Malaysian Journal of Mathematical Sciences 3(2): 135-146 (2009)

Control-Target Inversion Property on Abelian Groups

Massoud Amini
Department of Mathematics,
Tarbiat Modares University, B.O.Box 14115-175, Tehran, Iran
and Institute for Mathematical Research,
Universiti Putra Malaysia, 43400 UPM Serdang,
Selangor,Malaysia
E-mail: amini@modares.ac.ir,massoud@putra.upm.edu.my

ABSTRACT

We show that the quantum Fourier transform on finite fields used to solve query problems is a special case of the usual quantum Fourier transform on finite Abelian groups. We show that the control-target inversion property holds in general. We apply this to get a sharp query complexity separation between classical and quantum algorithms for a hidden homomorphism problem on finite Abelian groups.

Keywords: Quantum Fourier transform, inversion property, hidden homomorphism problem.

INTRODUCTION

One of the models which is used in checking the outperformance of quantum algorithms versus classical algorithms is the query model. In this model, the input can only be accessed by means queries to a black box. Efficiency of computation then is measured by the number of required queries. A famous example of query algorithm is Grover's algorithm (see Grover,(1998)) for searching a list of n elements with $O\left(\sqrt{n}\right)$quantum queries.

In query complexity computation, one usually tries to find efficient quantum algorithms as well as lower bounds on the number of queries that any quantum or classical algorithm needs. This lower bound or exact or bounded-error classical algorithms is used to check the outperformance of a given efficient quantum algorithm over all possible classical counterparts. Probably the first instance of a significant

Outperformance was demonstrated in the Deutsch algorithm appeared in Deutsch,(1985), extended by Deutsch and Jozsa in Deutsch-Jozsa,(1992). The later solves an $(n+1)-bit$ query problem using one query by a quantum algorithm with a lower bound of $\Omega(2n)$ queries in exact classical solutions. Although it turned out later that this problem could be solved using $0(1)$ queries with a bounded-error classical algorithm, the same query complexity separation has shown to exist between quantum and bounded-error classical algorithms, see Bernstein-Vazirani,(1997). This kind of separation has been pushed further in de Beaudrap *et al.*,(2000) in which a $2n$-query problem is presented that is solved by a quantum algorithm using one query and has a lower bound of $\Omega\left(2^{n/2}\right)$ in any bounded-error classical solution. The problem discussed in de Beaudrap *et al.,*(2000) is called the *hidden linear structure problem* and is defined on a finite field $\mathrm{GF}\left(2^n\right)$ (identified with $\{0,1\}^n$) as follows

Hidden Linear Structure Problem. *Let π be a permutation on* $GF(2^n)$ *and* $s \in GF(2^n)$. *Define a black box* B_s *on* $GF(2^n)\times GF(2^n)$ *by*

$$B_s(x,y) = (x, \pi(y+sx)).$$

Determine the value of s.

The quantum algorithm in de Beaudrap *et al.,*(2000) is based on a version of the quantum Fourier transform (QFT) on finite fields (a similar operation is used in van Dam-Hallgren,(2000) to solve a shifted quadratic character problem). The argument in de Beaudrap *et al.,*(2000) then proceeds using a control-target inversion property of the QFT. This is an intertwining property involving two linear operators defined by algebraic operations involving *s*.

In this paper we show that this is nothing but the usual quantum Fourier transform on the Abelian group $(GF(q),+)$ with respect to a special choice of the Fourier basis. Then we show that the control-target inversion property holds for a wide class of group homomorphisms on general finite Abelian groups. We use this to show that there is a sharp query complexity separation between the bounded-error classical and exact quantum algorithms in solving a generalization of the linear structure problem in the context of Abelian groups. This problem could be called a *hidden homomorphism problem* and is stated as follows.

Let G be a finite (additive) Abelian group and fix a Fourier basis Λ for the group algebra $\mathbb{C}G$, let $Hom_\Lambda(G,G)$ be the set of all group homomorphisms on G which are compatible with λ (see section 2 for details), then the problem is

Hidden Group Homomorphism Problem. *Let* π *be a permutation on* G*,* $a \in G$*, and* $\psi \in Hom_{\Lambda}(G,G)$*. Define a black box* B_{ψ} *on* $G \times G$ *by*

$$B_{\psi}(x, y) = (x, \pi(y + \psi(x))).$$

Determine the value of $\psi(a)$*.*

When $G = (GF(q),+), a = 1$ and $\psi(x) = sx$, this problem reduces to the hidden structure problem.

