Information Processing Letters 75 (2000) 101–107

Information Processing Letters

www.elsevier.com/locate/ipl

A new universal and fault-tolerant quantum basis ☆

P. Oscar Boykin [a], Tal Mor [a,b], Matthew Pulver [a], Vwani Roychowdhury [a], Farrokh Vatan [a,*]

[a] *Electrical Engineering Department, UCLA, Los Angeles, CA 90095, USA*

[b] *Electrical Engineering, College of Judea and Samaria, Ariel, Israel*

Received 6 August 1999; received in revised form 28 April 2000
Communicated by L.A. Hemaspaandra

Abstract

A novel universal and fault-tolerant basis (set of gates) for quantum computation is described. Such a set is necessary to perform quantum computation in a realistic noisy environment. The new basis consists only of two single-qubit gates (*Hadamard* and $\sigma_z^{1/4}$), and one two-qubit gate (Controlled-NOT). Moreover, a new general method for fault-tolerant implementation of quantum gates like Toffoli is introduced. This method is a generalization of the methods suggested by Shor (Proc. FOCS'96, 1996, p. 56) and later by Knill et al. (Proc. Roy. Soc. London Ser. A 454 (1998) 365). © 2000 Elsevier Science B.V. All rights reserved.

Keywords: Fault tolerance; Quantum computation; Unitary operation; Universal set of gates

1. Introduction

A new model of computation based on the laws of quantum mechanics [7] has been shown to be superior to standard (classical) computation models [19,12]. Potential realizations of such computing devices are currently under extensive research, and the theory of using them in a realistic noisy environment is still developing. Two of the main requirements for error-free operations are to have a set of gates that is both universal for quantum computing (see [1,3–5,8] and references therein), and that can operate in a noisy environment (i.e., fault-tolerant) [18,20,2,15,13,16].

A scheme to correct errors in quantum bits (qubits) was proposed by Shor [18] by adopting standard coding techniques and modifying them to correct quantum mechanical errors induced by the environment. To avoid errors in the computation itself, Shor [20] suggested performing the computations on the logical qubits (without first decoding them), and this type of computation is known as fault-tolerant computation.

There are significant restrictions on both the types of unitary operations that can be performed on the encoded logical qubits, and the quantum error-correcting codes that can be used to encode the logical qubits. For example, if the $((7,1,3))$ quantum code is used then

☆ A preliminary version of this paper appeared, as part of the paper by Boykin et al. in *Proceedings of 40th IEEE Annual Symposium on Foundations of Computer Science, FOCS'99*. This work was supported in part by grants from the Revolutionary Computing group at JPL (contract #961360), and from the DARPA Ultra program (subcontract from Purdue University #530-1415-01).

* Corresponding author.

E-mail addresses: boykin@ee.ucla.edu (P.O. Boykin), talmo@ee.ucla.edu (T. Mor), pulver@ee.ucla.edu (M. Pulver), vwani@ee.ucla.edu (V. Roychowdhury), vatan@ee.ucla.edu (F. Vatan).

PII: S0020-0190(00)00084-3

one can show that the following unitary operations can be fault-tolerantly implemented:

$$H := \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad \sigma_z^{1/2} := \begin{pmatrix}1 & 0\\ 0 & \mathrm{i}\end{pmatrix}, \tag{1}$$

$$\Lambda_1(\sigma_x) := \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix},$$

where $\mathrm{i} = \sqrt{-1}$, and $\Lambda_k(U)$ denotes the Controlled-U operation with k control bits (see [4]); $\Lambda_1(\sigma_x)$ is the Controlled-NOT (CNOT) gate. So far, these operations are the only ones that have been shown to be "directly" fault-tolerant operations (in the sense that no measurements and/or preparations of special states are required). It is well known, however, that the group generated by the above operations (often referred to as the *normalizer group*) is not universal for quantum computation. This leads to the interesting problem of determining a basis that is both universal and can be implemented fault-tolerantly.

The well-established results on the universality of quantum bases [1,3–5,8] rest primarily on the inclusion of at least one "non-elementary" gate, i.e., a gate that performs a rotation by an irrational multiple of π. A direct fault-tolerant realization of such a gate, however, is not possible; this property makes all the well-known universal bases inappropriate for practical and noisy quantum computation.

