# Matrix Decompositions and Quantum Circuit Design

Stephen S. Bullock
(joint with Vivek V.Shende,Igor L.Markov, U.M. EECS)

**Mathematical and Computational Sciences Division**
**Division Seminar**
**National Institute of Standards and Technology**

September 15, 2004

# Motivation

Classical Technique: For `AND-OR-NOT` circuit for function $\varphi$ on bit strings

- Build `AND-NOT` circuit firing on each bit-string with $\varphi = 1$
- Connect each such with an `OR`

Restatement:

- Produce a decomposition of the function $\varphi$
- Produce circuit blocks accordingly

# Motivation, Cont.

Quotation, *Feynman on Computation*, §2.4:

> However, the approach described here is so simple and general that it does not need an expert in logic to design it! Moreover, it is also a standard type of layout that can easily be laid out in silicon. (ibid.)

**Remarks:**

- Analog for quantum computers?
- Simple & general?

# Motivation, Cont.

- Quantum computation, $n$ quantum bits: $2^n \times 2^n$ unitary matrix

- Matrix decomposition: Algorithm for factoring matrices
  - Similar strategy: decomposition splits computation into parts
  - Divide & conquer: produce circuit design for each factor

# Outline

I. Introduction to Quantum Circuits
II. Two Qubit Circuits (CD)
III. Circuits for Diagonal Unitaries
IV. Half CNOT per Entry (CSD)
V. Differntial Topology & Lower Bounds

# Quantum Computing

- replace bit with qubit: two state quantum system, states $|0\rangle$, $|1\rangle$
  - Single qubit state space $\mathcal{H}_1 = \mathbb{C}|0\rangle \oplus \mathbb{C}|1\rangle \cong \mathbb{C}^2$
  - e.g. $|\psi\rangle = (1/\sqrt{2})(|0\rangle + i|1\rangle)$ or $|\psi\rangle = \begin{pmatrix} 1/\sqrt{2} \\ i/\sqrt{2} \end{pmatrix}$
  - $n$-qubit state space $\mathcal{H}_n = \otimes_1^n \mathcal{H}_1 = \oplus_{\bar{b}}$ an $n$ bit string$\mathbb{C}|\bar{b}\rangle \cong \mathbb{C}^{2^n}$
  - Kronecker (tensor) product $\Longrightarrow$ entanglement

# Nonlocality: Entangled States

- von Neumann measurement: $|\psi\rangle = \sum_{j=0}^{N} \alpha_j |j\rangle$, Prob$(j$ meas$) = |\alpha_j|^2 / \sum_{j=0}^{2^n-1} |\alpha_j|^2$

- Standard entangled state: $|\psi\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$

  – Prob$(00$ meas$)$ = Prob$(11$ meas$) = 1/2$

- Also $|GHZ\rangle = (1/\sqrt{2})(|00\cdots 0\rangle + |11\cdots 1\rangle)$,
  $|W\rangle = (1/\sqrt{n})(|100\cdots 0\rangle + |010\cdots 0\rangle + \cdots + |0\cdots 01\rangle)$

- quantum computations: apply unitary matrix $u$, i.e. $|\psi\rangle \mapsto u|\psi\rangle$

# Tensor (Kronecker) Products of Data, Computations

- $|\phi\rangle = |0\rangle + i|1\rangle$, $|\psi\rangle = |0\rangle - |1\rangle \in \mathcal{H}_1$
  - interpret $|10\rangle = |1\rangle \otimes |0\rangle$ etc.
  - composite state in $\mathcal{H}_2$: $|\phi\rangle \otimes |\psi\rangle = |00\rangle - |01\rangle + i|10\rangle - i|11\rangle$
- Most two-qubit states are not tensors of one-qubit states.
- If $A = \begin{pmatrix} \bar{\alpha} & -\beta \\ \beta & \bar{\alpha} \end{pmatrix}$ is one-qubit, $B$ one-qubit, then the two-qubit tensor $A \otimes B$ is $(A \otimes B) = \begin{pmatrix} \bar{\alpha}B & -\beta B \\ \beta B & \bar{\alpha}B \end{pmatrix}$. Most $4 \times 4$ unitary $u$ are not local.

