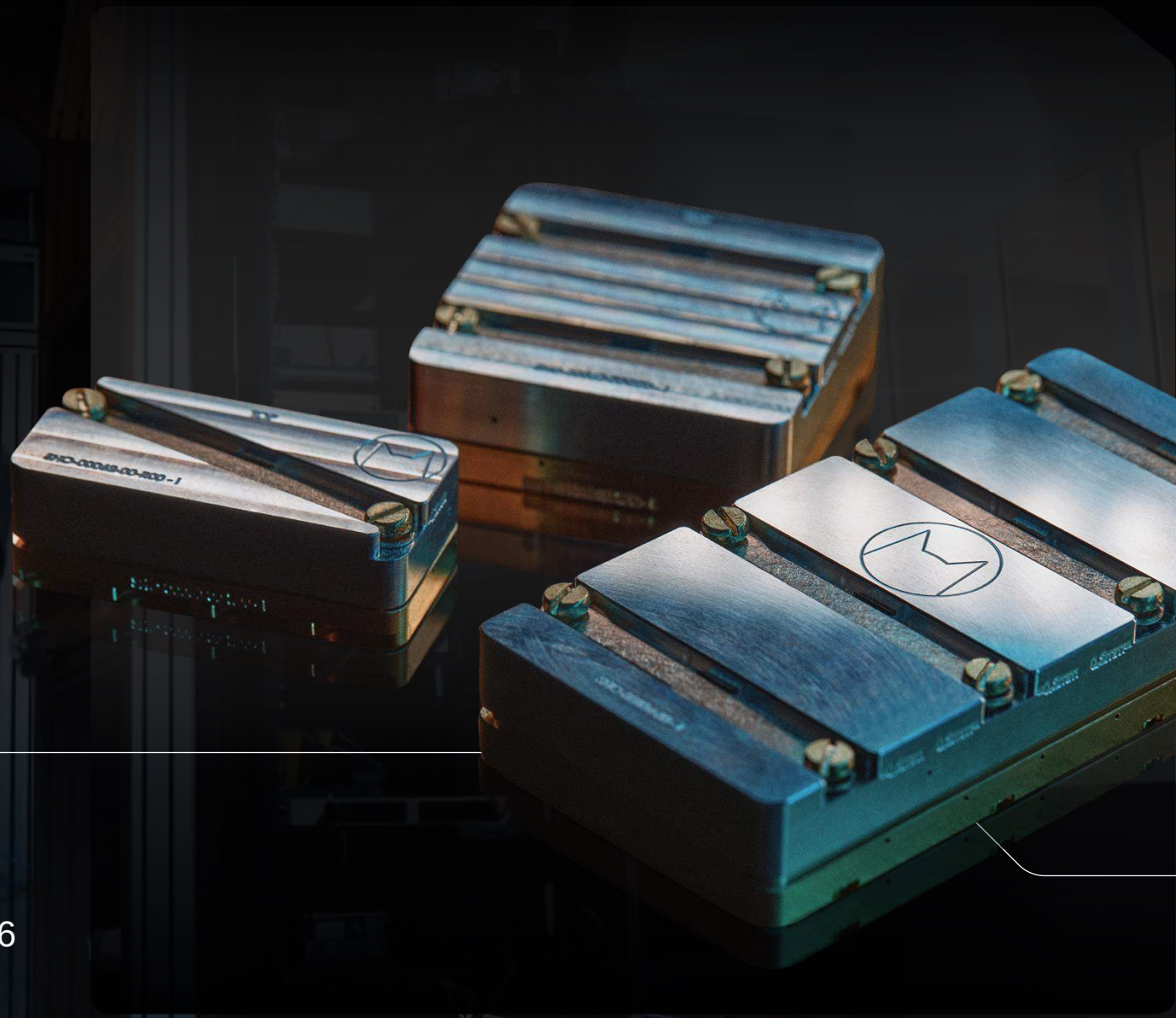
ALICE & BOB

Low-overhead fault-tolerant quantum computing with cat qubits: theory and state of play

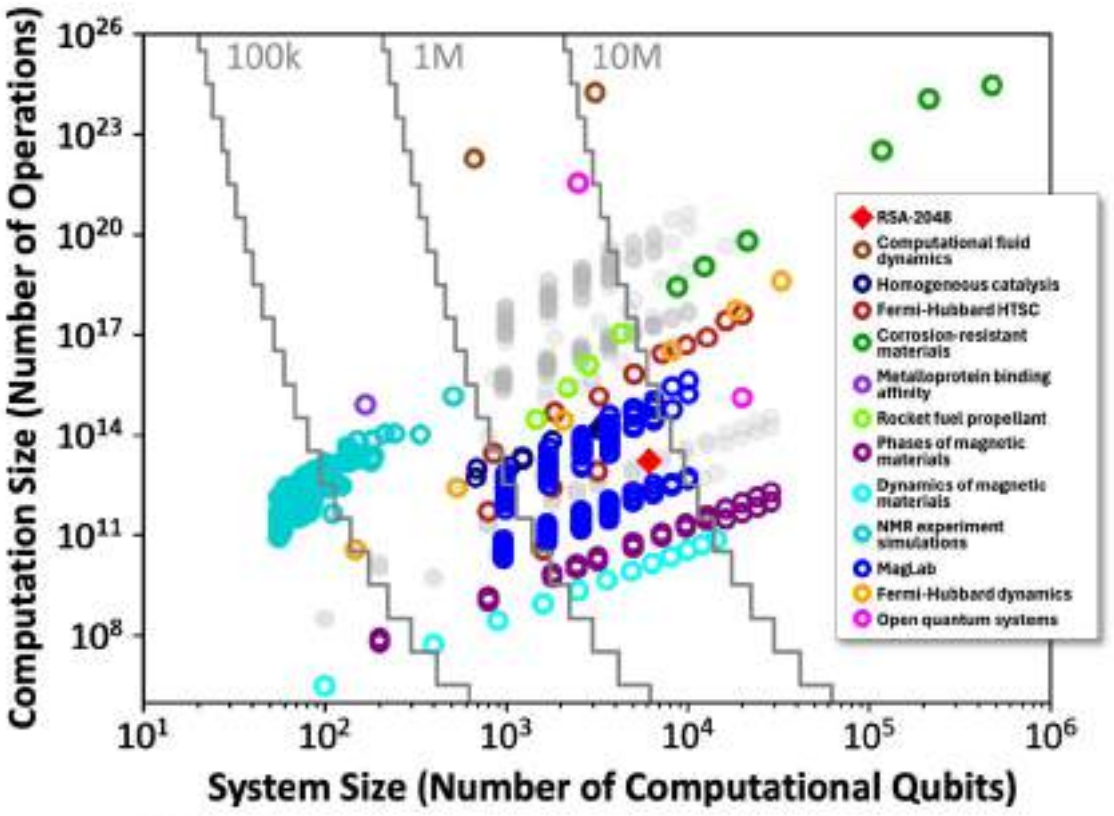


ÉLIE GOUZIEN, ALICE & BOB

3RD QUANTUM COMPUTING SCHOOL

ICTP-SAIFR, SÃO PAULO, 16 NOVEMBER 2026

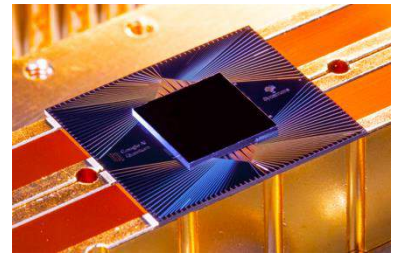
DARPA Quantum Benchmark



Grey solid circles represent pessimistic resource estimates. Colored circles are optimistic resource estimates based on known improvements. All points supported by detailed published pre-prints.

"If a fully functioning quantum computer magically appeared, what would it make possible that a standard computer cannot accomplish?"

$$\epsilon_L \sim \frac{1}{\text{Computation Size} \times \text{System Size}} \leq 10^{-10}$$

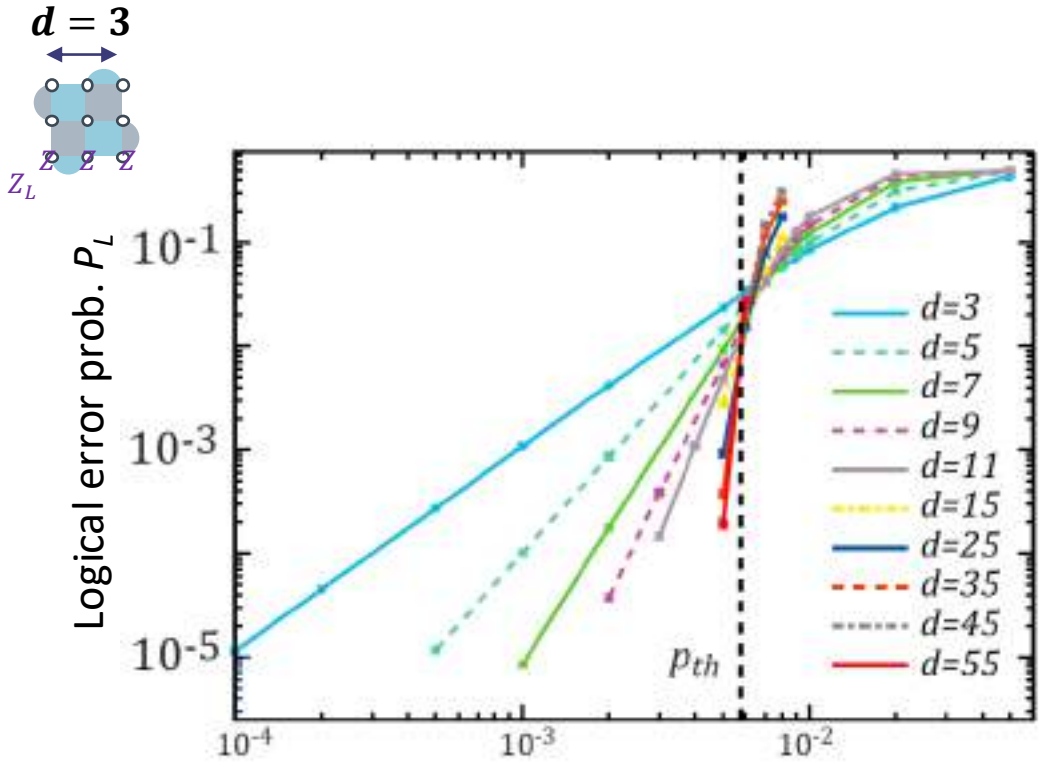


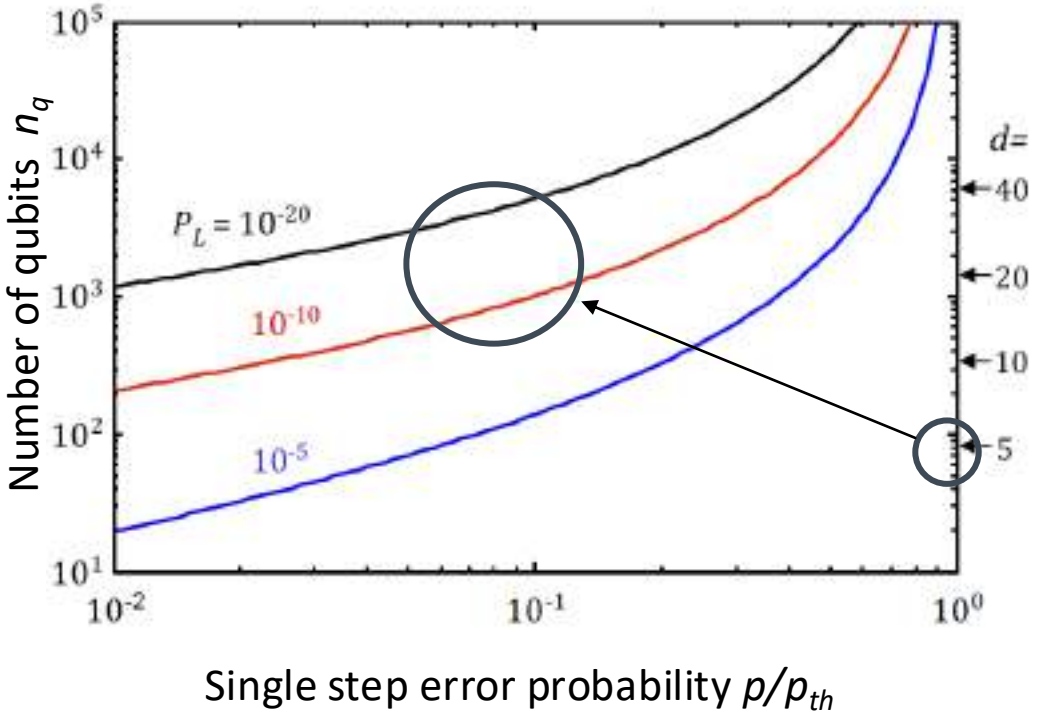
Quantum processor

$10^{-3} - 10^{-4}$ errors per bit per operation

https://www.darpa.mil/program/quantum-benchmarking

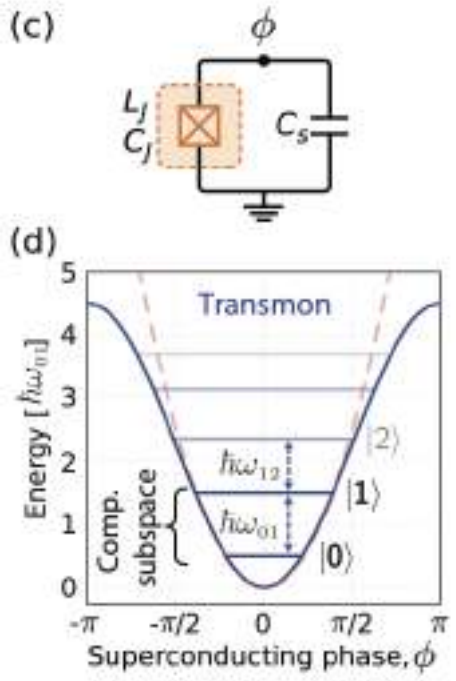
The threshold & QEC overhead





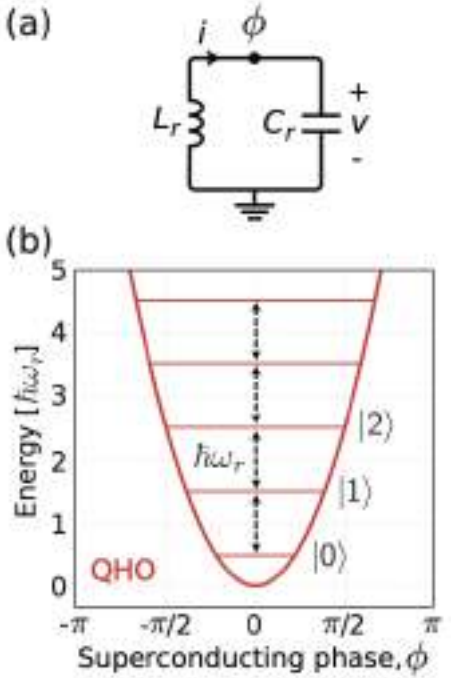
Figures borrowed from A. Fowler et al., Phys. Rev. A 86, 2012.

« Traditional » qubits



Qubit encoded in the energy $\{|0\rangle, |1\rangle\}$ subspace

Bosonic qubits



$\mathcal{H} = \text{span}\{|n\rangle, n \in \mathbb{N}\}$

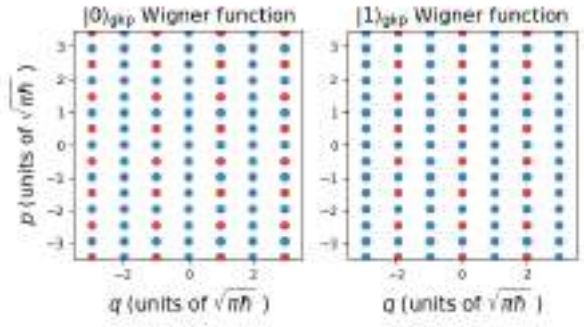
Qubit encoded in a subspace to be defined

- Interesting QEC properties
- « Easy » to stabilize

Figures from P. Krantz *et. al*, *A quantum engineer's guide to superconducting qubits*, Applied Physics Reviews (2019)

Main contenders?

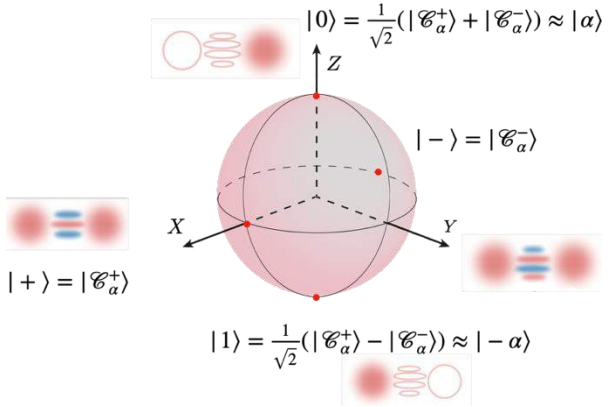
GKP qubit



D. Gottesman, A. Kitaev, J. Preskill Phys. Rev. A 64, 2001.

Nord Quantique

Cat qubit

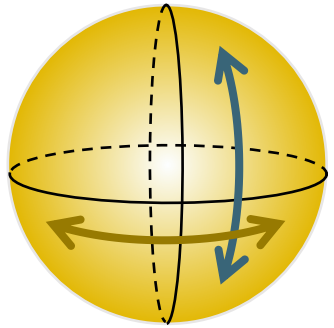


M. Mirrahimi et al, New J. Phys. 16 045014

aws

QEC property?	Minimizes the noise	Polarizes the noise
Experimental realization?	“Hard” to stabilize Clifford gates are “easy”	”Easy” to stabilize Bias-preserving CNOT is “hard”

The dissipative cat: a biased noise qubit



Bit-flip X

Phase-flip Z

Bit-flip $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = \alpha|1\rangle + \beta|0\rangle$

Phase-flip $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = \alpha|0\rangle - \beta|1\rangle$

TRANSMON QUBITS	CAT QUBITS
$T_X = T_Z \approx 100\ \mu s$ $\frac{T_Z}{T_X} \approx 1$	$T_X \approx 10\ s \quad T_Z \approx 1\ \mu s$ $\frac{T_Z}{T_X} \approx 10^7$

Réglade, Bocquet et. al, *Nature* 629, 778-783 (2024)

01

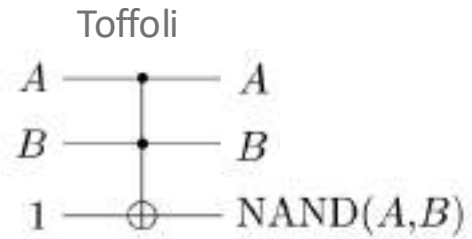
Introduction to quantum error correction

From classical codes to autonomous quantum error correction

Classical vs quantum computers

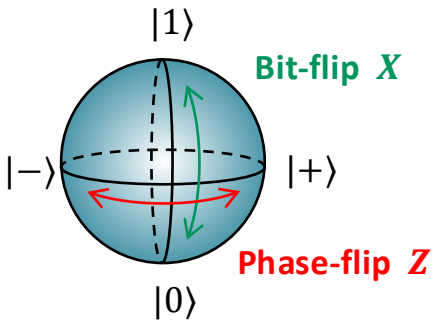
Classical computer

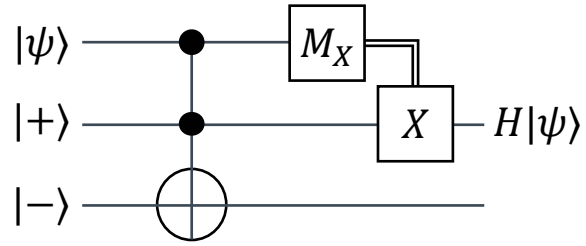
- Physical system → bit, stable (rare bit-flips)
- Initialize and measure $0/1$
- Universal gate → NAND or Toffoli



Quantum computer

- Physical system → qubit, stable (rare bit-flips)
  coherent (rare phase-flips)
- Initialize and measure $|0/1\rangle$, $|+/-\rangle$
- Universal set of gate → Toffoli and Hadamard



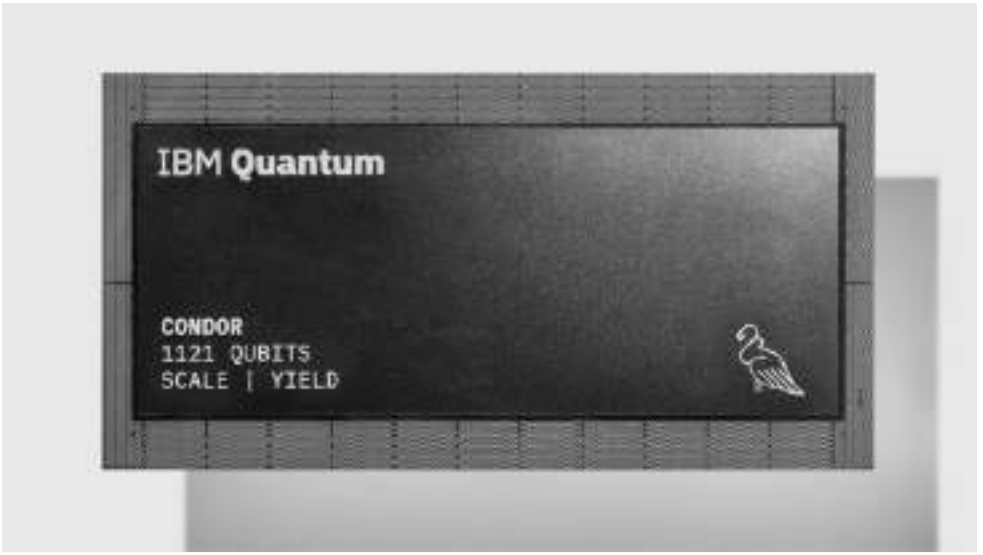


Why and how classical computers work so well?
To what extent can we learn? What needs to be added?

Yaoyun Shi. Quantum Info. Comput., 3(1):84–92, January 2003
Dorit Aharonov, 2003. arXiv:quant-ph/0301040.

The status of quantum computers

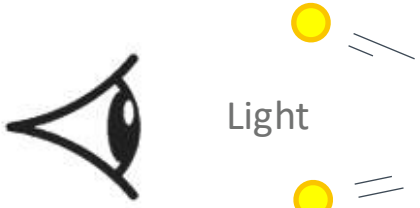




Scale	**1** Petabytes	**1000** qubits
Gate duration	**1** ps	**10** ns
Error probability	10^{-25}	10^{-3}

Focus on problems with exponential speed-up
Still, errors are too frequent → 10^{-8}

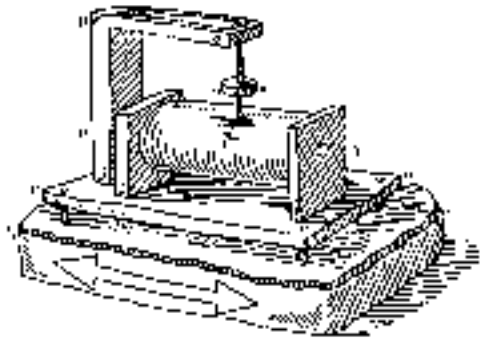
Quantum states are fragile



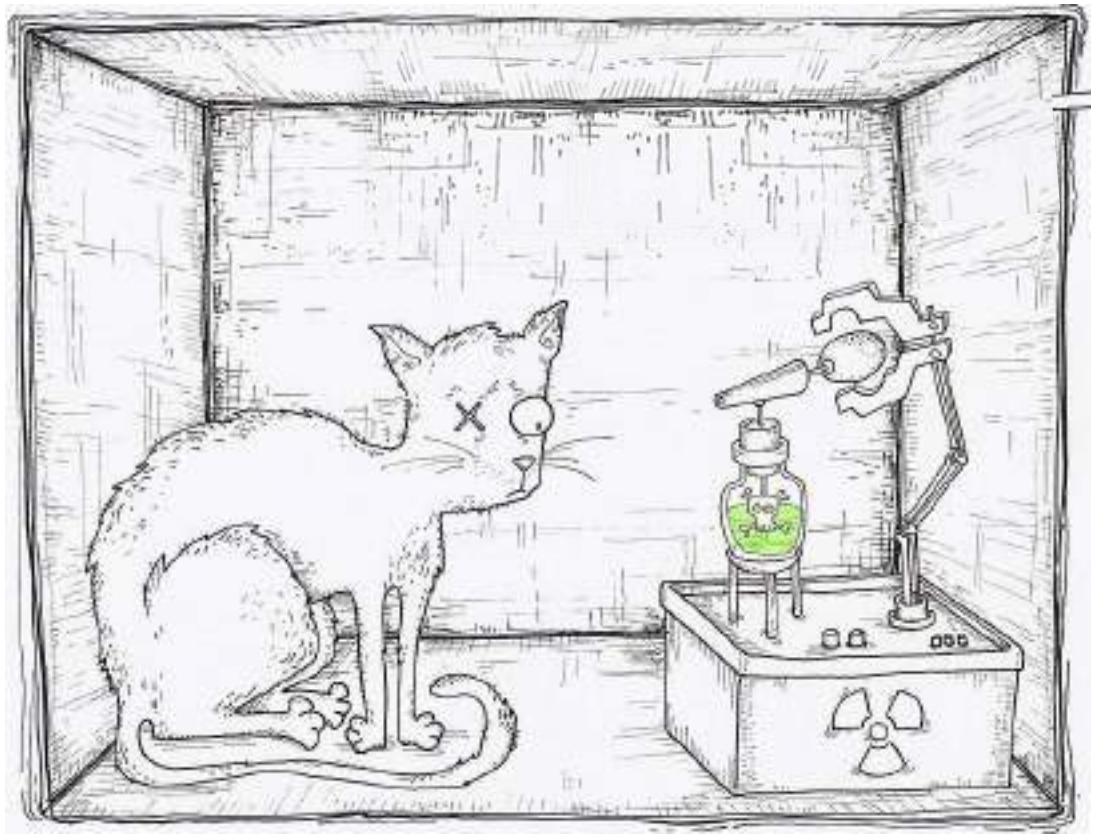
Light



Sound



Vibrations



By ADA and Neagoe

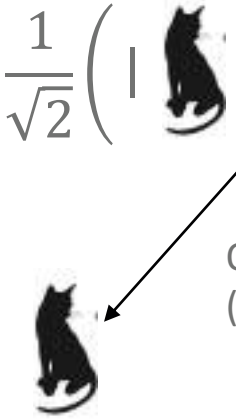
Information on the cat

Alive  0

Dead  1

Quantum superposition

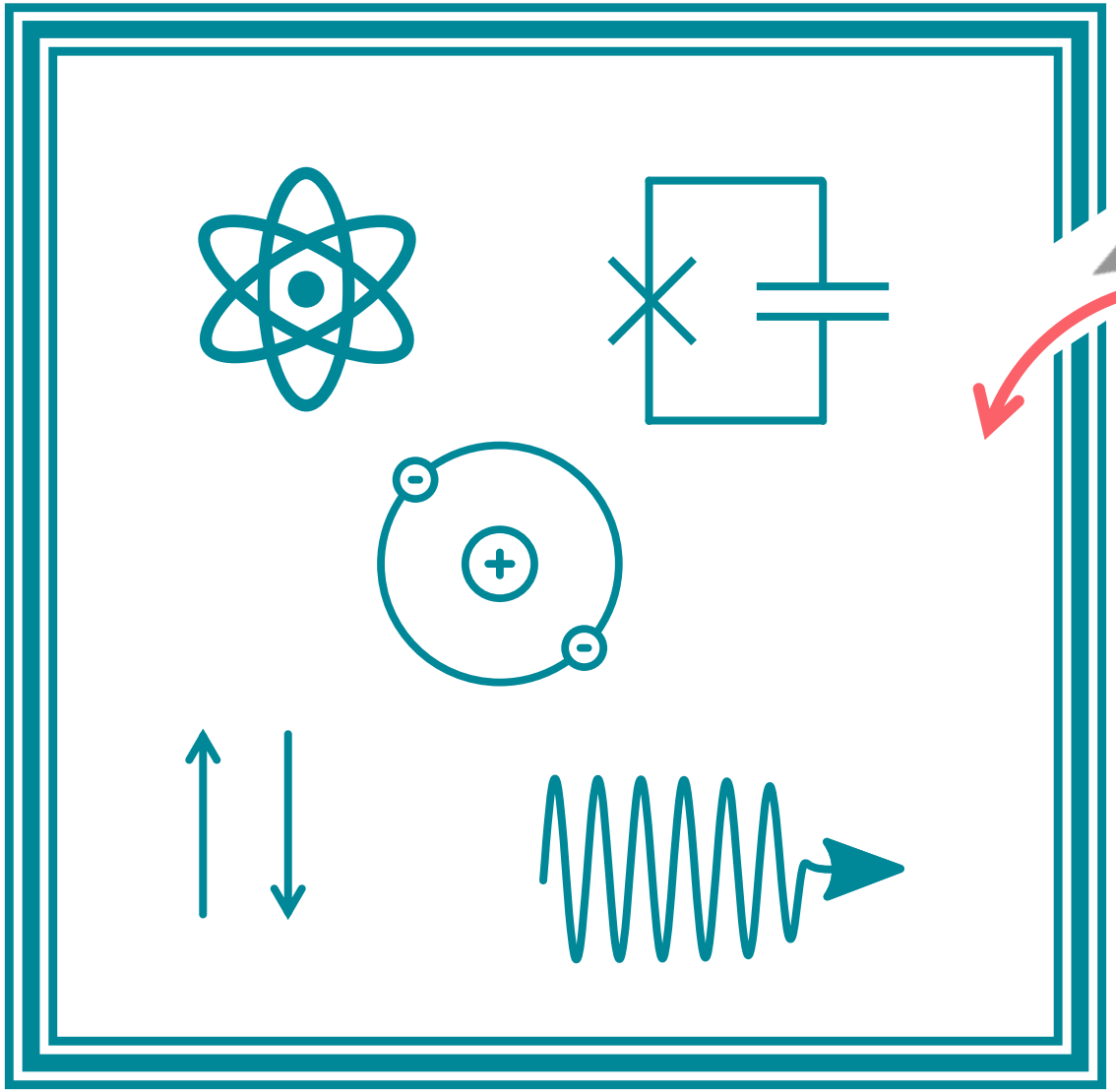
$$\frac{1}{\sqrt{2}}\left(|\ \rangle + |\ \rangle \right)$$



Opening
(measure)



The quantum computing paradox



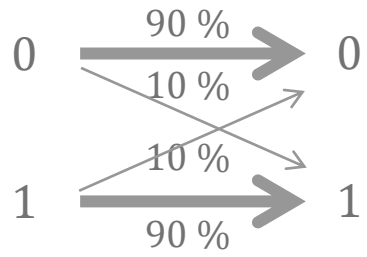
Controlable

Spurious noise

Quantum error correction is necessary

Classical error correction

Bob asks how Alice is doing ?



A sends x **B** receives 0

Best strategy

$$0 \to x = 0$$
$$1 \to x = 1$$

Failure risk 10 %

Encoding

A answers x, sends 000 for 0 and 111 for 1

B receives 001

Best strategy

$$000, 001, 010, 100 \to x = 0$$
$$111, 110, 101, 011 \to x = 1$$

Failure risk 2.8 %

Increase robustness

$00000 \to 0$, $11111 \to 1$ Failure risk 0.9 %

Exponential suppression of errors in the number of bits

Quantum error correction

How is the Schrödinger cat doing ?

A sends $\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$ → info (α, β)

B receives $\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$ 90 % chances to get (α, β)

$\boxed{|\psi\rangle = \alpha|1\rangle + \beta|0\rangle}$ 10 % chances to get (β, α)

Error correction strategy

A Sends $\boxed{|\psi\rangle = \alpha|000\rangle + \beta|111\rangle}$ **B** receives $\boxed{|\psi\rangle}$ and wishes to correct the state

Hypothesis, at most 1 error :

$\|\psi\rangle = \alpha\|000\rangle + \beta\|111\rangle$	No error
$\|\psi\rangle = \alpha\|001\rangle + \beta\|110\rangle$	Error on #3
$\|\psi\rangle = \alpha\|010\rangle + \beta\|101\rangle$	Error on #2
$\|\psi\rangle = \alpha\|100\rangle + \beta\|011\rangle$	Error on #1

Error syndromes

Which qubit suffered an error ?

$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ No error
$|\psi\rangle = \alpha|001\rangle + \beta|110\rangle$ Error sur #1
$|\psi\rangle = \alpha|010\rangle + \beta|101\rangle$ Error sur #2
$|\psi\rangle = \alpha|100\rangle + \beta|011\rangle$ Error sur #3



Rules of the game:
- You can ask several questions
- Yes/no questions
- Don't collapse quantum information (α, β)

Counter-example:
- "is the first qubit in 0 ?"

$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ Yes $|\psi\rangle = |000\rangle$, No $|\psi\rangle = |111\rangle$
$|\psi\rangle = \alpha|001\rangle + \beta|110\rangle$ Yes $|\psi\rangle = |001\rangle$, No $|\psi\rangle = |110\rangle$
$|\psi\rangle = \alpha|010\rangle + \beta|101\rangle$ Yes $|\psi\rangle = |010\rangle$, No $|\psi\rangle = |101\rangle$
$|\psi\rangle = \alpha|100\rangle + \beta|011\rangle$ Yes $|\psi\rangle = |011\rangle$, No $|\psi\rangle = |100\rangle$

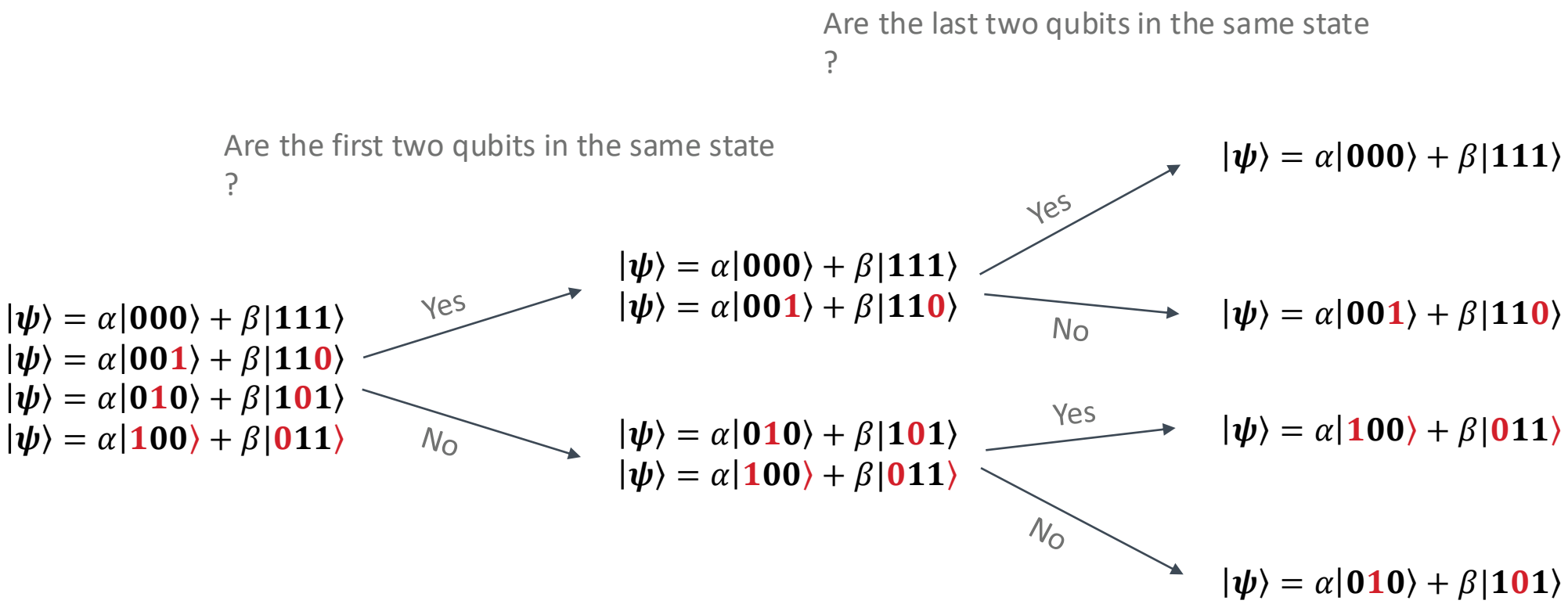
→ Lost information



Jérémie Guillaud
Chief of Theory at A&B

« Projection from the measurement is both a curse and a blessing ! »

Error syndromes



Yes, Yes → No error
Yes, No → Error on #3
No, No → Error on #2
No, Yes → Error on #1

We manage to locate the error without perturbing α and β !

How to measure error syndromes?

