arXiv:quant-ph/0407215 v1 27 Jul 2004

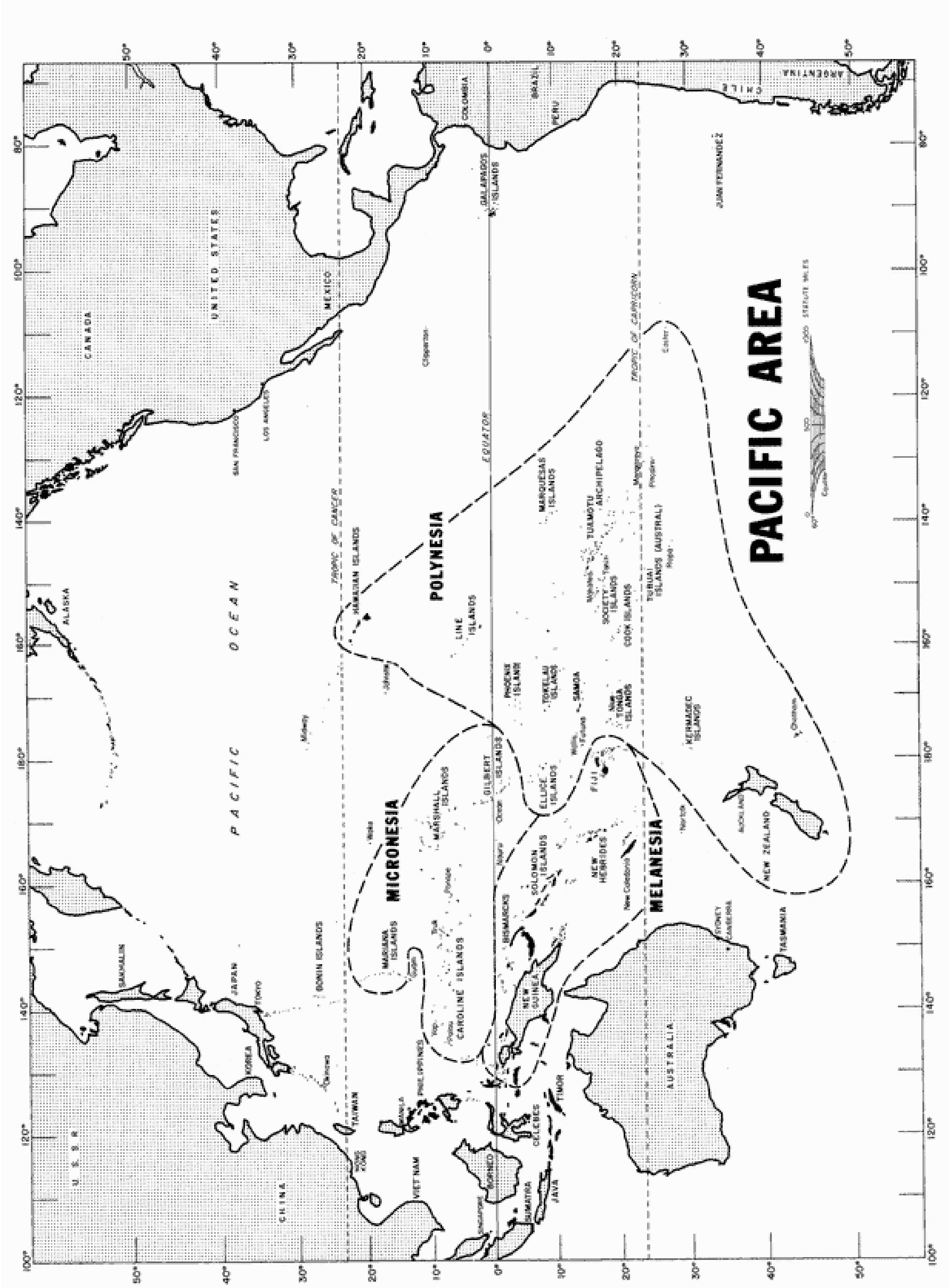
QC Paulinesia

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

August 24, 2006

An archipelago of identities, formed from the lava of Pauli Matrices, by the volcanic activity of Quantum Computing.

Figure 1: Aerial view of Bora Bora


PACIFIC AREA
POLYNESIA
MICRONESIA
MELANESIA
PACIFIC OCEAN
CANADA
UNITED STATES
MEXICO
ALASKA
U.S.S.R.
CHINA
JAPAN
KOREA
TAIWAN
VIET NAM
PHILIPPINES
BORNEO
SUMATRA
JAVA
CELEBES
TIMOR
NEW GUINEA
AUSTRALIA
TASMANIA
NEW ZEALAND
COLOMBIA
PERU
BRAZIL
CHILE
ARGENTINA
SAN FRANCISCO
LOS ANGELES
TOKYO
SYDNEY
CANBERRA
HAWAIIAN ISLANDS
LINE ISLANDS
MARQUESAS ISLANDS
TUAMOTU ARCHIPELAGO
SOCIETY ISLANDS
COOK ISLANDS
TUBUAI ISLANDS (AUSTRAL)
PHOENIX ISLANDS
TOKELAU ISLANDS
SAMOA
TONGA ISLANDS
KERMADEC ISLANDS
GILBERT ISLANDS
ELLICE ISLANDS
FIJI
MARSHALL ISLANDS
CAROLINE ISLANDS
MARIANA ISLANDS
BONIN ISLANDS
SOLOMON ISLANDS
NEW HEBRIDES
BISMARCKS
GALAPAGOS ISLANDS
JUAN FERNANDEZ
SAKHALIN
TROPIC OF CANCER
EQUATOR
TROPIC OF CAPRICORN

Contents

1 Introduction

This document is not a full course in Quantum Computing. My goal in producing it was to create a collection of qubit circuit identities that are used in Quantum Computing. Mathematicians and Physicists may consider it as being analogous to a Table of Integrals or a Mathematical Handbook such as Gradshteyn & Ryzhik or Abramowitz & Stegun. Computer Programmers may think of it as a scrapbook of code snippets that are elegant, instructive, well documented, and useful. Electronics experts may view it as a compendium of circuits for performing a large assortment of tasks.

The vast majority of the circuit identities collected in this work were not discovered for the first time by me, and I take no credit for discovering them. In producing this document, I am acting as a collector, not as a discoverer.

I plan to continue adding qubit circuit identities to this collection, and to release future versions of this document containing the new specimens. For example, there are some nice identities involving quantum error correction and quantum compiling that I have not included yet, but which I plan to include in future versions. Suggestions and comments are welcomed and appreciated.

This document benefitted greatly from the wonderful LaTeX macros: QCircuit (by B. Eastin, S. T. Flammia) and XYPic (by K.H. Rose and R.R. Moore), on which QCircuit is based.

2 Notation

Let $Bool = \{0, 1\}$. For integers a and b such that $a \leq b$, let $Z_{a,b} = \{a, a+1, a+2, \ldots b\}$.

$\delta(x, y)$ and δ^x_y will both denote the Kronecker delta function. It equals one when $x = y$ and zero otherwise.

For any statement $\mathcal{S}$, we define the truth function $\theta(\mathcal{S})$ to equal 1 if $\mathcal{S}$ is true and 0 if $\mathcal{S}$ is false. For example, $\theta(x > 0)$ represents the unit step function and $\delta(x, y) = \theta(x = y)$ the Kronecker delta function.

$\oplus$ will denote addition mod 2. Hence, for any $a, b \in Bool$, $a \oplus b = a + b - 2ab$ and $(-1)^{a\oplus b} = (-1)^{a+b}$. When speaking of bits with states 0 and 1, we will often use an overline to represent the opposite state: $\bar{0} = 1$, $\bar{1} = 0$. Note that if $x, k \in Bool$, then $\sum_k (-1)^{kx} = 1 + (-1)^x = 2\delta(x, 0)$. For $x \in Bool$, $\delta(x, 1) = x$.

We will often use $N_S = 2^{N_B}$, where N_B stands for number of bits and N_S for number of states. We will use lower case Latin letters $a, b, c \ldots \in Bool$ to represent bit values and lower case Greek letters $\alpha, \beta, \gamma, \ldots \in Z_{0,N_B-1}$ to represent bit positions.

Given a binary vector $\vec{x} \in Bool^{N_B}$, if its components are labelled as follows: $\vec{x} = (x_{N_B-1}, x_{N_B-2}, \ldots, x_1, x_0)$, then we will say that the components of $\vec{x}$ are labelled naturally. For some applications, it is very convenient to use natural labelling. For other applications, it doesn't much matter whether we use natural labelling or not. In cases where it doesn't matter, we may use other common labellings such as $\vec{x} = (x_1, x_2, \ldots, x_{N_B})$.

Let $\vec{\nu} = (N_B - 1, N_B - 2, \ldots, 1, 0)$, and $2^{\vec{\nu}} = (2^{N_B-1}, 2^{N_B-2}, \ldots, 2^1, 2^0)$.

Given any $x \in Z_{0,N_S-1}$, we can write $x = \sum_{i=0}^{N_B-1} 2^i x_i$. If we define the naturally labelled binary vector $\vec{x} = (x_{N_B-1}, \ldots, x_1, x_0)$, then $x = 2^{\vec{\nu}} \cdot \vec{x}$. We call $\vec{x} = (x_{N_B-1}, \ldots, x_1, x_0)$ the binary representation of x and denote it by $bin(x)$.

Given any naturally labelled binary vector $\vec{x} = (x_{N_B-1}, \ldots, x_1, x_0)$, we can write $x = 2^{\vec{\nu}} \cdot \vec{x}$. We call $x \in Z_{0,N_S-1}$ the decimal representation of $\vec{x}$ and denote it by $dec(\vec{x})$.

If $\vec{x}, \vec{y} \in Bool^{N_B}$, we will use $\vec{x} \cdot \vec{y} = \sum_{i=0}^{N_B-1} x_i y_i$, where the addition is normal, not mod 2.

We define the single-qubit states $|0\rangle$ and $|1\rangle$ by

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \ , \ \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \ . \tag{1}$$

Given any $\vec{x} = (x_1, x_2, \ldots, x_{N_B}) \in Bool^{N_B}$, and given a vector of distinct qubit labels $\vec{\beta} = (\beta_1, \beta_2, \ldots, \beta_{N_B})$, we define the N_B-qubit state $|\vec{x}\rangle$ as the following tensor product

$$|\vec{x}\rangle = |\vec{x}\rangle_{\vec{\beta}} = |x_1\rangle_{\beta_1} |x_2\rangle_{\beta_2} \ldots |x_{N_B}\rangle_{\beta_{N_B}} = |x_1\rangle \otimes |x_2\rangle \ldots \otimes |x_{N_B}\rangle \ . \tag{2}$$

For example,

$$|01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \ . \tag{3}$$

With natural labelling, we would use $\vec{x} = (x_{N_B-1}, \ldots, x_1, x_0)$, $\vec{\beta} = \vec{\nu}$ and $x = \sum_{i=0}^{N_B-1} 2^i x_i$. Instead of Eq.(2), we would have

$$|x\rangle = |\vec{x}\rangle = |\vec{x}\rangle_{\vec{\nu}} = |x_{N_B-1}\rangle_{N_B-1} \ldots |x_1\rangle_1 |x_0\rangle_0 = |x_{N_B-1}\rangle \otimes \ldots \otimes |x_1\rangle \otimes |x_0\rangle \ . \tag{4}$$

Of course, any N_B qubit state can be obtained as a linear combination of the states $|\vec{x}\rangle$ for all $\vec{x} \in Bool^{N_B}$.

I_r will represent the r dimensional unit matrix, for any integer $r \geq 1$.

