CGateSEO_writer Algebraic Details

Robert R. Tucci
P.O. Box 226
Bedford, MA 01730
tucci@ar-tiste.com

December 8, 2016

Abstract

The purpose of this paper is to present some algebra that underlies some quantum circuit identities from Ref.[1] that are used within the class CGateSEO_writer of Qubiter. By putting the algebra here, I hope it makes it easier for Qubiter users to follow the code and to spot & report any mistakes if there are any in the algebra.

1 Introduction

All the quantum circuit identities in this paper have been known for a long time. They appear in Ref.[1] published in 1995. The purpose of this paper is to present some algebra that underlies those identities. Most of that algebra is used within the class CGateSEO_writer of Qubiter.

Throughout this paper and in the Qubiter code, we use "1c_u2" to mean a singly controlled U(2) matrix and "mc_u2" to mean a multiply controlled U(2) matrix.

2 Notation and Preliminaries

In this section, we will review briefly some of the more unconventional notation used in this paper. For a more detailed discussion of Tucci's notation, especially its more idiosyncratic aspects, see, for example, Ref.[2].

Note that in our circuit diagrams, time points in this direction $\leftarrow$, in agreement with the usual ordering of operators in Dirac notation. This is contrary to most papers on quantum computing, which draw quantum circuits with time pointing in this direction $\rightarrow$.

As usual, the Pauli matrices are defined by:

$$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \ , \ \ \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \ , \ \ \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \ . \tag{1}$$

We will denote the projectors onto the states 0 and 1 by

$$P_1 = |1\rangle \langle 1| = n \tag{2}$$

(n is often referred to as the number operator because it equals 1 if the state has 1 particle and 0 if 0) and

$$P_0 = |0\rangle \langle 0| = 1 - n = \overline{n} \ . \tag{3}$$

Note that

$$n = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1 - \sigma_Z}{2} \tag{4}$$

and

$$\overline{n} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \frac{1 + \sigma_Z}{2} \ . \tag{5}$$

Recall that the 2-dim Hadamard matrix defined by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{6}$$

satisfies

$$H^2 = H \ , \ \ H\sigma_X H = \sigma_Z \ . \tag{7}$$

Let $\hat{r} \cdot \vec{\sigma} = \sigma_r$ for any (3-dim, real) unit vector $\hat{r}$.

One can show by Taylor expansion that

$$e^{i\theta\sigma_r} = \cos(\theta) + i\sigma_r \sin(\theta) \tag{8}$$

for any real number θ and unit vector $\hat{r}$.

For any unit vectors $\hat{r}$ and $\hat{s}$, the Pauli matrices satisfy:

$$\sigma_r\sigma_s = \hat{r} \cdot \hat{s} + i\sigma_r \times \sigma_s \ . \tag{9}$$

Any SU(2) matrix W can be expressed as $e^{i\theta_w\sigma_w}$ for some real number θ_w and unit vector $\hat{w}$. We will call $(\theta_w, \hat{w})$ the SU(2)-pair corresponding to W. Since the product of two SU(2) matrices equals another SU(2) matrix, the following equation:

$$e^{i\theta_{w_1}\sigma_{w_1}} e^{i\theta_{w_2}\sigma_{w_2}} = e^{i\theta_w\sigma_w} \tag{10}$$

defines a map of 2 SU(2)-pairs into a new one.

$$(\theta_{w_1}, \hat{w_1}), (\theta_{w_2}, \hat{w_2}) \rightarrow (\theta_w, \hat{w}) \ . \tag{11}$$

One can find analytic expressions for the output SU(2)-pair in terms of the two input SU(2)-pairs as follows. Let $c = \cos(\theta_w)$ and $s = \sin(\theta_w)$. Also abbreviate $c_j = \cos(\theta_{w_j})$ and $s_j = \sin(\theta_{w_j})$ for $j = 1, 2$. Then

$$\begin{aligned} (c_1 + i\sigma_{w_1}s_1)(c_2 + i\sigma_{w_2}s_2) &= \begin{cases} c_1c_2 - s_1s_2\hat{w_1} \cdot \hat{w_2} \\ +is_1c_2\sigma_{w_1} + is_2c_1\sigma_{w_2} - is_1s_2\sigma_{\hat{w_1}\times\hat{w_2}} \end{cases} & (12) \\ &= c + i\sigma_w s \ . & (13) \end{aligned}$$

Define

$$\vec{r} = s_1c_2\hat{w_1} + s_2c_1\hat{w_2} - s_1s_2\hat{w_1} \times \hat{w_2} \tag{14}$$

and

$$\hat{w} = \frac{\vec{r}}{|\vec{r}|} \ . \tag{15}$$

Then

$$\begin{array}{l} c = c_1c_2 - s_1s_2\hat{w_1} \cdot \hat{w_2} \\ s = |\vec{r}| \\ \theta_w = \arctan 2(s, c) = \arctan(s/c) \end{array} \ . \tag{16}$$