## Complexity of Unitary Evolutions

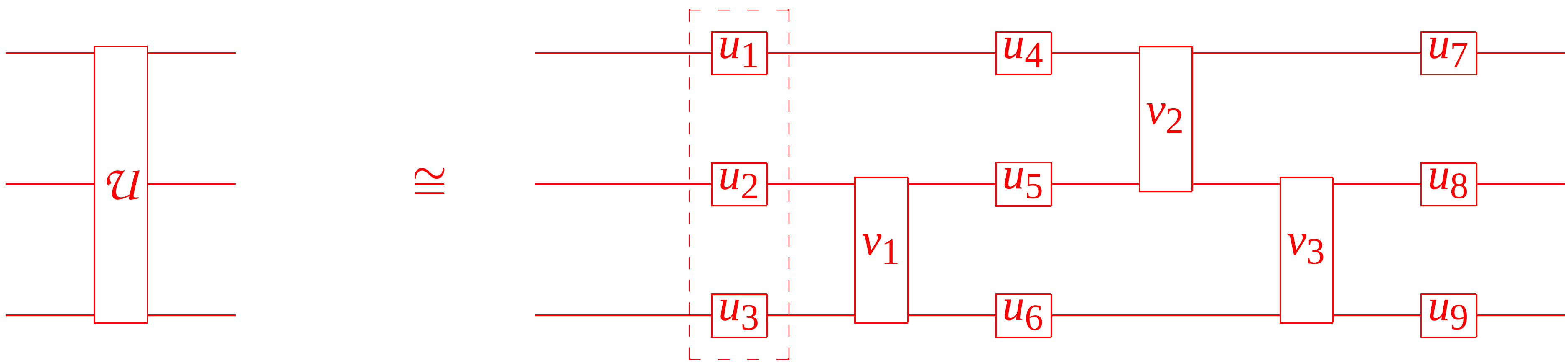
- Easy to do: $\otimes_{j=1}^{n} u_j$ for $2 \times 2$ factors,
  Slightly tricky: two-qubit operation $v \otimes I_{2^n/4}$, some $4 \times 4$ unitary v

- Optimization problem: Use as few such factors as possible

- Visual representation: Quantum circuit diagram

Thm: ('93, Bernstein-Vazirani) The Deutsch-Jozsa algorithm proves quantum computers would violate the strong Church-Turing hypothesis.

# Complexity of Unitary Evolutions Cont.

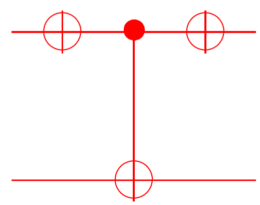



- Outlined box is Kronecker (tensor) product $u_1 \otimes u_2 \otimes u_3$
- Common practice: not arbitrary $v_1$, $v_2$, $v_3$ but CNOT, $|10\rangle \longleftrightarrow |11\rangle$

# Quantum Circuit Design

- For $\bigoplus = \texttt{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, sample quantum circuit:

$$u = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$ is implemented by



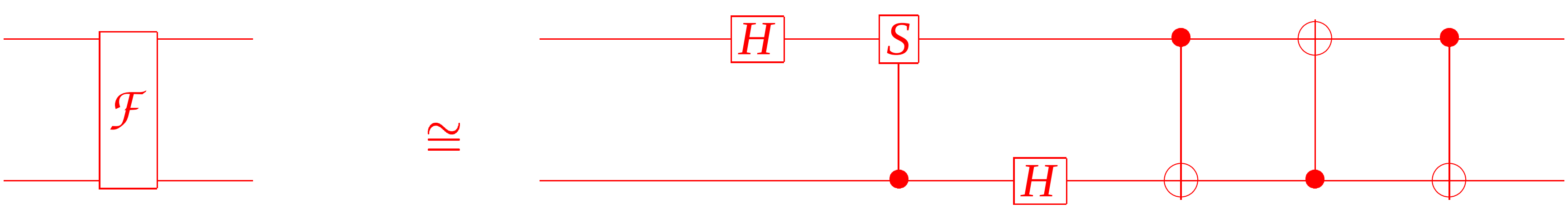
- good quantum circuit design: find tensor factors of computation $u$

