Conjugated Operators in Quantum Algorithms

Peter Høyer [*]

Odense University [†]

Abstract

This paper addresses the question of understanding quantum algorithms in terms of unitary operators. Many quantum algorithms can be expressed as applications of operators formed by conjugating so-called classical operators. The operators that are used for conjugation are determined by the problem and any additional structure possessed by the Hilbert space that is acted upon. We prove many new commutative laws between these different operators, and we use those to phrase and analyze old and new problems and algorithms. As an example, we review the Abelian subgroup problem. We then introduce the problem of determining a group homomorphism, and we give classical and quantum algorithms for it. We also generalize Deutsch's problem and improve the previous best algorithms for earlier generalizations of it.

1 Quantum computation

Here is an outline of the most popular quantum algorithm ever developed. It begins with elementary classical preprocessing, and then it applies the following quantum experiment: starting in an initial superposition of all possible states, it computes a classical function, applies a quantum Fourier transform, and finally performs a measurement. Depending on the outcome, it may carry out one or more similar quantum experiments, or complete the computation with some classical postprocessing.

This algorithm is in fact not just a single algorithm, but rather a large class of algorithms. It includes Shor's algorithms for factoring and discrete logarithms [1],

[*] Supported in part by the ESPRIT Long Term Research Programme of the EU under project number 20244 (ALCOM-IT).

[†] Department of Mathematics and Computer Science, Odense University, Campusvej 55, DK-5230 Odense M, Denmark. Email: u2pi@imada.ou.dk.

Deutsch's initiating algorithm [2], and the algorithms by Bernstein and Vazirani [3], Simon [4], and others.

It is the aim of this paper to investigate the properties and computational power of this kind of algorithms. Our focus is on the quantum part, the experiments, and to a smaller extent on the classical preprocessing and postprocessing. Below, we write these quantum experiments as conjugated classical operators acting on initial superpositions, followed by a measurement. We do not only consider the above problems and their algorithms, but more generally, problems that have a classical origin, and quantum algorithms obtained by conjugating classical operators (defined below).

The general setup for our considerations is as follows. Given a mapping $\gamma : A \to R$ between finite sets, the problem is to compute some property π of γ. As commonly done, we require that the length of the answer $\pi(\gamma)$ is polynomially bounded in the logarithm of the cardinality of A. Many interesting properties of functions $\gamma : A \to R$ are decision problems where π only takes the values 0 and 1. Assuming we have a polynomial-time algorithm computing γ, then some of these are known to be in $\mathcal{NP}$,[1] as for example: Is γ non-constant on A?

Our main assumption is that γ comes as a black box so that it is not possible to obtain knowledge about γ by any other means than evaluating it on points in its domain. We assume that the input to the black box is a pair $(a,r) \in A \times R$, and that the output $(a',r') \in A \times R$ satisfies that $a' = a$ for all inputs. Further, we assume that the set R contains a particular element denoted 0_R, such that the black box outputs $(a, \gamma(a))$ on the input $(a, 0_R)$. These restrictions are without loss of generality since Bennett [6] has shown that any classical computation can be reduced to one on the above form. They are needed since they provide us with a natural way to extend the black box to work on a quantum system.

We summarize a few important issues of computation on quantum systems before discussing how to extend γ to such systems. We otherwise assume that the reader is familiar with the basic notions of quantum computing [7]. For any finite set X, let $\mathbb{C}X$ denote the vector space of all finite $\mathbb{C}$–linear combinations of elements in X. On a quantum system, all computations on $\mathbb{C}X$ are done with respect to some preferred basis, called the *computational basis*. We shall always pick X itself as this basis since we find it the most natural choice if we are to compare classical and quantum algorithms. We require that the initialization and measurements are performed with respect to this basis, too. As normal in quantum computation, we use Dirac notation: the column vector of the basis element $x \in X$ is denoted by the *basis state* $|x\rangle$, and its row vector by $\langle x|$. Similarly, we denote the column vector of $\sum \alpha_x \, x \in \mathbb{C}X$ by the *superposition* $\sum \alpha_x |x\rangle$.

[1] $\mathcal{NP}$ denotes the class of decision problems that can be solved in polynomial time on a classical, non-deterministic computer. (See for example [5] for an introduction to complexity theory.)

Having fixed the computational basis to $A \otimes R$, the evaluation of γ is naturally extended to quantum systems. The quantum black box implements a unitary operator $\mathbf{U}_\gamma$ on the Hilbert space $\mathbb{C}A \otimes \mathbb{C}R$, and it satisfies that $\mathbf{U}_\gamma |a\rangle|0_R\rangle = |a\rangle|\gamma(a)\rangle$ for all $a \in A$. Here, the notation $|a\rangle|r\rangle$ is shorthand for $|a\rangle \otimes |r\rangle$.

The most naive approach to find property π for some given function $\gamma : A \to R$, is to initialize some state $|\Psi\rangle$, apply $\mathbf{U}_\gamma$, and then measure the system. That is, to perform the experiment $(z_1, z_2) = (\mathcal{M}_1 \otimes \mathcal{M}_2) \circ \mathbf{U}_\gamma |\Psi\rangle$ where $\mathcal{M}_i$ denotes a measurement of the ith register with outcome z_i. From the outcome, we then try classically to deduce nontrivial knowledge about $\pi(\gamma)$. By repeating this experiment for various initial states, we might hope to determine the sought property.

For many problems, this straightforward approach will not apply—simply because of the structure of the operator $\mathbf{U}_\gamma$. But this does of course not exclude fast quantum algorithms for the problem. An elementary, but very important, observation is that there might exists some other orthonormal basis $X \subset \mathbb{C}A \otimes \mathbb{C}R$ for which the unitary operator $\mathbf{U}_\gamma$ takes a simple form. In that case, we might consider the experiment

$$(z_1, z_2) = (\mathcal{M}_1 \otimes \mathcal{M}_2) \circ (\mathbf{M}\, \mathbf{U}_\gamma\, \mathbf{M}^\dagger)\, |\Psi\rangle$$

where $\mathbf{M}$ is the unitary operator that maps the basis X to the basis $A \otimes R$, and where we use the dagger symbol for the inverse. This experiment consists of three parts: the initialization of $|\Psi\rangle$, the application of the operator $(\mathbf{M}\, \mathbf{U}_\gamma\, \mathbf{M}^\dagger)$, and finally the read out.

In contrast to many papers on quantum computation, we shall refrain from intermixing our analysis of the first two parts. We believe that those two parts serve different purposes and to get a full understanding of the second, it needs its own investigation. This second part is obtained by conjugating a "classical" operator $\mathbf{U}_\gamma$ with a unitary operator $\mathbf{M}$. We refer to $\mathbf{M}$ as a *conjugation operator* and to $(\mathbf{M}\, \mathbf{U}_\gamma\, \mathbf{M}^\dagger)$ as the *conjugated operator*. In this context, rather than thinking of $\mathbf{M}$ as a unitary operator, we think of it as implementing a basis change from some orthonormal basis X to the computational basis $A \otimes R$. In all our examples in what follows, the basis X is the tensor product of a basis for $\mathbb{C}A$ and a basis for $\mathbb{C}R$. The second part of the above experiment then takes the simpler form

$$(\mathbf{A} \otimes \mathbf{R})\, \mathbf{U}_\gamma\, (\mathbf{A}^\dagger \otimes \mathbf{R}^\dagger).$$

It is worth noting that all quantum algorithms developed so far apply such a conjugated operator at some point during the computation.

1.1 Conjugating classical functions

In the above definitions, the function $\gamma : A \to R$ is a mapping between arbitrary finite sets. For most problems studied in quantum computing, the set A has a known structure of an additive group $G = \langle G, \oplus \rangle$. In that case, we reflect this by writing $\gamma : G \to R$. On the other hand, if the image R has a known structure of a group $H = \langle H, \oplus \rangle$, then we write $\gamma : A \to H$ and we assume that the black box $\mathbf{U}_\gamma$ implements the unitary operator defined by $|a\rangle|h\rangle \mapsto |a\rangle|h \oplus \gamma(a)\rangle$. Finally, we use the notation $\gamma : G \to H$ if γ is a mapping between finite additive groups. We do *not* assume that γ is a group homomorphism unless this is stated explicitly.

For convenience, from now on, A and R denote finite sets and G and H finite additive groups.

Suppose $\gamma : G \to R$ is defined on some finite group G, and consider the possible choices for the conjugation operator in the second part of the experiment discussed above. There are at least two natural candidates: the first is just the identity $\mathbf{I} \otimes \mathbf{I}$, and the second is to apply a Fourier transform on the first part of the system, that is, to conjugate $\mathbf{U}_\gamma$ by $\mathbf{F}_G \otimes \mathbf{I}$. A Fourier transform $\mathbf{F}_G$ for a finite group G is a unitary operator on $\mathbb{C}G$ and is defined in Sec. 2 below.