In section 2 we review the QFT on finite Abelian groups. Our basic reference is Jozsa,(1998). In section 3 we prove the control-target inversion property on groups. Section 4 is devoted to the quantum solution of the hidden group homomorphism problem and corresponding classical lower bounds. In this section we present a variation of the control-target inversion property which leads to another generalization of the results of de Beaudrap *et al.*,(2000) to non commutative rings.

QUANTUM FOURIER TRANSFORM ON ABELIAN GROUPS

Let G be a finite Abelian group. To emphasize that our group is Abelian, we use the addition as the group operation (this also helps to avoid any confusion when we later deal with the additive group of a finite field). Let H be a Hilbert space with the orthonormal basis $\{|x\rangle : x \in G\}$, called the standard basis of H. Indeed the group algebra $\mathbb{C}G$ is a candidate for this Hilbert space. There is a natural action of G on H by translation

$$x : |y\rangle \rightarrow |x + y\rangle \ (x, y \in G).$$

A character on G is a nonzero group homomorphism $\chi : G \rightarrow \mathbb{T}$ where $\mathbb{T}$ is the multiplicative group of the complex numbers of modulus 1. As each $x \in G$ has an order dividing $n := |G|$, the values $\chi(x)$ are n^{th} roots of unity. The set $\hat{G}$ of all characters on G is an Abelian group with respect to the point wise multiplication and is called the dual group of G. It is well known that $|\hat{G}|=|G|=n$, and if $\hat{G} = \{\chi_1,\ldots,\chi_n\}$ then we have the Schur's orthogonality relations

$$\tfrac{1}{|G|}\sum_{x\in G}\chi_i(x)\chi_j(-x)=\delta_{ij},$$

for each $1\le i,j\le n$.

We prefer to index the elements of $\hat{G}$ by elements of G, so we write $\hat{G}=\{\chi_x: x\in G\}$. For each $x\in G$ consider the state

$$|\chi_x\rangle=\sum_{y\in G}\chi_x(-y)|y\rangle,$$

then the above orthogonality relations imply that $\{|\chi_x\rangle : x\in G\}$ forms an orthonormal basis for *H*, called the *Fourier basis* of *H*. This basis is translation invariant in the sense that

$$x|\chi_x\rangle=\chi_y(x)|\chi_y\rangle \quad (x,y\in G).$$

Also we may always assume that $\chi_x\chi_y=\chi_{x+y}$ and $\chi_0=1$. Let $\psi: G\to G$ be a group homomorphism. We say that ψ is compatible with the Fourier basis of G if

$$\chi_y(\psi(z))=\chi_{\psi(x)}(z) \quad (y,z\in G).$$

Given a Fourier basis Λ (that is a given choice of the indexing Ĝ with *G*) we denote the set of all homomorphisms ψ of G compatible with Λ by $Hom_\Lambda(G,G)$. On any finite Abelian group G we have a family of such homomorphisms constructed using the structure theorem for G. Every finite Abelian group G is iso$G$orphic to the Cartesian product of cyclic groups, say $G=\prod_{1\le j\le k}\mathbb{Z}_{m_j}$. For each $x=(x_1,\ldots,x_k)\in G$ with $x_j\in\mathbb{Z}_{m_j}$, we have the character

$$\chi_x(y)=\prod_{1\le j\le k}\omega_j^{x_j y_j} \quad (y=(y_1,\ldots,y_k)\in G)$$

where $\omega_j=e^{\frac{2\pi i}{m_j}}$ and the product $x_j y_j$ is calculated (mod m_j). Then $\Lambda=\{\chi_x : x\in G\}$ is a Fourier basis and for each $s=(s_1,\ldots,s_k)\in G$ defines a homomorphism ψ_s by

$$\psi_s(y)=(s_1y_1,\ldots,s_ky_k) \quad (y=(y_1,\ldots,y_k)\in G)$$

which is clearly compatible with Λ. Here again the products $s_j y_j$ are defined (mod m_j). The quantum Fourier transform[1] on G is the unitary operator $F_G : H \to H$ defined by

$$\left|x\right\rangle \mapsto \tfrac{1}{\sqrt{|G|}} \sum\nolimits_{y \in G} \chi_x(y) \left|y\right\rangle \quad (x, y \in G) .$$

Note that one can extend this map by linearity on H and the fact that it is unitary follows from Pontryagin duality for Abelian groups, see Jozsa, (1998). Two classical examples are $G = \mathbb{Z}_m$ where

$$\chi_k(\ell) = e^{\frac{2\pi ik}{m}}, \; k, \ell = 0, \ldots, m-1$$

and $G = \{0,1\}^n$ where

$$\chi_x(y) = (-1)^{xy} \quad (x, y \in \{0,1\}^n)$$

in which F_G is the usual discrete Fourier transform DFT_m on $\mathbb{Z}_m$ and the Hadamard transform H_n, respectively. Another example would be the additive group of any finite field GF(q), which is discussed in details in the next section.