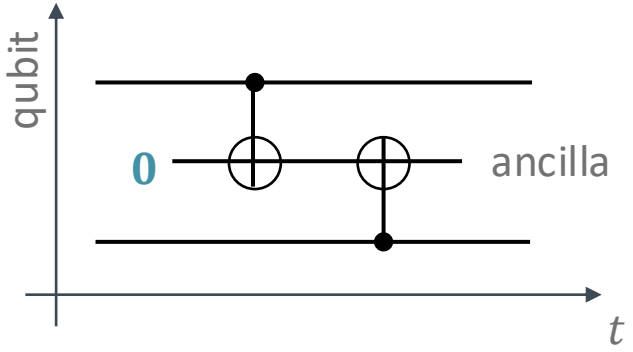
$|00\rangle$ or $|11\rangle$ yields 0
$|01\rangle$ or $|10\rangle$ yields 1

CNOT gate + ancilla qubit

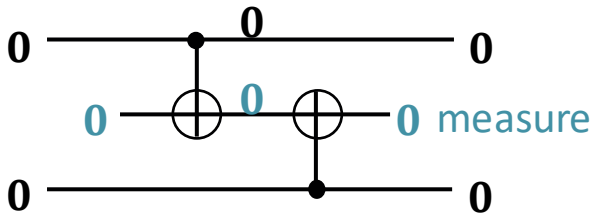
Qubit 2 flips according to the state qubit 1



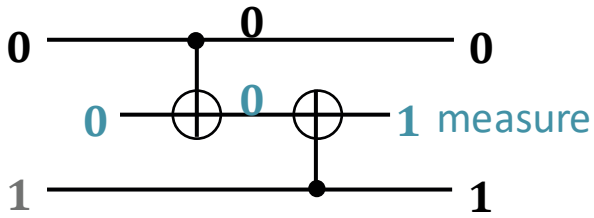
$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$



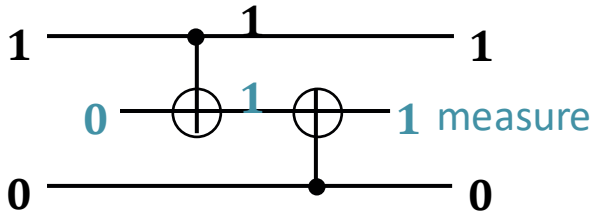
Case 1 : $|00\rangle$



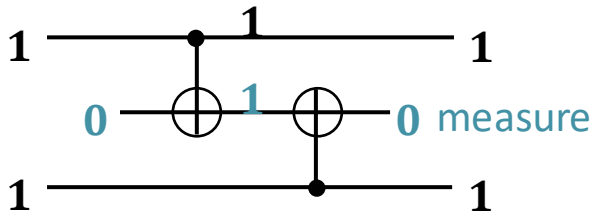
Case 2 : $|01\rangle$



Case 3 : $|10\rangle$



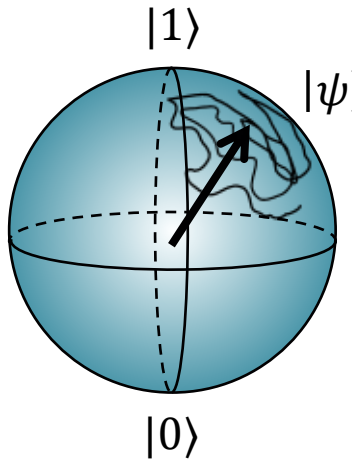
Case 4 : $|11\rangle$



Why can errors be digitized?

Error ≈ random diffusion (continuous)

Projection from measurement:
→ error digitization



$|\psi\rangle = |1\rangle$ —Small deviation→ $|\psi\rangle = \frac{1}{\sqrt{1+\epsilon^2}}|1\rangle + \frac{\epsilon}{\sqrt{1+\epsilon^2}}|0\rangle$ —Measure→

- $|1\rangle$ with probability $\frac{1}{1+\epsilon^2}$
- $|0\rangle$ with probability $\frac{\epsilon^2}{1+\epsilon^2}$

$|\psi\rangle = |1\rangle$ —Bit-flip with proba. $\frac{\epsilon^2}{1+\epsilon^2}$→

- $|\psi\rangle = |1\rangle$ —Measure→ $|1\rangle$ with probability $\frac{1}{1+\epsilon^2}$
- $|\psi\rangle = |0\rangle$ —Measure→ $|0\rangle$ with probability $\frac{\epsilon^2}{1+\epsilon^2}$

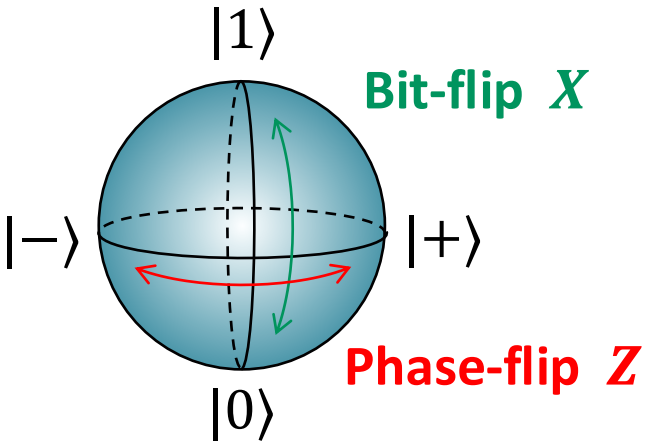
« Projection from the measurement is both a curse and a blessing ! »

There are two errors in quantum

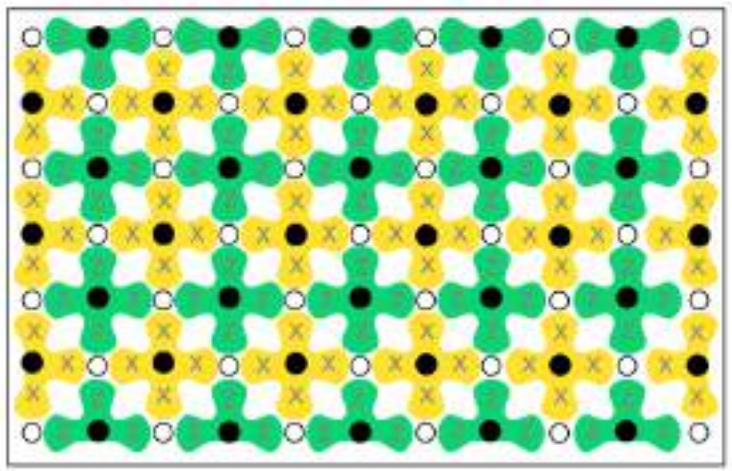
Bit-flip $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = \alpha|1\rangle + \beta|0\rangle$

Phase-flip $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = \alpha|0\rangle - \beta|1\rangle$

$(\alpha, \beta) \in \mathbb{C}^2$ but norm + global phase
→ 2 degrees of freedom

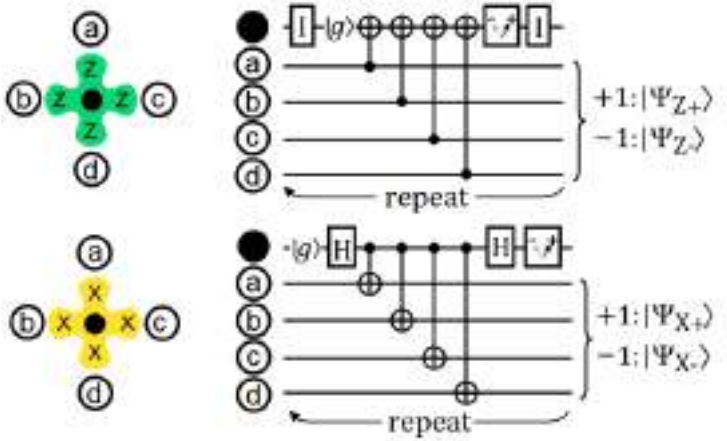


Redundancy in 2 dimensions is necessary: Surface code



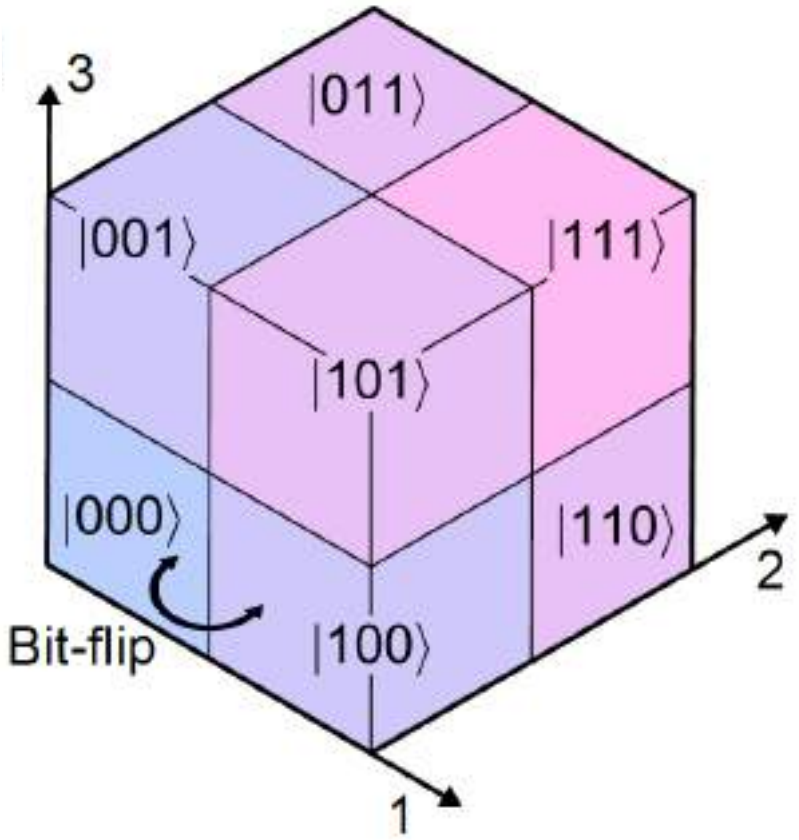
○ data

● ancilla



A. Fowler et al., Phys. Rev. A 86, 032324 (2012)

Fundamental principle of quantum error correction



Redundancy

We need a big Hilbert space to protect against (local) errors

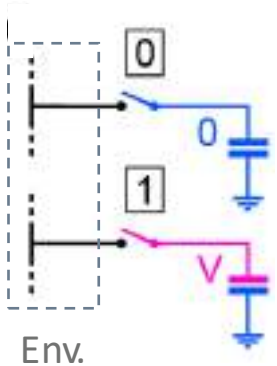
Distance

We encode information in distant location in this space

Typical storage methods in classical memories

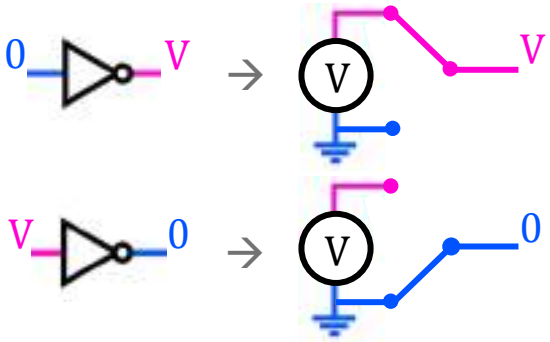
Dynamic RAM

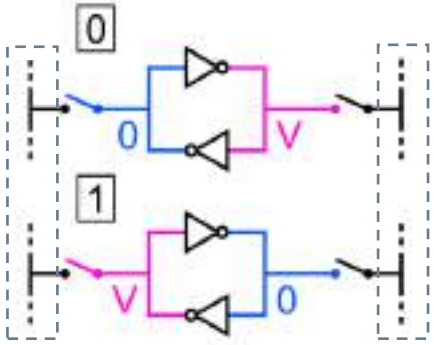
- Passive storing component
- Measurement/Feedback based



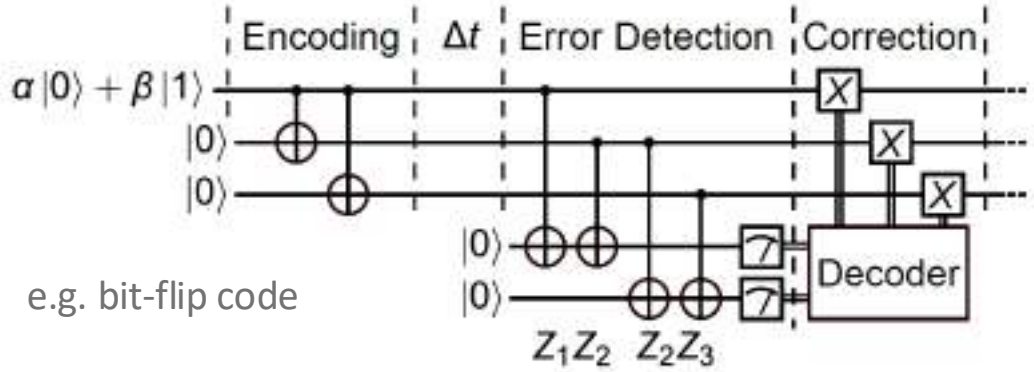
Static RAM

- Powered component
- Autonomous





Quantum Equivalent



e.g. bit-flip code

Which possible quantum equivalent ?

Dissipation is crucial for both C/Q computing

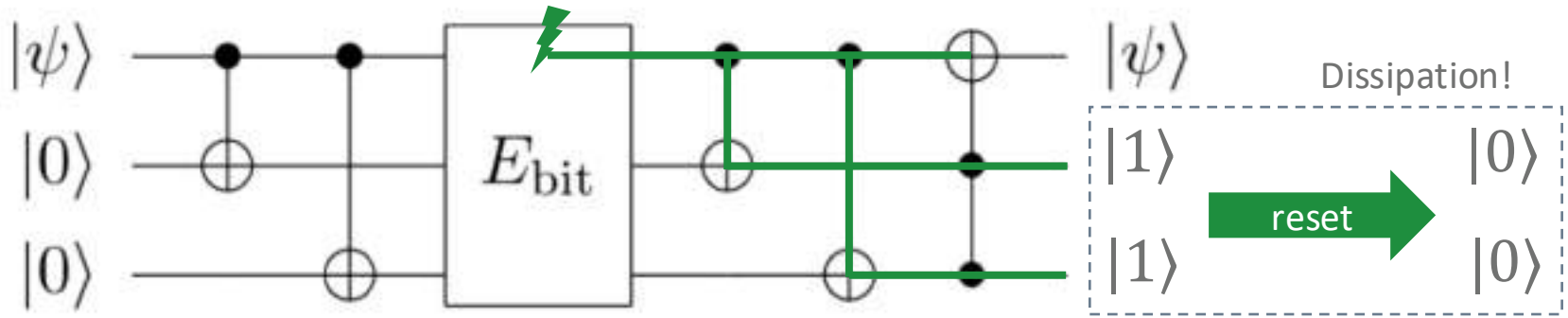
Classical systems

Dissipation ←→ Stability and controllabity

Quantum systems

Dissipation ←→ Decoherence

Tailored dissipation is required!



"The trick is to expel entropy without exposing the protected coherent quantum information to the environment"
J. Preskill

J. Preskill. Quantum Information and Computation, 13(3-4):0181–0194, jul 2012.

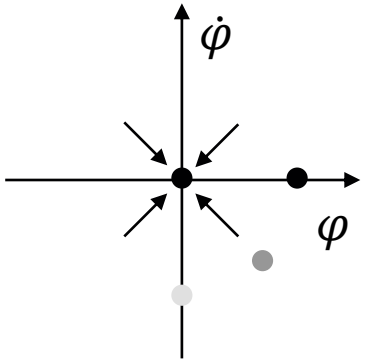
02

Driven-dissipative stabilization of cats

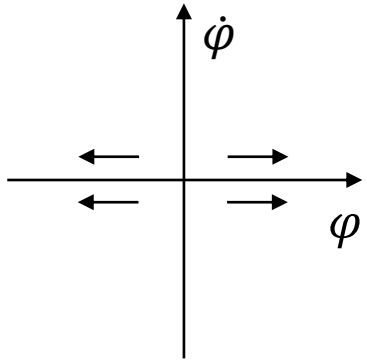
Fighting decoherence with dissipation

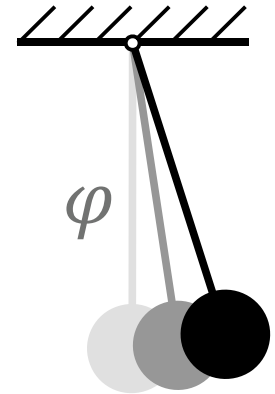
Bistable harmonic oscillator

Cold dissipative oscillator

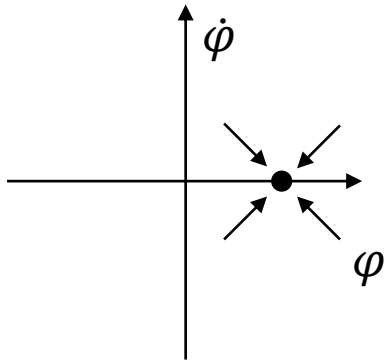


Parametric oscillator

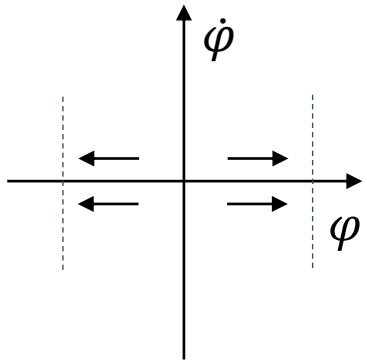




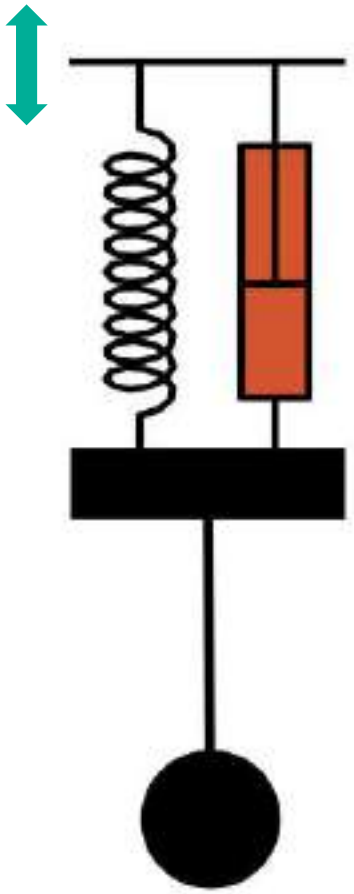
Driven dissipative oscillator



Bounded parametric oscillator?

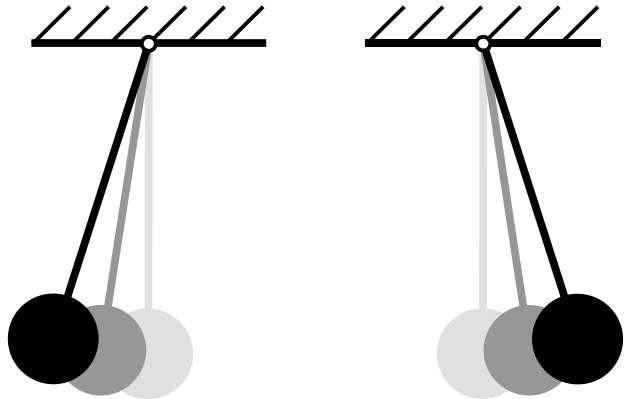


Mechanical solution



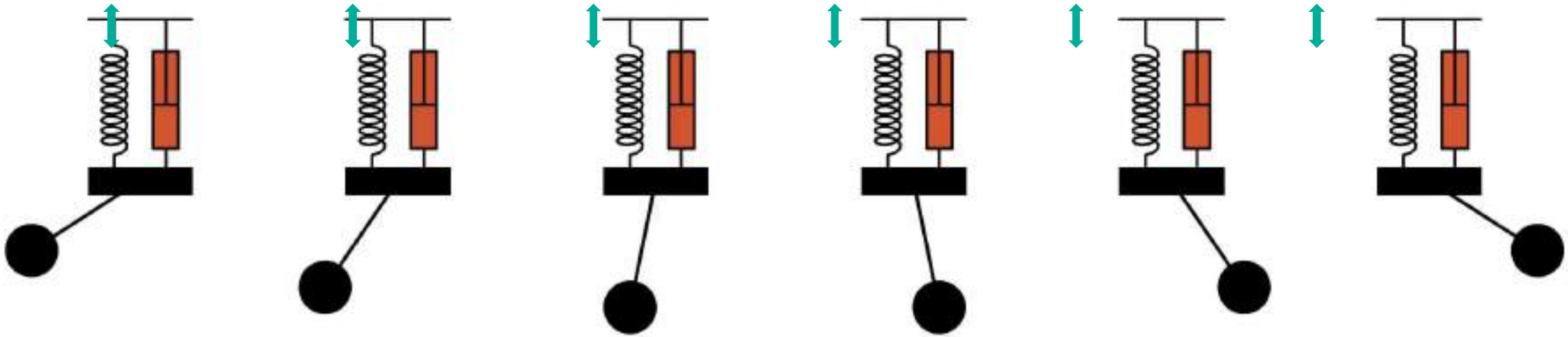
Dissipation prevents the motion from diverging.

From the problem symmetries, 2 possible solutions in which one can encode information.

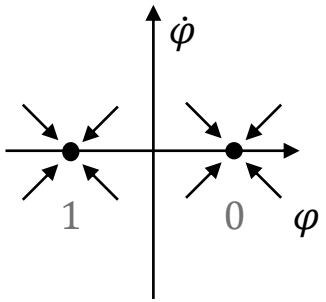


A. Marquet et al., 2023. arXiv:2307.06761

These 2 solutions are stable steady states



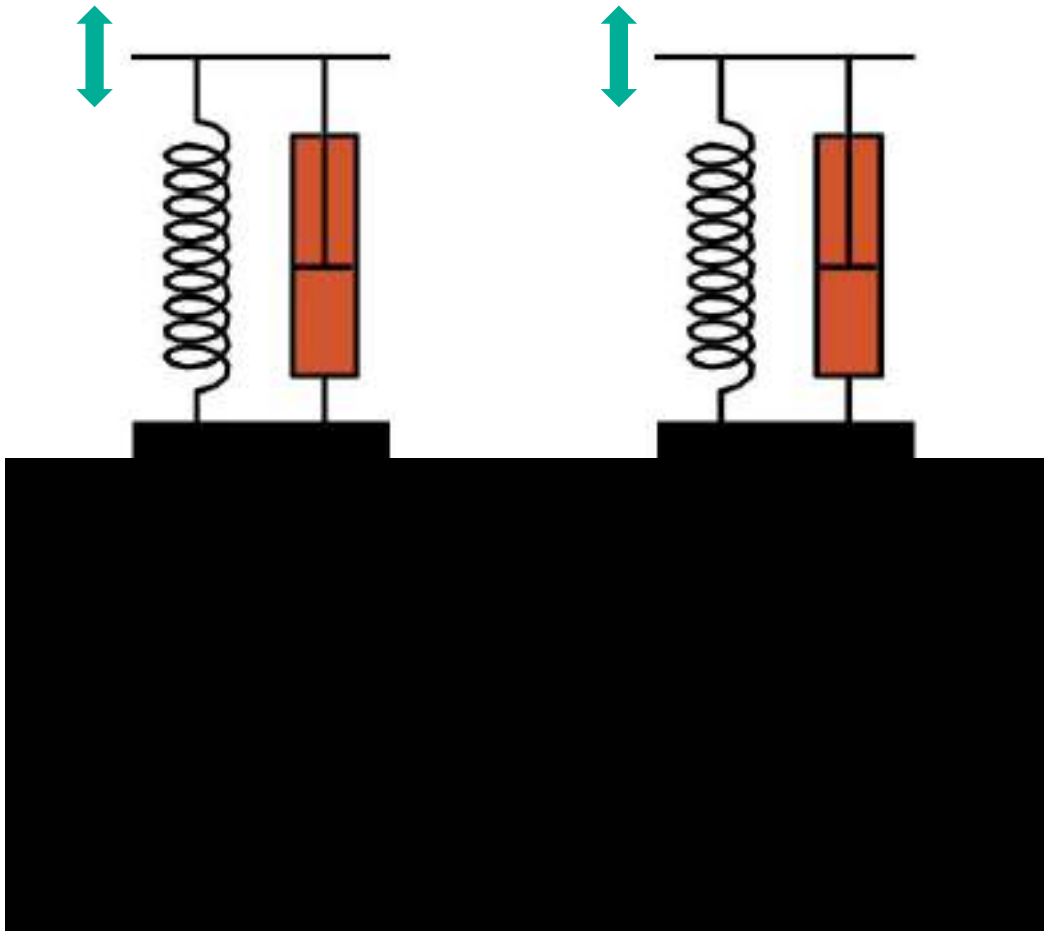
0 1



Dissipation stabilizes the system

Larger amplitude → unlikely bit-flips

Environment is oblivious to the phase mod π



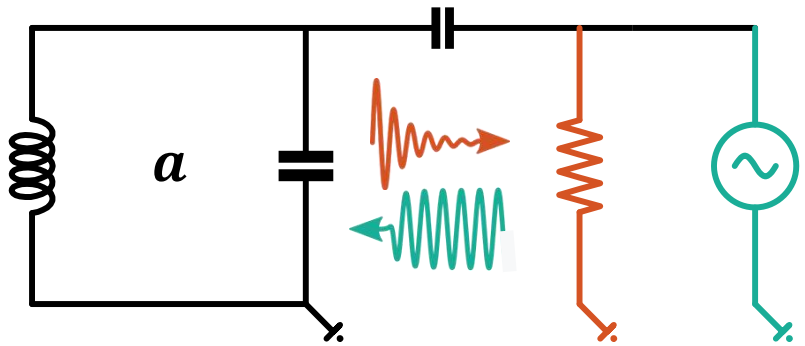
Stabilization compatible with quantum superposition

Key ingredient :
dissipation sensitive to φ^2

Quantum optics solution

$$\boldsymbol{a}|\alpha\rangle = \alpha|\alpha\rangle$$

Single photon coupling



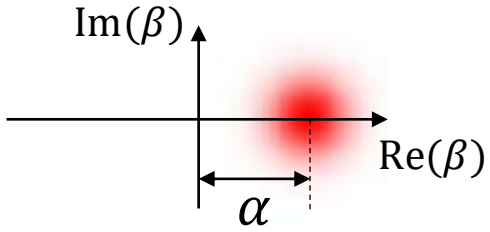
$$\boldsymbol{H}/\hbar = i\varepsilon_1(\boldsymbol{a}^\dagger - \boldsymbol{a}) \text{ (drive)}$$

$$\boldsymbol{L} = \sqrt{\kappa_1}\boldsymbol{a} \text{ (loss)}$$

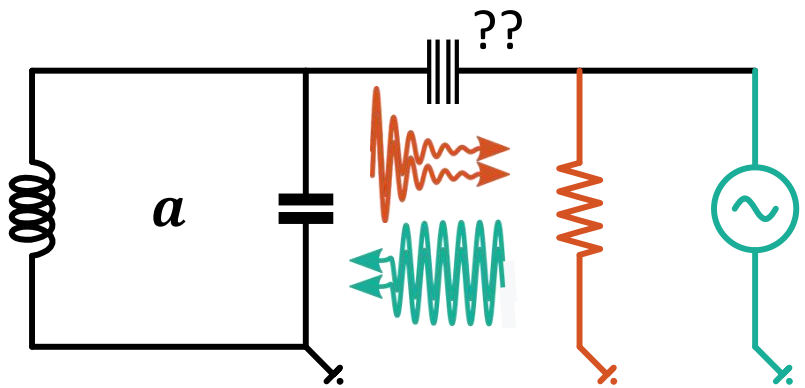
$$\boldsymbol{L} = \sqrt{\kappa_1}(\boldsymbol{a} - \alpha)$$

$$(\alpha = 2\varepsilon_1/\kappa_1)$$

$$\boldsymbol{L}|\alpha\rangle = 0$$



Two-photon coupling



$$\boldsymbol{H}/\hbar = i\varepsilon_2(\boldsymbol{a}^{\dagger 2} - \boldsymbol{a}^2) \text{ (drive)}$$

$$\boldsymbol{L} = \sqrt{\kappa_2}\boldsymbol{a}^2 \text{ (loss)}$$

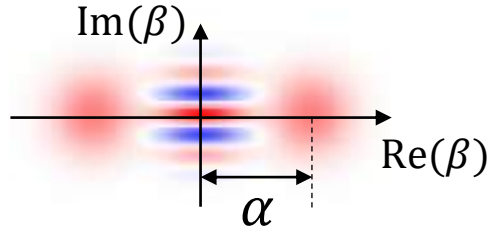
$$\boldsymbol{L} = \sqrt{\kappa_2}(\boldsymbol{a}^2 - \alpha^2)$$

$$(\alpha = \sqrt{2\varepsilon_2/\kappa_2})$$

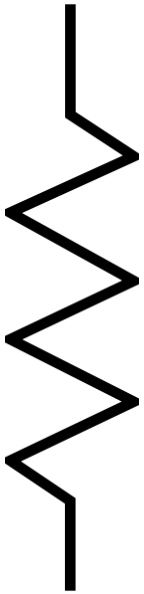
$$\boldsymbol{L}|\alpha\rangle = 0$$

$$\boldsymbol{L}|-\alpha\rangle = 0$$

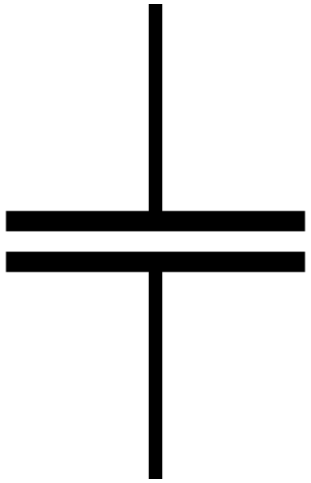
$$\boldsymbol{L}(\lambda|\alpha\rangle + \mu|-\alpha\rangle) = 0$$



Intro to superconducting circuits



Resistance
=
dissipation

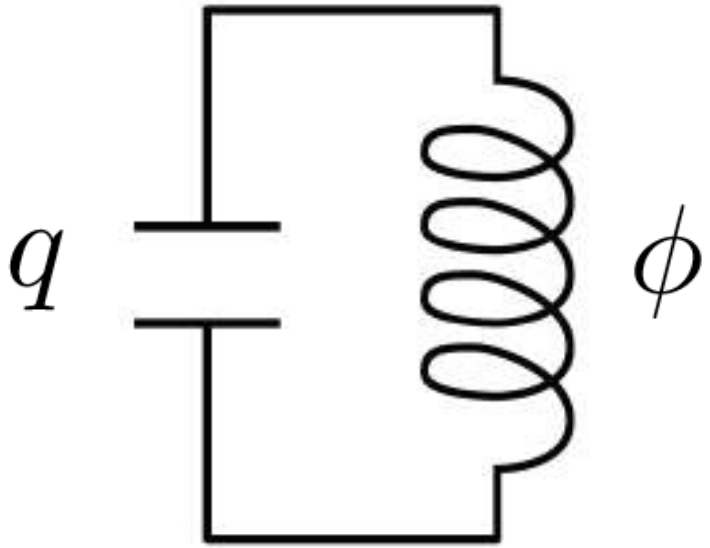


Capacitance



Inductance

Harmonic oscillator

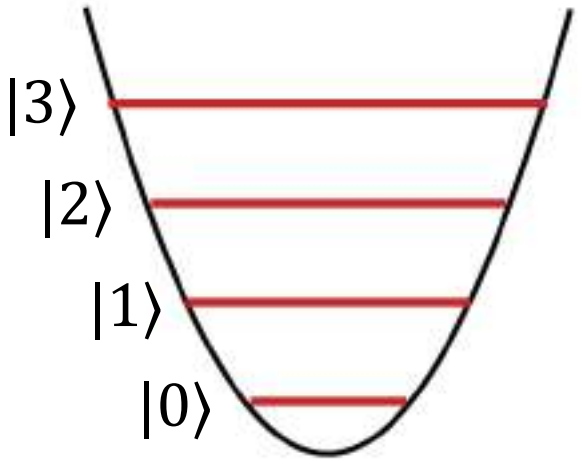


$$\hat{H} = \frac{\hat{q}^2}{2C} + \frac{\hat{\phi}^2}{2L}$$

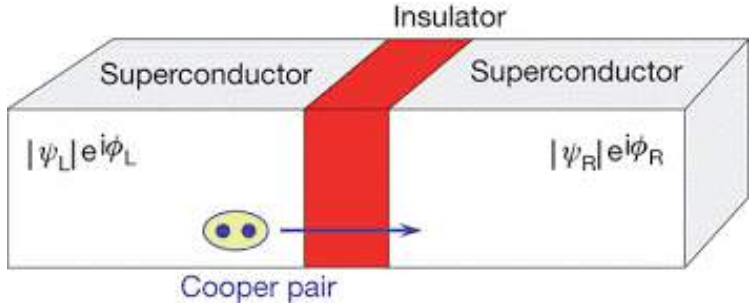
$$\hat{q} \propto \hat{a} - \hat{a}^\dagger$$

$$\hat{\phi} \propto \hat{a} + \hat{a}^\dagger$$

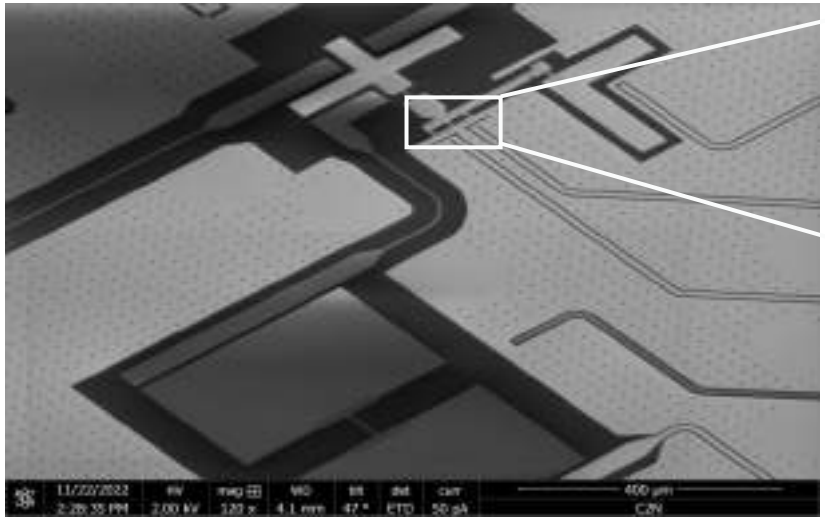
$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)$$



Josephson junction

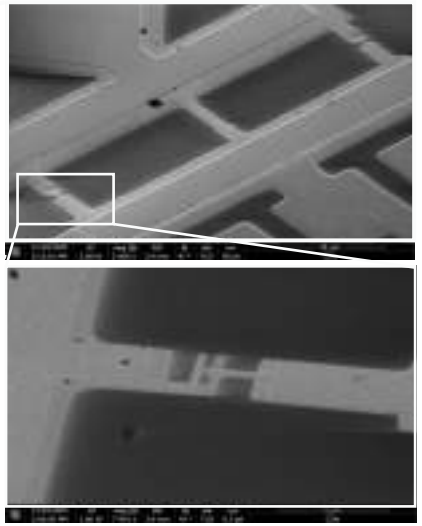


$$\hat{H} = -E_J \cos\left(\hat{\phi}\right)$$

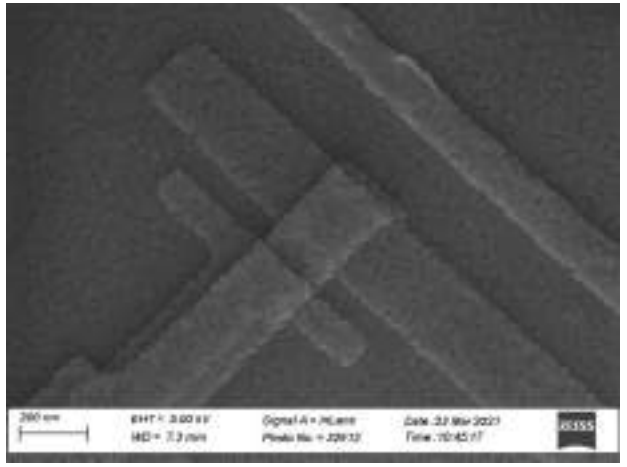


400 µm

20 µm

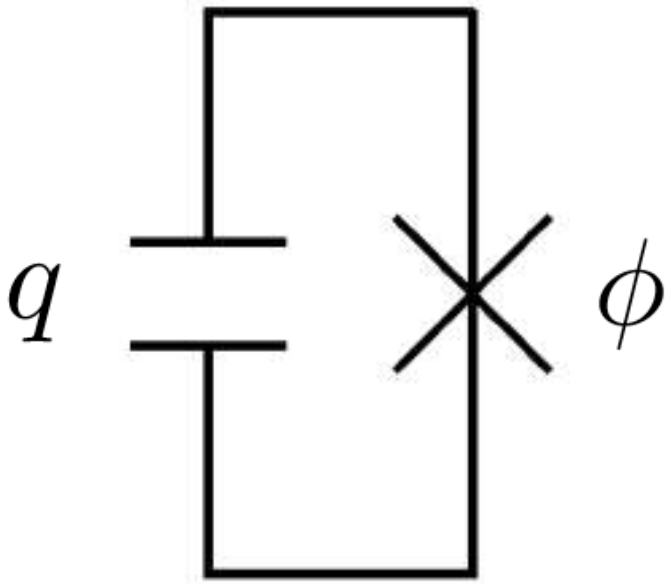


5 µm



200 nm

Transmon

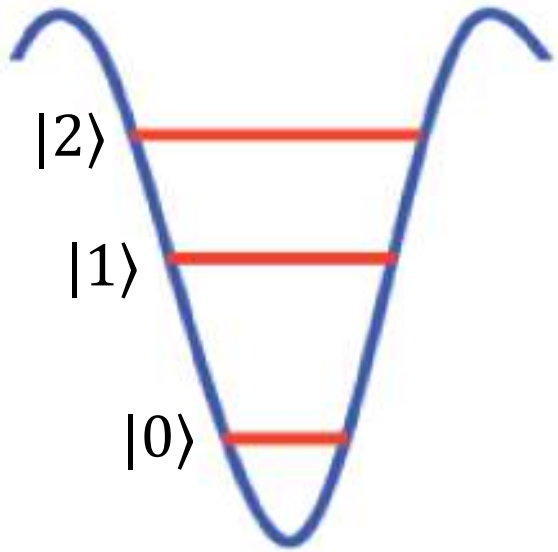


$$\hat{H} = \frac{\hat{q}^2}{2C} - E_J \cos\left(\hat{\phi}\right)$$

$$\hat{q} \propto \hat{a} - \hat{a}^\dagger$$

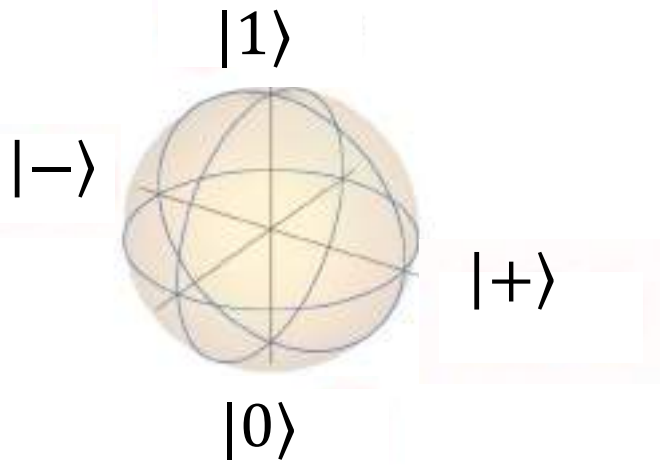
$$\hat{\phi} \propto \hat{a} + \hat{a}^\dagger$$

$$\hat{H}/\hbar = \omega_{01}\hat{a}^\dagger\hat{a} + \frac{\alpha}{2}\hat{a}^\dagger\hat{a}(\hat{a}^\dagger\hat{a} - 1)$$



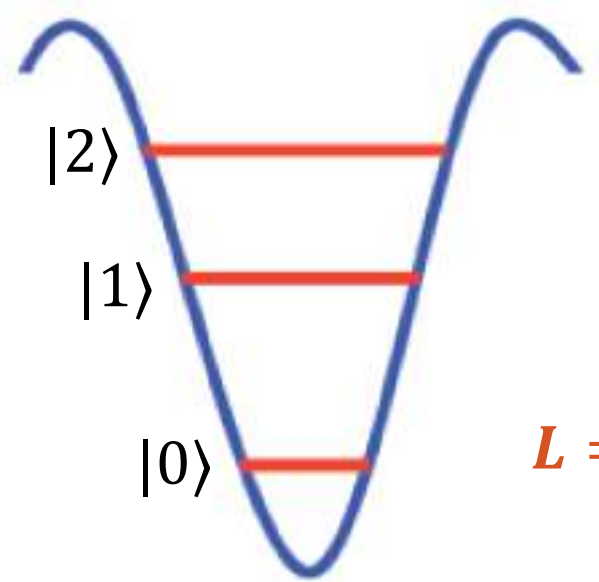
The **Josephson junction** introduces **non-linearities** in the system via the cosine potential

Transmon encoding



$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

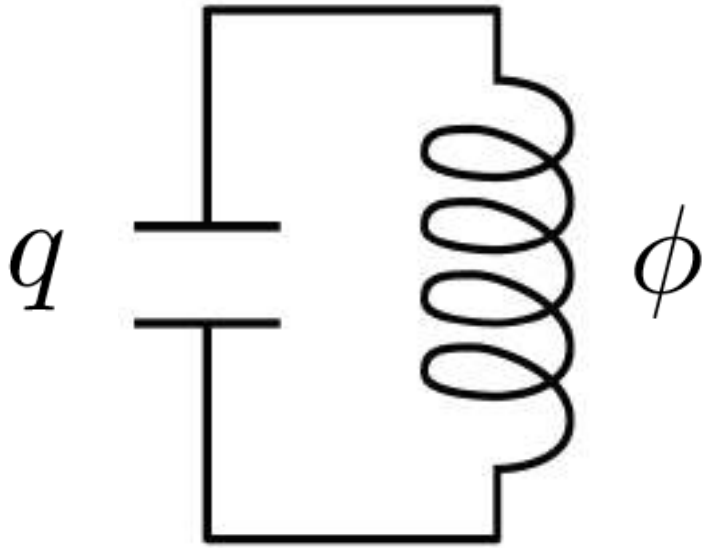


$$\boldsymbol{L = \sqrt{\kappa_1}\, a}$$

Transmons suffer from **single-photon loss**, which causes bit-flip and information loss.