Fourier transforms will be our most used operator for conjugation and we therefore give the corresponding conjugated operators their own symbols,

$$\boldsymbol{\mathcal{V}} = \boldsymbol{\mathcal{V}}(\gamma) = (\mathbf{F}_G \otimes \mathbf{I})\, \mathbf{U}_\gamma\, (\mathbf{F}_G^\dagger \otimes \mathbf{I}) \tag{1}$$

$$\boldsymbol{\mathcal{W}} = \boldsymbol{\mathcal{W}}(\gamma) = (\mathbf{F}_G \otimes \mathbf{F}_H)\, \mathbf{U}_\gamma\, (\mathbf{F}_G^\dagger \otimes \mathbf{F}_H^\dagger). \tag{2}$$

We sometimes refer to $\boldsymbol{\mathcal{V}}$ and $\boldsymbol{\mathcal{W}}$ as *G–operators*.

In Sec. 3, we state old and new properties of the G–operators. In the following three sections, we then discuss applications of the G–operators. First, in Sec. 4, we review the unknown subgroup problem and its quantum solutions. We introduce the problem of determining a group homomorphism $\gamma : G \to H$ in Sec. 5, and in the following section, we consider the problem of determining if a function is constant or not.

2 Fourier transforms for finite groups

Since the quantum Fourier transform plays a central role in the area of quantum algorithms, we now give a brief summary of the relevant theory. We refer the reader to for example [8] for further details.

2.1 Arbitrary groups

We define Fourier transforms for arbitrary finite groups and exemplify the definitions on the dihedral group

$$D_3 = \langle r, c : r^3 = c^2 = e, rc = cr^2 \rangle$$

of order 6 and with identity e. In the following subsections, we then discuss in much more detail the case when the group is Abelian. So far, all applications of the quantum Fourier transform have been for Abelian groups.

In this first subsection, we exceptionally use multiplicative notation for the group operation. Thus, here G denotes an arbitrary finite group, written multiplicative. We start by forming a vector space for G.

Let $\mathbb{C}G = \{\sum_{g \in G} \alpha_g g : \alpha_g \in \mathbb{C}\}$ be the set of all finite $\mathbb{C}$–linear combinations of elements in G and endow $\mathbb{C}G$ with the natural choice for addition, $\big(\sum_{g \in G} \alpha_g g\big) + \big(\sum_{g \in G} \beta_g g\big) = \sum_{g \in G} (\alpha_g + \beta_g) g$. Then $\mathbb{C}G$ is a complex vector space having G as a basis $\mathcal{B}_t$ and thus having dimension equal to $|G|$, the order of G. Equip $\mathbb{C}G$ further with the natural choice for multiplication $\big(\sum_{g \in G} \alpha_g g\big)\big(\sum_{h \in G} \beta_h h\big) = \sum_{g,h \in G} (\alpha_g \beta_h) gh$. Then $\mathbb{C}G$ becomes an algebra, called the *group algebra* of G over $\mathbb{C}$. Moreover, $\mathbb{C}G$ is a Hilbert space by endowing it with the standard complex inner product.

Consider the left action of G on $\mathbb{C}G$ obtained naturally by restricting the multiplication in $\mathbb{C}G$ to $G \times \mathbb{C}G$. In our example, the action of the group element $r \in D_3$ on the vector $e + 3r^2 - 2c \in \mathbb{C}D_3$ is the vector $r(e + 3r^2 - 2c) = 3e + r - 2cr^2$.

We say that a subspace U of $\mathbb{C}G$ is invariant under the action of G if $gU \subseteq U$ for all $g \in G$. Invariant subspaces endowed with the above action of G are called *$\mathbb{C}G$–modules*. Clearly, if U_1 and U_2 are $\mathbb{C}G$–modules, then so is the sum $U_1 + U_2$. Conversely, if a module U contains a submodule V, then U also contains a submodule W such that $U = V \oplus W$. Thus, we can restrict our attention to the nontrivial modules that contain no nontrivial, proper submodule. Such modules are called *irreducible $\mathbb{C}G$–modules*.

If we return to our example, then we see that the subspace $U_1 \subseteq \mathbb{C}D_3$ spanned by the vector $u_1 = \sum_{g \in D_3} g = e + r + r^2 + c + cr + cr^2$ is invariant since $gu_1 = u_1 \in U_1$ for all $g \in D_3$. Similarly, the vector $u_2 = (e + r + r^2) - (c + cr + cr^2)$ spans an invariant subspace U_2 of dimension 1 since $ru_2 = u_2$ and $cu_2 = -u_2$. Besides these two subspaces, there are no other invariant subspace of dimension 1. Let $\omega_n = \exp(2\pi\sqrt{-1}/n)$ denote the nth principal root of unity. Then the subspace U_3 spanned by $u_3 = e + \omega_3 r + \omega_3^2 r^2$ and $u_4 = c + \omega_3 cr + \omega_3^2 cr^2$ is invariant, and so is the subspace U_4 spanned by $u_5 = e + \omega_3^2 r + \omega_3 r^2$ and $u_6 = c + \omega_3^2 cr + \omega_3 cr^2$. Both U_3 and U_4 are irreducible since neither contains u_1.

The four irreducible $\mathbb{C}D_3$–modules U_i have dimension 1,1,2, and 2, respectively, and are mutually orthogonal. We can thus write $\mathbb{C}D_3$ as the direct sum $\mathbb{C}D_3 = U_1 \oplus U_2 \oplus U_3 \oplus U_4$. Such decomposition of $\mathbb{C}G$ into irreducible submodules exists for every finite group G (see for example [8]).

Theorem 1 *For all finite groups G, we have that $\mathbb{C}G$ can be written as a direct sum of irreducible $\mathbb{C}G$–modules, $\mathbb{C}G = U_1 \oplus \cdots \oplus U_s$.*

One may ask what relationship there are between these subspaces U_i? Continuing our example, since both U_1 and U_2 have dimension 1, they are isomorphic as vector spaces, and so are U_3 and U_4. The latter isomorphism is however stronger than the former in the sense that only it can be chosen such that it commutes with the action of G: Let $\varphi : U_3 \to U_4$ denote the vector space isomorphism defined by $\varphi(u_3) = u_6$ and $\varphi(u_4) = u_5$. Then $\varphi(gv) = g\varphi(v)$ for all $g \in D_3$ and $v \in U_3$. To prove that no such isomorphism for U_1 and U_2 exists, it suffices to note that $ru_1 + cu_1 = 2u_1$ whereas $ru_2 + cu_2 = 0$.

This motivates the following definition. Let G be a finite group and let U and V be $\mathbb{C}G$–modules. A mapping $\varphi : U \to V$ is an *isomorphism of* $\mathbb{C}G$*–modules* if φ is an isomorphism of vector spaces and $\varphi g = g\varphi$ for all $g \in G$. With this, we have in our example that

$$\mathbb{C}D_3 = U_1 \oplus U_2 \oplus (U_3 \oplus U_4) = V_1 \oplus V_2 \oplus V_3$$

where each V_i is the direct sum of isomorphic irreducible $\mathbb{C}D_3$–submodules. More generally, Theorem 1 can be refined as follows (see for example [8]).

Theorem 2 *For all finite groups G, there exist integers r and $d_1, \ldots, d_r$ such that $\mathbb{C}G = V_1 \oplus \cdots \oplus V_r$ where each $V_i = U_{i1} \oplus \cdots \oplus U_{id_i}$ is the direct sum of irreducible submodules, and U_{ik} and U_{jl} are isomorphic if and only if $i = j$. Furthermore, every $\mathbb{C}G$–module is isomorphic to the direct sum of a subset of the submodules U_{ik}.*

We are now ready to define Fourier transforms for an arbitrary finite group G. Pick an orthonormal basis $\mathcal{B}_i$ for each of the r subspaces V_i appearing in Theorem 2. Set $\mathcal{B}_f = \cup_i \mathcal{B}_i$ to be the joined basis for $\mathbb{C}G$. The *Fourier transform* $\mathbf{F}_G$ for G with respect to $\mathcal{B}_f$ is a change of basis from the standard basis $\mathcal{B}_t = G$ to $\mathcal{B}_f$. Given a vector $f \in \mathbb{C}G$ in the standard basis, the Fourier-transform of f is the same vector $\hat{f} \in \mathbb{C}G$, but now given with respect to the basis $\mathcal{B}_f$. The coordinates of $\hat{f}$ are called the *Fourier coefficients* of f with respect to $\mathcal{B}_f$. Note that the Fourier transform is unitary by definition.

