# 1. General Propaganda

Why study quantum computation?

- Nice abstract maths
- Nonclassical complexity theory (and possible consequences for markets)
- Interesting applications of quantum mechanics

Aim of this course: get to interesting topics fast

- Essentials elements of quantum mechanics
- Important toy problems
- Famous problems:
    - Quantum phone book
    - Period finding
    - Quantum error correction

Required: Linear algebra (finite dimensions)

## 2. Notation for (C)bits

Dirac notation for one bit:

$$|0\rangle \quad \text{or} \quad |1\rangle$$

and for several Cbits:

$$|1\rangle \otimes |0\rangle \otimes |1\rangle \quad \text{or} \quad |1\rangle\,|0\rangle\,|1\rangle \quad \text{or} \quad |101\rangle \quad \text{or} \quad |5\rangle_3$$

or more generally

$$|x\rangle_3$$

In matrix notation:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Classical/computational basis.

# 3. Unitary operations on one bit

Identity

$$\mathbf{1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

flip or NOT

$$\mathbf{X} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

More abstract

$$\mathbf{Y} \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \mathbf{Z} \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

give identities

$$\mathbf{X}\,\mathbf{Y} = -\,\mathbf{Y}\,\mathbf{X} = -\,\mathbf{Z}$$
$$\mathbf{Y}\,\mathbf{Z} = -\,\mathbf{Z}\,\mathbf{Y} = -\,\mathbf{X}$$
$$\mathbf{Z}\,\mathbf{X} = -\,\mathbf{X}\,\mathbf{Z} = \mathbf{Y}$$

Unitary and anticommuting (like Pauli matrices and quaternions).

Hadamard operator (unitary)

$$\mathbf{H} = \tfrac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) \equiv \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

gives

$$\mathbf{H}\,\mathbf{X}\,\mathbf{H} = \mathbf{Z} \quad \mathbf{H}\,\mathbf{Z}\,\mathbf{H} = \mathbf{X}$$

# 4. Number operator

Introduce $\mathbf{n}$ and $\bar{\mathbf{n}} = \mathbf{1} - \mathbf{n}$

$$\mathbf{n} \equiv \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \bar{\mathbf{n}} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

or

$$\mathbf{n} = \tfrac{1}{2}(\mathbf{1} - \mathbf{Z}) \quad \bar{\mathbf{n}} = \tfrac{1}{2}(\mathbf{1} + \mathbf{Z})$$

Identities

$$\mathbf{n}^2 = \mathbf{n} \qquad \bar{\mathbf{n}}^2 = \bar{\mathbf{n}} \qquad \mathbf{n}\,\bar{\mathbf{n}} = \bar{\mathbf{n}}\,\mathbf{n} = 0 \qquad \mathbf{n} + \bar{\mathbf{n}} = \mathbf{1}$$

$$\mathbf{n}\,\mathbf{X} = \mathbf{X}\,\bar{\mathbf{n}} \qquad \bar{\mathbf{n}}\,\mathbf{X} = \mathbf{X}\,\mathbf{n}$$

# 5. Unitary operations on two bits

More notation

$$\mathbf{A} \otimes \mathbf{B} \, |x\rangle \otimes |y\rangle = \mathbf{A} \, |x\rangle \otimes \mathbf{B} \, |y\rangle \quad \text{or}$$
$$\mathbf{A}_1 \, \mathbf{B}_2 \, |x\rangle \, |y\rangle = \mathbf{B}_2 \, \mathbf{A}_1 \, |x\rangle \, |y\rangle$$

Swap operator

$$\mathbf{S}_{12} = \mathbf{n}_1 \, \mathbf{n}_2 + \bar{\mathbf{n}}_1 \, \bar{\mathbf{n}}_2 + \mathbf{X}_1 \, \mathbf{X}_2 (\mathbf{n}_1 \, \bar{\mathbf{n}}_2 + \bar{\mathbf{n}}_1 \, \mathbf{n}_2)$$

Important cNOT operator

$$\mathbf{C}_{12} = |x\rangle \, |x \oplus y\rangle$$

$$\mathbf{C}_{12} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \mathbf{C}_{21} \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Also

$$\mathbf{C}_{12} = \bar{\mathbf{n}}_1 + \mathbf{X}_2 \, \mathbf{n}_1$$

with implied tensor products.

# 6. An identity for cNOT

Rewrite

$$\mathbf{C}_{12} = \bar{\mathbf{n}}_1 + \mathbf{X}_2\,\mathbf{n}_1$$

using

$$\mathbf{n} = \tfrac{1}{2}(\mathbf{1} - \mathbf{Z}) \quad \bar{\mathbf{n}} = \tfrac{1}{2}(\mathbf{1} + \mathbf{Z})$$

to get

$$\begin{aligned} \mathbf{C}_{12} &= \tfrac{1}{2}(\mathbf{1} + \mathbf{Z}_1) + \tfrac{1}{2}\,\mathbf{X}_2(1 - \mathbf{Z}_1) \\ &= \tfrac{1}{2}(\mathbf{1} + \mathbf{X}_2) + \tfrac{1}{2}\,\mathbf{Z}_1(1 - \mathbf{X}_2) \end{aligned}$$

then use

$$\mathbf{H}\,\mathbf{X}\,\mathbf{H} = \mathbf{Z} \quad \mathbf{H}\,\mathbf{Z}\,\mathbf{H} = \mathbf{X}$$

to get

$$\mathbf{C}_{21} = \mathbf{H}_1\,\mathbf{H}_2\,\mathbf{C}_{12}\,\mathbf{H}_1\,\mathbf{H}_2$$

# 7. An identity for swap

Rewrite

$$\mathbf{S}_{12} = \mathbf{n}_1\,\mathbf{n}_2 + \bar{\mathbf{n}}_1\,\bar{\mathbf{n}}_2 + \mathbf{X}_1\,\mathbf{X}_2(\mathbf{n}_1\,\bar{\mathbf{n}}_2 + \bar{\mathbf{n}}_1\,\mathbf{n}_2)$$

using

$$\mathbf{n} = \tfrac{1}{2}(\mathbf{1} - \mathbf{Z}) \quad \bar{\mathbf{n}} = \tfrac{1}{2}(\mathbf{1} + \mathbf{Z})$$

to get

$$\mathbf{S}_{12} = \tfrac{1}{2}(\mathbf{1} + \mathbf{Z}_1\,\mathbf{Z}_2) + \tfrac{1}{2}\,\mathbf{X}_1\,\mathbf{X}_2(\mathbf{1} - \mathbf{Z}_1\,\mathbf{Z}_2)$$

and simpler

$$\mathbf{S}_{12} = \tfrac{1}{2}(\mathbf{1} + \mathbf{X}_1\,\mathbf{X}_2 - \mathbf{Y}_1\,\mathbf{Y}_2 + \mathbf{Z}_1\,\mathbf{Z}_2)$$

# 8. Qbits

Complex $2n$-dimensional vector space spanned by Cbits

$$\sum_x \alpha_x \left|x\right\rangle_n \quad \sum_x \left|\alpha_x\right|^2 = 1$$

any unitary operator meaningful.

*Born rule:* measure Qbit

$$\text{prob}(x) = \left|\alpha_x\right|^2$$

leaves state $\left|x\right\rangle_n$

*Probability amplitude* $\alpha_x$, not $\sqrt{\text{prob}}$.

To see why, consider

$$\mathbf{H}\left|0\right\rangle = \tfrac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle) \qquad \mathbf{H}^2\left|0\right\rangle = \left|0\right\rangle$$

# 9. Entangled states

In states like

$$|0\rangle\,|0\rangle + |1\rangle\,|1\rangle$$

(entangled) cannot use Born rule for one Qbit.

In state

$$\sum_{xy} \alpha_{xy}\,|x\rangle_m\,|y\rangle_n \quad \sum_{xy} |\alpha_{xy}|^2 = 1$$

measure left $m$ Qbits.

*Generalized Born rule:* rewrite as

$$\sum_x \alpha_x\,|x\rangle_m \left(\alpha_x^{-1}\textstyle\sum_y \alpha_{xy}\,|y\rangle_n\right) \quad \alpha_x = \textstyle\sum_y |\alpha_{xy}|^2$$

and now

$$\text{prob}(x) = |\alpha_x|^2$$

leaving state

$$|x\rangle_m \left(\alpha_x^{-1}\textstyle\sum_y \alpha_{xy}\,|y\rangle_n\right)$$

# 10. Qbit transforms and 3D Rotations

Pauli matrices

$$\begin{array}{ccc} \sigma_x & \sigma_y & \sigma_z \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ \mathbf{X} & -i\,\mathbf{Y} & \mathbf{Z} \end{array}$$

make some expressions more concise.

For example

$$\begin{aligned} \mathbf{S}_{12} &= \tfrac{1}{2}(\mathbf{1} + \mathbf{X}_1\,\mathbf{X}_2 - \mathbf{Y}_1\,\mathbf{Y}_2 + \mathbf{Z}_1\,\mathbf{Z}_2) \\ &= \tfrac{1}{2}(\mathbf{1} + \boldsymbol{\sigma}_1 \cdot \boldsymbol{\sigma}_2) \end{aligned}$$

General 1-Qbit unitary transform (up to $e^{i\delta}$)

$$\begin{aligned}\mathbf{U} &= \exp\left(i\tfrac{1}{2}\theta\ \mathbf{n}\cdot\boldsymbol{\sigma}\right) = \cos\tfrac{1}{2}\theta + i(\mathbf{n}\cdot\boldsymbol{\sigma})\sin\tfrac{1}{2}\theta \\ &= \cos\tfrac{1}{2}\theta\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + i\sin\tfrac{1}{2}\theta\begin{pmatrix}n_z & n_x - in_y\\ n_x + in_y & -n_z\end{pmatrix} \\ &= \mathbf{R}(\mathbf{n},\theta) \text{ say}\end{aligned}$$

(Proof in Mermin)

$$\begin{aligned}\mathbf{X} &= -i\,\mathbf{R}(\mathbf{x},\pi)\\ \mathbf{Y} &= \mathbf{R}(\mathbf{y},\pi)\\ \mathbf{Z} &= -i\,\mathbf{R}(\mathbf{z},\pi)\\ \mathbf{H} &= -i\,\mathbf{R}(\tfrac{1}{\sqrt{2}}(\mathbf{x}+\mathbf{z}),\pi)\end{aligned}$$

Can also transform operators: $\mathbf{A} \to \mathbf{U}\,\mathbf{A}\,\mathbf{U}^\dagger$ etc.

Leads to

$$\begin{aligned}\mathbf{H}\,\mathbf{X}\,\mathbf{H} &= \mathbf{Z}\\ \mathbf{H}\,\mathbf{Z}\,\mathbf{H} &= \mathbf{X}\\ \mathbf{H} &= \mathbf{R}(\mathbf{y},\tfrac{\pi}{4})\,\mathbf{X}\,\mathbf{R}(\mathbf{y},-\tfrac{\pi}{4})\end{aligned}$$

# 11. Further Dirac notation

Introduce inner product between $|\phi\rangle$ and $|\psi\rangle$

$$\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$$
$$\langle\phi| \left(\alpha\,|\lambda\rangle + \beta\,|\mu\rangle\right) = \alpha\langle\phi|\lambda\rangle + \beta\langle\phi|\mu\rangle$$
$$\phi \neq 0 \Rightarrow \langle\phi|\phi\rangle > 0$$

In computational basis

$$\langle x|y\rangle = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

Introduce dual vector space

$$\left(\,|\phi\rangle\,\right)^\dagger \quad \text{or} \quad \langle\phi|$$
$$\left(\alpha\,|\lambda\rangle + \beta\,|\mu\rangle\,\right)^\dagger = \alpha^*\,\langle\lambda| + \beta^*\,\langle\mu|$$

Components

$$\sum_{x=0}^{2^n-1} \alpha_x^*\,\langle x|_n \;\text{ as row of } \alpha_x^*$$
$$\sum_{x=0}^{2^n-1} \alpha_x\,|x\rangle_n \;\text{ as column of } \alpha_x$$

Outer product

$$|\phi\rangle\,\langle\psi|$$

Operators act to left or right

$$\langle\phi|\,\mathbf{A} = \left(\,\mathbf{A}^\dagger\,|\phi\rangle\,\right)^\dagger$$

and $\langle\phi|\,\mathbf{A}\,|\psi\rangle$ associative.

Also meaningful

$$\langle\phi|\,\mathbf{A}\,|\psi\rangle^\dagger = \langle\phi|\,\mathbf{A}\,|\psi\rangle^* = \langle\psi|\,\mathbf{A}^\dagger\,|\phi\rangle$$

Matrix element

$$\langle x|\,\mathbf{A}\,|y\rangle$$

and $\langle x|\phi\rangle\langle\psi|y\rangle$ deliberately ambiguous.