MAIN RESULT

Let G be an (additive) Abelian group and $H = \mathbb{C}G$. Let Λ be a Fourier basis for H. To each homomorphism $\psi \in Hom_\Lambda(G, G)$, there correspond two operators on $H \otimes H$ defined by

$$A_\psi : \left|x\right\rangle \left|y\right\rangle \mapsto \left|x\right\rangle \left|y + \psi(x)\right\rangle$$
$$B_\psi : \left|x\right\rangle \left|y\right\rangle \mapsto \left|x + \psi(y)\right\rangle \left|y\right\rangle$$

We say that a unitary operator U on H satisfies the *control-target inversion property* at ψ if

$$\left(U^\dagger \otimes U\right) A_\psi \left(U \otimes U^\dagger\right) = B_\psi .$$

[1] This is the classical (discrete) Fourier transform, but we call it quantum Fourier transform, as this is nowadays the standard convention of all the articles on Quantum Computation.

Theorem 1 (Main Result). *Let G be a finite Abelian group and* ψ *be a group homomorphism on G. Choose a Fourier basis* Λ *of H=* $\mathbb{C}G$*, then for each* $\psi \in Hom_{\Lambda}(G,G)$*, the quantum Fourier transform* F_G *satisfies the control-target inversion property at* ψ.

Proof. Let $n = |G|$, for $x \in G$ put

$$\left|F_x\right\rangle = F_G\left|x\right\rangle = \tfrac{1}{\sqrt{n}}\sum_{y\in G}\chi_x(y)\left|x\right\rangle$$

and $P_x\left|y\right\rangle = \left|x+y\right\rangle$. Then

$$\begin{aligned} P_y\left|F_x\right\rangle &= \tfrac{1}{\sqrt{n}}\sum_{z\in G}\chi_{-x}(z)\left|y+z\right\rangle \\ &= \tfrac{1}{\sqrt{n}}\sum_{z\in G}\chi_{-x}(z-y)\left|y+z\right\rangle \\ &= \tfrac{1}{\sqrt{n}}\sum_{z\in G}\chi_{-x}(-y)\left|y+z\right\rangle \\ &= \chi_{-x}(-y)\left|F_{-x}\right\rangle = \chi_x(y)\left|F_{-x}\right\rangle \end{aligned}$$

Therefore

$$\begin{aligned} (F^{\dagger}{}_G \otimes F_G)A_{\psi}(F_G \otimes F^{\dagger}{}_G)\left|x\right\rangle\left|y\right\rangle &= (F^{\dagger}{}_G \otimes F_G)A_{\psi}\left(\tfrac{1}{\sqrt{n}}\sum_{z\in G}\chi_x(z)\left|z\right\rangle\left|F_{-y}\right\rangle\right) \\ &= (F^{\dagger}{}_G \otimes F_G)A_{\psi}\left(\tfrac{1}{\sqrt{n}}\sum_{z\in G}\chi_x(z)\left|z\right\rangle P_{\psi(z)}\left|F_{-y}\right\rangle\right) \\ &= (F^{\dagger}{}_G \otimes F_G)A_{\psi}\left(\tfrac{1}{\sqrt{n}}\sum_{z\in G}\chi_x(z)\left|z\right\rangle \chi_y(\psi(z))\left|F_{-y}\right\rangle\right) \\ &= (F^{\dagger}{}_G \otimes F_G)A_{\psi}\left(\tfrac{1}{\sqrt{n}}\sum_{z\in G}\chi_x(z)\chi_{\psi(y)}(z)\left|z\right\rangle\left|F_{-y}\right\rangle\right) \\ &= (F^{\dagger}{}_G \otimes F_G)A_{\psi}\left(\tfrac{1}{\sqrt{n}}\sum_{z\in G}\chi_{x+\psi(y)}(z)\left|z\right\rangle\left|F_{-y}\right\rangle\right) \\ &= (F^{\dagger}{}_G \otimes F_G)A_{\psi}\left(\left|F_{x+\psi(y)}(z)\right\rangle\left|F_{-y}\right\rangle\right) \\ &= \left|x+\psi(y)\right\rangle\left|y\right\rangle = B_{\psi}\left|x\right\rangle\left|y\right\rangle. QED \end{aligned}$$