The search for universal and fault-tolerant bases has led to a novel basis as proposed in the seminal work of Shor [20]. It includes the Toffoli gate in addition to the above-mentioned generators of the normalizer group; hence, the basis can be represented by the following set $\{H, \sigma_z^{1/2}, \Lambda_2(\sigma_x)\}$. A fault-tolerant realization of the Toffoli gate (involving only the generators of the normalizer group, preparation of a special state, and appropriate measurements) has been shown in [20]. Shor realized that this basis is universal, but a proof was not included. Later Kitaev [13] proved the universality of a basis, comprising the set $\{\Lambda_1(\sigma_z^{1/2}), H\}$, that is "equivalent" to Shor's basis, i.e., the gates in Kitaev's basis can be *exactly* realized using gates in Shor's basis and vice versa. This result provides the first published proof of the universality of a fault-tolerant basis. The resulting universality of Shor's basis is implicit in [13]; it is explicitly done in [6], and in the journal version of [2].

A number of other researchers have proposed fault-tolerant bases that are equivalent to Shor's basis. Knill et al. [14] considered the basis $\{H, \sigma_z^{1/2}, \Lambda_1(\sigma_z^{1/2}), \Lambda_1(\sigma_x)\}$ and the basis $\{\sigma_z^{1/2}, \Lambda_1(\sigma_z^{1/2}), \Lambda_1(\sigma_x)\}$ with the ability to prepare the encoded states $\frac{1}{2}\sqrt{2}(|0\rangle_L \pm |1\rangle_L)$.[1] The universality of these bases follows from the fact that gates in Shor's basis can be simulated by small size simple circuits over these new bases. Hence, while novel fault-tolerant realizations of the relevant gates in these bases were proposed, no new proofs of universality were required. The same authors later [15] studied a model in which the prepared state $\cos(\frac{1}{8}\pi)|0\rangle_L + \sin(\frac{1}{8}\pi)|1\rangle_L$ is made available, in addition to the normalizer group gates. In [15] it is shown that this set can realize the gate $\Lambda_1(H)$, and consequently the Toffoli gate and thus every gate in Shor's basis; this shows the universality of this set. One can verify that in the model proposed in [15] it is possible to perform $\sigma_y^{1/4}$, and hence this model is equivalent to the basis studied in this paper. In this paper we show that there is a simple proof of universality for this basis, moreover this basis is not equivalent to Shor's basis. We also note that Aharonov and Ben-Or [2] considered universal quantum systems with basic units that have $p > 2$ states (referred to as qubits). Gottesman and Chuang [11] present a technique for the general construction of our fault-tolerant implementation of the gates outside of the normalizer group.

It should be noted that once the existence of a *universal* fault-tolerant quantum basis is established, then any other universal basis available at the physical level can be utilized in a fault-tolerant computation: simply approximate each available gate by gates in the fault-tolerant universal basis. In this sense, any basis can be considered as fault-tolerant. But such implementation is conditioned on the existence of an *initial* universal fault-tolerant basis that works as a "seed" for other bases. We restrict the term "fault-tolerant basis" for such bases.

In this paper, we prove the existence of a novel basis for quantum computation that lends itself to an elegant proof (based solely on the geometry of real rotations in three dimensions) of universality and in which all the gates can be easily realized in a fault-tolerant manner.

[1] $|0\rangle_L$ and $|1\rangle_L$ refer to the states of the logical/encoded qubits.

In fact, we show that the addition of only one single-qubit operation to the set in (1), namely,

$$\sigma_z^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix}$$

leads to a universal and fault-tolerant basis for quantum computation. Since $\sigma_z^{1/2} = (\sigma_z^{1/4})^2$ our basis consists of the following three gates

$$H,\ \sigma_z^{1/4},\ \Lambda_1(\sigma_x). \tag{2}$$

Proving the universality of Shor's basis (see [13]) seems to be a more complicated process than proving the universality of the set of gates we suggest here, and our proof is different from Kitaev's proof. Moreover, we outline a general method for fault-tolerant realizations of a certain class of unitary operations; the fault-tolerant realizations of both the $\sigma_z^{1/4}$ and the Toffoli gates are shown to be special cases of this general formulation.

This paper is devoted to the proof of universality, followed by a discussion on the fault-tolerant realization of the $\sigma_z^{1/4}$ gate. We also show that the new basis proposed in this paper is not equivalent to Shor's basis: the gates in Shor's basis can be *exactly* realized using gates in our basis but not vice versa.