Returning to our example, let u_i' denote the unit vector found by multiplying u_i with the reciprocal of its norm. The matrix of $\mathbf{F}_{D_3}$ with respect to the ordered orthonormal bases, $\mathcal{B}_t = (e, r, r^2, c, cr, cr^2)$ and $\mathcal{B}_f = (u_1', u_3', u_5', u_2', u_4', u_6')$, is

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \overline{\omega}_3 & \overline{\omega}_3^2 & & & \\ 1 & \overline{\omega}_3^2 & \overline{\omega}_3 & & & \\ 1 & 1 & 1 & -1 & -1 & -1 \\ & & & 1 & \overline{\omega}_3 & \overline{\omega}_3^2 \\ & & & 1 & \overline{\omega}_3^2 & \overline{\omega}_3 \end{bmatrix}$$

where we have omitted normalization of the rows, and where $\overline{\lambda}$ denotes the complex conjugate of $\lambda \in \mathbb{C}$.

Consider the action of G on a vector $f \in \mathbb{C}G$. Fix an ordering of $\mathcal{B}_t = (g_1, \ldots, g_m)$ where m denotes the order of the group and represent f by the tuple, $f = (f(g_1), \ldots, f(g_m))$ For all elements $g \in G$, the tuple representing gf contains the same entries as the tuple representing f, but with the entries permuted. A drawback of the basis $\mathcal{B}_t$ is that the group action is global in the sense that for every two entries i and j, there exists an element $g \in G$ such that the jth entry in gf equals the ith entry in f.

Using the Fourier-transformed basis $\mathcal{B}_f$ instead helps on this problem since it decomposes the space $\mathbb{C}G$ into a direct sum of smallest possible subspaces that are invariant under the group action. Thus, we may say that the basis $\mathcal{B}_f$ makes the action of G on $\mathbb{C}G$ as local as possible. The given group G determines how small these subspaces can be. In particular, all the irreducible $\mathbb{C}G$–modules have dimension 1 if and only if G is Abelian. We consider this case in the rest of this section.

2.2 Abelian groups

Let $G = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ be a direct sum of finite additive cyclic groups, where $\mathbb{Z}_m$ denotes the cyclic group of order m. From now on, we again use addition as the group operation. To avoid confusion with vector addition, we use the symbol $\oplus$ for addition of group elements, and we denote the inverse of $g \in G$ by $\ominus g$ to distinguish it from the vector $-g = -1g$. As in the previous subsection, we exemplify all the following main concepts, this time using the Abelian group $K = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

We start by determining the irreducible $\mathbb{C}G$–modules. Define a bilinear map $\mu = \mu^G : G \times G \to \mathbb{C}^\star$ by

$$\mu(g, h) = \prod_{i=1}^{n} \omega_{m_i}^{-g_i h_i} \qquad (3)$$

where $g = (g_1, \ldots, g_n)$ and $h = (h_1, \ldots, h_n)$. Here, $\mathbb{C}^\star$ denotes the set of the nonzero complex numbers. For each $h \in G$, let U_h denote the subspace spanned by the vector $u_h = \sum_{g \in G} \mu(h, g) g \in \mathbb{C}G$. Then U_h is invariant under the action of G since for all $k \in \mathbb{C}G$, we have that $k u_h = \sum_{g \in G} \mu(h, g) k \oplus g = \mu(h, \ominus k) u_h \in U_h$. Thus, U_h is an irreducible $\mathbb{C}G$–module having dimension 1. The set $\{U_h\}_{h \in G}$ contains all irreducible $\mathbb{C}G$–modules since $\mathbb{C}G$ has dimension $|G|$ and u_h and u_k are orthogonal whenever $h \neq k$. It follows that there is a bijective correspondence between group elements of G and irreducible $\mathbb{C}G$–modules given by $g \longleftrightarrow u'_g$ where u'_g denotes u_g normalized.

Let G^* denote the set $\{u'_g\}$ and define a function $G^* \times G^* \to G^*$ by

$$(u'_g, u'_h) \longmapsto \frac{1}{\sqrt{|G|}} \sum_{k \in G} \mu(g,k)\mu(h,k)\, k.$$

Then $(u'_g, u'_h) \mapsto u'_{g \oplus h}$, and thus G^* is isomorphic to G under the above correspondence.

In our example, there are four irreducible $\mathbb{C}K$–modules, each spanned by one of the vectors

$$\begin{aligned}
u_{00} &= (0,0) + (0,1) + (1,0) + (1,1)\\
u_{01} &= (0,0) - (0,1) + (1,0) - (1,1)\\
u_{10} &= (0,0) + (0,1) - (1,0) - (1,1)\\
u_{11} &= (0,0) - (0,1) - (1,0) + (1,1).
\end{aligned}$$

Here we use the notation $u_{g_1 g_2}$ as shorthand for $u_{(g_1,g_2)}$, where $(g_1, g_2) \in K$. The set of these four subspaces admit a group structure which easily can be verified to be isomorphic to K by comparing their group operation tables.

Let $\mathcal{B}_t = G$ denote the standard basis for $\mathbb{C}G$ and $\mathcal{B}_f$ the basis $\{u'_g\}_{g \in G}$. The Fourier transform $\mathbf{F}_G$ for G maps a vector f given with respect to $\mathcal{B}_t$ to its representation $\hat{f}$ with respect to $\mathcal{B}_f$. A classical way to write this computation is as

$$\hat{f}(u'_h) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \mu(h,g) f(g) \quad \longleftrightarrow \quad f(g) = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \mu(g,h)^{-1} \hat{f}(u'_h).$$

For our purpose, Dirac notation is more suitable. Using it, the Fourier transform reads

$$\mathbf{F}_G = \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \mu(h,g) |u'_h\rangle\langle g|. \tag{4}$$

If we identify the two groups G and G^* in this equation, using the isomorphism $g \longleftrightarrow u'_g$, then we get to our definition of the quantum Fourier transform for an Abelian group G as the unitary operator

$$\mathbf{F}_G = \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \mu(h,g) |h\rangle\langle g| \tag{5}$$

for the Hilbert space $\mathbb{C}G$.

With respect to the ordered bases $\mathcal{B}_t = ((0,0),(0,1),(1,0),(1,1))$ and $\mathcal{B}_f = (u'_{00}, u'_{01}, u'_{10}, u'_{11})$, the matrix of $\mathbf{F}_K$ is

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

The Fourier transform for the cyclic group of 2 elements, $\mathbb{Z}_2$, has the matrix representation $\mathbf{W} = 1/\sqrt{2}\left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$. It is often referred to as the Walsh-Hadamard transform [9].

2.3 The orthogonal subgroup

The concept of orthogonality in Abelian groups is very useful for understanding the Fourier transform. We say that an element $g \in G$ is *orthogonal* to a subset $X \subseteq G$ if, for all $x \in X$, we have that $\mu(g, x)$ is the identity of the group $\mathbb{C}^\star$, that is, if $\mu(g, x) = 1$. For any subset $X \subseteq G$, let

$$X^\perp = \{g \in G \mid \mu(g, x) = 1 \text{ for all } x \in X\} \tag{6}$$

denote the set of elements in G that are orthogonal to X. Clearly, $X^\perp$ is a subgroup and we refer to it as the *orthogonal subgroup* of X. Let $\langle X \rangle$ denote the subgroup generated by X. Then,

$$X^\perp = \langle X^\perp \rangle = \langle X \rangle^\perp \tag{7}$$

$$X^{\perp\perp} = \langle X \rangle \tag{8}$$

$$|X^\perp||X^{\perp\perp}| = |G|. \tag{9}$$

Eq. (7) is easily proven, and for the last two, we sketch simple indirect proofs below.

Given a generating set for a subgroup, one can easily (classically or quantumly) deduce a generating set for its orthogonal subgroup using ideas similar to those used in Gaussian elimination. This fact is often used in coding theory: given the generator matrix of a binary linear code, one can compute the generator matrix of its dual. We state this formally in the following proposition.

Proposition 3 *There exists a classical deterministic algorithm that, given a subset $X \subseteq G$, returns a generating set for $X^\perp$. Moreover, the algorithm runs in time polynomial in* $\log |G|$ *and in the cardinality of X.*

Thus, knowing a small generating set for a subgroup $H \leqslant G$ is polynomial-time equivalent to knowing a small generating set for the orthogonal subgroup $H^\perp \leqslant G$.

