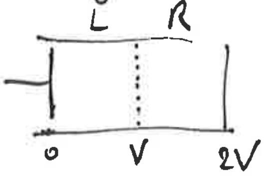
2x2 DECOMPOSITION OF QUANTUM & CLASSICAL REVERSIBLE CIRCUITS

(1) CLASSICAL REVERSIBLE : why? → $\boxed{\text{LANDAUER PRINCIPLE: Erasing information causes heat production!}}$

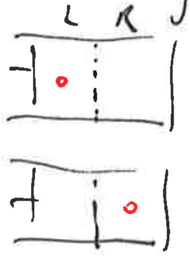
Toy model: Thermodynamics of 1 particle ideal gas in a piston. pneumatic cylinder with a piston



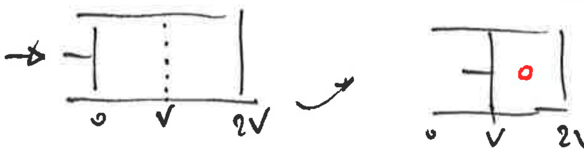
2 possibilities of the particle occupying

$+$ / $-$ defines a bit of information → associated entropy $S = k \ln 2$

$|0\rangle = |L\rangle =$ / $|1\rangle = |R\rangle =$



→ Goal: ERASE the information (at T = cst). →



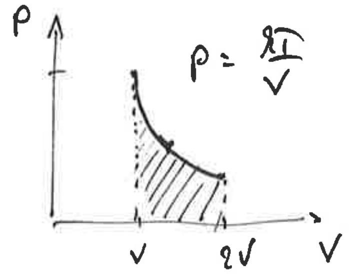
$(S = k \ln 1 = 0)$

- piston is moved adiabatically
- ideal gas $\Delta E = \frac{3}{2} k \Delta T = 0$.

Thermodynamics: $\Delta E = \underset{\text{work}}{\Delta W} + \underset{\text{heat exchange}}{\Delta Q}$ $\qquad \Delta W = -P$

ideal gas: $pV = kT \qquad \underline{\Delta E = 0}$.

$dE = 0 \rightarrow \delta W + \delta Q = 0 \rightarrow \delta Q = -\delta W \rightarrow \Delta Q = -\int_{2V}^{V} P\, dV$



$p = \frac{kT}{V}$

$= -\int_{2V}^{V} \frac{kT}{V}\, dV$

$= -kT\,[\ln V - \ln 2V]$

$\boxed{\Delta Q = kT \ln 2}$

→ By erasing one bit of information, we dissipate $\Delta Q = kT \ln 2$ info

note: $kT \approx 25.7$ meV at $T = 298$ K

(*) RESET TO ONE : IRREVERSIBLE GATE → It is impossible to reconstruct the input from the output

A	Q
0	1
1	1

how to make it reversible? ADD another bit Q that follows A

A	B	P	Q
0	1	1	0
1	1	1	1
0	0	0	0
1	0	0	1

follow

$\boxed{\text{SWAP GATE}}$

$P = B$
$Q = A$

How to "reset"?

A: set $B = 1$ & SWAP GATE → info about A is retained in Q!

note: a computation is a "reshuffling" of $(2^2)!$ strings

(*) LOGICAL GATE? e.g. AND

A B	R = AB
0 0	0
0 1	0
1 0	0
1 1	1

impossible to add only one

→ add "2" more bits to keep info about A & B.

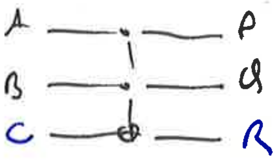
A	B	C	P	Q	R
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	0
1	1	0	1	1	1
0	0	1	0	0	1
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	0

$P = A$

$Q = B$

$R = C \oplus A \cdot B$

→ $\boxed{\text{TOFFOLI GATE}}$ CCNOT



importance: UNIVERSAL GATE

· makes the logical AND → non-linear f'ie so, universal

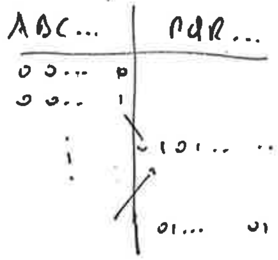
· CNOT  only makes linear f'ies (not universal)

· generalizable to CCC... CNOT.

note again: a computation is a "reshuffling" of $(2^N)!$ strings.

A reversible computation on w bits is a permutation on (2^w)! things

group S_{2^w}

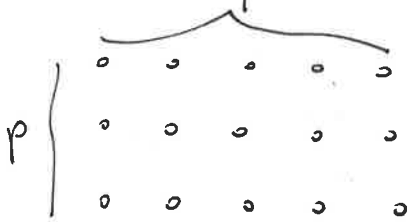


→ Q: How will you decompose?

