, as illustrated in Figure 1. For the function f of Figure 1(a), we have $P_f = 1+x+x^2+x^3+x^4+x^5+x^7+x^8$. For f in Figures 1(b), 1(c) and 1(d), we have $P_f = 4x(1+x^4)$, $P_f = 2x(1+x^2+x^4+x^6)$ and $P_f = x(3+x+3x^4+x^5)$, respectively.

We are now in a position to apply Theorem B.3, of Appendix B, and the following definition to characterise 1-balanced functions into $\mathbb{Z}_n$ for sufficiently simple n.

Definition 4.13. Let X and Y be sets, S a subset of Y and $f : X \to Y$ a function from X to Y. Then S is *evenly covered* by f if there exists $m \in \mathbb{Z}$ such that $|f^{-1}(s)| = m$, for all $s \in S$.

In keeping with the terminology of [**12**], if Y is evenly covered by f we shall say that f is *perfectly balanced*.

Theorem 4.14. *Let n be a positive integer, and let p and q be distinct primes such that $n = p^\alpha q^\beta$, where α and β are integers, $\alpha > 0$ and $\beta \geqslant 0$. Let X be a finite set and $f : X \to \mathbb{Z}_n$ a function. Define K_p to be the subgroup of $\mathbb{Z}_n$ generated by n/p and, if $\beta > 0$, define K_q to be the subgroup generated by n/q.*

(i) *If $\beta = 0$, then f is 1-balanced if and only if every coset of K_p is evenly covered by f.*

(ii) *If $\beta > 0$, then f is 1-balanced if and only if there exists a partition of X into disjoint subsets X_p and X_q such that every coset of K_p is evenly covered by $f|_{X_p}$ and every coset of K_q is evenly covered by $f|_{X_q}$.*

Remark 4.15. The obvious generalisation of this theorem to integers with 3 or more prime factors does not hold, as shown by Example 4.19 below. The best that we have been able to do is Proposition 4.16.

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

Proof of Theorem 4.14. From the discussion above, the function f is 1-balanced if and only if P_f is divisible by Φ_n. Consider first the case $\beta = 0$. From Theorem B.3, we have $P_f(x) = s(x)\Phi_p(x^{n/p})$, where $s \in \mathbb{Z}[x]$ and the coefficients of s are all non-negative. As $\deg(P_f) \leqslant n-1$ and $\deg(\Phi_p) = p-1$, it follows that $\deg(s) \leqslant n/p - 1$. Let $s(x) = u_0 + u_1(x) + \ldots + u_{n/p-1}x^{n/p-1}$. Fix $t \in \mathbb{Z}$ with $0 \leqslant t < n-1$. Since $\Phi_p(x) = 1 + x + \ldots + x^{p-1}$, the coefficient p_t of x^t in P_f is u_j, where j is the unique integer such that $j \equiv t \bmod n/p$ and $0 \leqslant j < n/p$. Therefore the coefficient p_t equals the coefficient p_r, for all r such that $r \equiv t \bmod n/p$. Thus, if $0 \leqslant t < n/p$, we have $p_t = p_r$, for $r = t, n/p + t, \ldots, (p-1)n/p + t$. As $p_t = |f^{-1}(t)|$, it follows that the coset $t + K_p$ is evenly covered by f. The converse follows easily, by reversing this argument.

Now suppose that $\beta > 0$. This time Theorem B.3 implies that f is 1-balanced if and only if $P_f(x) = s_1(x)\Phi_p(x^{n/p}) + s_2(x)\Phi_q(x^{n/q})$, where $s_i \in \mathbb{Z}[x]$ and the coefficients of s_i are all non-negative. Let $A(x) = s_1(x)\Phi_p(x^{n/p})$ and $B(x) = s_2(x)\Phi_q(x^{n/q})$, and suppose that $A(x) = a_0 + a_1x + \ldots + a_{n-1}a^{n-1}$ and $B(x) = b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$. As in the case $\beta = 0$, the coefficients a_r and a_t are equal for all r, t such that $0 \leqslant r, t < n$ and $r \equiv t \bmod n/p$. A similar statement, involving q instead of p, holds for the coefficients of B. For fixed t we have $|f^{-1}(t)| = a_i + b_j$, where $i \equiv t \bmod n/p$ and $j \equiv t \bmod n/q$. Hence we may partition $f^{-1}(t)$ into disjoint (possibly empty) subsets $X_{p,t}$ and $X_{q,t}$ such that $|X_{p,t}| = a_i$ and $X_{q,t} = b_j$. Now $t \equiv r \bmod n/p$ implies that $a_r = a_t$, so also $|X_{p,t}| = |X_{p,r}|$. Setting $X_p = \bigcup_{t=0}^{n-1} X_{p,t}$, we see that $f|_{X_p}$ covers $t + K_p$ evenly, for $t = 0, \ldots, p-1$. Similarly, if $X_q = \bigcup_{t=0}^{n-1} X_{q,t}$, then $f|_{X_q}$ covers $t + K_q$ evenly, for $t = 0, \ldots, q-1$. As $X = X_p \cup X_q$ and $X_p \cap X_q = \emptyset$, this completes the proof of the theorem. □

Proposition 4.16. *Let n be a positive integer with prime factorisation $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Let K_{p_i} be the subgroup of $\mathbb{Z}_n$ generated by n/p_i. Let $f : X \to \mathbb{Z}_n$ be a function with associated polynomial P_f such that*

$$P_f(x) = \sum_{i=1}^{k} s_i(x)\Phi_{p_i}(x^{n/p_i}),$$

where $s_i \in \mathbb{Z}[x]$ and the coefficients of s_i are all non-negative. Then f is 1-balanced and there exists a partition of X into disjoint subsets $X_1, \ldots, X_k$ such that $f|_{X_i}$ evenly covers the cosets of K_{p_i}, $i = 1, \ldots, k$. Moreover, setting N_i equal to the sum of the coefficients of s_i, we have $|X_i| = nN_i/p_i$.

The proof of Proposition 4.16 is similar to (the appropriate part of) the proof of Theorem 4.14, and we leave the details to the reader.

Example 4.17. Consider the polynomials of Example 4.12 corresponding to the functions of Example 4.4 and Figure 1. Here $K_p = K_2 = \langle 4 \rangle = \{1, 4\}$. For Figure 1(a) we have $P_f = 1 + x + x^2 + x^3 + x^4 + x^5 + x^7 + x^8 = (1 + x + x^2 + x^3)\Phi_2(x^4)$. In this case, every coset of K_2 is covered evenly by one element of X. Corresponding to Figure 1(b), $P_f = 4x(1 + x^4) = 4x\Phi_2(x^4)$. Here $1 + K_2$ is evenly covered by four elements, and all other cosets are covered by zero elements. Figure 1(c) gives $P_f = 2x(1 + x^2 + x^4 + x^6) = 2x(1+x)\Phi_2(x^4)$. This time K_2 and $3 + K_2$ are covered by 0 elements, and $1 + K_2$ and $2 + K_2$ by two elements. With Figure 1(d) we have $P_f = x(3 + x + 3x^4 + x^5) = x(3 + x)\Phi_2(x^4)$; the coset $1 + K_2$ is covered by three elements, the coset $2 + K_2$ is covered by one element and both other cosets by zero elements.