# Example: $\mathcal{F}$ the Two-Qubit Fourier Transform in $\mathbb{Z}/4\mathbb{Z}$

- Relabelling $|00\rangle, \ldots |11\rangle$ as $|0\rangle, \ldots, |3\rangle$, the discrete Fourier transform $\mathcal{F}$:

$$|j\rangle \xrightarrow{\mathcal{F}} \frac{1}{2}\sum_{k=0}^{3}(\sqrt{-1})^{jk}|k\rangle \quad \text{or} \quad \mathcal{F} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

- one-qubit unitaries: $H = (1/\sqrt{2})\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $S = (1/\sqrt{2})\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$



# Outline

I. Introduction to Quantum Circuits
II. Two Qubit Circuits (CD)
III. Circuits for Diagonal Unitaries
IV. Half CNOT per Entry (CSD)
V. Differntial Topology & Lower Bounds

# The Magic Basis of Two-Qubit State Space

$$\begin{cases} |\mathsf{m0}\rangle &= (|00\rangle + |11\rangle)/\sqrt{2} \\ |\mathsf{m1}\rangle &= (|01\rangle - |10\rangle)/\sqrt{2} \\ |\mathsf{m2}\rangle &= (i|00\rangle - i|11\rangle)/\sqrt{2} \\ |\mathsf{m3}\rangle &= (i|01\rangle + i|10\rangle)/\sqrt{2} \end{cases}$$

Remark: Bell states up to global phase; global phases needed for theorem

**Theorem** (Lewenstein, Kraus, Horodecki, Cirac 2001)
Consider a $4 \times 4$ unitary $u$, global-phase chosen for $\det(u) = 1$

- Compute matrix elements in the magic basis
- (All matrix elements are real) $\Longleftrightarrow$ $(u = a \otimes b)$

# Two-Qubit Canonical Decomposition

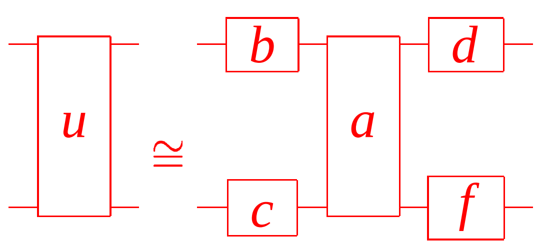
Two-Qubit Canonical Decomposition: Any $u$ a four by four unitary admits a matrix decomposition of the following form:

$$u = (d \otimes f)a(b \otimes c)$$

for $b \otimes c, d \otimes f$ are tensors of one-qubit computations, $a = \sum_{j=0}^{3} \mathrm{e}^{i\theta_j} |\mathrm{mj}\rangle\langle \mathrm{mj}|$

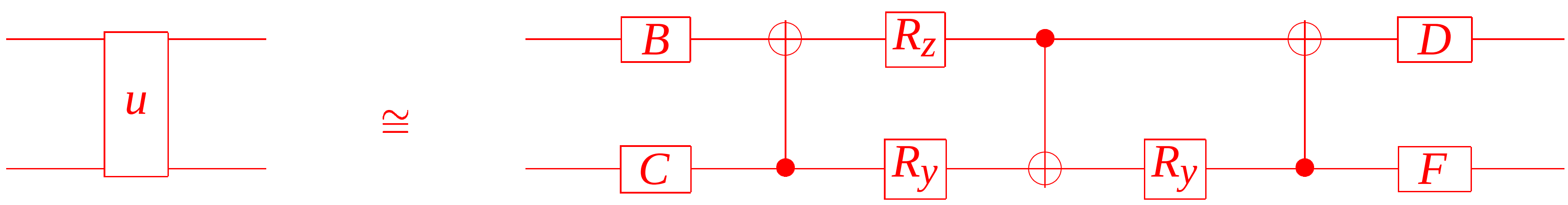
Note that $a$ applies relative phases to the magic or Bell basis.