Consider the computation for the group K, defined in Sec. 2.2,

$$\mathbf{F}_K\left(|00\rangle + |10\rangle\right) = |00\rangle + |01\rangle$$
$$\mathbf{F}_K\left(|00\rangle + |11\rangle\right) = |00\rangle + |11\rangle,$$

where $|xy\rangle$ is shorthand for $|(x,y)\rangle$. The vector $|00\rangle + |10\rangle$ on the left hand side of the first equation is the superposition of the two basis states $|00\rangle$ and $|10\rangle$. If we think of these as group elements, then they constitute exactly the elements of the subgroup $H = \{(0,0),(1,0)\}$. Likewise, the basis elements in the superposition on the right hand side form the subgroup $H^\perp = \{(0,0),(0,1)\}$. We may thus say that the subgroup $H \leqslant K$ is mapped to the subgroup $H^\perp \leqslant K$ by the Fourier transform for K.

This property holds more generally: For all finite Abelian groups G and subgroups $H \leqslant G$, we have $\mathbf{F}_G|H\rangle = |H^\perp\rangle$, where $|H\rangle$ denotes the equally-weighted superposition $\big(1/\sqrt{|H|}\,\big)\sum_{h\in H}|h\rangle$. Since $\mathbf{F}_G$ is unitary and hence preserves the norm, $|H^\perp| = [G:H]$ as stated in Eq. (9). Similarly, $\mathbf{F}_G^\dagger|H\rangle = |H^\perp\rangle$, so $|H\rangle = \mathbf{F}_G\mathbf{F}_G^\dagger|H\rangle = |H^{\perp\perp}\rangle$, and Eq. (8) follows.

2.4 Characters for Abelian groups

Fourier transforms for finite groups can be defined in a variety of ways. In particular, when the group G is Abelian, it can be interpreted by referring to group homomorphisms instead of irreducible $\mathbb{C}G$–modules. For this, rewrite u_k as $\sum_{g\in G}\alpha_g g$ where coefficient α_g equals $\mu(k,g)$. The set of coefficients $\{\alpha_g\}_g$ gives naturally rise to a mapping $\chi_k : G \to \mathbb{C}^\star$ defined by $g \mapsto \alpha_g = \mu(k,g)$. Since μ is bilinear, then $\chi_k(g \oplus h) = \chi_k(g)\chi_k(h)$ so χ_k is a group homomorphism. The set $\{\chi_k\}_{k\in G}$ contains all homomorphisms from G to $\mathbb{C}^\star$, and thus we have a bijective correspondence between group elements of G and homomorphisms $G \to \mathbb{C}^\star$ given by $g \longleftrightarrow \chi_g$. Not surprisingly, the set $\{\chi_g\}$ admits a group structure under the operation $\chi_g\chi_h = \chi_{g\oplus h}$, so the correspondence is again a group isomorphism.

A group homomorphism $\chi_g = \chi_g^G$ from G to $\mathbb{C}^\star$ is called a linear *character* for G. Note that since μ is symmetric then $\chi_h(g) = \chi_g(h)$ for all $g,h \in G$.

3 Commutative laws of the G–operators

Let G be a finite Abelian group and $\gamma : G \to R$ some mapping defined on G. In Sec. 1, we defined two G–operators, $\boldsymbol{\mathcal{V}}(\gamma)$ and $\boldsymbol{\mathcal{W}}(\gamma)$. Suppose we apply, say, the operator $\boldsymbol{\mathcal{V}}(\gamma)$ on the state $\mu^G(h,g)|g\rangle|r\rangle$ where $g,h \in G$ and $r \in R$. What is the resulting superposition? One way to answer this question is to do the direct calculations. However, a much more elegant and useful solution is to define two more operators for G and then determine the commutative laws of all operators introduced so far. Having first established these laws, we can then easily answer the above question and others in a general setting in the next subsections.

We define two more unitary operators for the group G, the *translation operator* $\boldsymbol{\tau}_t$ $(t \in G)$ and the *phase-change operator* $\boldsymbol{\phi}_s$ $(s \in G)$,

$$\boldsymbol{\tau}_t = \sum_{g \in G} |g \oplus t\rangle\langle g|$$
$$\boldsymbol{\phi}_s = \sum_{g \in G} \mu(s,g)|g\rangle\langle g|.$$

Trivially, $\boldsymbol{\tau}_{t_1}\boldsymbol{\tau}_{t_2} = \boldsymbol{\tau}_{t_1 \oplus t_2}$ and $\boldsymbol{\phi}_{s_1}\boldsymbol{\phi}_{s_2} = \boldsymbol{\phi}_{s_1 \oplus s_2}$ for all $t_1, t_2, s_1, s_2 \in G$. Together with the Fourier transform, these G–operators satisfy the following commutative laws, which we shall use intensively throughout the remaining part of this paper.

Proposition 4 *For all $s, t \in G$,*

$$\mu(s,t)\,\boldsymbol{\tau}_t\,\boldsymbol{\phi}_s = \boldsymbol{\phi}_s\,\boldsymbol{\tau}_t$$
$$\mathbf{F}_G\,\boldsymbol{\phi}_s = \boldsymbol{\tau}_{\ominus s}\,\mathbf{F}_G$$
$$\mathbf{F}_G\,\boldsymbol{\tau}_t = \boldsymbol{\phi}_t\,\mathbf{F}_G\,.$$

Proof Each of these three identities can be proven by a few rewritings. We give here only the proof of the second identity,

$$\begin{aligned}
\mathbf{F}_G\,\boldsymbol{\phi}_s &= \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \mu(g,h)|g\rangle\langle h| \sum_{k \in G} \mu(s,k)|k\rangle\langle k| \\
&= \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \mu(g,h)\mu(s,h)|g\rangle\langle h| \\
&= \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \mu(g \oplus s,h)|g \oplus s \ominus s\rangle\langle h| \\
&= \sum_{k \in G} |k \ominus s\rangle\langle k| \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \mu(g,h)|g\rangle\langle h| \\
&= \boldsymbol{\tau}_{\ominus s}\,\mathbf{F}_G\,.
\end{aligned}$$

□

The lemma states that the Fourier transform maps a coset into phases, and phases into a coset. The dualities between subgroups and orthogonal subgroups, and between phases and cosets, are crucial for all quantum algorithms for Abelian groups developed so far.

As a simple corollary to Proposition 4, we get that $\mathbf{F}_G^\dagger\,\boldsymbol{\phi}_s = \boldsymbol{\tau}_s\,\mathbf{F}_G^\dagger$ and $\mathbf{F}_G^\dagger\,\boldsymbol{\tau}_t = \boldsymbol{\phi}_{\ominus t}\,\mathbf{F}_G^\dagger$. Furthermore, for all $\gamma : G \to R$, we have that $\mathbf{U}_\gamma\,(\boldsymbol{\phi}_s \otimes \mathbf{I}) = (\boldsymbol{\phi}_s \otimes \mathbf{I})\,\mathbf{U}_\gamma$ and $\mathbf{U}_\gamma\,(\boldsymbol{\tau}_{t_1} \otimes \mathbf{I}) = (\boldsymbol{\tau}_{t_1} \otimes \mathbf{I})\,\mathbf{U}_{\gamma'}$ where $\gamma' : G \to R$ is given by $\gamma'(g) = \gamma(g \oplus t_1)$. From these identities, we easily derive the following commutative laws involving operator $\boldsymbol{\mathcal{V}}$.

Lemma 5 *Let $\gamma : G \to R$. Then for all $s, t \in G$,*

$$\boldsymbol{\mathcal{V}}(\gamma)\,(\boldsymbol{\phi}_s \otimes \mathbf{I}) = (\boldsymbol{\phi}_s \otimes \mathbf{I})\,\boldsymbol{\mathcal{V}}(\gamma')$$
$$\boldsymbol{\mathcal{V}}\,(\boldsymbol{\tau}_t \otimes \mathbf{I}) = (\boldsymbol{\tau}_t \otimes \mathbf{I})\,\boldsymbol{\mathcal{V}}$$

where $\gamma' : G \to R$ is defined by $\gamma'(g) = \gamma(g \oplus s)$.

Lemma 5 remains true if we replace $\boldsymbol{\mathcal{V}}$ by $\boldsymbol{\mathcal{W}}$ in the two identities. There is no meaning in considering how $\boldsymbol{\mathcal{V}}$ commutes with operators acting on the second subsystem (that is, R) since we have not assumed any knowledge on its structure, as discussed in Sec. 1. However, for operator $\boldsymbol{\mathcal{W}}$ this is different. If $\gamma : A \to H$ then we also have that $\mathbf{U}_\gamma\,(\mathbf{I}\otimes\boldsymbol{\tau}_t) = (\mathbf{I}\otimes\boldsymbol{\tau}_t)\,\mathbf{U}_\gamma$. This implies that for operator $\boldsymbol{\mathcal{W}}$, we can add one commutative law to the two already stated in Lemma 5.