A: BIRKHOFF theorem.

→ **Theorem** (Birkhoff).

Given a permutation of $n = pq$ elements, it can be decomposed into



(a) p permutations of q elements (rows)

q " " p " (column)

p " " q " (rows.)

(b) dual

example (slides)

for reversible computation $n = 2^w = 2 \cdot 2^{w-1}$

(a) $2^{w-1} \cdot S_2$ (col)

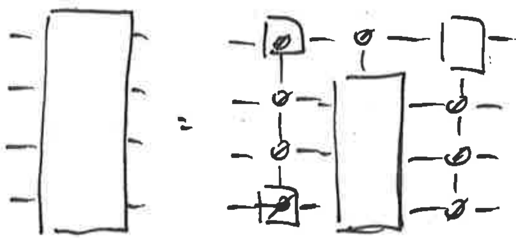
$2 \cdot S_{2^{w-1}}$ (row)

$2^{w-1} \cdot S_2$ (col)

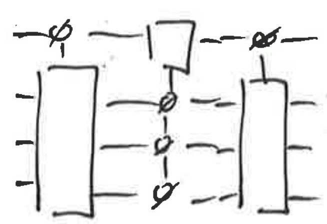
(b) $2 \cdot S_{2^{w-1}}$ (row)

$2^{w-1} \cdot S_2$ (col)

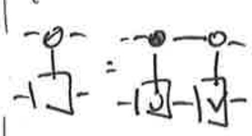
$2 \cdot S_{2^{w-1}}$ (row).



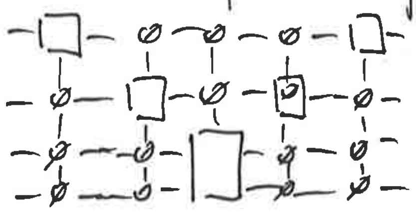
=



note



↓ further decomposition

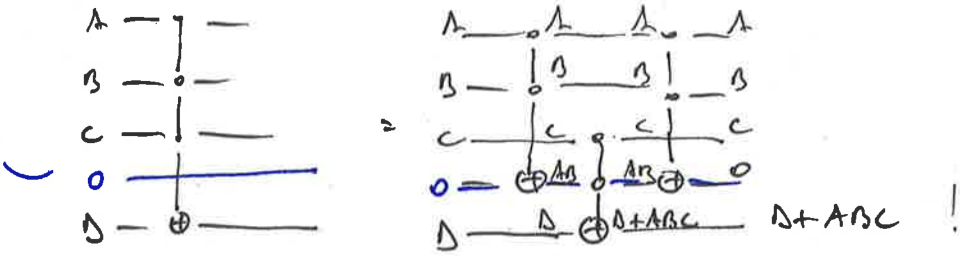


almost efficient: $2w-1$ CCC..NOT

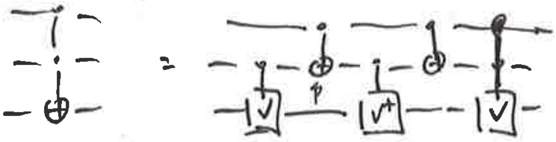
→ $2w-1$

TOF Further reduction: CCC…NOT → TOFFOLI (NOT CNOT).

add one



Then comes quantum! → further reduction of toffoli → 2 (qu)bits



$-\boxed{V}- \; = \; -\boxed{\sqrt{NOT}}-$

V: square-root of ~~root~~ NOT → $V^2 = X$

~~group structure~~ $V = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$

group structure $V \in U(2)$

$\cup$

$X \in S_2$ $\quad \det(V) = i \neq 1$ →

note: $(V^\dagger)^2 V^2 X = (V^\dagger)^2 X X$

$X = (V^\dagger)^2.$

note: line sum of V:

$$\begin{array}{cc} \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} & \begin{matrix} 1 \\ 1 \end{matrix} \\ \begin{matrix} 1 & \quad 1 \end{matrix} & \end{array}$$

equal to $\underline{\underline{1}}$

easy to check: equal line sums form a (semi) group.