Some U(2) matrices to which Qubiter allows one to attach controls are:

$$e^{i\theta\overline{n}} = e^{i\frac{\pi}{2}} e^{i\frac{\theta}{2}\sigma_Z} \ , \tag{17a}$$

$$e^{i\theta n} = e^{i\frac{\pi}{2}} e^{-i\frac{\theta}{2}\sigma_Z} \ , \tag{17b}$$

$$\sigma_a = (-i)(i\sigma_a) = e^{-i\frac{\pi}{2}} e^{i\frac{\pi}{2}\sigma_a} \tag{17c}$$

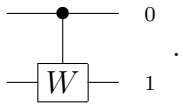
for $a = X, Y, Z$, and

$$H = \frac{\sigma_X + \sigma_Z}{\sqrt{2}} = (-i)(i\sigma_a) = e^{-i\frac{\pi}{2}} e^{i\frac{\pi}{2}\sigma_a} \tag{17d}$$

for $a = \frac{\hat{x}+\hat{z}}{\sqrt{2}}$.

3 One Controlled U(2) (1c_u2)

In this section, we will show how to express a 1c_u2 as a product of CNOTs and single qubit rotations. Pictorially , if W is any U(2) matrix, we want to expand:

$W(1)^{n(0)} =$ 

. (18)

In general, a 1c_u2 requires 3 CNOTs to express it, but in some special cases, one can get away with using only 1 or 2 CNOTs. This section contains 3 subsections dealing with the cases of 1, 2 and 3 CNOTs, in that order.

We will express W in two ways:

$$W = e^{i\delta} e^{i\theta_w \sigma_w} \ , \tag{19}$$

and

$$W = e^{i\delta} e^{i\alpha\sigma_Z} e^{i\gamma\sigma_Y} e^{i\beta\sigma_Z} \ , \tag{20}$$

for real numbers $\delta, \theta_w, \alpha, \gamma, \beta$ and a unit vector $\hat{w}$. Next, we shall express the parameters (α, γ, β) in terms of the SU(2)-pair $(\theta, \hat{w})$.

Define $w_\pm = w_x \pm i w_y$. For any angle ξ, we will use the abbreviations $c_\xi = \cos(\xi)$ and $s_\xi = \sin(\xi)$. One has

$$\begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix} \begin{bmatrix} c_\gamma & s_\gamma \\ -s_\gamma & c_\gamma \end{bmatrix} \begin{bmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{bmatrix} = \begin{bmatrix} c_{\theta_w} + i w_z s_{\theta_w} & i s_{\theta_w} w_- \\ i s_{\theta_w} w_+ & c_{\theta_w} - i w_z s_{\theta_w} \end{bmatrix} \tag{21}$$

so

$$e^{i(\alpha+\beta)} c_\gamma = c_{\theta_w} + i w_z s_{\theta_w} \tag{22}$$

and

$$e^{i(\alpha-\beta)}s_\gamma = is_{\theta_w}w_- \ . \tag{23}$$

Define mag, c_γ and s_γ by

$$mag = \sqrt{c_{\theta_w}^2 + w_z^2 s_{\theta_w}^2} \ , \tag{24}$$

$$c_\gamma = mag \tag{25}$$

and

$$s_\gamma = s_{\theta_w}|w_-| \ . \tag{26}$$

Then

$$e^{i(\alpha+\beta)} = \frac{c_{\theta_w} + iw_z s_{\theta_w}}{mag} = e^{\theta_1} \tag{27}$$

and

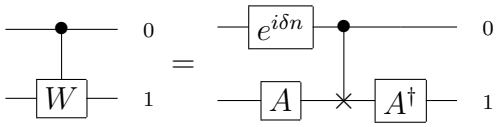
$$e^{i(\alpha-\beta)} = \frac{iw_x + w_y}{|w_-|} = e^{i\theta_2} \ . \tag{28}$$

The last two equations should be taken as the definitions of the real parameters θ_1 and θ_2. It follows that

$$\begin{array}{l} \alpha = \frac{\theta_1+\theta_2}{2} \\ \beta = \frac{\theta_1-\theta_2}{2} \\ \gamma = \arctan 2(s_{\theta_w}|w_-|, mag) \end{array} \ . \tag{29}$$

3.1 1 CNOTS, 2 target rots

Assume that we can write



(30)

for U(2) matrices W, A and a real parameter δ.