Can we find a smarter encoding?

Harmonic oscillator

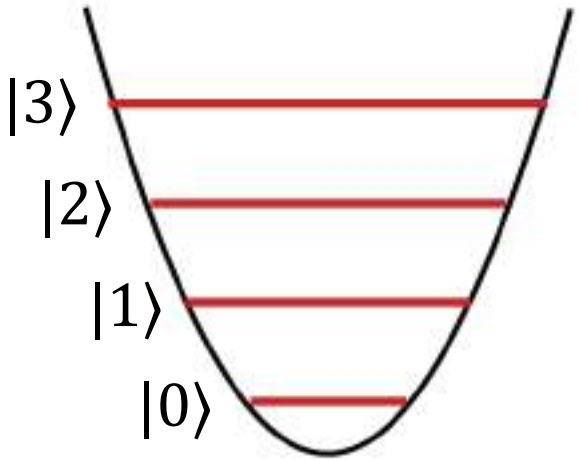


$$\hat{H} = \frac{\hat{q}^2}{2C} + \frac{\hat{\phi}^2}{2L}$$

$$\hat{q} \propto \hat{a} - \hat{a}^\dagger$$

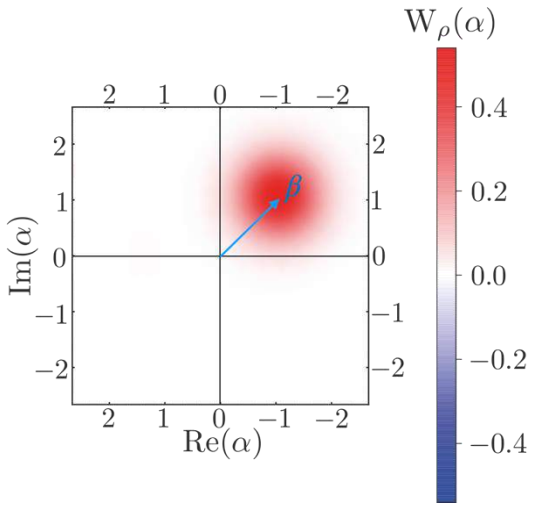
$$\hat{\phi} \propto \hat{a} + \hat{a}^\dagger$$

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)$$

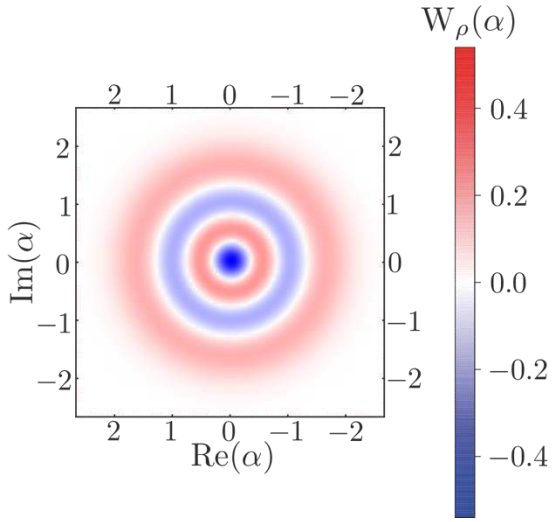


Wigner function

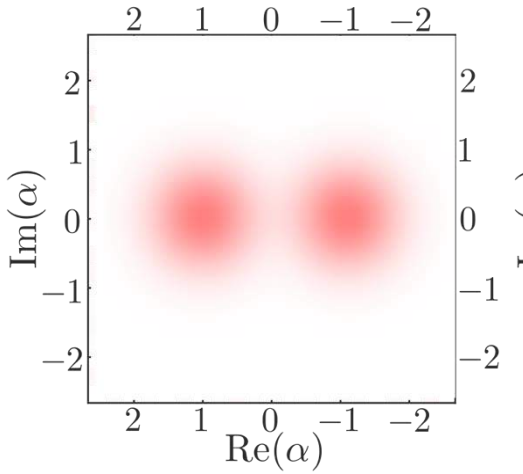
coherent state $|\beta\rangle$



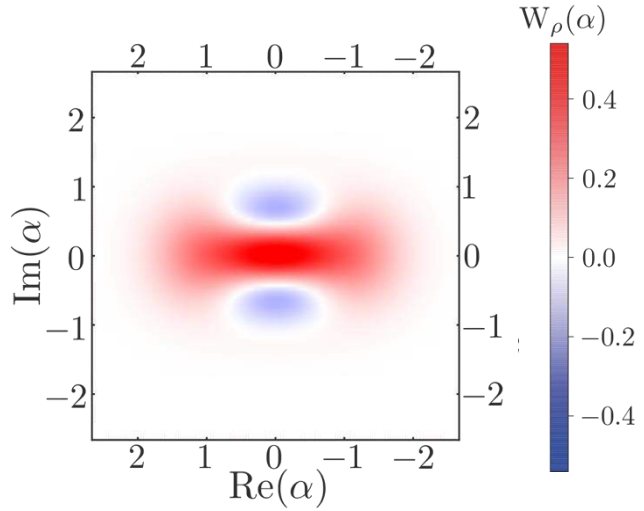
Fock state $|3\rangle$



$|\beta\rangle\langle\beta| + |-\beta\rangle\langle-\beta|$



$|\beta\rangle + |-\beta\rangle$



The **Wigner function** is a representation in phase space of the harmonic oscillator state

- negativity is a signature of non-classical state

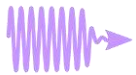
Wigner function

$$W(\alpha) = \mathrm{Tr}(D^\dagger(\alpha)\rho D(\alpha)P) \text{ with } P = e^{i\pi\hat{a}^\dagger\hat{a}}$$

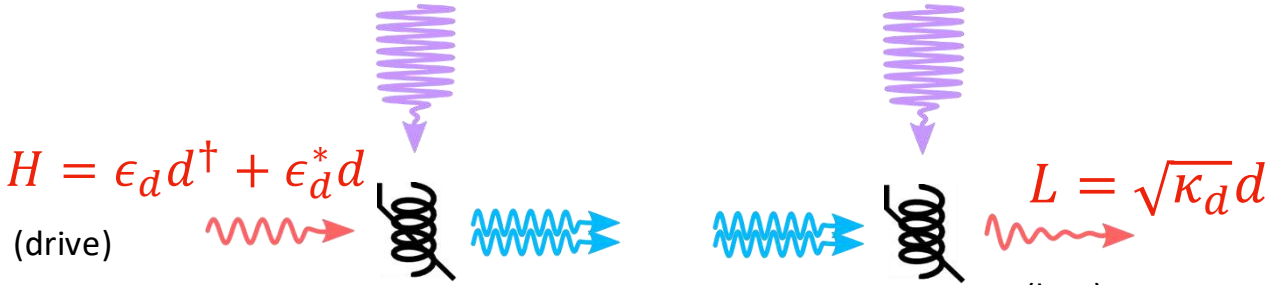
Stabilizing the cat manifold

Parametric pumping for 2-photon coupling

$$H = g_2 a^{\dagger 2} d + g_2 a^2 d^\dagger$$



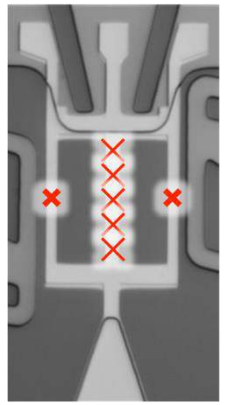
$$\omega_p = 2\omega_a - \omega_d$$



$$H_{eff} = \epsilon_2^* a^2 + \epsilon_2 a^{\dagger 2}$$
(two-photon drive)

$$L_{eff} = \sqrt{\kappa_2} a^2$$
(two-photon loss)

The ATS



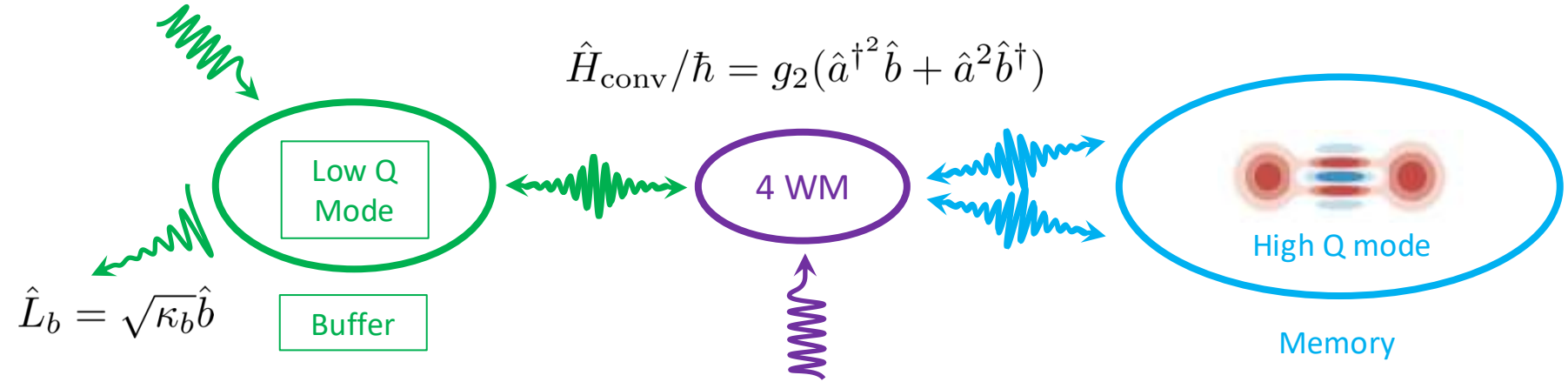
Parametric mixing device
(4-wave mixing Hamiltonian)

Z. Leghtas et al, Science 2015
S. Touzard et al, PRX 2018
R. Lescanne et al., Nature Physics 2020

Dissipative cat qubits – Hamiltonian model

$\hat{H}_{\text{drive}}/\hbar = \epsilon_d(\hat{b}^\dagger + \hat{b})$

$\hat{H}_{\text{conv}}/\hbar = g_2(\hat{a}^{\dagger 2}\hat{b} + \hat{a}^2\hat{b}^\dagger)$



$\hat{L}_b = \sqrt{\kappa_b}\hat{b}$

$g_2 \ll \kappa_b$

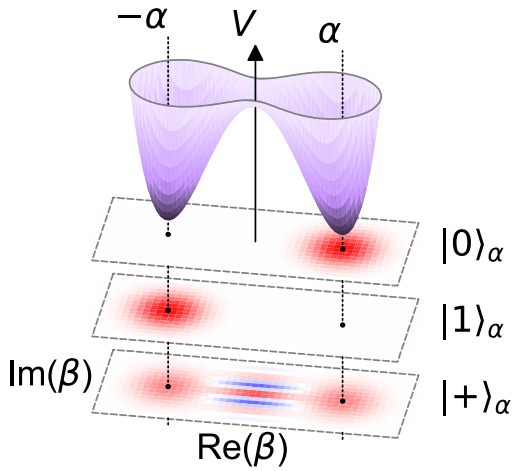
$\kappa_2 = \frac{4g_2^2}{\kappa_b}$ $\quad \hat{L}_2 = \sqrt{\kappa_2}(\hat{a}^2 - \alpha^2)$

$\alpha^2 = -\frac{\epsilon_d}{g_2}$

Effective dynamics of the memory mode

$\dot{\rho} = \kappa_2 D[\hat{a}^2 - \alpha^2]\rho$

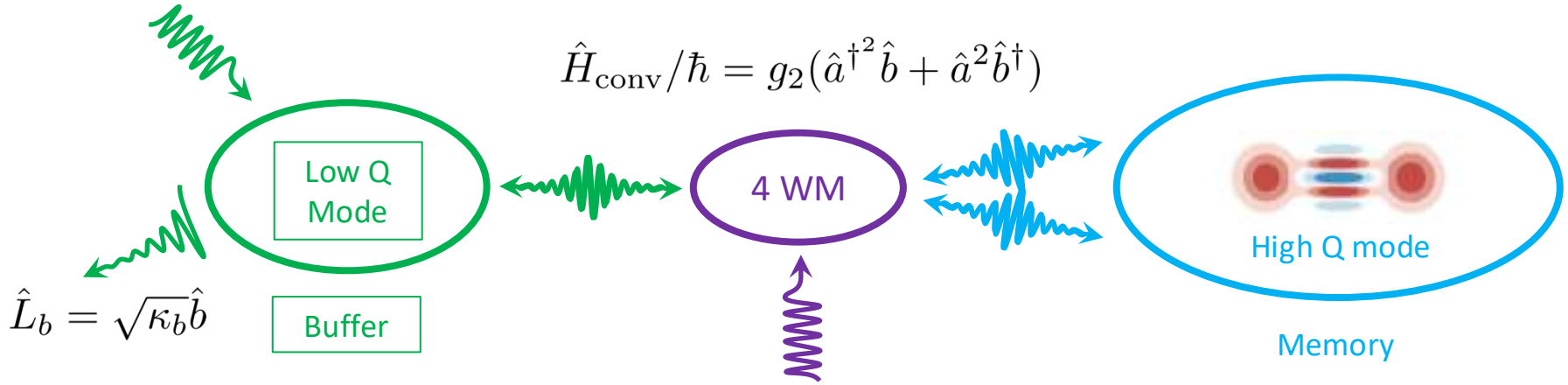
Superpositions of $|\pm\alpha\rangle$ are steady-states



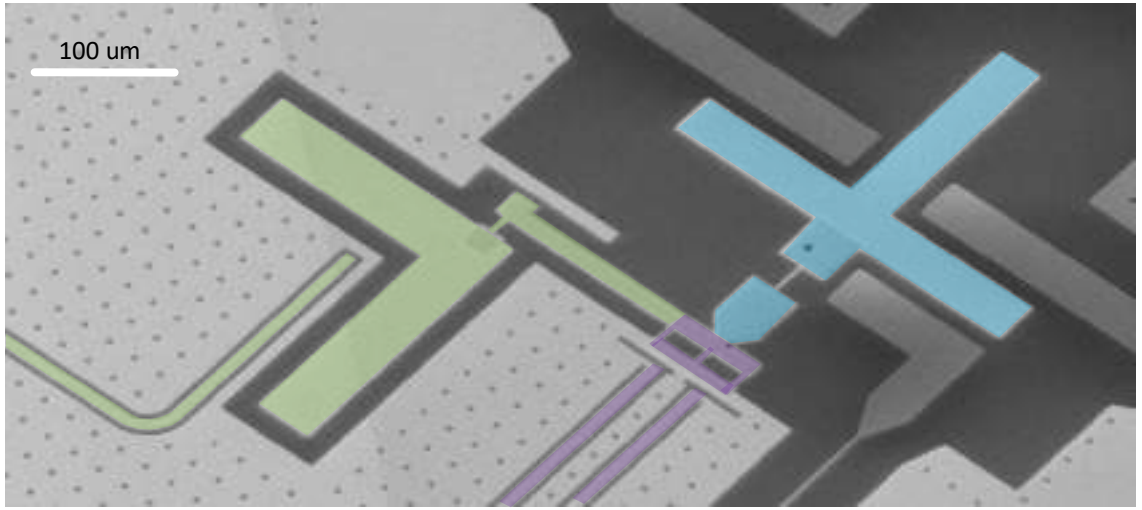
Dissipative cat qubits – Hamiltonian model

$$\hat{H}_{\text{drive}}/\hbar = \epsilon_d(\hat{b}^\dagger + \hat{b})$$

$$\hat{H}_{\text{conv}}/\hbar = g_2(\hat{a}^{\dagger 2}\hat{b} + \hat{a}^2\hat{b}^\dagger)$$



$$\hat{L}_b = \sqrt{\kappa_b}\hat{b}$$



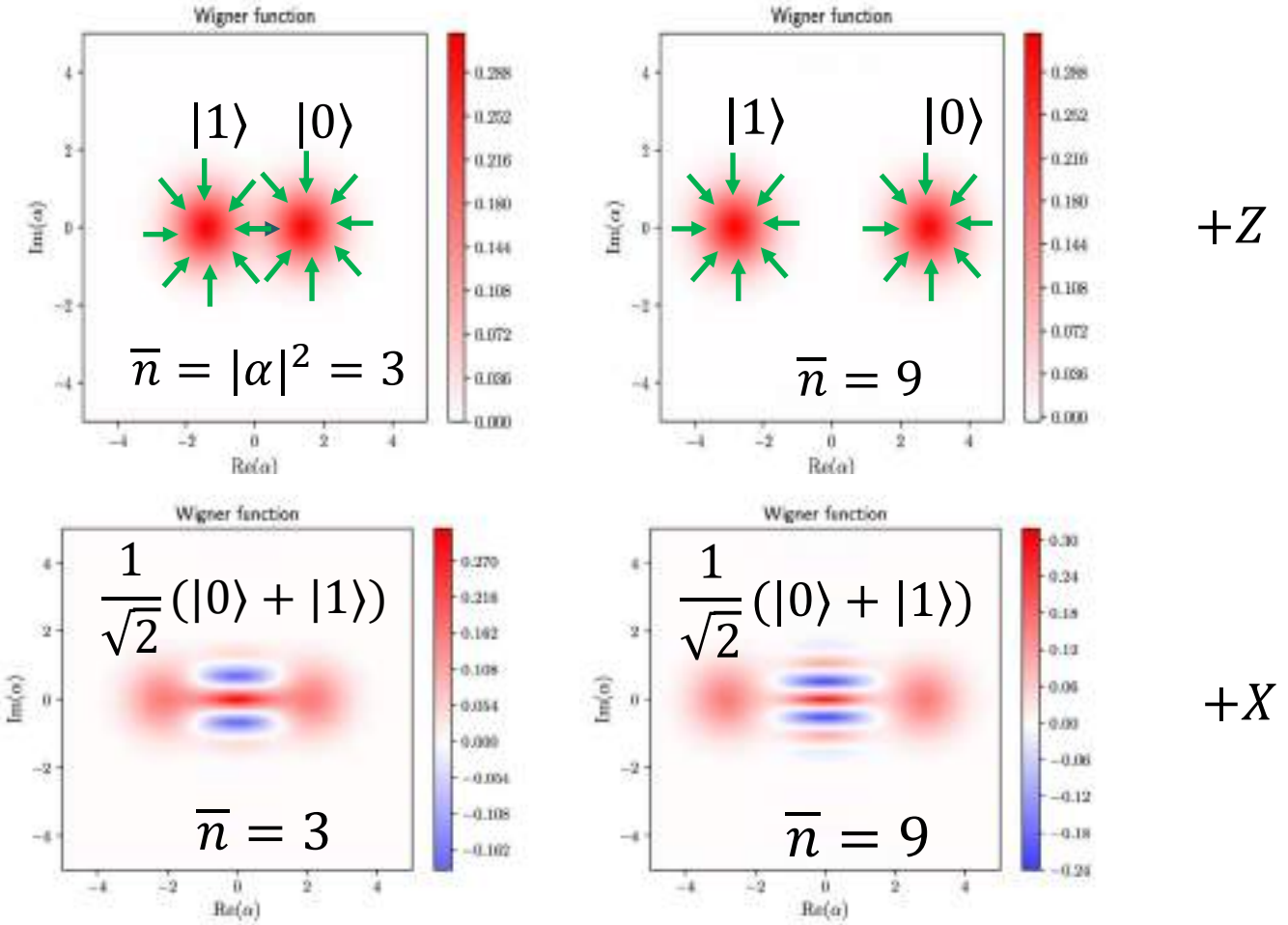
The dissipative cat: a biased noise qubit

Exponential reduction of bit-flips

Typical noise acts locally in phase-space

$$\frac{dW_\rho}{dt} = \frac{\kappa_1}{2}\left(\frac{\partial^2}{\partial\alpha\partial\alpha^*} + \frac{\partial}{\partial\alpha}\alpha + \frac{\partial}{\partial\alpha^*}\alpha^*\right)W_\rho$$

Linear increase of phase-flips

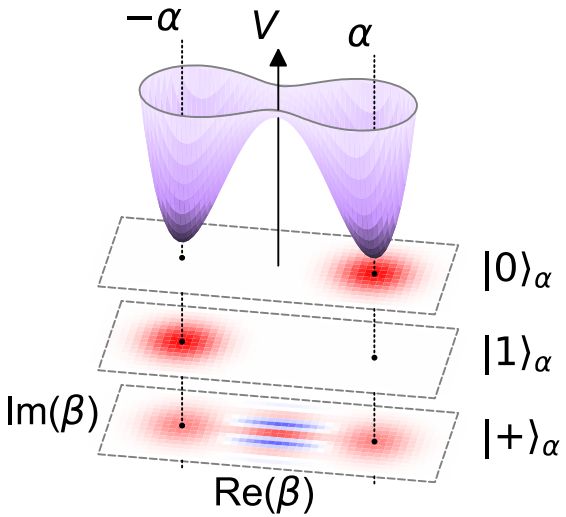


see J. Cohen, PhD thesis, 2017

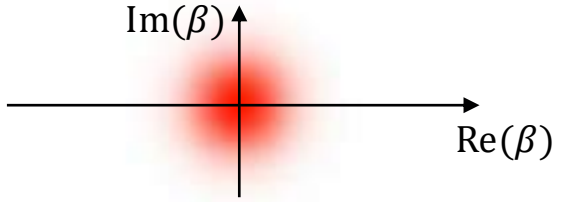
A biased noise qubit

Bias : $\Gamma_{bf} \ll \Gamma_{pf}$

Bit-flips are suppressed exponentially → $\Gamma_{bf} \propto e^{-|\alpha|^2}$
Phase-flips increase linearly → $\Gamma_{pf} = 2|\alpha|^2\kappa_1$



Preparation

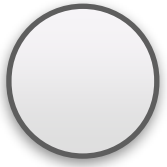


- Qubit, stable (rare bit-flips)
  coherent (rare phase-flips)
- Initialize and measure $|0/1\rangle$, $|+/-\rangle$
- How to apply gates?

Z. Leghtas et al. Science 347, 853 (2015).
S. Touzard et al. Phys. Rev. X, 8:021005, Apr 2018
R. Lescanne et al. Nature Physics 16, 509 (2020).
U. Reglade, A. Bocquet et al., 2023. arXiv:2307.06617

« Hardware-efficient » protection against bit-flips

$p_X = p_Z$



$$|0\rangle_L = |0\ldots0\rangle = |0\rangle^{\otimes d}$$

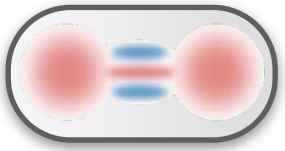
$$|1\rangle_L = |1\ldots1\rangle = |1\rangle^{\otimes d}$$

$$|\pm\rangle_L = \frac{1}{\sqrt{2}}(|0\rangle_L \pm |1\rangle_L)$$

$$\mathbb{P}[X_L] = \mathbb{P}[\text{majority of qubits bit-flipped }] \propto \binom{d}{\frac{d+1}{2}} {p_X}^{\frac{d+1}{2}} \quad \to 0$$

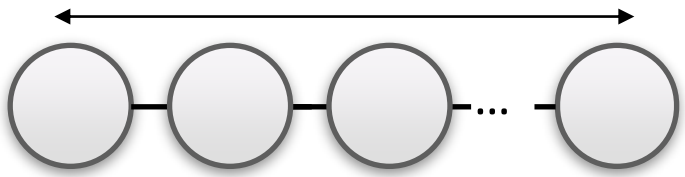
$$\mathbb{P}[Z_L] = \mathbb{P}[\text{any of the qubits phase-flipped }] \propto d \times p_Z$$

α^2



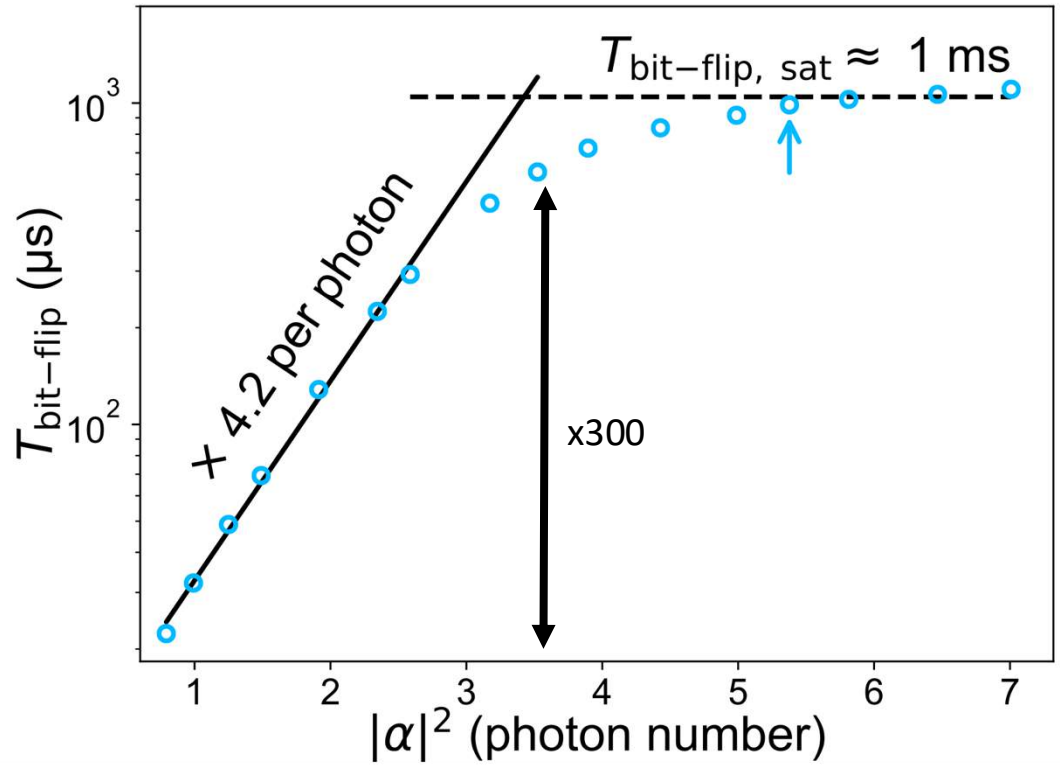
« ⟺ »

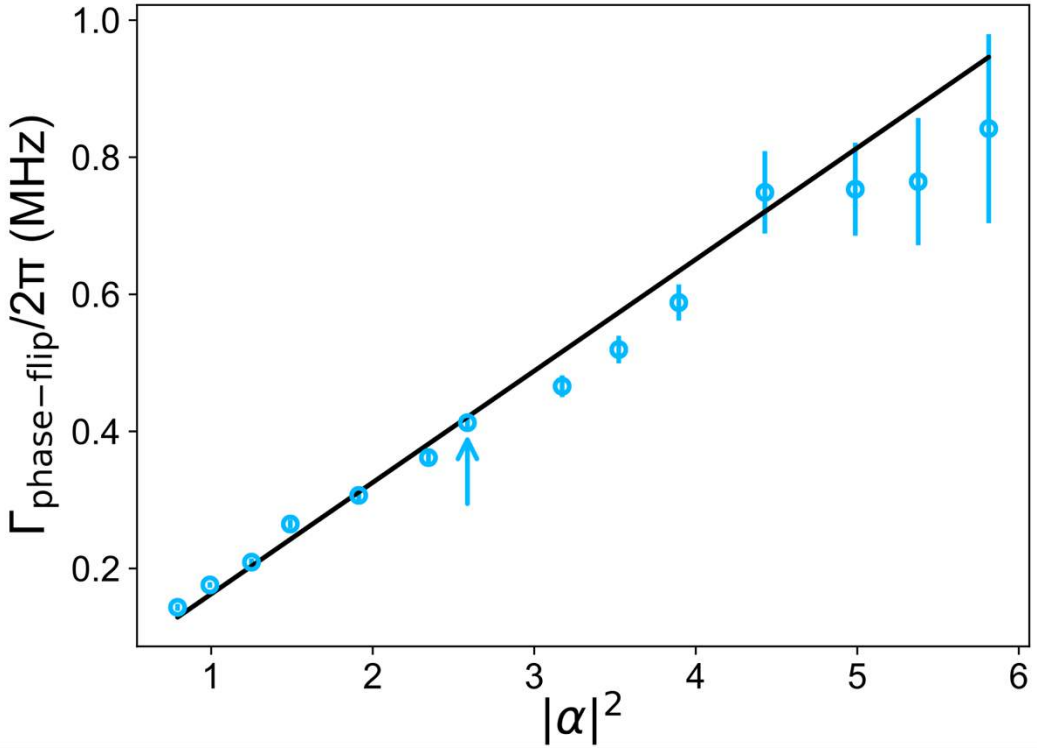
d



Experimental macroscopic bit-flip times?