Lemma 6 *Let $\gamma : G \to H$. Then for all $s_1, t \in G$ and all $s_2 \in H$,*

$$\boldsymbol{\mathcal{W}}(\gamma)\,(\boldsymbol{\phi}_{s_1} \otimes \boldsymbol{\phi}_{s_2}) = (\boldsymbol{\phi}_{s_1} \otimes \boldsymbol{\phi}_{s_2})\,\boldsymbol{\mathcal{W}}(\gamma')$$
$$\boldsymbol{\mathcal{W}}\,(\boldsymbol{\tau}_t \otimes \mathbf{I}) = (\boldsymbol{\tau}_t \otimes \mathbf{I})\,\boldsymbol{\mathcal{W}}$$

where $\gamma' : G \to H$ is defined by $\gamma'(g) = \gamma(g \oplus s_1)$.

For $\gamma : G \to H$, we only lack determining the commutative law between the operators U_γ and $(\mathbf{I} \otimes \boldsymbol{\phi}_s)$. In the next subsection, we prove two new lemmas for that case.

3.1 Commutative laws for $\boldsymbol{\mathcal{W}}$ and $(\mathbf{I} \otimes \boldsymbol{\tau}_t)$

Let $g \in G$ and $h \in H$. Then

$$\begin{aligned}
\mathbf{U}_\gamma\,(\mathbf{I} \otimes \boldsymbol{\phi}_s)\,|g\rangle|h\rangle &= \mu^H(s,h)\,|g\rangle|h \oplus \gamma(g)\rangle \\
&= \mu^H(s, \ominus\gamma(g))\,\mu^H(s, h \oplus \gamma(g))\,|g\rangle|h \oplus \gamma(g)\rangle \\
&= \mu^H(s, \ominus\gamma(g))\,(\mathbf{I} \otimes \boldsymbol{\phi}_s)\,\mathbf{U}_\gamma\,|g\rangle|h\rangle.
\end{aligned}$$

The leading phasefactor can also be written

$$\mu^H(s, \ominus\gamma(g)) = \mu^H(\ominus s, \gamma(g)) = \chi^H_{\ominus s}(\gamma(g)) = (\chi^H_{\ominus s} \circ \gamma)(g),$$

giving

$$\mathbf{U}_\gamma\,(\mathbf{I} \otimes \boldsymbol{\phi}_s) = (\mathbf{X}_{\ominus s} \otimes \mathbf{I})\,(\mathbf{I} \otimes \boldsymbol{\phi}_s)\,\mathbf{U}_\gamma, \tag{10}$$

where, for each $t \in H$, operator $\mathbf{X}_t$ is defined by $\mathbf{X}_t\,|g\rangle = (\chi^H_t \circ \gamma)(g)\,|g\rangle$.

Having established Eq. (10), we can supplement Lemma 6 with the fourth case.

Lemma 7 *Let $\gamma : G \to H$. Then for all $t \in H$,*

$$\boldsymbol{\mathcal{W}}\,(\mathbf{I} \otimes \boldsymbol{\tau}_t) = (\mathbf{I} \otimes \boldsymbol{\tau}_t)\,(\mathbf{F}_G \mathbf{X}_t \otimes \mathbf{F}_H)\,\mathbf{U}_\gamma\,(\mathbf{F}_G^\dagger \otimes \mathbf{F}_H^\dagger)$$

where $\mathbf{X}_t\,|g\rangle = (\chi_t^H \circ \gamma)(g)\,|g\rangle$.

If the two operators $\mathbf{F}_G$ and $\mathbf{X}_t$ satisfy a commutative law, then so do the operators $\boldsymbol{\mathcal{W}}$ and $\mathbf{I} \otimes \boldsymbol{\tau}_t$. The most simple example where this holds is when $\gamma = h$ is a constant function. Then $(\chi_t^H \circ \gamma)(g) = \chi_t^H(h)$ for all $g \in G$, so operator $\mathbf{X}_t$ acts by multiplication with a global phase factor, $\mathbf{X}_t|g\rangle = \chi_t^H(h)\,|g\rangle$. Thus, $\mathbf{F}_G\,\mathbf{X}_t = \chi_t^H(h)\,\mathbf{F}_G$ and we find that

$$\boldsymbol{\mathcal{W}}\,(\mathbf{I} \otimes \boldsymbol{\tau}_t) = \chi_t^H(h)\,(\mathbf{I} \otimes \boldsymbol{\tau}_t)\,\boldsymbol{\mathcal{W}}.$$

With more effort, we can also find a commutative law for $\mathbf{F}_G$ and $\mathbf{X}_t$ if the mapping $\gamma : G \to H$ happens to be a group homomorphism.

Lemma 8 *Let $\gamma : G \to H$ be a homomorphism of groups. Then for all $t \in H$,*

$$\boldsymbol{\mathcal{W}}\,(\mathbf{I} \otimes \boldsymbol{\tau}_t) = (\boldsymbol{\tau}_{\ominus s} \otimes \boldsymbol{\tau}_t)\,\boldsymbol{\mathcal{W}}$$

where $s \in G$ is defined by $\chi_s^G = \chi_t^H \circ \gamma$. Moreover, s and γ uniquely determine t if and only if γ is onto.

Proof First notice that the composed transform $\chi_t^H \circ \gamma$ is a mapping from G to $\mathbb{C}^*$. Since γ is a group homomorphism, then so is the composed mapping $\chi_t^H \circ \gamma$ and thus there exists a unique $s \in G$ such that $\chi_s^G = \chi_t^H \circ \gamma$. The first part follows by writing $\mathbf{F}_G\,\mathbf{X}_t = \mathbf{F}_G\,\boldsymbol{\phi}_s = \boldsymbol{\tau}_{\ominus s}\,\mathbf{F}_G$ and applying Lemma 7. To prove the second part, since γ is a homomorphism, its image is a subgroup K of H. If and only if K is proper in H, then there exist distinct elements $t_1, t_2 \in H$ such that $\chi_{t_1}^H(k) = \chi_{t_2}^H(k)$ for all $k \in K$. $\square$

3.2 The action of operators $\boldsymbol{\mathcal{V}}$ and $\boldsymbol{\mathcal{W}}$

Having determined various commutative laws for the four G–operators $\boldsymbol{\mathcal{V}}$, $\boldsymbol{\mathcal{W}}$, $\boldsymbol{\phi}$, and $\boldsymbol{\tau}$, we now discuss their actions. Fortunately, this can be simplified largely by knowing their commutative laws. For example, we have

$$\boldsymbol{\mathcal{V}}(\gamma)\mu(s,g)|g\rangle|0_R\rangle = \boldsymbol{\mathcal{V}}(\gamma)(\boldsymbol{\phi}_s \otimes \mathbf{I})\,(\boldsymbol{\tau}_g \otimes \mathbf{I})|0\rangle|0_R\rangle = (\boldsymbol{\phi}_s \otimes \mathbf{I})\,(\boldsymbol{\tau}_g \otimes \mathbf{I})\boldsymbol{\mathcal{V}}(\gamma')|0\rangle|0_R\rangle$$

where $\gamma'(g) = \gamma(g \oplus s)$. As this illustrates, if we just know the action of $\boldsymbol{\mathcal{V}}$ on the basis state $|0\rangle|0_R\rangle$, then we can apply the commutative laws to determine the action of $\boldsymbol{\mathcal{V}}$ on other states. Straightforward calculations give that

$$\boldsymbol{\mathcal{V}}(\gamma)\,|0\rangle|0_R\rangle = \frac{1}{|G|}\sum_{g,h\in G}\mu(h,g)\,|h\rangle|\gamma(g)\rangle. \tag{11}$$

The previous subsection already gives how $\boldsymbol{\mathcal{W}}$ commutes with both $\boldsymbol{\phi}$ and $\boldsymbol{\tau}$ applied on either register, so again, we only need to determine the action of $\boldsymbol{\mathcal{W}}$ on the initial state $|0\rangle|0\rangle$. Going through the calculations shows that this state is an eigenstate with eigenvalue 1. In a slightly more general form, we have that $\boldsymbol{\mathcal{W}}(\gamma)\,|g\rangle|0\rangle = |g\rangle|0\rangle$ for all $g \in G$.

This ends our discussion of the G–operators, and we now turn our attention to applications of these. In the following three sections, we consider problems of the form where we are to determine some property of a mapping γ. Shor's celebrated quantum algorithm for the discrete logarithm problem [1] can easily be understood in terms of the unknown subgroup problem, which we review in the next section. Then, in Sec. 5, we introduce the problem of determining a group homomorphism. Finally, in Sec. 6, we give an algorithm for a generalization of Deutsch's problem [2].

