Suppose that a quantum circuit with $K$ elementary gates is known for a unitary matrix $U$, and assume that $U^m$ is a scalar matrix for some positive integer $m$. We show that a function of $U$ can be realized on a quantum computer with at most $O(mK + m^2 \log m)$ elementary gates. The functions of $U$ are realized by a generic quantum circuit, which has a particularly simple structure. Among other results, we obtain efficient circuits for the fractional Fourier transform.

PACS numbers: 03.67.Lx

Let $U$ be a unitary matrix, $U \in U(2^n)$. Suppose that a fast quantum algorithm is known for $U$, which is given by a factorization of the form

$$U = U_1 U_2 \cdots U_K,$$

where the unitary matrices $U_i$ are realized by controlled-not gates or by single qubit gates [1]. We are interested in the following question:

Are there efficient quantum algorithms for unitary matrices, which are functions of $U$?

The question is puzzling, because the knowledge of the factorization of $U$ does not seem to be of much help in finding similar factorizations for, say, $V = U^{1/3}$. The purpose of this letter is to give an answer to the above question for a wide range of unitary matrices $U$.

Our solution to this problem is based on a generic circuit which implements arbitrary functions of $U$, assuming that $U^m$ is a scalar matrix for some positive integer $m$. If $m$ is small, then our method provides an efficient quantum circuit for $V$.

Notations. We denote by $U(m)$ the group of unitary $m \times m$ matrices, by $I$ the identity matrix, and by $C$ the field of complex numbers.

I. PRELIMINARIES

We recall some standard material on matrix functions, see [2, 3, 4] for more details. Let $U$ be a unitary matrix. The spectral theorem states that $U$ is unitarily equivalent to a diagonal matrix $D$, that is, $U = TDT^{-1}$ for some unitary matrix $T$. The elements $\lambda_i$ on the diagonal of $D = \text{diag}(\lambda_1, \ldots, \lambda_{2^n})$ are the eigenvalues of $U$.

Let $f$ be any function of complex scalars such that its domain contains the eigenvalues $\lambda_i$, $1 \leq i \leq 2^n$. The matrix function $f(U)$ is then defined by

$$f(U) = T\text{diag}(f(\lambda_1), \ldots, f(\lambda_{2^n}))T^{-1},$$

where $T$ denotes the diagonalizing matrix of $U$, as above.

Notice that any two scalar functions $f$ and $g$, which take the same values on the spectrum of $U$, yield the same matrix value $f(U) = g(U)$. In particular, one can find an interpolation polynomial $g$, which takes the same values as $f$ on the eigenvalues $\lambda_i$. It is possible to assume that the degree of $g$ is smaller than the degree of the minimal polynomial of $U$. In other words, $V = f(U)$ can be expressed by a linear combination of integral powers of the matrix $U$,

$$V = f(U) = \sum_{i=0}^{m-1} \alpha_i U^i,$$

where $m$ is the degree of the minimal polynomial of the matrix $U$, and $\alpha_i \in C$ for $i = 0, \ldots, m-1$. In order for $V$ to be unitary, it is necessary and sufficient that the function $f$ maps the eigenvalues $\lambda_i$ of $U$ to elements on the unit circle.

Remark. There exist several different definitions for matrix functions. The relationship between these definitions is discussed in detail in [5]. We have chosen the most general definition that allows to express the function values by polynomials.

II. THE GENERIC CIRCUIT

Let $U$ be a unitary $2^n \times 2^n$ matrix with minimal polynomial of degree $m$. We assume that an efficient quantum circuit is known for $U$. How can we go about implementing the linear combination $V$? We will use an ancillary system of $\mu$ quantum bits, where $\mu$ is chosen such that $2^{\mu-1} < m \leq 2^\mu$ holds. This will allow us to create the linear combination by manipulating somewhat larger matrices, which on input $|0\rangle \otimes |\psi\rangle \in C^{2^\mu} \otimes C^2$ produce the state $|0\rangle \otimes V |\psi\rangle$. 