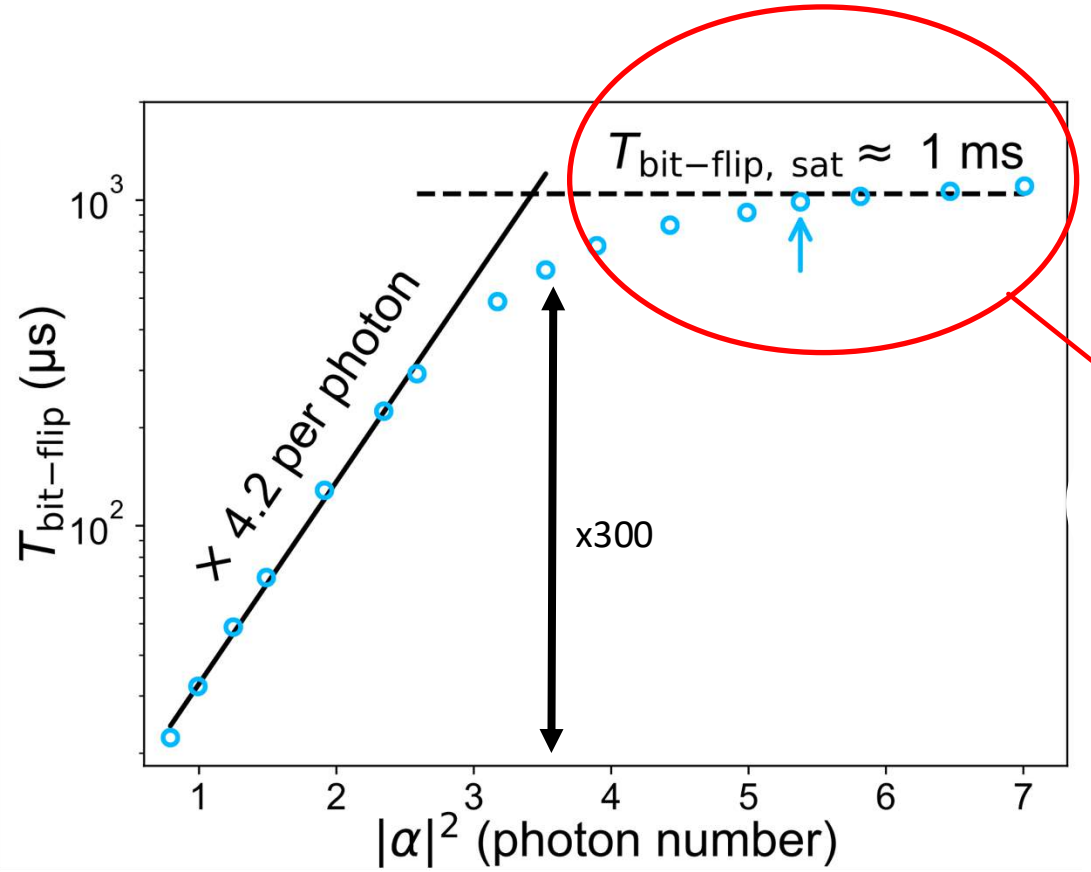
Experimental realization of error scaling



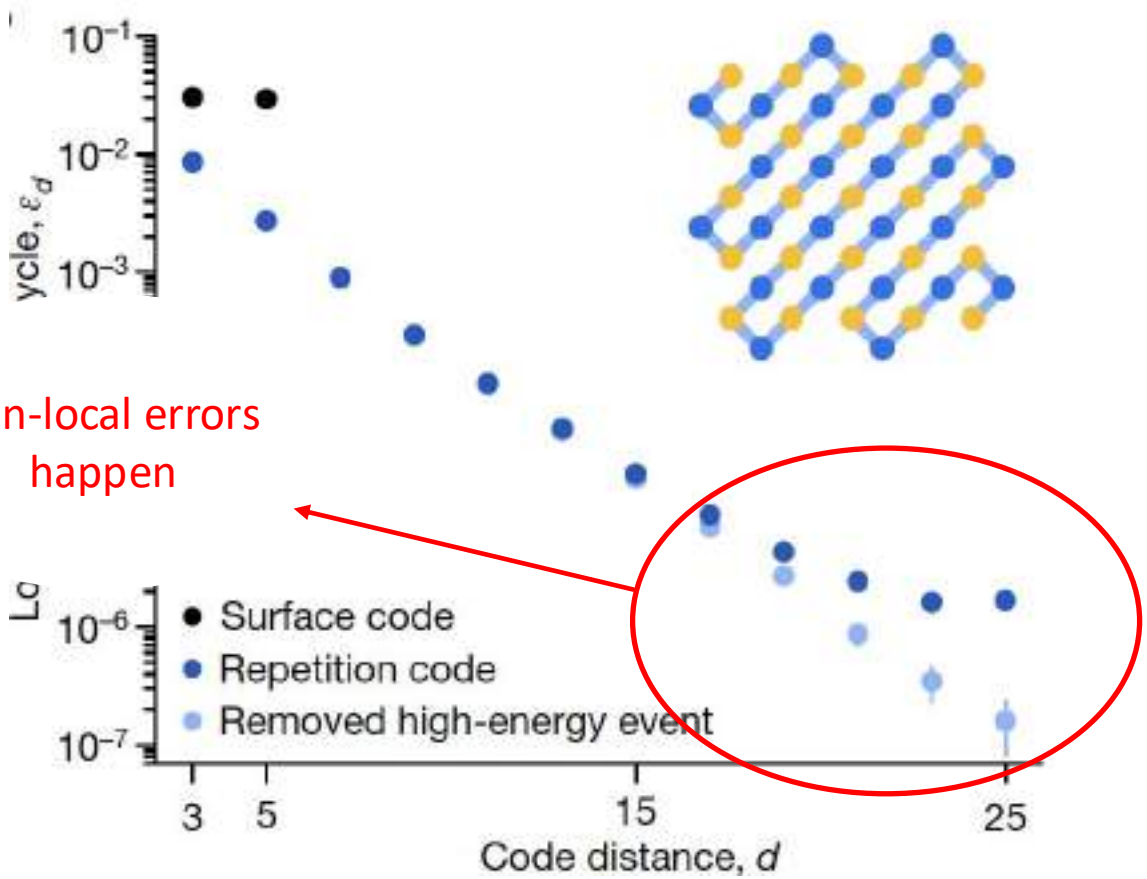


R. Lescanne, Z. Leghtas et al., Nature Physics, 2020

Experimental realization of error scaling

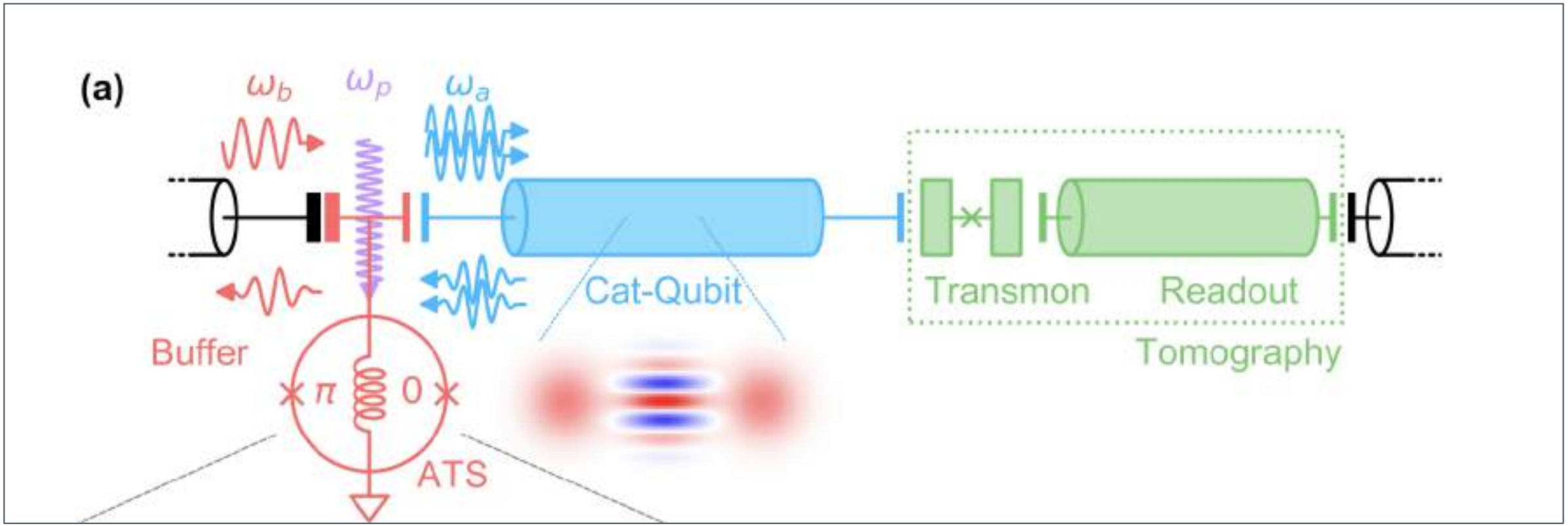


R. Lescanne, Z. Leghtas et al., Nature Physics, 2020



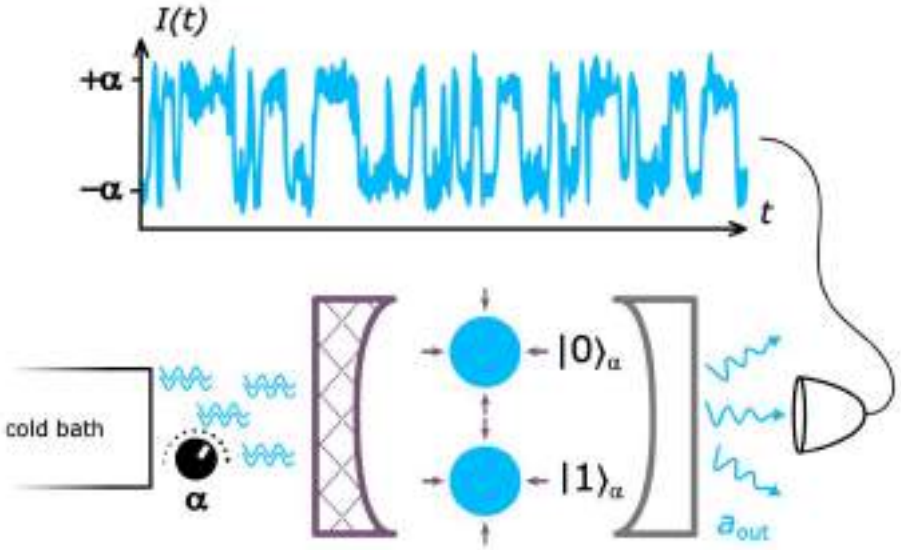
Google Quantum AI, Nature, 2023

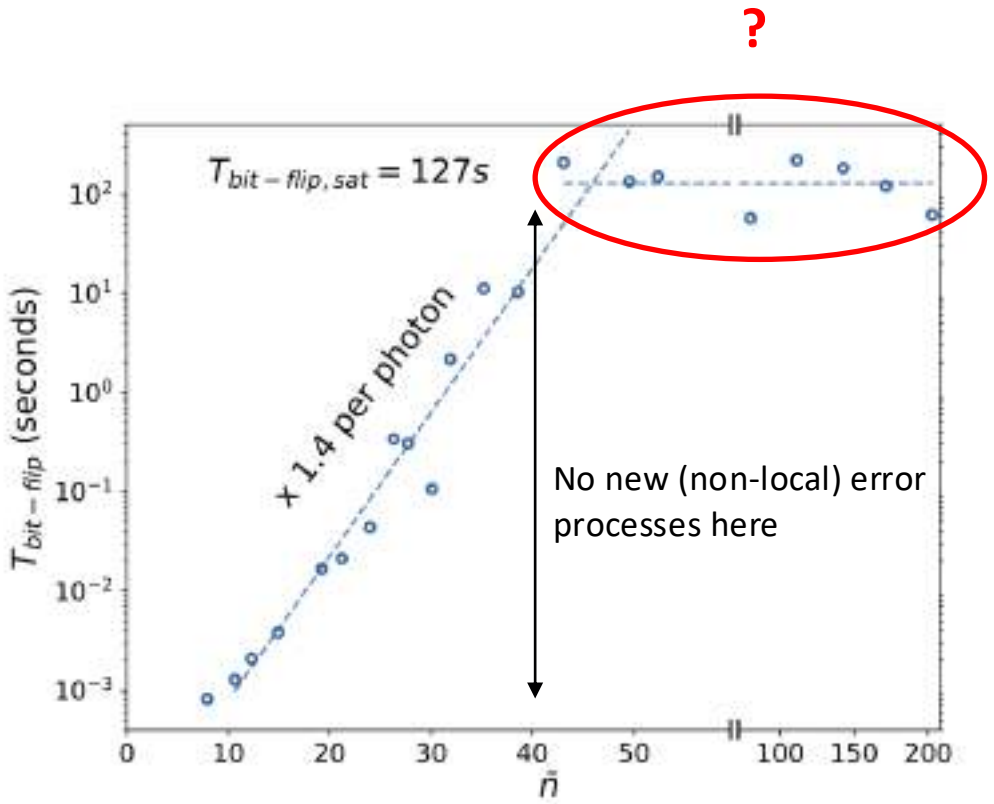
Experimental suppression of bit-flips



R. Lescanne, Z. Leghtas et al., Nature Physics, 2020

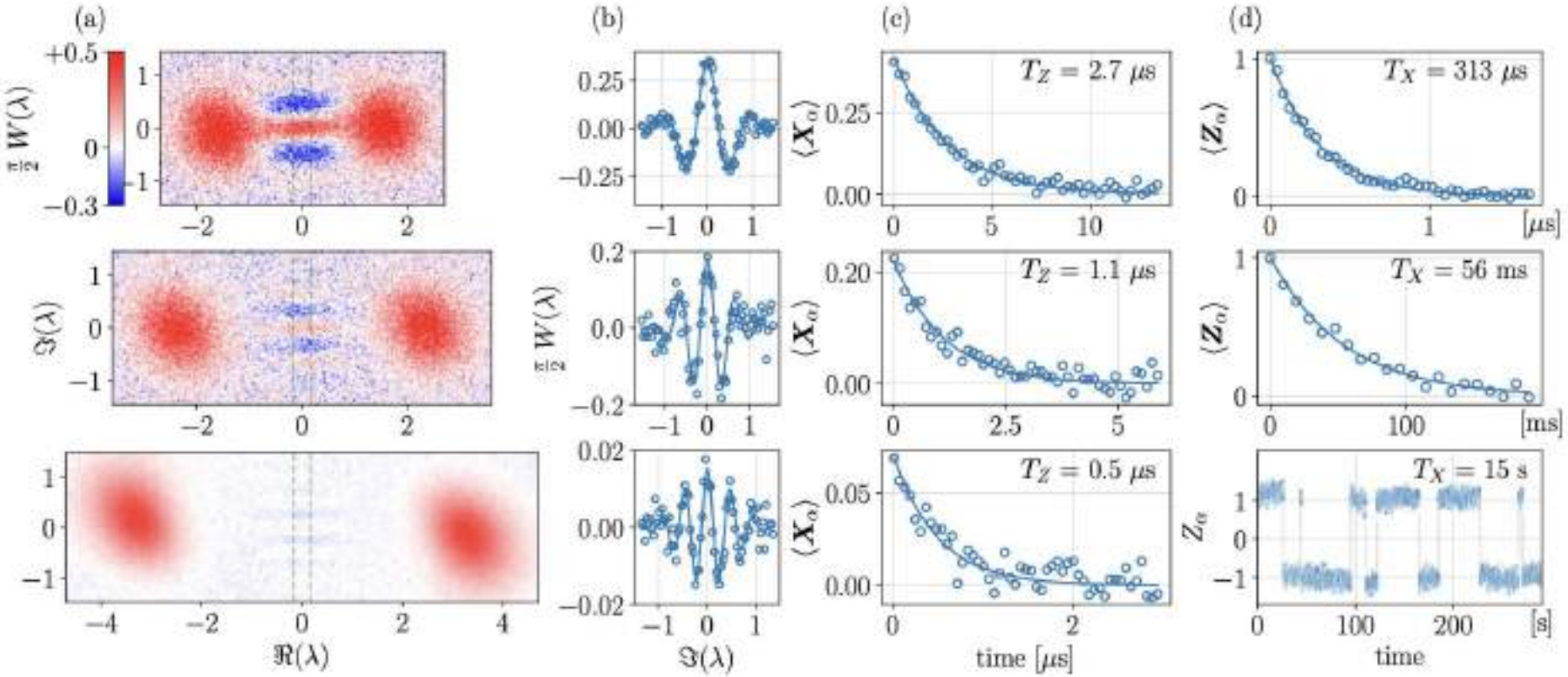
Experimental suppression of bit-flips





C. Berdou, Z. Leghtas et al., PRX Quantum, 2023, doi:10.1103/PRXQuantum.4.020350
K. Dubovitskii et al., arxiv:2403.15310

Experimental suppression of bit-flips



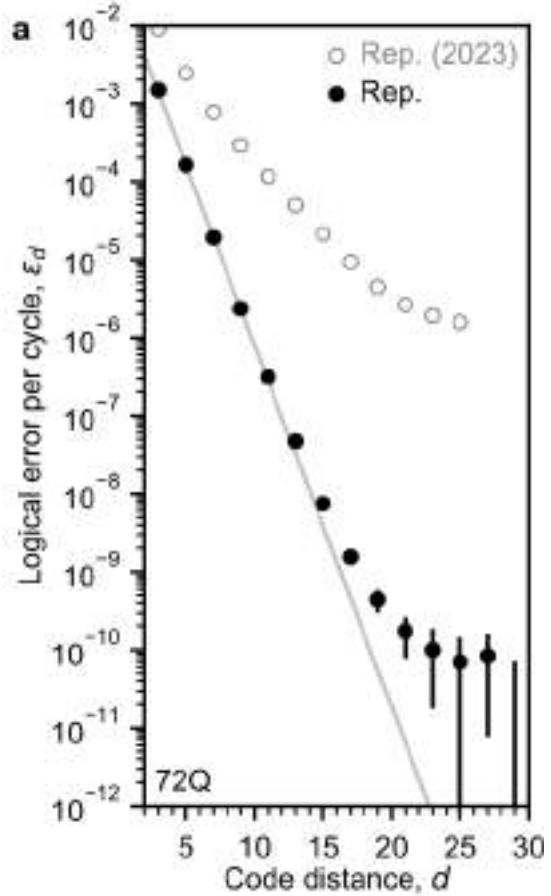
$\alpha^2 = 2.5$

$\alpha^2 = 5.6$

$\alpha^2 = 11.3$

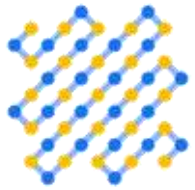
U. Réglade, A. Bocquet et. al, Nature 629, 778-783 (2024)

Hour long bit-flip time



Google Quantum AI et al., Nature (2023)

Google AI Quantum



$1/\Gamma_Z \approx 1$ s

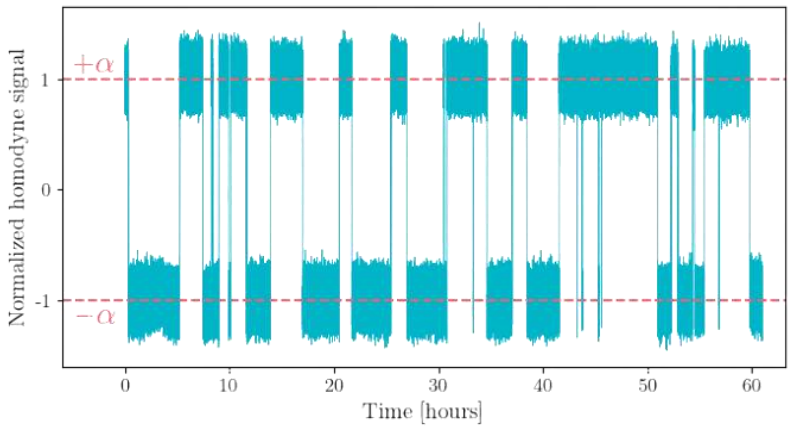
Limited by cosmic events

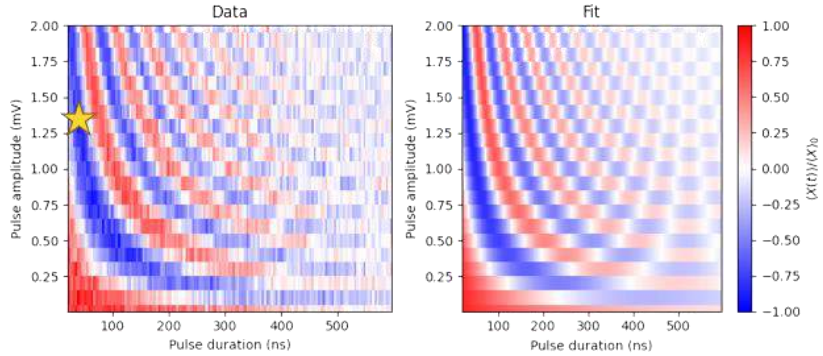
$1/\Gamma_Z \approx 3$ h

Limited by cosmic events (higher energy)

Google Quantum AI et al., Nature (2025)

$1/\Gamma_Z \in [33, 60]$ min $\quad \bar{n} = 11$





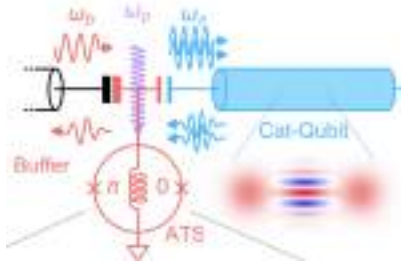
$\mathcal{F}_{Z_\pi} = 94.2\%$ $\quad T_{Z_\pi} = 26.5$ns $\quad 1/\Gamma_X = 420$ ns

https://alice-bob.com/blog/just-out-of-the-lab-a-cat-qubit-that-jumps-every-hour/

κ_1/κ_2 and Concept Cats

Breeding cats at Alice & Bob

2D capacitive cat qubit (Boson1)

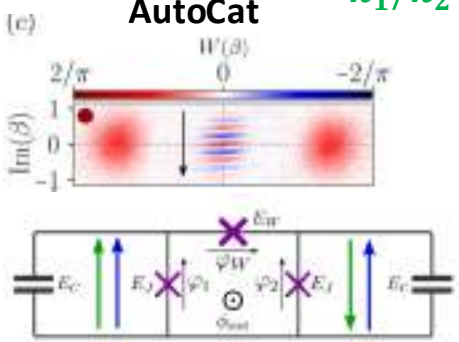


R. Lescanne et al.,
Nature Physics (2020)

Resonant 2–1 photon interaction

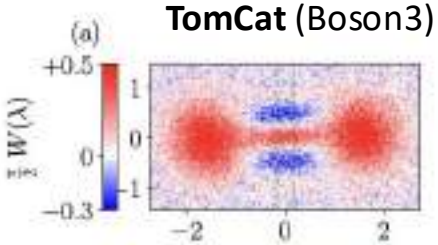
$\kappa_1/\kappa_2 = 6.5\times10^{-3}$

AutoCat



A. Marquet et al.,
PRX (2024)

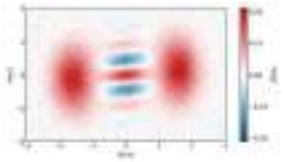
TomCat (Boson3)

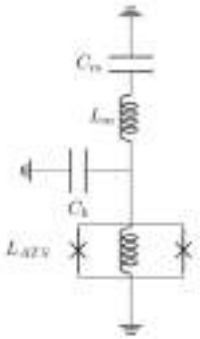


U. Réglade, A. Bocquet et al.,
Nature (2024)

Transmon-free readout

MoonCat (and FatCat, and GalvanicCat)





R. Rousseau et al.,
arXiv: 2502.07892

Squeezed cat

See also Boson4 on Alice&Bob cloud

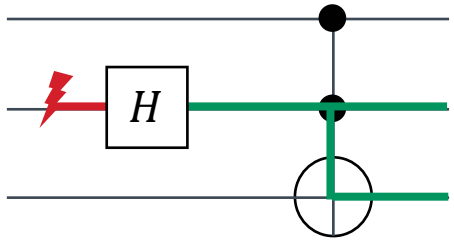
03

Bias-preserving gates

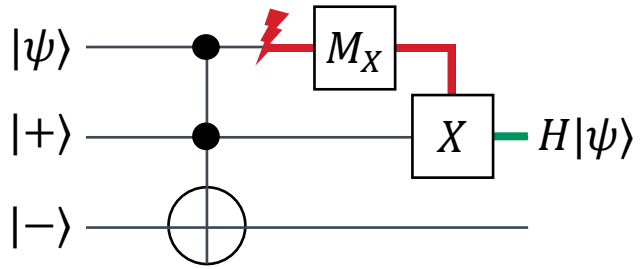
And the curse of universality

Taking advantage of a biased noise qubit

Circuit with universal gates



$ZH = HX$



Two consequences

- Universality + useful bias noise → need correct phase-flip **before** going universal
- Physical gates need to **preserve** the bias

- Qubit, stable (rare bit-flips)
  coherent (rare phase-flips)
- Initialize and measure $|0/1\rangle$, $|+/-\rangle$
- Physical bias-preserving gates
- Logical universal set of gate

Bias preserving gates with cat qubits: Z gate

Rotations around the Z axis

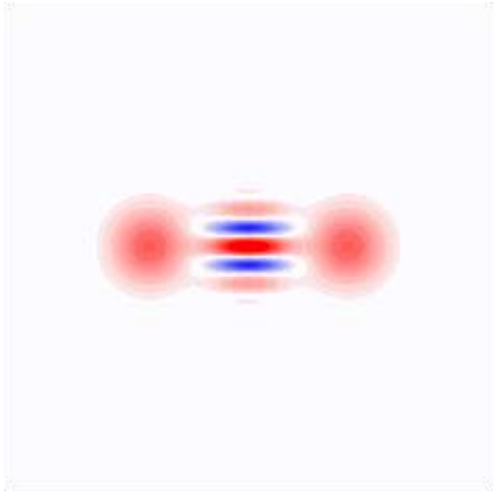
$$L = \kappa_2 \mathcal{D}[a^2 - \alpha^2]$$

$$\text{or } \mathrm{H} = g_2(a^2 - \alpha^2)\sigma_+ + h.c$$

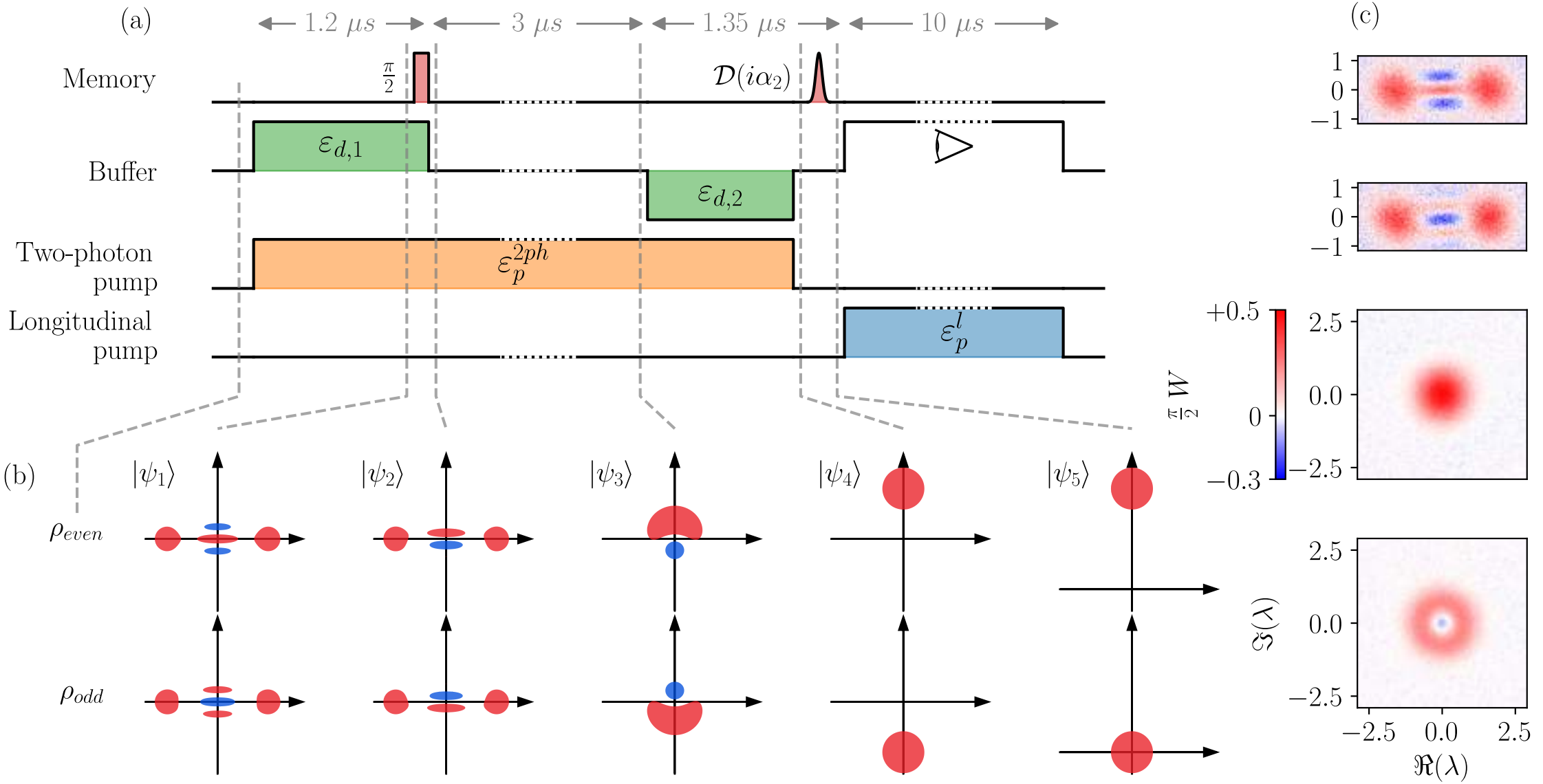
$$\text{or } \mathrm{H} = K(a^2 - \alpha^2)^\dagger(a^2 - \alpha^2)$$

$$+ H = g_Z\left(a + a^\dagger\right)$$

$$T = \pi/4\alpha g_Z$$



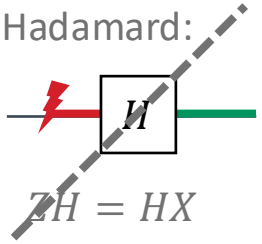
X measurement: holonomic gate



Bias preserving gates with cat qubits: X gate

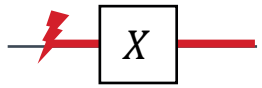
Some evolutions

Hadamard:



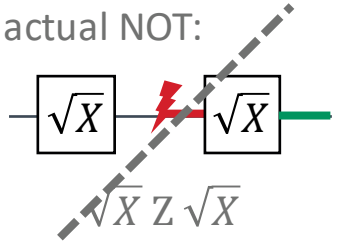
$ZH = HX$

NOT:



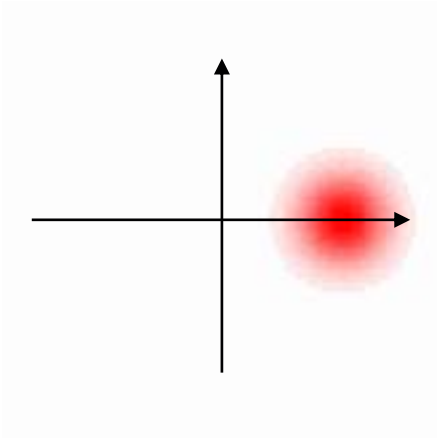
$ZX = X(-Z)$

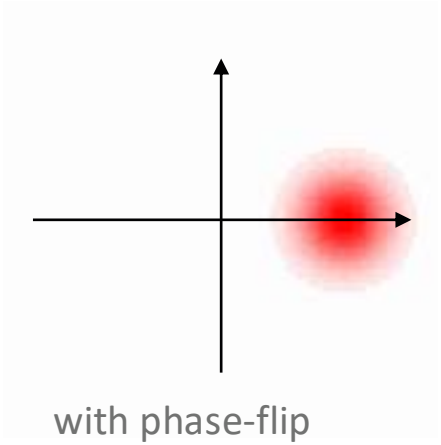
actual NOT:



$\sqrt{X}\,\mathrm{Z}\,\sqrt{X} = XY$

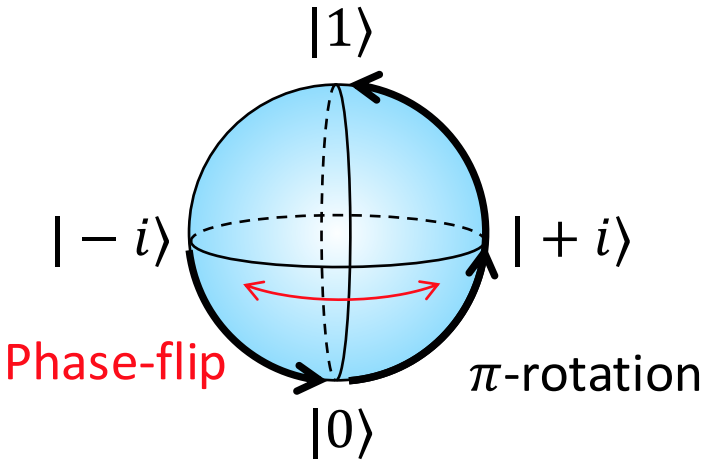
Noise-Depolarizing NOT gate





with phase-flip

X gate should convert $|0\rangle$ to $|1\rangle$



J. Guillaud and M. Mirrahimi Physical Review X 9, 10.1103(2019)
S. Puri et al., Science Advances 6, eaay5901 (2020)

Bias preserving gates with cat qubits: X gate

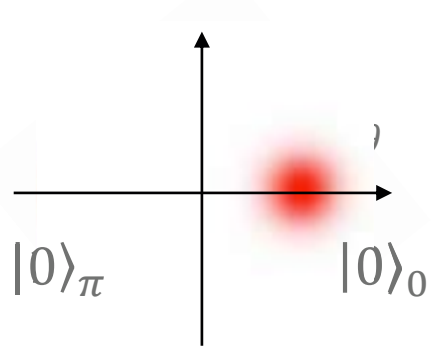
Some evolutions

Hadamard: H $ZH = HX$

NOT: X $ZX = X(-Z)$

actual NOT: $\sqrt{X}$ $\sqrt{X}$ $\sqrt{X}\,Z\,\sqrt{X} = XY$

Bias preserving NOT gate (beyond 2 levels)



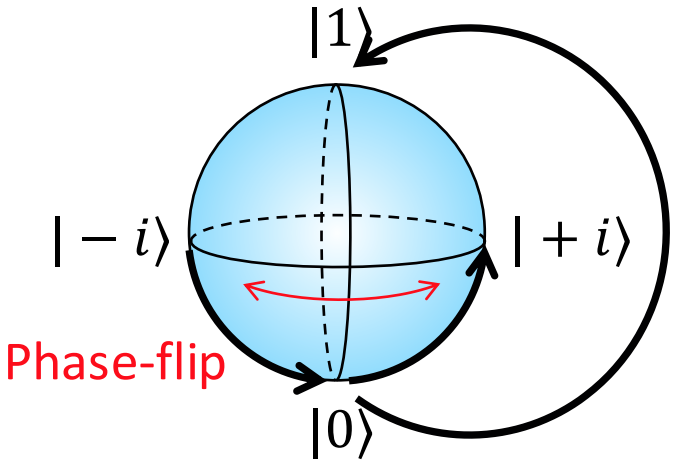
Code deformation : $\{|0\rangle, |1\rangle\}_\theta$

$|0\rangle_0 \rightarrow |0\rangle_\theta \rightarrow |0\rangle_\pi = |1\rangle_0 = X|0\rangle_0$

Adiabatic limit for high fidelity:

$\kappa_2 \gg \dot{\theta} \gg \kappa_1$

X gate should convert $|0\rangle$ to $|1\rangle$



- Qubit, stable (rare bit-flips)
  coherent (rare phase-flips)
- Initialize and measure $|0/1\rangle$, $|+/-\rangle$
- Physical bias-preserving gates
- Logical universal set of gate

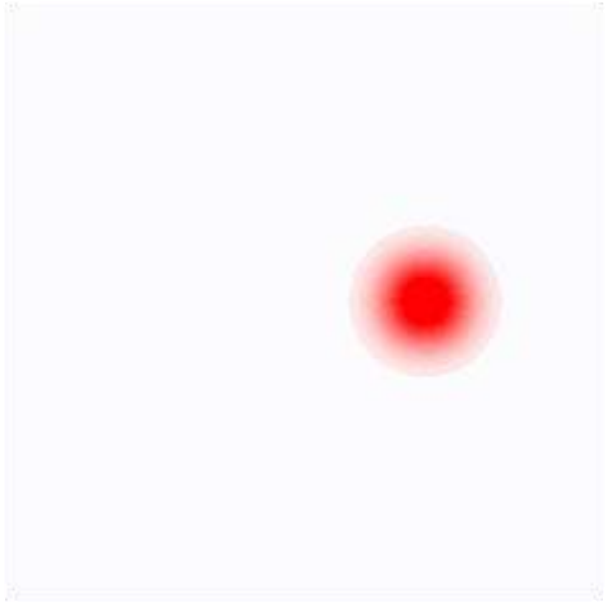
J. Guillaud and M. Mirrahimi Physical Review X 9, 10.1103(2019)

S. Puri et al., Science Advances 6, eaay5901 (2020)

Bias preserving gates with cat qubits: X gate

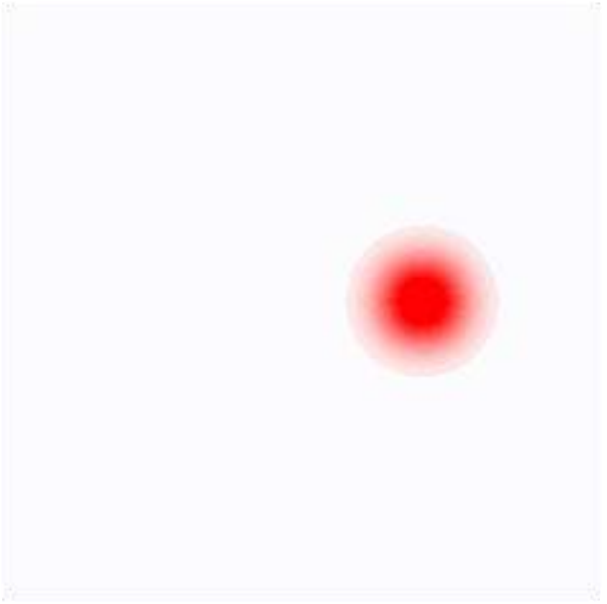
Dissipative X gate

$$\kappa_2 \mathcal{D}\left[a^2 - \left(\alpha e^{i\pi t/T}\right)^2\right]$$



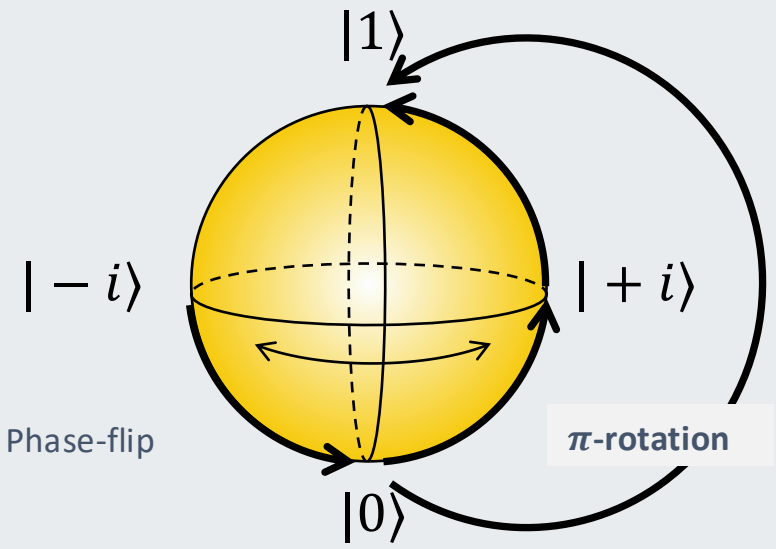
Dissipative + Hamiltonian X gate

$$\kappa_2 \mathcal{D}\left[a^2 - \left(\alpha e^{i\pi t/T}\right)^2\right] + \frac{\pi}{T} a^\dagger a$$

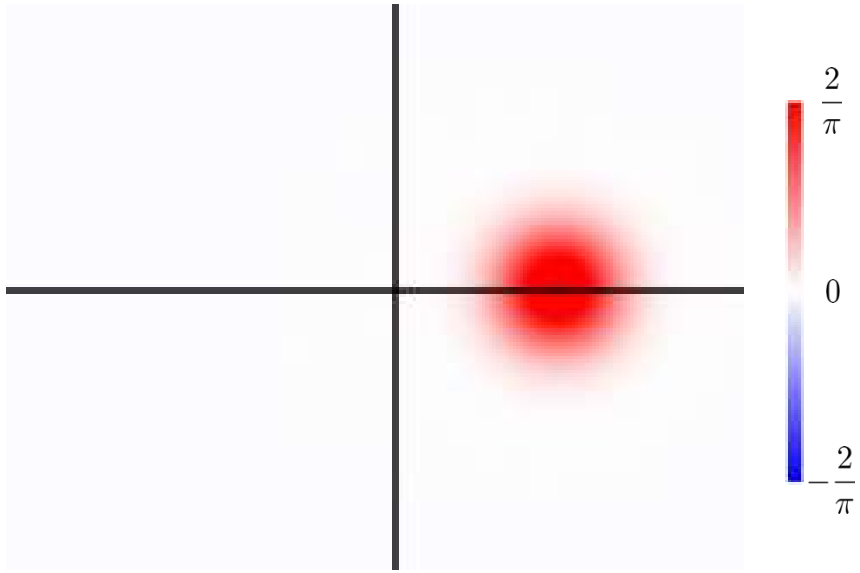


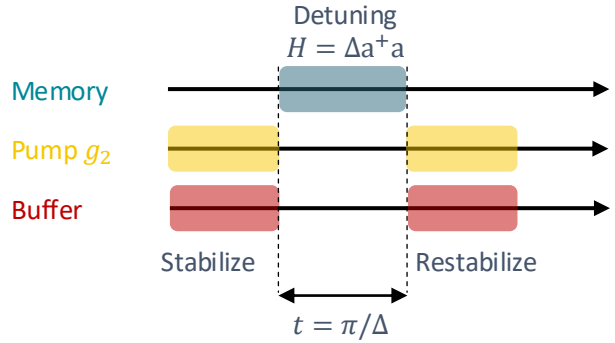
Bias preserving gates with cat qubits: X gate Hamiltonian protocol

X gate should convert $|0\rangle$ into $|1\rangle$



Passing through a “fragile” state converts a phase-flip into a bit-flip





Towards an experimental bias-preserving CNOT gate

Theory of the dissipative CNOT gate

$$\kappa_2\mathcal{D}[a_c^2-\alpha^2]+\kappa_2\mathcal{D}\left[a_t^2-\frac{\alpha}{2}(a_c+\alpha)+\frac{\alpha e^{\frac{2i\pi t}{T}}}{2}(a_c-\alpha)\right]+g_{\mathrm{CX}}\left(a_c+a_c^\dagger-2\alpha\right)\left(a_t^\dagger a_t-\alpha^2\right)$$