4 The unknown subgroup problem

Let G be a finite group and let $\gamma : G \to R$. Suppose there exists a subgroup $H_0 \leqslant G$ such that γ is *constant* and *distinct* on each coset of H_0. That is, suppose $\gamma(g) = \gamma(h)$ if and only if $g \ominus h \in H_0$. Then, following [10], we say of γ that it *fulfills the subgroup promise* with respect to H_0. The *unknown subgroup problem* is: given a black box computing γ, find a generating set for H_0.

This problem can be turned into a decision-problem by instead asking if the subgroup H_0 is nontrivial. Then the problem can trivially be solved in $\mathcal{NP}$. Moreover, Graph Automorphism reduces to it by letting G be the symmetric group S on the vertices V and setting $\gamma(\sigma) = (\sigma(V), E)$ where $\sigma \in S$ and the given graph is (V, E). Since Graph Isomorphism reduces to Graph Automorphism, that problem also reduces to the unknown subgroup problem.

If the given group $G = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}$ is commutative, then we refer to this problem as the *Abelian subgroup problem.* Also in this case, there are classical difficult problems that reduce to it: The *discrete logarithm problem* is, given a prime p, a generator ζ of $\mathbb{Z}_p^\star$, and an element $a \in \mathbb{Z}_p^\star$, find $0 \leq r < p$ such that $\zeta^r = a$ in $\mathbb{Z}_p^\star$. Here $\mathbb{Z}_p^\star$ denotes the multiplicative cyclic group of the positive integers smaller than p. Let $G = \mathbb{Z}_{p-1}^2$ and define the group homomorphism $\gamma : G \to \mathbb{Z}_p^\star$ by $\gamma((g_1, g_2)) = \zeta^{g_1} a^{g_2}$ for $(g_1, g_2) \in G$. Let $H_0 \leqslant G$ be the cyclic subgroup of order $p-1$ generated by the element $(r, -1) = (r, p-2)$. Then γ is constant and distinct on each coset of H_0. The discrete logarithm problem reduces to finding the unique element $(g_1, g_2) \in H_0$ for which $g_2 = -1$.[2] This element can, given a small generating set for H_0, be found classically in deterministic

[2]It also reduces to finding the unique element $(g_1, g_2) \in H_0^\perp$ for which $g_1 = 1$, but we do not need that here.

polynomial time by computing greatest common divisors using the Euclidean algorithm.

Quantum algorithms for the Abelian subgroup problem have been investigated by several authors. First, Simon [4] considered the case when $G = \mathbb{Z}_2^n$ and H_0 is promised to have order at most 2. Assuming that γ can be computed in polynomial time on a quantum computer, he proved that there exists a $\mathcal{ZQP}$–algorithm finding a generating set for H_0. Here and below, we use the term $\mathcal{ZQP}$–algorithm (resp. $\mathcal{QP}$–algorithm) to denote an algorithm that runs in expected (resp. guaranteed worst-case) polynomial time on a quantum computer. Shortly after, Shor [1] showed that the discrete logarithm problem also can be solved by a $\mathcal{ZQP}$–algorithm. His solution consists essentially of first using the above described reduction and then solving the resulting special case of the Abelian subgroup problem. In neither of the two papers just mentioned, is a group-theoretical language used.

To solve the Abelian subgroup problem, by Proposition 3, it suffices to find a generating set for the orthogonal subgroup $H_0^\perp$. Such a set can be found efficiently if we have a fast algorithm for finding a random element of $H_0^\perp$ (see [10] for details). Thus, an efficient sampling algorithm of $H_0^\perp$ yields a $\mathcal{ZQP}$–algorithm for the Abelian subgroup problem.

In [4], Simon gave an efficient quantum algorithm for sampling a random element of $H_0^\perp$ when the given group G is the direct sum $\mathbb{Z}_2^n$. His algorithm can be generalized in a natural way to arbitrary finite Abelian groups. In terms of the operator $\boldsymbol{\mathcal{V}}$, it can be stated simply as performing the experiment

$$z = \mathcal{M}_1 \circ \boldsymbol{\mathcal{V}}(\gamma)\,|0\rangle|0_R\rangle.$$

We refer the reader to [10] for details.

The results by Simon and Shor were extended by Boneh and Lipton [11] and Grigoriev [12] to include $\mathcal{ZQP}$–algorithms for several variations of the Abelian subgroup problem. Kitaev [13] then gave an algorithm for efficiently computing the quantum Fourier transform for any finite Abelian group. His method applies the transform not with perfection, but only with arbitrarily good precision (see [13] for details). Yet, this suffices to imply a sampling algorithm that succeeds with arbitrarily high probability, and hence also a $\mathcal{ZQP}$–algorithm for the general Abelian subgroup problem.

A natural next question to ask is if it is possible to solve the Abelian subgroup problem in *worst-case* polynomial time, as opposed to in expected polynomial time as just described? A partial answer to that question was first given in [14] by showing that, under some additional assumptions, a single nonzero element of $H_0^\perp$ can be found deterministically. Brassard and Høyer [10] then showed that for some groups of smooth order, it is possible deterministically to find a generating set for $H_0^\perp$, and not only a single nonzero element. Here the order of a group G is *smooth* if all its prime factors are at most $\log^c |G|$ for some fixed constant c. Building on the work in [14], Beals [15] has subsequently, for the case $G = \mathbb{Z}_2^n$, found an alternative deterministic quantum algorithm for finding a generating set for $H_0^\perp \leqslant \mathbb{Z}_2^n$.

5 Determining a group homomorphism

In this section, we introduce the problem of determining a group homomorphism and we compare classical and quantum solutions for it. Let G and H be finite Abelian groups, and let $\gamma : G \to H$ be a homomorphism given as a black box. The *group homomorphism problem* is to compute the value of γ on a generating set for G.

This problem reduces to the case where G and H have the same exponents. To see this, let $\gamma : G \to H$ be a homomorphism. Let e_G (e_H) be the smallest exponent for G (H). We now show that the problem of determining γ can easily be done by solving a problem $\gamma' : G' \to H'$ where $e_{G'} = e_{H'} = \gcd(e_G, e_H)$ and $e_{G'}$ ($e_{H'}$) is the smallest exponent of G' (H'). Since γ is a homomorphism, the order of $\gamma(g)$ divides the order of g for all elements $g \in G$. Thus, the image of γ is contained in the subgroup $H' \leqslant H$ of all elements of order dividing e_G and we therefore regard γ a mapping from G to H'. Let $e = e_{H'}$ be the smallest exponent for H'. Then the subgroup $eG = \{eg : g \in G\}$ is contained in the kernel of γ. Set $G' = G/eG$ and define $\gamma' : G' \to H'$ by $\gamma'(g' \oplus eG) = \gamma(g')$. This mapping is a well-defined homomorphism, and if we know the value of γ' on a generating set for G', then we can easily deduce the value of γ on a generating set for G.

We show in the next lemma that if G and H have the same exponents, then classically, it is necessary to evaluate γ on a generating set for G to determine γ uniquely.

Lemma 9 *Let G and H be finite Abelian groups having the same exponents. Given a group homomorphism $\gamma : G \to H$ as a black box, we can uniquely determine γ if and only if we know the value of γ on a generating set for G.*

Proof Suppose we have evaluated the black box on the subset $X \subseteq G$. Let K be the subgroup generated by X, and let $\gamma_K : K \to H$ be the unique homomorphism consistent with those answers. If $K = G$, then trivially $\gamma = \gamma_K$.

Now, suppose K is proper in G. Let γ'_K be any extension of γ_K to G. Consider the group of homomorphisms from G/K to H, denoted $\mathrm{Hom}(G/K, H)$. Since G/K is nontrivial and since the smallest exponent of G/K divides every exponent of H, then $\mathrm{Hom}(G/K, H)$ is nontrivial. Let $\gamma'_1, \gamma'_2 \in \mathrm{Hom}(G/K, H)$ be two distinct elements. For $i = 1, 2$, define the mapping $\gamma_i : G \to H$ by $\gamma_i(g) = \gamma'_i(g \oplus K) \oplus$

$\gamma'_K(g)$. Clearly, γ_1 and γ_2 are homomorphisms, and since they are distinct and both are extensions of γ_K, the lemma follows. □

It follows that any classical algorithm solving the group homomorphism problem must apply the black box on a generating set for G.

Corollary 10 *Let G and H be finite Abelian groups having the same exponents. Let a group homomorphism $\gamma : G \to H$ be given as a black box. Then any classical deterministic algorithm solving the group homomorphism problem must apply the black box at least n times, where n is the cardinality of the smallest set generating G.*

On a quantum computer, we can beat this bound if H is generated by a set smaller than any set generating G.