2. Definitions and identities

The identity I and the Pauli σ matrices are:

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_y := \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

We mention the following useful identities:

$$H := \tfrac{1}{2}\sqrt{2}(\sigma_x + \sigma_z), \qquad \sigma_y = \mathrm{i}\sigma_x\sigma_z,$$

and also, with

$$\sigma_z^\alpha = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi\alpha} \end{pmatrix},$$

we have

$$\sigma_x = H\,\sigma_z\,H \quad \text{and} \quad \sigma_y = \sigma_z^{1/2}\,\sigma_x\,\sigma_z^{-1/2}. \tag{3}$$

We review some properties of matrices in SU(2). Let $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. Every traceless and Hermitian 2×2 unitary matrix A can be represented as $A = \hat{n} \cdot \vec{\sigma} = n_x\sigma_x + n_y\sigma_y + n_z\sigma_z$, where $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ is a unit vector. From commutation relations $(\hat{n} \cdot \vec{\sigma})^2 = I$, and using this fact exponentiation of these Pauli matrices can be easily performed to give $\mathrm{e}^{\mathrm{i}\varphi\hat{n}\cdot\vec{\sigma}} = \cos\varphi\ I + \mathrm{i}\sin\varphi(\hat{n} \cdot \vec{\sigma})$. Then, we have

$$\mathrm{e}^{\mathrm{i}\varphi_1\hat{n}\cdot\vec{\sigma}} \cdot \mathrm{e}^{\mathrm{i}\varphi_2\hat{n}\cdot\vec{\sigma}} = \mathrm{e}^{\mathrm{i}(\varphi_1+\varphi_2)\hat{n}\cdot\vec{\sigma}}$$

and

$$\left(\mathrm{e}^{\mathrm{i}\phi\vec{n}\cdot\sigma}\right)^m = \mathrm{e}^{\mathrm{i}m\phi\vec{n}\cdot\sigma}.$$

It should be noted that for every element, U in SU(2) there exist an angle φ_U and a unit vector $\hat{n}_U \in \mathbb{R}^3$, such that [17, p. 170]

$$U = \mathrm{e}^{\mathrm{i}\varphi_U\hat{n}_U\cdot\vec{\sigma}}.$$

From the similarity transformations (see identities (3)) it follows that:

$$\sigma_x^\alpha = H\,\sigma_z^\alpha\,H,$$
$$\sigma_y^\alpha = \sigma_z^{1/2}\,\sigma_x^\alpha\,\sigma_z^{-1/2},$$
$$H^\alpha = \sigma_y^{1/4}\,\sigma_z^\alpha\,\sigma_y^{-1/4}.$$

Note that we can also equivalently write

$$\sigma_j^\alpha = \mathrm{e}^{\mathrm{i}(\pi\alpha/2)}\mathrm{e}^{-\mathrm{i}(\pi\alpha/2)\sigma_j}.$$

So, using our basis (2), it is possible to compute σ_j^m and H^m for $j \in \{x, y, z\}$ and $m \in \{1, \frac{1}{2}, \frac{1}{4}\}$.

3. A proof of universality

All that is needed for universal quantum computation is $\Lambda_1(\sigma_x)$ and SU(2) (see [4]). Thus, the proof of universality of our basis follows from the fact that H and $\sigma_z^{1/4}$ form a dense set in SU(2); i.e., for any element of SU(2) and desired degree of precision, there exists a finite product of H and $\sigma_z^{1/4}$ that approximates it to this desired degree of precision.

The unitary operations $U_1 = \sigma_z^{-1/4}\,\sigma_x^{1/4}$ and $U_2 = H^{-1/2}\,\sigma_z^{-1/4}\,\sigma_x^{1/4}\,H^{1/2}$ are exactly computable by our basis. As mentioned in Section 1, there are unit vectors $\hat{n}_1, \hat{n}_2 \in \mathbb{R}^3$ and angles λ_1 and λ_2 such that $U_1 =$

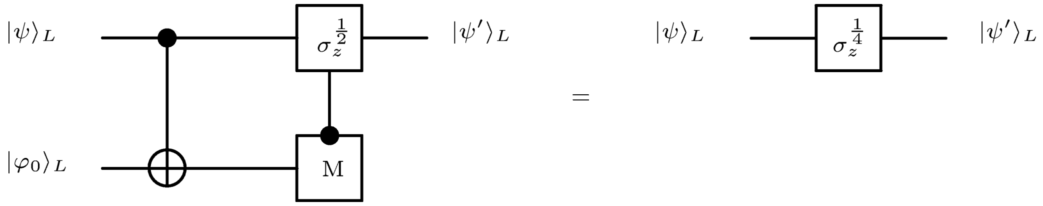

Fig. 1. Implementing $\sigma_z^{1/4}$ fault-tolerantly.