Projection operator

$$\mathbf{P}_\psi = |\psi\rangle \langle\psi|$$
$$\mathbf{1} = \sum_x |x\rangle \langle x|$$

In the Born rule

$$|\phi\rangle = \sum_x \langle x|\phi\rangle \, |x\rangle$$

so $\text{prob}(x) = |\langle x|\phi\rangle|^2$

Also in generalized Born rule

$$|\lambda\rangle \, |0\rangle + |\mu\rangle \, |1\rangle = \sum_x \alpha_x \, |x\rangle \;\; \alpha_x^{-1} \Big( \langle x|\lambda\rangle \, |0\rangle + \langle x|\mu\rangle \, |1\rangle \Big)$$
$$\alpha_x^2 = |\langle x|\lambda\rangle|^2 + |\langle y|\mu\rangle|^2$$

# 12. Spooky action at a distance

Hardy state $|\Psi\rangle$ and transforms

$$|\Psi\rangle = \tfrac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle) \qquad \text{no } |11\rangle$$

$$\mathbf{H}_a |\Psi\rangle = \tfrac{1}{\sqrt{6}}(2\,|00\rangle + |01\rangle + |11\rangle) \qquad \text{no } |10\rangle$$

$$\mathbf{H}_b |\Psi\rangle = \tfrac{1}{\sqrt{6}}(2\,|00\rangle + |10\rangle + |11\rangle) \qquad \text{no } |01\rangle$$

$$\mathbf{H}_a \mathbf{H}_b |\Psi\rangle = \tfrac{1}{2\sqrt{3}}(3\,|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

Consider $\langle 11| \mathbf{H}_a \mathbf{H}_b |\Psi\rangle$ (Alice and Bob measure 1)

- $\langle 01| \mathbf{H}_b |\Psi\rangle = 0$ (Bob gets 1 $\Rightarrow$ Alice gets 1)
- $\langle 10| \mathbf{H}_a |\Psi\rangle = 0$ (Alice gets 1 $\Rightarrow$ Bob gets 1))
- $\langle 11|\Psi\rangle = 0$ (Both can't get 1)

# 13. Computational process

To compute $f(x)$

$$\mathbf{U}_f(|x\rangle_n |y\rangle_m) = |x\rangle_n |y \oplus f(x)\rangle_m$$

and $\mathbf{U}_f \mathbf{U}_f = \mathbf{1}$

Take argument as

$$(\mathbf{H} \otimes \mathbf{H}) |00\rangle = \tfrac{1}{2}\big( |0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2 \big)$$

or more generally

$$\mathbf{H}^{\otimes n} |0\rangle_n = \tfrac{1}{2^n} \sum_{x=0}^{2^n-1} |x\rangle_n$$

We get

$$\mathbf{U}_f \left(\mathbf{H}^{\otimes n} \otimes \mathbf{1}^{\otimes m}\right) |0\rangle_n |0\rangle_m = \tfrac{1}{2^n} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_m$$

But . . . no-cloning theorem.

# 14. Deutsch's problem

$$f : \langle \text{one bit} \rangle \rightarrow \langle \text{one bit} \rangle$$

Four possibilities

| | $x = 0$ | $x = 1$ |
|---|---|---|
| $f_0$ | 0 | 0 |
| $f_1$ | 0 | 1 |
| $f_2$ | 1 | 0 |
| $f_3$ | 1 | 1 |

Problem: $f(0) = f(1)$?

Not necessarily trivial...

# 15. Deutsch algorithm

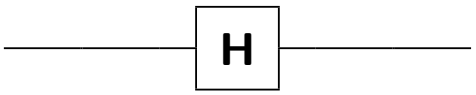
$$
\begin{aligned}
&\mathbf{U}_f(\mathbf{H}\otimes\mathbf{H})\,|1\rangle\,|1\rangle = \\
&\mathbf{U}_f\ \tfrac{1}{2}\big(\,|00\rangle - |10\rangle - |01\rangle + |11\rangle\,\big) = \\
&\quad \tfrac{1}{2}\big(\,|0\,f(0)\rangle - |1\,f(1)\rangle - |0\,\bar{f}(0)\rangle + |1\,\bar{f}(1)\rangle\,\big) = \\
&\quad \tfrac{1}{2}\big(\,|0\rangle - |1\rangle\,\big)\big(\,|f(0)\rangle - |\bar{f}(0)\rangle\,\big) \quad \text{if } f(0) = f(1) \\
&\quad \tfrac{1}{2}\big(\,|0\rangle + |1\rangle\,\big)\big(\,|f(0)\rangle - |\bar{f}(0)\rangle\,\big) \quad \text{if } f(0) \neq f(1)
\end{aligned}
$$

$$
(\mathbf{H}\otimes\mathbf{1})\,\mathbf{U}_f(\mathbf{H}\otimes\mathbf{H})\,|1\rangle\,|1\rangle = \begin{cases}
|1\rangle\,\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) & \text{if } 0\ 0 \\
|0\rangle\,\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) & \text{if } 0\ 1 \\
|0\rangle\,\frac{1}{\sqrt{2}}\big(\,|1\rangle - |0\rangle\,\big) & \text{if } 1\ 0 \\
|1\rangle\,\frac{1}{\sqrt{2}}\big(\,|1\rangle - |0\rangle\,\big) & \text{if } 1\ 1
\end{cases}
$$

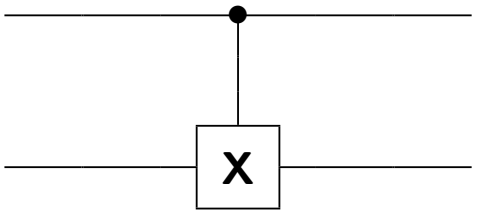
Is there an easier way to write $(\mathbf{H}\otimes\mathbf{H})\,\mathbf{U}_f(\mathbf{H}\otimes\mathbf{H})$?

