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 circuit which implements arbitrary functions of 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 $\mathcal{U}(m)$ the group of unitary $m \times m$ matrices, by $\mathbf{1}$ the identity matrix, and by $\mathbb{C}$ the field of complex numbers.

**I. PRELIMINARIES**

We recall some standard material on matrix functions, see [1, 2, 3] 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, $U = TDT^\dagger$ 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 $f(U) = T \text{diag}(f(\lambda_1), \ldots, f(\lambda_{2^n})) T^\dagger$, 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 $\alpha_i \in \mathbb{C}$ 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 [3]. 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 (2)? 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 $|0\rangle \otimes |\psi\rangle \in \mathbb{C}^{2^\mu} \otimes \mathbb{C}^2$ produce the state $|0\rangle \otimes V |\psi\rangle$.

---

*Electronic address: roettele@ira.uka.de*

1Research partly supported by NSF grant EIA 0218582, and a Texas A&V TITF grant.

2Electronic address: roettele@ira.uka.de

3Research 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 $|0\rangle \otimes |\psi\rangle \in \mathbb{C}^{2^\mu} \otimes \mathbb{C}^{2^n}$ is mapped to the state

$$\frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \otimes |\psi\rangle. \quad (3)$$

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

Notice that there exists an efficient implementation of the block diagonal matrix $A = \text{diag}(1, U, U^2, \ldots, U^{2^{\mu}-1})$. Indeed, $A$ can be composed of the matrices $U^{2^k}$, $0 \leq \eta < \mu$, 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

$$\frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \otimes U^i |\psi\rangle. \quad (4)$$

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 (4) is mapped to

$$\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle \otimes U^k V |\psi\rangle \quad (5)$$

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

$$\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle \otimes V |\psi\rangle. \quad (6)$$

We can clean up the ancillae bits by applying the $2^\mu \times 2^\mu$ matrix $B^\dagger$. This yields then the output state

$$|0\rangle \otimes V |\psi\rangle = |0\rangle \otimes f(U) |\psi\rangle. \quad (7)$$

The steps from the input state $|0\rangle \otimes |\psi\rangle$ to the final output state $|0\rangle \otimes V |\psi\rangle$ are illustrated in Fig. 2 for the case $\mu = 2$.

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 $2^\mu \times 2^\mu$ 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. [1]. 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 [2], and a controlled single qubit gate can be implemented with six or fewer elementary gates [1].

We observe that $2^{\mu} - 1$ copies of $\Lambda_1(U)$ suffice to implement $A$. Indeed, we certainly can implement $\Lambda_1(U^k)$ 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 $14(2^\mu - 1)K \in O(14mK)$ operations. Combining our counts yields the result. $\square$

**III. UNITARITY OF THE MATRIX $M$**

It remains to show that the state (5) can be transformed into the state (6) 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

$$V = \sum_{i=0}^{m-1} \alpha_i U^i. \quad (8)$$
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

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

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

The coefficients $\beta_i$ are explicitly given by

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

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

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

The $2^n \times 2^n$ 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 $(2^n - m) \times (2^n - m)$ 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 (5) the state

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

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

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

which coincides with (5), as claimed.

**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

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

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

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

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

Consider the equation

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

(11)

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 (11) is exactly the right hand side of equation (10). 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 $x^n - 1$ if $n \geq 3$. Thus, any unitary matrix $V$, which is a function of $F_n$, can be realized with $O(n^3)$ operations.

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

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

where the coefficients $\alpha_i(x)$ are given by (cf. 3):

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

$$\alpha_2(x) = \frac{1}{2} (-1 + e^{ix}) \cos x, \quad \alpha_3(x) = \frac{1}{2} (1 - ie^{ix}) \sin x.$$
In this case, $F_n^\tau$ is realized by the circuit in Fig. 3 with $U = F_n$ and $M = (\alpha_{j-1}(x))_{i,j=0,...,3}$. 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. $\Box$

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, $U^m = \tau \mathbf{1}$ 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 $U_A$:

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

The approach detailed in Section III 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 $2^\mu - 1 < m \leq 2^\mu$ implements this linear combination of the matrices $U^i$, $0 \leq i < m$, provided we use the matrix $M$ constructed above. $\Box$

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 conjuction with the Fourier sampling techniques by Shor [4], the eigenvalue estimation technique by Kitaev [9], and the probability amplitude amplification method by Grover [10], to design more elaborate quantum algorithms.