Suppose $\vec{\beta} = (\beta_1, \beta_2, \ldots, \beta_{N_B})$ is a vector of bit labels, $(M_1, M_2, \ldots, M_{N_B})$ is a vector of 2×2 complex matrices, and $(\phi_1, \phi_2, \ldots, \phi_{N_B})$ is a vector of 2-dimensional complex column vectors. For $i \in Z_{1,N_B}$, we define $M_i(\beta_i)$ by

$$M_i(\beta_i) = I_2 \otimes \cdots \otimes I_2 \otimes M_i \otimes I_2 \otimes \cdots \otimes I_2 \ , \tag{5}$$

where the matrix M_i on the right hand side is located at bit position i (counting from left to right, starting at 1) in the tensor product of N_B 2×2 matrices. We often define a product operator $M(\vec{\beta})$ by

$$M(\vec{\beta}) = \prod_{i=1}^{N_B} M_i(\beta_i) = M_1(\beta_1) \otimes M_2(\beta_2) \otimes \ldots M_{N_B}(\beta_{N_B}) \ , \tag{6}$$

and a product state $|\phi\rangle_{\vec{\beta}}$

$$|\phi\rangle_{\vec{\beta}} = \prod_{i=1}^{N_B} |\phi_i\rangle_{\beta_i} = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \ldots |\phi_{N_B}\rangle \ . \tag{7}$$

For example, we might find it useful to define an operator $M(\vec{\beta})$ and a state $|\phi\rangle_{\vec{\beta}}$ by

$$M(\vec{\beta}) = \prod_{i=1}^{N_B} \sigma_X(\beta_i) = \sigma_X \otimes \sigma_X \otimes \ldots \otimes \sigma_X \ , \tag{8}$$

$$|\phi\rangle_{\vec{\beta}} = |0\rangle_{\vec{\beta}} = \prod_{i=1}^{N_B} |0\rangle_{\beta_i} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = [1, 0, 0, \ldots, 0]^T \ . \tag{9}$$

With natural labelling, we use $\vec{\beta} = \vec{\nu}$. Let $(M_{N_B-1}, \ldots, M_1, M_0)$ be a vector of 2×2 complex matrices, and let $(\phi_{N_B-1}, \ldots, \phi_1, \phi_0)$ be a vector of 2-dimensional complex column vectors. With natural labelling, for $i \in Z_{0,N_B-1}$, we define $M_i(i)$ by

$$M_i(i) = I_2 \otimes \cdots \otimes I_2 \otimes M_i \otimes I_2 \otimes \cdots \otimes I_2 \ , \tag{10}$$

where the matrix M_i on the right hand side is located at bit position i (counting from right to left, starting at 0) in the tensor product of N_B 2×2 matrices. We often define a product operator $M(\vec{\nu})$ by

$$M(\vec{\nu}) = \prod_{i=0}^{N_B-1} M_i(i) = M_{N_B-1}(N_B - 1) \otimes \ldots \otimes M_1(1) \otimes M_0(0) \ , \tag{11}$$

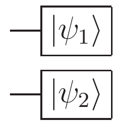
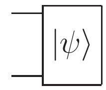
and a product state $|\phi\rangle_{\vec{\nu}}$

$$|\phi\rangle_{\vec{\nu}} = \prod_{i=0}^{N_B-1} |\phi_i\rangle_i = |\phi_{N_B-1}\rangle \otimes \ldots \otimes |\phi_1\rangle \otimes |\phi_0\rangle \ . \tag{12}$$

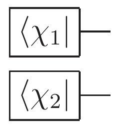
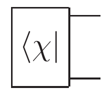
Next we explain our circuit diagram notation. In our qubit circuit diagrams, each horizontal wire represents a single qubit (except when stated explicitly that the wire represents several qubits). Different wires represent different qubits. We label single qubit wires by Greek letters or by integers as follows:

$$\begin{array}{l} - \ \alpha \\ - \ \beta \\ - \ \gamma \\ - \ \delta \\ \ \vdots \end{array} \quad , \quad \begin{array}{l} - \ 0 \\ - \ 1 \\ - \ 2 \\ - \ 3 \\ \ \vdots \end{array} \quad . \tag{13}$$

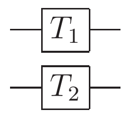
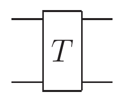
Thus, the first (topmost) wire is labelled either α or 0, the second wire is labelled either β or 1, and so forth. For some special applications, we label qubits differently from Eq.(13). For example, we might label the first two wires α_1, α_2, and the next two wires β_1, β_2, or we might want to label the first wire (α_1, α_2), and make it represent two qubits. In cases where bit labelling is different from Eq.(13), this will be stated explicitly. Bras are represented by

$$|\psi_1\rangle_\alpha |\psi_2\rangle_\beta =$$  , $$|\psi\rangle_{\alpha\beta} =$$  , (14)

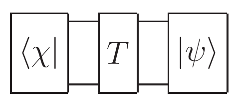
and kets by

$$\langle\chi_1|_\alpha \langle\chi_2|_\beta =$$  , $$\langle\chi|_{\alpha\beta} =$$  . (15)

Operators are represented by

$$T_1(\alpha)T_2(\beta) =$$  , $$T(\alpha,\beta) =$$  . (16)

Matrix elements are represented by combining the above rules for bras, kets, and operators. For example,

$$\langle\chi|_{\alpha\beta} T(\alpha,\beta) |\psi\rangle_{\alpha\beta} =$$  . (17)

Note that in our circuit diagrams, time flows from the right to the left of the diagram. Careful: Many workers in Quantum Computing draw their diagrams so that time flows from left to right. We eschew their convention because it forces one to reverse the order of the operators every time one wishes to convert between a circuit diagram and its algebraic equivalent in Dirac Notation.

Next, we will introduce a slight enhancement to the standard Dirac Notation. Given a ket $|\psi\rangle$, if we can find an operator Ω such that $|\psi\rangle$ is a unique (up to a scalar factor) eigenvector of Ω with eigenvalue λ, then we will sometimes denote $|\psi\rangle$ by $|\Omega = \lambda\rangle$. Sometimes, in order to specify $|\psi\rangle$ uniquely, one needs to find a complete set of commuting operators $\{\Omega_i : i \in Z_{1,N}\}$ such that $\Omega_i |\psi\rangle = \lambda_i |\psi\rangle$ for all i, and then we can denote $|\psi\rangle$ by $\left|\vec{\Omega} = \vec{\lambda}\right\rangle$. Note that if U is a unitary operator that acts on the same Hilbert space as an operator Ω, then $\left|U\Omega U^\dagger = \lambda\right\rangle = U|\Omega = \lambda\rangle$. If operator Ω has an eigenspace with eigenvalue λ, then we denote the projector onto that eigenspace by $\pi(\Omega = \lambda)$. If the eigenspace is one dimensional, then $\pi(\Omega = \lambda) = |\Omega = \lambda\rangle\langle\Omega = \lambda|$. If the eigenspace has dimension greater than one, then we can always find an orthonormal basis $\{|\psi^i_\lambda\rangle : i \in S\}$ for the eigenspace, and then $\pi(\Omega = \lambda) = \sum_{i\in S} |\psi^i_\lambda\rangle\langle\psi^i_\lambda|$. Note that if U is a unitary operator that acts on the same Hilbert space as operator Ω, then $U\pi(\Omega = \lambda)U^\dagger = \pi(U\Omega U^\dagger = \lambda)$.

The Pauli matrices are defined by:

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{18}$$

More information about the Pauli matrices may be found in the section entitled Pauli Matrices.

We will often abbreviate $n-$fold tensor products of Pauli matrices as follows. If $w_1, w_2, \ldots, w_n \in \{X, Y, Z\}$, and $b_1, b_2, \ldots, b_n \in Bool$, then let

$$\sigma^{b_1,b_2,\ldots,b_n}_{w_1,w_2,\ldots,w_n} = \sigma^{b_1}_{w_1} \otimes \sigma^{b_2}_{w_2} \otimes \ldots \otimes \sigma^{b_n}_{w_n} \ . \tag{19}$$

For example, $\sigma^{1,0,1}_{XYY} = {\sigma_X}^1 \otimes {\sigma_Y}^0 \otimes {\sigma_Y}^1$. Equivalently, for n bits $\vec{\alpha} = (\alpha_1, \alpha_2, \ldots \alpha_n)$,

$$\sigma^{b_1,b_2,\ldots,b_n}_{w_1,w_2,\ldots,w_n}(\vec{\alpha}) = \prod_{i=1}^{n} \sigma^{b_i}_{w_i}(\alpha_i) \ . \tag{20}$$

Also let

$$\sigma_{w_1,w_2,\ldots,w_n} = \sigma^{1,1,\ldots,1}_{w_1,w_2,\ldots,w_n} = \sigma_{w_1} \otimes \sigma_{w_2} \otimes \ldots \otimes \sigma_{w_n} \ . \tag{21}$$

For example, $\sigma_{XYY} = \sigma^{1,1,1}_{XYY} = \sigma_X \otimes \sigma_Y \otimes \sigma_Y$.

It is sometimes convenient to define the following operator for any $x, z \in Bool$ and any qubit α:

$$\Lambda^{x,z}(\alpha) = {\sigma_X}^x(\alpha){\sigma_Z}^z(\alpha) \ . \tag{22}$$

Note that $\Lambda^{x,z\dagger} = (-1)^{xz}\Lambda^{x,z}$, and $\Lambda^{00} = 1$, $\Lambda^{10} = \sigma_X$, $\Lambda^{11} = (-i)\sigma_Y$, $\Lambda^{00} = \sigma_Z$. $\Lambda^{x,z}$ arises, for example, when dealing with Bell states.

For any $j \in Bool$ and $w_1, w_2 \in \{X, Y, Z\}$, let $\Pi^j_{w_1,w_2}$ be the projection operator that projects the 2 qubit Hilbert space onto the eigenspace of σ_{w_1,w_2} with eigenvalue $(-1)^j$. Thus,

$$\Pi^j_{w_1,w_2} = \pi[\sigma_{w_1,w_2} = (-1)^j] \ . \tag{23}$$

Note that

$$\sigma_{ZZ} = \sigma_Z \otimes \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = diag(1, -1, -1, 1) \ . \tag{24}$$

From Eq.(24), it is clear that for any $j, a, b \in Bool$,

$$\Pi^j_{ZZ} |a, b\rangle = \delta^j_{a\oplus b} |a, b\rangle \ . \tag{25}$$

3 Pauli Matrices

The Pauli matrices are defined by:

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ , \ \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \ , \ \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ . \tag{26}$$

Sometimes one refers to $\sigma_X, \sigma_Y, \sigma_Z$ as $\sigma_1, \sigma_2, \sigma_3$, respectively. One can then use σ_0 to denote the 2×2 identity matrix. It is often convenient to use the vector of Pauli matrices $\vec{\sigma} = (\sigma_X, \sigma_Y, \sigma_Z)$.

All 3 Pauli matrices are their own inverses:

$$\sigma_X{}^2 = \sigma_Y{}^2 = \sigma_Z{}^2 = 1 \ . \tag{27}$$

Distinct Pauli matrices anticommute. For example,

$$\sigma_X \sigma_X = -\sigma_Y \sigma_X \ . \tag{28}$$

It is easy to check that

$$\sigma_X \sigma_Y = i\sigma_Z \ , \quad \sigma_Y \sigma_Z = i\sigma_X \ , \quad \sigma_Z \sigma_X = i\sigma_Y \ . \tag{29}$$

Note that Eqs.(27), (28) and (29) specify a 3×3 multiplication table for the 3 Pauli matrices with each other.

For $w \in \{X, Y, Z\}$, if $|+_w\rangle$ and $|-_w\rangle$ represent the eigenvectors of σ_w with eigenvalues $+1$ and -1, respectively, then

$$|+_X\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \ , \quad |-_X\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \ , \tag{30}$$

$$|+_Y\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \ , \quad |-_Y\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \ , \tag{31}$$

$$|+_Z\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ , \quad |-_Z\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ . \tag{32}$$

We define

$$|0\rangle = |+_Z\rangle \ , \tag{33}$$

and

$$|1\rangle = |-_Z\rangle \ . \tag{34}$$

We will use n to denote the "number operator". Thus,

$$n = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = |-_Z\rangle \langle -_Z| = \frac{1 - \sigma_Z}{2} \ , \tag{35}$$

and

$$\overline{n} = 1 - n = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |+_Z\rangle \langle +_Z| = \frac{1 + \sigma_Z}{2} \ . \tag{36}$$

Since n and σ_Z are diagonal, it is easy to see that

$$\sigma_Z = (-1)^n = 1 - 2n \ . \tag{37}$$

Most of the definitions and results stated so far for σ_Z have counterparts for σ_Z and σ_Y. The counterpart results can be easily proven by applying a rotation that interchanges the coordinate axes. Let $w \in \{X, Y, Z\}$. If $|+_w\rangle$ and $|-_w\rangle$ represent the eigenvectors of σ_w with eigenvalues $+1$ and -1, respectively, then we define

$$|0_w\rangle = |+_w\rangle \ , \tag{38}$$

and

$$|1_w\rangle = |-_w\rangle \ . \tag{39}$$

Let

$$n_w = |-_w\rangle \langle -_w| = \frac{1 - \sigma_w}{2} \ , \tag{40}$$

$$\overline{n}_w = 1 - n_w = |+_w\rangle \langle +_w| = \frac{1 + \sigma_w}{2} \ . \tag{41}$$

As when $w = Z$, one has

$$\sigma_w = (-1)^{n_w} = 1 - 2n_w \ . \tag{42}$$

Note that whenever we use $|0\rangle$, $|1\rangle$ or n , without an X, Y or Z subscript, the subscript Z should be inferred.

The one bit Hadamard matrix is defined by:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\sigma_X + \sigma_Z) \ . \tag{43}$$

It is easy to check that

$$H^2 = 1 \ , \tag{44}$$

$$H\sigma_X H = \sigma_Z \ , \quad H\sigma_Z H = \sigma_X \ , \tag{45}$$

$$|0_X\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = H\,|0\rangle \ , \tag{46}$$

$$|1_X\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = H\,|1\rangle \ . \tag{47}$$

The matrix i^n is defined by

$$i^n = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} . \tag{48}$$

It is easy to check that

$$(i^n)^2 = \sigma_Z , \tag{49}$$

$$i^n \sigma_X i^{-n} = \sigma_Y , \quad i^{-n} \sigma_X i^n = -\sigma_Y . \tag{50}$$

Note that for $a, b \in Bool$,

$$\sigma_X{}^b \left|a\right\rangle = \left|a \oplus b\right\rangle , \tag{51}$$

$$\sigma_Z{}^b \left|a\right\rangle = (-1)^{ab} \left|a\right\rangle , \tag{52}$$

$$\left\langle a\right| H \left|b\right\rangle = \frac{(-1)^{ab}}{\sqrt{2}} . \tag{53}$$

A general qubit rotation is defined by $e^{i\vec{\theta}\cdot\vec{\sigma}}$, where $\vec{\theta}$ is a 3 dimensional real vector. For any real number θ,

$$e^{i\theta\sigma_Z} = \cos\theta + i\sigma_Z \sin\theta . \tag{54}$$

Eq.(54) can be proven by expressing both sides of it as a power series. Applying a rotation to Eq.(54), it becomes

$$e^{i\vec{\theta}\cdot\vec{\sigma}} = \cos\theta + i\vec{\sigma}\cdot\hat{\theta}\sin\theta , \tag{55}$$

where $\vec{\theta}$ is a 3 dimensional real vector, θ is its magnitude, and $\hat{\theta} = \vec{\theta}/\theta$.