# 16. Quantum circuits

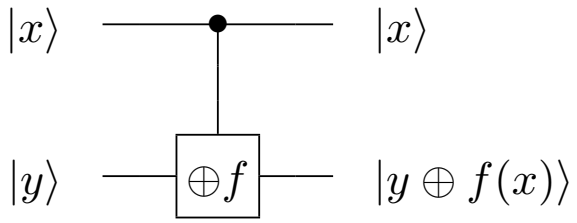
Hadamard gate



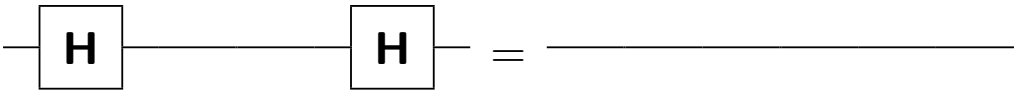

cNOT gate

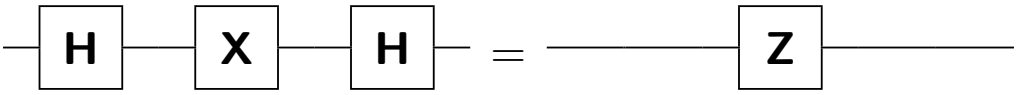


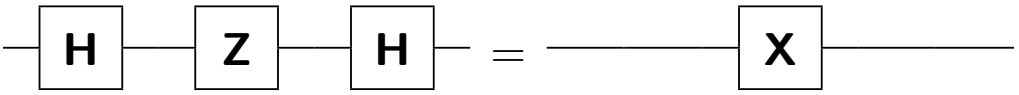

general computation



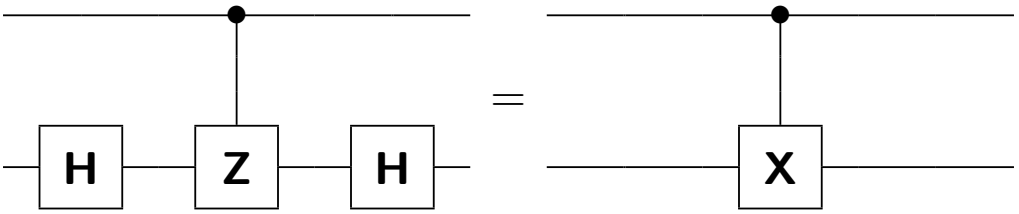
# 17. Circuit identities

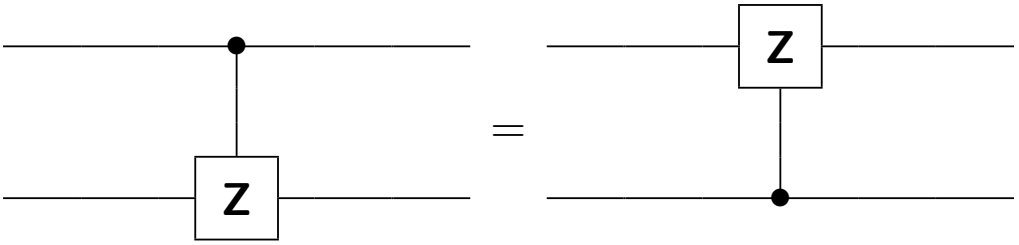


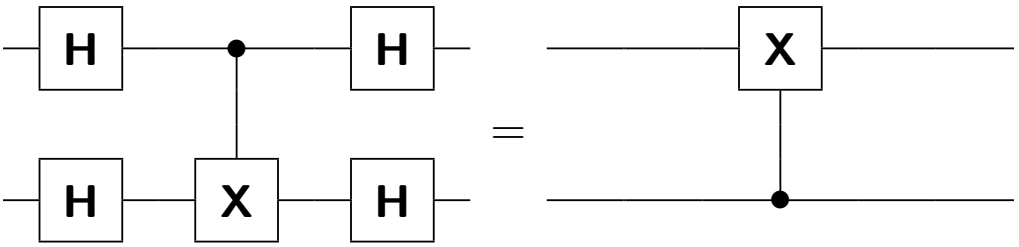



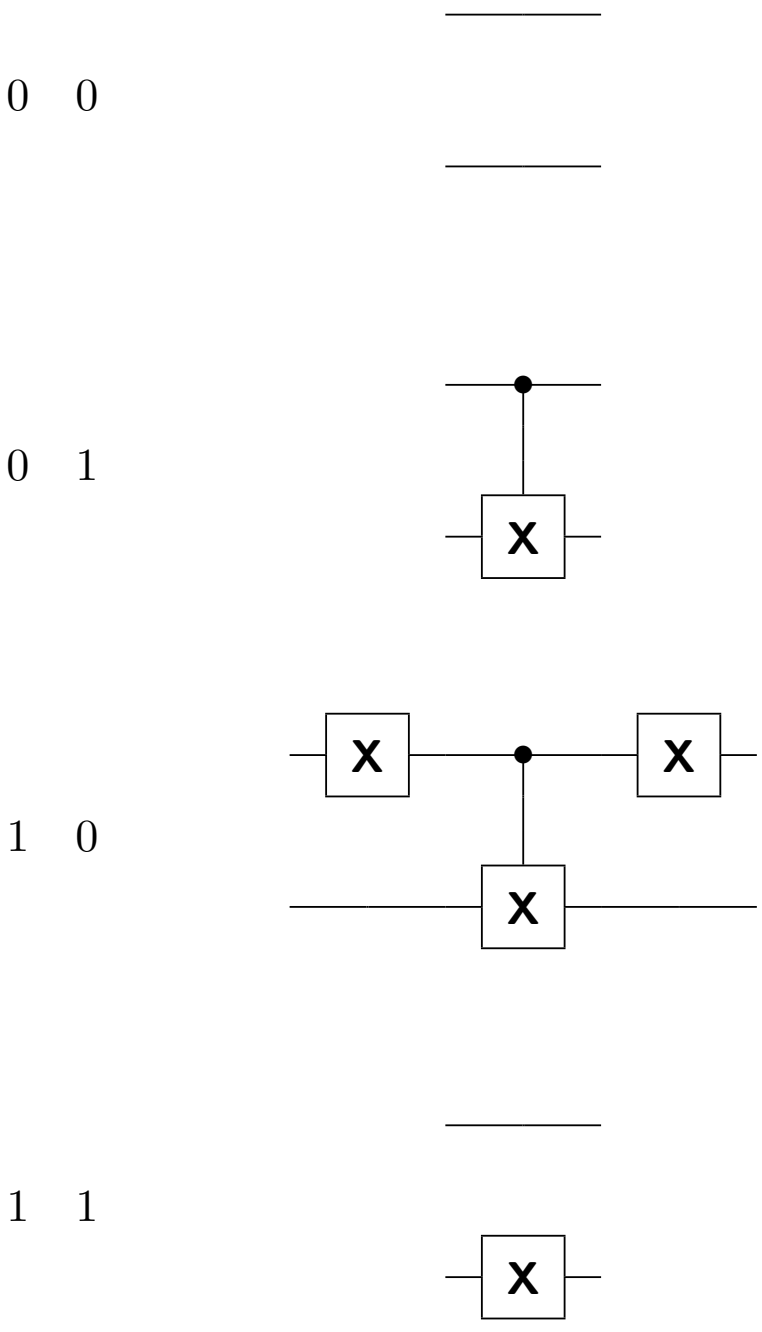
# 18. More Circuit identities



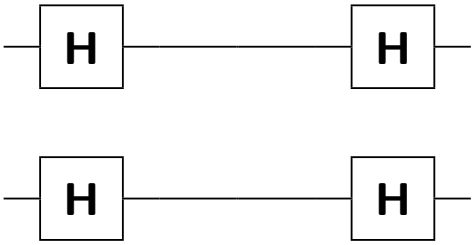



# 19. Deutsch problem

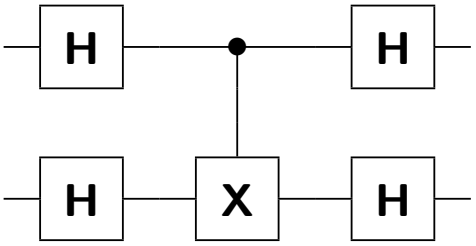


# 20. Deutsch solver

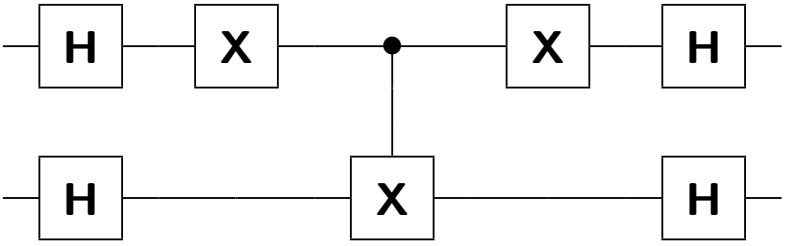
0 0



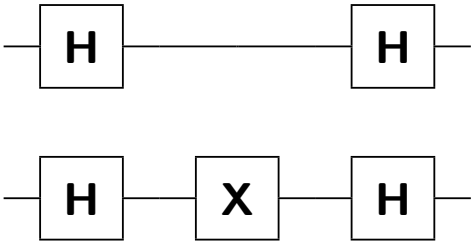

0 1



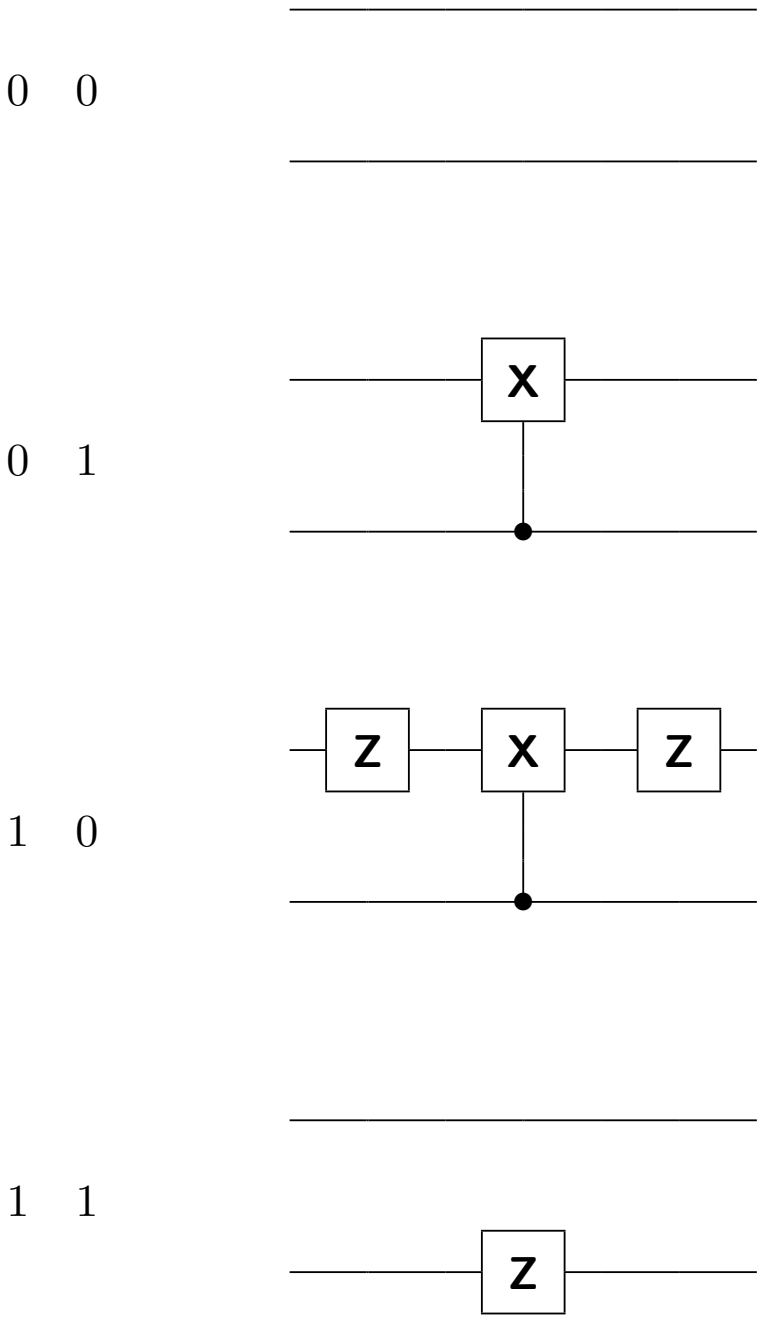

1 0



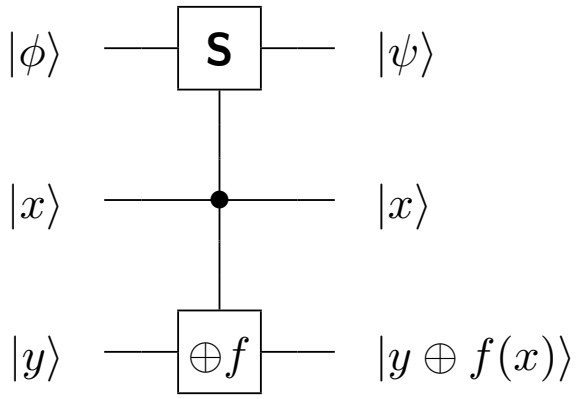

1 1

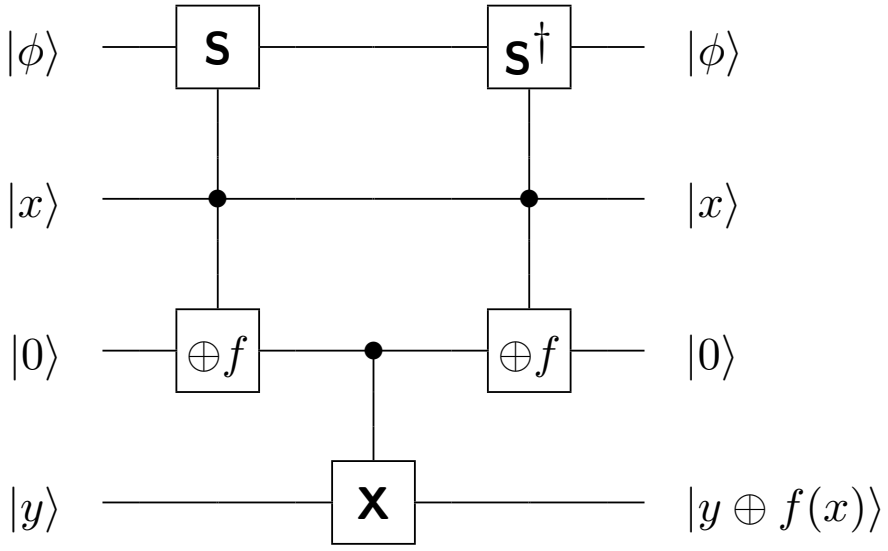


# 21. Deutsch solution



# 22. Subroutine Qbits



# 23. Bernstein-Vazirani problem

$$f : \langle n \text{ bits} \rangle \to \langle \text{one bit} \rangle$$
$$f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n = a \cdot x$$

Problem: determine $a_1 \ldots a_n$

Answer:

$$\mathbf{H}^{\otimes(n+1)} \mathbf{U}_f \mathbf{H}^{\otimes(n+1)} |0\rangle_n |1\rangle = |a\rangle_n |1\rangle$$

To show this, first note

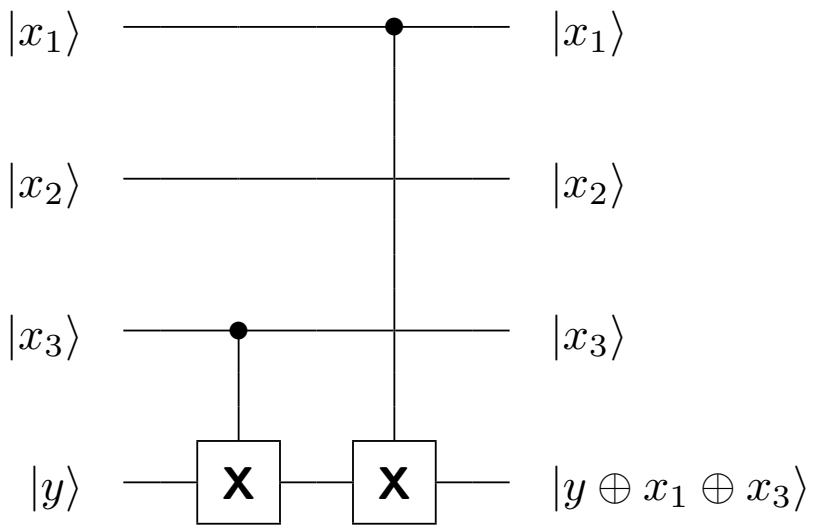
$$\mathbf{U}_f |x\rangle_n \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f(x)} |x\rangle_n \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\mathbf{U}_f |x\rangle_n (\mathbf{H}|1\rangle) = (-1)^{f(x)} |x\rangle_n (\mathbf{H}|1\rangle)$$

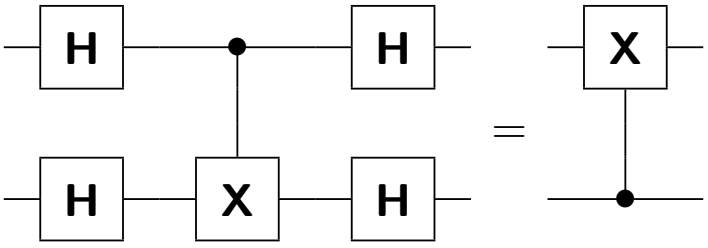
and

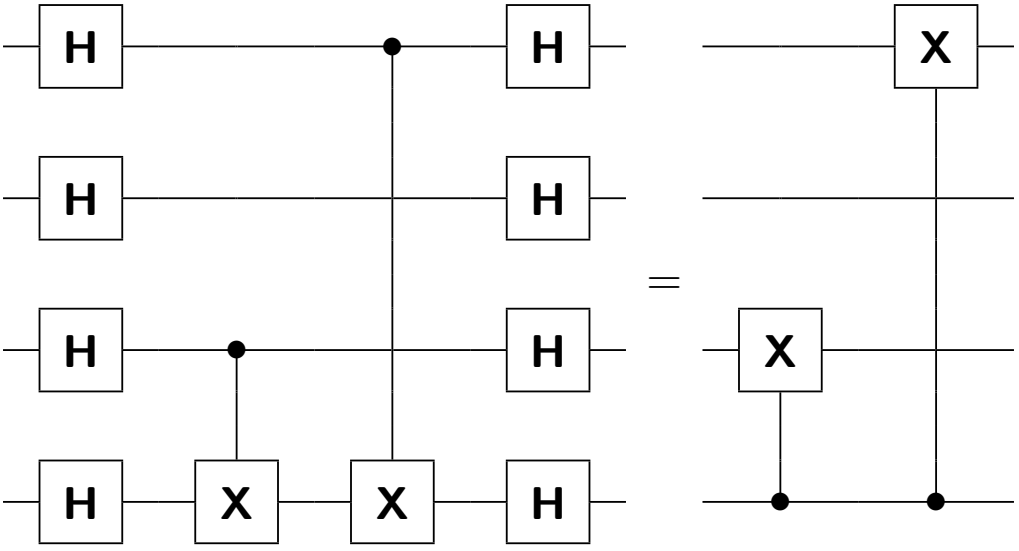
$$\mathbf{H}|x\rangle_1 = \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle) = \tfrac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle$$
$$\mathbf{H}^{\otimes n} |x\rangle_n = 2^{-n/2} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle_n$$

$$\mathbf{H}^{\otimes(n+1)}\,\mathbf{U}_f\,\mathbf{H}^{\otimes(n+1)}\,|0\rangle_n\,|1\rangle =$$
$$\mathbf{H}^{\otimes(n+1)}\,\mathbf{U}_f\left(2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle_n\right)(\mathbf{H}\,|1\rangle) =$$
$$2^{-n/2}\left(\mathbf{H}^{\otimes n}\sum_{x=0}^{2^n-1}(-1)^{a\cdot x}\,|x\rangle_n\right)|1\rangle =$$
$$2^{-n}\left(\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{a\cdot x+x\cdot y}\,|y\rangle_n\right)|1\rangle$$

If $y \neq a$, $x = 0, 1$ in a discrepant bit gives cancelling terms.


$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|y\rangle$
X
X
$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|y \oplus x_1 \oplus x_3\rangle$


H
H
H
X
H
=
X


H
H
H
H
H
H
H
X
X
H
=
X
X

# 24. Simon's problem

$$f : \langle n \text{ bits} \rangle \to \langle n-1 \text{ bits} \rangle$$
$$f(y) = f(x) \text{ iff } x \oplus y = a$$

Problem: determine $a$

Classically $O(2^{n/2})$ evaluations (details in Mermin).

In QC, evaluate

$$2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle \, |f(x)\rangle$$

then measure output Qbits $= f(x_0)$ (say). In Qbits now

$$\tfrac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle)$$

Now consider

$$\mathbf{H}^{\otimes n} \tfrac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle) =$$
$$2^{-(n+1)/2} \sum_{y=0}^{2^n-1} \left((-1)^{x_0 \cdot y} + (-1)^{(x_0+a)\cdot y}\right) |y\rangle =$$
$$2^{-(n-1)/2} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} \, |y\rangle$$

Measuring gives $y$ satisfying

$$a_1 y_1 \oplus a_2 y_2 \oplus \ldots \oplus a_n y_n = 0$$

Need $O(n \log n)$ iterations (details in Mermin).