$\mathrm{e}^{\mathrm{i}\pi\lambda_1\hat{n}_1\cdot\vec{\sigma}}$ and $U_2 = \mathrm{e}^{\mathrm{i}\pi\lambda_2\hat{n}_2\cdot\vec{\sigma}}$. By calculating the values of $\hat{n}_j$ and λ_j we get $\lambda_1 = \lambda_2 = \lambda$ and

$$\cos\lambda\pi = \cos^2\tfrac{1}{8}\pi = \tfrac{1}{2}\big(1+\tfrac{1}{2}\sqrt{2}\big),$$
$$\vec{n}_1 = \big(\sqrt{2}\cot\tfrac{1}{8}\pi\big)\tfrac{1}{2}\sqrt{2}\,(\hat{z}-\hat{x}) + \hat{y},$$
$$\vec{n}_2 = \big(\sqrt{2}\cot\tfrac{1}{8}\pi\big)\hat{y} - \tfrac{1}{2}\sqrt{2}\,(\hat{z}-\hat{x}),$$

where $\hat{n}_j = \vec{n}_j/\|\vec{n}_j\|$ and $\hat{x}$, $\hat{y}$, and $\hat{z}$ are the unit vectors along the respective axes. One can easily verify that $\vec{n}_1$ and $\vec{n}_2$ are orthogonal (these vectors would need to be normalized when used in exponentiation).

The number $\mathrm{e}^{\mathrm{i}2\pi\lambda}$ is a root of the irreducible monic polynomial

$$x^4 + x^3 + \tfrac{1}{4}x^2 + x + 1$$

which is not cyclotomic (since not all coefficients are integers), and thus λ is an irrational number (see Appendix A, Theorem A.1). Since λ is irrational, it can be used to approximate any angle φ as $\lambda m \approx \varphi$, for some $m \in \mathbb{N}$. So we have

$$\big(\mathrm{e}^{\mathrm{i}\pi\lambda\hat{n}_j\cdot\sigma}\big)^m = \mathrm{e}^{\mathrm{i}m\pi\lambda\hat{n}_j\cdot\sigma} \approx \mathrm{e}^{\mathrm{i}\pi\varphi\hat{n}_j\cdot\sigma}.$$

Fortunately, this is all that is needed. Since, from orthogonality of $\vec{n}_1$ and $\vec{n}_2$, it follows that for any $U \in \mathrm{SU}(2)$ there are angles α, β and γ such that [17, p. 173]:

$$\begin{aligned} U &= \mathrm{e}^{\mathrm{i}\varphi_U\hat{n}_U\cdot\vec{\sigma}} \\ &= \big(\mathrm{e}^{\mathrm{i}\alpha\hat{n}_1\cdot\vec{\sigma}}\big)\big(\mathrm{e}^{\mathrm{i}\beta\hat{n}_2\cdot\vec{\sigma}}\big)\big(\mathrm{e}^{\mathrm{i}\gamma\hat{n}_1\cdot\vec{\sigma}}\big). \end{aligned} \tag{4}$$

The representation in (4) is clearly analogous to Euler rotations about three orthogonal vectors. Expansion of (4) gives:

$$\cos\phi = \cos\beta\cos(\gamma+\alpha), \tag{5}$$
$$\begin{aligned} \hat{n}\sin\phi = {}& \hat{n}_1\cos\beta\sin(\gamma+\alpha) \\ &+ \hat{n}_2\sin\beta\cos(\gamma-\alpha) \\ &+ \hat{n}_1\times\hat{n}_2\sin\beta\sin(\gamma-\alpha). \end{aligned} \tag{6}$$

For any element of $U \in \mathrm{SU}(2)$ Eqs. (5) and (6) can be inverted to find α, β and γ.

There is no guarantee that, in general, it is possible to *efficiently approximate* an arbitrary phase $\mathrm{e}^{\mathrm{i}\varphi}$ by repeated applications of the available phase $\mathrm{e}^{\mathrm{i}\pi\lambda}$. But using an argument similar to the one presented in [1], we can show that for the given λ (as defined in (3)), for any given $\varepsilon > 0$, with only poly$(1/\varepsilon)$ iterations of $\mathrm{e}^{\mathrm{i}\pi\lambda}$ we can get $\mathrm{e}^{\mathrm{i}\varphi}$ within ε. However, since our basis is already proven to be universal, one can make use of an even better result. As it is shown by Kitaev [13] and Solovay and Yao [21], every universal quantum basis $\mathcal{B}$ is efficient, in the sense that any unitary operation in $\mathrm{U}(2^m)$, for constant m, can be approximated within ε by a circuit of size poly-log$(1/\varepsilon)$ over the basis $\mathcal{B}$.