Circuit diagram: For any $u$ a two-qubit computation, we have:



# Application: Three CNOT Universal Two-Qubit Circuit

- **Many groups: 3 CNOT circuit for $4 \times 4$ unitary:** (F.Vatan, C.P.Williams), (G.Vidal, C.Dawson), (V.Shende, I.Markov, B-)
  - Implement $a$ somehow, commute SWAP through circuit to cancel
  - Earlier B-,Markov: 4 CNOT circuit w/o SWAP, CD & naïve $a$

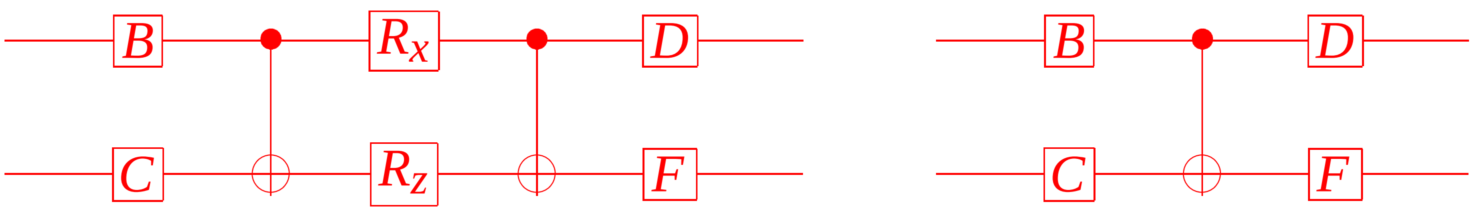


# Two-Qubit CNOT-Optimal Circuits

Theorem:(Shende,B-,Markov) Suppose $v$ is a $4 \times 4$ unitary normalized so $\det(v) = 1$. Label $\gamma(v) = (-i\sigma^y)^{\otimes 2} v (-i\sigma^y)^{\otimes 2} v^T$. Then any $v$ admits a circuit holding elements of $SU(2)^{\otimes 2}$ and $3$ CNOT's, up to global phase. Moreover, for $p(\lambda) = \det[\lambda I_4 - \gamma(v)]$ the characteristic poly of $\gamma(v)$:

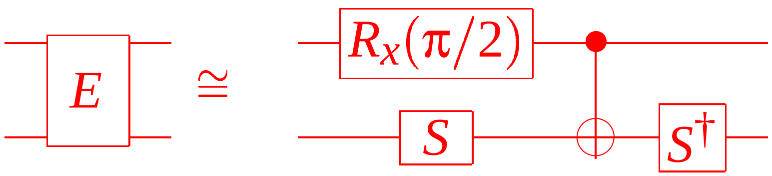
- ($v$ admits a circuit with $2$ CNOT's) $\Longleftrightarrow$ ($p(\lambda)$ has real coefficients)
- ($v$ admits a circuit with $1$ CNOT) $\Longleftrightarrow$ ($p(\lambda) = (\lambda + i)^2 (\lambda - i)^2$)
- ($v \in SU(2) \otimes SU(2)$) $\Longleftrightarrow$ ( $\gamma(v) = \pm I_4$ )

# Optimal Structured Two-qubit Circuits




- Quantum circuit identities: All $1,2$ CNOT diagrams reduce to these

- Computing parameters: useful to use operator $E$, $E|j\rangle = |\text{mj}\rangle$



# Outline

I. Introduction to Quantum Circuits
II. Two Qubit Circuits (CD)
III. Circuits for Diagonal Unitaries
IV. Half CNOT per Entry (CSD)
V. Differntial Topology & Lower Bounds

# Relative Phase Group

- Easiest concievable $n$-qubit circuit question: How to build circuits for

$$A(2^n) \;=\; \left\{ \sum_{j=0}^{2^n-1} \mathrm{e}^{i\theta_j} |j\rangle\langle j| \;;\; \theta_j \in \mathbb{R} \right\}?$$

- $A(2^n)$ commutative $\Longrightarrow$ vector group
  - $\log : A(2^n) \to \mathfrak{a}(2^n)$ carries matrix multiplication to vector sum
  - Strategy: build decompositions from vector space decompositions
  - Subspaces encoded by characters, i.e. continuous group maps $\chi : A(2^n) \to \{\mathrm{e}^{it}\}$