As a basic example let us consider the main example of de Beaudrap et al. (2000). Let $GF(q)$ be the finite field with $q = p^m$ elements and fix an irreducible polynomial $f(Z) = Z^m - \sum_{i=0}^{m-1} a_i Z^i$ over $GF(p)$, and let $\langle f \rangle$ be the ideal generated by *f*, then

$$GF(q) \simeq GF(p)[\mathrm{Z}]/\langle f \rangle$$

Fix a nonzero linear map $\varphi: GF(q) \rightarrow GF(p)$ and define the quantum Fourier transform

$F_{q,\varphi}: CGF(q) \rightarrow CGF(q)$ by

$$F_{q,\varphi}: |x\rangle \mapsto \tfrac{1}{\sqrt{q}} \sum_{y \in GF(q)} e^{\frac{2\pi i \varphi(xy)}{p}} |y\rangle$$

extended by linearity. Then the additive group $G := (GF(q), +)$ is an Abelian group and for each $x \in G$

$$\chi_x(y) = e^{\frac{2\pi\varphi(xy)}{p}} \qquad (y \in G)$$

defines a character on G. Also we have the orthogonality relations

$$\tfrac{1}{q} \sum_{x \in GF(q)} \chi_y(x)\chi_z(-x) = \tfrac{1}{q} \sum_{x \in GF(q)} e^{\frac{2\pi\varphi(x(y-z))}{p}} = \delta_{yz}$$

(see the proof of [BCW,Theorem1]). Also if $\chi_x = \chi_v$ then $e^{\frac{2\pi\varphi(xz)}{p}} = e^{\frac{2\pi\varphi(yz)}{p}}$, for each $z \in G$. Since the range of φ is in $GF(p) = \mathbb{Z}_p$ and the analytic map $\omega \mapsto \exp(\omega)$ is one-to-one in the strip $\{\omega \in C : 0 \leq Im(\omega) < 2\pi\}$, we get $\varphi(xz) = \varphi(yz)$, for each $z \in G$. If $x = y$, then we have q distinct elements $z(x-y)$ in $\ker(\varphi)$, which means that $ker(\varphi) = G$, i.e. $\varphi = 0$, which is a contradiction. Hence $x = y$, that is $\{\chi_x : x \in G\}$ is a complete set of Fourier basis elements for G. Now it is clear that, with respect to this basis, $F_G = F_{q,\varphi}$. Next let $s \in G$ be any nonzero element and define $\psi_s(x) = sx (x \in G)$. This is clearly a group homomorphism of G which is compatible with the above Fourier basis, namely

$$\begin{aligned} \chi_{\psi s}(y)(z) &= \exp(2\pi\varphi((sy)z)/p) = \exp(2\pi\varphi((sz)y)/p) \\ &= \exp(2\pi i\varphi(\psi_s(z)y)/p) = \exp(2\pi i\varphi(y\psi_s(z))/p) = \chi_y(\psi_s(z)) \end{aligned}$$

In particular, Theorem 1 of (de Beaudrap *et al.*, 2000) is a special case of our main theorem. Also note that for the additive group G of a commutative ring all the above observations are valid except that $\{x_x : x \in G\}$ is not necessarily a complete set of Fourier basis elements for G (we need commutativity of the ring in the second equality of the second line of the above calculation to show that ψ_s is compatible with the Fourier basis).