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

EXAMPLE 4.18. Let $n = 15$, and let f be a function $\mathbb{Z}_{45} \to \mathbb{Z}_{15}$. In this case, $K_3 = \langle 5 \rangle$ and $K_5 = \langle 3 \rangle$. If $P_f = (4 + 2x + x^2 + 3x^4)\Phi_3(x^5) + (2 + x^2)\Phi_5(x^3)$, then f is 1-balanced. We can partition X into subsets X_3 of size 30 and X_5 of size 15 such that $f|_{X_3}$ covers K_3 evenly with four elements, $1 + K_3$ with two elements, $2 + K_3$ with one element, $3 + K_3$ with zero elements and $4 + K_3$ with three elements. Similarly, $f|_{X_5}$ covers cosets $t + K_5$, for $t = 0, 1, 2$, evenly with two, zero and one elements, respectively.

EXAMPLE 4.19. We are grateful to C. Smyth for pointing this example out to us. Let $n = 105$, $\omega = \exp 2\pi i/105$, $\zeta = \omega^7$ and $\eta = \omega^{15}$, so $\zeta^{15} = \eta^7 = 1$. The minimum polynomial of ζ over $\mathbb{Q}$ is $\Phi_{15}(x) = 1-x+x^3-x^4+x^5-x^7+x^8$, so we have $1+\zeta^3+\zeta^5+\zeta^8 = \zeta+\zeta^4+\zeta^7$. The minimum polynomial of η is $\Phi_7(x)$, so we have $1 + \eta + \eta^2 + \ldots + \eta^6 = 0$. Therefore

$$(\zeta + \zeta^4 + \zeta^7)(\eta + \eta^2 + \eta^3 + \eta^4 + \eta^5 + \eta^6) + (1 + \zeta^3 + \zeta^5 + \zeta^8) = 0.$$

Writing this out as a polynomial in ω, we obtain $P = \sum_{t=0}^{104} p_t \omega^t = 0$, where $p_t = 1$, for t equal to 0, 4, 13, 19, 21, 22, 34, 35, 37, 43, 52, 56, 58, 64, 67, 73, 79, 82, 88, 94, 97 and 103, and $p_t = 0$ otherwise. Let f be a function $\mathbb{Z}_{105} \to \mathbb{Z}_{105}$ such that $P_f = P$. Then f is 1-balanced, as $P(\omega) = 0$. Any straightforward analogue of Theorem 4.14 would (at the least) assert that there are a subset S of $\mathbb{Z}_{105}$ and a subgroup K of $\mathbb{Z}_{105}$ such that the restriction of f to S covers every coset of K evenly. Since $p_0 = 1$, this would imply that $f|_S$ covers K evenly. Thus f should map one element of $\mathbb{Z}_{105}$ to each element of K. Hence p_t should be equal to 1 for t equal to some divisor of 105 and all its multiples. This is clearly not the case, so no such generalisation of Theorem 4.14 exists.

COROLLARY 4.20. *If p is a prime number, then a function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is 1-balanced if and only if it is a bijection.*

4.2. *Non-Abelian examples.*

The following examples involve the symmetric groups S_n and the alternating group A_4. It follows from the results of [**16**] (see the end of Section 3) that there are efficient implementations of the quantum Fourier transform for these groups. Therefore efficient quantum algorithms for the problems of these examples may be constructed.

EXAMPLE 4.21. Consider the simplest possible non-Abelian finite group, S_3, considered as a dihedral group and generated by a rotation r and a reflection s. The irreducible representations of S_3 are ρ^1, the trivial representation, ρ^2, the alternating representation, and ρ^3, the two-dimensional representation. The corresponding Fourier coefficients are given in the following table.

	1	r	r^2	s	$t = r^2s$	$u = rs$
$\tau^1_{1,1}$	$1/\sqrt{6}$	$1/\sqrt{6}$	$1/\sqrt{6}$	$1/\sqrt{6}$	$1/\sqrt{6}$	$1/\sqrt{6}$
$\tau^2_{1,1}$	$1/\sqrt{6}$	$1/\sqrt{6}$	$1/\sqrt{6}$	$-1/\sqrt{6}$	$-1/\sqrt{6}$	$-1/\sqrt{6}$
$\tau^3_{1,1}$	$1/\sqrt{3}$	$e^{2\pi i/3}/\sqrt{3}$	$e^{-2\pi i/3}/\sqrt{3}$	0	0	0
$\tau^3_{1,2}$	0	0	0	$1/\sqrt{3}$	$e^{-2\pi i/3}/\sqrt{3}$	$e^{2\pi i/3}/\sqrt{3}$
$\tau^3_{2,1}$	0	0	0	$1/\sqrt{3}$	$e^{2\pi i/3}/\sqrt{3}$	$e^{-2\pi i/3}/\sqrt{3}$
$\tau^3_{2,2}$	$1/\sqrt{3}$	$e^{-2\pi i/3}/\sqrt{3}$	$e^{2\pi i/3}/\sqrt{3}$	0	0	0

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

1. First consider the alternating representation ρ^2, which is linear. To say that a function $f : X \to S_3$ is ρ^2-*constant* means that the image of f is contained in $\langle r\rangle$ or its coset $\langle r\rangle s$. To say that f is ρ^2-*balanced* means that $|f^{-1}(\langle r\rangle)| = |f^{-1}(\langle r\rangle s)|$.