4. A fault-tolerant realization of $\sigma_z^{1/4}$

We provide a simple scheme for the fault-tolerant realization of the $\sigma_z^{1/4}$ gate. The method describes a general procedure that works for any quantum code for which the elements of the normalizer group can be implemented fault-tolerantly and involves the creation of special eigenstates of unitary transformations.

To perform $\sigma_z^{1/4}$ fault-tolerantly we use the following state:

$$|\varphi_0\rangle = \sigma_z^{1/4}H|0\rangle = \frac{|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}|1\rangle}{\sqrt{2}}, \tag{7}$$

(for which we later present the preparation process). To apply $\sigma_z^{1/4}$ to a general single qubit state $|\psi\rangle$ using this special state $|\varphi_0\rangle$, first apply $\Lambda_1(\sigma_x)$ from $|\psi\rangle$ to $|\varphi_0\rangle$. See Fig. 1. Then measure the second qubit (i.e., $|\varphi_0\rangle$) in the computation basis. If the result is $|1\rangle$, apply $\sigma_z^{1/2}$ to the first qubit (i.e., $|\psi\rangle$). This leads to the desired operation, as demonstrated in the following:

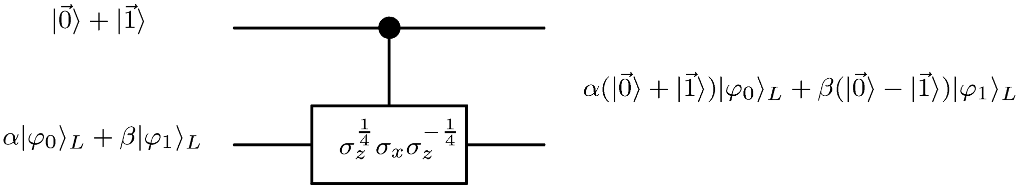
$|\vec{0}\rangle + |\vec{1}\rangle$
$\alpha|\varphi_0\rangle_L + \beta|\varphi_1\rangle_L$
$\sigma_z^{\frac{1}{4}}\sigma_x\sigma_z^{-\frac{1}{4}}$
$\alpha(|\vec{0}\rangle + |\vec{1}\rangle)|\varphi_0\rangle_L + \beta(|\vec{0}\rangle - |\vec{1}\rangle)|\varphi_1\rangle_L$

Fig. 2. Creation of the $|\varphi_0\rangle$ eigenstate.

$$\begin{aligned}|\psi\rangle\otimes|\varphi_0\rangle &= \big(\alpha|0\rangle+\beta|1\rangle\big)\otimes\frac{|0\rangle+\mathrm{e}^{\mathrm{i}\pi/4}|1\rangle}{\sqrt{2}}\\ &\xrightarrow{\Lambda_1(\sigma_x)} \big(\alpha|0\rangle+\mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle\big)\otimes\frac{|0\rangle}{\sqrt{2}}\\ &\qquad + \big(\alpha|0\rangle+\mathrm{e}^{-\mathrm{i}\pi/4}\beta|1\rangle\big)\otimes\mathrm{e}^{\mathrm{i}\pi/4}\frac{|1\rangle}{\sqrt{2}}\\ &= \sigma_z^{1/4}|\psi\rangle\otimes\frac{|0\rangle}{\sqrt{2}}+\sigma_z^{-1/4}|\psi\rangle\otimes\mathrm{e}^{\mathrm{i}\pi/4}\frac{|1\rangle}{\sqrt{2}}.\end{aligned}$$

Clearly, the above analysis shows that all that is necessary to perform $\sigma_z^{1/4}$ fault-tolerantly is the state $|\varphi_0\rangle$ and the ability to do $\Lambda_1(\sigma_x)$ and $\sigma_z^{1/2}$ fault-tolerantly. For a class of quantum codes, called CSS codes (see, e.g., [20]), $\Lambda_1(\sigma_x)$, H and $\sigma_z^{1/2}$ can be done fault-tolerantly [20,10]. We next show how to generate the state $|\varphi_0\rangle$ fault-tolerantly.