Eq.(30) implies that

$$W = e^{i\delta}A\sigma_X A^\dagger \ . \tag{31}$$

Therefore

$$W = e^{i\delta}\sigma_w \ . \tag{32}$$

Next we show that Eq.(31) can be satisfied if we assume A can be expressed as:

$$A = i\sigma_a \ . \tag{33}$$

Eqs.(31), (32) and (33) imply

$$\sigma_w = \sigma_a \sigma_X \sigma_a \ . \tag{34}$$

But

$$\begin{aligned} \sigma_a \sigma_X \sigma_a &= (a_x + i\sigma_{\hat{a}\times\hat{x}})\sigma_a && (35)\\ &= a_x\sigma_a + i\underbrace{(\hat{a}\times\hat{x})\cdot\hat{a}}_{0} - \sigma\underbrace{(\hat{a}\times\hat{x})\times\hat{a}}_{\hat{x}-a_x\hat{a}} && (36)\\ &= 2a_x\sigma_a - \sigma_X \ , && (37) \end{aligned}$$

so

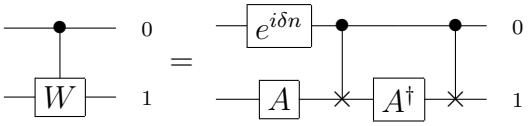
$$\begin{aligned} w_x &= 2a_x^2 - 1 \\ w_y &= 2a_x a_y \\ w_z &= 2a_x a_z \end{aligned} \tag{38}$$

which can be inverted to

$$\begin{aligned} a_x &= \sqrt{\tfrac{w_x+1}{2}} \\ a_y &= \tfrac{w_y}{2a_x} \\ a_z &= \tfrac{w_z}{2a_x} \end{aligned} \quad . \tag{39}$$

3.2 2 CNOTS, 2 target rots

Assume that we can write



(40)

for U(2) matrices W, A and a real parameter δ.

Eq.(40) implies that

$$W = e^{i\delta} A \sigma_X A^\dagger \sigma_X \ . \tag{41}$$

Therefore

$$w_x = 0 \ . \tag{42}$$

Next we show that Eq.(41) can be satisfied if we assume A can be expressed as:

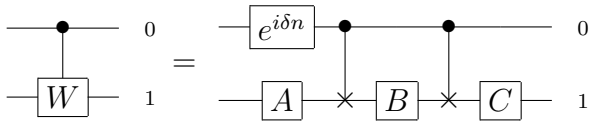
$$A = e^{i\alpha\sigma_Z} e^{i\frac{\gamma}{2}\sigma_Y} \tag{43}$$

for real parameters α, γ. Indeed, just set (this is a special case of Eqs.(29)):

$$\begin{array}{l} \alpha = \beta = \frac{\theta_1}{2} \\ \gamma = \arctan 2(s_{\theta_w} w_y, mag) \end{array} . \tag{44}$$

3.3 3 CNOTS, 3 target rots

Assume that we can write



(45)

for U(2) matrices W, A, B, C and a real parameter δ.

Eq.(45) implies

$$1 = ABC \tag{46}$$

and

$$W = e^{i\delta} A \sigma_X B \sigma_X C \, . \tag{47}$$

The last two equations are satisfied if we set

$$A = e^{i\alpha\sigma_Z} e^{i\frac{\gamma}{2}\sigma_Y} \, , \tag{48}$$

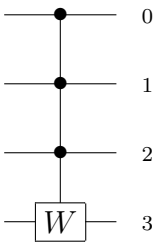
$$B = e^{-i\frac{\gamma}{2}\sigma_Y} e^{-i\frac{\alpha+\beta}{2}\sigma_Z} \, , \tag{49}$$

$$C = e^{i\frac{\beta-\alpha}{2}\sigma_Z} \tag{50}$$

with the real parameters α, β, γ given by Eqs.(29).

4 Multi Controlled U(2) (mc_u2)

In this section, we will show how to express a mc_u2 as a product of CNOTs and single qubit rotations. Pictorially , if W is any U(2) matrix, we want to expand:

$W(3)^{n(2)n(1)n(0)} =$ 

. (51)

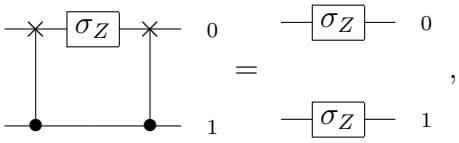
This example has 3 controls, but we are interested in any number greater or equal to 1. The one control case was dealt with in the previous section, so in this section we will only show how to express an mc_u2 as a product of single qubit rotations, CNOTs and 1c_u2's.