2. Now consider the two-dimensional representation ρ^3. To say that $f : X \to S_3$ is ρ_1^3-*constant* means that for $i = 1$ and 2 there is a constant $c_i \in \mathbb{C}$ such that for all $g \in X$, $\tau_{1,i}^3(f(g)) = c_i$. For $i = 1$ or 2, the table above shows that f has to be constant. Since one coset of $\langle r\rangle$ always maps to zero under a matrix coefficient of ρ^3, the meaning of ρ_1^3-*balanced* is that

$$\sum_{g\in f^{-1}(\langle r\rangle)} \tau_{1,1}^3(f(g)) = 0 \qquad \text{and} \qquad \sum_{g\in f^{-1}(\langle r\rangle s)} \tau_{1,2}^3(f(g)) = 0.$$

In other words, setting $m_j = |f^{-1}(r^j)|$ and $n_j = |f^{-1}(r^j s)|$, $j = 0, 1, 2$, we have

$$\sum_{j=0}^{2} m_j e^{2\pi ij/3} = 0 \qquad \text{and} \qquad \sum_{j=0}^{2} n_j e^{2\pi ij/3} = 0.$$

If we set

$$P(x) = \sum_{j=0}^{2} m_j x^j \qquad \text{and} \qquad Q(x) = \sum_{j=0}^{2} n_j x^j,$$

it follows that f is ρ_1^3-balanced if and only if $\Phi_3|P$ and $\Phi_3|Q$. Let $X_1 = f^{-1}(\langle r\rangle)$ and $X_2 = f^{-1}(\langle r\rangle s$; so X is the disjoint union of X_1 and X_2, and set $f_i = f|_{X_i}$. Then, as in Section 4.1, it follows that f is ρ_1^3-balanced if and only if $\langle r\rangle$ is evenly covered by f_1 and $\langle r\rangle s$ is evenly covered by f_2.

In this case (in the terminology of Theorem 4.6), $\mathrm{Ann}(e_1) = \mathrm{Ann}(e_2)$, the ideal of $\mathbb{Z}S_3$ generated by the element $1 + r + r^2$. Hence f is ρ_1^3-balanced if and only if it is ρ_2^3-balanced.

EXAMPLE 4.22. Let S_m be the symmetric group on m objects, and let A_m denote its alternating subgroup of index 2. Let χ be the alternating character of S_m: that is, χ is the linear character of S_m given by $\chi(h) = 1$ if $h \in A_m$ and $\chi(h) = -1$ otherwise. Let $f : X \to S_m$ be a function, and assume that we are promised that either: (a) $\mathrm{im}(f) \subset A_m$ or $\mathrm{im}(f) \subset S_m - A_m$, or (b) $|f^{-1}(A_m)| = |f^{-1}(S_m - A_m)|$. Then f is χ-constant in case (a), and χ-balanced in case (b).

EXAMPLE 4.23. The alternating group A_4 may be regarded as the orientation-preserving group of symmetries of a regular tetrahedron, whose 1-skeleton is embedded in $\mathbb{R}^3$ as diagonals of faces of a cube with vertices $(\pm1, \pm1, \pm1)$. This gives rise to a three-dimensional unitary irreducible representation ρ of A_4 generated by the matrices

$$N = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \qquad \text{and} \qquad R = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The elements of A_4 may then be listed as

$$I,\ N,\ N^2,\ R,\ RN,\ RN^2,\ NR,\ NRN,\ NRN^2,\ N^2R,\ N^2RN,\ N^2RN^2.$$

Then $\mathrm{Stab}_{A_4}(e_1) = \{I, N^2RN\}$. Therefore a function $f : X \to A_4$ is ρ_1-constant if and only if $f(X)$ is contained in one of the cosets

$$\{I, N^2RN\},\ \{N, N^2RN^2\},\ \{N^2, N^2R\},\ \{R, NRN^2\},\ \{RN, NR\},\ \{RN^2, NRN\}.$$

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

Calculation of $e_1 M$, for each $M \in A_4$, in turn shows that $\mathrm{Ann}(e_1)$ is the subset of $\mathbb{Z}A_4$ consisting of elements $\sum_{M \in A_4} m_M M$ such that

$$m_I - m_R + m_{N^2RN} - m_{NRN^2} = 0,$$
$$m_N - m_{RN} + m_{N^2RN^2} - m_{NR} = 0$$

and

$$m_{N^2} - m_{RN^2} + m_{N^2R} - m_{NRN} = 0.$$

Therefore f is is ρ_1-balanced if and only if r_f has such a form. We may also characterise ρ_i-constant and ρ_i-balanced functions in this way, for $i = 2, 3$; the results are very similar.

5. *The Deutsch–Jozsa–Høyer algorithm with generalised promises*

In this section we assume that we have a finite set X, a finite group H and a map $f : X \to H$, and we work with an oracle U_f as in Section 2. We use the notation of Section 3.1 for representations of the group H. In particular, let H have irreducible unitary representations $\rho^1, \ldots, \rho^R$, so we have

$$\tau^k_{i,j} = \sqrt{\frac{\dim \rho^k}{|H|}} \cdot \rho^k_{i,j},$$

for $1 \leqslant k \leqslant R$ and $1 \leqslant i, j \leqslant \dim \rho^k$. Then, since $\{\tau_h\}_{h \in H}$ is an orthonormal basis of $L^2(H)$, we have

$$\langle \tau^k_{i,j}, \tau^t_{r,s} \rangle = \delta_{i,r}\delta_{j,s}\delta_{k,t}. \tag{5}$$

Lemma 5.1. *Let X be a finite set and H a finite group, and let $f : X \to H$ be a map. Then, for fixed i, j, k, r, s, t, we have*

$$\sum_{h \in H} \tau^k_{i,j}(h)\overline{\tau^t_{r,s}(f(g)h)} = \overline{\tau^k_{r,i}(f(g))}\delta_{j,s}\delta_{k,t}.$$

Proof. Let $n = \dim \rho^t$. Using the formula for matrix multiplication, we have

$$\begin{aligned}
\sum_{h \in H} \tau^k_{i,j}(h)\overline{\tau^t_{r,s}(f(g)h)} &= \sum_{h \in H} \tau^k_{i,j}(h) \sum_{q=1}^{n} \overline{\tau^t_{r,q}(f(g))\tau^t_{q,s}(h)} \\
&= \sum_{q=1}^{n} \overline{\tau^t_{r,q}(f(g))} \sum_{h \in H} \tau^k_{i,j}(h)\overline{\tau^t_{q,s}(h)} \\
&= \sum_{q=1}^{n} \overline{\tau^t_{r,q}(f(g))}\langle \tau^k_{i,j}, \tau^t_{q,s} \rangle \\
&= \sum_{q=1}^{n} \overline{\tau^t_{r,q}(f(g))}\delta_{i,q}\delta_{j,s}\delta_{k,t} \qquad \text{(by (5))} \\
&= \overline{\tau^k_{r,i}(f(g))}\delta_{j,s}\delta_{k,t}
\end{aligned}$$

as required. □

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

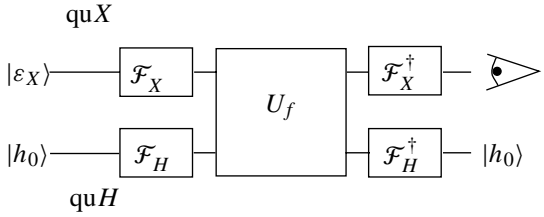


Figure 2: The quantum circuit for the Deutsch–Jozsa–Høyer algorithm.