→ decomposition possible in terms of permutation matrices (

$$V = \frac{1}{2}(1+i)\mathbb{1} + \frac{(1-i)}{2} NOT$$

$$= \frac{(1+i)}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{(1-i)}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

(cf. Birkhoff-von Neumann)

generalise this: what are the unitary line-sum = 1 ones!

$$\begin{cases} U = (1-t)\mathbb{1} + t\, NOT & (\to \text{implies linesum} = 1) \\ U^\dagger U = \mathbb{1} & (\to \text{implies unitarity}) \end{cases}$$

solution:

$$t = \frac{1}{2}(1 - e^{i\theta})$$

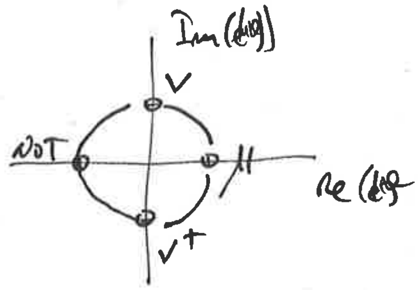
$$\Rightarrow \boxed{U(\theta) = \frac{1}{2}(1 + e^{i\theta})\mathbb{1} + \frac{1}{2}(1 - e^{i\theta})\,NOT.}$$

$U(\theta=0) = \mathbb{1}$

$U(\theta=\pi) = NOT$

$U(\theta=\frac{\pi}{2}) = V$

$U(\theta=-\frac{\pi}{2}) = V^{+}$

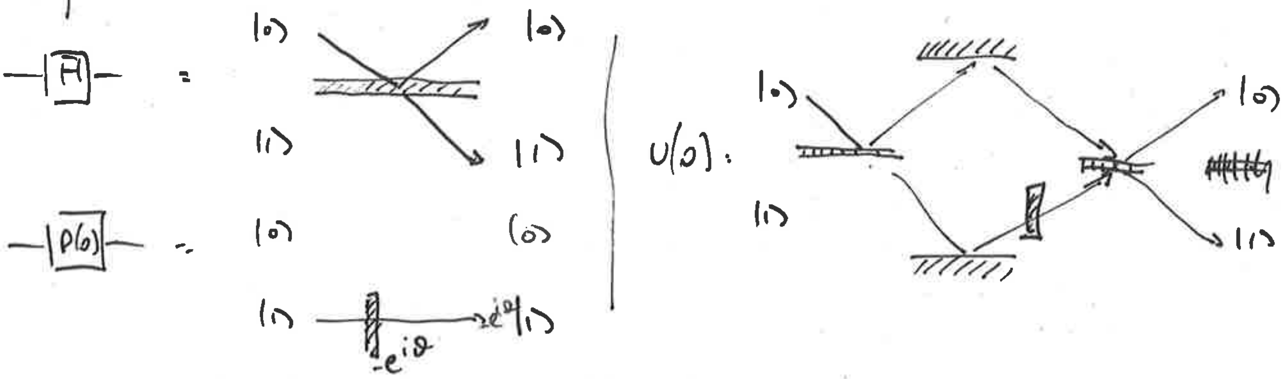


MATH → 1-parameter group. $\theta \in [0, 2\pi]$. ~ isomorphic to $U(1)$

similarity transform with H.

$$H\,U(\theta)\,H = \begin{pmatrix} 1 & 0 \\ 0 & -e^{i\theta} \end{pmatrix} \rightarrow U(\theta) = H\,P(\theta)\,H$$

PHYSICS: Beamsplitters & Phases



+ : physically possible with optical setup

− : # channels = dim($\mathcal{H}$) ....

generalization: $XU(M)$: Unitary matrices with linesum 1

$$XU(M) \cong U(M-1)$$

$$\rightarrow F_M^{+} X F_M = \begin{pmatrix} 1 & 0 \\ 0 & U(M-1) \end{pmatrix}$$

Q: Is it possible to "SCALE" $U(m)$ to $XU(m)$?

A. Yes, SINKHORN normal form (cfr Talk Martin Idel).

$$\underbrace{\begin{pmatrix} e^{i\alpha_1} & & & \\ & e^{i\alpha_2} & & \\ & & \ddots & \\ & & & e^{i\alpha_m} \end{pmatrix}}_{L} \begin{pmatrix} & & \\ & U(m) & \\ & & \end{pmatrix} \underbrace{\begin{pmatrix} e^{i\beta_1} & & & \\ & e^{i\beta_2} & & \\ & & \ddots & \\ & & & e^{i\beta_m} \end{pmatrix}}_{R} = XU(m).$$

+ : simple decomposition

− : not compatible with (qu)bit structure

| sinkhorn: $m \to m-1 \to m-2 \dots$
| (qu)bit: $2^w \to 2^{w-1} \to 2^{w-2} \dots$

$$U(2^w) \to L\,U(2^w-1)\,R = XU(2^{w-1}) \to F^\dagger XU(2^{w-1}) F = U(2^w-1) \dots$$

Special case: $n=2$ $\quad U(2) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \frac{1}{2}\begin{pmatrix} 1+t & 1-t \\ 1-t & 1+t \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$ $\quad a,b,c,t \in U(1).$