Theorem 11 *Let G and H be finite Abelian groups having the same exponents. Let a group homomorphism $\gamma : G \to H$ be given as a black box. Then there exists a quantum algorithm solving the group homomorphism problem using only m applications of the black box, where m is the cardinality of the smallest set generating H.*

Let $G = \mathbb{Z}_{q_1} \oplus \cdots \oplus \mathbb{Z}_{q_n}$ and $H = \mathbb{Z}_{r_1} \oplus \cdots \oplus \mathbb{Z}_{r_m}$. For $1 \leq i \leq n$, let g_i denote the element in G that contains 1 at its ith entry, and 0 everywhere else. Similarly, for $1 \leq i \leq m$, let t_i denote the element in H that contains 1 at its ith entry, and 0 everywhere else. The algorithm in the above theorem consists of two steps. First, it performs the experiment $s_i = \mathcal{M}_1 \circ \boldsymbol{\mathcal{W}}(\gamma)|0\rangle|t_i\rangle$ for each of the m elements t_i. Then, from the m pairs $(s_i, t_i) \in G \times H$, it classically deduces the value of γ on each of the n elements $g_i \in G$. That this second step is possible follows from Lemmas 8 and 12.

Lemma 12 *Let $\gamma : G \to H$ be a homomorphism of groups. Suppose the order of every element of H divides every exponent of G. Then, given a set of pairs (s_i, t_i) for which $\chi^G_{s_i} = \chi^H_{t_i} \circ \gamma$, we can uniquely determine γ if and only if the t_i's generate H.*

Proof We prove each of the two directions separately. First suppose that H is generated by the t_i's. Let g be an arbitrary element of G and set $h = \gamma(g)$. By assumption, for all i,

$$\chi^H_h(t_i) = \chi^H_{t_i}(h) = (\chi^H_{t_i} \circ \gamma)(g) = \chi^G_{s_i}(g).$$

Since the t_i's generate H, we know the value of χ_h^H on every element in its domain, and hence h is uniquely determined.[3]

For the opposite direction, suppose the t_i's only generate a proper subgroup K of H. Let $\gamma_1 : G \to H$ be any homomorphism satisfying that

$$\chi_{s_i}^G = \chi_{t_i}^H \circ \gamma_1 \quad \text{for all } i. \tag{12}$$

We now construct another homomorphism $\gamma_2 : G \to H$ also satisfying Eq. (12).

Since K is proper in H, there exist distinct elements $h_1, h_2 \in H$ such that $\chi_k^H(h_1) = \chi_k^H(h_2)$ for all $k \in K$. Let $g' \in G$ be an element of maximal order. Write $G = G_0 \oplus \langle g' \rangle$ as a direct sum of two subgroups, one of them being the subgroup generated by g'. Define the mapping $\gamma_2 : G \to H$ by setting

$$\begin{aligned} \gamma_2(g') &= \gamma_1(g') \oplus (h_1 \ominus h_2) \\ \gamma_2(g) &= \gamma_1(g) \qquad\qquad (g \in G_0) \end{aligned}$$

and extending it linearly to G. We need to show three properties of γ_2: first of all that γ_2 is well-defined, secondly that γ_2 is a homomorphism, and finally that it satisfies Eq. (12). The mapping γ_2 is well-defined since the order of every element $g \in \{g'\} \cup G_0$ is a multiple of the order of its image. By construction, the last two properties hold. □

An early result by Bernstein and Vazirani [3] can be seen as a special case of Theorem 11: Let $G = \mathbb{Z}_2^n$ and $H = \mathbb{Z}_2$. By identifying $\mathbb{Z}_2$ with the cyclic subgroup $\{1, -1\} \subset \mathbb{C}^\star$, any group homomorphism $\gamma : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is a character. Since there is a bijective correspondence between the characters and the group elements of $\mathbb{Z}_2^n$ (see Sec. 2.4), finding γ is equivalent to finding its corresponding group element. It was shown in [3] that this corresponding element $g \in \mathbb{Z}_2^n$ can be found on a quantum computer by applying γ only twice. Adding to this the idea from Lemma 5.5 in [16], this can be improved to just 1 application of γ. On the other hand, Terhal and Smolin [17] showed that any classical algorithm cannot find the element $g \in \mathbb{Z}_2^n$ with less than n evaluations of γ. Independently of our work, Cleve *et al.* [18] have proven Theorem 11 for the case when $G = \mathbb{Z}_2^n$ and $H = \mathbb{Z}_2^m$.

6 Deciding if a function is constant

One of the earliest problems considered for quantum computation is the problem of deciding constant functions: Given an arbitrary mapping $\gamma : A \to R$ of finite

[3] Not only is h uniquely determined, but it can also be found efficiently on a classical computer.

sets, determine if γ is constant or not. In his seminal paper [2], Deutsch considered the case when we are given a two-valued function $\gamma : \{0,1\} \to \{0,1\}$ of a two-valued variable, and we are to compute the bit $\pi(\gamma) = \gamma(0) \oplus \gamma(1)$ where $\oplus$ denotes the exclusive-or. He gave a quantum algorithm that uses only one evaluation of γ, and that with equal probabilities returns either $\pi(\gamma)$ or a special value denoted "fail" from which one can deduce nothing about γ. Independently, Tapp [19] and Cleve, Ekert, and Macchiavello (see reference [17] in [20]) then discovered that, still using only one evaluation of γ, there is another algorithm that always returns $\pi(\gamma)$. This is to be compared with any classical algorithm that needs two evaluations of γ to decide with certainty if γ is constant or not.

Deutsch's problem can be generalized in the following natural way. We say that a function is *perfectly balanced* if $\#(\gamma, r) = \#(\gamma, r')$ for all $r, r' \in R$. In [21], Deutsch and Jozsa showed that there is a quantum algorithm that using just two evaluations of a given function $\gamma : \mathbb{Z}_{2n} \to \mathbb{Z}_2$, either correctly concludes that it is non-constant, or correctly concludes that it is not perfectly balanced. Note that at least one of these two statements must be true. Related to this, Jozsa considered in [22] how well a quantum algorithm can determine a property π of a given function $\gamma : \mathbb{Z}_n \to \mathbb{Z}_m$ if we only allow one evaluation of γ. Further, Costantini and Smeraldi [23] analyzed how well a specific quantum algorithm correctly determines if a given function $\gamma : \{0, \ldots, n-1\} \to \{0, \ldots, m-1\}$ $(n, m \geq 2)$ is non-constant.

Both Deutsch's algorithm and its generalizations in [21, 23] can be written in the form we discussed in Sec. 1: $z_1 = \mathcal{M}_1 \circ \boldsymbol{\mathcal{V}}(\gamma)\, |0\rangle|0\rangle$ where $\gamma : G \to H$ is considered a mapping between cyclic groups. In Deutsch's algorithm, $G = H = \mathbb{Z}_2$, and in its generalization in [21], $G = \mathbb{Z}_{2n}$ and $H = \mathbb{Z}_2$, and in [23], $G = \mathbb{Z}_n$ and $H = \mathbb{Z}_m$.

We now show that hardly any structure on either the set G, or H, is needed to prove their result in an even more general form. For this, let $\gamma : A \to R$ be any mapping. For any nonempty set X, let $|X\rangle$ denote the superposition $\left(1/\sqrt{|X|}\,\right) \sum_{x \in X} |x\rangle$. Let $\mathbf{A}$ be a unitary operator on $\mathbb{C}A$ satisfying that $\mathbf{A}\,|A\rangle = |0_A\rangle$. Then the operator $\mathbf{A} \otimes \mathbf{I}$ maps $|A\rangle|r\rangle$ to the basis state $|0_A\rangle|r\rangle$ for all $r \in R$. In words, $\mathbf{A} \otimes \mathbf{I}$ maps the superposition corresponding to the constant function $\gamma = r$ to the basis vector $|0_A\rangle|r\rangle$. Intuitively, if we perform a measurement of the first register and we measure some value different from 0_A, then we know that γ is non-constant. The next theorem shows that these ideas indeed work as just described.

Theorem 13 *Let $\gamma : A \to R$ and let $\mathbf{A}$ be a unitary operator on $\mathbb{C}A$ for which $\mathbf{A}\,|A\rangle = |0_A\rangle$. Consider the experiment*

$$z = \mathcal{M}_1 \circ (\mathbf{A} \otimes \mathbf{I})\, \mathbf{U}_\gamma\, (\mathbf{A}^\dagger \otimes \mathbf{I})\, |0_A\rangle|0_R\rangle.$$

Then the probability that $z = 0$ is

$$p_1 = \frac{1}{|A|^2} \sum_{r \in R} (\#(\gamma, r))^2 \tag{13}$$

where $\#(\gamma, r)$ is the number of elements in A that are mapped to r by γ.