We shall use the circuit in Figure 2, which was introduced in [**12**], where it was used to distinguish between perfectly balanced and constant functions. In order to apply the quantum Fourier transform to the X register, we assume that $X = \mathbb{Z}_n$, where $n = |X|$. By ε_X we mean the element of X that corresponds to $1_{\mathbb{Z}_n}$. Our main result is Theorem 5.2, where it is shown that the range of promises that the algorithm can deal with extends beyond perfectly balanced and constant.

If we omit the $\mathcal{F}_H$ and $\mathcal{F}_H^\dagger$ gates in Figure 2 and h_0 is set to be the identity, then we obtain the non-Abelian analogue of the circuit used in Shor's algorithm. This has been proposed as a quantum algorithm for the hidden subgroup problem. We note, however, that it has been shown in [**10**] that while a polynomial number of Fourier samples will reconstruct a *normal* hidden subgroup, the circuit fails to solve the hidden subgroup problem in S_n for general subgroups, even in a very restricted situation (see also [**9**], where the latter result was obtained independently).

When working with query complexity, only the number of calls to the oracle is relevant, and we do not discuss the efficient implementation of the Fourier transform on a finite group any further here (but see the end of Section 3).

THEOREM 5.2 (GENERAL FORM OF THE DEUTSCH–JOZSA–HØYER ALGORITHM). *Let $f : X \to H$ be a function from the finite set X to the finite group G, and let ρ^k be a non-trivial irreducible representation of H. Let $n = \dim \rho^k$. Suppose that we are promised that for some $i \in \{1, \ldots, n\}$, f is either ρ_i^k-constant or ρ_i^k-balanced. Then there exists a quantum algorithm which distinguishes between these two possibilities with certainty, using a single quantum query.*

Proof. Let $j \in \{1, \ldots, n\}$, and let h_0 correspond to the triple (i, j, k) under the bijection θ described in Section 3.1. (Note that h_0 is necessarily a non-trivial element of H.) We assume that we have gates $\mathcal{F}_X$ and $\mathcal{F}_H$ at our disposal to perform the quantum Fourier transforms on $X = \mathbb{Z}_n$ and H. We use the quantum circuit in Figure 2. This operates as follows.

$$
\begin{aligned}
|\varepsilon_X, h_0\rangle &\xrightarrow{\mathcal{F}_X \otimes \mathcal{F}_H} \sum_{g \in X, h \in H} \tau_X^{\varepsilon_X}(g)\tau_H^{h_0}(h)|g, h\rangle \\
&= \frac{1}{\sqrt{|X|}} \sum_{g \in X, h \in H} \tau_H^{h_0}(h)|g, h\rangle, \qquad \text{using (2)}, \\
&\xrightarrow{U_f} \frac{1}{\sqrt{|X|}} \sum_{g \in X, h \in H} \tau_H^{h_0}(h)|g, f(g)h\rangle \\
&\xrightarrow{\mathcal{F}_X^\dagger \otimes \mathcal{F}_H^\dagger} \frac{1}{\sqrt{|X|}} \sum_{g, g' \in X, h, h' \in H} \tau_H^{h_0}(h)\overline{\tau_X^{g'}(g)\tau_H^{h'}(f(g)h)}|g', h'\rangle.
\end{aligned}
$$

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

Given that θ is a bijection from H to R, with $\theta(h_0) = (i, j, k)$ we may sum over triples $(r, s, t) \in R$ instead of $h' \in H$. The expression above then becomes

$$\frac{1}{\sqrt{|X|}} \sum_{g,g' \in X, h \in H, r,s,t} \tau^k_{i,j}(h) \overline{\tau^{g'}_X(g) \tau^t_{r,s}(f(g)h)} |g', h'\rangle.$$

Applying Lemma 5.1, this is equal to

$$\frac{1}{\sqrt{|X|}} \sum_{g,g' \in X, r,s,t} \overline{\tau^{g'}_X(g) \tau^k_{r,i}(f(g))} \delta_{j,s} \delta_{k,t} |g', (r, s, t)\rangle$$

$$= \frac{1}{\sqrt{|X|}} \sum_{g,g' \in X, r=1,\ldots,n} \overline{\tau^{g'}_X(g) \tau^k_{r,i}(f(g))} |g', (r, j, k)\rangle. \quad (6)$$

Restricting to $g' = \varepsilon_X$ on the right-hand side of equation (6), we obtain

$$\frac{1}{|X|} \sum_{g \in X, r=1,\ldots,n} \overline{\tau^k_{r,i}(f(g))} |\varepsilon_X, (r, j, k)\rangle. \quad (7)$$

If f is ρ^k_i-balanced then we have $\sum_{g \in X} \overline{\tau^k_{r,i}(f(g))} = 0$, for $r = 1, \ldots, n$; so (7) is equal to 0. Thus measurement of the first register never results in $|\varepsilon_X\rangle$. On the other hand, if f is ρ^k_i-constant, then there exists a non-zero complex constant c_r such that we have $\tau^k_{i,r}(f(g)) = c_r$, for all $g \in X$, for $r = 1, \ldots, n$. In this case the right-hand side of equation (6) becomes

$$\sum_{r=1}^{m} \overline{c_r} |\varepsilon_X, (r, j, k)\rangle,$$

and measurement of the first register always results in $|\varepsilon_X\rangle$. □

6. *Conclusion*

From Theorem 5.2 it follows that we can distinguish in a single step, with certainty, between ρ^k_i-constant and ρ^k_i-balanced functions in all the examples of Section 4. In particular, for an Abelian group A this means that we may distinguish between k-constant and k-balanced functions, for all $k \in A$, as described in Section 4.1. In the case of non-Abelian groups, as shown in Section 4.2, there are many functions which may fall into the category of ρ^k_i-constant or ρ^k_i-balanced for an appropriate choice of representation ρ. Here we summarise various known algorithms which are also covered by Theorem 5.2.

6.1. *The Deutsch–Jozsa–Høyer algorithm*

Suppose that X and H are finite groups with H nontrivial such that $|X| = m|H|$, and assume that f is constant or m-to-one (the second possibility is called 'perfectly balanced' in [**12**]). If f is constant, then it is χ-constant for any linear character χ of H. Suppose that f is m-to-one and χ is a nontrivial linear character of H. Let χ_0 be the trivial character of H. Then we have

$$\sum_{g' \in X} \chi(f(g')) = m \sum_{h' \in H} \chi(h')$$
$$= m\langle \chi, \chi_0 \rangle$$
$$= 0,$$

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

by orthogonality of irreducible characters, since χ is non-trivial. So f is χ-balanced.