*Electronic address: klappi@cs.tamu.edu
† Research partly supported by NSF grant EIA 0218582, and a Texas A&M TITF grant.
‡Electronic address: roettele@ira.uka.de
§Research supported by EC grant IST-1999-10596 (Q-ACTA).
We first bring the ancillary system into a superposition of the first \( m \) computational base states, such that an input state \( |0\rangle \otimes |\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^{2^m} \) is mapped to the state
\[
\frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \otimes |\psi\rangle.
\]

This can be done by acting with a \( 2^m \times 2^m \) unitary matrix \( B \) on the ancillary system, where the first column of \( B \) is of the form \( 1/\sqrt{m}(1, \ldots, 1, 0, \ldots, 0)^T \). Efficient implementations of \( B \) exist.

Notice that there exists an efficient implementation of the block diagonal matrix \( A = \text{diag}(1, U, U^2, \ldots, U^{2^m-1}) \). Indeed, \( A \) can be composed of the matrices \( U^i \), \( 0 \leq \eta < \mu \), conditioned on the \( \mu \) ancillae bits. The resulting implementation is shown in Fig. 1. The state (3) is transformed by this circuit into the state
\[
\frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \otimes U^i |\psi\rangle.
\]

In the next step, we let a \( 2^\mu \times 2^\mu \) matrix \( M \) act on the ancillae bits. We choose \( M \) such that the state (3) is mapped to
\[
\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle \otimes U^k V |\psi\rangle.
\]

It turns out that \( M \) can be realized by a unitary matrix, assuming that the minimal polynomial of \( U \) is of the form \( x^m - \tau, \tau \in \mathbb{C} \). This will be explained in some detail in the next section.

We apply the inverse \( A^\dagger \) of the block diagonal matrix \( A \). This transforms the state (5) to
\[
\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle \otimes V |\psi\rangle.
\]

We can clean up the ancillae bits by applying the \( 2^\mu \times 2^\mu \) matrix \( B^\dagger \). This yields then the output state
\[
|0\rangle \otimes V |\psi\rangle = |0\rangle \otimes f(U) |\psi\rangle.
\]

The following theorem gives an upper bound on the complexity of the method. We use the number of elementary gates (that is, the number of single qubit gates and controlled-not gates) as a measure of complexity.

**Theorem 1** Let \( U \) be a \( 2^n \times 2^n \) unitary matrix with minimal polynomial \( x^m - \tau, \tau \in \mathbb{C} \). Suppose that there exists a quantum algorithm for \( U \) using \( K \) elementary gates. Then a unitary matrix \( V = f(U) \) can be realized with at most \( O(mK + m^2 \log m) \) elementary operations.

**Proof.** A matrix acting on \( \mu \in O(\log m) \) qubits can be realized with at most \( O(m^2 \log m) \) elementary operations, cf. [6]. Therefore, the matrices \( B, B^\dagger, \) and \( M \) can be realized with a total of at most \( O(3m^2 \log m) \) operations.

If \( K \) operations are needed to implement \( U \), then at most \( 14K \) operations are needed to implement \( \Lambda_1(U) \), the operation \( U \) controlled by a single qubit. The reason is that a doubly controlled NOT gate can be implemented with 14 elementary gates [8], and a controlled single qubit gate can be implemented with six or fewer elementary gates [9].

We observe that \( 2^\mu - 1 \) copies of \( \Lambda_1(U) \) suffice to implement \( A \). Indeed, we can implement \( \Lambda_1(U^2) \) by a sequence of \( 2^k \) circuits \( \Lambda_1(U) \). This bold implementation yields the estimate for \( A \). Typically, we will be able to find much more efficient implementations. Anyway, we can conclude that \( A \) and \( A^\dagger \) can both be implemented by at most \( 14(2^m - 1)K \in O(14mK) \) operations. Combining our counts yields the result. \( \square \)

### III. Unitarity of the Matrix \( M \)

It remains to show that the state (6) can be transformed into the state (3) by acting with a unitary matrix \( M \) on the system of \( \mu \) ancillae qubits. This is the crucial step in the previously described method.