4 Hadamard Matrices

The 1 bit Hadamard matrix is defined by

$$H_1 = \frac{1}{\sqrt{2}} \begin{array}{c|cc} & {\scriptstyle 0} & {\scriptstyle 1} \\ \hline {\scriptstyle 0} & 1 & 1 \\ {\scriptstyle 1} & 1 & \text{-1} \end{array} . \tag{56}$$

The N_B-bit Hadamard matrix is defined as the N_B-fold tensor product of H_1:

$$H_{N_B} = \underbrace{H_1 \otimes H_1 \otimes \ldots \otimes H_1}_{N_B \text{ factors}} . \tag{57}$$

For example, for $N_B = 2$,

$$H_2 = \frac{1}{2} \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 1 & 1 & 1 \\ 01 & 1 & -1 & 1 & -1 \\ 10 & 1 & 1 & -1 & -1 \\ 11 & 1 & -1 & -1 & 1 \end{array} , \quad (58)$$

where we have labelled the rows and columns with binary numbers in increasing dictionary order. Equivalently, for bits $\vec{\alpha} = (\alpha_1, \alpha_1, \ldots, \alpha_{N_B})$,

$$H_{N_B}(\vec{\alpha}) = \prod_{i=1}^{N_B} H_1(\alpha_i) \ . \quad (59)$$

We will often use a plain H to represent H_1. Since $(H_1)_{b,b'} = \frac{(-1)^{bb'}}{\sqrt{2}}$ for $b, b' \in Bool$, it follows that

$$(H_{N_B})_{\vec{b},\vec{b}'} = \frac{(-1)^{\vec{b}\cdot\vec{b}'}}{\sqrt{2^{N_B}}} \quad (60)$$

for $\vec{b}, \vec{b}' \in Bool^{N_B}$. Since $H_1^2 = 1$ and $H_1^T = H_1$, where T=transpose, it follows that

$$H_{N_B}^2 = 1 \ , \quad (61)$$

and

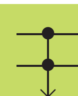
$$H_{N_B}^T = H_{N_B} \ . \quad (62)$$

5 CNOTs

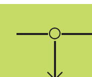
We define a CNOT (C = controlled, NOT = σ_X) by:

$$CNOT(\alpha \to \beta) = CNOT(\beta \leftarrow \alpha) = \sigma_X(\beta)^{n(\alpha)} = (-1)^{n(\alpha)n_X(\beta)} =$$  . (63)

α is called the **control qubit** and β is called the **target qubit**. The CNOT can be easily generalized to have more than one control qubit:

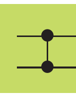
$$\sigma_X^{n(\alpha)n(\beta)}(\gamma) = (-1)^{n(\alpha)n(\beta)n_X(\gamma)} =$$  . (64)

Other operators related to CNOT are

$$\sigma_X(\beta)^{\overline{n}(\alpha)} = (-1)^{\overline{n}(\alpha)n_X(\beta)} =$$  , (65)

and

$$\sigma_Z{}^{n(\alpha)}(\beta) = \sigma_Z{}^{n(\beta)}(\alpha) = (-1)^{n(\alpha)n(\beta)} = \quad \text{(66)}$$



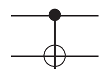
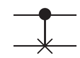
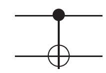
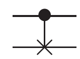
For any $a, b, c \in Bool$,

$$\sigma_X(\beta)^{n(\alpha)} \left|a, b\right\rangle_{\alpha\beta} = \left|a, b \oplus a\right\rangle \ , \tag{67}$$

$$\sigma_X^{n(\alpha)n(\beta)}(\gamma) \left|a, b, c\right\rangle_{\alpha\beta\gamma} = \left|a, b, c \oplus ab\right\rangle \ , \tag{68}$$

$$\sigma_X(\beta)^{\overline{n}(\alpha)} \left|a, b\right\rangle_{\alpha\beta} = \left|a, b \oplus \overline{a}\right\rangle \ , \tag{69}$$

$$(-1)^{n(\alpha)n(\beta)} \left|a, b\right\rangle_{\alpha\beta} = (-1)^{ab} \left|a, b\right\rangle \ . \tag{70}$$

Some workers represent a CNOT by  instead of . The  notation reminds us of the $\oplus$ in Eq.(67), whereas the  notation reminds us of the X in $\sigma_X(\beta)^{n(\alpha)}$.

Claim:

$$\sigma_X(\alpha)^{n(\beta)} = \sigma_X(\alpha)n(\beta) + \overline{n}(\beta) \ . \tag{71}$$

proof:
Check that both sides agree when $n(\beta)$ equals zero and one.
QED

Claim:

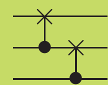
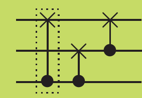
$$\sigma_X(\alpha)^{n(\beta)} = \frac{1}{2} \sum_{(x,z)\in Bool^2} \sigma_X{}^x(\alpha)\sigma_Z{}^z(\beta)(-1)^{xz} \ . \tag{72}$$

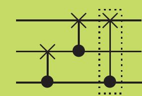
proof:

$$\begin{aligned}
\sigma_X(\alpha)^{n(\beta)} &= (-1)^{n_X(\alpha)n_Z(\beta)} && (73)\\
&= 1 - 2n_X(\alpha)n_Z(\beta) && (74)\\
&= 1 - 2\left(\frac{1-\sigma_X(\alpha)}{2}\right)\left(\frac{1-\sigma_Z(\beta)}{2}\right) && (75)\\
&= \frac{1}{2}[1 + \sigma_X(\alpha) + \sigma_Z(\beta) - \sigma_{XZ}(\alpha,\beta)] \ . && (76)
\end{aligned}$$

QED

Claim: (Permuting 2 CNOTs in a chain)

 $=$  (77)

$=$  . (78)

proof:
Let LHS and RHS stand for the left and right hand sides of Eq.(77). For $a, b, c \in Bool$,

$$
\begin{aligned}
LHS \left|a, b, c\right\rangle_{\alpha\beta\gamma} &= \sigma_X(\alpha)^{n(\beta)} \sigma_X(\beta)^{n(\gamma)} \left|a, b, c\right\rangle && (79)\\
&= \sigma_X(\alpha)^{n(\beta)} \left|a, b \oplus c, c\right\rangle && (80)\\
&= \left|a \oplus b \oplus c, b \oplus c, c\right\rangle \ . && (81)
\end{aligned}
$$

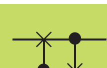
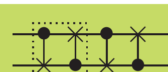
$$
\begin{aligned}
RHS \left|a, b, c\right\rangle_{\alpha\beta\gamma} &= \sigma_X(\alpha)^{n(\gamma)} \sigma_X(\beta)^{n(\gamma)} \sigma_X(\alpha)^{n(\beta)} \left|a, b, c\right\rangle && (82)\\
&= \sigma_X(\alpha)^{n(\gamma)} \sigma_X(\beta)^{n(\gamma)} \left|a \oplus b, b, c\right\rangle && (83)\\
&= \sigma_X(\alpha)^{n(\gamma)} \left|a \oplus b, b \oplus c, c\right\rangle && (84)\\
&= \left|a \oplus b \oplus c, b \oplus c, c\right\rangle \ . && (85)
\end{aligned}
$$

Finally, note that $CNOT(\gamma \rightarrow \alpha)$ and $CNOT(\gamma \rightarrow \beta) CNOT(\beta \rightarrow \alpha)$ commute.
QED

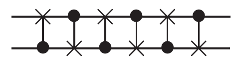
A mnemonic for remembering Eq.(77): On the left hand side of Eq.(77), we have a "chain" CNOT($\alpha \leftarrow \beta$) CNOT($\beta \leftarrow \gamma$) of CNOTs. When CNOT($\alpha \leftarrow \beta$) is moved to the right (or to the left), over CNOT($\beta \leftarrow \gamma$), it leaves behind as a "wake" the CNOT within the dotted box. The wake CNOT($\alpha \leftarrow \gamma$) points from the beginning to the end of the original chain CNOT($\alpha \leftarrow \beta$) CNOT($\beta \leftarrow \gamma$).

Throughout QC Paulinesia, we will refer to equations, like Eq.(77), wherein two operators are permuted and a wake is produced, as "wake identities". Eq.(77) is the first of many wake identities we will present.

Claim: (Permuting 2 CNOTs in a chain, when first and last qubit of chain are the same)

 $=$  . (86)

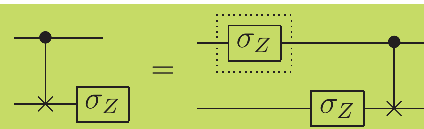
proof:
Eq.(86) is the same as

$1 =$  , (87)

which is just the fact that $E^2 = 1$, where E is the exchange operator.
QED

A mnemonic for remembering Eq.(86): On the left hand side of Eq.(86), we have a "loop chain" CNOT($\alpha \leftarrow \beta$) CNOT($\beta \leftarrow \alpha$) of CNOTs. When CNOT($\alpha \leftarrow \beta$) is moved over CNOT($\beta \leftarrow \alpha$), it leaves behind as a "wake" the two CNOTs within the dotted box. The wake and the non-wake parts are identical.

Claim:



. (88)

(Dotted box encloses wake.)
proof:
Let LHS and RHS stand for the left and right hand sides of Eq.(88). For $a, b \in Bool$,

$$\begin{aligned} LHS \left|a, b\right\rangle_{\alpha\beta} &= \sigma_X(\beta)^{n(\alpha)}\sigma_Z(\beta)\left|a, b\right\rangle & (89)\\ &= (-1)^b \left|a, b \oplus a\right\rangle \ . & (90) \end{aligned}$$

$$\begin{aligned} RHS \left|a, b\right\rangle_{\alpha\beta} &= \sigma_Z(\alpha)\sigma_Z(\beta)\sigma_X(\beta)^{n(\alpha)}\left|a, b\right\rangle & (91)\\ &= \sigma_Z(\alpha)\sigma_Z(\beta)\left|a, b \oplus a\right\rangle & (92)\\ &= (-1)^b \left|a, b \oplus a\right\rangle \ . & (93) \end{aligned}$$

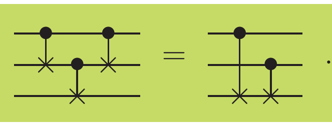
QED

alternative proof:

$$\begin{aligned} \sigma_X(\beta)^{n(\alpha)}\sigma_Z(\beta)\sigma_X(\beta)^{n(\alpha)} &= [\sigma_X(\beta)n(\alpha) + \overline{n}(\alpha)]\sigma_Z(\beta)[\sigma_X(\beta)n(\alpha) + \overline{n}(\alpha)] & (94)\\ &= \sigma_Z(\beta)[-\sigma_X(\beta)n(\alpha) + \overline{n}(\alpha)][\sigma_X(\beta)n(\alpha) + \overline{n}(\alpha)] & (95)\\ &= \sigma_Z(\beta)[-n(\alpha) + \overline{n}(\alpha)] & (96)\\ &= \sigma_Z(\beta)\sigma_Z(\alpha) \ . & (97) \end{aligned}$$

QED

Claim:

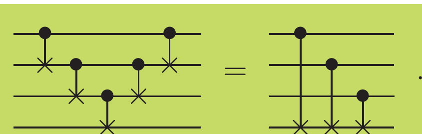


(98)

proof:
Apply Eq.(77) once to left hand side of Eq.(98).
QED

Note that in Eq.(98), the left hand side contains only nearest neighbor CNOTs, whereas the right hand side contains only commuting CNOTs.

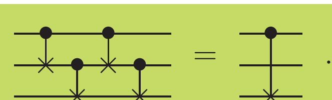
Claim:



(99)

proof:
Apply Eq.(77) twice to left hand side of Eq.(99).
QED

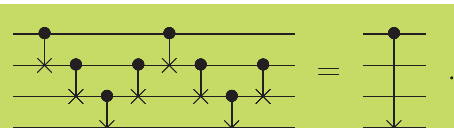
Claim:



(100)

proof:
This follows immediately from Eq.(98).
QED

Claim:



(101)

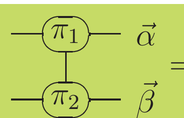
proof:
The product of left hand sides of Eqs.(98) and (99), equals the product of their right hand sides.
QED

Eqs.(100) and (101) suggest a way of converting a non-nearest neighbor CNOT into a sequence of nearest neighbor ones.