Thus we recover Hoyer's result from [12]: that we can distinguish between perfectly balanced and constant functions from X to H with certainty in a single quantum query.

6.2. *The Deutsch–Jozsa–Constantini–Smeraldi algorithm*

In the case where $X = \mathbb{Z}_{mn}$ and $H = \mathbb{Z}_n$, we recover the result of [3], which is itself a subcase of Hoyer's result 6.1.

6.3. *The Deutsch algorithm*

In the case where $X = \mathbb{Z}_2$ and $H = \mathbb{Z}_2$, we obtain Deutsch's algorithm [5].

6.4. *Limited surjectivity testing*

Suppose that $f : \mathbb{Z}_p \to \mathbb{Z}_p$, where p is prime. If we are promised that f is either constant or surjective, then we can decide which is the case in a single quantum query, by Corollaries 4.10 and 4.20. Classically, we would clearly require two queries. (This is also a special case of the Constantini–Smeraldi result above.)

6.5. *The Deutsch–Jozsa algorithm*

In the case where $X = \mathbb{Z}_2^n$ and $H = \mathbb{Z}_2$, we obtain the Deutsch–Jozsa algorithm [6], in the form in which it appears in in [2].

These examples cover the main instances of the Deutsch–Jozsa–Høyer algorithm of which we are aware, and in which the circuit is used to give an exact result. Moreover the examples of Section 4 cover much wider classes of functions than those covered by the examples described in this section. It therefore seems that Theorem 5.2 is a genuine generalisation of the algorithms existing in the literature.

Appendix A. *Representations of finite groups*

In this section we provide a short summary of the standard properties of representations of finite groups. Proofs may be found in any introductory text book on representation theory, for example [14] or [8].

A *representation* of a group G is a homomorphism $\rho : G \to \mathrm{GL}(n, \mathbb{C})$ for some $n \in \mathbb{N}$. Given a basis B of $\mathbb{C}^n$ and an element $g \in G$, we denote by $\rho_B(g)$ the matrix of the linear transformation $\rho(g)$ with respect to the basis B. (If B is understood, we use $\rho(g)$ for both the linear transformation and its matrix.) Suppose that ρ' is another representation of G and there exists a matrix $T \in \mathrm{GL}(n, \mathbb{C})$ such that $\rho = T^{-1}\rho' T$. Then these representations are not equal, because they are different homomorphisms. However, there exists a basis B' of $\mathbb{C}^n$ (T is the change of basis matrix from B to B') such that for all $g \in G$, $\rho'_{B'}(g) = \rho_B(g)$. In this case we say that ρ and ρ' are *equivalent* representations.

If there is a proper subspace V of $\mathbb{C}^n$ which is invariant under the action of $\rho(g)$ for all $g \in G$ (that is, for all $g \in G$ we have $[\rho(g)](V) = V$), then ρ is equivalent to a direct sum $\rho_1 \oplus \rho_2$ of smaller-dimensional representations ρ_1 and ρ_2. If there is no such subspace, then we say that ρ is *irreducible*.

A group G always has the one-dimensional representation $\rho^1 : G \to \mathbb{C}$ given by $\rho^1(g) = 1$ for all $g \in G$. This is called the *trivial* representation of G, and is clearly

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

irreducible. Let $\mathbb{C}G$ be the vector space spanned by the elements of G. In the case where G is finite, this is of course finite-dimensional. G acts on itself by left (or right) multiplication, and this action extends to a linear map of $\mathbb{C}G$ to itself by permuting the vectors in its G-basis. This is known as the left (or right) *regular representation* of G. The regular representation is not irreducible unless G is trivial (see [14, Section 2.2]). Furthermore, the regular representation of a finite group G decomposes as a direct sum of all of the (inequivalent) irreducible representations ρ of G, each one appearing $\dim(\rho)$ times in the decomposition. It follows that: (a) there are only finitely many irreducible representations of G, and (b) the sum of the squares of the dimensions of the irreducible representations is equal to $|G|$.

If ρ is a representation of G such that for all $g \in G$, $\rho(g)$ is a unitary map, then ρ is called a *unitary representation* of G. If G is a finite group, then a technique known as 'Weyl's unitary trick' can be used to unitarize any irreducible representation (that is, find an equivalent representation which is unitary). That we can do this is important for the definition of the Fourier transform on G, so we recall its proof from [21]. Let ρ be an irreducible representation of G with $n = \dim \rho$, and let $\langle \cdot, \cdot \rangle$ denote the standard inner product on $\mathbb{C}^n$. First, we form an inner product $\langle \cdot, \cdot \rangle_{\text{inv}}$ on $\mathbb{C}^n$ which is invariant under $\rho(g)$ for all $g \in G$. This is done simply by defining

$$\langle u, v \rangle_{\text{inv}} = \sum_{g \in G} \langle \rho(g)u, \rho(g)v \rangle.$$

We show that, since the latter inner product is invariant under $\rho(g)$ for all $g \in G$, ρ is conjugate to a unitary representation. Suppose that $\{e_i\}_{i=1}^n$ is the standard basis of $\mathbb{C}^n$. Let $C = \{c_{i,j}\}$ be the matrix given by $c_{i,j} = \langle e_i, e_j \rangle_{\text{inv}}$. Then C is positive definite and Hermitian ($C^* = C$). Thus, by the spectral theorem for Hermitian matrices, $C = U^* D U$ where U is unitary and D is diagonal with positive real entries. Thus we can define $\sqrt{D}$ to be the matrix with entries the square roots of the diagonal entries of D. Let $R = U^* \sqrt{D} U$. Then $C = R^2$, and since the inner product which gave rise to C is invariant under ρ, we have $\rho(g) C [\rho(g)]^* = C$ for all $g \in G$. Let $\rho_U(g) = R^{-1} \rho(g) R$. We claim that ρ_U is a unitary representation. This follows because for all $g \in G$ we have

$$\begin{aligned}
\rho_U(g)[\rho_U(g)]^* &= R^{-1}\rho(g)RR^*[\rho(g)]^*(R^{-1})^* \\
&= R^{-1}\rho(g)R^2[\rho(g)]^*(R^{-1})^* \qquad \text{since } R \text{ is also Hermitian} \\
&= R^{-1}\rho(g)C[\rho(g)]^*(R^{-1})^* \\
&= R^{-1}C(R^{-1})^* \\
&= R^{-1}RR^*(R^*)^{-1} \\
&= I
\end{aligned}$$

and similarly, for all g in G, $[\rho_U(g)]^* \rho_U(g) = I$.