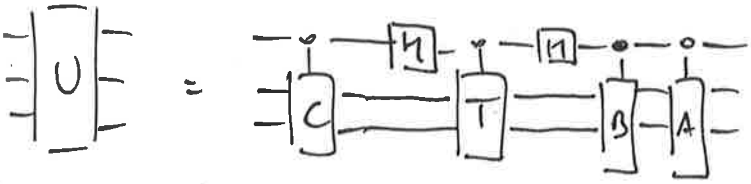
Special case: $n=2^w$ (FÜHR & RZESZOTNIK LIN ALG APP 484, 86 (2015)).

$$\boxed{U(2m) = \left(\begin{array}{c:c} A & 0 \\ \hdashline 0 & B \end{array}\right) \frac{1}{2}\left(\begin{array}{c:c} 1+T & 1-T \\ \hdashline 1-T & 1+T \end{array}\right) \left(\begin{array}{c:c} 1 & 0 \\ \hdashline 0 & C \end{array}\right)} \quad A,B,C,T \in U(m).$$

+ : it is compatible with (qu)bit structure, because

$$H_1 \frac{1}{2}\begin{pmatrix} 1+T & 1-T \\ 1-T & 1+T \end{pmatrix} H_1 = \left(\begin{array}{c:c} 1 & 0 \\ \hdashline 0 & T \end{array}\right)$$

$$\to U(2m) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right) H_1 \begin{pmatrix} 1 & 0 \\ 0 & T \end{pmatrix} H \begin{pmatrix} 1 & 0 \\ 0 & C \end{pmatrix}$$



EXPLICIT CONSTRUCTION:

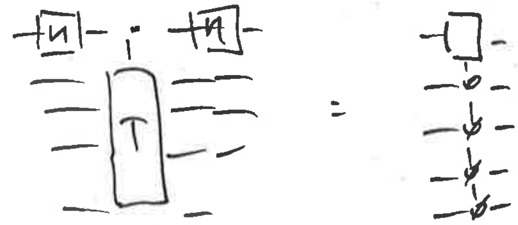
$U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}$ → polar decomposition. $U_{ij} = P_{ij} V_{ij}$ $\left| \begin{array}{l} P_{ij}^\dagger = P_{ij} \\ V_{ij}^\dagger V_{ij} = \mathbb{1} \end{array} \right.$

$$\rightarrow \left| \begin{array}{ll} A = (P_{11} \pm i P_{12}) V_{11} & \\ B = (P_{21} \mp i P_{22}) V_{21} & \\ T = V_{11}^\dagger (P_{11} \mp i P_{12})^2 & \left(= V_{21}^\dagger (P_{12} \mp i P_{21})^2\right) \\ C = \mp i V_{11}^\dagger V_{12} & \left(= \pm i V_{21}^\dagger V_{22}\right). \end{array} \right.$$

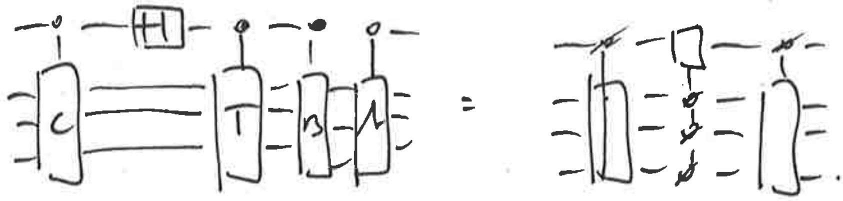
note: (1) A dual decomposition exists (like in Birkhoff).

(decomposition of HUH).

(2) for a permutation matrix



and $C \in S_{2n}$ (can be chosen).

→ 

BIRKHOFF!

e.g.: $P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ → $U_{11} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ x & 0 \end{pmatrix}$

$U_{12} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}$

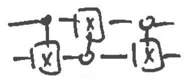
$A = \begin{pmatrix} 0 & 1 \\ ix & 0 \end{pmatrix}$ ← $\left| \begin{array}{l} U_{21} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix} \\ U_{22} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & w \\ 1 & 0 \end{pmatrix} \end{array} \right.$

$B = \begin{pmatrix} 1 & 0 \\ 0 & -iz \end{pmatrix}$

$T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

$C = \begin{pmatrix} 0 & -ix^* \\ -iy & 0 \end{pmatrix}$

choose: $\left| \begin{array}{l} y = z = i \\ x = i \end{array} \right.$ → $P = \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 1 & 0 \\ & & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & & 1 & \\ & 1 & & 0 \\ 1 & & 0 & \\ & 0 & & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix}$

→  ↵