In the last section of de Beaudrap *et al*.,(2000) there is a version of the control-target inversion property for the ring of $m\times m$ matrices over a commutative ring *R*. This is again a special case of a minor modification of the above theorem. Consider a pair (ψ,φ) of homomorphisms of *G* such that $\psi\circ\varphi=\varphi\circ\psi$ .We say that (ψ,φ) is compatible with a given Fourier basis Λ of *G* if

$$\chi_y(\psi(z))=\chi_{\varphi(y)}(z) \qquad (y,z\in G).$$

We denote the set of all such pairs by $Hom_{\Lambda,\Lambda}(G,G)$. We say that a unitary operator *U* on *H* satisfies the control-target inversion property at (ψ,ϕ) if

$$(U^{\dagger}\otimes U)A_{\psi}(U\otimes U^{\dagger})=B_{\varphi}.$$

Then a slight modification of the proof of Theorem 1 shows that

Theorem 2. *Let G be a finite Abelian group and choose a Fourier basis* Λ *of H=* $\mathbb{C}G$*, then for each* $(\psi,\varphi)\in Hom_{\Lambda\Lambda}(G,G)$, *the quantum Fourier transform* F_G *satisfies the control-target inversion property at* (ψ,φ). QED

Now in section 4 of de Beaudrap *et al.,* (2000), we are dealing with a ring *R* with QFT F_R for which a QFT $F_{R,m}$ is defined on the ring $R^{m\times m}$ of $m\times m$ matrices over *R* via tensor product. It is clear that if F_R is the QFT on the additive group $G=(R,+)$, then $F_{R,m}$ is the QFT on the product group $G^m\times G^m$ (which is the additive group of the ring $R^{m\times m}$). The two group homomorphisms of $G^m\times G^m$ are then $\psi(X)=SX$ and $\varphi(X)=XS(X\in R^{m\times m})$, where S is an element of $R^{m\times m}$. Now with the natural choice of the Fourier basis for $G=(R,+)$ we would have

$$\chi_y(sz)=\chi_{ys}(z) \qquad (s,y,z\in R)$$

Define the Fourier basis of $G^m \times G^m$ by

$$\chi_Y(Z) = \prod_{j,j=1}^{m} \chi_{y_{ij}}(z_{ji}) \quad (Y = [y_{ij}], Z = [z_{ij}] \in R^{m\times m}).$$

Then for each $S, Y, Z \in R^{m\times m}$, we have

$$\begin{aligned}\chi_Y(SZ) &= \prod_{i,j=1}^{m} \chi_{y_{ij}}\left((SZ)_{ji}\right) = \prod_{i,j=1}^{m} \chi_{y_{ij}}\left(\sum_{i,j=1}^{m} s_{jk} z_{ki}\right) \\ &= \prod_{i,j=1}^{m} \chi_{y_{ij}}(s_{jk} z_{ki}) = \prod_{i,j=1}^{m} \chi_{y_{ij}s_{jk}}(z_{ki}) \\ &= \prod_{i,j=1}^{m} \chi_{\cdot \sum_{j=1}^{m} y_{ij}s_{jk}}(z_{ki}) = \prod_{i,j=1}^{m} \chi_{\cdot (YS)_{ik}}\left((Z_{ki})\right) = \chi_{YS}(Z).\end{aligned}$$

Therefore the control-target inversion property presented in section 4 of de Beaudrap *et al.*, (2000) follows from Theorem 2 above.

THE HIDDEN HOMOMORPHISM PROBLEM

For a finite (additive) Abelian group G let $a \in G$ be a fixed element (usually the generator of G, when G is cyclic), π be an arbitrary permutation of elements of G, and for a fixed Fourier basis $\Lambda := \{\chi_x : x \in G\}$ of $H = \mathbb{C}G$, let $\psi \in Hom_\Lambda(G, G)$ be a homomorphism of G compatible with Λ, then the hidden homomorphism problem on G is as follows.

Hidden homomorphism problem. *Given a black-box performing the unitary transformation that map* $|x\rangle|y\rangle$ *to* $|x\rangle|\pi(y + \psi(a))\rangle$, *find* $\psi(a)$.

In this section we show that, using the QFT, a single query is sufficient to solve the problem exactly, whereas in the classical case, even for cyclic groups, $\Omega\left(|G|^{\frac{1}{2}}\right)$ queries are needed to solve the problem with bounded error.

Theorem 3. *On any finite Abelian group G, performing* F_G *and* $F^{\dagger}_{G,}$ *a single query is sufficient to solve the hidden homomorphism problem exactly.*

Proof. Consider the unitary transformation

$$U_{\pi} : |y\rangle \mapsto |\pi(y)\rangle$$

implementing π, and recall that

$$A_{\psi} : |x\rangle|y\rangle \mapsto |x\rangle|y+\psi(x)\rangle,$$

then the black-box is implemented by

$$U_{\pi,\psi} = (I \otimes U_{\pi})A_{\psi} : |x\rangle|y\rangle \mapsto |x\rangle|\pi(y+\psi(x))\rangle.$$