6 CNOT Generalizations

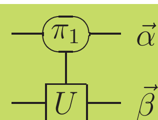
In this section, $\vec{\alpha}$, $\vec{\beta}$ and $\vec{\gamma}$ will denote disjoint sets of distinct qubits. That is, any two different components of the same vector, or two components of different vectors represent different qubits.

Suppose U is a unitary matrix. Furthermore, for $j = 1, 2$, suppose π_j is a projection operator (i.e., $\pi_j^2 = \pi_j$, the eigenvalues of π_j are all 0 or 1). Some examples of projection operators π_j that are of interest to us: 1, $n(\alpha)$, $n(\alpha)n(\beta)$, $n(\alpha)\overline{n}(\beta)$, $n(\alpha)n(\beta)n(\gamma)$, etc. It is convenient to generalize CNOT diagrammatic notation as follows. Let



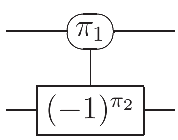
$$= (-1)^{\pi_1(\vec{\alpha})\pi_2(\vec{\beta})} \ , \tag{102}$$

and

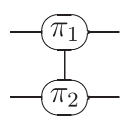


$$= U(\vec{\beta})^{\pi_1(\vec{\alpha})} \ . \tag{103}$$

We will refer to an operator of the form Eq.(103) as a **projector controlled unitary operator**, or simply as a **controlled U**, in analogy to a controlled NOT, for which $U = \sigma_X =$ the NOT operator. The set of operators of the form Eq.(102) is a subset of the set of operators of the form Eq.(103). Indeed, given any projection operator $\pi_2(\vec{\beta})$, one can always define the unitary operator $U(\vec{\beta}) = (-1)^{\pi_2(\vec{\beta})} = 1 - 2\pi_2(\vec{\beta})$. Hence,



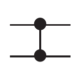
$=$



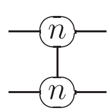
$$. \tag{104}$$

Special cases of Eqs.(102) and (103) are:

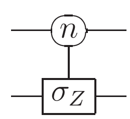
$(-1)^{n(\alpha)n(\beta)} =$



$=$

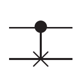


$=$

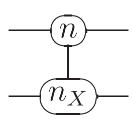


$$, \tag{105}$$

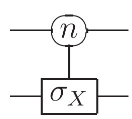
$\sigma_X(\beta)^{n(\alpha)} =$



$=$

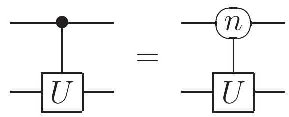


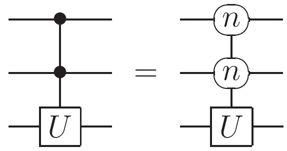
$=$



$$, \tag{106}$$

and, for any 2×2 unitary matrix U:

$U(\beta)^{n(\alpha)} =$  , (107)

$U(\gamma)^{n(\alpha)n(\beta)} =$  . (108)

We will refer to the operator of Eq.(107) as an n^1 **controlled U**, and to the operator of Eq.(108) as an n^2 **controlled U**.

Suppose U is any 2×2 unitary matrix. It can always be diagonalized as follows:

$$U = V diag(e^{i\theta_1}, e^{i\theta_2})V^\dagger \ , \tag{109}$$

where θ_1, θ_2 are reals numbers and V is a unitary matrix. If we set

$$\Delta = \frac{\theta_1 - \theta_2}{2} \ , \tag{110}$$

and

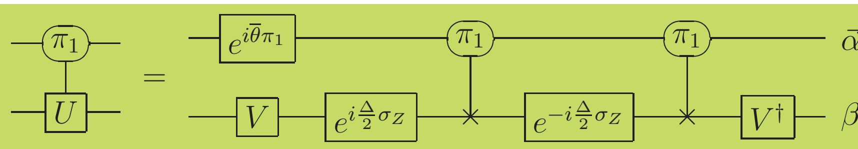
$$\overline{\theta} = \frac{\theta_1 + \theta_2}{2} \ , \tag{111}$$

then

$$U = e^{i\overline{\theta}} V e^{i\Delta\sigma_Z} V^\dagger \ . \tag{112}$$

Claim:

For any 2×2 unitary matrix $U(\beta)$ given by Eq.(112), and projection operator $\pi_1(\vec{\alpha})$,

 . (113)

proof:
Check that both sides agree when π_1 equals 0 and 1.
QED

alternative proof:

$$U(\beta)^{n(\alpha)} = e^{i\overline{\theta} n(\alpha)} V(\beta) e^{i\Delta\sigma_Z(\beta)n(\alpha)} V(\beta)^\dagger \ . \tag{114}$$

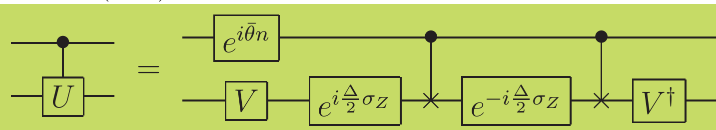
$$e^{i\Delta\sigma_Z(\beta)n(\alpha)} = e^{i\Delta\sigma_Z(\beta)\frac{1}{2}[1-\sigma_Z(\alpha)]} \quad (115)$$

$$= e^{i\frac{\Delta}{2}\sigma_Z(\beta)}e^{-i\frac{\Delta}{2}\sigma_Z(\beta)\sigma_Z(\alpha)} \quad (116)$$

$$= e^{i\frac{\Delta}{2}\sigma_Z(\beta)}\sigma_X(\beta)^{n(\alpha)}e^{-i\frac{\Delta}{2}\sigma_Z(\beta)}\sigma_X(\beta)^{n(\alpha)} \ . \quad (117)$$

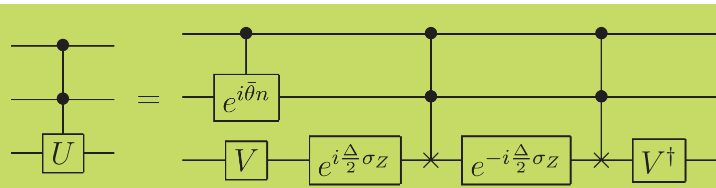
This proof still holds if we replace $n(\alpha)$ by $\pi_1(\vec{\alpha})$ and $\sigma_Z(\alpha)$ by $(-1)^{\pi_1(\vec{\alpha})}$.
QED

Examples of Eq.(113) are:



, (118)

and

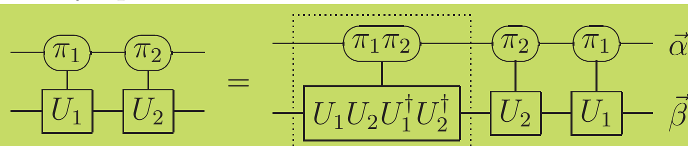


. (119)

Eqs.(118) and (119) suggest a way of converting any n^r controlled U, for an integer $r \geq 1$, into a sequence of gates containing no controlled U's but containing n^s controlled NOTs, where $s \leq r$.

Claim: (Permuting two projector controlled U's)

Suppose $\pi_1(\vec{\alpha}), \pi_2(\vec{\alpha})$ are commuting ($[\pi_1, \pi_2] = 0$) projection operators and $U_1(\vec{\beta}), U_2(\vec{\beta})$ are unitary operators. Then



. (120)

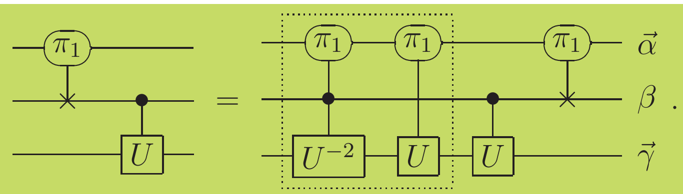
(Dotted box encloses wake.) Algebraically,

$$U_1(\vec{\beta})^{\pi_1(\vec{\alpha})}U_2(\vec{\beta})^{\pi_2(\vec{\alpha})} = (U_1U_2U_1^\dagger U_2^\dagger)^{\pi_1\pi_2}U_2^{\pi_2}U_1^{\pi_1} \ . \quad (121)$$

proof:
Check that both sides of Eq.(120) agree when (π_1, π_2) equals each element of $Bool^2$.
QED

Claim:

For any projection operator $\pi_1(\vec{\alpha})$ and unitary matrix $U(\vec{\gamma})$,



(122)

(Dotted box encloses wake.)

proof:

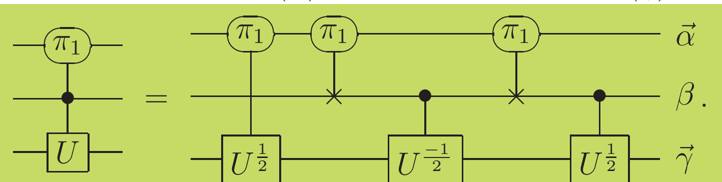
Consider Eq.(120) with the following replacements: $U_1 \rightarrow \sigma_X(\beta)$, $U_2 \rightarrow U(\vec{\gamma})^{n(\beta)}$, $\pi_2 \rightarrow 1$. Thus,

$$U_1 U_2 U_1^\dagger U_2^\dagger \rightarrow \sigma_X(\beta) U(\vec{\gamma})^{n(\beta)} \sigma_X(\beta) U(\vec{\gamma})^{-n(\beta)} = U(\vec{\gamma})^{\overline{n}(\beta) - n(\beta)} = U(\vec{\gamma})^{1-2n(\beta)} \ . \quad (123)$$

QED

Claim:

For any projection operator $\pi_1(\vec{\alpha})$ and unitary matrix $U(\vec{\gamma})$,



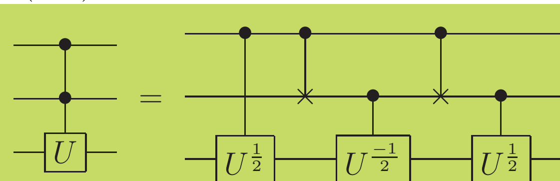
(124)

proof:

Apply Eq.(122) to the right hand side of Eq.(124) to permute $\sigma_X(\beta)^{\pi_1(\vec{\alpha})}$ and $U(\vec{\gamma})^{\frac{-1}{2} n(\beta)}$.

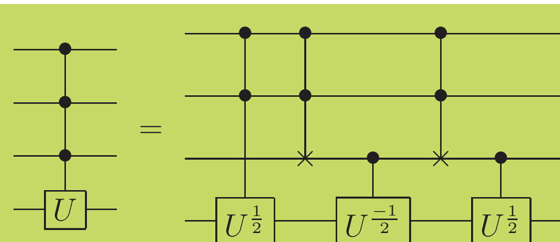
QED

Examples of Eq.(124) are



, (125)

and

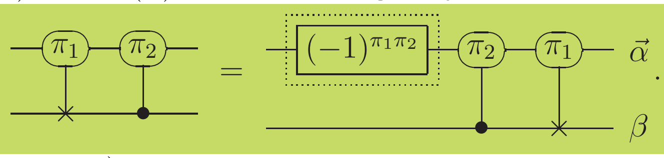


. (126)

Eqs.(125) and (126) suggest a way of converting an n^r controlled U, for an integer $r \geq 2$, into a sequence of gates that contains no controlled U's except n^1 controlled U's.

Claim:

Suppose $\pi_1(\vec{\alpha})$ and $\pi_2(\vec{\alpha})$ are commuting projection operators. Then



(127)

(Dotted box encloses wake.)

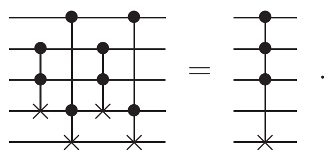
proof:

Consider Eq.(120) with the following replacements: $U_1 \to \sigma_X(\beta)$, $U_2 \to \sigma_Z(\beta)$. Thus,

$$U_1 U_2 U_1^\dagger U_2^\dagger \to \sigma_X \sigma_Z \sigma_X \sigma_Z = -1 \ . \tag{128}$$

QED

Eq.(127) can be used to transform sequences of n^r controlled NOTs. For example, the following identity can be easily proven by applying Eq.(127):

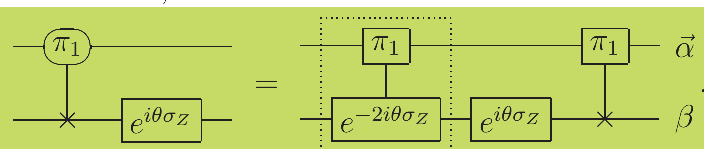


(129)

Note that Eq.(129) reduces an n^3 controlled NOT into a sequence of n^2 controlled NOTs.