# 25. Control-Unitary gates

Recall general $\mathbf{U}$ (up to $e^{i\alpha}$)

$$\begin{aligned}\mathbf{U} &= \exp\left(i\tfrac{1}{2}\theta\ \mathbf{n}\cdot\boldsymbol{\sigma}\right) = \cos\tfrac{1}{2}\theta + i(\mathbf{n}\cdot\boldsymbol{\sigma})\sin\tfrac{1}{2}\theta \\ &= \cos\tfrac{1}{2}\theta\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + i\sin\tfrac{1}{2}\theta\begin{pmatrix}n_z & n_x - in_y\\ n_x + in_y & -n_z\end{pmatrix}\end{aligned}$$

Given $\mathbf{b}$ can choose $\mathbf{W}$ such that

$$\mathbf{W}\,\mathbf{X}\,\mathbf{W}^\dagger = \mathbf{W}(\mathbf{x}\cdot\boldsymbol{\sigma})\,\mathbf{W}^\dagger = \mathbf{b}\cdot\boldsymbol{\sigma}$$

[$\mathbf{W}$ will be rotation matrix for $\mathbf{x}\to\mathbf{b}$]

Similarly

$$\mathbf{V}\,\mathbf{X}\,\mathbf{V}^\dagger = \mathbf{V}(\mathbf{x}\cdot\boldsymbol{\sigma})\,\mathbf{V}^\dagger = \mathbf{a}\cdot\boldsymbol{\sigma}$$

Since

$$(\mathbf{V}\,\mathbf{X}\,\mathbf{V}^\dagger)(\mathbf{W}\,\mathbf{X}\,\mathbf{W}^\dagger) = (\mathbf{a}\cdot\boldsymbol{\sigma})(\mathbf{b}\cdot\boldsymbol{\sigma}) = (\mathbf{a}\cdot\mathbf{b}) + i(\mathbf{a}\times\mathbf{b})\cdot\boldsymbol{\sigma}$$

we can choose $\mathbf{V},\mathbf{W}$ to give

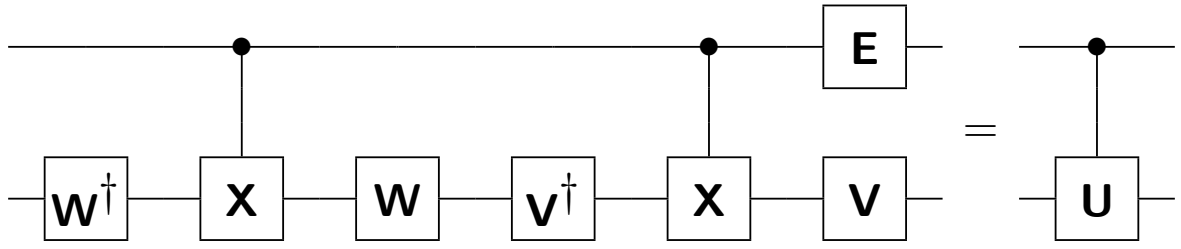
$$\mathbf{U} = (\mathbf{V}\,\mathbf{X}\,\mathbf{V}^\dagger)(\mathbf{W}\,\mathbf{X}\,\mathbf{W}^\dagger)$$

up to $e^{i\alpha}$

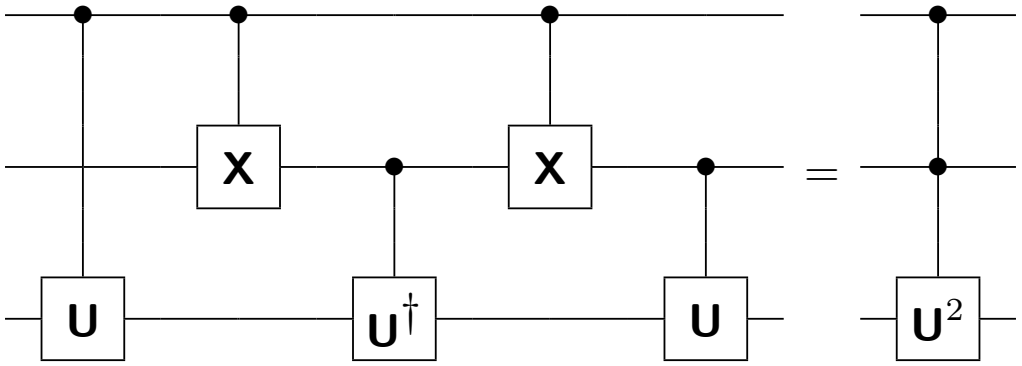
Now

- replace $\mathbf{X}$ with $c\,\mathbf{X}$ in $\mathbf{U} = (\mathbf{V}\,\mathbf{X}\,\mathbf{V}^\dagger)(\mathbf{W}\,\mathbf{X}\,\mathbf{W}^\dagger)$
- note $|x\rangle\, e^{i\alpha x}\, |y\rangle$ equivalent to $e^{i\alpha x}\, |x\rangle\, |y\rangle$

to get $c\,\mathbf{U}$

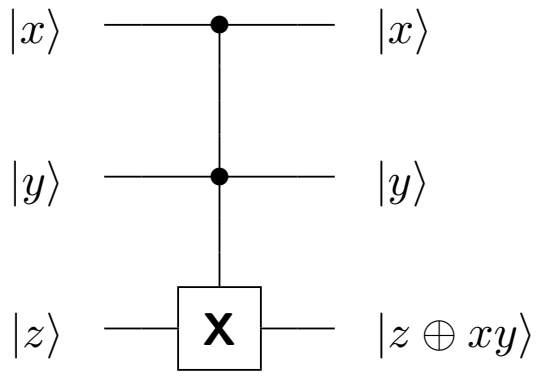


# 26. Toffoli gate




Hence can build Toffoli (aka ccNOT, NAND) gate

$$\mathbf{T}\,|x\rangle\,|y\rangle\,|z\rangle = |x\rangle\,|y\rangle\,|z \oplus xy\rangle$$
$$\mathbf{T}\,|1\rangle\,|1\rangle\,|z\rangle = |1\rangle\,|1\rangle\,|\bar{z}\rangle$$

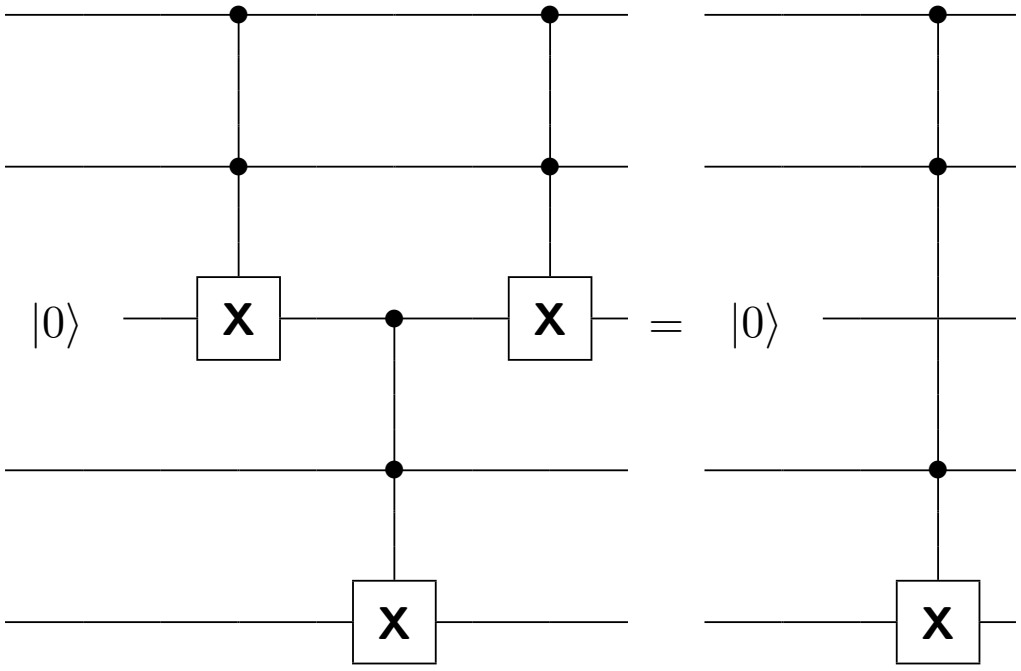



Enough for all Boolean algebra (hence classical reversible computation).

# 27. Cascaded ANDs

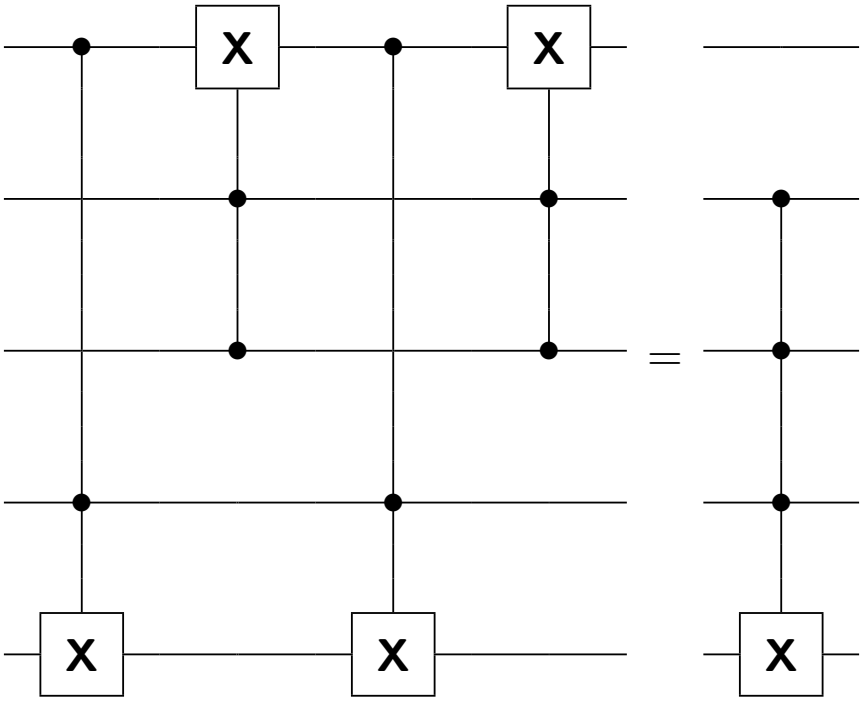
Several possible circuits

1) c$^n$ **X** using $(n-2)$ auxiliary Qbits




(cf Fig 4.4 in Mermin)

2) c$^n$ **X** using 1 ancilla (but more gates)




(cf Fig 4.7 in Mermin)

Complexity $O(n)$.

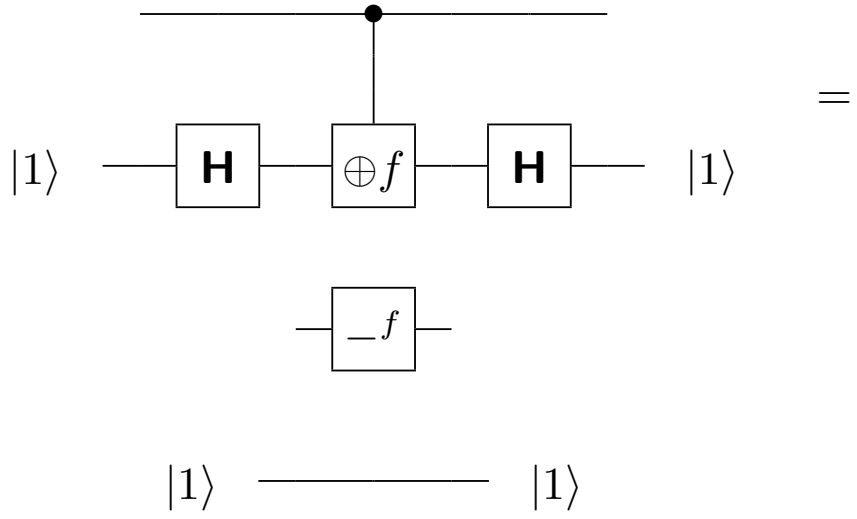
# 28. The phonebook problem

$$f : \langle n \text{ bits} \rangle \rightarrow \langle \text{one bit} \rangle$$

$$f(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{otherwise} \end{cases}$$

$$\mathbf{U}_f(|x\rangle_n |y\rangle) = |x\rangle_n |y \oplus f(x)\rangle$$

$$\mathbf{U}_f(|x\rangle_n \otimes \mathbf{H}|1\rangle) = (-1)^{f(x)} |x\rangle_n \otimes \mathbf{H}|1\rangle$$

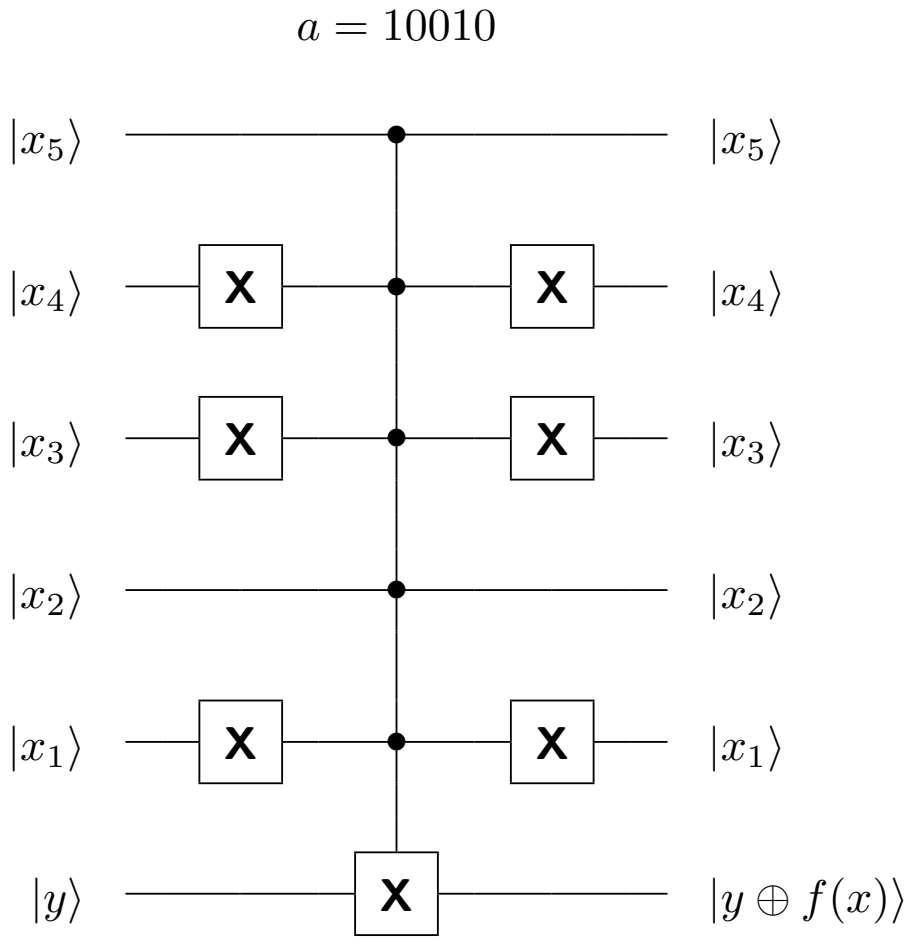



Reflection operator:

$$\mathbf{V}|x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} -|a\rangle & \text{if } x = a \\ |x\rangle & \text{otherwise} \end{cases}$$

$$\mathbf{V} = \mathbf{1} - 2|a\rangle\langle a|$$

# 29. Possible black box




(cf Fig 4.1 in Mermin)