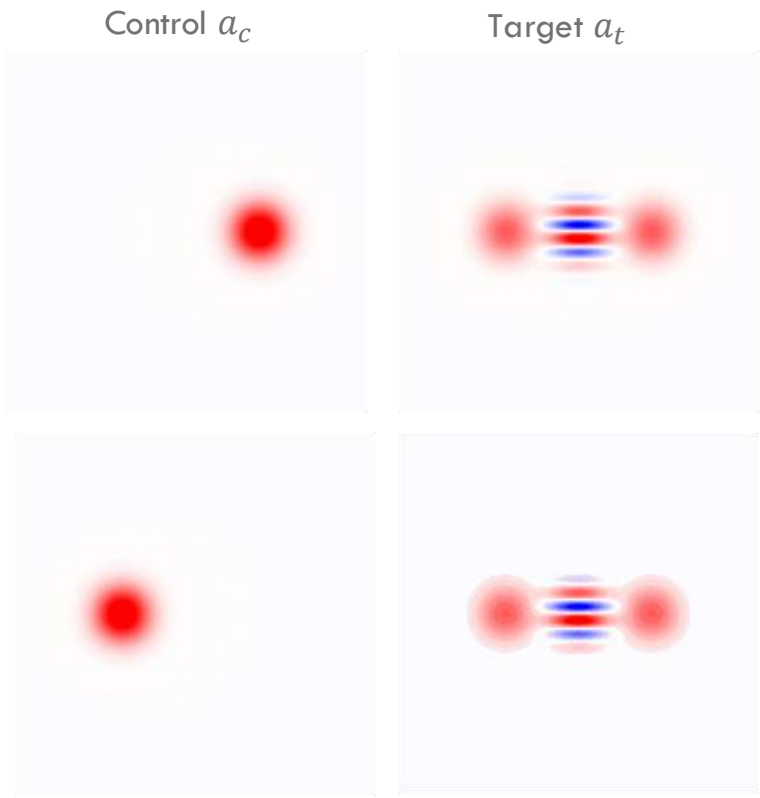
or $g_2(a_c^2-\alpha^2)\sigma_+ + h.c$

or $K(a_c^2-\alpha^2)^\dagger(a_c^2-\alpha^2)$

$$\kappa_2\mathcal{D}\left[a_t^2-\frac{\alpha}{2}(a_c+\alpha)+\frac{\alpha e^{\frac{i\pi t}{T}}}{2}(a_c-\alpha)\right]$$

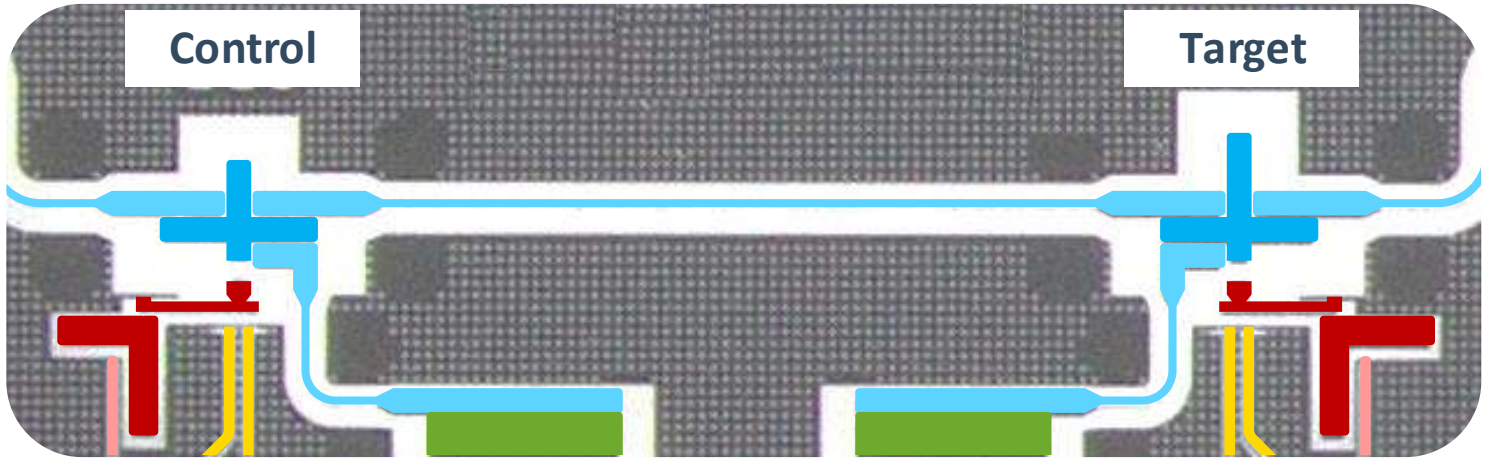
a_c in $|\alpha\rangle$ → $\kappa_2\mathcal{D}[a_t^2-\alpha^2]$

a_c in $|-\alpha\rangle$ → $\kappa_2\mathcal{D}\left[a_t^2-\left(\alpha e^{i\pi t/T}\right)^2\right]$



$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

CNOT scheme



Two-photon pump
at $\omega_p = 2\omega_a^{ctrl} - \omega_b^{ctrl}$

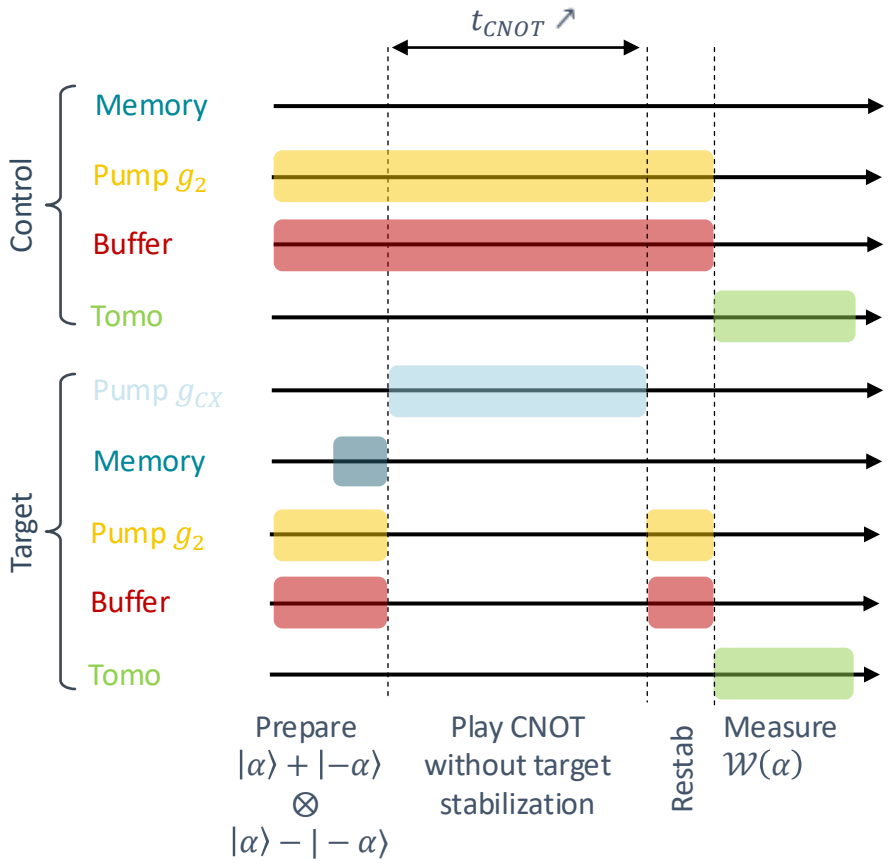
$\kappa_2 \mathcal{D}[a_c^2 - \alpha^2]$

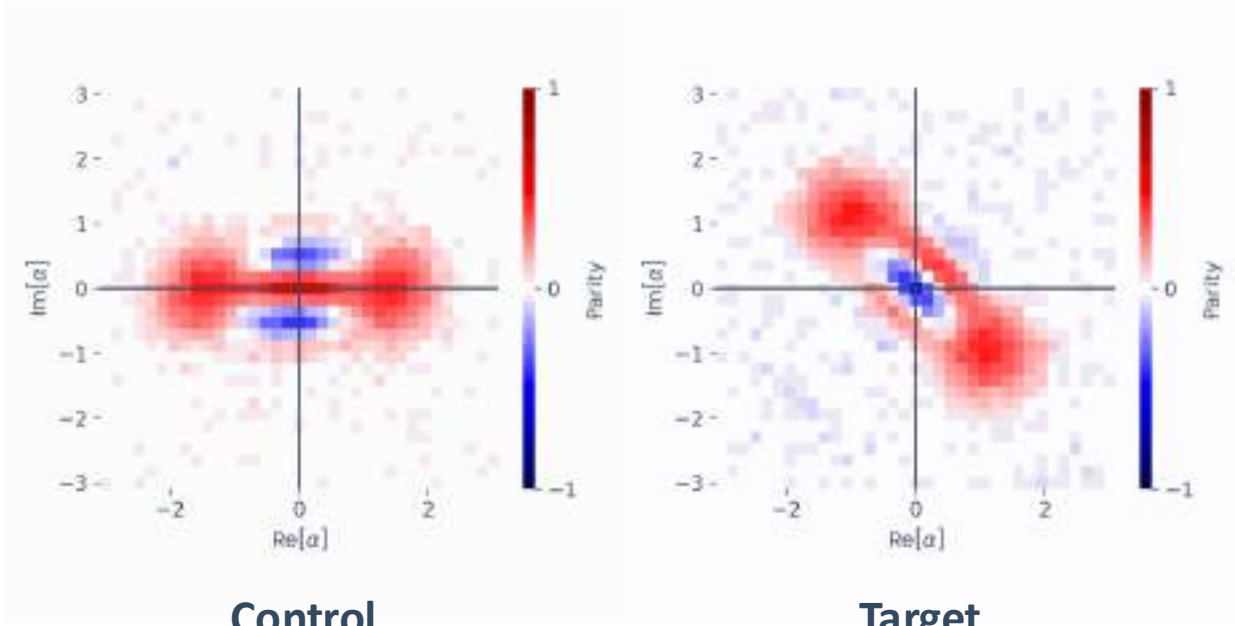
Longitudinal pump
at $\omega_p = \omega_a^{ctrl}$

Selects longitudinal coupling

$+g_{\mathrm{CX}}(a_c + a_c^\dagger - 2\alpha)(a_t^\dagger a_t - \alpha^2)$

CNOT at play





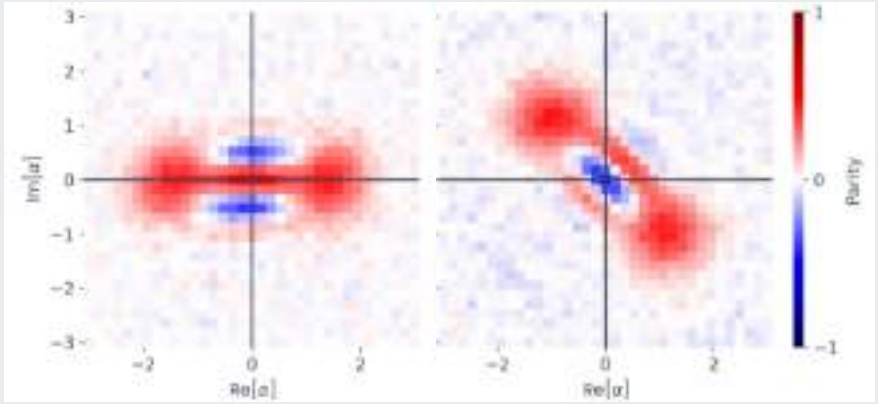
$g_{CX}/2\pi = 220$ kHz

$\alpha^2_{ctrl} = \alpha^2_{target} = 2$

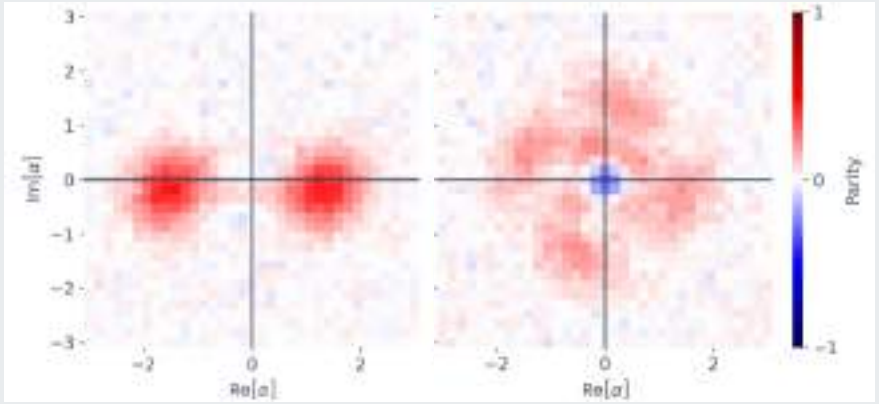
$T_{CX} = \pi/4\alpha g_{CX} = 400$ ns

CNOT dynamics (CNOT$|\pm -\rangle = |\mp -\rangle$)

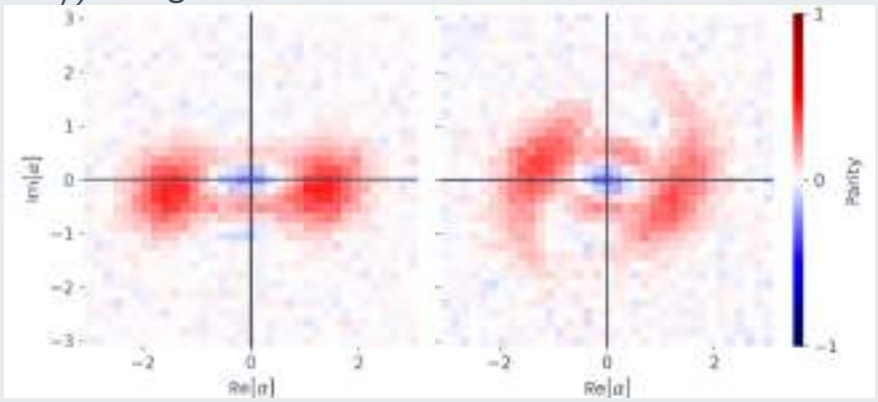
At start $(|\alpha\rangle + |-\alpha\rangle)\otimes(|\alpha\rangle - |-\alpha\rangle)$



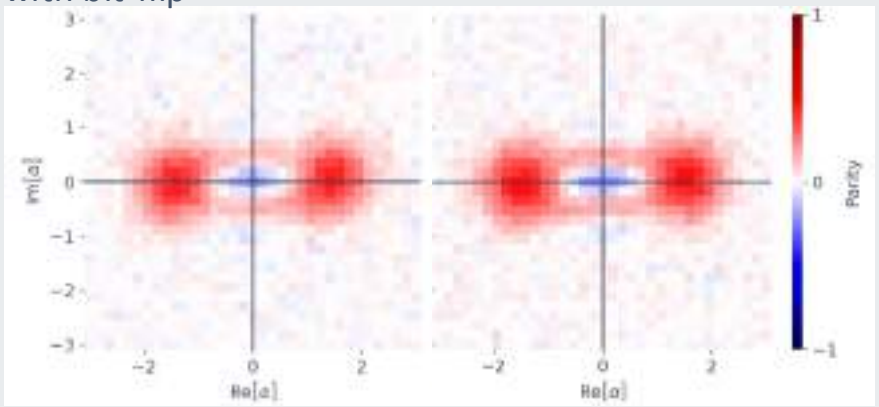
After ½ CNOT $|\alpha\rangle\otimes(|i\alpha\rangle - |-i\alpha\rangle) + |-\alpha\rangle\otimes(|\alpha\rangle - |-\alpha\rangle)$



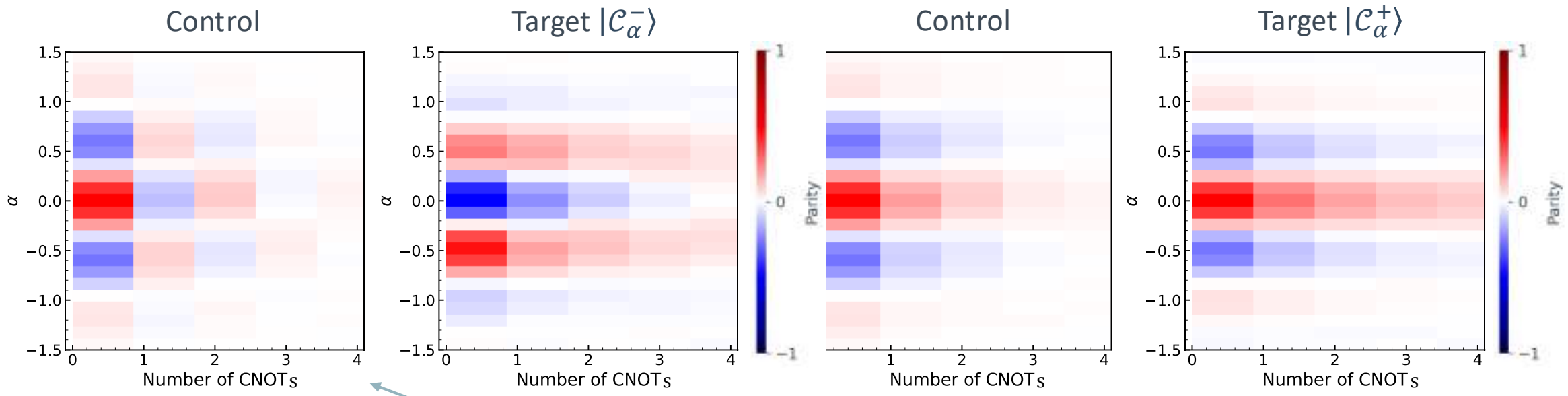
After full CNOT $(|\alpha\rangle - |-\alpha\rangle)\otimes(|\alpha\rangle - |-\alpha\rangle)$
with leakage



After re-stabilisation
with bit-flip $(|\alpha\rangle - |-\alpha\rangle)\otimes(|\alpha\rangle - |-\alpha\rangle)$



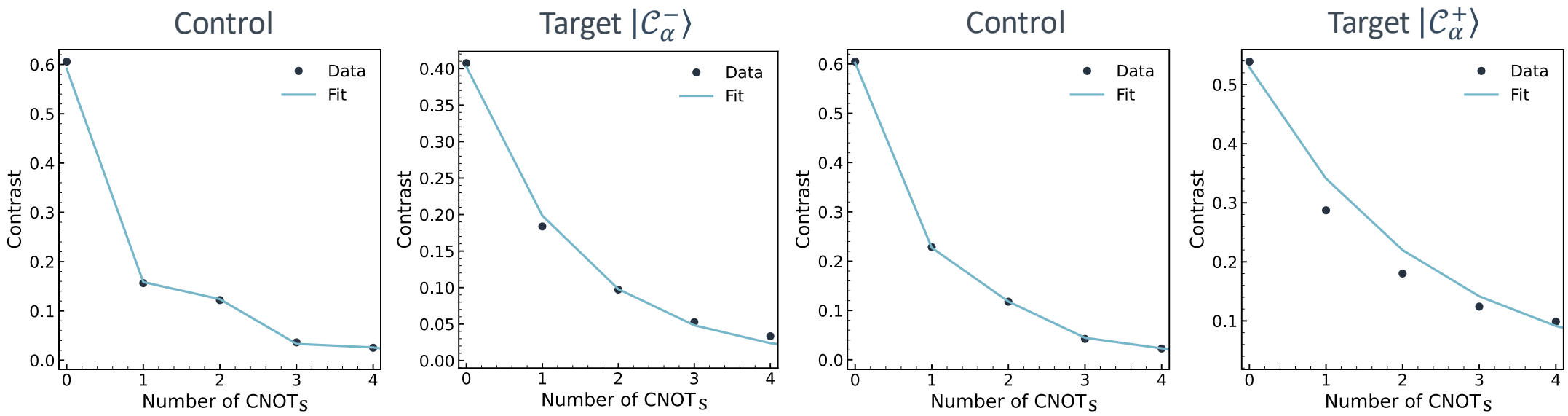
Characterizing phase-flips



Faster decay of control due to **propagation** of target phase-flips

Conditionnal flip of the control state $|\pm\rangle \rightarrow |\mp\rangle$ when target is in $|-\rangle$

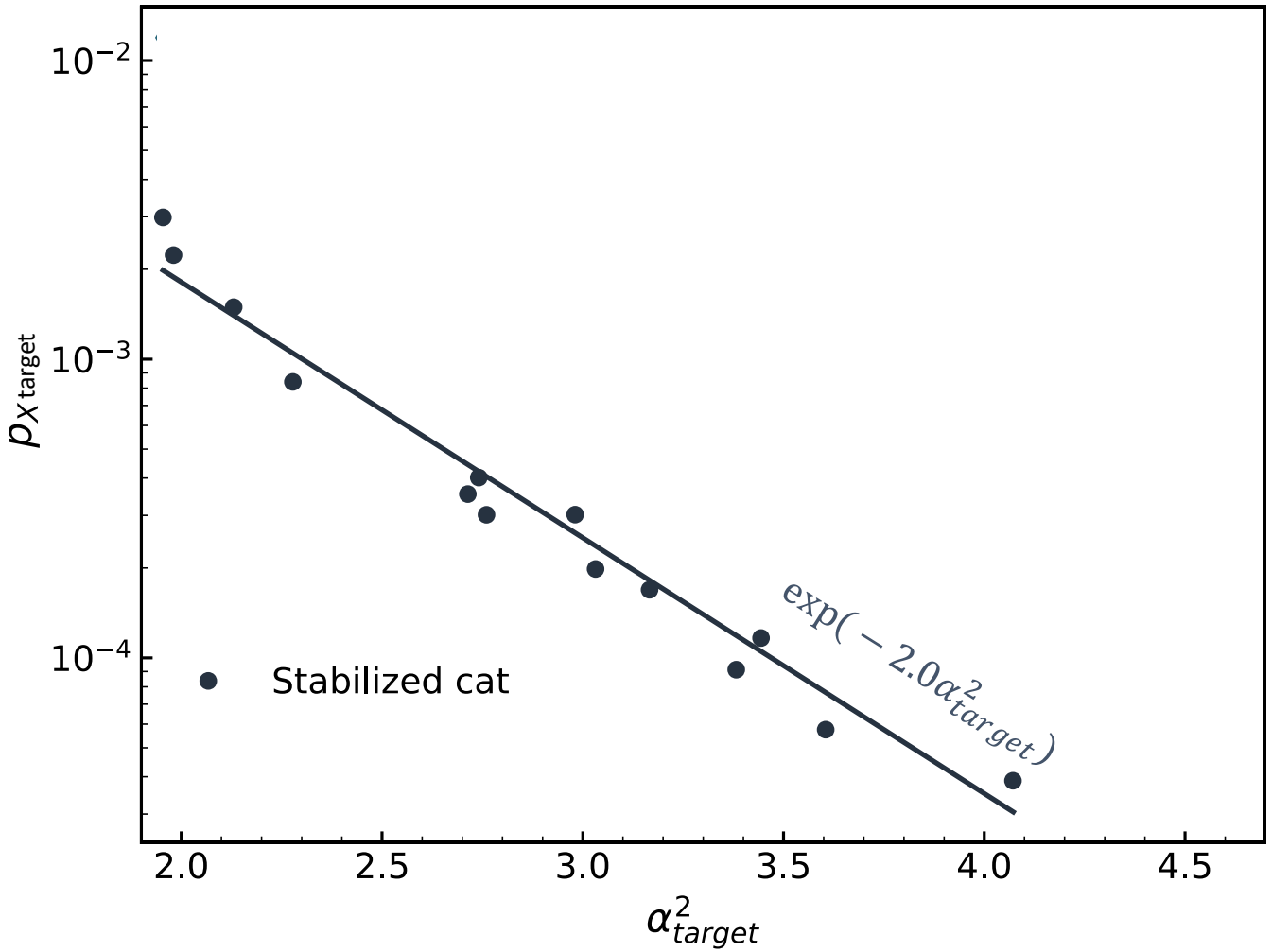
Characterizing phase-flips



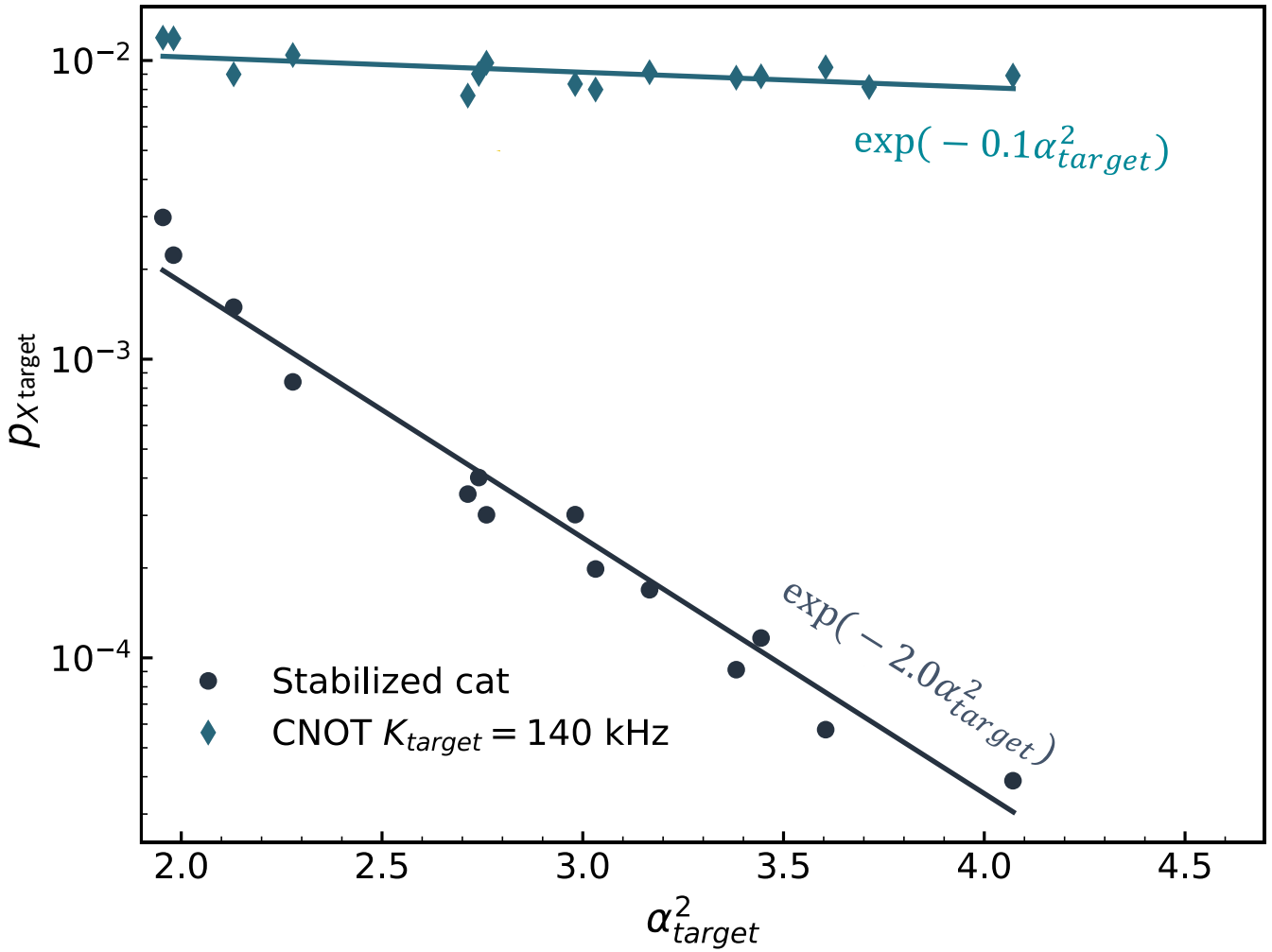
$$\begin{cases} C_t(k) = C_{t,SPAM} \times \left(C_{t,CNOT} \times C_{t,restab}\right)^k \\ C_c(k) = C_{c,SPAM} \times \left(C_{c,CNOT} \times C_{c,restab}\right)^k \times C_{t,CNOT}^{k/2} \times C_{t,restab}^{\lfloor k/2 \rfloor} \times C_{t,prep}^{k\%2} \end{cases}$$

$p_{ZA}^{CNOT} \approx 0.15 \quad p_{ZD}^{CNOT} \approx 0.15$ → 200% of threshold error budget

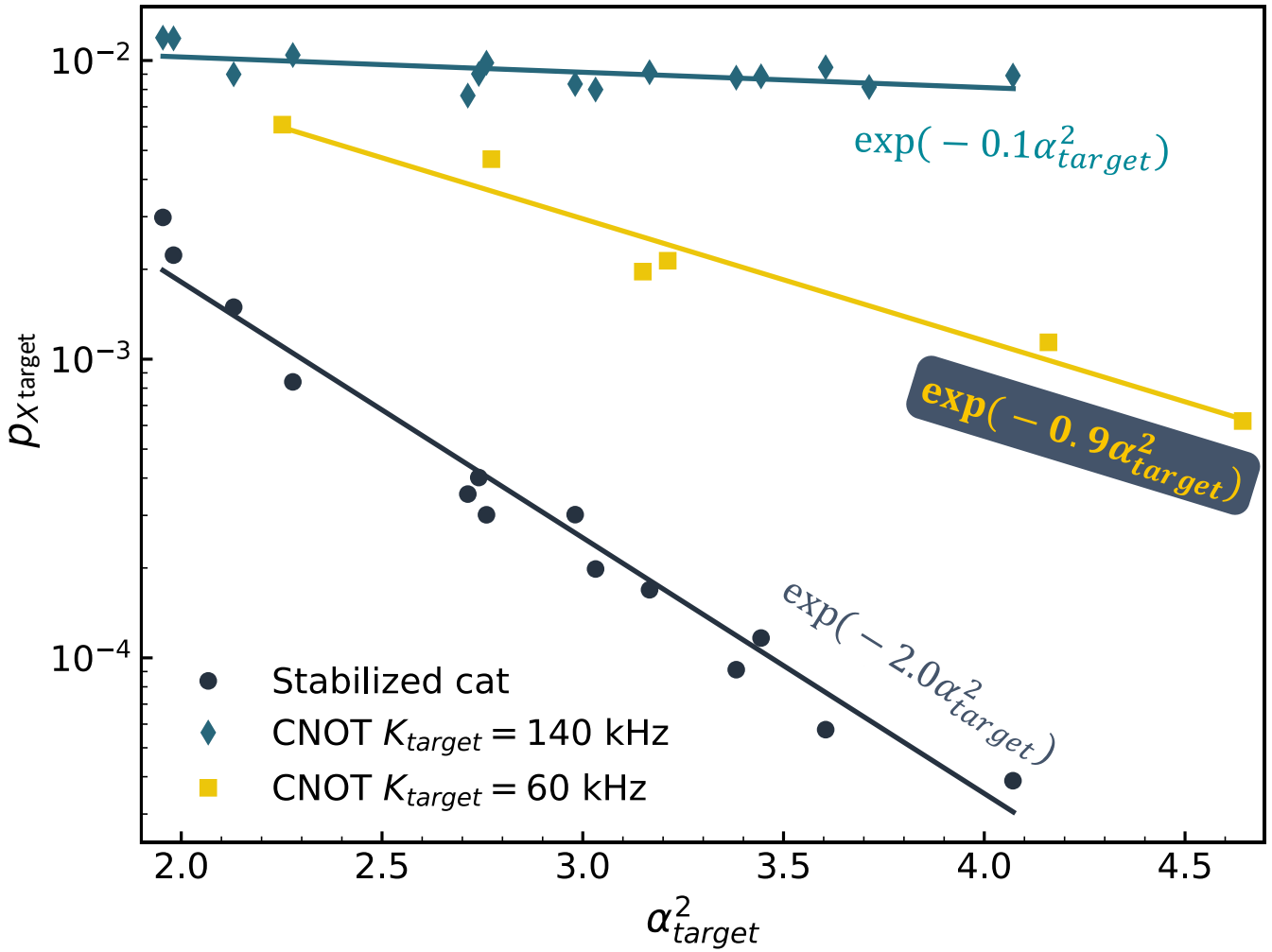
Characterizing bit-flips



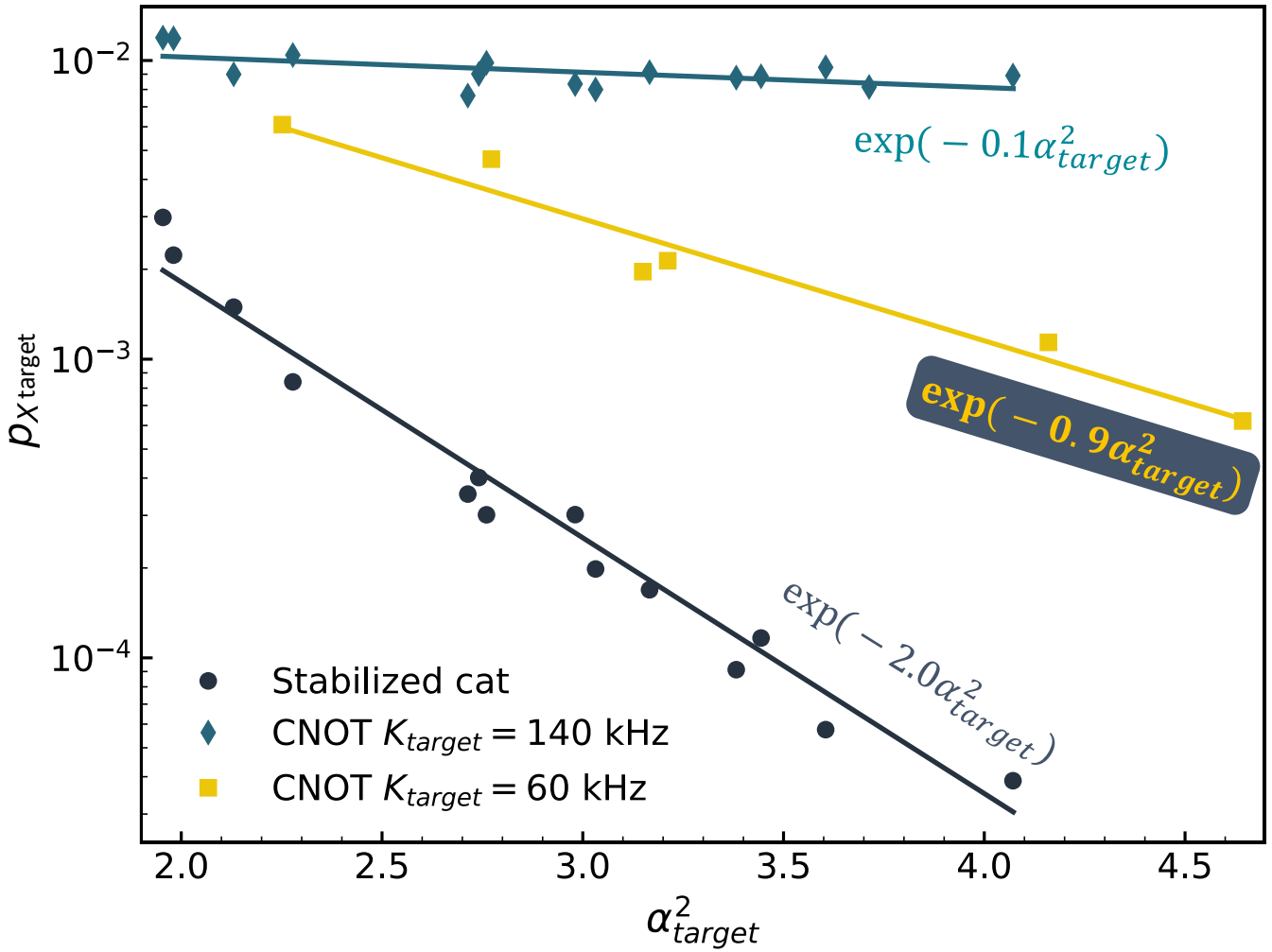
Characterizing bit-flips



Characterizing bit-flips



Characterizing bit-flips



Bit-flip scaling of the target is **limited by leakage** while the stabilization is turned off

Solutions

- Further reduce Kerr (and dephasing)*
- Engineer **conditional** rotation of the two-photon dissipation on the target

Guillaud & Mirrahimi, PRX 9, 041053 (2019)

*H. Putterman et al, arxiv:2409.17556

04

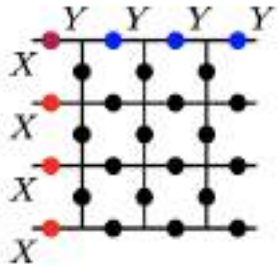
Logical qubits and gates

Repetition-cat architecture

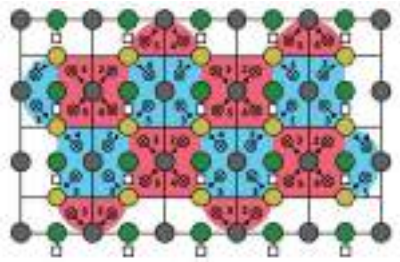
Fully protected logical qubit?