Claim:

For any real number θ,



(130)

(Dotted box encloses wake.)

proof:

Consider Eq.(120) with the following replacements: $U_1 \to \sigma_X(\beta)$, $U_2 \to e^{i\theta\sigma_Z(\beta)}$, $\pi_2 \to 1$. Thus,

$$U_1 U_2 U_1^\dagger U_2^\dagger \to \sigma_X(\beta) e^{i\theta\sigma_Z(\beta)} \sigma_X(\beta) e^{-i\theta\sigma_Z(\beta)} = e^{-2i\theta\sigma_Z(\beta)} \ . \tag{131}$$

QED

7 Exchanger

We define the Exchanger (a.k.a. Swapper or Exchange Operator or Bit Transposition) by

$$E(\alpha,\beta)\,|a,b\rangle_{\alpha\beta} = |b,a\rangle_{\alpha\beta}\ , \tag{132}$$

for all $a, b \in Bool$. Therefore

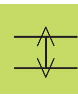
$$E(\alpha,\beta) = E(\beta,\alpha)\ , \tag{133}$$

and

$$E(\alpha,\beta)^2 = 1\ . \tag{134}$$

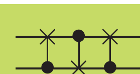
Throughout QC Paulinesia, we will represent Exchanger by

$$E(\alpha,\beta) = \tag{135}$$



Claim:

$$E(\alpha,\beta) = \sigma_X(\alpha)^{n(\beta)}\sigma_X(\beta)^{n(\alpha)}\sigma_X(\alpha)^{n(\beta)} = \tag{136}$$

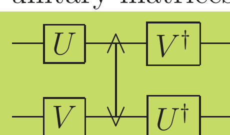


proof:

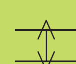
$$\begin{aligned}
\sigma_X(\alpha)^{n(\beta)}\sigma_X(\beta)^{n(\alpha)}\sigma_X(\alpha)^{n(\beta)}\,|a,b\rangle_{\alpha\beta} &= \sigma_X(\alpha)^{n(\beta)}\sigma_X(\beta)^{n(\alpha)}\,|a\oplus b, b\rangle & (137)\\
&= \sigma_X(\alpha)^{n(\beta)}\,|a\oplus b, a\rangle & (138)\\
&= |b,a\rangle\ . & (139)
\end{aligned}$$

QED

Claim: If U and V are 2×2 unitary matrices, then



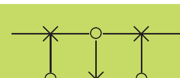
$$= \tag{140}$$



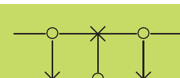
proof:
Obvious.
QED

Claim:

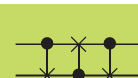
$$=$$



$$=$$

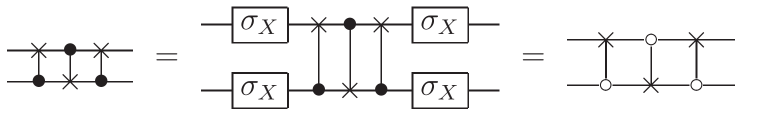


$$=$$



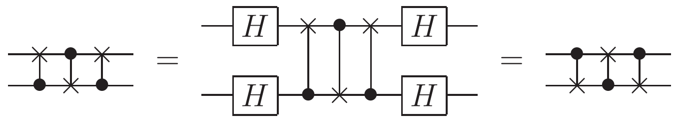
$$\tag{141}$$

proof:
By virtue of Eq.(140),



(142)

Likewise,



(143)

QED

Claim:

$$E(\alpha,\beta) = [n(\alpha)n(\beta) + \overline{n}(\alpha)\overline{n}(\beta)] + \sigma_X(\alpha)\sigma_X(\beta)[n(\alpha)\overline{n}(\beta) + \overline{n}(\alpha)n(\beta)] \; . \tag{144}$$

proof:
Let RHS be the right hand side of Eq.(144). For any $a, b \in Bool$, if $a = b$, $RHS\,|a,b\rangle = |a,b\rangle$, whereas when $a \neq b$, $RHS\,|a,b\rangle = \left|\overline{a},\overline{b}\right\rangle$.
QED

For any $x, z \in Bool$ and bit α, let $\Lambda^{x,z}(\alpha) = {\sigma_X}^x(\alpha){\sigma_Z}^z(\alpha)$. Note that $[\Lambda^{x,z}]^\dagger = (-1)^{xz}\Lambda^{x,z}$ and that $\Lambda^{00} = 1$, $\Lambda^{10} = \sigma_X$, $\Lambda^{11} = (-i)\sigma_Y$, $\Lambda^{01} = \sigma_Z$. As usual, let $\sigma_{w_1 w_2} = \sigma_{w_1} \otimes \sigma_{w_2}$ for $w_1, w_2 \in \{X, Y, Z\}$.

Claim:

$$E(\alpha,\beta) = \frac{1}{2}\sum_{(x,z)\in Bool^2} \Lambda^{xz}(\alpha)[\Lambda^{xz}(\beta)]^\dagger \tag{145}$$

$$= \frac{1}{2}(1 + \sigma_{XX} + \sigma_{YY} + \sigma_{ZZ})(\alpha,\beta) \tag{146}$$

$$= \frac{1}{2}[1 + \vec{\sigma}(\alpha)\cdot\vec{\sigma}(\beta)] \; . \tag{147}$$

proof:

$$\frac{1}{2}\sum_{x,z}\Lambda^{xz}(\alpha)(-1)^{xz}\Lambda^{xz}(\beta)\left|a,b\right\rangle_{\alpha,\beta} = \tag{148}$$

$$= \frac{1}{2}\sum_{x,z}(-1)^{xz}({\sigma_X}^x{\sigma_Z}^z\left|a\right\rangle_\alpha)({\sigma_X}^x{\sigma_Z}^z\left|b\right\rangle_\beta) \tag{149}$$

$$= \frac{1}{2}\sum_{x,z}(-1)^{(x+a+b)z}\left|a\oplus x, b\oplus x\right\rangle \tag{150}$$

$$= \frac{1}{2}\sum_{x}2\delta^x_{a\oplus b}\left|a\oplus x, b\oplus x\right\rangle \tag{151}$$

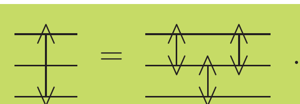
$$= \left|b,a\right\rangle\ . \tag{152}$$

QED

alternative proof:
Replace the 3 CNOTs in $E(\alpha,\beta) = \sigma_X(\alpha)^{n(\beta)}\sigma_X(\beta)^{n(\alpha)}\sigma_X(\alpha)^{n(\beta)}$ by $\sigma_X(\alpha)^{n(\beta)} = \frac{1}{2}\sum_{x,z}{\sigma_X}^x(\alpha){\sigma_Z}^z(\beta)(-1)^{xz}$. Details left to the reader.
QED

We could have predicted that $E(\alpha,\beta)$ would have the form Eq.(147) due to the invariance of Exchanger under identical rotations of both bits; that is, due to Eq.(140) with $U = V = e^{i\vec{\theta}\cdot\vec{\sigma}}$, where $\vec{\theta}$ is an arbitrary 3 dimensional real vector.

Claim:



(153)

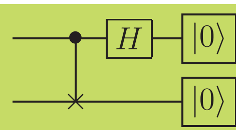
proof:
Check that both sides map $\alpha\to\gamma$, $\beta\to\beta$, $\gamma\to\alpha$.
QED

8 Bell States

Define the Bell state $\left|B^{00}\right\rangle$ by

$$\left|B^{00}\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)\ . \tag{154}$$

Claim:

$$\left|B^{00}\right\rangle_{\alpha\beta} =$$  . (155)

proof:

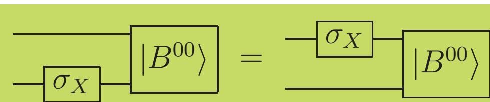
$$\sigma_X(\beta)^{n(\alpha)} H(\alpha) |00\rangle_{\alpha\beta} = \sum_{a\in Bool} \sigma_X(\beta)^{n(\alpha)} |a\rangle_\alpha \langle a|_\alpha H(\alpha) |00\rangle \tag{156}$$

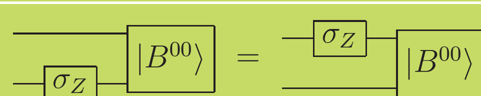
$$= \sum_a \sigma_X{}^a(\beta) |a, 0\rangle_{\alpha\beta} (\frac{1}{\sqrt{2}}) \tag{157}$$

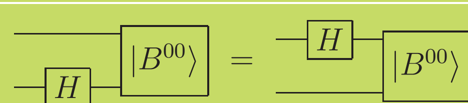
$$= \frac{1}{\sqrt{2}} \sum_a |a, a\rangle \ . \tag{158}$$

QED

Claim:

 , (159)

 , (160)

 . (161)

proof:

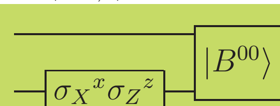
$$\sigma_X(\beta) \sum_{a\in Bool} |a, a\rangle = \sum_a |a, \overline{a}\rangle = \sum_a |\overline{a}, a\rangle = \sigma_X(\alpha) \sum_a |a, a\rangle \ . \tag{162}$$

$$\sigma_Z(\beta) \sum_{a\in Bool} |a, a\rangle = \sum_a (-1)^a |a, a\rangle = \sigma_Z(\alpha) \sum_a |a, a\rangle \ . \tag{163}$$

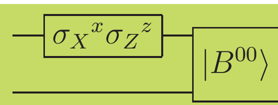
Eq.(161) follows from the previous two equations and the observation that $H = \frac{1}{\sqrt{2}}(\sigma_X + \sigma_Z)$.

QED

Define the Bell states $|B^{x,z}\rangle$ and $|B_{x,z}\rangle$ for $x, z \in Bool$ by

$$|B_{x,z}\rangle =$$  , (164)

and

$$|B^{x,z}\rangle = $$ 

. (165)

Note that $|B^{00}\rangle = |B_{00}\rangle$. Since

$$\begin{aligned} |B_{x,z}\rangle &= \sigma_X{}^x(\beta)\sigma_Z{}^z(\beta)(\frac{1}{\sqrt{2}})(|00\rangle + |11\rangle)_{\alpha\beta} &(166)\\ &= \frac{1}{\sqrt{2}}(|0x\rangle + (-1)^z\,|1\overline{x}\rangle)\,, &(167)\end{aligned}$$

it follows that

$$\begin{array}{rrl} |B_{00}\rangle = & 1\,|B_{00}\rangle = & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\\ |B_{10}\rangle = & \sigma_X(\beta)\,|B_{00}\rangle = & \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\\ |B_{11}\rangle = & (-i)\sigma_Y(\beta)\,|B_{00}\rangle = & \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\\ |B_{01}\rangle = & \sigma_Z(\beta)\,|B_{00}\rangle = & \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \end{array}\ . \qquad (168)$$

Claim:

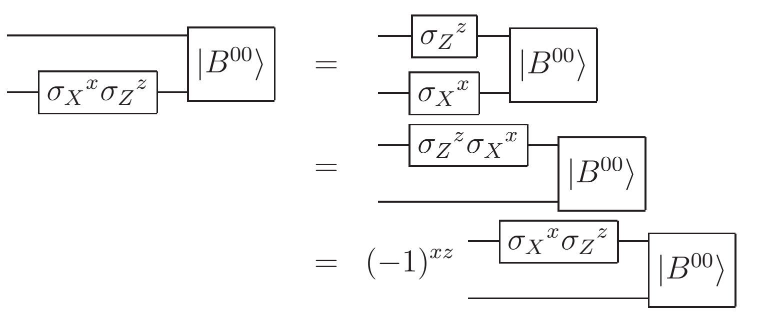
For any $x, z \in Bool$,

$$\begin{aligned} |B_{x,z}\rangle_{\alpha\beta} &= E(\alpha,\beta)\,|B^{x,z}\rangle_{\alpha\beta} &(169)\\ &= (-1)^{xz}\,|B^{x,z}\rangle_{\alpha\beta}\ . &(170)\end{aligned}$$

Thus, $|B^{x,z}\rangle$ and $|B_{x,z}\rangle$ are both eigenfunctions of E with eigenvalue $(-1)^{xz}$.

proof:

Eq.(169) is obvious. Eq.(170) follows from



(171)

(172)

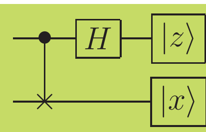
(173)

QED

Claim:

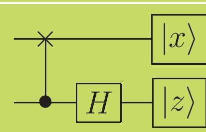
For any $x, z \in Bool$,

$$|B_{x,z}\rangle =$$



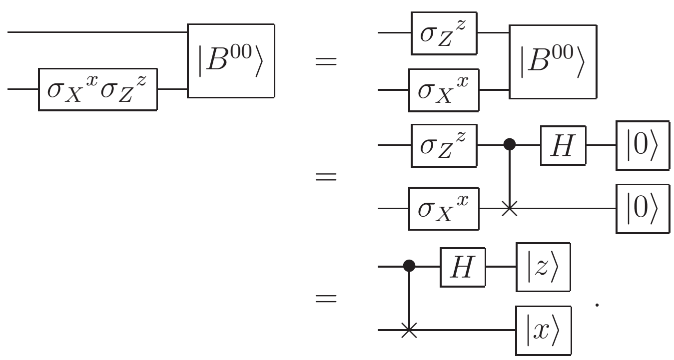
, (174)

$$|B^{x,z}\rangle =$$



. (175)

proof:



(176)

(177)

(178)