Appendix B. *Cyclotomic polynomials*

Here we recall the definition and some of the basic properties of cyclotomic polynomials, and we establish the identity that we require in Section 4. Let n be a positive integer, let $\omega = \exp(2\pi i/n)$, and let $R = \{d : d \in \mathbb{Z}, 1 \leqslant d < n, \gcd(d, n) = 1\}$. The nth cyclotomic polynomial is defined to be

$$\Phi_n(x) = \prod_{d \in R} (x - \omega^d).$$

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

It follows from the definition that the degree of Φ_n is $\phi(n)$, where ϕ is Euler's totient function. As shown in, for example, [13, p.194], we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

from which it follows that $\Phi_n \in \mathbb{Z}[x]$. Moreover (see [13]) Φ_n is irreducible in $\mathbb{Z}[x]$, and so is the minimum polynomial of w over $\mathbb{Q}$. The following identity is standard; we cast it in the particular form that we require below. Let $n = p^\gamma s$, where p is prime, $\gamma \geqslant 1$ and $p \nmid s$. We have

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \Phi_d(x) \\ &= \prod_{d|s} \Phi_{p^\gamma d}(x) \prod_{d|n/p} \Phi_d(x) \\ &= \prod_{d|s} \Phi_{p^\gamma d}(x)(x^{n/p} - 1). \end{aligned}$$

As $x^n - 1 = (x^{n/p} - 1)\Phi_p(x^{n/p})$, it follows that

$$\Phi_p(x^{n/p}) = \prod_{d|s} \Phi_{p^\gamma d}(x). \tag{8}$$

We shall also require the following fact.

LEMMA B.1. *Let $a_1, \ldots, a_n$ be non-negative integers, $n \geqslant 2$, and let $d = \gcd(a_1 + 1, \ldots, a_n + 1)$. Then there exist polynomials $s_i(x) \in \mathbb{Z}[x]$, $i = 1, \ldots, n$, such that*

$$\sum_{i=1}^{n} s_i(x)(1 + x + \ldots + x^{a_i}) = 1 + x + \ldots + x^{d-1}.$$

Proof. First consider the case $n = 2$. Note that if $a_1 = a_2$, then $d = a_1 + 1$ and $s_1 = 1$, $s_2 = 0$ have the required property. Use induction on $a_1 + a_2$, starting with the case $a_1 = a_2 = 0$. In this case the result follows from the previous remark. Now suppose that $a_1 + a_2 > 0$. It may be assumed that $a_1 < a_2$. Set $f = 1 + x + \ldots + x^{a_1}$, $g = 1 + x + \ldots + x^{a_2}$, $t = -x^{a_2 - a_1}$ and $h = 1 + x + \ldots + x^{a_2 - a_1 - 1} = tf + g$.

Then $\gcd(a_1+1, (a_2-a_1-1)+1) = \gcd(a_1+1, a_2+1-(a_1+1)) = \gcd(a_1+1, a_2+1) = d$, so by induction there exist s_1', s_2' such that $s_1' f + s_2' h = 1 + x + \ldots + x^{d-1}$. Hence

$$\begin{aligned} 1 + x + \ldots + x^{d-1} &= s_1' f + s_2'(tf + g) \\ &= (s_1' + s_2' t) f + s_2' g, \end{aligned}$$

as required. Thus the result holds when $n = 2$.

Now suppose that $n > 2$. Let $d_1 = \gcd(a_1 + 1, \ldots, a_{n-1} + 1)$ and $d_2 = \gcd(a_{n-1} + 1, a_n + 1)$. From the inductive hypothesis, there exist $u_1, \ldots, u_{n-1}, v_1, v_2 \in \mathbb{Z}[x]$ such that

$$\sum_{1}^{n-1} u_i(x)(1 + x + \ldots + x^{a_i}) = 1 + x + \ldots + x^{d_1 - 1} \tag{9}$$

and

$$v_1(x)(1 + x + \ldots + x^{a_{n-1}}) + v_2(x)(1 + x + \ldots + x^{a_n}) = 1 + x + \ldots + x^{d_2 - 1}. \tag{10}$$

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

As $d = \gcd(d_1, d_2)$, there are $u, v \in \mathbb{Z}[x]$ such that

$$u(x)(1 + x + \ldots + x^{d_1-1}) + v(x)(1 + x + \ldots + x^{d_2-1}) = 1 + x + \ldots + x^{d-1}. \quad (11)$$

Combining (9), (10) and (11) gives the required result. □

Define $F_n(x) = 1 + x + \ldots + x^{n-1}$, for all integers $n \geqslant 1$.

COROLLARY B.2. *If $p_1, \ldots, p_n$ are distinct primes, set $m = p_1 \cdots p_n$ and $m_i = m/p_i$. Then there exist $s_1, \ldots, s_n \in \mathbb{Z}[x]$ such that*

$$\sum_1^n s_i F_{m_i} = 1.$$

THEOREM B.3. *Let $n = p^\alpha q^\beta$ be a positive integer, where p and q are distinct primes and α and β are non-negative integers. Let $g \in \mathbb{Z}[x]$ such that $\Phi_n(x) | g(x)$, $deg(g) = n - 1$ and the coefficients of g are all non-negative.*

(i) *If $\alpha \geqslant 1$ and $\beta = 0$, then*

$$g(x) = s(x)\Phi_p(x^{n/p}), \quad (12)$$

for some $s \in \mathbb{Z}[x]$ with non-negative coefficients.

(ii) *If $\alpha \geqslant 1$ and $\beta \geqslant 1$, then there exist $s_1, s_2 \in \mathbb{Z}[x]$ such that*

$$g(x) = s_1(x)\Phi_p(x^{n/p}) + s_2(x)\Phi_q(x^{n/q}), \quad (13)$$

and the coefficients of s_1 and s_2 are all non-negative.

Proof. We begin by proving that there exist elements s or s_i in $\mathbb{Z}[x]$ such that (12) or (13) holds, as appropriate, and we subsequently show that s or the s_i may be chosen so that their coefficients are non-negative.

If $n = p^\alpha$, then (8) yields $\Phi_n(x) = \Phi_p(x^{n/p})$, so we may write $g(x) = s_p(x)\Phi_n(x) = s_p(x)\Phi_p(x^{n/p})$, with $s_p \in \mathbb{Z}[x]$, as required. Assume then that $\alpha \geqslant 1$ and $\beta \geqslant 1$. As $\Phi_r = F_r$ when r is prime, we have

$$F_p(x^{n/p}) = \prod_{d | q^\beta} \Phi_{p^\alpha d}(x) \quad (14)$$

and

$$F_q(x^{n/q}) = \prod_{d | p^\alpha} \Phi_{q^\beta d}(x). \quad (15)$$

Write

$$g(x) = f(x)\Phi_n(x), \qquad \text{where } f \in \mathbb{Z}[x]. \quad (16)$$

From Corollary B.2 there are polynomials s_1 and $s_2 \in \mathbb{Z}[x]$ such that $1 = s_1(x)F_p(x) + s_2(x)F_q(x)$. Let $k = n/pq$, and replace x with x^k in the previous equality to obtain $1 = s_1(x^k)F_p(x^k) + s_2(x^k)F_q(x^k)$. Multiplying through by $f(x)$ gives $f(x) = s_p(x)F_p(x^k) + s_q(x)F_q(x^k)$, for some $s_p, s_q \in \mathbb{Z}[x]$. Hence $g(x) = (s_p(x)F_p(x^k) + s_q(x)F_q(x^k))\Phi_n(x)$.