Let \( U \) be a unitary matrix with a minimal polynomial of degree \( m \). A unitary matrix \( V = f(U) \) can then be represented by a linear combination
\[
V = \sum_{i=0}^{m-1} \alpha_i U^i.
\]
We will motivate the construction of the matrix $M$ by examining in some detail the resulting linear combinations of the matrices $U^k V$. From (8), we obtain

$$U^k V = \sum_{i=0}^{m-1} \alpha_i U^{i+k}. \quad (9)$$

Suppose that the minimal polynomial of $U$ is of the form $m(x) = x^m - g(x)$, with $g(x) = \sum_{i=0}^{m-1} g_i x^i$. The right hand side of (3) can be reduced to a polynomial in $U$ of degree less than $m$ using the relation $U^m = g(U)$:

$$U^k V = \sum_{i=0}^{m-1} \beta_{ki} U^i.$$

The coefficients $\beta_{ki}$ are explicitly given by

$$(\beta_{k0}, \beta_{k1}, \ldots, \beta_{k(m-1)}) = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) P^k$$

where $P$ denotes the companion matrix of $m(x)$, that is,

$$P = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_0 & g_1 & g_2 & \cdots & g_{m-1} \end{pmatrix}.$$

The $2^\mu \times 2^\mu$ matrix $M$ is defined by

$$M = \begin{pmatrix} C & 0 \\ 0 & 1 \end{pmatrix},$$

where $C = (\beta_{ki})_{k,i=0,\ldots,m-1}$, and 1 is a $(2^\mu \times 2^\mu)$ identity matrix. Under the assumptions of Theorem 1, it turns out that the matrix $M$ is unitary. Before proving this claim, let us formally check that the matrix $M$ transforms the state (4) into the state (5). If we apply the matrix $M$ to the ancillary system, then we obtain from (4) the state

$$\frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} M |i\rangle \otimes U^i |\psi\rangle = \frac{1}{\sqrt{m}} \sum_{k,i=0}^{m-1} \beta_{ki} |k\rangle \otimes U^i |\psi\rangle$$

$$= \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle \otimes \sum_{i=0}^{m-1} \beta_{ki} U^i |\psi\rangle$$

$$= \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle \otimes U^k V |\psi\rangle$$

which coincides with (5), as claimed.

**Lemma 2** Let $U$ be a unitary matrix with minimal polynomial $m(x) = x^m - \tau$. Let $V$ be a matrix satisfying (4). If $V$ is unitary, then $M$ is unitary.

**Proof.** It suffices to show that the matrix $C$ is unitary. Notice that the assumption on the minimal polynomial $m(x)$ implies that $C$ is of the form

$$C = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{m-2} & \alpha_{m-1} \\ \tau \alpha_{m-1} & \alpha_0 & \cdots & \alpha_{m-3} & \alpha_{m-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \tau \alpha_1 & \tau \alpha_2 & \cdots & \tau \alpha_{m-1} & \alpha_0 \end{pmatrix},$$

that is, $C$ is obtained from a circulant matrix by multiplying every entry below the diagonal by $\tau$. In other words, we have

$$C = \left( [\tau]_{i>j} \alpha_{j-i \bmod m} \right)_{i,j=0,\ldots,m-1}$$

where $[\tau]_{i>j} = \tau$ if $i > j$, and $[\tau]_{i>j} = 1$ otherwise.