Include some bit-flip error correction capability ? → bias-tailored codes

D. Tuckett *et al,* PRL 120,0505 5 (2018)



C. Chamberland *et al,*
PRX Quantum 3, 010329 (2022)

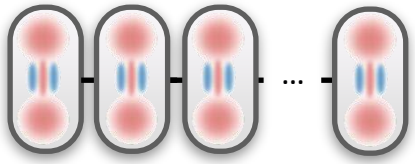


J. Pablo Bonilla Ataides *et al,*
Nature Com. 12, 2171 (2021)



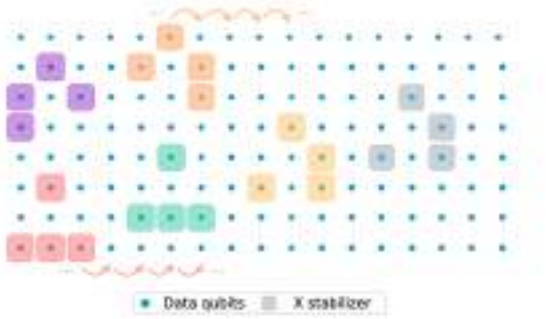
$\overline{n} = |\alpha|^2$ **large enough to handle bit-flips alone ?** → phase-flip codes (« classical » codes)

JG and M. Mirrahimi, Phys. Rev. X 9, 041053 (2019)
C. Chamberland et al, PRX Quantum 3, 010329 (2022)



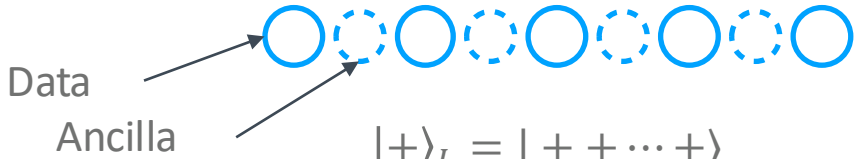
H. Putterman et al, arxiv:2409.13025

D. Ruiz *et al,* arxiv:2401.09541



Phase-flip correction

1D repetition code with n cat-qubits

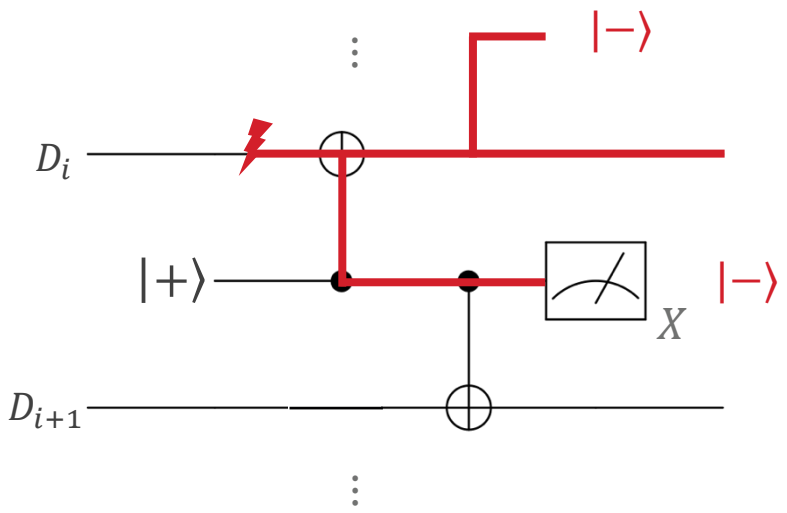


$$|+\rangle_L = |++\cdots+\rangle$$
$$|-\rangle_L = |--\cdots-\rangle$$

$$Z_L : |++\cdots+\rangle \to |--\cdots-\rangle = \otimes_i Z_i$$

$$X_L : \frac{|++\cdots+\rangle + |--\cdots-\rangle}{\sqrt{2}} \to \frac{|++\cdots+\rangle - |--\cdots-\rangle}{\sqrt{2}}$$
$$= \text{any } X_i$$

Stabilizer : X_iX_{i+1} measured using b.p. CX gates



- Qubit, stable (rare bit-flips)
  coherent (rare phase-flips)
- Initialize and measure $|0/1\rangle$, $|+/-\rangle$
- Physical bias-preserving gates
- Logical universal set of gate

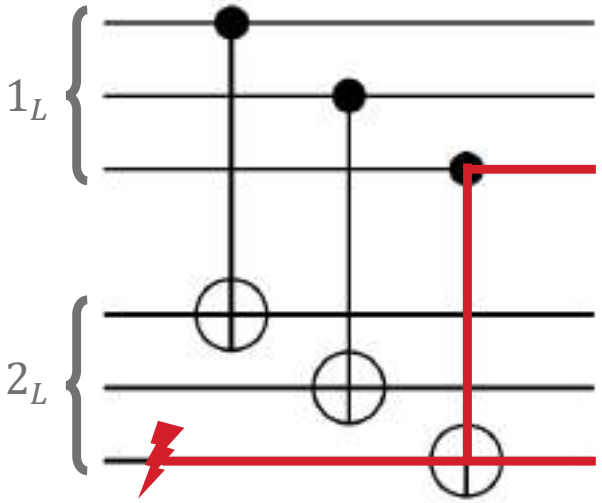
} Logical qubit in **1D** array
Bacon-Shor like

$P_{bf} \propto e^{-\alpha^2}$	$P_{bf} \propto n$
$P_{pf} \propto \alpha^2$	$P_{pf} \propto e^{-n}$
Auto. EC	1D ECC

Logical gates

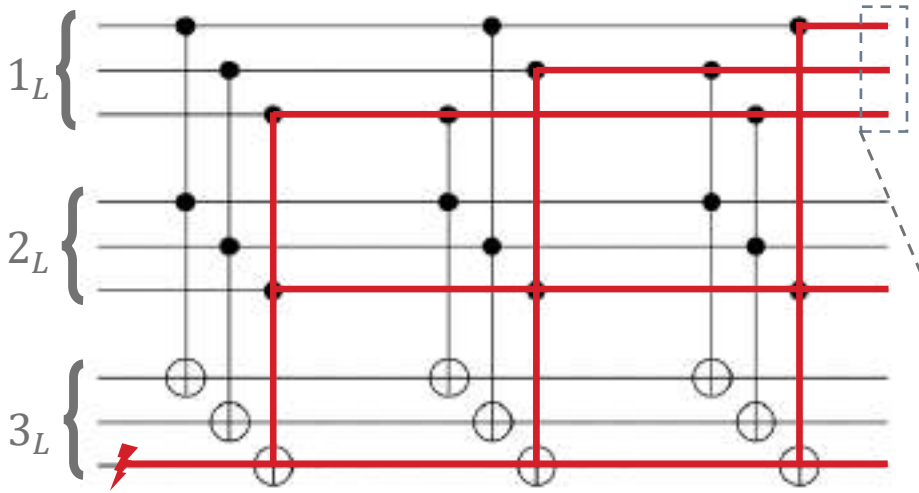
$Z_L = \bigotimes_i Z_i$ and $X_L = X_i$

CNOT gate



$CX \propto (I_1 + Z_1)I_2 + (I_1 - Z_1)X_2$

Toffoli gate



$$CCX \propto (I_1 + Z_1)(I_1 + Z_2)I_3 + (I_1 + Z_1)(I_1 - Z_2)I_3 + (I_1 - Z_1)(I_1 + Z_2)I_3 + (I_1 - Z_1)(I_1 - Z_2)X_3$$

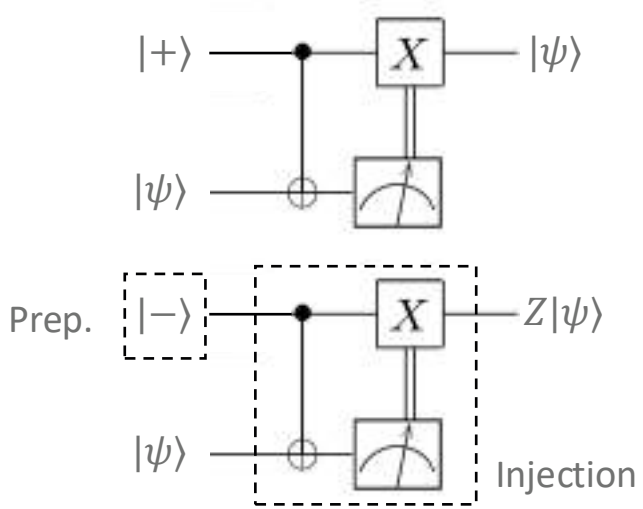


Not Fault-Tolerant

Eastin–Knill theorem : “no quantum error correcting code can transversely implement a universal gate set”

Gate teleportation

Simple/gate teleportation

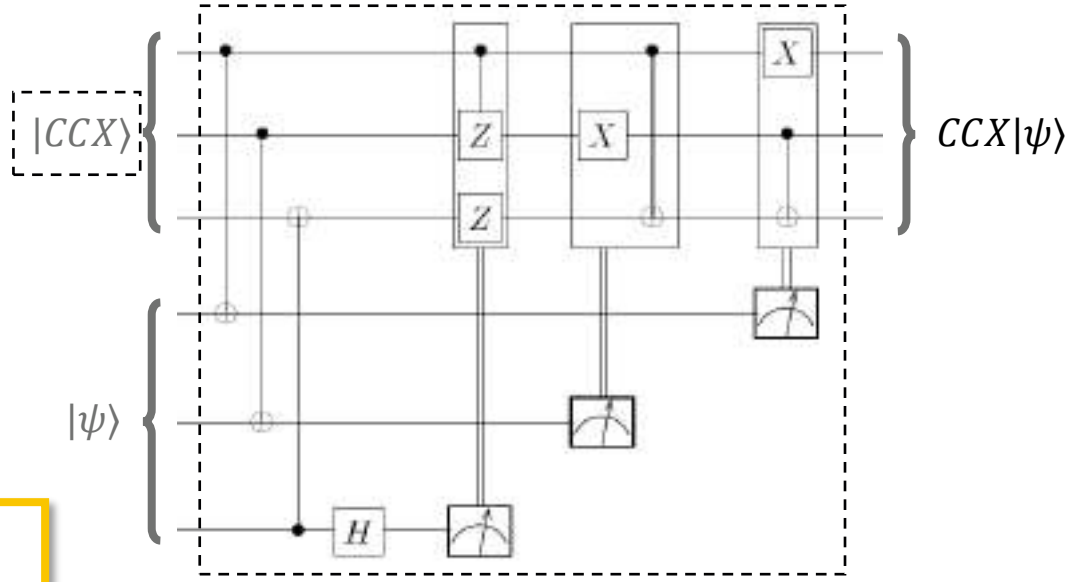


- Qubit, stable (rare bit-flips)
  coherent (rare phase-flips)
- Initialize and measure $|0/1\rangle$, $|+/-\rangle$
- Physical bias-preserving gates
- Logical universal set of gate

Toffoli teleportation

$|CCX\rangle = (|000\rangle + |100\rangle + |010\rangle + |111\rangle)/2$

Fault-tolerant preparation using measurement

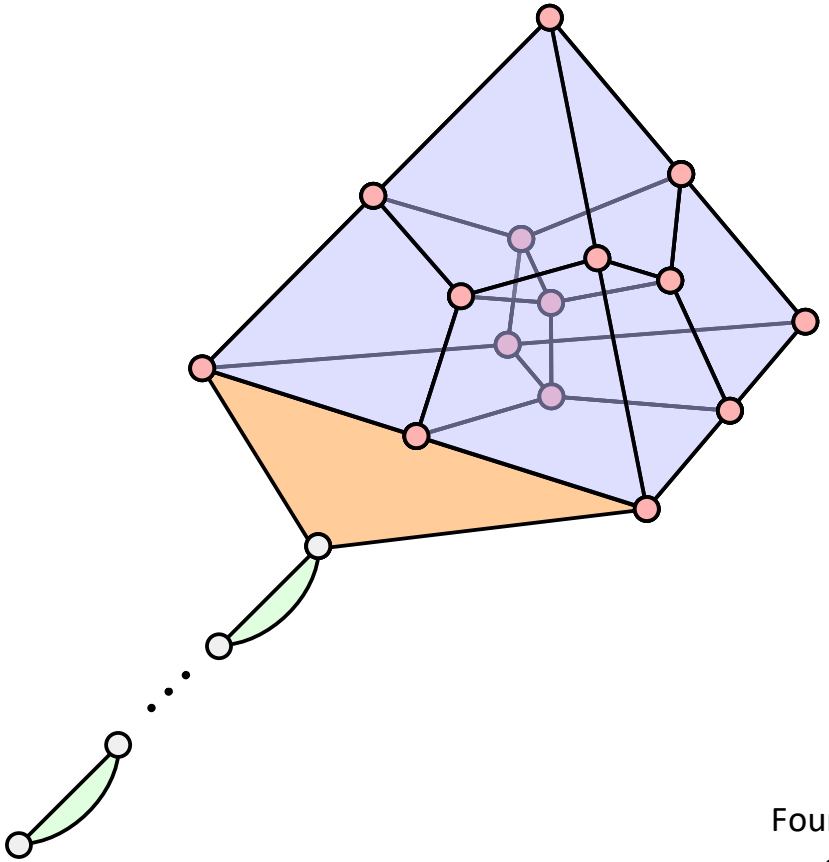


D. Gottesman et al, Nature 402, 390–393 (1999)

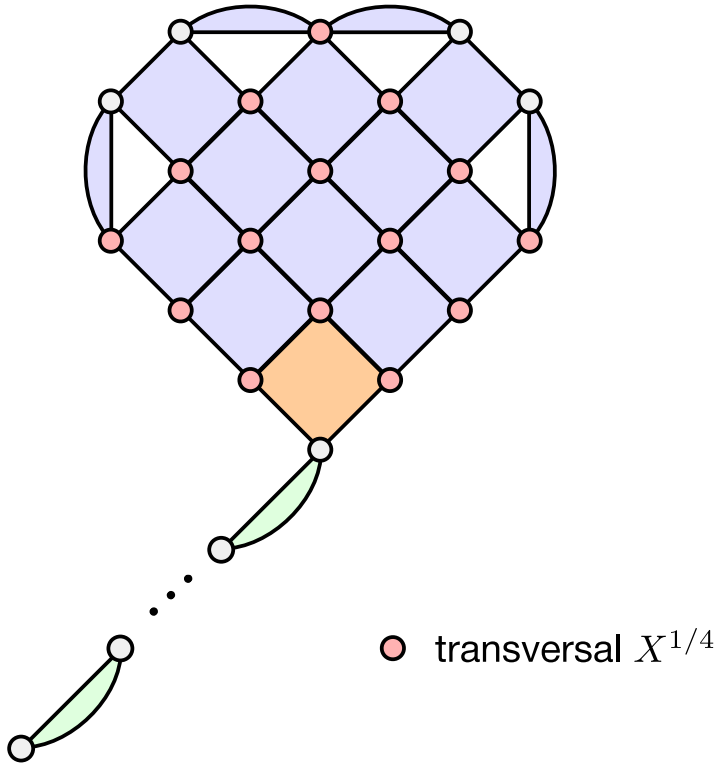
Unfolded distillation

Biased-noise qubit reduce the spatial dimension

➢ distillation at the physical level



unfolding

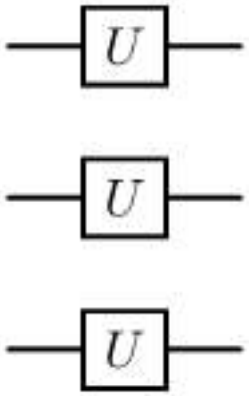


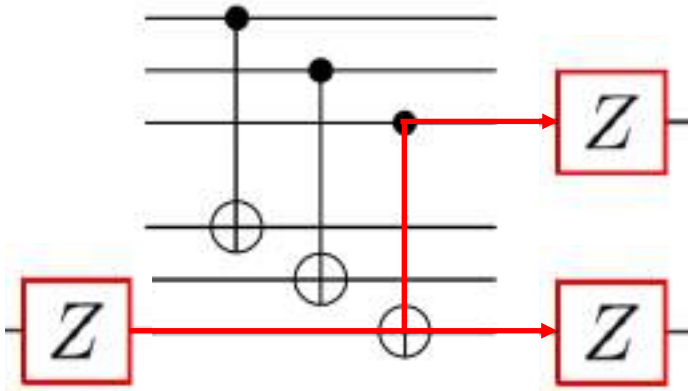
Found with the SAT solver *kissat*

Ruiz et al, arXiv:2507.12511, 2025

Fault-tolerant tranversal gates

Transversal gates





Eastin-Knill

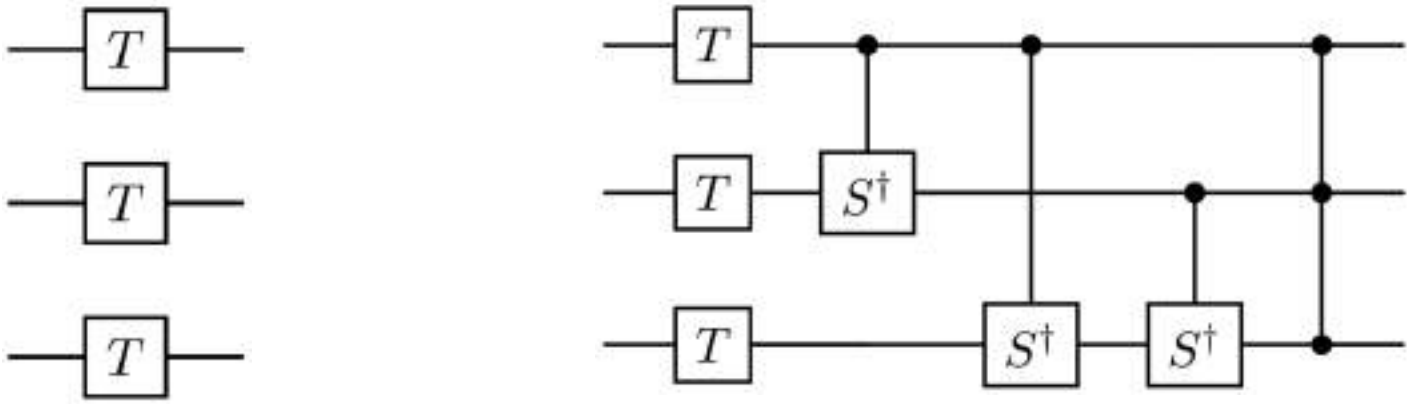
Restrictions on Transversal Encoded Quantum Gate Sets

Bryan Eastin* and Emanuel Knill
National Institute of Standards and Technology, Boulder, Colorado 80305, USA
(Received 28 November 2008; published 18 March 2009)

Here we show that the ability of a quantum code to detect an arbitrary error on any single physical subsystem is incompatible with the existence of a universal, transversal encoded gate set for the code.

Example with the repetition code:

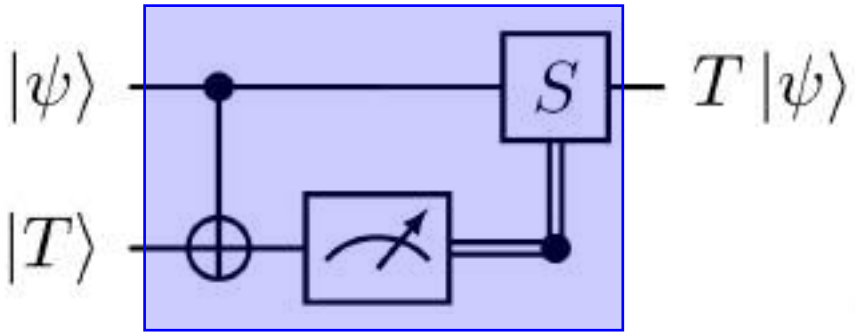
$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$



Credit: Elie Gouzien

Teleporting a T gate

teleportation circuit



$$|T\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$$

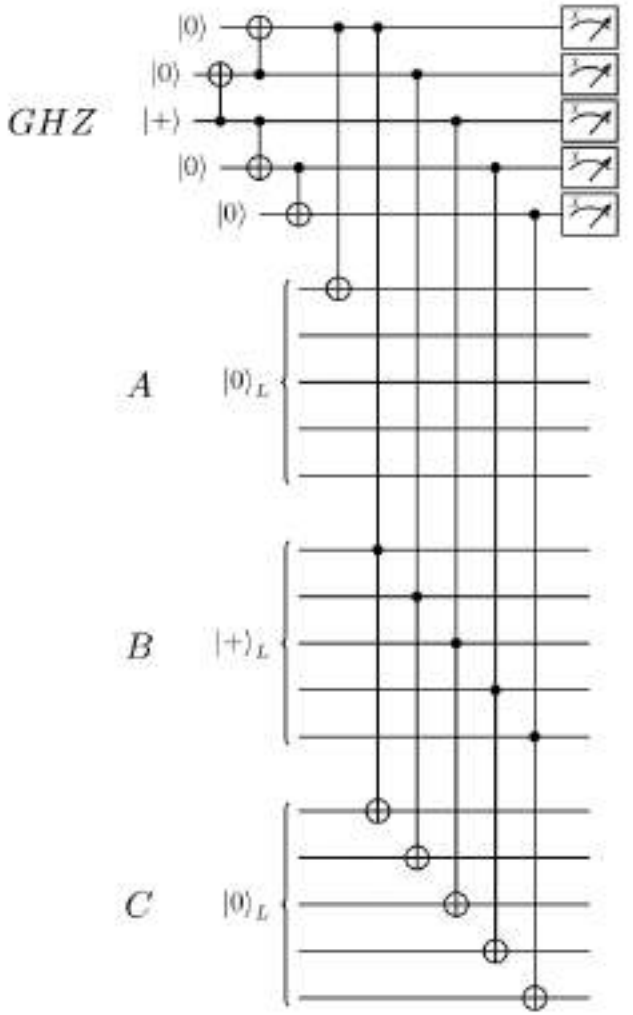
Previous state of the art

Toffoli gate:

- Piecable fault-tolerance Guillaud *et al*, Phys. Rev. X 9 (2019)
- Clifford measurement Chamberland *et al*, PRX Quantum 3 (2022)
- Improved Clifford measurement
  Gouzien *et al*, Phys. Rev. Lett. 131, (2023)

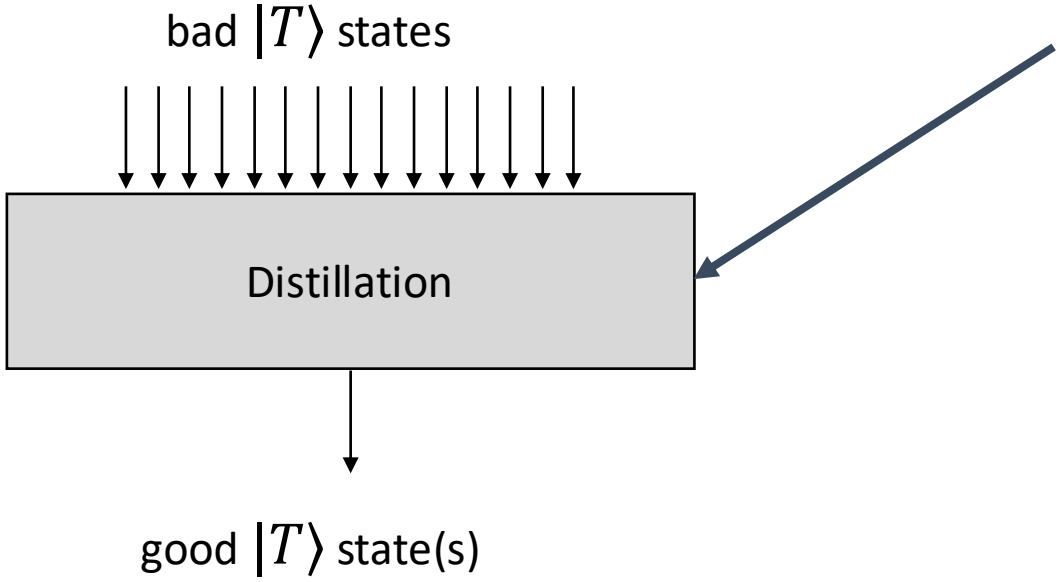
Performance:

To have a 10^{-7} logical error rate,
You need 46 physical qubits
You need ~10 cycles of error correction
~~Acceptance at 0.1% - 5% ($\frac{\kappa_1}{\kappa_2} = 10^{-4} - 10^{-5}$)~~



Distillation

Distillation:



Logical qubits and operations at the logical level

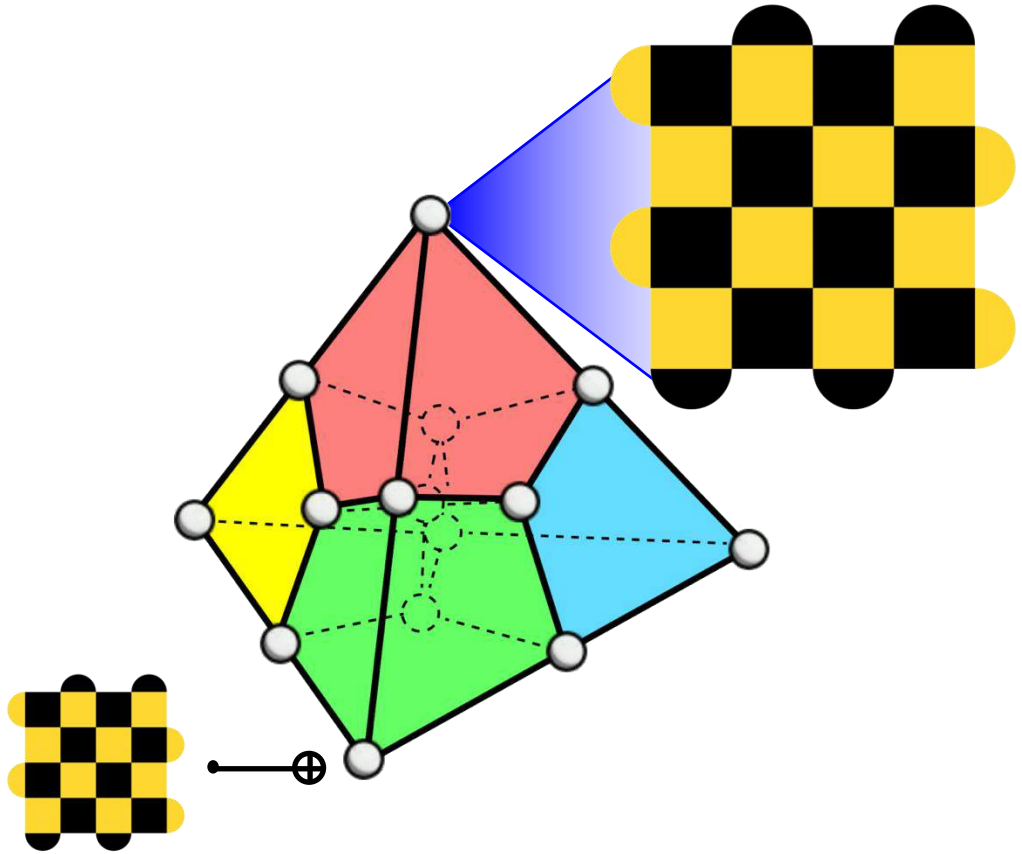
Noise bias enables:

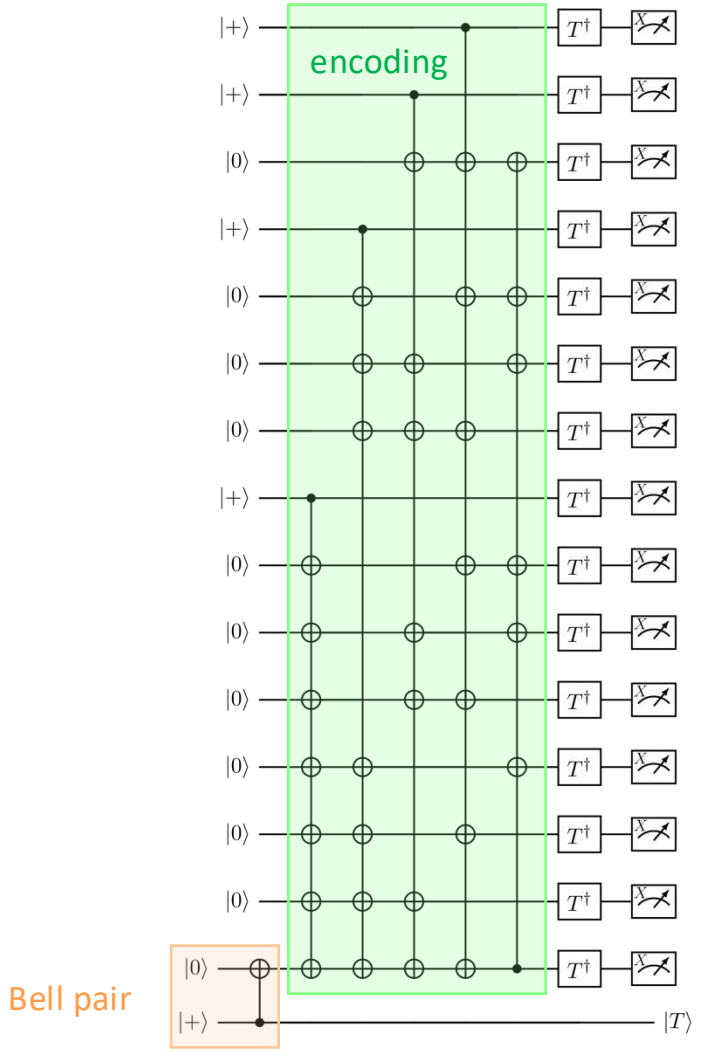
- To perform distillation at physical level (using LDPC codes)