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

Applying (14) and (15), with n/q and n/p, respectively, in place of n, we obtain

$$\begin{aligned} g(x) &= \left(s_p(x) \prod_{d \mid q^{\beta-1}} \Phi_{p^\alpha d}(x) + s_q(x) \prod_{d \mid p^{\alpha-1}} \Phi_{q^\beta d}(x) \right) \Phi_n \\ &= s_p(x) \prod_{d \mid q^\beta} \Phi_{p^\alpha d}(x) + s_q(x) \prod_{d \mid p^\alpha d} \Phi_{q^\beta d}(x) \\ &= s_p(x) F_p(x^{n/p}) + s_q(x) F_q(x^{n/q}), \end{aligned}$$

using (14) and (15) again. Thus we have s_p and $s_q \in \mathbb{Z}[x]$, as required. Next we shall show that s_p and s_q may be chosen so that their coefficients are all non-negative.

Note that as $\deg(g) = n - 1$ and $\deg(F_r) = r - 1$, we have $\deg(s_p) \leqslant n/p - 1$ and $\deg(s_q) \leqslant n/q - 1$. Let $n_p = n/p$ and $n_q = n/q$. Then we may write

$$s_p(x) = u_0 + u_1 x + \ldots + u_{n_p - 1} x^{n_p - 1} \qquad \text{and} \qquad s_q(x) = v_0 + v_1 x + \ldots + v_{n_q - 1} x^{n_q - 1},$$

for suitable u_i and $v_i \in \mathbb{Z}$. Set $A_p(x) = s_p(x) F_p(x^{n_p})$ and $A_q(x) = s_q(x) F_q(x^{n_q})$. If $0 \leqslant r < n$, then the coefficient of x^r in $A_p(x)$ is $\sum u_j$, where the sum runs over those j such that $0 \leqslant j < n_p$ and $j + k n_p = r$, for some $k \in \mathbb{Z}$. There is a unique pair (k, j) with this property, for each such r. Hence the coefficient of x^r in $A_p(x)$ is u_j, where j is the unique integer such that $0 \leqslant j < n_p$ and $r \equiv j \pmod{n_p}$. If $\beta = 0$, then $g(x) = A_p(x)$ and it follows that the u_j are all non-negative; the result follows with $s = s_p$. Assume from now on that $\beta \geqslant 1$. Then the coefficient of x^r in $A_q(x)$ is u_l, where l is the unique integer such that $0 \leqslant l < n_q$ and $r \equiv l \pmod{n_q}$.

Let $d = \gcd(n_p, n_q) = p^{\alpha-1} q^{\beta-1}$. For $j = 0, \ldots, d-1$, define

$$s_{p,j}(x) = \sum_{i=0}^{q-1} u_{id+j} x^{id+j}$$

and

$$s_{q,j}(x) = \sum_{i=0}^{p-1} v_{id+j} x^{id+j}.$$

Then

$$s_p(x) = \sum_{j=0}^{d-1} s_{p,j}(x) \qquad \text{and} \qquad s_q(x) = \sum_{j=0}^{d-1} s_{q,j}(x).$$

Fix j and a with $0 \leqslant j < d$ and $0 \leqslant a < q$. If $0 \leqslant l < n_q$, then there exists r such that $0 \leqslant r < n$ with $r \equiv ad + j \pmod{n_p}$ and $r \equiv l \pmod{n_q}$ if and only if $ad + j \equiv l \pmod{d}$ (using the Chinese remainder theorem) if and only if $l = bd + j$, for some $b \in \mathbb{Z}$. Moreover, $0 \leqslant b < p$, as $0 \leqslant l < n_q$.

Therefore, for all j, a, b with $0 \leqslant j < d$, $0 \leqslant a < q$ and $0 \leqslant b < p$, there exists an integer $r = r(j, a, b)$, unique modulo n, such that

$$n_r = u_{ad+j} + v_{bd+j}. \tag{17}$$

Conversely, if $0 \leqslant r < n$, then there exist j, a, b in the above ranges, such that (17) holds. For fixed j with $0 \leqslant j < d$, define

$$c_j = \min\{u_{ad+j}, v_{bd+j} : 0 \leqslant a < q, 0 \leqslant b < p\}.$$

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

If $c_j \geqslant 0$, define $t_{p,j} = s_{p,j}$ and $t_{q,j} = s_{q,j}$. If $c_j < 0$, then there is some a or b such that $c_j = u_{ad+j}$ or $c_j = v_{bd+j}$. Suppose that $c_j = u_{ad+j} < 0$. Since $n_r \geqslant 0$, for $r = 0, \ldots, n-1$, it follows from (17) that $u_{ad+j} + v_{bd+j} \geqslant 0$ and so $v_{bd+j} \geqslant |c_j|$, for $b = 0, \ldots, p-1$. By definition, $u_{id+j} \geqslant c_j$, for $i = 0, \ldots, q-1$, so if we set

$$t_{p,j}(x) = s_{p,j}(x) + |c_j| x^j F_q(x^d)$$

and

$$t_{q,j}(x) = s_{q,j}(x) - |c_j| x^j F_p(x^d),$$

then the polynomials $t_{p,j}$ and $t_{q,j}$ have non-negative integer coefficients. If $c_j \neq u_{ad+j}$ but $c_j = v_{bd+j}$, for some b, we construct $t_{p,j}$ and $t_{q,j}$ in the same way, reversing the roles of p and q, and obtain the same result.