To perform the quantum procedure, first initialize state of the two G-valued registers to $|0\rangle|a\rangle$, where 0 is the identity of G, then perform the following consecutive operations: apply $F_G \otimes F_G^{\dagger}$ then query the black-box and apply $F_G^{\dagger} \otimes F_G$. Finally measure the first register. The states of the two registers during the execution of this algorithm are as follows:

$$\begin{aligned}
|0\rangle|a\rangle &\xrightarrow{F_G^{\dagger}\otimes F_G} F_G|0\rangle F_G^{\dagger}|a\rangle \xrightarrow{U_{\pi\psi}} (I\otimes U_{\pi})A_{\psi}(F_G\otimes F_G^{\dagger})|0\rangle|a\rangle \\
&= (I\otimes U_{\pi})(F_G\otimes F_G^{\dagger})|0\rangle|a\rangle = (I\otimes U_{\pi})(F_G\otimes F_G^{\dagger})|\psi(a)\rangle|a\rangle \\
&= F_G|\psi(a)\rangle U_{\pi}F_G^{\dagger}|a\rangle \xrightarrow{F_G^{\dagger}\otimes F_G} |\psi(a)\rangle(F_G U_{\pi} F_G^{\dagger})|a\rangle.
\end{aligned}$$

Now measuring the first register gives $|\psi(a)\rangle$. QED

Theorem 4. *On any finite cyclic group* G *of prime order,* $\Omega\left(|G|^{\frac{1}{2}}\right)$ *queries are necessary to solve the hidden homomorphism problem within probability error* $\frac{1}{2}$.

Proof. By an argument similar to Theorem 3 in de Beaudrap *et al.,*(2000) we may use deterministic algorithms with probabilistic input data (here we put $a=1$, the generator of G). Set $\psi \in Hom(G,G)$ and π randomly with uniform distribution. After k (distinct) queries $(x_1, y_1),...,(x_k, y_k)$, if there are two indecies $i \neq j$ such that $\pi(y_i+\psi(x_i)) = \pi(y_j+\psi(x_j))$, then, as π is one-to-one, $y_i - y_j = \psi(x_j - x_i) = (x_j - x_i)\psi(1)$, and $\psi(1)$ is uniquely determined, otherwise we have $|G| - k(k-1)/2$ possibilities for $\psi(1)$ which are equally likely. A simple argument shows that the probability of a collision occurring at the k^{th} query is at most $\frac{k-1}{|G|-(k-1)(k-2)/2}$. Therefore the probability of a collision occurring in the first m queries is bounded above by

$$\sum_{k=1}^{m} \frac{k-1}{|G|-(k-1)(k-2)/2}$$

which is no bigger than $\sum_{k=1}^{m} \frac{2k}{2|G|-k^2} \leq \sum_{k=1}^{m} \frac{m^2}{2|G|-m^2}$, and this being at least $\frac{1}{2}$,

we get $m \geq \left(\frac{2}{3}|G|\right)^{\frac{1}{2}}$. QED

ACKNOWLEDGMENTS

This research was done while I was visiting *University of Calgary*, I would like to thank the Department of Mathematics and Statistics in U of C for their support. I am grateful to Professor *Richard Cleve*, for introducing me to this problem.

REFERENCES

Bernstein, E. and Vazirani, U. 1997. Quantum complexity theory, *SIAM Journal of Computing*, **26**(5):1411-1473.

de Beaudrap, J.N., Cleve, R. and Watrous, J. Sharp quantum versus classical query complexity separations, *arXive:quant-ph/0011065*.

Deutsch, D. 1985. Quantum theory, the Church-Turing principle and the universal quantum computer, *Proc. Roy. Soc. London Series A*, **400**:97-117.

Deutsch, D. and Jozsa, R. 1992. Rapid solution of problems by quantum computation, *Proc. Roy. Soc. London, ser. A*, **439**:553-558.

Grover, L.K. 1996. A fast quantum mechanical algorithm for database search, *Proceedings of 28th STOC*, 212-219, also available online at *arXive:quant-ph*/9605043.

Jozsa, R. 1998. Quantum algorithms and the Fourier transform, quantum coherence and decoherence, *Roy. Soc. London Proc. Series A*, **454**(1969): 323-332, also available online at *arXiv:quant-ph*/97033.

van Dam, W. and Hallgren, S. Efficient quantum algorithms for shifted quadratic character problems, *arXive:quant-ph/0011067*.