QED

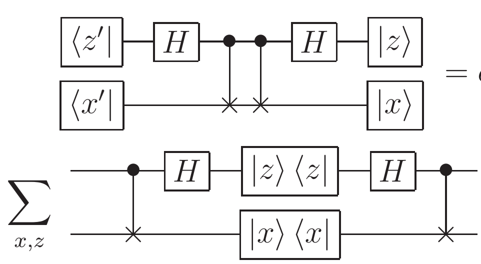
Claim: (Orthonormality)

$$\langle B_{xz} | B_{x'z'} \rangle = \delta^{x',z'}_{x,z} \tag{179}$$

for any $x, z, x'z' \in Bool$, and

$$\sum_{(x,z) \in Bool^2} |B_{xz}\rangle \langle B_{xz}| = 1 \ . \tag{180}$$

proof:



$= \delta^{x',z'}_{x,z}$. (181)

$= 1$. (182)

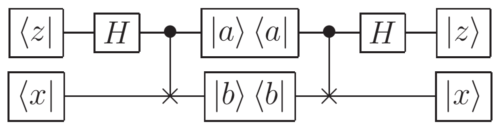
QED

Claim:

For all $a, b, x, z \in Bool$, if $P(a,b|x,z) = |\langle a,b|B_{x,z}\rangle|^2$, then the marginals $P(a|x,z)$ and $P(b|x,z)$ are both identically equal to $\frac{1}{2}$.

proof:

$$\sum_a P(a,b|x,z) = \sum_a \quad \text{(183)}$$



$$= \sum_a \left| \frac{(-1)^{za}}{\sqrt{2}} \langle x| \sigma_X{}^a |b\rangle \right|^2 \quad (184)$$

$$= \frac{1}{2} \sum_a |\langle x|a \oplus b\rangle|^2 \quad (185)$$

$$= \frac{1}{2} \sum_a \delta_a^{x \oplus b} = \frac{1}{2} \ . \quad (186)$$

QED

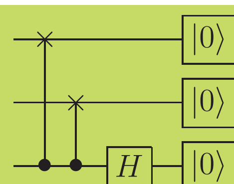
9 GHZ

The GHZ state is defined by

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \ . \quad (187)$$

Claim:

$$|GHZ\rangle = \quad . \quad (188)$$



proof:
Let RHS denote right hand side of Eq.(188).

$$RHS = \sigma_X(\alpha)^{n(\gamma)} \sigma_X(\beta)^{n(\gamma)} H(\gamma) |000\rangle_{\alpha\beta\gamma} \quad (189)$$

$$= \sigma_X(\alpha)^{n(\gamma)} \sigma_X(\beta)^{n(\gamma)} \frac{1}{\sqrt{2}} \sum_{a \in Bool} |0,0,a\rangle \quad (190)$$

$$= \frac{1}{\sqrt{2}} \sum_{a \in Bool} |a,a,a\rangle = |GHZ\rangle \ . \quad (191)$$

QED

Claim:

$$\sigma_{XYY} |GHZ\rangle = \sigma_{YXY} |GHZ\rangle = \sigma_{YYX} |GHZ\rangle = - |GHZ\rangle \ . \tag{192}$$

Hence,

$$\sigma_{XYY}\sigma_{YXY}\sigma_{YYX} |GHZ\rangle = - |GHZ\rangle \ . \tag{193}$$

However,

$$\sigma_{XXX} |GHZ\rangle = + |GHZ\rangle \ . \tag{194}$$

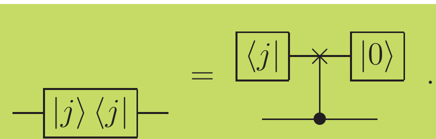
proof:
For any $a \in Bool$, $\sigma_Y |a\rangle = i(-1)^a |\overline{a}\rangle$ and $\sigma_X |a\rangle = |\overline{a}\rangle$ so

$$\begin{aligned}
\sigma_{XYY} |GHZ\rangle &= \sigma_X \otimes \sigma_Y \otimes \sigma_Y \frac{1}{\sqrt{2}} \sum_{a \in Bool} |a, a, a\rangle & (195) \\
&= (-1) \frac{1}{\sqrt{2}} \sum_a |\overline{a}, \overline{a}, \overline{a}\rangle & (196) \\
&= - |GHZ\rangle \ . & (197)
\end{aligned}$$

This establishes Eq.(192). Eq.(193) follows from Eq.(192). Eq.(194) can be proven in the same way as Eq.(192).
QED

10 One and Two Qubit Projective Measurements

Claim: (Conversion: 1 qubit internal measurement → 1 qubit final measurement)
For any $j \in Bool$,



(198)

proof:
Let LHS and RHS stand for the left and right hand sides of Eq.(198). For any $b \in Bool$,

$$LHS |b\rangle_\beta = |b\rangle_\beta \delta_j^b \ . \tag{199}$$

$$
\begin{aligned}
RHS\,|b\rangle_\beta &= \langle j|_\alpha\, \sigma_X(\alpha)^{n(\beta)}\, |0,b\rangle_{\alpha\beta} && (200)\\
&= \langle j|_\alpha\, |b,b\rangle_{\alpha\beta} && (201)\\
&= |b\rangle_\beta\, \delta^b_j\,. && (202)
\end{aligned}
$$

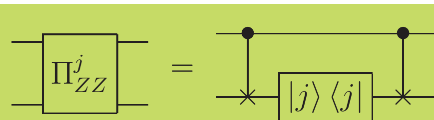
QED

One qubit operations (such as internal or final one qubit measurements or one qubit rotations) are "cheap" compared with two qubit operations such as CNOTs and two qubit measurements (either internal or final). This is because two qubit operations are slower and they require two qubits to interact, which opens the door for noise from the environment to creep in. So in this section we will pay attention only to the number of two qubit operations. Let **bibit** stand for two bits. Next we will show what I like to call the "one to two" conversion rules. Namely, given a single CNOT, one can always convert it to two bibit operations. Likewise, given a single bibit operation, one can always convert it to two CNOTs.

As usual in this document, for $j \in Bool$, we define $\Pi^j_{ZZ}(\alpha,\beta) = \pi[\sigma_{ZZ}(\alpha,\beta) = (-1)^j]$; i.e, Π^j_{ZZ} is the projection operator onto the 2 qubit subspace with $(-1)^j$ as eigenvalue for $\sigma_Z \otimes \sigma_Z$.

Claim: (Conversion: 1 bibit measurement → 2 CNOTs)

For any $j \in Bool$,



. (203)

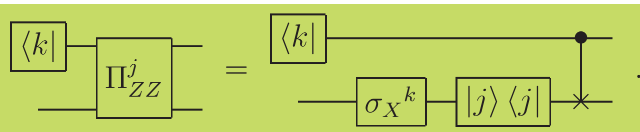
proof:
Let RHS stand for the right hand side of Eq.(203). For any $a, b \in Bool$,

$$
\begin{aligned}
RHS\,|a,b\rangle_{\alpha\beta} &= \sigma_X(\beta)^{n(\alpha)}\, |j\rangle_\beta \langle j|_\beta\, \sigma_X(\beta)^{n(\alpha)}\, |a,b\rangle_{\alpha\beta} && (204)\\
&= \sigma_X(\beta)^{n(\alpha)}\, |j\rangle_\beta\, \delta^j_{a\oplus b}\, |a\rangle_\alpha && (205)\\
&= \delta^j_{a\oplus b}\, |a,b\rangle_{\alpha\beta} && (206)\\
&= \Pi^j_{ZZ}\, |a,b\rangle_{\alpha\beta}\ . && (207)
\end{aligned}
$$

QED

Claim: (Conversion: 1 bibit measurement → 1 CNOT. Special case of Eq.(203).)

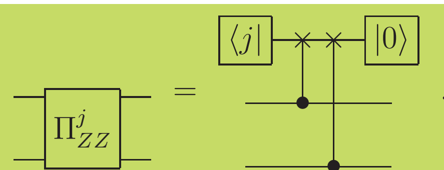
For any $j, k \in Bool$,



(208)

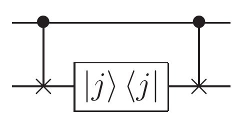
proof:
Follows immediately from Eq.(203).
QED

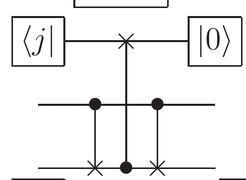
Claim: (Another Conversion of: 1 bibit measurement → 2 CNOTs)
For any $j \in Bool$,

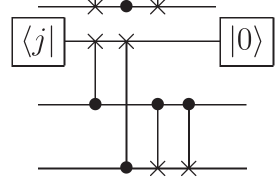


(209)

proof:
Let LHS and RHS denote the left and right hand sides of Eq.(209).

LHS =  (210)

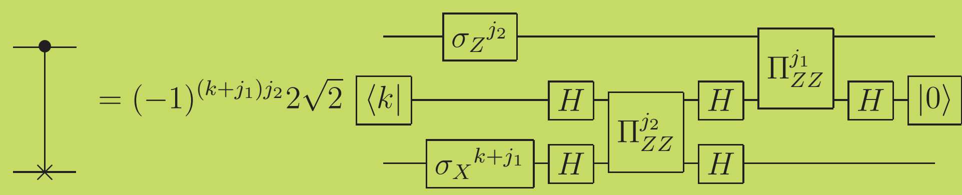
=  (211)

=  (212)

$$= RHS \ . \tag{213}$$

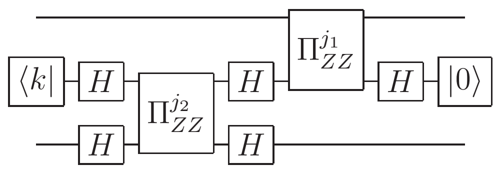
QED

Claim: (Conversion: 1 CNOT → 2 bibit measurements)
For any $k, j_1, j_2 \in Bool$,



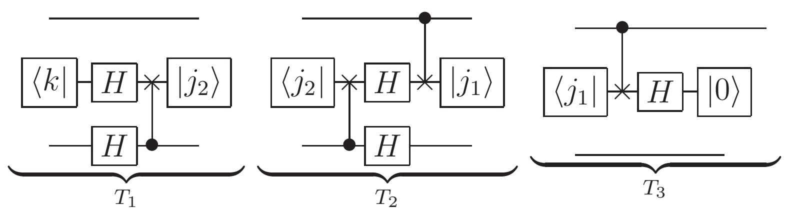
(214)

proof:
Define T by



(215)

Then

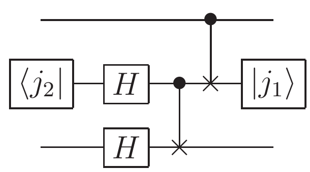


(216)

$$T_1 = \frac{(-1)^{kj_2}}{\sqrt{2}} H(\gamma)\sigma_Z{}^k(\gamma) , \tag{217}$$

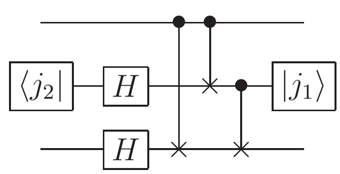
$$T_3 = \frac{1}{\sqrt{2}} , \tag{218}$$

$T_2 =$



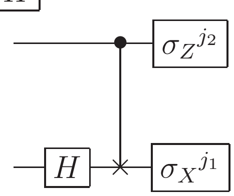
(219)

$=$



(220)

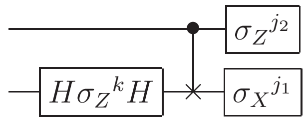
$= \frac{(-1)^{j_1 j_2}}{\sqrt{2}}$

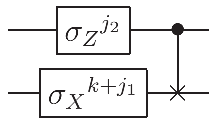


(221)

Putting all this together,

$$T = T_1 T_2 T_3 \tag{222}$$

$$= \frac{(-1)^{(k+j_1)j_2}}{2\sqrt{2}}$$  (223)

$$= \frac{(-1)^{(k+j_1)j_2}}{2\sqrt{2}}$$  . (224)

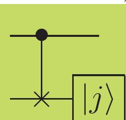
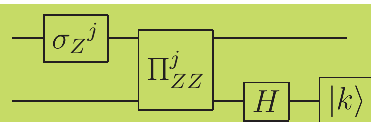
QED

alternative proof:
Define operator S such that for all $a, c \in Bool$,

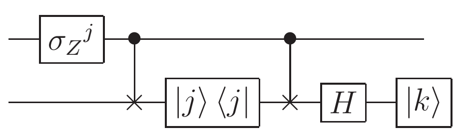
$$S\left|a,c\right\rangle_{\alpha\gamma} = \left\langle k\right|_\beta H(\beta)\Pi^{j_2}_{ZZ}(\beta,\gamma)H(\beta)\Pi^{j_1}_{ZZ}(\alpha,\beta)H(\beta)\left|a,0,c\right\rangle_{\alpha\beta\gamma} \;. \tag{225}$$

In Eq.(225), insert a partition of unity $\sum_{(a_1,b_1,c_1)\in Bool^3}\left|a_1,b_1,c_1\right\rangle\left\langle a_1,b_1,c_1\right|$ before the first bibit measurement and another $\sum_{(a_2,b_2,c_2)\in Bool^3}\left|a_2,b_2,c_2\right\rangle\left\langle a_2,b_2,c_2\right|$ before the second. Then use the fact that for $a, b, j \in Bool$, $\Pi^j_{ZZ}\left|a,b\right\rangle = \delta^j_{a\oplus b}\left|a,b\right\rangle$. Details left to the reader.
QED

Claim: (Conversion: 1 CNOT $\rightarrow$ 1 bibit measurement. Special case of Eq.(214).)
For any $j, k \in Bool$,

 $= (-1)^{jk}\sqrt{2}$  . (226)

proof:
Let LHS and RHS stand for the left and right hand sides of Eq.(226). Then

$RHS = (-1)^{jk}\sqrt{2}$  $= LHS$. (227)

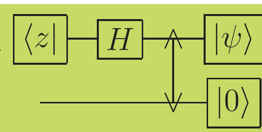
QED

11 Two Qubit Exchange Scattering

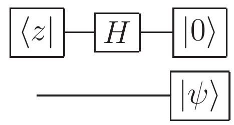
Throughout this section, $|\psi\rangle$ will denote an arbitrary one qubit state.