Needs c$^n$ **X**

# 30. Another reflection operator

Recall

$$\mathbf{V} = \mathbf{1} - 2\,|a\rangle\,\langle a|$$

Define

$$\mathbf{V}_{|0\rangle} \equiv 1 - 2\,|0\rangle\,\langle 0| = \mathbf{X}^{\otimes n}(\mathrm{c}^{n-1}\,\mathbf{Z})\,\mathbf{X}^{\otimes n}$$

$$\mathbf{W} \equiv -\,\mathbf{H}^{\otimes n}\,\mathbf{V}_{|0\rangle}\,\mathbf{H}^{\otimes n} = 2\,\mathbf{H}^{\otimes n}\,|0\rangle\,\langle 0|\,\mathbf{H}^{\otimes n} - \mathbf{1}$$

Say

$$|\phi\rangle = \mathbf{H}^{\otimes n}\,|0\rangle_n = 2^{-n/2}\sum_{x=0}^{2^n-1}|x\rangle_n$$

then

$$\mathbf{W} = 2\,|\phi\rangle\,\langle\phi| - \mathbf{1}$$

# 31. Grover's search algorithm

Consider plane containing $|a\rangle$ and $|\phi\rangle$

$$|\phi\rangle = \cos\theta\,|a_\perp\rangle + \sin\theta\,|a\rangle$$

In this basis

$$\mathbf{W} = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} \qquad \mathbf{V} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and hence $\mathbf{W}\,\mathbf{V}$ rotates by $2\theta$

But

$$\sin\theta = \langle a|\phi\rangle = 2^{-n/2} \leq 1/\sqrt{N}$$

hence

$$\theta \simeq 2^{-n/2}$$

and

$$(\mathbf{W}\,\mathbf{V})^M\,|\phi\rangle \simeq |a\rangle \quad M \simeq \tfrac{\pi}{4}\,2^{n/2}$$

Complexity $O(\sqrt{N}\log N)$

# 32. Fourier transform

Most important integral transforms

$$F(k) = (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{\infty} e^{iky} f(y)\, dy$$
$$f(y) = (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{\infty} e^{-iky} F(k)\, dk$$

Discrete Fourier transform

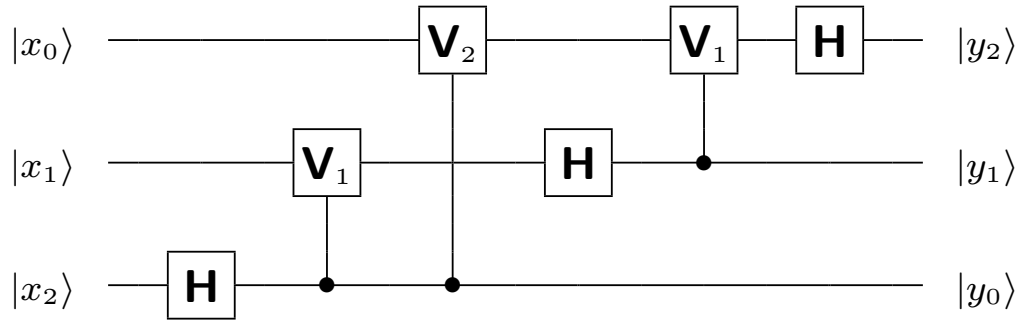
$$F(x) = 2^{-n/2} \sum_{y=0}^{2^n-1} \exp(2\pi ixy/2^n)\, f(y)$$
$$f(y) = 2^{-n/2} \sum_{x=0}^{2^n-1} \exp(-2\pi ixy/2^n)\, F(x)$$

Fast Fourier Transform (FFT) has complexity $O(n2^n)$

# 33. Quantum Fourier transform

$$\mathbf{U}_{\mathrm{FT}} \left|x\right\rangle_n = 2^{-n/2} \sum_{y=0}^{2^n-1} \exp(2\pi i x y/2^n) \left|y\right\rangle_n$$

Shor's algorithm:




(and its generalizations for $n > 3$) where

$$\mathbf{V}_k = \exp\left(i\pi\,\mathbf{n}\,/2^k\right)$$

Quantum complexity $O(n^2)$

# 34. Quantum FT operator

$$\mathbf{U}_{\mathrm{FT}} \left|x\right\rangle_n = 2^{-n/2} \sum_{y=0}^{2^n-1} \exp(2\pi i x y/2^n) \left|y\right\rangle_n$$

Introduce $\mathcal{Z}$

$$\mathcal{Z} \left|y\right\rangle_n = \exp(2\pi i y/2^n) \left|y\right\rangle_n$$

and recall

$$\mathbf{H}^{\otimes n} \left|0\right\rangle_n = 2^{-n/2} \sum_{y=0}^{2^n-1} \left|y\right\rangle_n$$

to see

$$\mathbf{U}_{\mathrm{FT}} \left|x\right\rangle_n = \mathcal{Z}^x \, \mathbf{H}^{\otimes n} \left|0\right\rangle_n$$

For 4 Qbits

$$\mathbf{U}_{\mathrm{FT}} \left|x_3\right\rangle \left|x_2\right\rangle \left|x_1\right\rangle \left|x_0\right\rangle = \mathcal{Z}^x \, \mathbf{H}_3 \, \mathbf{H}_2 \, \mathbf{H}_1 \, \mathbf{H}_0 \left|0\right\rangle \left|0\right\rangle \left|0\right\rangle \left|0\right\rangle$$

and generalizations obvious

Now simplify $\mathcal{Z}^x$

$$\mathcal{Z}\,|y\rangle_n = \exp(2\pi i y/2^n)\,|y\rangle_n$$
$$\mathcal{Z} = \exp\left[i\tfrac{\pi}{8}(8\,\mathbf{n}_3 + 4\,\mathbf{n}_2 + 2\,\mathbf{n}_1 + \mathbf{n}_0)\right]$$
$$\mathcal{Z}^x = \exp(i\pi\,\mathbf{W})$$
$$\mathbf{W} = \tfrac{1}{8}(8x_3 + 4x_2 + 2x_1 + x_0)(8\,\mathbf{n}_3 + 4\,\mathbf{n}_2 + 2\,\mathbf{n}_1 + \mathbf{n}_0)$$

Since $\exp(2\pi i\,\mathbf{n}) = \mathbf{1}$ drop multiples of $(2\,\mathbf{n})$

$$\begin{aligned}\mathbf{W} &= x_0\,\mathbf{n}_3 + (x_1 + \tfrac{1}{2}x_0)\,\mathbf{n}_2 + (x_2 + \tfrac{1}{2}x_1 + \tfrac{1}{4}x_0)\,\mathbf{n}_1 + \\ &\quad (x_3 + \tfrac{1}{2}x_2 + \tfrac{1}{4}x_1 + \tfrac{1}{8}x_0)\,\mathbf{n}_0 \\ &= \tfrac{1}{2}x_0\,\mathbf{n}_2 + (\tfrac{1}{2}x_1 + \tfrac{1}{4}x_0)\,\mathbf{n}_1 + (\tfrac{1}{2}x_2 + \tfrac{1}{4}x_1 + \tfrac{1}{8}x_0)\,\mathbf{n}_0 + \\ &\quad x_0\,\mathbf{n}_3 + x_1\,\mathbf{n}_2 + x_2\,\mathbf{n}_1 + x_3\,\mathbf{n}_0\end{aligned}$$

Also

$$\exp(i\pi x\,\mathbf{n})\,\mathbf{H}\,|0\rangle = \mathbf{H}\,|x\rangle$$

because

$$(-1)^{\mathbf{n}}\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$
\begin{aligned}
& \mathbf{U}_{\mathrm{FT}} \left|x_3\right\rangle \left|x_2\right\rangle \left|x_1\right\rangle \left|x_0\right\rangle \\
= \; & \exp\left[i\pi\Big(\tfrac{1}{2}x_0\,\mathbf{n}_2 + (\tfrac{1}{2}x_1 + \tfrac{1}{4}x_0)\,\mathbf{n}_1 + (\tfrac{1}{2}x_2 + \tfrac{1}{4}x_1 + \tfrac{1}{8}x_0)\,\mathbf{n}_0\Big)\right] \\
& \exp\left[i\pi\Big(x_0\,\mathbf{n}_3 + x_1\,\mathbf{n}_2 + x_2\,\mathbf{n}_1 + x_3\,\mathbf{n}_0\Big)\right] \\
& \mathbf{H}_3\,\mathbf{H}_2\,\mathbf{H}_1\,\mathbf{H}_0 \left|0\right\rangle \left|0\right\rangle \left|0\right\rangle \left|0\right\rangle \quad \ldots \text{using expression for } \mathcal{Z}^x \\
= \; & \exp\left[i\pi\Big(\tfrac{1}{2}x_0\,\mathbf{n}_2 + (\tfrac{1}{2}x_1 + \tfrac{1}{4}x_0)\,\mathbf{n}_1 + (\tfrac{1}{2}x_2 + \tfrac{1}{4}x_1 + \tfrac{1}{8}x_0)\,\mathbf{n}_0\Big)\right] \\
& \mathbf{H}_3\,\mathbf{H}_2\,\mathbf{H}_1\,\mathbf{H}_0 \left|x_0\right\rangle \left|x_1\right\rangle \left|x_2\right\rangle \left|x_3\right\rangle \quad \ldots \text{using last identity} \\
= \; & \mathbf{H}_3 \exp\left[i\pi\,\mathbf{n}_2\,\tfrac{1}{2}x_0\right] \mathbf{H}_2 \exp\left[i\pi\,\mathbf{n}_1\left(\tfrac{1}{2}x_1 + \tfrac{1}{4}x_0\right)\right] \\
& \mathbf{H}_1 \exp\left[i\pi\,\mathbf{n}_0\left(\tfrac{1}{2}x_2 + \tfrac{1}{4}x_1 + \tfrac{1}{8}x_0\right)\right] \mathbf{H}_0 \\
& \left|x_0\right\rangle \left|x_1\right\rangle \left|x_2\right\rangle \left|x_3\right\rangle \quad \ldots \text{because } \mathbf{n}_1\,\mathbf{H}_2 = \mathbf{H}_2\,\mathbf{n}_1 \text{ etc} \\
= \; & \mathbf{H}_3 \exp\left[i\pi\tfrac{1}{2}\,\mathbf{n}_2\,\mathbf{n}_3\right] \mathbf{H}_2 \exp\left[i\pi\,\mathbf{n}_1\left(\tfrac{1}{2}\,\mathbf{n}_2 + \tfrac{1}{4}\,\mathbf{n}_3\right)\right] \\
& \mathbf{H}_1 \exp\left[i\pi\,\mathbf{n}_0\left(\tfrac{1}{2}\,\mathbf{n}_1 + \tfrac{1}{4}\,\mathbf{n}_2 + \tfrac{1}{8}\,\mathbf{n}_3\right)\right] \mathbf{H}_0 \\
& \left|x_0\right\rangle \left|x_1\right\rangle \left|x_2\right\rangle \left|x_3\right\rangle \quad \ldots \text{remember permutation of RHS kets} \\
= \; & \mathbf{H}_3(\mathbf{V}_{32}\,\mathbf{H}_2)(\mathbf{V}_{31}\,\mathbf{V}_{21}\,\mathbf{H}_1)(\mathbf{V}_{30}\,\mathbf{V}_{20}\,\mathbf{V}_{10}\,\mathbf{H}_0) \left|x_0\right\rangle \left|x_1\right\rangle \left|x_2\right\rangle \left|x_3\right\rangle
\end{aligned}
$$

$$
\mathbf{V}_{ij} = \exp\left(i\pi\,\mathbf{n}_i\,\mathbf{n}_j\,/2^{|i-j|}\right)
$$

# 35. Quantum FT circuit

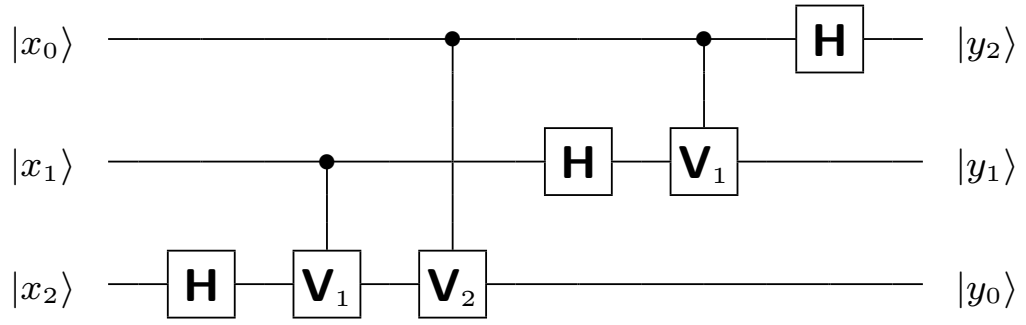
For 3 Qbits:

$$\begin{aligned}
&\mathbf{U}_{\mathrm{FT}}\,|x_2\rangle\,|x_1\rangle\,|x_0\rangle \\
&\quad = \mathbf{H}_2(\mathbf{V}_{21}\,\mathbf{H}_1)(\mathbf{V}_{20}\,\mathbf{V}_{10}\,\mathbf{H}_0) \\
&\qquad |x_0\rangle\,|x_1\rangle\,|x_2\rangle \quad \ldots \text{remember permutation of kets}
\end{aligned}$$