Now fix j such that $c_j < 0$. Assume that $c_j = u_{ad+j}$. Then

$$\begin{aligned} t_{p,j}(x)F_p(x^{n/p}) + t_{q,j}(x)F_q(x^{n/q}) &= s_{p,j}(x)F_p(x^{n/p}) + s_{q,j}(x)F_q(x^{n/q}) \\ &\quad + |c_j| x^j (F_q(x^d)F_p(x^{n/p}) - F_p(x^d)F_q(x^{n/q})) \end{aligned} \tag{18}$$

We have

$$\begin{aligned} F_q(x^d)F_p(x^{n/p}) &= F_q(x^{p^{\alpha-1}q^{\beta-1}})F_p(x^{p^{\alpha-1}q^{\beta}}) \\ &= \prod_{d \mid p^{\alpha-1}} \Phi_{q^\beta d}(x) \prod_{e \mid q^\beta} \Phi_{p^\alpha e}(x), \qquad \text{from (14) and (15)}, \\ &= \left(\prod_{d \mid p^{\alpha-1}} \Phi_{q^\beta d}(x) \prod_{e \mid q^{\beta-1}} \Phi_{p^\alpha e}(x) \right) \Phi_{p^\alpha q^\beta}(x) \\ &= \prod_{d \mid p^{\alpha}} \Phi_{q^\beta d}(x) \prod_{e \mid q^{\beta-1}} \Phi_{p^\alpha e}(x) \\ &= F_q(x^{n/q})F_p(x^d). \end{aligned}$$

Therefore, from (18),

$$t_{p,j}(x)F_p(x^{n/p}) + t_{q,j}(x)F_q(x^{n/q}) = s_{p,j}(x)F_p(x^{n/p}) + s_{q,j}(x)F_q(x^{n/q}). \tag{19}$$

Now define

$$s_1(x) = \sum_{j=0}^{d-1} t_{p,j}(x)$$

and

$$s_2(x) = \sum_{j=0}^{d-1} t_{q,j}(x).$$

Then the coefficients of s_1 and s_2 are non-negative, and it follows from (19) that

$$g(x) = s_p(x)F_p(x^{n/p}) + s_q(x)F_q(x^{n/q}) = s_1(x)F_p(x^{n/p}) + s_2(x)F_q(x^{n/q}),$$

as required. □

Acknowledgements. The authors are grateful to H. Buhrman, S. Linton, M. Mosca and C. Smyth for useful contributions and helpful suggestions during the writing of this paper.

References

1. R. Beals, 'Quantum computation of Fourier transforms over the symmetric groups', *Proc. 29th Annual ACM Symposium on Theory of Computing*, El Paso, Texas, May 1997 (ACM, New York, 1999) 48–53. 43
2. R. Cleve, A. Ekert, C. Macchiavello and M.Mosca, 'Quantum algorithms revisited', *Proc. Royal Soc. London, Ser. A* 454 (1998) 339. 56
3. G. Constantini and F. Smeraldi, 'A generalisation of Deutsch's example', 1997, http://lanl.arxiv.org/abs/quant-ph/9702020. 56
4. D. Coppersmith, 'An Approximate Fourier transform useful for quantum factoring', Technical Report RC 19642, IBM Research Division, Yorktown Heights, NY, December 1994. 43
5. D. Deutsch, 'Quantum theory, the Church–Turing principle and the universal quantum computer', *Proc. Royal Soc. London, Ser. A* 400 (1985) 97–117. 40, 56
6. D. Deutsch and R. Jozsa, 'Rapid solution of problems by quantum computation', *Proc. Royal Soc. London, Ser. A* 439 (1992) 553–558. 40, 56
7. M. Ettinger and P. Høyer, 'On quantum algorithms for noncommutative hidden subgroups', *Adv. Appl. Math.* 25 (2000) 239–251. 43
8. W. Fulton and J. Harris, *Representation theory*, Grad. Texts in Math. 129 (Springer, New York, 1991). 42, 56
9. M. Grigni, L. J. Schulman, M. Vazirani and U. Vazirani, 'Quantum mechanical algorithms for the nonabelian hidden subgroup problem', STOC (2001), *Combinatorica* 24 (2004) 137–154. 54
10. S. Hallgren, A. Russell and A. Ta-Shma, 'Normal subgroup reconstruction and quantum computation using group representations', *Proc. 32nd Annual ACM Symposium on Theory of Computing* (ACM, New York, 2000) 627–635. 54
11. P. Høyer, 'Efficient quantum transforms', 1997, http://lanl.arxiv.org/abs/quant-ph/9702028. 43
12. P. Høyer, 'Conjugated operators in quantum algorithms', *Phys. Rev. A* 59 (1999) 3280–3289. 40, 49, 54, 55, 56
13. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Grad. Texts in Math. 84 (Springer, New York, 1982). 58
14. W. Ledermann, *Introduction to group characters* (Cambridge Univ. Press, Cambridge, 1987). 56, 57
15. D. K. Maslen and D. N. Rockmore, 'Generalised FFTs — a survey of some recent results', *Proc. 1995 DIMACS Workshop in Groups and Computation*, ed. L. Finkelstein and W. Kantor, DIMACS Ser. Discrete Math. Comput. Sci. 28 (Amer. Math. Soc., Providence, RI, 1997) 183–238. 43
16. C. Moore, D. Rockmore and A. Russell, 'Generic quantum Fourier transforms', *Proc. Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms* (*SODA*), New Orleans, LA, January 11–13 2004 (SIAM, Philadelphia, PA, 2004) 778–787. 43, 51
17. M. A. Nielsen and I. L.Chuang, *Quantum computation and quantum information* (Cambridge Univ. Press, Cambridge UK, 2000). 46

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press

18. M. Püschel, M. Rötteler and T. Beth, 'Fast quantum Fourier transforms for a class of non-abelian Groups', *Applied algebra, algebraic algorithms and error correcting codes*, Proc. 13th international symposium, AAECC-13, Honolulu, HI, USA, November 15–19, 1999, ed. Marc Fossorier, *et al.*, Lect. Notes in Comput. Sci. 1719 (Springer, Berlin, 1999) 148–159. 43

19. M. Rötteler and T. Beth, 'Polynomial-time solution to the hidden subgroup problem for a class of non-Abelian groups', v1, 1998, http://lanl.arxiv.org/abs/quant-ph/9812070. 43

20. P. W. Shor, 'Algorithms for quantum computation: discrete logarithm and factoring', *Proc. 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, 1994) 124–134. 43

21. A. Terras, *Fourier analysis on finite groups and applications*, London. Math. Soc. Student Texts 43 (Cambridge Univ. Press, Cambridge, UK, 1999). 42, 57

Michael Batty Michael.Batty@ncl.ac.uk
http://www.mas.ncl.ac.uk/∼nmb45/
Andrew J. Duncan A.Duncan@ncl.ac.uk
http://www.mas.ncl.ac.uk/∼najd2/

Department of Mathematics
School of Mathematics and Statistics
Merz Court
University of Newcastle upon Tyne
Newcastle upon Tyne, NE1 7RU
United Kingdom

Samuel L. Braunstein schmuel@cs.york.ac.uk
http://www-users.cs.york.ac.uk/∼schmuel/

Department of Computer Science
University of York
York, YO10 5DD
United Kingdom.

https://doi.org/10.1112/S1461157000001182 Published online by Cambridge University Press