For any x^r denoting the labels of r distinct qubits, we will abbreviate a tensor product of r Z-Pauli matrices by:

$$\sigma_Z(x^r) = \prod_{j=0,1,\ldots,r-1} \sigma_Z(x_j) \tag{52}$$

For example, $\sigma_Z(1,3) = \sigma_Z(1)\sigma_Z(3)$

A useful identity is

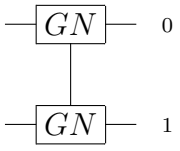


, (53)

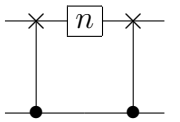
or, written in algebraic language,

$$\sigma_X(0)^{n(1)}\sigma_Z(0)\sigma_X(0)^{n(1)} = \sigma_Z(0,1)\ . \tag{54}$$

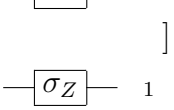
Define the "generalized n (GN)" $n(1,0)$ by

$n(1,0)$ =


(55)

=


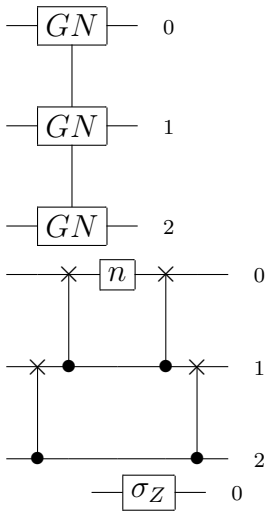
(56)

=
$\frac{1}{2}[1 -$


$]$ (57)

$$= \frac{1}{2}[1 - \sigma_Z(1,0)]\ . \tag{58}$$

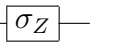
Define the "generalized-n (GN)" $n(2,1,0)$ by

$$n(2,1,0) \;=\;$$ 

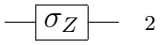
(59)

$$=$$

(60)

$$= \frac{1}{2}[1 -$$ 

$$]$$ (61)



$$= \frac{1}{2}[1 - \sigma_Z(2,1,0)] \; . \tag{62}$$

It's clear from the definitions of $n(1,0)$ and $n(2,1,0)$ how one can define by analogy a generalized-n denoted by $n(x^r)$, where the indices x^r denote r distinct qubits. Note that $n(x^r)$ is a diagonal matrix that contains ± 1 along its diagonal and is symmetric in its indices.

Note that

$$n(1)n(0) = \frac{1}{4}[1 - \sigma_Z(1)][1 - \sigma_Z(0)] \tag{63}$$

$$= \frac{1}{4}[1 - \underbrace{\sigma_Z(0)}_{1-2n(0)} - \underbrace{\sigma_Z(1)}_{1-2n(1)} + \underbrace{\sigma_Z(1,0)}_{1-2n(1,0)}] \tag{64}$$

$$= \frac{1}{2}[n(0) + n(1) - n(1,0)] \; . \tag{65}$$

Note also that

$$n(2)n(1,0) = \frac{1}{4}[1 - \sigma_Z(2)][1 - \sigma_Z(1,0)] \tag{66}$$

$$= \frac{1}{4}[1 - \sigma_Z(1,0) - \sigma_Z(2) + \sigma_Z(2,1,0)] \tag{67}$$

$$= \frac{1}{2}[n(1,0) + n(2) - n(2,1,0)] \; . \tag{68}$$

Therefore,

$$
\begin{aligned}
n(2)n(1)n(0) &= \frac{1}{2}n(2)[n(0)+n(1)-n(1,0)] && (69)\\
&= \frac{1}{2}[\underbrace{n(2)n(0)}_{\frac{1}{2}[n(2)+n(0)-n(2,0)]} + \underbrace{n(2)n(1)}_{\frac{1}{2}[n(2)+n(1)-n(2,1)]} - \underbrace{n(2)n(1,0)}_{\frac{1}{2}[n(1,0)+n(2)-n(2,1,0)]}] && (70)\\
&= \frac{1}{4}\left\{\begin{array}{l}[n(0)+n(1)+n(2)]\\ -[n(1,0)+n(2,0)+n(2,1)]\\ +n(2,1,0)\end{array}\right\} . && (71)
\end{aligned}
$$

It's clear that Eq.(65) for a tensor product of 2 n's and Eq.(71) for a tensor product of 3 n's can be generalized by induction to a formula that expresses a tensor product of an arbitrary number of n's as a linear combination of generalized-n's. That generalization is

$$
\prod_{r=0}^{R-1} n(r) = \frac{1}{2^{R-1}}\sum_{r=1}^{R}\sum_{y^r\in Comb_r(\{0,1,\ldots,R-1\})}(-1)^{r+1}n(y^r) , \qquad (72)
$$

where $Comb_r(S)$ denotes the r-length combinations of a set S. Eq.(72) can now be used to achieve the original goal of this section, which is to expand an mc_u2 as a product of CNOTs, single qubit rotations and 1c_u2's.

References

[1] A. Barenco, et al, "Elementary gates for quantum computation", https://arxiv.org/abs/quant-ph/9503016

[2] R.R. Tucci, "QC Paulinesia", http://arxiv.org/abs/quant-ph/0407215