# Characters Detecting Tensors

- $\ker \log \chi$ is a subspace of $\mathfrak{a}(2^n)$

- Subspaces $\bigcap_j \ker \log \chi_j$ exponentiate to closed subgroups

Example: $a = \sum_{j=0}^{2^n-1} z_j |j\rangle\langle j| \in A(2^n)$ has $a = \tilde{a} \otimes R_z(\alpha)$ if and only if

$$z_0/z_1 \;=\; z_2/z_3 \;=\; \cdots \;=\; z_{2^n-2}/z_{2^n-1}$$

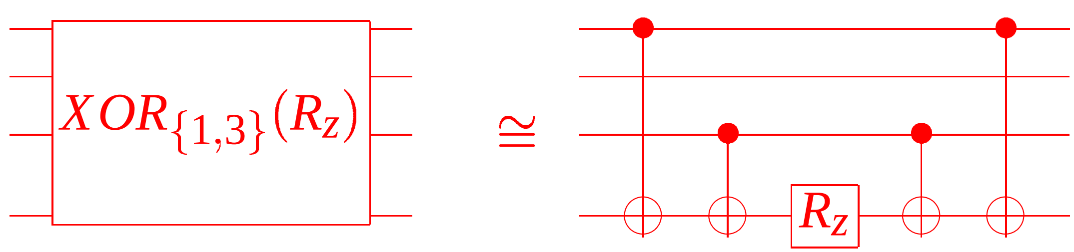
So $a$ factors on the bottom line if and only if $a \in \bigcap_{j=0}^{2^{n-1}-1} \ker \chi_j$
for $\chi_j(a) = z_{2j} z_{2j+2}/(z_{2j+1} z_{2j+3})$.

# Circuits for $A(2^n)$

**Outline of Synthesis for $A(2^n)$:**

- Produce circuit blocks capable of setting all $\chi_j = 1$
- After $a = \tilde{a} \otimes R_z$, induct to $\tilde{a}$ on top $n-1$ lines

**Remark:** $2^{n-1}-1$ characters to zero $\Longrightarrow 2^{n-1}-1$ blocks, i.e. one for each nonempty subset of the top $n-1$ lines



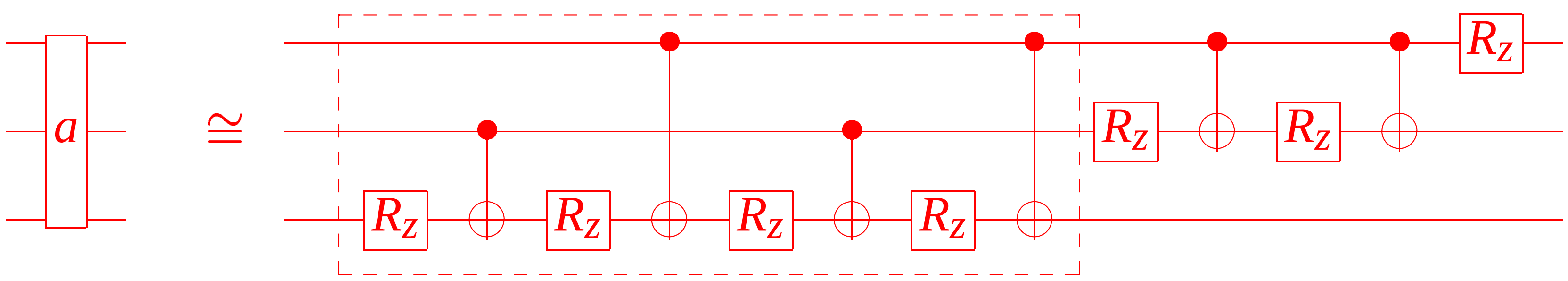
# Circuits for $A(2^n)$, Cont.

Tricks in Implementing Outline:

- If $\#[(S_1 \cup S_2) - (S_1 \cap S_2)] = 1$, then all but one CNOT in center of $XOR_{S_1}(R_z)\, XOR_{S_2}(R_z)$ cancel.