Claim: (Exchange scattering via Exchanger)

For any $z \in Bool$,

$\sqrt{2}$  $=$  . (228)

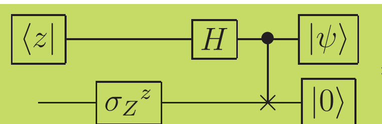
proof:
Let LHS and RHS stand for the left and right hand sides of Eq.(228).

$LHS = \sqrt{2}$  $= RHS$. (229)

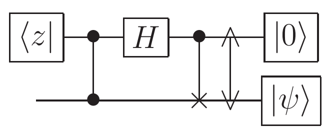
QED

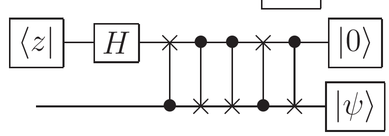
Claim: (Exchange scattering via CNOT)

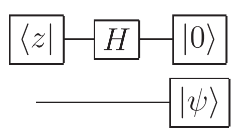
For any $z \in Bool$,

$\sqrt{2}$  $=$  . (230)

proof:
Let LHS and RHS stand for the left and right hand sides of Eq.(230).

$LHS = \sqrt{2}$  (231)

$= \sqrt{2}$  (232)

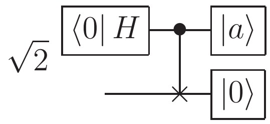
$= \sqrt{2}$  (233)

$= RHS$. (234)

QED

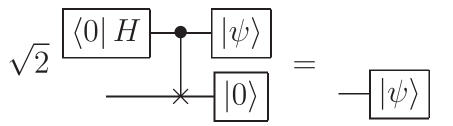
alternative proof:

For any $a \in Bool$:



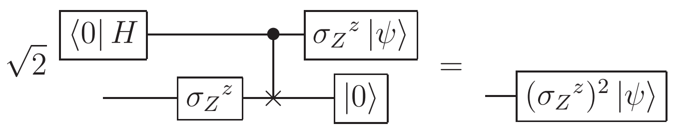
$$= \sigma_X{}^a(\beta)\,|0\rangle_\beta = |a\rangle_\beta \ . \tag{235}$$

Thus, for an arbitrary state $|\psi\rangle$,



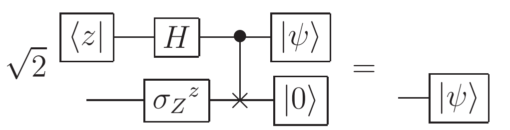
(236)

In Eq.(236), if we multiply ket $|\psi\rangle$ by a pre-processing and a post-processing $\sigma_Z{}^z$, then we obtain



(237)

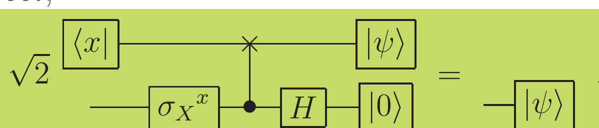
which easily yields



(238)

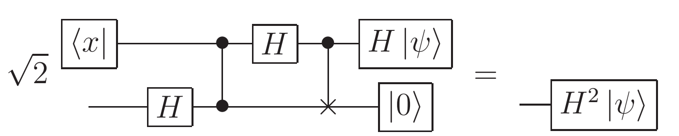
QED

Claim: (Another example of exchange scattering via CNOT)
For any $x \in Bool$,



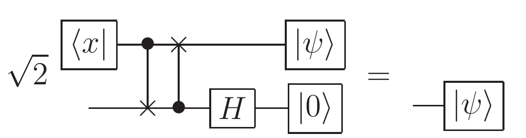
(239)

proof:
In Eq.(230), if we replace z by x and multiply the ket $|\psi\rangle$ by a pre-processing and a post-processing H, then we obtain:



(240)

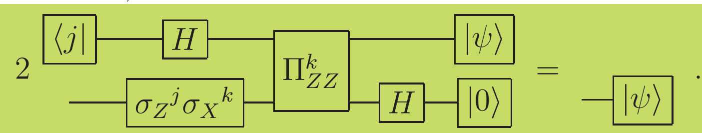
The last identity simplifies to



(241)

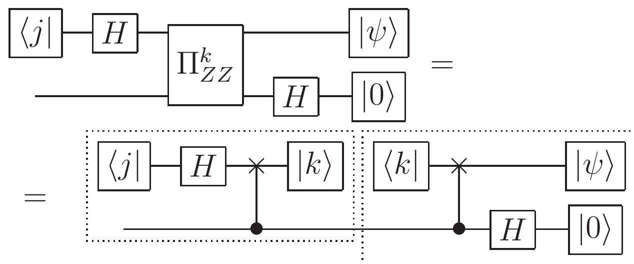
which is the same as the claim that we set out to prove.
QED

Claim: (Exchange scattering via a 2 qubit projective measurement)
For any $j, k \in Bool$,



(242)

proof:



(243)

(244)

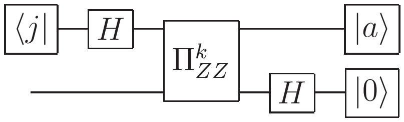
$$= \left[\frac{(-1)^{jk}}{\sqrt{2}}\sigma_Z{}^j(\beta)\right]\left[\frac{\sigma_X{}^k(\beta)}{\sqrt{2}}\left|\psi\right\rangle_\beta\right] \quad (245)$$

$$= \sigma_X{}^k(\beta)\sigma_Z{}^j(\beta)\left|\psi\right\rangle_\beta/2\ . \quad (246)$$

To go from Eq.(243) to Eq.(244), we expressed the two qubit projective measurement in terms of 2 CNOTs, as described in the section entitled One and Two Qubit Projective Measurements. To go from Eq.(244) to Eq.(245), we used identity Eq.(239) to reduce the second dotted box of Eq.(244).
QED

alternative proof:

For any $a \in Bool$,



$$
\begin{aligned}
&= \qquad (247)\\
&= \langle j|_\alpha H(\alpha)\Pi^k_{ZZ}\left(\sum_{(a',b')\in Bool^2} |a',b'\rangle\langle a',b'|\right) H(\beta)|a,0\rangle_{\alpha\beta} \qquad (248)\\
&= \sum_{a',b'} \langle j|_\alpha H(\alpha)|a'\rangle_\alpha |b'\rangle_\beta \delta^k_{a'\oplus b'}\langle a',b'|H(\beta)|a,0\rangle_{\alpha\beta} \qquad (249)\\
&= \sum_{a',b'} \frac{(-1)^{ja'}}{\sqrt{2}}|b'\rangle_\beta \delta^k_{a'\oplus b'}\frac{\delta^{a'}_a}{\sqrt{2}} \qquad (250)\\
&= \frac{(-1)^{ja}}{2}|k\oplus a\rangle_\beta \qquad (251)\\
&= \sigma_X{}^k(\beta)\sigma_Z{}^j(\beta)|a\rangle_\beta/2\ . \qquad (252)
\end{aligned}
$$

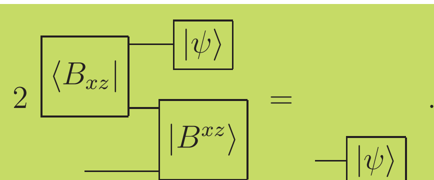
QED

12 Teleportation

Throughout this section, $|\psi\rangle$ will denote an arbitrary one qubit state.

Claim:

For any $x, z \in Bool$,



(253)

proof:
Let LHS denote the left hand side of Eq.(253). Then

$$
\begin{aligned}
LHS &= \left\langle B^{00}\right|_{\alpha\beta}\sigma_Z{}^z(\beta)\sigma_X{}^x(\beta)\sigma_X{}^x(\beta)\sigma_Z{}^z(\beta)|\psi\rangle_\alpha\left|B^{00}\right\rangle_{\beta\gamma} \qquad (254)\\
&= \left\langle B^{00}\right|_{\alpha\beta}|\psi\rangle_\alpha\left|B^{00}\right\rangle_{\beta\gamma}\ , \qquad (255)
\end{aligned}
$$

so we only need to prove Eq.(253) for $x = z = 0$.

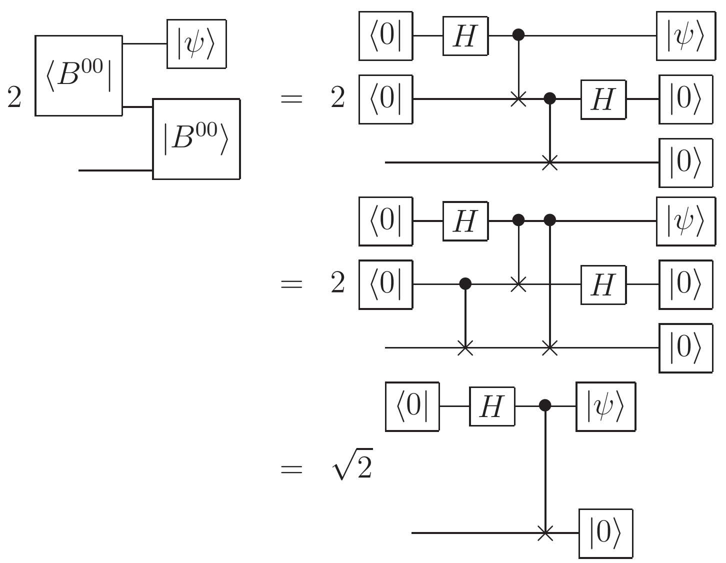
For an arbitrary $a \in Bool$,

$$\langle B^{00}|_{\alpha\beta} |a\rangle_\alpha |B^{00}\rangle_{\beta\gamma} = (\frac{1}{2})(\langle 00|_{\alpha\beta} + \langle 11|_{\alpha\beta}) |a\rangle_\alpha (|00\rangle_{\beta\gamma} + |11\rangle_{\beta\gamma}) \tag{256}$$

$$= \frac{\langle a|_\beta}{2}(|00\rangle_{\beta\gamma} + |11\rangle_{\beta\gamma}) \tag{257}$$

$$= \frac{|a\rangle_\gamma}{2} \ . \tag{258}$$

Alternatively, note that



(259)

(260)

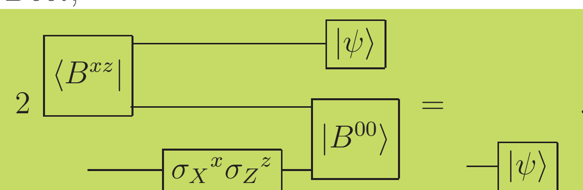
(261)

$$= |\psi\rangle_\gamma \ . \tag{262}$$

QED

Claim:

For any $x, z \in Bool$,



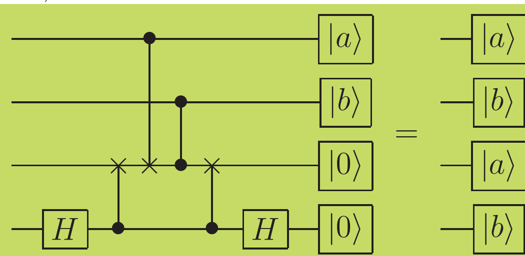
(263)

proof:
Follows immediately from Eq.(253).
QED

13 Dense Coding

Claim:

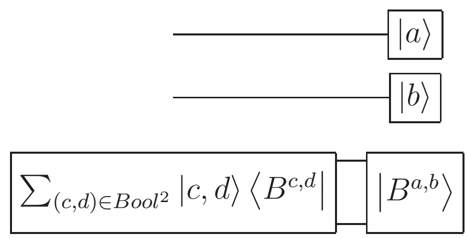
For any $a, b \in Bool$,



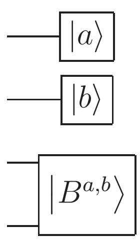
. (264)

proof:
Let LHS and RHS denote the left and right hand sides of Eq.(264).