Note that the inner product of row $a$ with row $b$ of matrix $C$ is the same as the inner product of row $a + 1$ with row $b + 1$. Thus, to prove the unitarity of $C$, it suffices to show that

$$\delta_{a,0} \delta_{b,0} = \langle \text{row } a | \text{row } 0 \rangle = \sum_{j=0}^{m-1} \tau \alpha_{j-a} \alpha_j + \sum_{j=a}^{m-1} \alpha_{j-a} \alpha_j$$

holds, where $\delta_{a,0}$ denotes the Kronecker delta and the indices of $a$ are understood modulo $m$.

Consider the equation

$$1 = V^\dagger V = \left( \sum_{i=0}^{m-1} \tau_i U^{-i} \right) \left( \sum_{i=0}^{m-1} \alpha_i U^i \right)$$

The right hand side can be simplified to a polynomial in $U$ of degree less than $m$ using the identity $\tau U^m = 1$. The coefficient of $U^a$ in (10) is exactly the right hand side of equation (11). Since the minimal polynomial of $U$ is of degree $m$, it follows that the matrices $U^0, U^1, \ldots, U^{m-1}$ are linearly independent. Thus, comparing coefficients on both sides of equation (11) shows (10). Hence the rows of $C$ are pairwise orthogonal and of unit norm.

**A Simple Example.** Let $F_n$ be the discrete Fourier transform matrix

$$F_n = 2^{-n/2}(\exp(-2\pi i k \ell/2^n))_{k,\ell=0,\ldots,2^n-1},$$

with $i^2 = -1$. Recall that the Cooley-Tukey decomposition yields a fast quantum algorithm, which implements $F_n$ with $O(n^3)$ elementary operations. The minimal polynomial of $F_n$ is $x^4 - 1$ if $n \geq 3$. Thus, any unitary matrix $V$, which is a function of $F_n$, can be realized with $O(n^2)$ operations.

For instance, if $n \geq 3$, then the fractional power $F_n^x$, $x \in \mathbb{R}$, can be expressed by

$$F_n^x = \alpha_0(x) I + \alpha_1(x) F_n + \alpha_2(x) F_n^2 + \alpha_3(x) F_n^3,$$

where the coefficients $\alpha_i(x)$ are given by (cf. 2):

$$\alpha_0(x) = \frac{1}{2} (1 + e^{ix}) \cos x, \quad \alpha_1(x) = \frac{1}{2} (1 - e^{ix}) \sin x,$$

$$\alpha_2(x) = \frac{1}{2} (1 + e^{ix}) \cos x, \quad \alpha_3(x) = \frac{1}{2} (1 - e^{ix}) \sin x.$$
In this case, $F^\tau_2$ is realized by the circuit in Fig. 3 with $U = F_n$ and $M = (a_{j-1}(x))_{i,j=0,...,n-1}$. The circuit can be implemented with $O(n^2)$ operations.

IV. LIMITATIONS

The previous sections showed that a unitary matrix $f(U)$ can be realized by a linear combination of the powers $U^i$, $0 \leq i < m$, if the minimal polynomial $m(x)$ of $U$ is of the form $x^m - \tau$, $\tau \in \mathbb{C}$. One might wonder whether the restriction to minimal polynomials of this form is really necessary. The next lemma explains why we had this limitation:

**Lemma 3** Let $U$ be a unitary matrix with minimal polynomial $m(x) = x^m - g(x)$, $\deg g(x) < m$. If $g(x)$ is not a constant, then the matrix $M$ is in general not unitary.

*Proof.* Suppose that $g(x) = \sum_{i=0}^{m-1} g_i x^i$. We may choose for instance $V = U^m = g(U)$. Then the norm of first row in $M$ is greater than 1. Indeed, we can calculate this norm to be $|g_0|^2 + |g_1|^2 + \cdots + |g_{m-1}|^2$. However, $|g_0|^2 = 1$, because $g_0$ is a product of eigenvalues of $U$. By assumption, there is another nonzero coefficient $g_i$, which proves the result. $\square$

V. EXTENSIONS

We describe in this section one possibility to extend our approach to a larger class of unitary matrices $U$. We assumed so far that $f(U)$ is realized by a linear combination (2) of linearly independent matrices $U^i$. The exponents were restricted to the range $0 \leq i < m$, where $m$ is degree of the minimal polynomial of $U$. We can circumvent the problem indicated in the previous section by allowing $m$ to be larger than the degree of the minimal polynomial.