- Subsets in Gray code: most CNOTs cancel

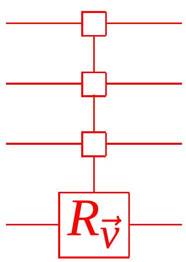
- Final count: $2^n - 2$ CNOTs



# Uniformly Controlled Rotations (M.Möttönen, J.Vartiainen)

Let $\vec{v}$ be any axis on Block sphere. Uniformly-controlled rotation requires $2^{n-1}$ CNOTs:

$$\bigwedge_k^{\text{uni}}[R_{\vec{v}}] = \begin{pmatrix} R_{\vec{v}}(\theta_0) & \mathbf{0}_2 & \cdots & \mathbf{0}_2 \\ \mathbf{0}_2 & R_{\vec{v}}(\theta_1) & \cdots & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \ddots & \mathbf{0}_2 \\ \mathbf{0}_2 & \mathbf{0}_2 & \cdots & R_{\vec{v}}(\theta_{2^{n-1}-1}) \end{pmatrix}$$




Example: Outlined block is diag$[R_z(\theta_1), R_z(\theta_2), \cdots, R_z(\theta_{2^{n-1}})] = \bigwedge_{n-1}^{\text{uni}}[R_z]$ up to SWAP of qubits $1,n$

**Shende, q-ph/0406176:** Short proof of $2^{n-1}$ CNOTs using induction:
$\mathfrak{a}(2^n) = I_2 \otimes \mathfrak{a}(2^{n-1}) \oplus \sigma^z \otimes \mathfrak{a}(2^{n-1})$

# Outline

I. Introduction to Quantum Circuits
II. Two Qubit Circuits (CD)
III. Circuits for Diagonal Unitaries
IV. Half CNOT per Entry (CSD)
V. Differntial Topology & Lower Bounds

# Universal Circuits

Goal: Build a universal quantum circuit for $u$ be $2^n \times 2^n$ unitary evolution

- Change rotation angles: any $u$ up to phase
- Preview: At least $4^n - 1$ rotation boxes $R_{\vec{v}}$, at least $\frac{1}{4}(4^n - 3n - 1)$ CNOTs
- Prior art
  - Barenco Bennett Cleve DiVincenzo Margolus Shor Sleator J.Smolin Weinfurter (1995) $\approx 50n^2 \times 4^n$ CNOTs
  - Vartiainen, Möttönen, Bergholm, Salomaa, $\approx 8 \times 4^n$ (2003), $\approx 4^n$ (2004)

# Cosine Sine Decomposition

Cosine Sine Decomposition: Any $v$ a $2^n \times 2^n$ unitary may be written

$$v = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} c & -s \\ s & c \end{pmatrix} \begin{pmatrix} a_2 & 0 \\ 0 & b_2 \end{pmatrix} = (a_1 \oplus b_1)\gamma(a_2 \oplus b_2)$$

where $a_j, b_j$ are $2^{n-1} \times 2^{n-1}$ unitary, $c = \sum_{j=0}^{2^{n-1}-1} \cos t_j |j\rangle\langle j|$ and $s = \sum_{j=0}^{2^{n-1}-1} \sin t_j |j\rangle\langle j|$

- Studied extensively in numerical matrix analysis literature

- Fast CSD algorithms exist; reasonable on laptop for $n = 10$

# Strategy for $\approx 4^n/2$ CNOT Circuit

- Use CSD for $v = (a_1 \oplus b_1)\gamma(c_1 \oplus d_1)$

- Implement $\gamma = \begin{pmatrix} c & -s \\ s & c \end{pmatrix}$ as uniformly controlled rotations
  - uniform control $\Longrightarrow$ few CNOTs

- Implement $a_j \oplus b_j = \begin{pmatrix} a_j & 0 \\ 0 & b_j \end{pmatrix}$ as quantum multiplexor
  - Also includes uniformly controlled rotations, also inductive