➢ Reduce the space cost

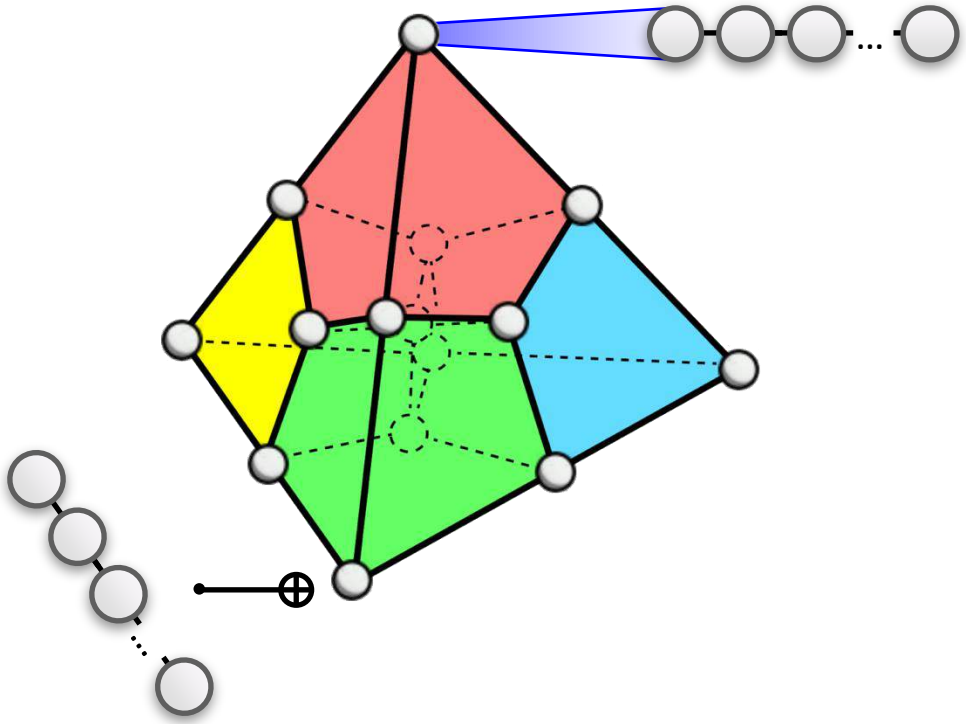
➢ Reduce the time cost

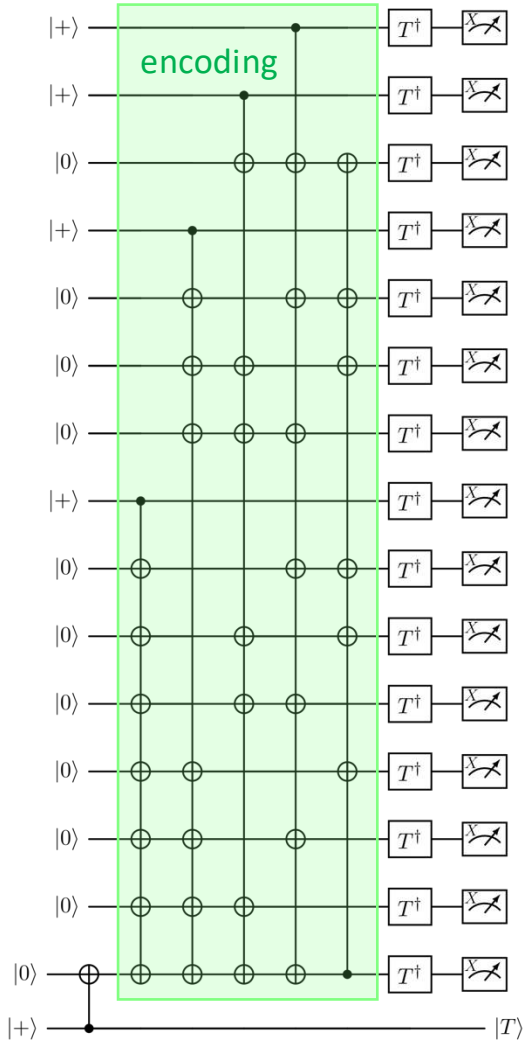
Distillation





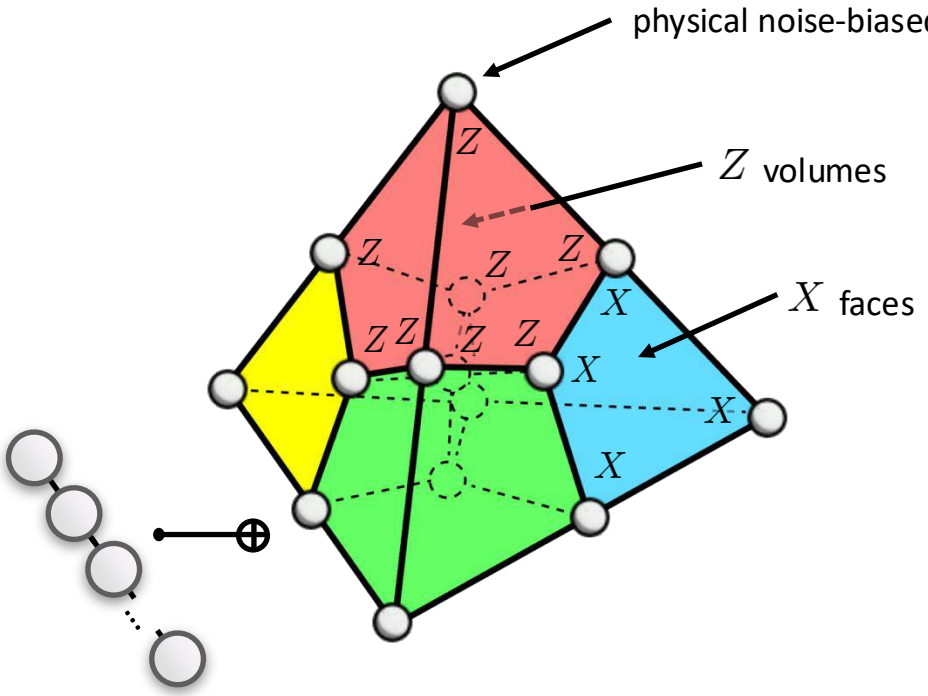
Distillation in 3D

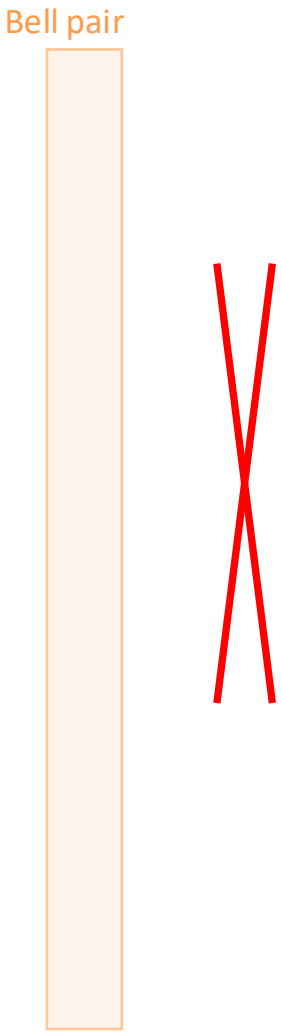




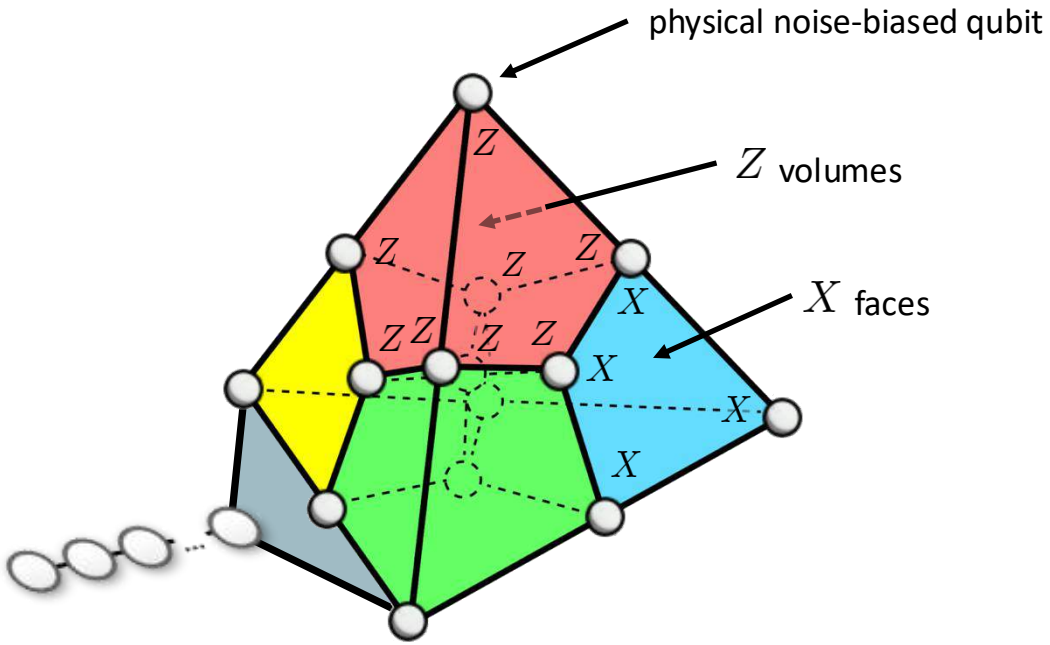
Bell pair

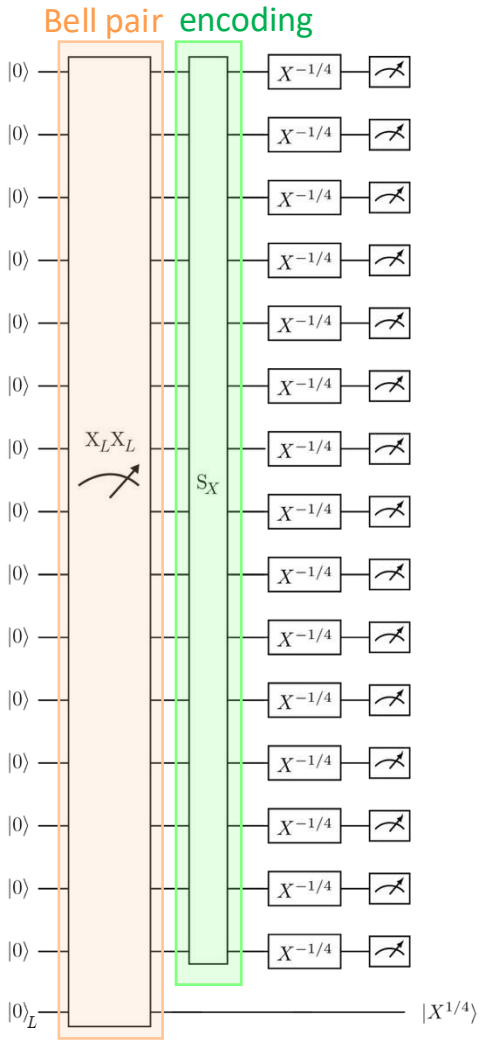
Distillation in 3D



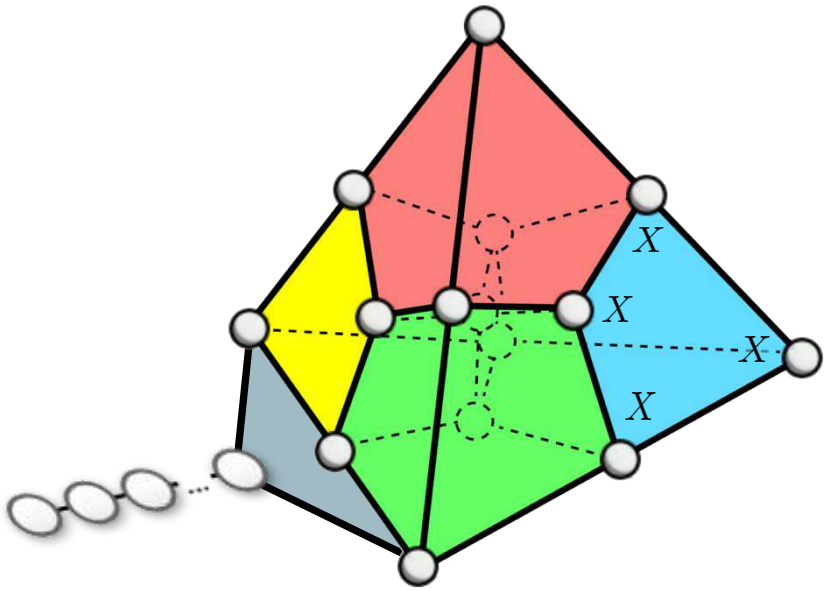


Distillation in 3D





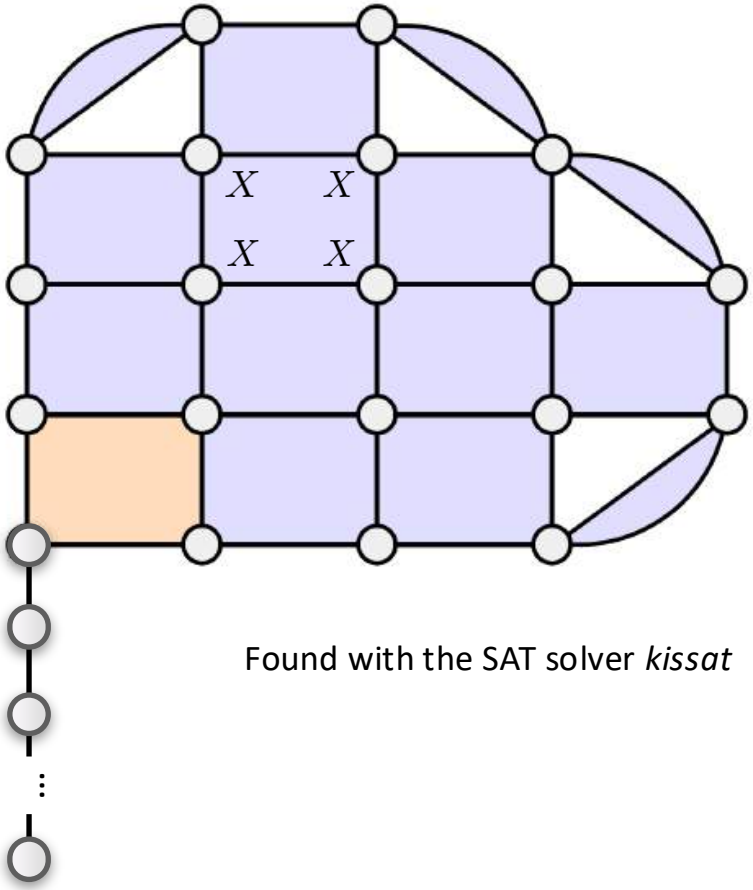
Unfolded distillation



unfolding

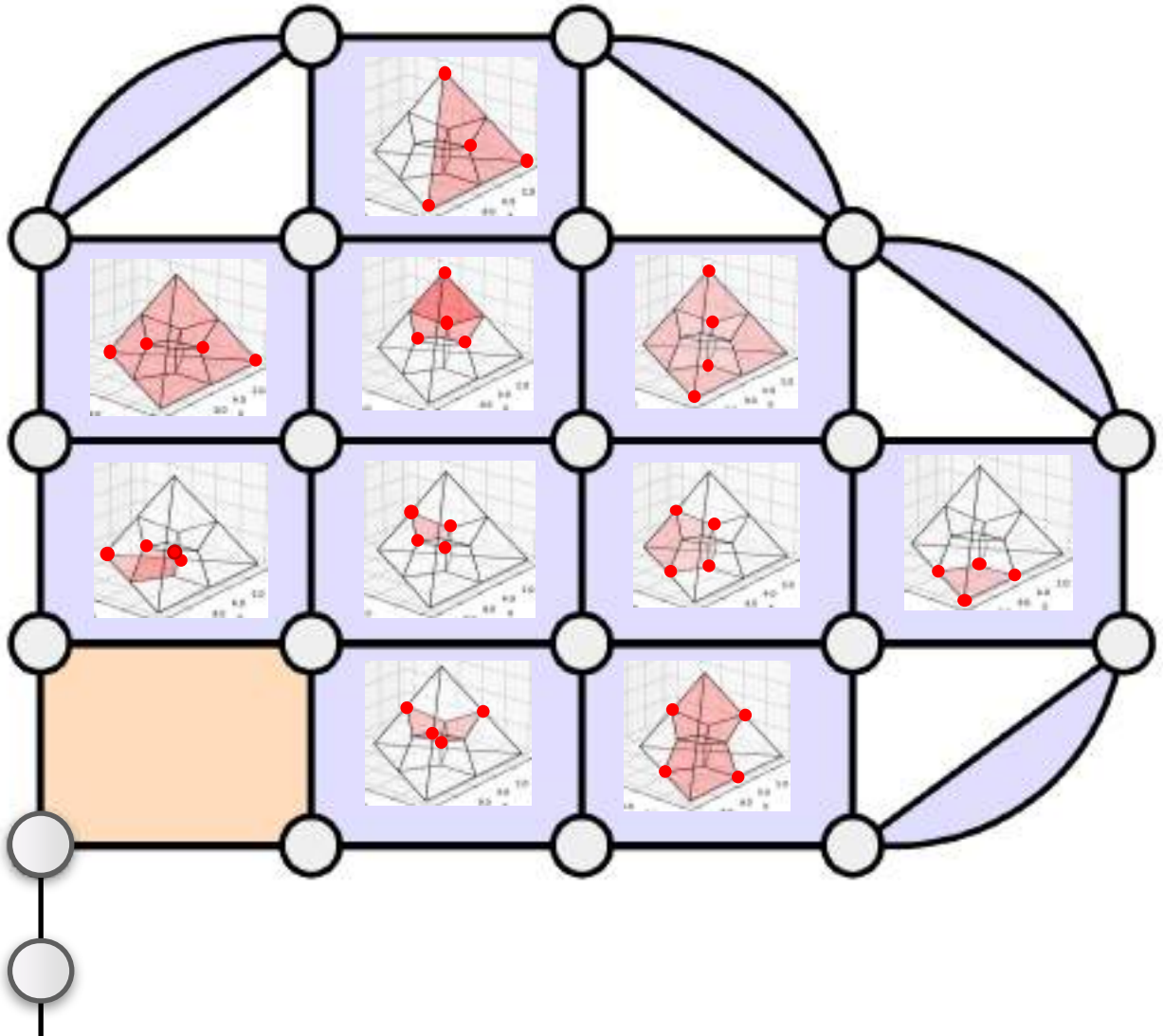
Biased-noise qubit reduce the spatial dimension

- distillation at the physical level

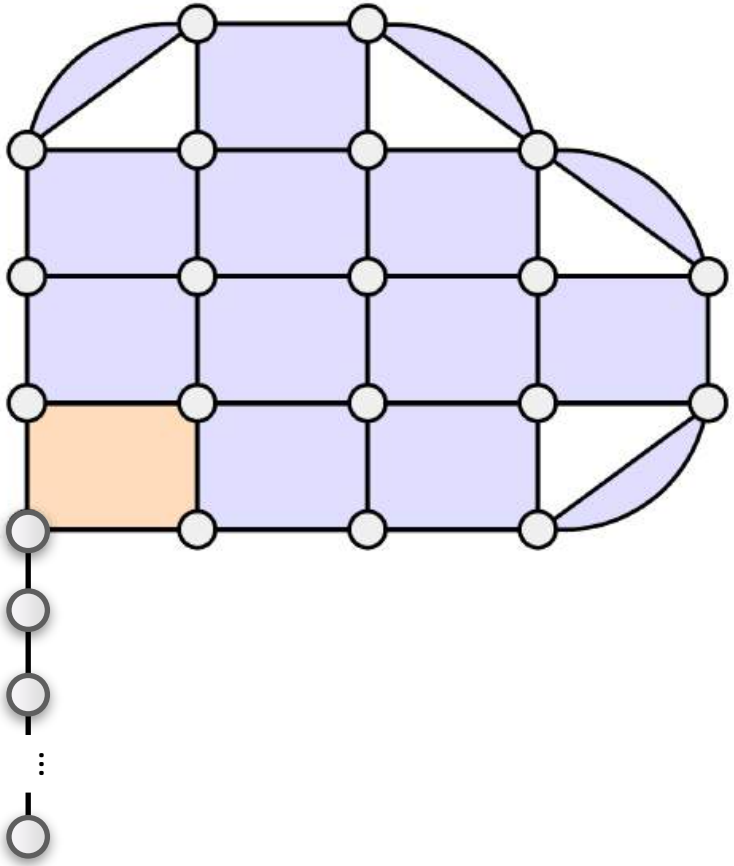


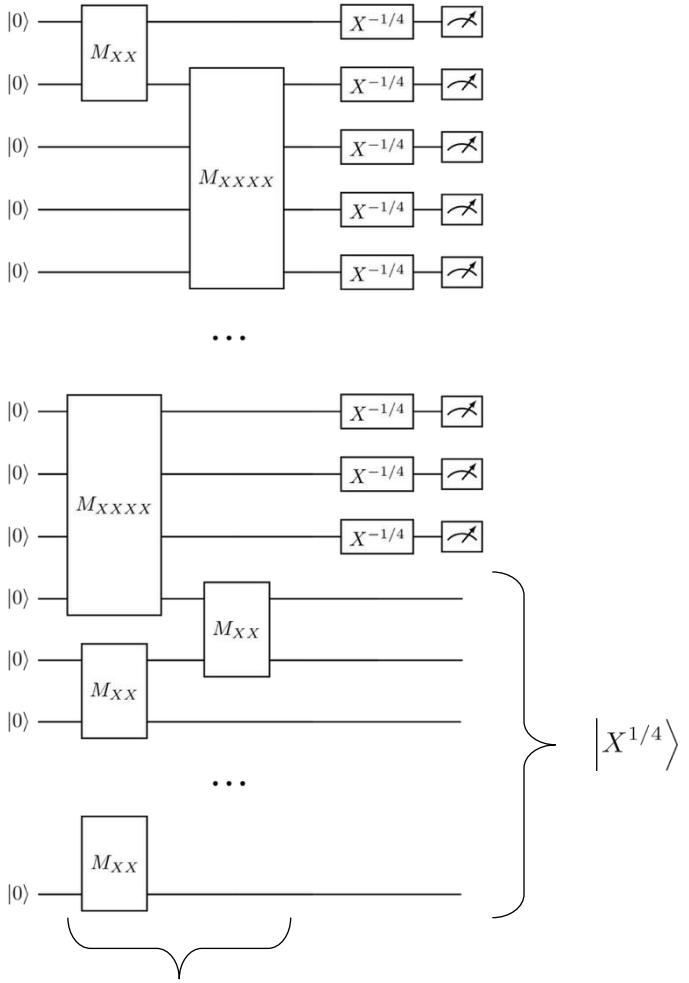
Found with the SAT solver *kissat*

Unfolding



Distillation factory





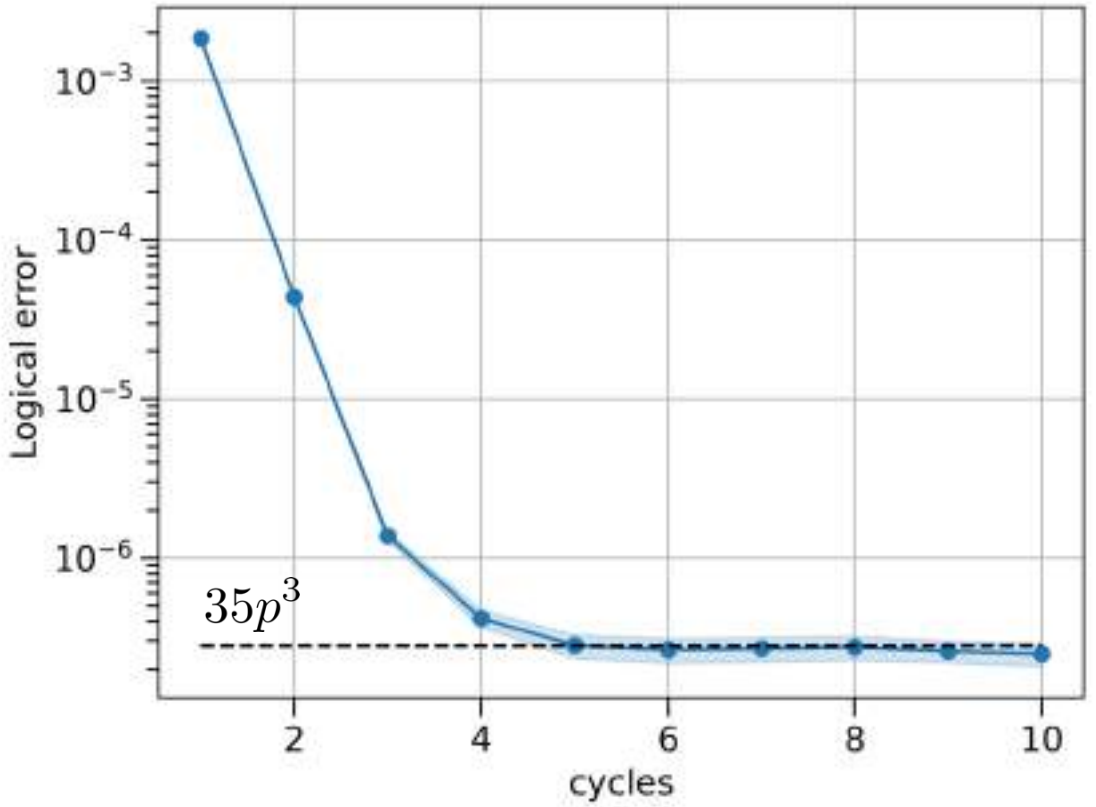
Multiple cycles

Numerical results

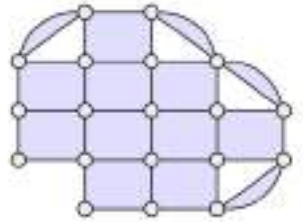
Gidney, Quantum 5, 497, 2021

Roffe, PRR 2, 043423, 2020

Depolarizing noise $p_Z = 10^{-3}$



STIM + BPOSD

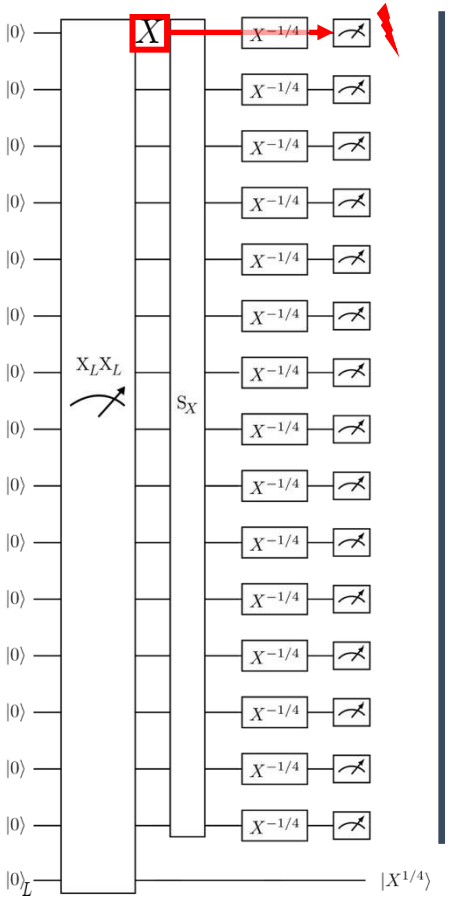


57 qubits

5.3 cycles (including post-selection)

$p_X = 0?$

Maximum bit-flip tolerable?

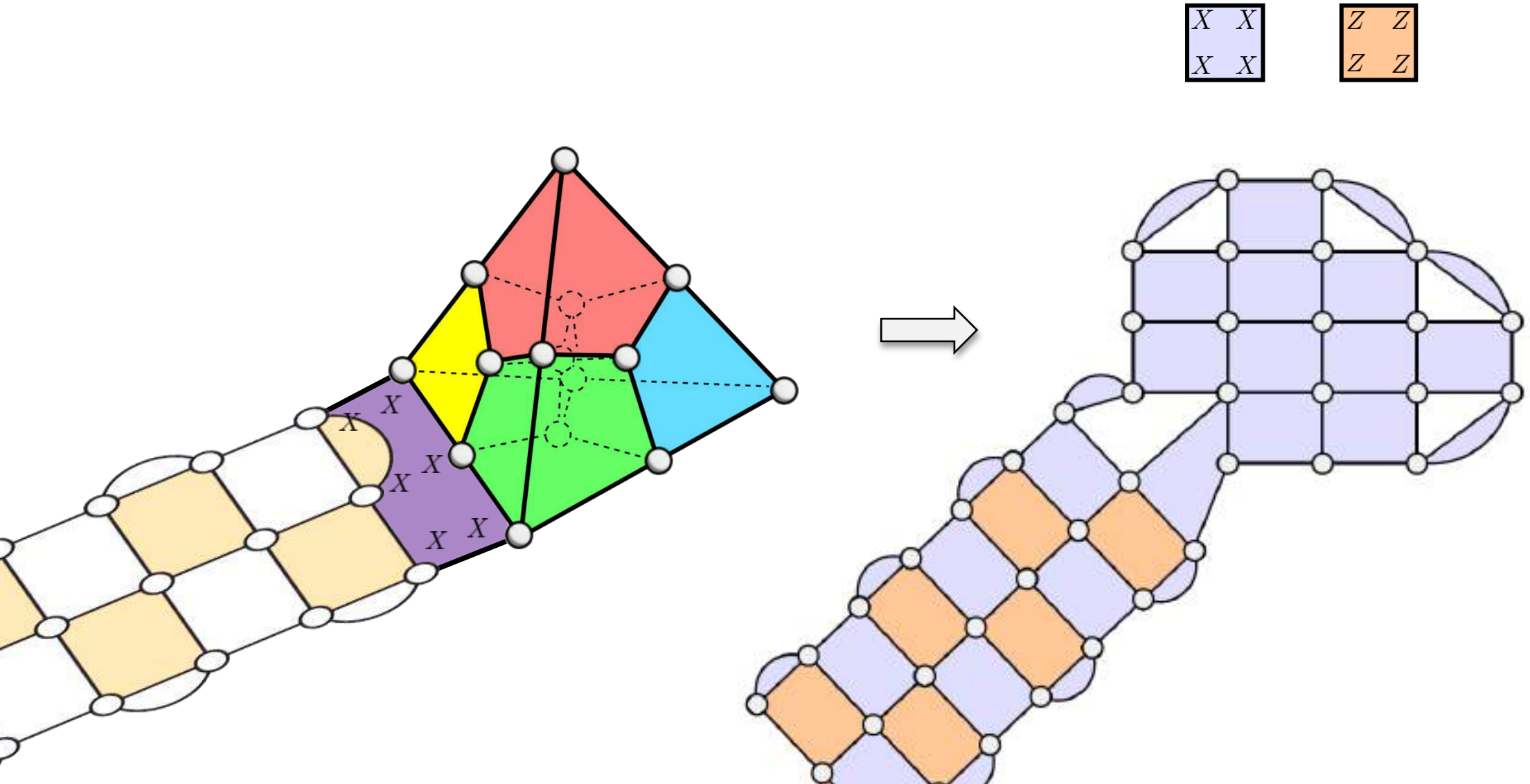


Use the outer code to detect bitflip errors

Detect up to 2 bitflips → $\eta \approx 30$

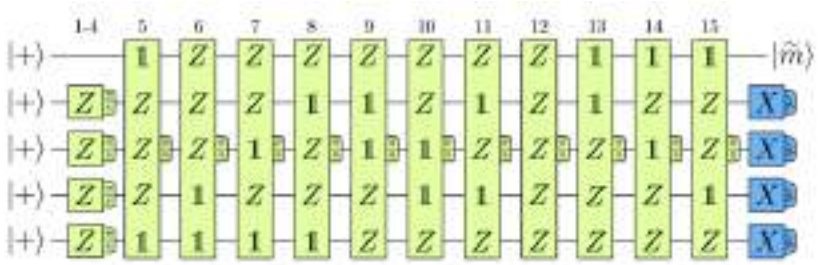
Schemes with Toffoli gates required $\eta = 10^5 - 10^6$

Merge to a surface code



Unfolded distillation

Magic State Distillation: Not as Costly as You Think

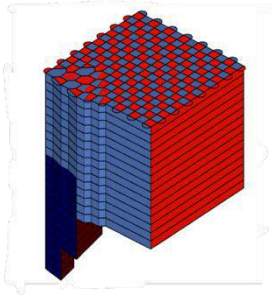


Litinski, Quantum 3, 205, 2019

4 620 qubits
42.6 rounds
197 000 Qubitcycles

$\Rightarrow 10^{-3} \to 4.5 \times 10^{-8}$

Magic state cultivation



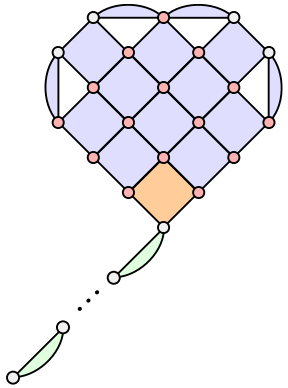
Gidney *et al*, arXiv:2409, 2024

500 qubits
50 rounds
25 000 Qubitcycles (/10)

$\Rightarrow 10^{-3} \to 10^{-6}$

Unfolded distillation

Ruiz *et al*, arXiv:2507.12511, 2025

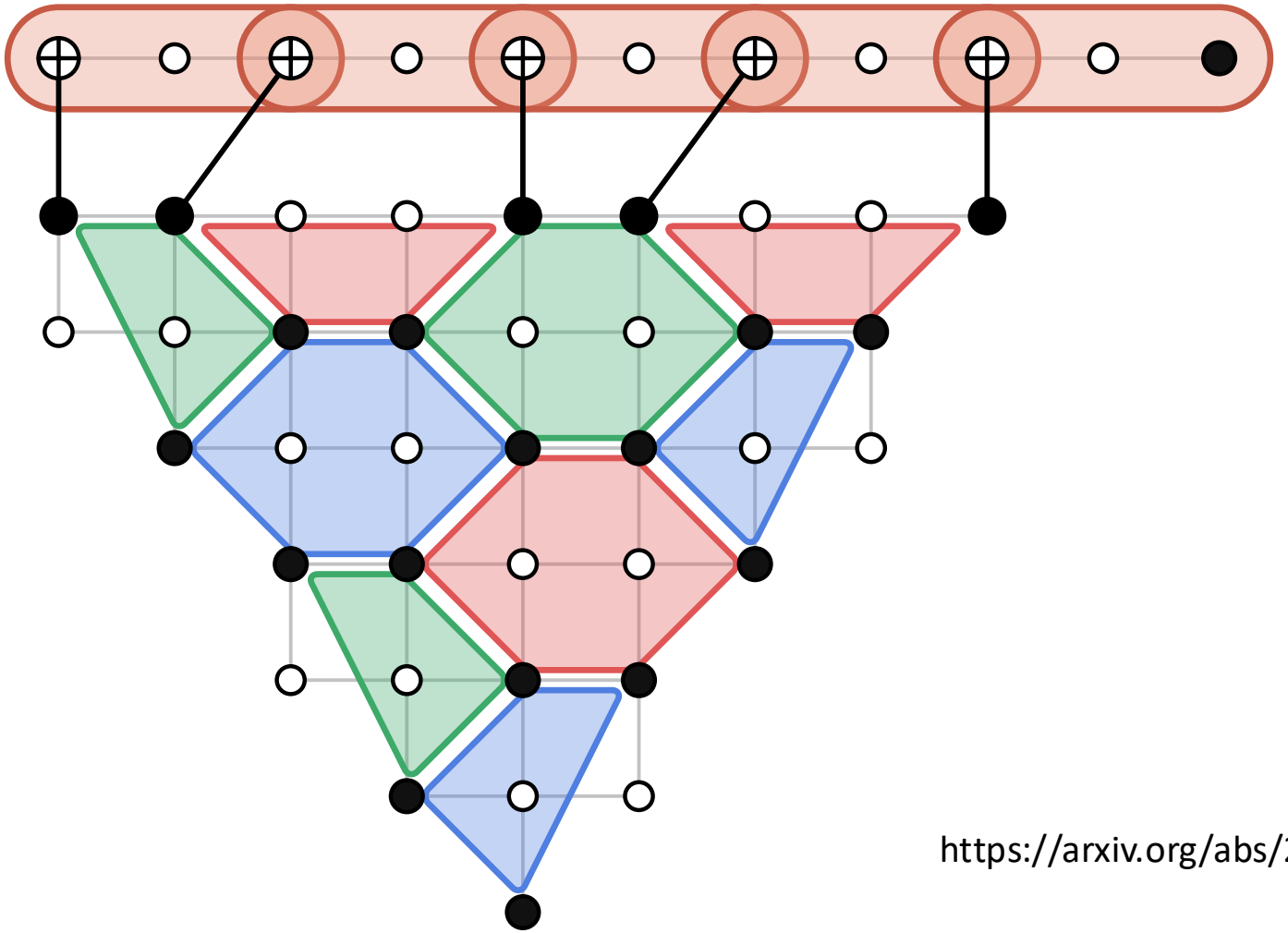


53 qubits (incl rep code)
5.5 rounds
300 Qubitcycles (/650)

$\Rightarrow \begin{cases} p_{Z,\mathrm{in}} = 10^{-3} \\ \eta = 5 \times 10^{6} \end{cases} \longrightarrow p_{\mathrm{out}} = 3 \times 10^{-7}$

Not enough for Shor, chemistry…

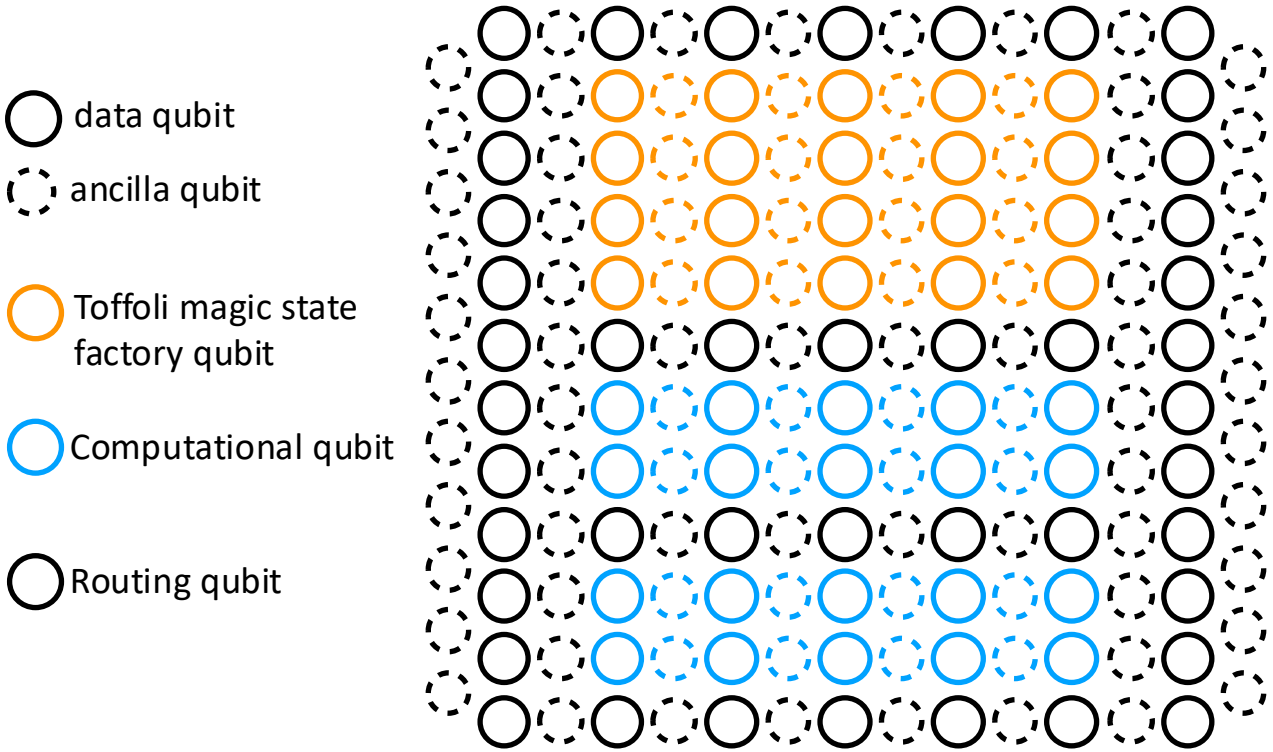
$|i\rangle$ state distillation



https://arxiv.org/abs/2610.37840

Quantum computing building block

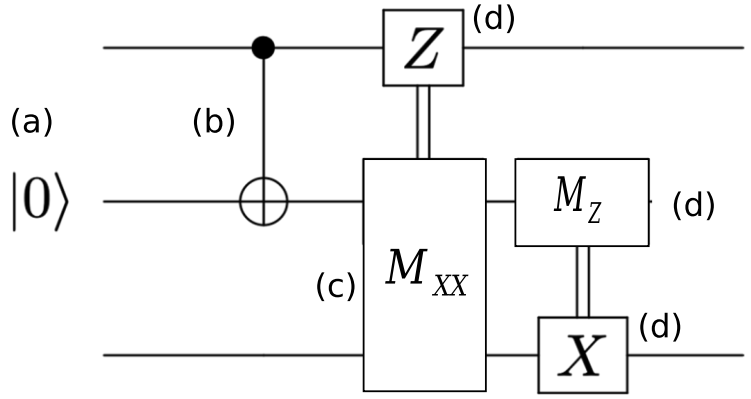
e.g. A 4-logical, 178-physical qubit processor

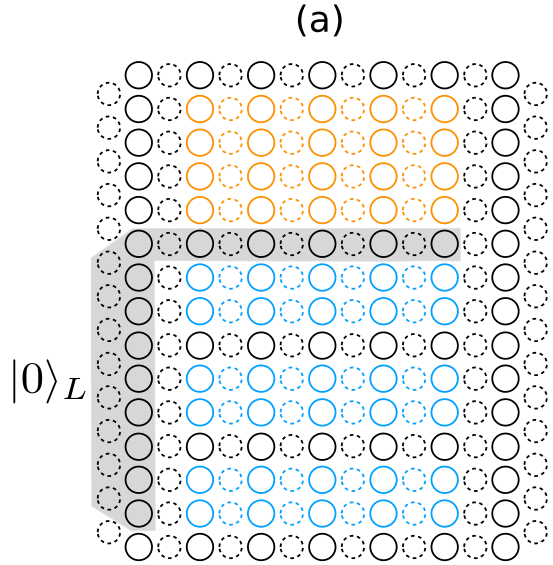


→ 60-fold hardware reduction

Gouzien et al., PRL 131 040602 (2023)

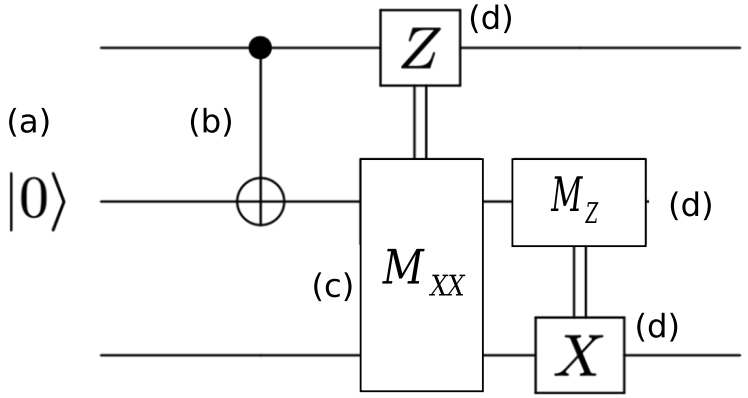
Long-range CNOT



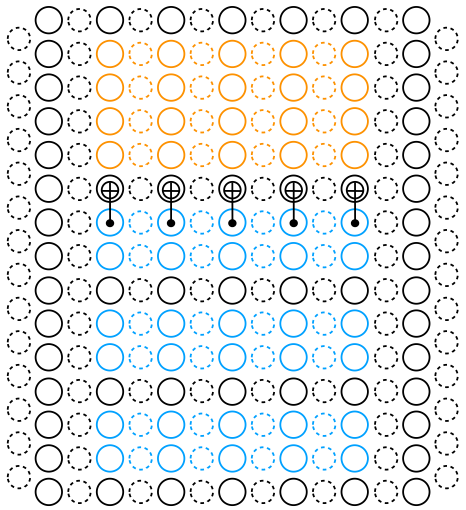


Gouzien et al., PRL 131 040602 (2023)

Long-range CNOT

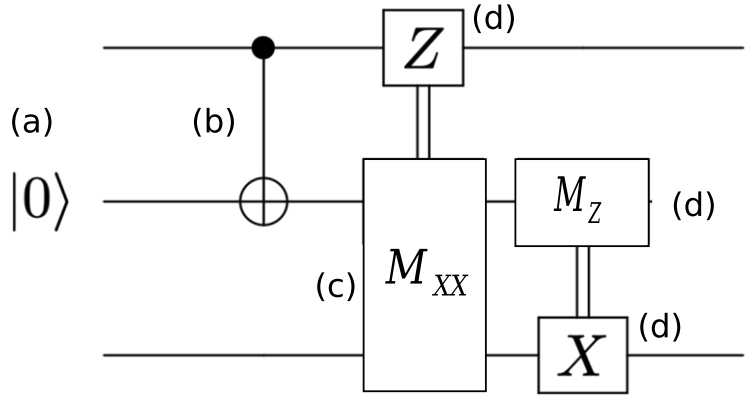


(b)

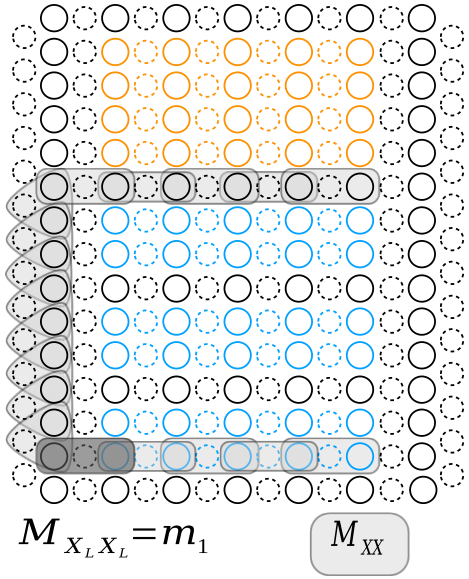


Gouzien et al., PRL 131 040602 (2023)

