II. THE GENERIC CIRCUIT

Let $\mathcal{A}$ be a matrix with complex elements that allows to express the unitary transformation $f$. The matrix $f$ is defined by the equation

$$f |\psi\rangle = \sum_{i} f_i |i\rangle,$$

where $f$ is a matrix and $|\psi\rangle$ is the input state. The matrix $f$ is characterized by the eigenvalues $\lambda_i$ of the matrix $f$. The eigenvalues are defined as

$$\lambda_i = \sum_{j} f_{ij} \langle j | i \rangle,$$

where $|i\rangle$ and $|j\rangle$ are the eigenvectors of the matrix $f$. The eigenvalues are the characteristic of the matrix $f$ and they determine the behavior of the circuit.

The generic circuit is defined by the equation

$$f |\psi\rangle = \sum_{i} f_i |i\rangle,$$

where $f$ is a matrix and $|\psi\rangle$ is the input state. The matrix $f$ is characterized by the eigenvalues $\lambda_i$ of the matrix $f$. The eigenvalues are defined as

$$\lambda_i = \sum_{j} f_{ij} \langle j | i \rangle,$$

where $|i\rangle$ and $|j\rangle$ are the eigenvectors of the matrix $f$. The eigenvalues are the characteristic of the matrix $f$ and they determine the behavior of the circuit.
FIG. 1: A quantum circuit realizing the block diagonal matrix $A = \text{diag}(1, U, U^2, \ldots, U^{2^\mu-1})$.

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

$$\frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \otimes |\psi\rangle.$$  \hfill (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 $1/\sqrt{m}(1, \ldots, 1, 0, \ldots, 0)^T$. Efficient implementations of $B$ exist.

Notice that there exists an efficient implementation of the block diagonal matrix $A = \text{diag}(1, U, U^2, \ldots, U^{2^\mu-1})$. Indeed, $A$ can be composed of the matrices $U^k$, $0 \leq k < \mu$, conditioned on the ancilla bits. The resulting implementation is shown in Fig. 1. The state (3) is transformed by this circuit into the state

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

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

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

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

$$|0\rangle \otimes \overline{V} |\psi\rangle = |0\rangle \otimes f(U) |\psi\rangle.$$  \hfill (7)

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

FIG. 2: Generic circuit realizing a linear combination $V$. The case $\mu = 2$ is shown.

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 $x^m - \tau \in \mathbb{C}$. 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 [6], 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 $\Lambda_1(U^{2^\mu})$ by a sequence of $2^{\mu}$ 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 $14(2^\mu - 1)K = O(14mK)$ operations. Combining our counts yields the result. \hfill \Box

III. UNITARITY OF THE MATRIX $M$

It remains to show that the state (4) can be transformed into the state (5) 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

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

The matrix $M$ is then given by

$$M = \sum_{i=0}^{m-1} a_i B^i.$$
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
\[
U^k V = \sum_{i=0}^{m-1} \alpha_i U^{i+k}.
\] (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 (9) reduces to a polynomial in \( U \) of degree less than \( m \) using the relation \( U^m = g(U) \):
\[
U^k V = \sum_{i=0}^{m-1} \beta_k i U^i.
\]
The coefficients \( \beta_k i \) are explicitly given by
\[
(\beta_k 0, \beta_k 1, \ldots, \beta_k (m-1)) = (\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) P^k
\]
where \( P \) denotes the companion matrix of \( m(x) \), that is,
\[
P = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
g_0 & g_1 & g_2 & \cdots & \beta_{m-1}
\end{pmatrix}.
\]
The \( 2^m \times 2^m \) matrix \( M \) is defined by
\[
M = \begin{pmatrix} C & 0 \\ 0 & 1 \end{pmatrix}
\]
where \( C = (\beta_k i)_{k,i=0,\ldots,m-1} \), and \( 1 \) is a \((2^m-m) \times (2^m-m)\) 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 (4) the state
\[
\frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} M |i\rangle \otimes U^i |\psi\rangle = \frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} \beta_k i |k\rangle \otimes U^i |\psi\rangle
\]
\[
= \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle \otimes \sum_{i=0}^{m-1} \beta_k i U^i |\psi\rangle
\]
\[
= \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle \otimes U^k V |\psi\rangle
\]
which coincides with (5), as claimed.

**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
\[
C = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{m-1} \\ \tau \alpha_0 & \alpha_0 & \cdots & \alpha_{m-2} \\ \cdots & \cdots & \cdots & \cdots \\ \tau \alpha_0 & \tau \alpha_1 & \cdots & \alpha_0 \end{pmatrix}
\]
that is, \( C \) is obtained from a circulant matrix by multiplying every entry below the diagonal by \( \tau \). In other words, we have
\[
C = \left[ \begin{array}{cccc}
\tau_{[i,j]} & \alpha_j \mod m \\
\vdots & \ddots & \vdots \\
\alpha_0 & \cdots & \cdots & \alpha_0 \\
\end{array} \right]_{i,j=0,\ldots,m-1}
\]
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
\[
d_{a,b} = \langle \text{row } a | \text{row } 0 \rangle = \sum_{j=0}^{m-1} \tau \alpha_j a_j + \sum_{j=0}^{m-1} \alpha_j a_j
\]
holds, where \( d_{a,b} \) denotes the Kronecker delta and the indices of \( a \) are understood modulo \( m \).

Considering 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 \( U^k \) 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
\[
F_n = 2^{-n/2} \exp(-2\pi i k l / 2^n) |k,l = 0,\ldots,2^n-1,\]
with \( \tau^2 = -1 \). Recall that the Cooley-Tukey decomposition yields a fast quantum algorithm, which implements \( F_n \) with \( O(n^2) \) 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 \( O(n^2) \) operations.

For instance, if \( n \geq 3 \), then the fractional power \( F_n^{\frac{1}{2}} \), \( x \in \mathbb{R} \), can be expressed by
\[
F_n^{\frac{1}{2}} = \alpha_0(x) I + \alpha_1(x) F_n + \alpha_2(x) F_n^2 + \alpha_3(x) F_n^3,
\]
where the coefficients \( \alpha_i(x) \) are given by (cf. [7]):
\[
\begin{align*}
\alpha_0(x) &= \frac{1}{2} (1 + e^{i\pi} c x), \quad \alpha_1(x) = \frac{1}{2} (1 - i e^{i\pi} \sin x) \\
\alpha_2(x) &= \frac{1}{2} (-1 + e^{i\pi} \cos x), \quad \alpha_3(x) = \frac{1}{2} (1 - i e^{i\pi} \cos x).
\end{align*}
\]
In this case, $F_2^n$ is realized by the circuit in Fig. 2 with $U = F_n$ and $M = (a_{j-1}(x))_{i,j=0,1}$. The circuit can be implemented with $O(n^3)$ 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, $|g_i|^2 = 1$, because $g_i$ 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 $O(mK + n \log m)$ elementary operations.

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

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

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. 2 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. $\square$

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 [8], the eigenvalue estimation technique by Kitaev [9], and the probability amplitude amplification method by Grover [10], to design more elaborate quantum algorithms.