**Theorem 4** Let $U \in U(2^n)$ be a unitary matrix such that $U^m$ is a scalar matrix for some positive integer $m$. Suppose that there exists a quantum circuit which implements $U$ with $K$ elementary gates. Then a unitary matrix $V = f(U)$ can be realized with $O(mK + m^2 \log m)$ elementary operations.

*Proof.* By assumption, $U^m = \tau 1$ for some $\tau \in \mathbb{C}$. This means that the minimal polynomial $m(x)$ of $U$ divides the polynomial $x^m - \tau$, that is, $x^m - \tau = m(x)m_2(x)$ for some $m_2(x) \in \mathbb{C}[x]$.

We may assume without loss of generality that the function $f$ is defined at all roots of $x^m - \tau$. Indeed, we can replace $f$ by an interpolation polynomial $g$ satisfying $f(U) = g(U)$ if this is necessary.

Choose any unitary matrix $A \in U(2^n)$ with minimal polynomial $m_2(x)$. The minimal polynomial of the block diagonal matrix $U_A = \text{diag}(U, A)$ is $x^m - \tau$, the least common multiple of the polynomials $m(x)$ and $m_2(x)$. Express $f(U_A)$ by powers of the block diagonal matrix $U_A$:

$$f(U_A) = \text{diag}(f(U), f(A)) = \sum_{i=0}^{m-1} \alpha_i \text{diag}(U^i, A^i). \quad (12)$$

The approach detailed in Section IIA yields a unitary matrix $M$ to realize this linear combination. On the other hand, we obtain from (12) the relation

$$f(U) = \sum_{i=0}^{m-1} \alpha_i U^i$$

by ignoring the auxiliary matrices $A^i$, $0 \leq i < m$. It is clear that a circuit of the type shown in Fig. 3 with $\mu$ chosen such that $2^{\mu - 1} \leq m \leq 2^{\mu}$ implements this linear combination of the matrices $U^i$, $0 \leq i < m$, provided we use the matrix $M$ constructed above. $\square$

VI. CONCLUSIONS

Few methods are currently known that facilitate the engineering of quantum algorithms. Linear algebra allowed us to derive efficient quantum circuits for $f(U)$, given an efficient quantum circuit for $U$, as long as $U^m$ is a scalar matrix for some small integer $m$. This method can be used in conjunction with the Fourier sampling techniques by Shor [9], the eigenvalue estimation technique by Kitaev [10], and the probability amplitude amplification method by Grover [11], to design more elaborate quantum algorithms.

[1] A. Barenco et al., Phys. Rev. A 52, 3457 (1995).
[2] W. Ferrar, Finite Matrices (Oxford University Press, London, 1951).
[3] F. Gantmacher, The Theory of Matrices, vol. I (Chelsea, 1960).
[4] R. Horn and C. Johnson, Topics in Matrix Analysis (Cambridge University Press, New York, 1991).
[5] R. Rinehart, Amer. Math. Monthly 62, 395 (1955).
[6] D. DiVincenzo, Proc. R. Soc. London A 454, 261 (1998).
[7] B. Santhanam and J. McClellan, IEEE Trans. Signal Processing 44, 994 (1996).
[8] P. W. Shor, in Proc. FOCS 94 (IEEE Computer Society Press, 1994), pp. 124–134.
[9] A. Y. Kitaev, Russian Math. Surveys 52, 1191 (1997).
[10] L. Grover, in Proc. STOC (ACM, New York, 1996).