$RHS =$



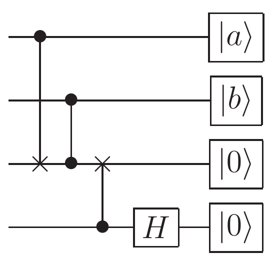
. (265)



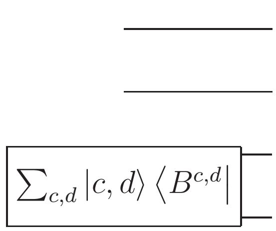
$$= |a, b\rangle_{\alpha\beta} \, {\sigma_X}^a(\gamma){\sigma_Z}^b(\gamma) \left|B^{00}\right\rangle_{\gamma\delta} \quad (266)$$

$$= {\sigma_X}^{n(\alpha)}(\gamma){\sigma_Z}^{n(\beta)}(\gamma) \, |a, b\rangle_{\alpha\beta} \left|B^{00}\right\rangle_{\gamma\delta} \quad (267)$$

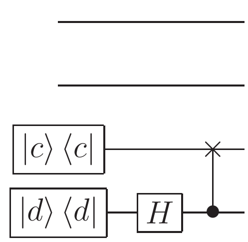
=



. (268)



$= \sum_{c,d}$



. (269)

QED

14 Quantum Fourier Transform

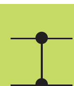
For this section, it is especially important that the reader read the Notation section of QC Paulinesia. The Notation section explains what we mean by natural labelling. Natural labelling will be used in this section.

Given a vector $\vec{x} = (x_{N_B-1}, \ldots, x_1, x_0) \in Bool^{N_B}$, let $R\vec{x} = (x_0, x_1, \ldots, x_{N_B-1})$. Thus R is the matrix that reverses the components of an N_B dimensional vector. For example, for $N_B = 4$,

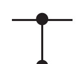
$$R = \begin{pmatrix} 0 & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & 0 \end{pmatrix} . \tag{270}$$

We will also use R to denote a map from the Hilbert space of N_B qubits to itself such that $R|\vec{x}\rangle = |R\vec{x}\rangle$ for $\vec{x} \in Bool^{N_B}$. We will also use R to denote the map $R : Z_{0,N_B-1} \rightarrow Z_{0,N_B-1}$ such that $R(i) = N_B - 1 - i$. For example, for $N_B = 4$, R maps $0 \rightarrow 3$, $1 \rightarrow 2$, $2 \rightarrow 1$, $3 \rightarrow 0$.

For any $\alpha, \beta \in Z_{0,N_B-1}$, define



$$= V(\alpha, \beta) = \exp[i\pi \frac{n(\alpha)n(\beta)}{2^{|\alpha-\beta|}}] = (-1)^{\frac{n(\alpha)n(\beta)}{2^{|\alpha-\beta|}}} . \tag{271}$$

Note that normally in QC Paulinesia, we use  $= \sigma_Z{}^{n(\alpha)}(\beta) = (-1)^{n(\alpha)n(\beta)}$, so the definition given by Eq.(271) applies only to this section.

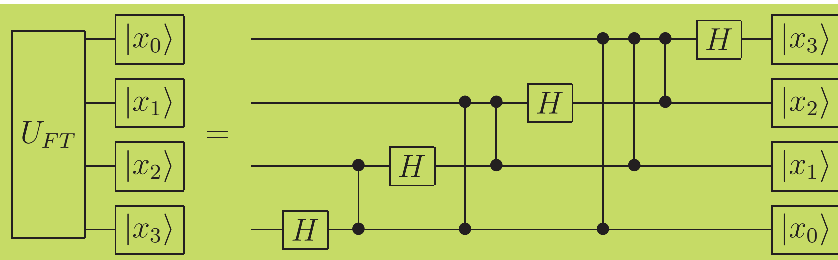
For any $x \in Z_{0,N_S-1}$, the **Quantum Fourier Transform** of $|x\rangle$ is defined by

$$U_{FT}|x\rangle = \frac{1}{\sqrt{N_S}} \sum_{y=0}^{N_S-1} e^{i\frac{2\pi xy}{N_S}} |y\rangle \ . \tag{272}$$

Henceforth, for simplicity, we will often assume $N_B = 4$. It will be obvious how to extend our arguments to other values of N_B.

Claim:

For any $\vec{x} = (x_3, x_2, x_1, x_0) \in Bool^4$,



, (273)

proof:

Recall from the Notation section that $\vec{\nu} = (N_B - 1, \ldots, 2, 1, 0)$. Let $n = 2^{\vec{\nu}} \cdot \vec{n}$ and $x = 2^{\vec{\nu}} \cdot \vec{x}$. Then

$$U_{FT} |\vec{x}\rangle_{\vec{\nu}} = \frac{1}{\sqrt{N_S}} e^{\frac{i2\pi xn}{N_S}} \sum_{\vec{y} \in Bool^{N_B}} |\vec{y}\rangle_{\vec{\nu}} \tag{274}$$

$$= e^{i\frac{2\pi xn}{N_S}} H(\vec{\nu}) |0\rangle_{\vec{\nu}} \ . \tag{275}$$

Furthermore,

$$\exp[\frac{i2\pi xn}{16}] = e^{\left[\frac{i2\pi}{16}(8x_3+4x_2+2x_1+x_0)(8n(3)+4n(2)+2n(1)+n(0))\right]} \tag{276}$$

$$= \exp[i2\pi \left\{ \begin{array}{l} \quad n(3)(\frac{x_0}{2}) \\ +n(2)(\frac{x_1}{2} + \frac{x_0}{4}) \\ +n(1)(\frac{x_2}{2} + \frac{x_1}{4} + \frac{x_0}{8}) \\ +n(0)(\frac{x_3}{2} + \frac{x_2}{4} + \frac{x_1}{8} + \frac{x_0}{16}) \end{array} \right\}] \ , \tag{277}$$

where, in Eq.(277), we omitted all terms in the argument of the exponential that yielded contributions of the form $e^{i2\pi(integer)}$.

Note that for any $x \in Bool$ and bit α,

$$(-1)^{xn(\alpha)} H(\alpha) |0\rangle_\alpha = {\sigma_Z}^x(\alpha) H(\alpha) |0\rangle_\alpha = H(\alpha) |x\rangle_\alpha \ . \tag{278}$$

Thus,

$$\exp[\frac{i2\pi xn}{16}]H(\vec{\nu})|0\rangle_{\vec{\nu}} = \left\{\begin{array}{l} \exp[i\pi n(3)x_0]H(3)|0\rangle_3 \\ \exp[i\pi n(2)(x_1+\frac{x_0}{2})]H(2)|0\rangle_2 \\ \exp[i\pi n(1)(x_2+\frac{x_1}{2}+\frac{x_0}{4})]H(1)|0\rangle_1 \\ \exp[i\pi n(0)(x_3+\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8})]H(0)|0\rangle_0 \end{array}\right. \tag{279}$$

$$= \left\{\begin{array}{l} H(3)|x_0\rangle_3 \\ \exp[i\pi n(2)(\frac{x_0}{2})]H(2)|x_1\rangle_2 \\ \exp[i\pi n(1)(\frac{x_1}{2}+\frac{x_0}{4})]H(1)|x_2\rangle_1 \\ \exp[i\pi n(0)(\frac{x_2}{2}+\frac{x_1}{4}+\frac{x_0}{8})]H(0)|x_3\rangle_0 \end{array}\right. \tag{280}$$

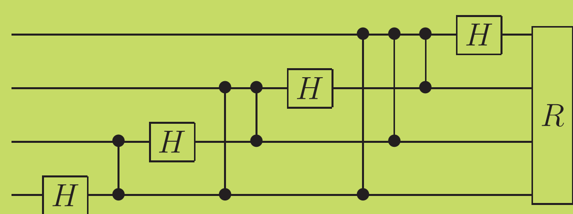
$$= \left\{\begin{array}{l} H(3) \\ \exp[i\pi n(2)(\frac{n(3)}{2})]H(2) \\ \exp[i\pi n(1)(\frac{n(2)}{2}+\frac{n(3)}{4})]H(1) \\ \exp[i\pi n(0)(\frac{n(1)}{2}+\frac{n(2)}{4}+\frac{n(3)}{8})]H(0) \end{array}\right\} R|\vec{x}\rangle \tag{281}$$

$$= H(3)V(3,2)H(2)V(3,1)V(2,1)H(1)V(3,0)V(2,0)V(1,0)H(0)R|\vec{x}\rangle\ . \tag{282}$$

QED

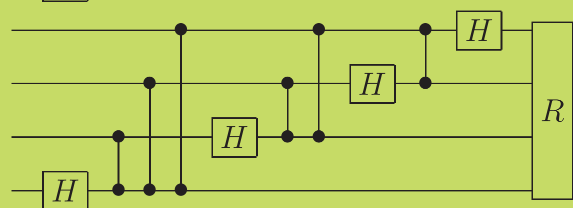
Claim: (3-2-1 form equals 1-2-3 form)

U_{FT} =



(283)

=



. (284)

proof:
Obvious.
QED

We call "the 1-2-3 form" the form of U_{FT} given by Eq.(283). We call "the 3-2-1 form" the form given by Eq.(284). The numbers 1,2,3 refer to the number of V operators between the H operators.

Claim:

U_{FT} is a symmetric matrix.

proof:

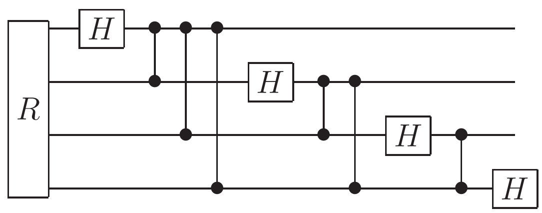
Let † = Hermitian conjugate, ∗ = complex conjugate, so †∗ = transpose. For any $x, y \in Z_{0,N_S-1}$,

$$\langle y| U_{FT} |x\rangle = \exp(\frac{i2\pi xy}{N_S}) = \langle y| U_{FT}^{\dagger *} |x\rangle \ . \tag{285}$$

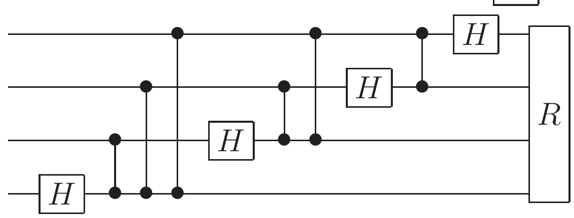
QED

alternative proof:

$U_{FT}^{\dagger *} \ =$ (286)



$=$ (287)



$$= \ U_{FT} \ . \tag{288}$$

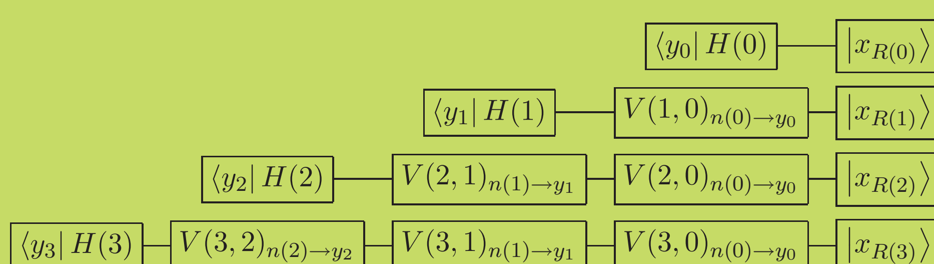
QED

For distinct bits α, β, let $V(\alpha, \beta)_{n(\beta)\to b}$ denote the result of substituting $n(\beta)$ in $V(\alpha, \beta)$ by $b \in Bool$.

Claim:

For any $\vec{x} = (x_3, x_2, x_1, x_0) \in Bool^4$ and $\vec{y} = (y_3, y_2, y_1, y_0) \in Bool^4$,

$\langle \vec{y}| U_{FT} |\vec{x}\rangle =$

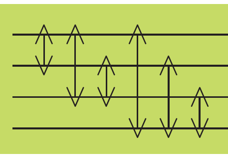


. (289)

proof:

Obvious.
QED

Claim:

$R =$  . (290)

proof:
Check that the right hand side of Eq.(290) maps $0 \rightarrow 3$, $1 \rightarrow 2$, $2 \rightarrow 1$, and $3 \rightarrow 0$.
QED

15 References

The following documents were useful in preparing this document.

References

[1] (good on controlled U) Cast of Thousands (Barenco et al.), "Elementary Gates for Quantum Computation", ArXiv eprint quant-ph/9503016

[2] (this guy thinks just like me) R.R. Tucci, "A Rudimentary Quantum Compiler(2cnd ed.)", ArXiv eprint quant-ph/9902062 .

[3] (good on projective measurements) A. M. Childs, D. W. Leung, M. A. Nielsen, "Unified derivations of measurement-based schemes for quantum computation", ArXiv eprint quant-ph/0404132

[4] (original paper on teleportation) Charles H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Ashes Peres, and William K. Wootters, Phys. Rev. Lett. 70, 1895 (1993)

[5] (original paper on dense coding) C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992).

[6] (original paper on quantum Fourier Transform) D. Coppersmith, "An approximate Fourier transform useful in quantum factoring", ArXiv eprint quant-ph/0201067

[7] D. Gottesman, "The Heisenberg Representation of Quantum Computers", ArXiv eprint quant-ph/9807006

[8] N. David Mermin, lecture notes for Quantum Computing course taught at Cornell.

[9] Paul Theroux, "The Happy Isles of Oceania" (G.F. Putnam's Sons, NY, 1992).