We omit the simple proof. The probability p_1 of measuring 0 is 1 if and only if γ is constant. At the other end, p_1 takes its minimum when γ is as balanced as possible. That is, if $\#(\gamma, r) = \#(\gamma, r') \pm 1$ for all $r, r' \in R$. Thus, p_1 is a measure for how constant γ is. Unfortunately, this minimum is never zero, but instead at least $\max\{1/|A|, 1/|R|\}$.

If we have some partial knowledge on the set R, then we can show that it is possible to improve the experiment in Theorem 13 to obtain a minimum equal to zero. Let $\mathbf{R}$ be a unitary operator on $\mathbb{C}R$ for which $\mathbf{R}|0_R\rangle = \mathbf{R}^\dagger|0_R\rangle = |R\rangle$. Suppose that the set R is endowed with an addition operation satisfying that $R + r = R$ for all elements r in the image of γ. Then the operator $\mathbf{U}_\gamma$ given by $|a\rangle|r\rangle \mapsto |a\rangle|r + \gamma(a)\rangle$ is unitary.

These assumptions are fulfilled, for example, if R has the structure of an Abelian group. They imply that the vector $|0_A\rangle|0_R\rangle$ is an eigenvector of the operator $(\mathbf{A} \otimes \mathbf{R})\, \mathbf{U}_\gamma\, (\mathbf{A}^\dagger \otimes \mathbf{R}^\dagger)$. We therefore exclude the zero state in our initial state and we obtain the following slightly better result.

Theorem 14 *Let $\gamma : A \to R$. Suppose that $\mathbf{A}\,|A\rangle = |0_A\rangle$, $\mathbf{R}\,|0_R\rangle = \mathbf{R}^\dagger\,|0_R\rangle = |R\rangle$, and that R is endowed with an addition for which $R + \gamma(a) = R$ for all $a \in A$. Consider the experiment*

$$z = \mathcal{M}_1 \circ (\mathbf{A} \otimes \mathbf{R})\, \mathbf{U}_\gamma\, (\mathbf{A}^\dagger \otimes \mathbf{R}^\dagger)\, |0_A\rangle|R \setminus \{0_R\}\rangle.$$

Then the probability that $z = 0$ is

$$p_2 = \frac{p_1|R| - 1}{|R| - 1} \tag{14}$$

where p_1 is given by Eq. (13). Furthermore, $p_2 \leq p_1$ for all γ, and this inequality is strict when $p_1 < 1$.

As mentioned above, the assumptions in Theorem 14 are satisfied if $\gamma : G \to H$, $\mathbf{A} = \mathbf{F}_G$, and $\mathbf{R} = \mathbf{F}_H$. In that case, if we perform the experiment $z = \mathcal{M}_1 \circ \boldsymbol{\mathcal{W}}(\gamma)\, |0\rangle|H\rangle$, the probability that the outcome z equals a is given by $q_a = (1/|G|^2) \sum_{h \in H} |\lambda_a(\gamma, h)|^2$. Here $\lambda_a(\gamma, h) = \sum_g \mu^G(a, g)$ where the sum is taken over all elements g in G for which $\gamma(g) = h$. If we remove the zero state from the initial state $|H\rangle$ and instead perform the experiment $z = \mathcal{M}_1 \circ \boldsymbol{\mathcal{W}}(\gamma)\, |0\rangle|H \setminus \{0\}\rangle$, then we obtain a slight change of these probabilities similar to the change from p_1 to p_2. That is, the probability to measure zero is now $(q_0|H|-1)/(|H|-1)$, while the probability to measure the nonzero element $g \in G$ is $(q_g|H|)/(|H|-1)$.

Unlike p_1, the probability p_2 takes the value 0 when the given function γ is perfectly balanced. In particular, for the special case that $A = R = \mathbb{Z}_2$, and $\mathbf{A} = \mathbf{R} = \mathbf{W}$, then we obtain the improvement of Deutsch's algorithm that we discussed in the first paragraph of this section. Here $\mathbf{W}$ denotes the Fourier transform for $\mathbb{Z}_2$, as defined in Sec. 2.2.

The probability p_1 for measuring 0 in the first register is 1 if and only if the given function $\gamma : A \to R$ is constant. If γ is constant, except for one element of the domain, then $p_1 = 1 - 2(n-1)/n^2$ where $n = |A|$. That is, with probability $2(n-1)/n^2 \approx 2/n$, we measure a nonzero value in the first register. Thus, using one evaluation of γ, we can distinguish non-constant functions from constant functions with probability at least roughly $2/n$. If we apply the experiment in Theorem 14 instead, then we improve this probability by a factor of $|R|/(|R|-1)$. This factor is worthy of consideration if (and only if) the cardinality of R is small, as, for example, in Grover's searching problem [24].

Suppose we want to distinguish non-constant functions from constant functions with probability better than roughly $2/n$. Then we can of course repeat the experiment, say, k times, giving a successprobability close to kp for small k, where p denotes either p_1 or p_2. However, since our computation is done on a quantum computer, we can show that we can improve this to approximately $(k^2/2)p$ by applying our amplitude amplification technique that will be published elsewhere.

Until now, we have interpreted the probabilities p_1 and p_2 as measures for how constant the function γ is. From the closed formulas given in the above theorems, we see that p_1 and p_2 also can be interpreted as measures for the number of collisions of γ: Suppose we pick a subset of cardinality two of A at random with respect to the uniform probability distribution. Then the probability that γ takes the same value on both elements of the subset is given by

$$\frac{p_1|A|-1}{|A|-1}.$$

In particular, if A and R have the same cardinality, then p_2 equals this probability.

Acknowledgments

I am grateful to Joan Boyar, Gilles Brassard, Ivan Damgård, and Mark Ettinger for discussions and comments. This research was carried out while I was at the Laboratoire d'informatique théorique et quantique at Université de Montréal.

References

[1] P. W. Shor, in *Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, California, 1994), p. 124. (Final version to be published in *SIAM J. Comp.*)

[2] D. Deutsch, Proc. R. Soc., London, Sect. A **400**, 97 (1985).

[3] E. Bernstein and U. Vazirani, in *Proceedings of the 25th Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, New York, 1993), p. 11. (Final version to be published in *SIAM J. Comp.*)

[4] D. R. Simon, in *Proceedings of the 35th Annual IEEE Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, California, 1994), p. 116. (Final version to be published in *SIAM J. Comp.*)

[5] C. H. Papadimitriou, *Computational Complexity* (Addison-Wesley Publishing Company, 1994).

[6] C. H. Bennett, IBM J. Res. Dev. **17**, 525 (1973).

[7] A. Barenco, Contemp. Phys. **38**, 357 (1996); A. Berthiaume, in *Complexity Theory Retrospective II*, edited by L. Hemaspaandra and A. Selman (Springer-Verlag, 1997).

[8] D. K. Maslen and D. N. Rockmore, in *Proceedings of the DIMACS Workshop in Groups and Computation—II*, 1995; J.-P. Serre, *Linear representations of finite groups* (Springer-Verlag, 1977), Graduate texts in mathematics, Vol. 42.

[9] M. J. Hadamard, Bull. Sci. Math. **17**, 240 (1893); M. J. L. Walsh, Am. J. Math. **45**, 5 (1923).

[10] G. Brassard and P. Høyer, in *Proceedings of Fifth Israeli Symposium on Theory of Computing and Systems* (IEEE Computer Society Press, California), 1997, p. 12.

[11] D. Boneh and R. J. Lipton, in *Proceedings of Advances in Cryptology* (Springer-Verlag, 1995), Lecture Notes of Computer Science, Vol. 963, p. 424.

[12] D. Yu. Grigoriev, J. Math. Sci. **82** (1996).

[13] A. Yu. Kitaev, Report No. quant-ph/9511026.

[14] G. Brassard and P. Høyer, Report No. quant-ph/9612017.

[15] R. Beals (unpublished).

[16] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[17] B. M. Terhal and J. A. Smolin, Report No. quant-ph/9705041.

[18] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Report No. quant-ph/9708016.

[19] A. Tapp (private communication through G. Brassard).

[20] A. Ekert, Report No. quant-ph/9703035.

[21] D. Deutsch and R. Jozsa, Proc. R. Soc., London, Sect. A **439**, 553 (1992).

[22] R. Jozsa, Proc. R. Soc., London, Sect. A **435**, 563 (1991).

[23] G. Costantini and F. Smeraldi, Report No. quant-ph/9702020.

[24] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).