- Induction ends at specialty two-qubit circuit

# Quantum Multiplexors

- Multiplexor: route computation as control bit $0,1$

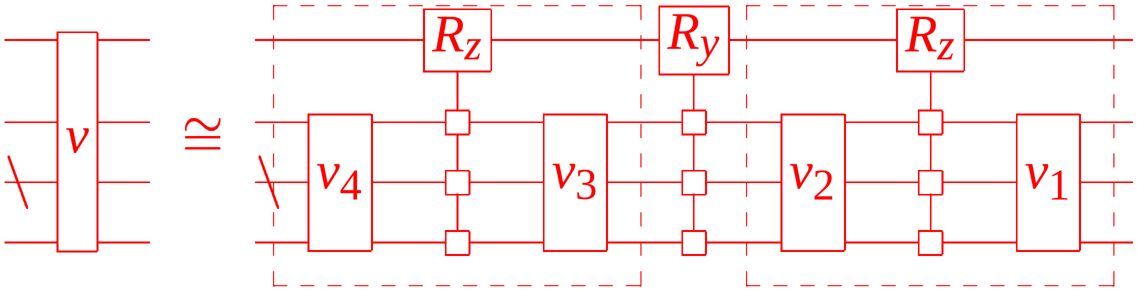
- $v = a \oplus b$: Do $a$ or $b$ as top qubit $|0\rangle$, $|1\rangle$

- Diagonalization trick: Solve following system, $d \in A(2^{n-1})$, $u,w$ each some $2^{n-1} \times 2^{n-1}$ unitary

$$\begin{cases} a &= udw \\ b &= ud^{\dagger}w \end{cases}$$

- Result: $a \oplus b = (u \oplus u)(d \oplus d^{\dagger})(w \oplus w) = (I_2 \otimes u) \wedge_{n-1}^{\text{uni}}[R_z](I_2 \otimes w)$

# Circuit for $(1/2)$ CNOT per Entry




- Outlined sections are multiplexor implementations
- Cosine Sine matrix $\gamma$: uniformly controlled $\wedge_{n-1}^{\text{uni}}[R_y]$
- Induction ends w/ $2$-qubit specialty circuit

# Circuit Errata

- Lower bound $\Longrightarrow$ (can be improved by no more than factor of $2$)

- $21$ CNOTs in $3$ qubits: currently best known

- $\approx 50\%$ CNOTs on bottom two lines
  - Adapts to spin-chain architecture with $(4.5) \times 4^n$ CNOTs
  - Quantum charge couple device (QCCD) with $3$ or $4$ qubit chamber?

# Outline

I. Introduction to Quantum Circuits
II. Two Qubit Circuits (CD)
III. Circuits for Diagonal Unitaries
IV. Half CNOT per Entry (CSD)
V. Differntial Topology & Lower Bounds

# Sard's Theorem

**Def:** A critical value of a smooth function of smooth manifolds $f : M \to N$ is any $n \in N$ such that there is some $p \in M$ with $f(p) = n$ with the linear map $(df)_p : T_pM \to T_nN$ not onto.

**Sard's theorem:** The set of critical values of any smooth map has measure zero.

**Corollary:** If dim $M <$ dim $N$, then image(f) is measure $0$.

- $U(2^n) = \{u \in \mathbb{C}^{2^n \times 2^n} ;\, uu^\dagger = I_{2^n}\}$: smooth manifold

- Circuit topology $\tau$ with $k$ one parameter rotation boxes induces smooth evaluation map $f_\tau : U(1) \times \mathbb{R}^k \to U(2^n)$

# Dimension-Based Bounds

- Consequence: Any universal circuit must contain $4^n - 1$ one parameter rotation boxes

- No consolidation: Boxes separated by at least $\frac{1}{4}(4^n - 3n - 1)$ CNOTs
  - $v$ Bloch sphere rotation: $v = R_x R_z R_x$ or $v = R_z R_x R_z$
  - Diagrams below: consolidation if fewer CNOTs

# On-going Work

- Subgroups $H$ of unitary group $U(2^n)$
  - More structure, smaller circuits?
  - Symmetries encoded within subgroups $H$
  - Native gate libraries?

- Special purpose circuits
  - Backwards: quantum circuits for doing numerical linear algebra?
  - Entanglement dynamics and circuit structure

## `http://www.arxiv.org` **Coordinates**

- Two-qubits: `q-ph/0308045`
- Diagonal circuits: `q-ph/0303039`
- Uniform control: `q-ph/0404089`
- $(1/2)$ CNOT/entry: `q-ph/0406176`
- Circuit diagrams by `Qcircuit.tex`: `q-ph/0406003`