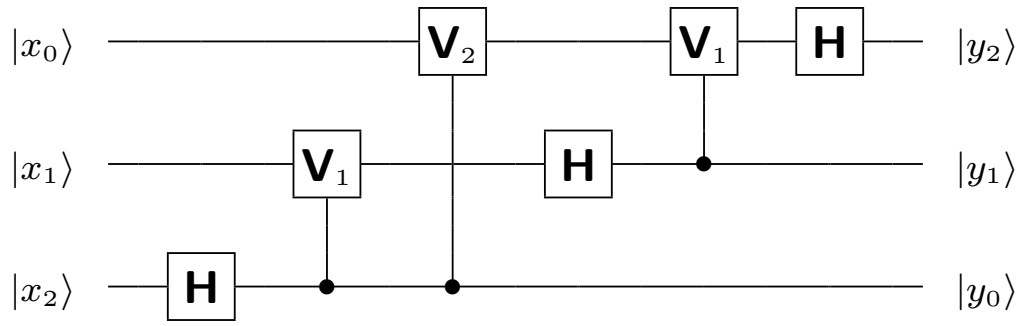
Replace $\mathbf{V}_{ij}$ by $\mathrm{c}_i\,\mathbf{V}_{i-j}$

$$\mathbf{V}_{i-j} = \exp\left(i\pi\,\mathbf{n}_j\,/2^{|i-j|}\right)$$

to get (permute left kets first!)




or better still



# 36. Groups and subgroups

**Thm:** (Lagrange) For any subgroup $S$ of a group $G$, $\mathcal{N}(S)$ divides $\mathcal{N}(G)$.

**Proof:** First we have

$$as_1 = as_2 \Rightarrow s_2 = s_2$$

hence distinct $s \in S$ give distinct coset elements.

Hence $\mathcal{N}(aS) = \mathcal{N}(S)$.

Second, for $s_1, s_2 \in S$

$$as_1 = bs_2 \quad \Rightarrow \quad a(s_1 S) = b(s_2 S) \quad \Rightarrow \quad aS = bS$$

hence cosets of $S$ either equal or disjoint.

Finally all $a \in G$ in some coset of $S$.

# 37. Modular arithmetic

**Def:** $G_N = \{a = 1, \ldots, N-1, \text{ if } a, N \text{ coprime}\}$

**Lemma:** $G_N$ is a group under multiplication.

**Proof:** Closure and identity obvious.

Inverse findable by Euclidean algorithm:

$$a_{n+1} = a_{n-1} - q_n a_n \quad \text{preserves common factors}$$

Start with $a_1 = N,\ a_2 = c \in G_N$ till

$$1 = a_{m-1} - q_m a_m$$

then work backwards to $1 = jN + kc$. Then choose $l$ such that $k = d + lN$ for $d \in [1, N-1]$. We get

$$1 = qN + dc$$

and $d$ is inverse.

**Thm:** $a^k = 1 \pmod N$ for some $k$ divides $\mathcal{N}(G_N)$

**Proof:** $1, a, a^2, \ldots, a^k$ is a subgroup for some $k$. Then use Lagrange's theorem.

**Cor 1:** (FLT) For any prime $p$ and $a$ not a multiple of $p$.

$$a^{p-1} = 1 \pmod{p}.$$

**Proof:** $a \in [1, p-1] \Rightarrow a \in G_p$.

For larger $a$, note that $(a+mp)^{p-1} = a^{p-1} \pmod{p}$.

**Cor 2:** For primes $p, q$ and $a \in G_{pq}$

$$a^{(p-1)(q-1)} = 1 \pmod{pq}$$

**Proof:** $\mathcal{N}(G_{pq}) = pq - 1 - (p-1) - (q-1) = (p-1)(q-1)$

**Cor 3:** For primes $p, q$ and any $a$

$$a^{1+s(p-1)(q-1)} = a \pmod{pq}$$

**Proof:** For $a \in G_{pq}$, follows from Cor 2.

For larger $a$, consider $(a+mpq)$ like before.

If $a = mpq$ also true (trivially).

If $a = mq$, $a \neq kp$ then $a^{s(q-1)} \in G_p$ and

$$\left(a^{s(q-1)}\right)^{p-1} = 1 + np \qquad \text{by FLT, hence}$$

$$a^{1+s(p-1)(q-1)} = a + mqnp$$

# 38. RSA

Bob computes $c, d \in G_{(p-1)(q-1)}$

$$cd = 1 + s(p-1)(q-1)$$

makes $pq, c$ public key, keeps $p, q, d$ secret

$$\begin{array}{ll} \text{Alice sends} & b = a^c \pmod{pq} \\ \text{Bob decodes} & a = b^d \pmod{pq} \end{array}$$

Fails if $a \notin G_{pq}$ (but unlikely).

Typically 200-digit primes, $a^c$ has complexity $\propto$ bits.

Suppose Eve intercepts $b$ and computes period $r$

$$b^r = 1 \pmod{pq}$$

Since $a = b^d$ follows that $a^r = 1 \pmod{pq}$.

This $r$ is the order of $a$, and since $a \in G_{pq}$, $r$ must divide $(p-1)(q-1)$.

Now $c$ coprime with $(p-1)(q-1)$ hence $r$, hence $c \in G_r$.

Eve chooses $d'$ such that $cd' = 1 + mr$.

Then $b^{d'} = a^{cd'} = a^{1+mr} = a(a^r)^m = a \pmod{pq}$.

# 39. Period-finding

Given $f(x)$ has period $r < N$, choose $n$ such that $2^n > N^2$.

Compute

$$2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle\, |f(x)\rangle$$

then suppose $|f(x)\rangle$ measures $|x_0\rangle$

Leaves

$$|\Psi\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle$$

Then Fourier transform

$$\mathbf{U}_{\mathrm{FT}}\, |\Psi\rangle = m^{-1/2}\, 2^{-n/2} \sum_{k=0}^{m-1} \sum_{y=0}^{2^n-1} \exp\left[2\pi i(x_0 + kr)y/2^n\right] |y\rangle$$

$$= \sum_{y=0}^{2^n-1} \exp\left[2\pi i x_0 y/2^n\right]$$

$$m^{-1/2}\, 2^{-n/2} \sum_{k=0}^{m-1} \exp\left[2\pi i k r y/2^n\right] |y\rangle$$

$$p(y) = \frac{1}{2^n m} \Big| \sum_{k=0}^{m-1} \exp\left(2\pi i k r y / 2^n\right) \Big|^2$$

Suppose $y = j\, 2^n / r + \delta_j \qquad |\delta_j| \leq \frac{1}{2}$

$$p(y) = \frac{1}{2^n m} \, \frac{\sin^2(\pi \delta_j m r / 2^n)}{\sin^2(\pi \delta_j r / 2^n)}$$

Recall $mr \simeq 2^n$, then use $x/(\frac{1}{2}\pi) \leq \sin x \leq x$ for $0 \leq x \leq \frac{1}{2}\pi$.

$$p(y) \geq (4/\pi^2)\,(m/2^n) \simeq (4/\pi^2)/r$$

Since $r - 1$ such values of $j$

$$p(y) \simeq 4/\pi^2 \simeq 40\%$$

If such $y$ found,

$$\Big| \frac{y}{2^n} - \frac{j}{r} \Big| \leq \frac{1}{2^{n+1}} \leq \frac{1}{2N^2}$$

Two such fractions differ by $> 1/N^2$, hence $j/r$ unique.

To find: best continued-fraction approximation of $y/2^n$ with denom $< N$.

# 40. Error-correction

Noise from environment (decoherence):

$$|e\rangle\,|0\rangle \rightarrow |e_0\rangle\,|0\rangle + |e_1\rangle\,|1\rangle$$

Very unlike classical noise

- happens on atomic scale
- not just **X**, phase errors too
- errors can be continuous
- premature measurement not allowed
- must correct without measuring

# 41. Pseudo-measurement

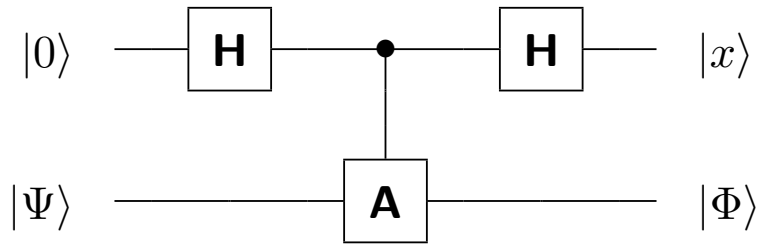
Consider unitary hermitian $\mathbf{A}$ (like $\mathbf{Z}_1\,\mathbf{X}_2\,\mathbf{X}_4\,\mathbf{Z}_5$)

We have projection operators for eigen-subspaces

$$\mathbf{P}_0^A = \tfrac{1}{2}(\mathbf{1}+\mathbf{A}) \quad \mathbf{P}_1^A = \tfrac{1}{2}(\mathbf{1}-\mathbf{A})$$

[Note 0 as label, not eigenvalue.]

Now introduce ancilla and c $\mathbf{A}$




$$(\mathbf{H}\otimes\mathbf{1})\mathrm{c}\,\mathbf{A}(\mathbf{H}\otimes\mathbf{1}) = |0\rangle\,\mathbf{P}_0^A\,|\psi\rangle + |1\rangle\,\mathbf{P}_1^A\,|\psi\rangle$$

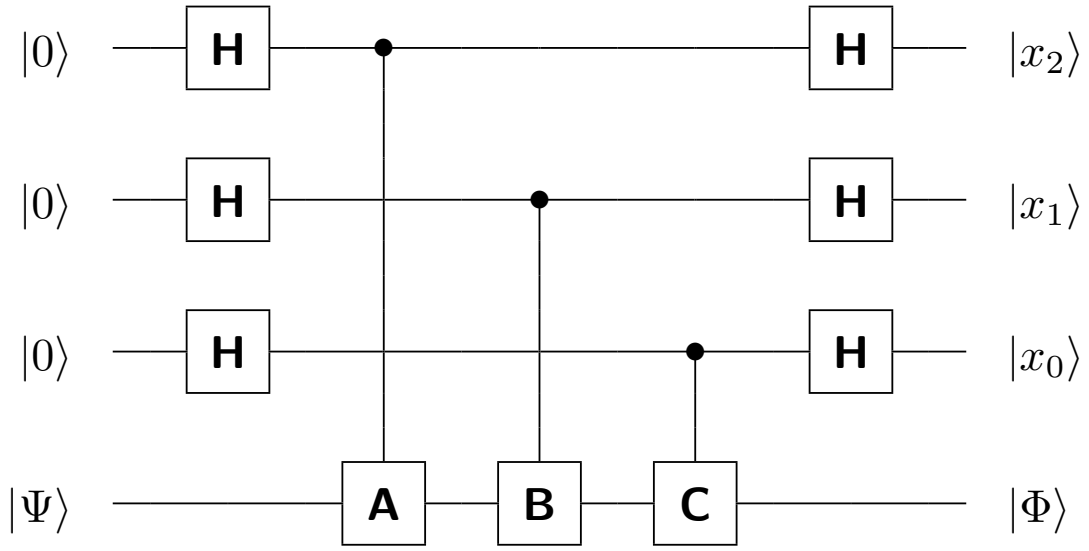
Ergo measuring ancilla like measuring $\mathbf{A}$.

Alternatively, since

$$\mathbf{A}(\mathbf{1}+(-1)^x\,\mathbf{A}) = (-1)^x(\mathbf{1}+(-1)^x\,\mathbf{A})$$

$\mathbf{P}_x^A\,|\Psi\rangle$ is an eigenstate of $\mathbf{A}$ with eigenvalue $(-1)^x$.