Fault-tolerant creation of certain particular encoded eigenstates has been discussed in [20,15]. We present it in a more general way. Suppose that the fault-tolerant operation U_η operates as follows:

$$U_\eta|\eta_i\rangle = (-1)^i|\eta_i\rangle$$

on the states $|\eta_i\rangle$. Thus, U_η has the states $|\eta_i\rangle$ as eigenvectors with ±1 as the eigenvalues. Suppose that we have access to a vector $|\tau\rangle$ such that:

$$|\tau\rangle = \alpha|\eta_0\rangle+\beta|\eta_1\rangle.$$

We show that using only bitwise operations, measurements, and this $|\tau\rangle$, the eigenvectors $|\eta_i\rangle$ can be obtained. Now, to get the eigenvector of U_η we make use of a $|\mathsf{cat}\rangle$ state:

$$|\mathsf{cat}\rangle = \tfrac{1}{2}\sqrt{2}\big(|00\ldots0\rangle+|11\ldots1\rangle\big) = \tfrac{1}{2}\sqrt{2}\big(|\vec{0}\rangle+|\vec{1}\rangle\big).$$

See Fig. 2. Applying $\Lambda_1(U_\eta)$ bitwise, on $|\mathsf{cat}\rangle\otimes|\tau\rangle$ we obtain:

$$|\mathsf{cat}\rangle\otimes|\tau\rangle \xrightarrow{\Lambda_1(U_\eta)} \alpha\big(\tfrac{|\vec{0}\rangle+|\vec{1}\rangle}{\sqrt{2}}\big)|\eta_0\rangle+\beta\big(\tfrac{|\vec{0}\rangle-|\vec{1}\rangle}{\sqrt{2}}\big)|\eta_1\rangle.$$

A fault-tolerant measurement can be made to distinguish $\frac{1}{2}\sqrt{2}(|\vec{0}\rangle+|\vec{1}\rangle)$ from $\frac{1}{2}\sqrt{2}(|\vec{0}\rangle-|\vec{1}\rangle)$ [20]. This measurement can be repeated to verify that we have it correct.

The fault-tolerant version of $\sigma_z^{1/4}$ needs the state $|\varphi_0\rangle$, which can be generated using this formalism. In fact, $|\varphi_0\rangle$ is an eigenstate of $U_\varphi = \sigma_z^{1/4}\sigma_x\sigma_z^{-1/4}$. By commutation properties of the $\sigma_z^{-1/4}$ operator, it is shown that U_φ can be realized with elements only from the normalizer group:

$$U_\varphi = \sigma_z^{1/4}\,\sigma_x\,\sigma_z^{-1/4} = \mathrm{e}^{\mathrm{i}\pi/4}\,\sigma_z^{1/2}\,\sigma_x.$$

Since $\sigma_z^{1/2}$ and σ_x can be done fault-tolerantly, so can U_φ. We consider the vector $|\varphi_0\rangle$ (defined by (7)) and the vector

$$|\varphi_1\rangle = \sigma_z^{1/4}H|1\rangle = \frac{|0\rangle-\mathrm{e}^{\mathrm{i}\pi/4}|1\rangle}{\sqrt{2}};$$

in short $|\varphi_j\rangle = \sigma_z^{1/4}H|j\rangle$. One can verify now that these $|\varphi_j\rangle$ are eigenvectors of U_φ (using identities (3)):

$$\begin{aligned}U_\varphi|\varphi_j\rangle &= \sigma_z^{1/4}\sigma_x\sigma_z^{-1/4}\big(\sigma_z^{1/4}H|j\rangle\big)\\ &= \sigma_z^{1/4}H(-1)^j|j\rangle = (-1)^j|\varphi_j\rangle.\end{aligned}$$

Since the $|\varphi_j\rangle$ vectors are orthogonal, any single qubit state $|\psi\rangle$ can be represented as a superposition of the $|\varphi_j\rangle$:

$$|\psi\rangle = \alpha|0\rangle+\beta|1\rangle = \alpha'|\varphi_0\rangle+\beta'|\varphi_1\rangle.$$

So, all the necessary ingredients are here: $|\psi\rangle$ and an appropriate fault-tolerant operation, U_φ. If the outcome gives $|\varphi_1\rangle$ rather than $|\varphi_0\rangle$ we can flip the state:

$$|\varphi_0\rangle = \sigma_z|\varphi_1\rangle = \sigma_z\frac{|0\rangle-\mathrm{e}^{\mathrm{i}\pi/4}|1\rangle}{\sqrt{2}} = \frac{|0\rangle+\mathrm{e}^{\mathrm{i}\pi/4}|1\rangle}{\sqrt{2}}.$$

Shor's implementation of Toffoli [20] also uses a special case of this general procedure. For performing

Toffoli one uses $U = \Lambda_1(\sigma_z) \otimes \sigma_z$ to get the eigenstates:

$$|\mathsf{AND}\rangle = \tfrac{1}{2}\bigl(|000\rangle + |010\rangle + |100\rangle + |111\rangle\bigr),$$
$$|\mathsf{NAND}\rangle = \tfrac{1}{2}\bigl(|001\rangle + |011\rangle + |101\rangle + |110\rangle\bigr).$$

Shor uses the $|\psi\rangle$ state of:

$$\begin{aligned}|\psi\rangle &= \tfrac{1}{2}\sqrt{2}\bigl(|\mathsf{AND}\rangle + |\mathsf{NAND}\rangle\bigr)\\ &= \bigl(H|0\rangle\bigr) \otimes \bigl(H|0\rangle\bigr) \otimes \bigl(H|0\rangle\bigr).\end{aligned}$$

Thus the special state in [20] can be obtained by the same general procedure.

5. Shor's basis and $\{H, \sigma_z^{1/4}, \Lambda_1(\sigma_x)\}$ are not equivalent

In this section we show that Shor's basis and our basis $\{H, \sigma_z^{1/4}, \Lambda_1(\sigma_x)\}$ are not equivalent. Every gate in Shor's basis can be exactly represented by a circuit over our basis, but the opposite is not true. It is not hard to see that the basis $Q_1 = \{\Lambda_1(\sigma_z^{1/2}), H\}$ is equivalent to Shor's basis (see [13,6] and the journal version of [2]).

The following identity shows that our basis can exactly implement any gate from Q_1:

$$\begin{aligned}\Lambda_1(\sigma_z^{1/2}) = {}&\bigl(I \otimes \sigma_z^{-1/4}\bigr)\Lambda_1(\sigma_x)\bigl(I \otimes \sigma_z^{-1/4}\bigr)\Lambda_1(\sigma_x)\\ &\times \bigl(\sigma_z^{1/4} \otimes \sigma_z^{1/2}\bigr).\end{aligned}$$

Hence, with our basis we can exactly implement any gate from Shor's basis. We prove that the converse is not true. Toward this end, we show that the unitary operation $\sigma_z^{1/4}$, can be computed exactly by our basis but not by Shor's basis. First we prove a useful lemma about unitary operations computable exactly by Shor's basis. Note that the set of integer complex numbers is the set $\mathbb{Z} + \mathrm{i}\mathbb{Z}$ of the complex numbers with integer real and imaginary parts.

Lemma 5.1. *Suppose that the unitary operation $U \in \mathrm{U}(2^m)$ is the transformation performed by a circuit $\mathcal{C}$ defined over Shor's basis with m inputs. Then U is of the form $(\frac{1}{2}\sqrt{2})^{\ell}M$, where M is a $2^m \times 2^m$ matrix with only complex integer entries.*

Proof. Suppose that $g_1, \ldots, g_t$ are the gates of $\mathcal{C}$. Each gate g_j can be considered as a unitary operation in $\mathrm{U}(2^m)$ by acting as an identity operator on the qubits that are not inputs of g_j. Let the matrix $M_j \in \mathrm{U}(2^m)$ represent g_j. Then $U = M_t \cdots M_1$. If g_j is a $\sigma_z^{1/2}$ gate then M_j is a diagonal matrix with 1 or i on its diagonal. If g_j is a Toffoli gate then M_j is a permutation matrix (which is a 0–1 matrix). Finally, if g_j is a Hadamard gate, then $M_j = \frac{1}{2}\sqrt{2}M'_j$, where the entries of M'_j are integers. This completes the proof. □

Now since

$$\sigma_z^{1/4} = \tfrac{1}{2}\sqrt{2}\begin{pmatrix}\sqrt{2} & 0\\ 0 & 1+\mathrm{i}\end{pmatrix},$$

by Lemma 5.1 it cannot be realized exactly by gates from Shor's basis.

Acknowledgements

We thank Alexei Kitaev and Peter Shor for helpful discussions on the subject of this paper. We are grateful to Dorit Aharonov for her comments on an earlier version of this work.