Generalizes to several commuting unitary hermitians $\mathbf{A}, \mathbf{B}, \mathbf{C}$




Now measuring the ancilla leaves

$$|\Phi\rangle = \mathbf{P}^C_{x_2}\, \mathbf{P}^B_{x_1}\, \mathbf{P}^A_{x_0}\, |\Psi\rangle$$

which is a simultaneous eigenstate of $\mathbf{C}, \mathbf{B}, \mathbf{A}$ with eigenvalues

$$(-1)^{x_2} \quad (-1)^{x_1} \quad (-1)^{x_0}$$

# 42. Single-Qbit errors

General decoherence

$$|e\rangle\,|0\rangle \to |e_0\rangle\,|0\rangle + |e_1\rangle\,|1\rangle$$
$$|e\rangle\,|1\rangle \to |e_2\rangle\,|0\rangle + |e_3\rangle\,|1\rangle$$

Rewrite using $\mathbf{P}_x^Z = \frac{1}{2}(1 + (-1)^x\,\mathbf{Z})$ as

$$\begin{aligned}|e\rangle\,|x\rangle \to &\big(\,|e_0\rangle\,\mathbf{1} + |e_1\rangle\,\mathbf{X}\,\big)\,\mathbf{P}_0^Z\,|x\rangle \\ &+\big(\,|e_2\rangle\,\mathbf{X} + |e_3\rangle\,\mathbf{1}\,\big)\,\mathbf{P}_1^Z\,|x\rangle \\ &= \Big(\tfrac{1}{2}(|e_0\rangle + |e_3\rangle)\,\mathbf{1} + \tfrac{1}{2}(|e_0\rangle - |e_3\rangle)\,\mathbf{Z} + \\ &\quad \tfrac{1}{2}(|e_2\rangle + |e_1\rangle)\,\mathbf{X} + \tfrac{1}{2}(|e_2\rangle - |e_1\rangle)\,\mathbf{Y}\Big)\end{aligned}$$

Rename environment kets and superpose basis states:

$$|e\rangle\,|\psi\rangle \to \Big(\,|d\rangle\,\mathbf{1} + |a\rangle\,\mathbf{X} + |b\rangle\,\mathbf{Y} + |c\rangle\,\mathbf{Z}\,\Big)\,|\psi\rangle$$

Now consider single-Qbit error in $n$-Qbit state $\Psi$

$$|e\rangle\,|\Psi\rangle \to \Big(\,|d\rangle\,\mathbf{1} + \textstyle\sum_{i=1}^{n}\big(\,|a\rangle\,\mathbf{X} + |b\rangle\,\mathbf{Y} + |c\rangle\,\mathbf{Z}\,\big)\Big)\,|\Psi\rangle$$

# 43. Error correction: basic algorithm

Encode computational Qbits as $n$-Qbit words

$$|\bar{0}\rangle = \mathbf{V}\,|0\rangle_n \quad |\bar{1}\rangle = \mathbf{W}\,|0\rangle_n$$
$$|\Psi\rangle = a\,|\bar{0}\rangle + b\,|\bar{1}\rangle \quad \text{spans } 2^n \text{ dimensions}$$

Single-Qbit corruption leaves

$$|\Psi'\rangle \left( |d\rangle\,\mathbf{1} + \textstyle\sum_{i=1}^{n} \left( |a_i\rangle\,\mathbf{X}_i + |b_i\rangle\,\mathbf{Y}_i + |c_i\rangle\,\mathbf{Z}_i \right) \right) |\Psi\rangle$$

Need commuting 'diagnostic' operators $\mathbf{A}, \mathbf{B}, \mathbf{C}$ etc with eigenvals $\pm 1$ such that

- $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are degenerate
- $|\Psi\rangle$, $\mathbf{X}_i\,|\Psi\rangle$, $\mathbf{Y}_i\,|\Psi\rangle$, $\mathbf{Z}_i\,|\Psi\rangle$ [spanning $2(1+3n)$ dimensions] are non-degenerate

Pseudo-measurement on $|\Psi'\rangle$ leaves eigenstate of $\mathbf{A}, \mathbf{B}, \mathbf{C}$ with eigenvalues

$$(-1)^{x_2} \quad (-1)^{x_1} \quad (-1)^{x_0}$$

by design a particular corrupted state.

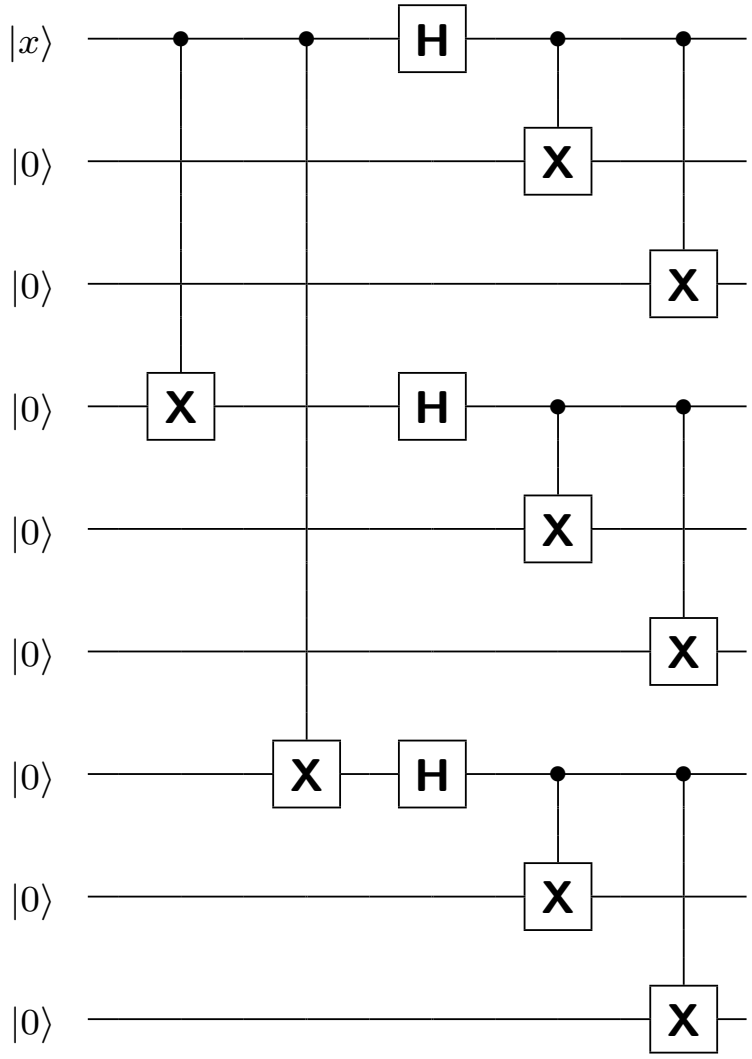
# 44. Shor's 9-Qbit code

Encoded by

$$|\bar{0}\rangle = 2^{-\frac{3}{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|\bar{1}\rangle = 2^{-\frac{3}{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

To prepare $|\bar{x}\rangle$



Single-Qbit corruption leaves [22 terms]

$$\Big( |d\rangle\, \mathbf{1} + |c\rangle\, \mathbf{Z}_1 + |c'\rangle\, \mathbf{Z}_4 + |c''\rangle\, \mathbf{Z}_7 + \sum_{i=1}^{9} \big( |a_i\rangle\, \mathbf{X}_i + |b_i\rangle\, \mathbf{Y}_i \big) \Big)\, |\Psi\rangle$$

Diagnostic operators

$$\begin{array}{cc} \mathbf{Z}_1\,\mathbf{Z}_2 & \mathbf{Z}_2\,\mathbf{Z}_3 \\ \mathbf{Z}_4\,\mathbf{Z}_5 & \mathbf{Z}_5\,\mathbf{Z}_6 \\ \mathbf{Z}_7\,\mathbf{Z}_8 & \mathbf{Z}_8\,\mathbf{Z}_9 \\ \mathbf{X}_1\,\mathbf{X}_2\,\mathbf{X}_3\,\mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6 & \mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6\,\mathbf{X}_7\,\mathbf{X}_8\,\mathbf{X}_9 \end{array}$$

[circuits in Mermin] have the properties

- eigenvalues $\pm 1$
- mutually commuting (zero or two anti-commuting factors)
- encoding states have eigenval 1
- corrupted states have eigenval $\pm 1$

Need to verify corrupted states are non-degenerate

| | $\mathbf{Z}_1$ | $\mathbf{Z}_4$ | $\mathbf{Z}_7$ |
|---|---|---|---|
| $\mathbf{Z}_1\,\mathbf{Z}_2$ | | | |
| $\mathbf{Z}_2\,\mathbf{Z}_3$ | | | |
| $\mathbf{Z}_4\,\mathbf{Z}_5$ | | | |
| $\mathbf{Z}_5\,\mathbf{Z}_6$ | | | |
| $\mathbf{Z}_7\,\mathbf{Z}_8$ | | | |
| $\mathbf{Z}_8\,\mathbf{Z}_9$ | | | |
| $\mathbf{X}_1\,\mathbf{X}_2\,\mathbf{X}_3\,\mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6$ | $-1$ | $-1$ | |
| $\mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6\,\mathbf{X}_7\,\mathbf{X}_8\,\mathbf{X}_9$ | | $-1$ | $-1$ |

| | $\mathbf{X}_1$ | $\mathbf{X}_2$ | $\mathbf{X}_3$ | $\mathbf{X}_4$ | $\mathbf{X}_5$ | $\mathbf{X}_6$ | $\mathbf{X}_7$ | $\mathbf{X}_8$ | $\mathbf{X}_9$ |
|---|---|---|---|---|---|---|---|---|---|
| $\mathbf{Z}_1\,\mathbf{Z}_2$ | $-1$ | $-1$ | | | | | | | |
| $\mathbf{Z}_2\,\mathbf{Z}_3$ | | $-1$ | $-1$ | | | | | | |
| $\mathbf{Z}_4\,\mathbf{Z}_5$ | | | | $-1$ | $-1$ | | | | |
| $\mathbf{Z}_5\,\mathbf{Z}_6$ | | | | | $-1$ | $-1$ | | | |
| $\mathbf{Z}_7\,\mathbf{Z}_8$ | | | | | | | $-1$ | $-1$ | |
| $\mathbf{Z}_8\,\mathbf{Z}_9$ | | | | | | | | $-1$ | $-1$ |
| $\mathbf{X}_1\,\mathbf{X}_2\,\mathbf{X}_3\,\mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6$ | | | | | | | | | |
| $\mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6\,\mathbf{X}_7\,\mathbf{X}_8\,\mathbf{X}_9$ | | | | | | | | | |

| | $\mathbf{Y}_1$ | $\mathbf{Y}_2$ | $\mathbf{Y}_3$ | $\mathbf{Y}_4$ | $\mathbf{Y}_5$ | $\mathbf{Y}_6$ | $\mathbf{Y}_7$ | $\mathbf{Y}_8$ | $\mathbf{Y}_9$ |
|---|---|---|---|---|---|---|---|---|---|
| $\mathbf{Z}_1\,\mathbf{Z}_2$ | $-1$ | $-1$ | | | | | | | |
| $\mathbf{Z}_2\,\mathbf{Z}_3$ | | $-1$ | $-1$ | | | | | | |
| $\mathbf{Z}_4\,\mathbf{Z}_5$ | | | | $-1$ | $-1$ | | | | |
| $\mathbf{Z}_5\,\mathbf{Z}_6$ | | | | | $-1$ | $-1$ | | | |
| $\mathbf{Z}_7\,\mathbf{Z}_8$ | | | | | | | $-1$ | $-1$ | |
| $\mathbf{Z}_8\,\mathbf{Z}_9$ | | | | | | | | $-1$ | $-1$ |
| $\mathbf{X}_1\,\mathbf{X}_2\,\mathbf{X}_3\,\mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | | | |
| $\mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6\,\mathbf{X}_7\,\mathbf{X}_8\,\mathbf{X}_9$ | | | | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ | $-1$ |

# 45. 5-Qbit code

Optimal for single-Qbit errors because

$$2(1+3n) = 2^n$$

Diagnostic operators $\mathbf{M}_1$ to $\mathbf{M}_4$ where

$$\begin{aligned}
\mathbf{M}_0 &= \mathbf{X}_1\,\mathbf{Z}_2\,\mathbf{Z}_3\,\mathbf{X}_4 \\
\mathbf{M}_1 &= \mathbf{X}_2\,\mathbf{Z}_3\,\mathbf{Z}_4\,\mathbf{X}_5 \\
\mathbf{M}_2 &= \mathbf{X}_3\,\mathbf{Z}_4\,\mathbf{Z}_5\,\mathbf{X}_1 \\
\mathbf{M}_3 &= \mathbf{X}_4\,\mathbf{Z}_5\,\mathbf{Z}_1\,\mathbf{X}_2 \\
\mathbf{M}_4 &= \mathbf{X}_5\,\mathbf{Z}_1\,\mathbf{Z}_2\,\mathbf{X}_3
\end{aligned}$$

*Note:* each $\mathbf{M}_i$ flips two Qbits and $\mathbf{M}_0\,\mathbf{M}_1\,\mathbf{M}_2\,\mathbf{M}_3\,\mathbf{M}_4 = \mathbf{1}$

Evident properties

- eigenvalues $\pm 1$
- mutually commuting (two anti-commuting factors)

Encoding words

$$|\bar{0}\rangle = \tfrac{1}{4}(\mathbf{1}+\mathbf{M}_1)(\mathbf{1}+\mathbf{M}_2)(\mathbf{1}+\mathbf{M}_3)(\mathbf{1}+\mathbf{M}_4)\,|00000\rangle$$

$$|\bar{1}\rangle = \tfrac{1}{4}(\mathbf{1}+\mathbf{M}_1)(\mathbf{1}+\mathbf{M}_2)(\mathbf{1}+\mathbf{M}_3)(\mathbf{1}+\mathbf{M}_4)\,|11111\rangle$$

Have required properties:

- orthogonal because $|\bar{0}\rangle$ ($|\bar{1}\rangle$) has odd (even) number of $|0\rangle$ Qbits
- normalized because $(\mathbf{1}+\mathbf{M}_i)^2 = 2(\mathbf{1}+\mathbf{M}_i)$
- diagnostic operators act as identity on encoding words because $\mathbf{M}_i(\mathbf{1}+\mathbf{M}_i) = (1+\mathbf{M}_i)$

The set $\mathbf{M}_1, \ldots, \mathbf{M}_4$ has distinct anticomm pattern with each of $\mathbf{X}_1, \mathbf{Y}_1, \ldots, \mathbf{Z}_5$:

| | $\mathbf{X}_1$ | $\mathbf{Y}_1$ | $\mathbf{Z}_1$ | $\mathbf{X}_2$ | $\mathbf{Y}_2$ | $\mathbf{Z}_2$ | $\mathbf{X}_3$ | $\mathbf{Y}_3$ | $\mathbf{Z}_3$ | $\mathbf{X}_4$ | $\mathbf{Y}_4$ | $\mathbf{Z}_4$ | $\mathbf{X}_5$ | $\mathbf{Y}_5$ | $\mathbf{Z}_5$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mathbf{M}_1$ | + | + | + | + | − | − | − | − | + | − | − | + | + | − | − |
| $\mathbf{M}_2$ | + | − | − | + | + | + | + | − | − | − | − | + | − | − | + |
| $\mathbf{M}_3$ | − | − | + | + | − | − | + | + | + | + | − | − | − | − | + |
| $\mathbf{M}_4$ | − | − | + | − | − | + | + | − | − | + | + | + | + | − | − |