Appendix A. The cyclotomic/rational number theorem

Theorem A.1. *For any $c \in \mathbb{R}$, the following two statements are logically equivalent*:

- *The minimum monic polynomial $m_\alpha(x) \in \mathbb{Q}[x]$ for $\alpha \equiv \mathrm{e}^{\mathrm{i}2\pi c}$ exists and is cyclotomic.*
- *$c \in \mathbb{Q}$.*

Proof. A number of algebraic theorems will be taken for granted in this proof, in particular, properties of cyclotomic polynomials $\Phi_n(x)$. See, for instance, Dummit and Foote [9] for a more thorough discussion of these polynomials, as well as general properties of polynomial rings.

Assume $m_\alpha(x)$ exists and $m_\alpha(x) = \Phi_n(x)$ for some $n \in \mathbb{Z}^+$.

$$\begin{aligned}0 &= m_\alpha(\alpha) && \text{(definition of } m_\alpha(x))\\ &= \Phi_n(\alpha) && \text{(by assumption)}\\ &= \prod_{d|n} \Phi_d(\alpha) && \text{(0 times anything is 0)}\end{aligned}$$

$$= \alpha^n - 1 \qquad \text{(property of cyclotomic polynomials)}$$
$$= \mathrm{e}^{\mathrm{i}2\pi cn} - 1 \quad \text{(definition of } \alpha\text{)}.$$

$nc \in \mathbb{Z}$. Thus $c \in \mathbb{Q}$.

Conversely, assume $c \in \mathbb{Q}$. $c = p/q$ for some $p, q \in \mathbb{Z}$. $m_\alpha(x)$ exists, since $\alpha^q - 1 = \mathrm{e}^{\mathrm{i}2\pi cq} - 1 = \mathrm{e}^{\mathrm{i}2\pi p} - 1 = 0$. Moreover, $m_\alpha(x)$ divides $x^q - 1 = \prod_{d|q} \Phi_d(x)$ in $\mathbb{Q}[x]$. $m_\alpha(x) \propto \Phi_n(x)$ for some $n|q$. Since both are monic, $m_\alpha(x) = \Phi_n(x)$. □

References

[1] L.M. Adleman, J. Demarrais, M.-D.A. Huang, Quantum computability, SIAM J. Comput. 26 (1997) 1524–1540.

[2] D. Aharonov, M. Ben-Or, Fault-tolerant quantum computation with constant error, in: Proc. 29th Annual ACM Symposium on Theory of Computing (STOC'97), 1997, pp. 46–55.

[3] A. Barenco, A universal two-bit gate for quantum computation, Proc. Roy. Soc. London Ser. A 449 (1995) 679–683.

[4] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A 52 (1995) 3457–3467.

[5] E. Bernstein, U. Vazirani, Quantum complexity theory, SIAM J. Comput. 26 (1997) 1411–1473.

[6] P.O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, F. Vatan, On universal and fault-tolerant quantum computing, in: Proc. 40th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, 1999; LANL eprint quant-ph/9906054.

[7] D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, Proc. Roy. Soc. London Ser. A 400 (1985) 97–117.

[8] D. Deutsch, Quantum computational networks, Proc. Roy. Soc. London Ser. A 245 (1989) 73–90.

[9] D.S. Dummit, R.M. Foote, Abstract Algebra, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1991.

[10] D. Gottesman, Theory of fault-tolerant quantum computation, Phys. Rev. A 57 (1998) 127–137.

[11] D. Gottesman, I.L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature 402 (1999) 390–393.

[12] L. Grover, A fast quantum mechanical algorithm for database search, in: Proc. 28th ACM Symposium on Theory of Computing, 1996, pp. 212–219.

[13] A. Kitaev, Quantum computations: Algorithms and error correction, Russian Math. Surveys 52 (1997) 1191–1249.

[14] E. Knill, R. Laflamme, W.H. Zurek, Accuracy threshold for quantum computation, LANL eprint quant-ph/9611025, 1996.

[15] E. Knill, R. Laflamme, W.H. Zurek, Resilient quantum computation: Error models and thresholds, Proc. Roy. Soc. London Ser. A 454 (1998) 365–384.

[16] J. Preskill, Reliable quantum computers, Proc. Roy. Soc. London Ser. A 454 (1998) 385–410.

[17] J.J. Sakurai, Modern Quantum Mechanics, rev. edn., Addison-Wesley, Reading, MA, 1994.

[18] P. Shor, Scheme for reducing decoherence in quantum computer memory, Phys. Rev. A 52 (1995) 2493–2496.

[19] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (1997) 1484–1509.

[20] P. Shor, Fault-tolerant Quantum Computation, in: Proc. 37th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, 1996, pp. 56–65.

[21] R. Solovay, A. Yao, Preprint, 1996.