Now introduce

$$\mathbf{N} = \mathbf{Z}_1\,\mathbf{Z}_2\,\mathbf{Z}_3\,\mathbf{Z}_4\,\mathbf{Z}_5$$

Commute with all $\mathbf{M}_i$, hence

$$\mathbf{N}\,|\bar{0}\rangle = |\bar{0}\rangle \quad \mathbf{N}\,|\bar{1}\rangle = -\,|\bar{1}\rangle$$

Also either commutes or anticommutes with corruptions

Take five Qbits in arbitrary state, measure $\mathbf{N}, \mathbf{M}_1, \ldots, \mathbf{M}_4$, get a known corruption of $|\bar{0}\rangle$ or $|\bar{1}\rangle$

# 46. 7-Qbit code: operators

Diagnostic operators

$$\mathsf{M}_1 = \mathsf{X}_4\,\mathsf{X}_5\,\mathsf{X}_6\,\mathsf{X}_7 \qquad \mathsf{N}_1 = \mathsf{Z}_4\,\mathsf{Z}_5\,\mathsf{Z}_6\,\mathsf{Z}_7$$
$$\mathsf{M}_2 = \mathsf{X}_2\,\mathsf{X}_3\,\mathsf{X}_6\,\mathsf{X}_7 \qquad \mathsf{N}_2 = \mathsf{Z}_2\,\mathsf{Z}_3\,\mathsf{Z}_6\,\mathsf{Z}_7$$
$$\mathsf{M}_3 = \mathsf{X}_1\,\mathsf{X}_3\,\mathsf{X}_5\,\mathsf{X}_7 \qquad \mathsf{N}_3 = \mathsf{Z}_1\,\mathsf{Z}_3\,\mathsf{Z}_5\,\mathsf{Z}_7$$

Evident properties

- eigenvalues $\pm 1$
- Mutually commuting (zero or two anticomm factors)

More operators

$$\bar{\mathsf{X}} = \mathsf{X}_1\,\mathsf{X}_2\,\mathsf{X}_3\,\mathsf{X}_4\,\mathsf{X}_5\,\mathsf{X}_6\,\mathsf{X}_7$$
$$\bar{\mathsf{Z}} = \mathsf{Z}_1\,\mathsf{Z}_2\,\mathsf{Z}_3\,\mathsf{Z}_4\,\mathsf{Z}_5\,\mathsf{Z}_6\,\mathsf{Z}_7$$
$$\bar{\mathsf{H}} = \mathsf{H}_1\,\mathsf{H}_2\,\mathsf{H}_3\,\mathsf{H}_4\,\mathsf{H}_5\,\mathsf{H}_6\,\mathsf{H}_7$$

# 47. 7-Qbit code: encoding words

Encoding words

$$|\bar{x}\rangle = 2^{-3/2}(\mathbf{1}+\mathbf{M}_1)(\mathbf{1}+\mathbf{M}_2)(\mathbf{1}+\mathbf{M}_3)\bar{\mathbf{X}}^x\,|0\rangle_7$$

Have required properties:

- orthogonal because $|\bar{0}\rangle$ ($|\bar{1}\rangle$) has odd (even) number of $|0\rangle$ Qbits
- normalized because $(\mathbf{1}+\mathbf{M}_i)^2 = 2(\mathbf{1}+\mathbf{M}_i)$
- $\mathbf{M}_i$ have eigenval 1 because $\mathbf{M}_i(\mathbf{1}+\mathbf{M}_i) = (1+\mathbf{M}_i)$
- $\mathbf{N}_i$ have eigenval 1 with $|\bar{0}\rangle$ because do so with $|0\rangle_7$ and commute with $\mathbf{M}_i$
- $\mathbf{N}_i$ have eigenval 1 with $|\bar{1}\rangle$ because also commute with $\bar{\mathbf{X}}$

# 48. 7-Qbit code: error diagnosis

Single-Qbit corrupted states [1+21 of them]

$$\Big( |d\rangle\, \mathbf{1} + \textstyle\sum_{i=1}^{7} \big( |a_i\rangle\, \mathbf{X}_i + |b_i\rangle\, \mathbf{Y}_i + |c_i\rangle\, \mathbf{Z}_i \big) \Big)\, |\Psi\rangle$$

identifiable from

| | $\mathbf{Y}_1$ $\mathbf{Z}_1$ | $\mathbf{Y}_2$ $\mathbf{Z}_2$ | $\mathbf{Y}_3$ $\mathbf{Z}_3$ | $\mathbf{Y}_4$ $\mathbf{Z}_4$ | $\mathbf{Y}_5$ $\mathbf{Z}_5$ | $\mathbf{Y}_6$ $\mathbf{Z}_6$ | $\mathbf{Y}_7$ $\mathbf{Z}_7$ |
|---|---|---|---|---|---|---|---|
| $\mathbf{X}_4\,\mathbf{X}_5\,\mathbf{X}_6\,\mathbf{X}_7$ | | | | – | – | – | – |
| $\mathbf{X}_2\,\mathbf{X}_3\,\mathbf{X}_6\,\mathbf{X}_7$ | | – | – | | | – | – |
| $\mathbf{X}_1\,\mathbf{X}_3\,\mathbf{X}_5\,\mathbf{X}_7$ | – | | – | | – | | – |
| | $\mathbf{X}_1$ $\mathbf{Y}_1$ | $\mathbf{X}_2$ $\mathbf{Y}_2$ | $\mathbf{X}_3$ $\mathbf{Y}_3$ | $\mathbf{X}_4$ $\mathbf{Y}_4$ | $\mathbf{X}_5$ $\mathbf{Y}_5$ | $\mathbf{X}_6$ $\mathbf{Y}_6$ | $\mathbf{X}_7$ $\mathbf{Y}_7$ |
| $\mathbf{Z}_4\,\mathbf{Z}_5\,\mathbf{Z}_6\,\mathbf{Z}_7$ | | | | – | – | – | – |
| $\mathbf{Z}_2\,\mathbf{Z}_3\,\mathbf{Z}_6\,\mathbf{Z}_7$ | | – | – | | | – | – |
| $\mathbf{Z}_1\,\mathbf{Z}_3\,\mathbf{Z}_5\,\mathbf{Z}_7$ | – | | – | | – | | – |

To generate $|\bar{0}\rangle$ measure $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$ on $|0\rangle_7$ to get

$$2^{-3/2}(\mathbf{1} \pm \mathbf{M}_1)(\mathbf{1} \pm \mathbf{M}_2)(\mathbf{1} \pm \mathbf{M}_3)\, |0\rangle_7$$

then apply a chosen $\mathbf{Z}_i$

# 49. 7-Qbit code: encoded Hadamard

$$
\begin{aligned}
\langle \bar{x}| \, \bar{\mathbf{H}} \, |\bar{y}\rangle &= 2^{-3} \, {}_7\langle 0| \, \bar{\mathbf{X}}^x (\mathbf{1}+\mathbf{M}_1)(\mathbf{1}+\mathbf{M}_2)(\mathbf{1}+\mathbf{M}_3) \\
&\qquad \bar{\mathbf{H}} (\mathbf{1}+\mathbf{M}_1)(\mathbf{1}+\mathbf{M}_2)(\mathbf{1}+\mathbf{M}_3) \bar{\mathbf{X}}^y \, |0\rangle_7 \\
&\quad [\text{Use } \mathbf{H}\,\mathbf{X} = \mathbf{Z}\,\mathbf{H} \text{ and } \mathbf{X}\,\mathbf{H} = \mathbf{H}\,\mathbf{Z}] \\
&= 2^{-3} \, {}_7\langle 0| \, \bar{\mathbf{X}}^x (\mathbf{1}+\mathbf{N}_1)(\mathbf{1}+\mathbf{N}_2)(\mathbf{1}+\mathbf{N}_3) \\
&\qquad \bar{\mathbf{H}} (\mathbf{1}+\mathbf{N}_1)(\mathbf{1}+\mathbf{N}_2)(\mathbf{1}+\mathbf{N}_3) \bar{\mathbf{X}}^y \, |0\rangle_7 \\
&\quad [\text{Use } \mathbf{N}_i \, \mathbf{X}_i = \mathbf{X}_i \, \mathbf{N}_i] \\
&= 2^{-3} \, {}_7\langle 0| (\mathbf{1}+\mathbf{N}_1)(\mathbf{1}+\mathbf{N}_2)(\mathbf{1}+\mathbf{N}_3) \\
&\qquad \bar{\mathbf{X}}^x \bar{\mathbf{H}} \bar{\mathbf{X}}^y (\mathbf{1}+\mathbf{N}_1)(\mathbf{1}+\mathbf{N}_2)(\mathbf{1}+\mathbf{N}_3) \, |0\rangle_7 \\
&\quad [\text{Use } \mathbf{N}_i \, |0\rangle = |0\rangle] \\
&= 2^3 \, {}_7\langle 0| \, \bar{\mathbf{X}}^x \bar{\mathbf{H}} \bar{\mathbf{X}}^y \, |0\rangle_7 \\
&\quad [\text{Use } \mathbf{X}^y \, |0\rangle = |y\rangle] \\
&= 2^3 \, \langle x| \, \bar{\mathbf{H}} \, |y\rangle^7
\end{aligned}
$$

Writing out cases

$$\langle \bar{0}| \, \bar{\mathbf{H}} \, |\bar{0}\rangle = \langle \bar{0}| \, \bar{\mathbf{H}} \, |\bar{1}\rangle = \langle \bar{1}| \, \bar{\mathbf{H}} \, |\bar{0}\rangle = \tfrac{1}{\sqrt{2}} \qquad \langle \bar{1}| \, \bar{\mathbf{H}} \, |\bar{1}\rangle = -\tfrac{1}{\sqrt{2}}$$

hence

$$\bar{\mathbf{H}} \, |\bar{0}\rangle = \tfrac{1}{\sqrt{2}}(|\bar{0}\rangle + |\bar{1}\rangle) \qquad \bar{\mathbf{H}} \, |\bar{1}\rangle = \tfrac{1}{\sqrt{2}}(|\bar{0}\rangle - |\bar{1}\rangle)$$

# 50. 7-Qbit code: fault tolerance

For encoded cNOT simply use $\mathrm{c}\,\mathbf{X}^{\otimes 7}$ on $|0\rangle_7$ and $|1\rangle_7$.

Hence single-gate malfunction produces only single-Qbit corruption.

# 51. Quantum dynamics

Schrödinger equation

$$\frac{[\hbar]}{i}\,\frac{d}{dt}\,|\psi\rangle = \mathcal{H}\,|\psi\rangle$$

Time evolution

$$|t\rangle = \exp\left(i\mathcal{H}t\right)|t=0\rangle$$

Dynamics specified by Hamiltonian operator $\mathcal{H}$.

For example

$$\mathcal{H} = \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}$$

has stationary states

$$\tfrac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

# 52. Two interacting spins (Qbits)

$$\mathcal{H} = J\boldsymbol{\sigma}_1 \cdot \boldsymbol{\sigma}_2 = J(\mathbf{X}_1\,\mathbf{X}_2 - \mathbf{Y}_1\,\mathbf{Y}_2 + \mathbf{Z}_1\,\mathbf{Z}_2)$$

Recall $\mathbf{S}_{12} = \frac{1}{2}(\mathbf{1} + \mathbf{X}_1\,\mathbf{X}_2 - \mathbf{Y}_1\,\mathbf{Y}_2 + \mathbf{Z}_1\,\mathbf{Z}_2)$

$$\mathcal{H} = J(2\,\mathbf{S}_{12} - \mathbf{1})$$

In computational basis

$$\mathcal{H} = J\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 2 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

which has

| eigenstates | eigenval |
|---|---|
| $\|00\rangle$ | 1 |
| $\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$ | 1 |
| $\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$ | $-3$ |
| $\|11\rangle$ | 1 |

Triplet and singlet (and 21 cm H line)

Exchange of $|01\rangle$ and $|10\rangle$

# 53. In singlet-triplet basis

Consider

$$|00\rangle \quad \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad |11\rangle$$

as basis.

Add 'external magnetic field'

$$\mathcal{H} = J(2\,\mathbf{S}_{12} - 1) + \tfrac{1}{2}A(\mathbf{Z}_1 + \mathbf{Z}_2) + \tfrac{1}{2}B(\mathbf{Z}_1 - \mathbf{Z}_2)$$

$$\mathcal{H} = \begin{pmatrix} J+A & 0 & 0 & 0 \\ 0 & J & B & 0 \\ 0 & B & -3J & 0 \\ 0 & 0 & 0 & J-A \end{pmatrix}$$

Middle eigenvalues $-J \pm \sqrt{4J^2 + B^2}$ (cf Zeeman effect)

Cunningly choose

$$A = 2J \quad B = 2\sqrt{3}J \quad t = \tfrac{1}{4}\pi/J$$

which gives

$$\exp(i\mathcal{H}t) = \begin{pmatrix} e^{3i\pi/4} & 0 & 0 & 0 \\ 0 & e^{3i\pi/4} & 0 & 0 \\ 0 & & e^{-5i\pi/4} & 0 \\ 0 & 0 & 0 & e^{-i\pi/4} \end{pmatrix}$$

But this is

$$e^{3i\pi/4}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix}$$

which amount to $e^{3i\pi/4}\,(\mathrm{c}\,\mathbf{Z})$

Idea for realizing cNOT