Long-range CNOT

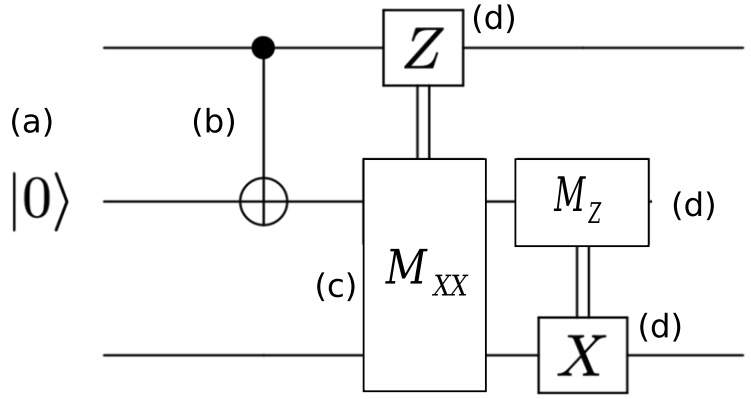


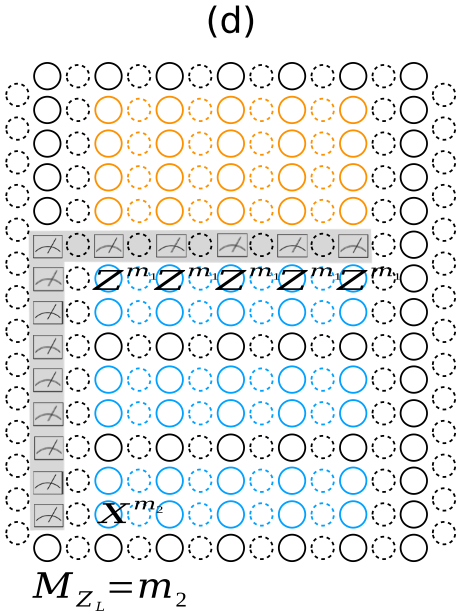
(c)



Gouzien et al., PRL 131 040602 (2023)

Long-range CNOT



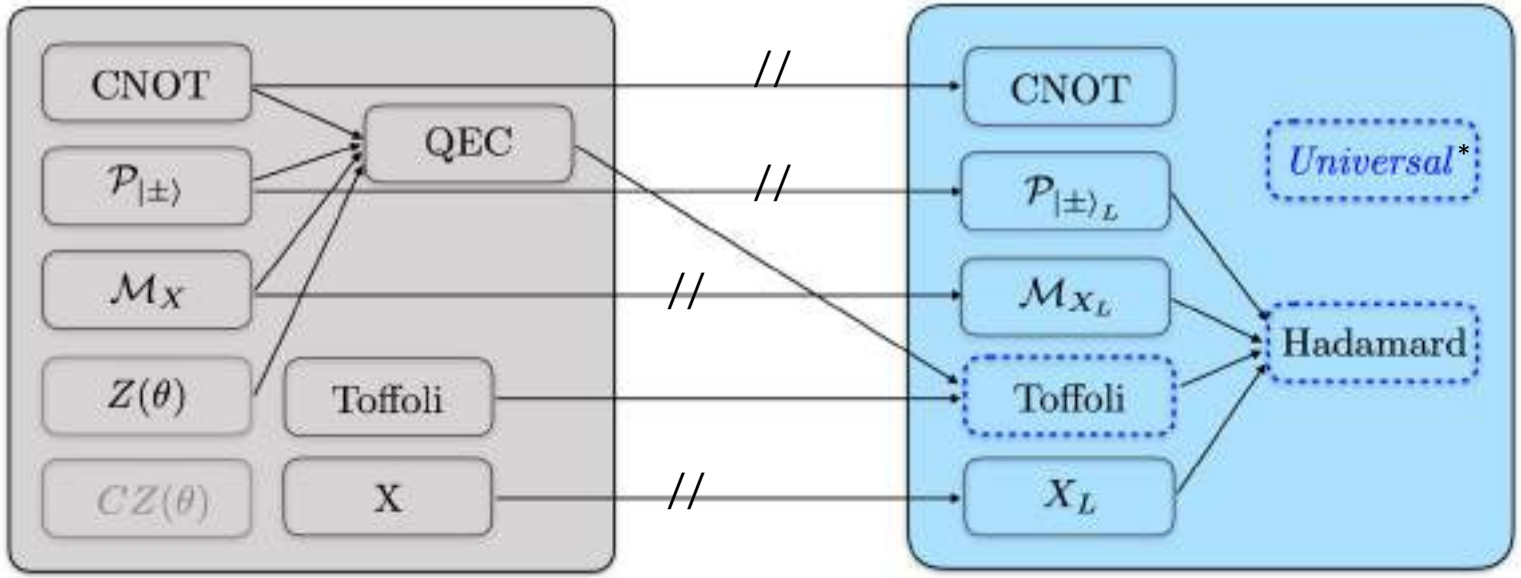


Gouzien et al., PRL 131 040602 (2023)

Scheme for universal quantum computation

« Bias-preserving » operations

Fault-tolerant logical operations

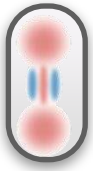


// Transversal

Single cat-qubit level

$|+\rangle = |\mathcal{C}_\alpha^+\rangle$

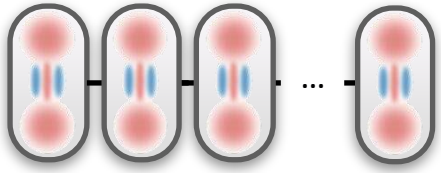
$|-\rangle = |\mathcal{C}_\alpha^-\rangle$



Repetition cat-qubit level

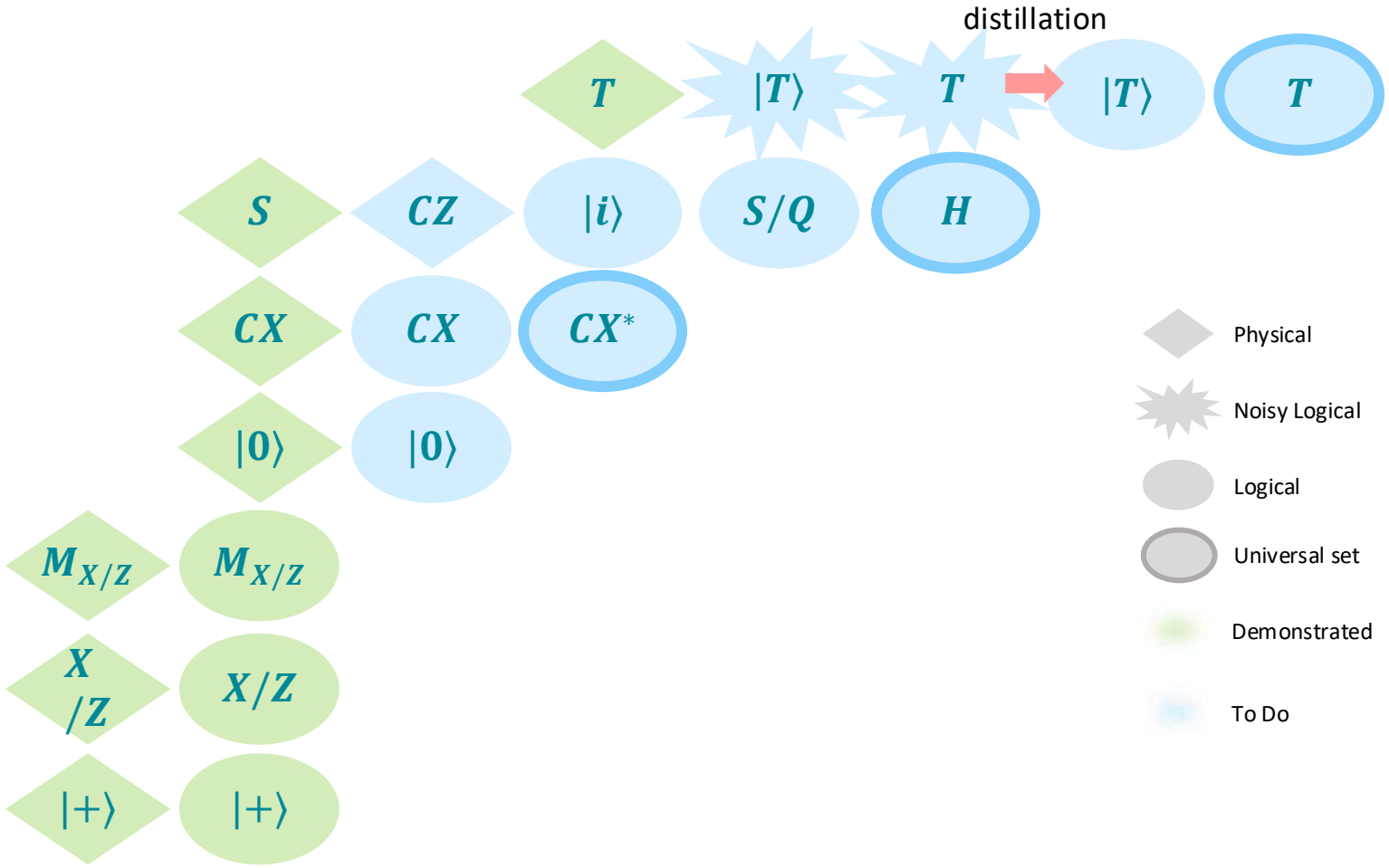
$|+\rangle_L = |\mathcal{C}_\alpha^+\rangle^{\otimes n}$

$|-\rangle_L = |\mathcal{C}_\alpha^-\rangle^{\otimes n}$



JG and M. Mirrahimi, Phys. Rev. X 9, 041053

Universal logical set from bias-preserving operations



J. Guillaud and M. Mirrahimi Physical Review X 9, 10.1103 (2019)
D. Litinski Quantum 3, 205 (2019)
C. Gidney, A. G. Fowler Quantum 3, 135 (2019)

05

LDPC-cat architecture

Dense encoding

Concatenating cat qubits in phase-flip LDPC codes

LDPC-cat codes for low-ov

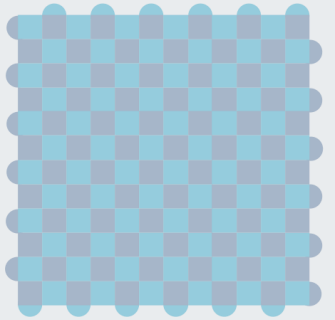
Diego Ruiz,[1,2,*] Jérémie Guillaud,[1] Anthony ,4

	Surface code + sc qubits [1, 2]	H co	ate LDPC cat qubits
Short-range interactions	yes (2D)		s (2D)
Tanner graph degree	3-4		4
$N_L = 100$ footprints, $\epsilon = 10^{-3}$, $\kappa_1/\kappa_2 = 10^{-4}$ $\rightarrow \epsilon_L \leq 10^{-8}$	N = 33,700		-
	-		(N/44)

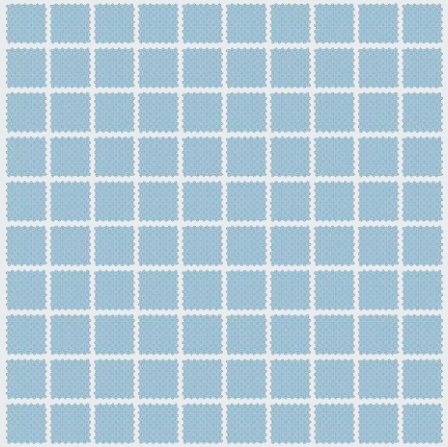
$\epsilon_L \approx 0.1(100p)^{(d+1)/2}$

$d = 13,$
$p = 10^{-3} \rightarrow \epsilon_L = 10^{-8}$

$N_{sc} = 2d^2 - 1 = 337$



$N = 100N_{sc} = 33{,}700$



arxiv:2401.09541

Quantum LDPC codes

Low **D**ensity **P**arity **C**heck codes:

- Constant stabilizer weight
- Each data qubit participates in a constant number of stabilizer



→ each physical qubit participates in several logical qubits

Physical constraints:

We prefer to have 2D local codes

BPT bound:

2D local codes → $kd^2 \leq \mathcal{O}(n)$

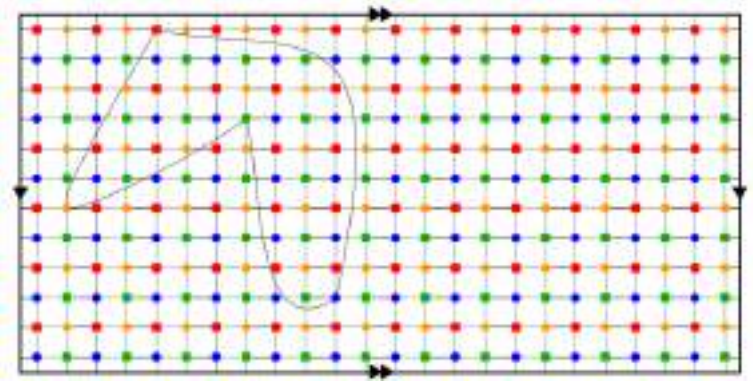
with n number of physical data qubits

k number of logical qubits

d code distance

Surface code: $[[n, k = 1, d = \sqrt{n}]]$

Long-range connections needed:



D. Gottesman, Q. Information & Computation 14, 2013

S. Bravyi et al, PRL 104, 2010

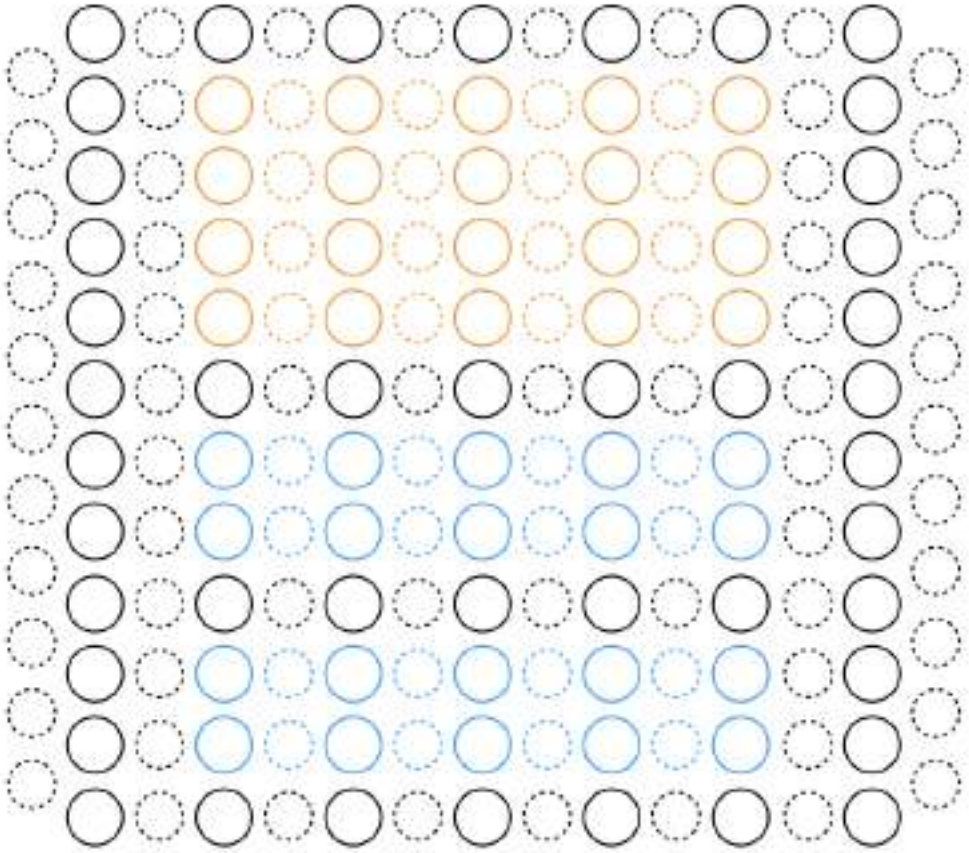
S. Bravyi et al, Nature 627, 2024

2D local phase-flip codes

BPT bound for 2D classical codes:

$$k\sqrt{d} \leq \mathcal{O}(n)$$

→ Room for improvement over the repetition code $[n, k = 1, d = n]$



S. Bravyi et al, PRL 104, 2010

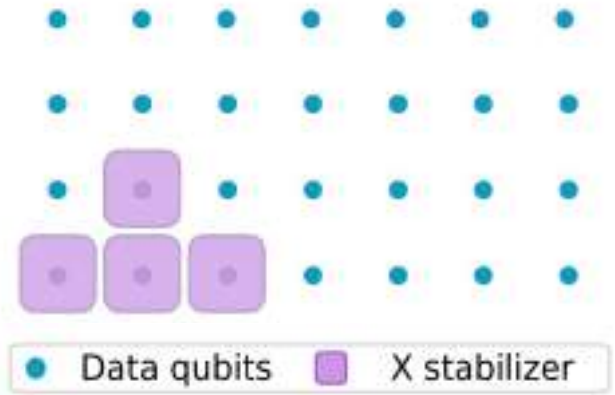
2D local phase-flip codes

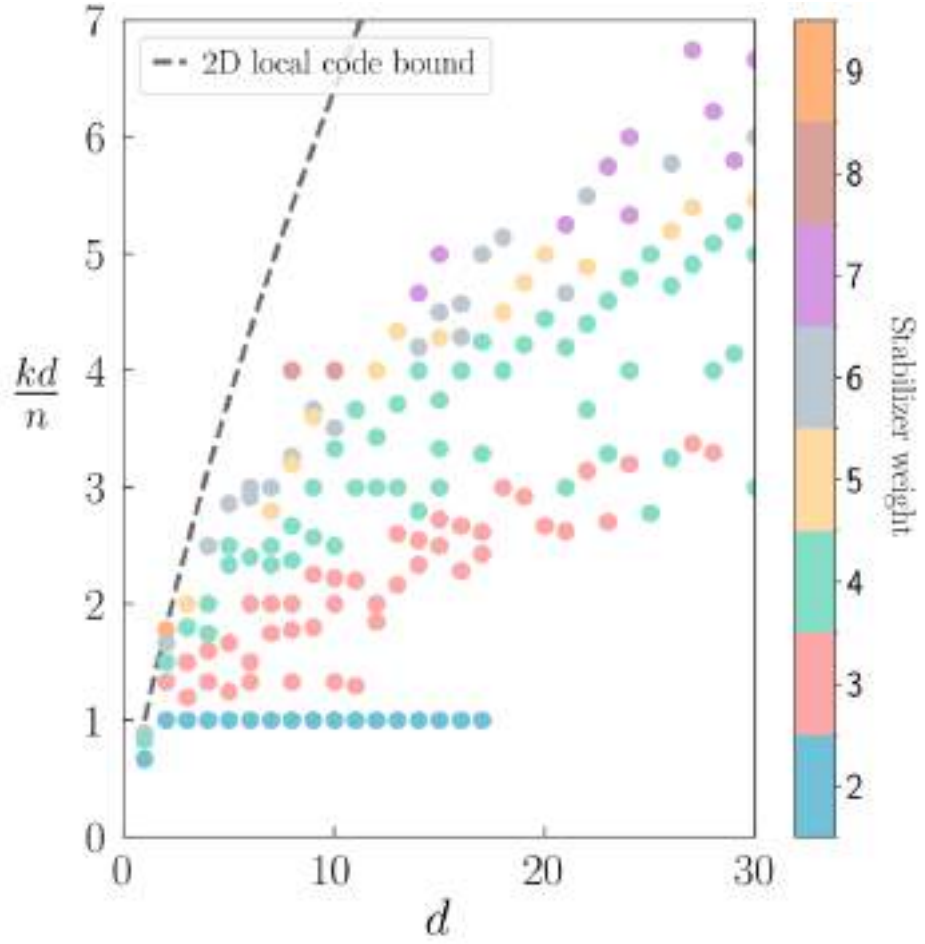
BPT bound for 2D classical codes:

$$k\sqrt{d} \leq \mathcal{O}(n)$$

→ Room for improvement over the repetition code $[n, k = 1, d = n]$

- Single stabilizer shape translated





S. Bravyi et al, PRL 104, 2010

2D local phase-flip codes

BPT bound for 2D classical codes:

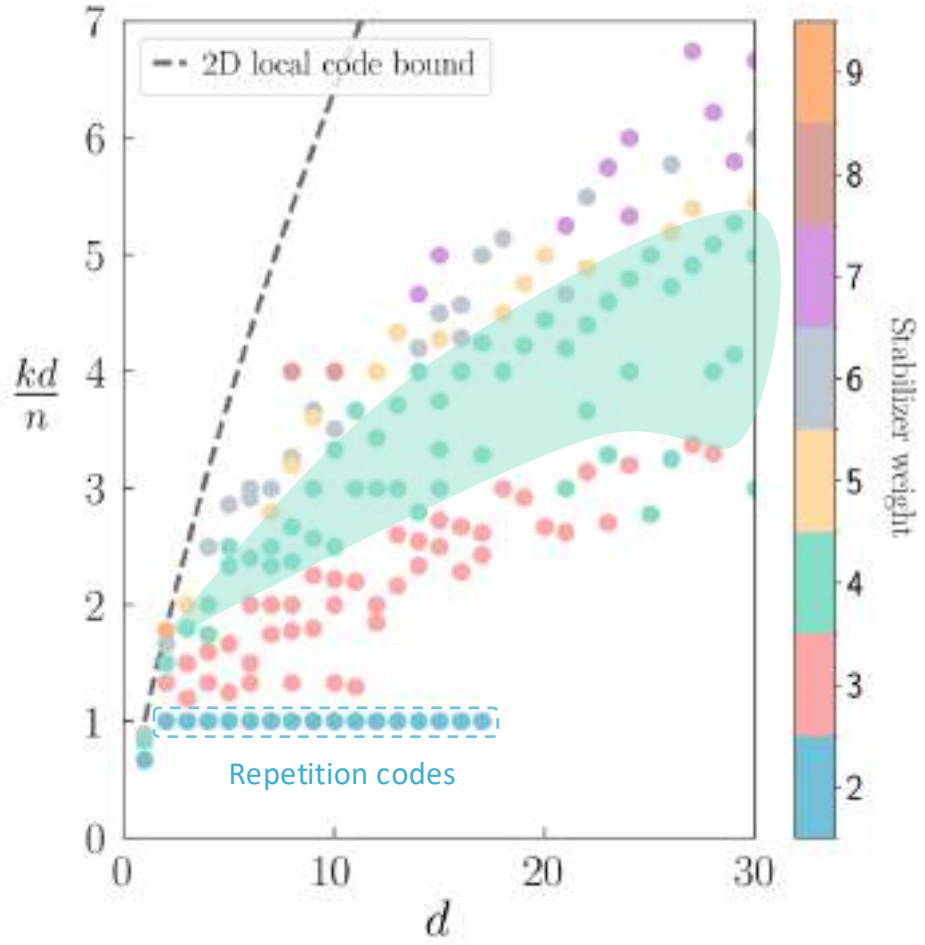
$$k\sqrt{d} \leq \mathcal{O}(n)$$

→ Room for improvement over the repetition code $[n, k = 1, d = n]$

- Single stabilizer shape translated

kd/n qubit reduction compared to the repetition code

→ Weight-4 stabilizer is a good compromise



S. Bravyi et al, PRL 104, 2010

2D local phase-flip codes

BPT bound for 2D classical codes:

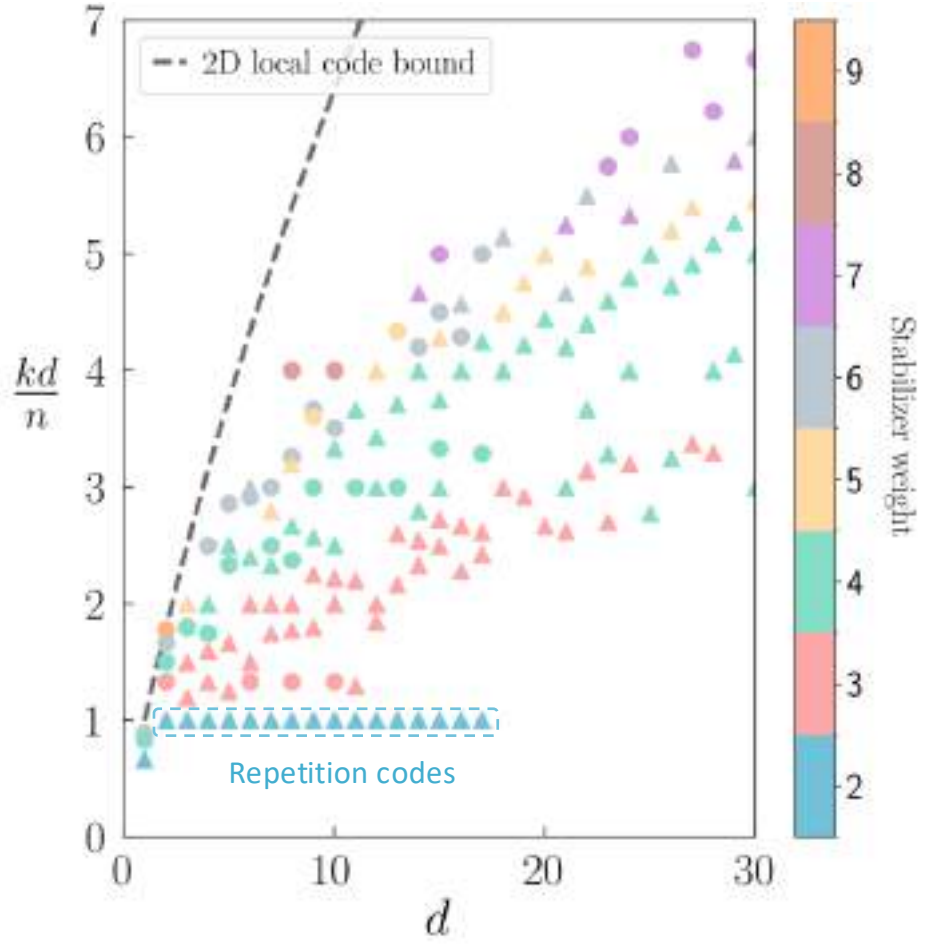
$$k\sqrt{d} \leq \mathcal{O}(n)$$

→ Room for improvement over the repetition code $[n, k = 1, d = n]$

- ● Single stabilizer shape translated
- ▲ Cellular automaton codes

kd/n qubit reduction compared to the repetition code

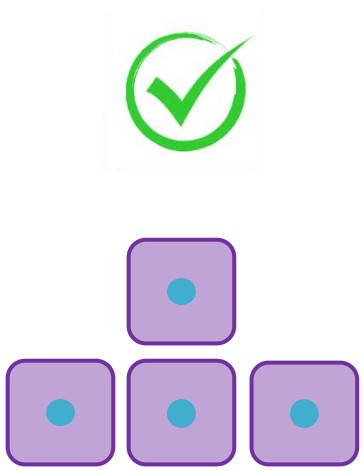
→ Weight-4 stabilizer is a good compromise

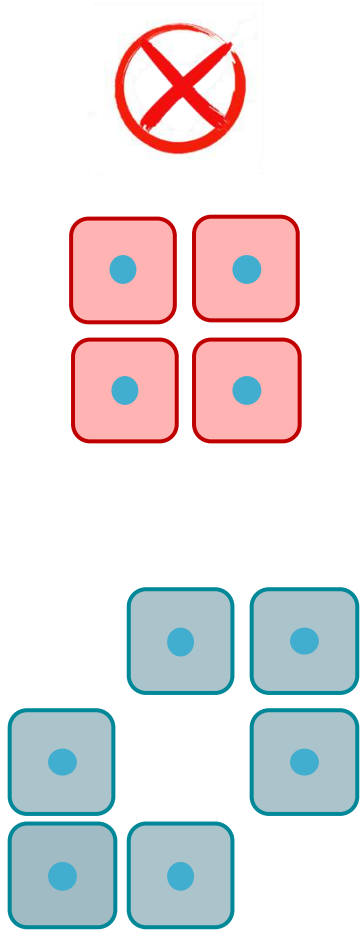


S. Bravyi et al, PRL 104, 2010

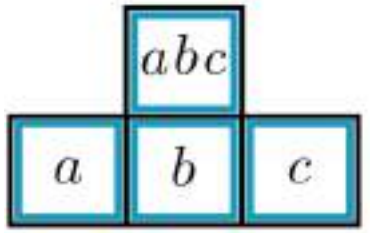
Cellular automaton codes

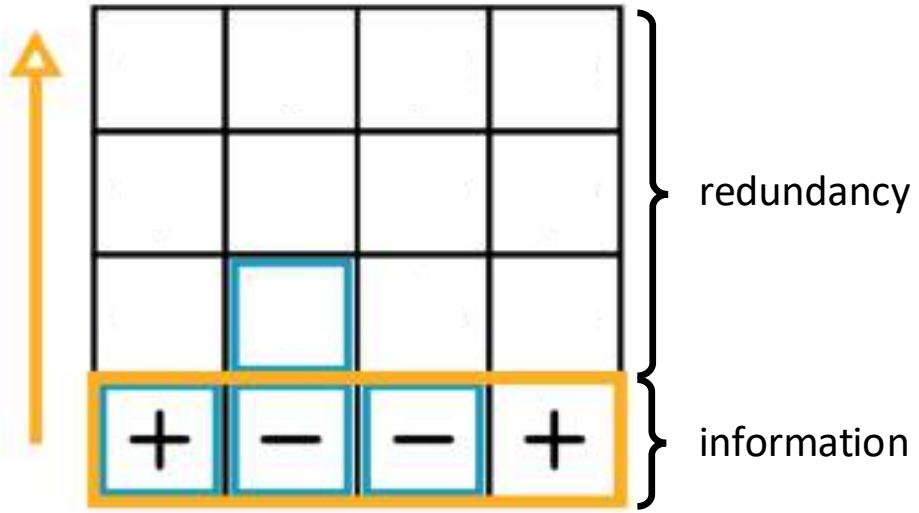
S. Bravyi et al, PRL 104, 2010
M. Newman et al, PRE 60, 1999
G. M. Nixon et al, IEEE 67, 2021





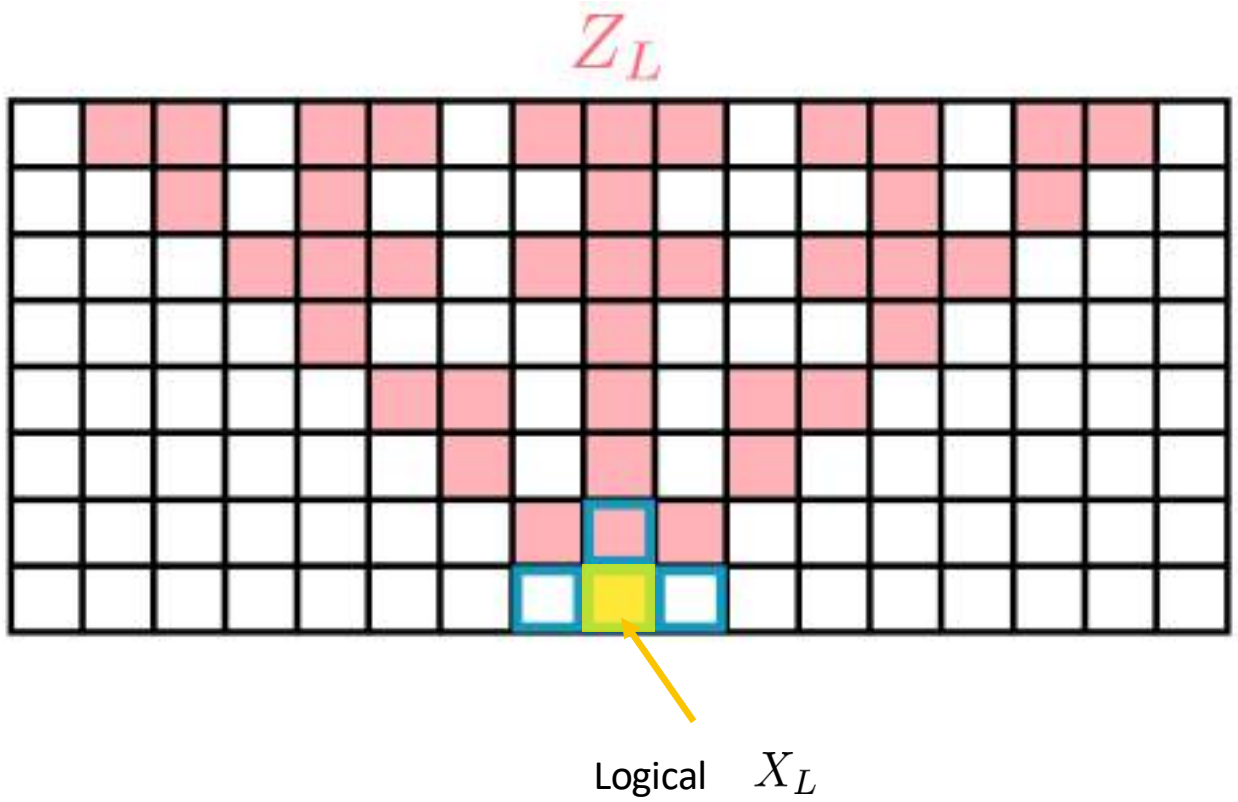
Cellular automaton rule to construct the codewords:





number of logical qubits

Fractal (phase-flip) codes



$= Z$ $= I$

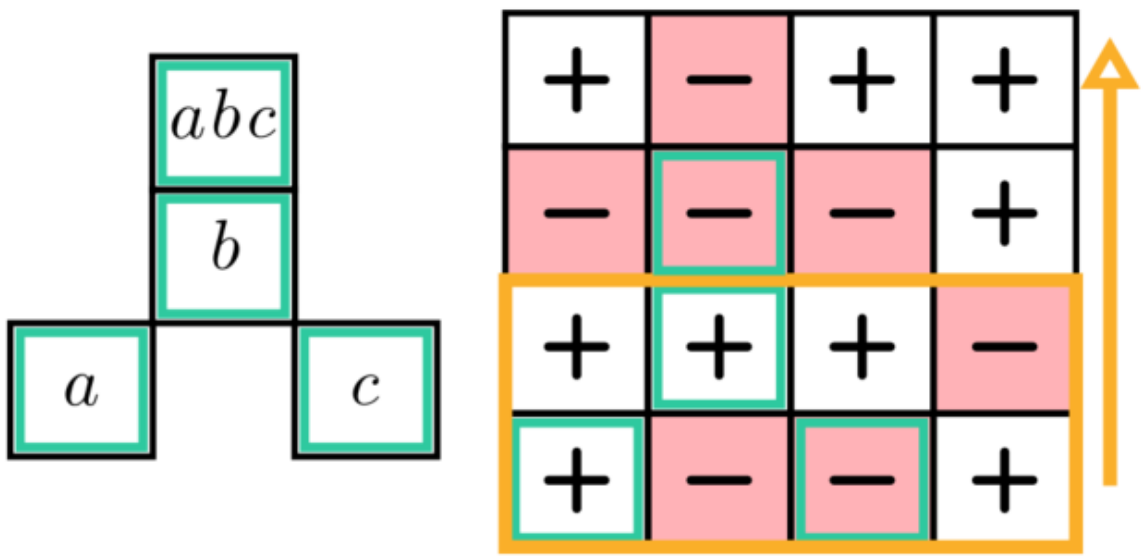
Minimum weight logical Z_L operator with fractal support

Basis of logical operator can be formed by horizontal translation

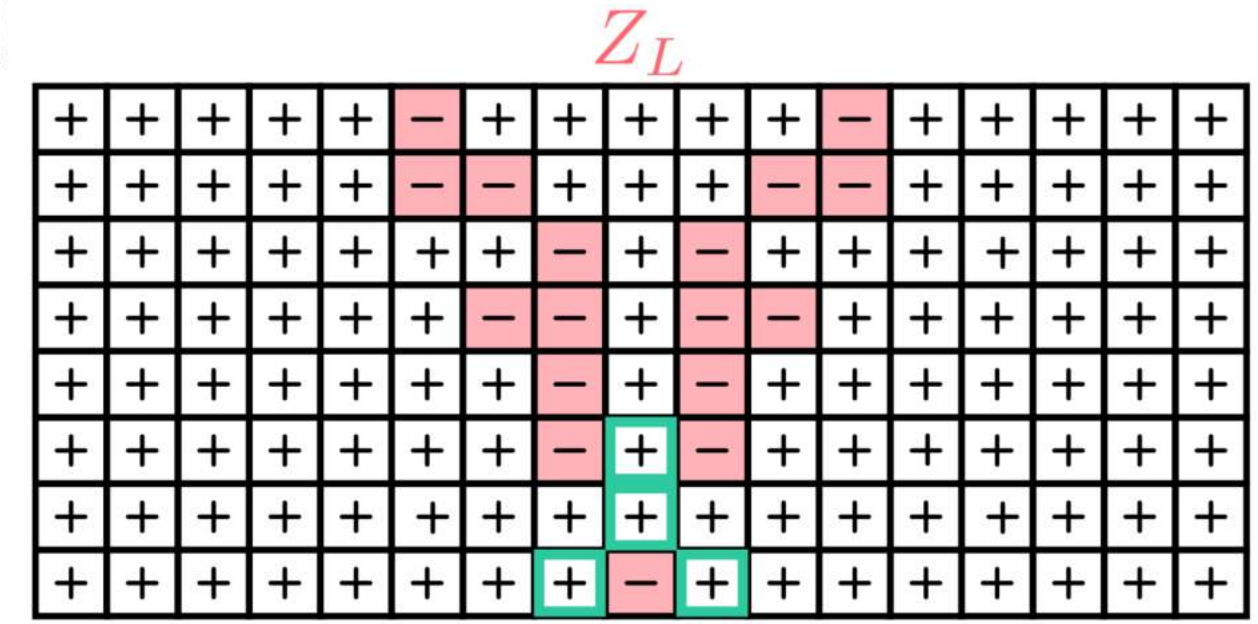
Logical X_L of weight one
→ bit-flip correction handled by cat qubits

B. Yoshida, Annals of Physics 338:134-166, 2013

Cellular automaton codes on multiple rows



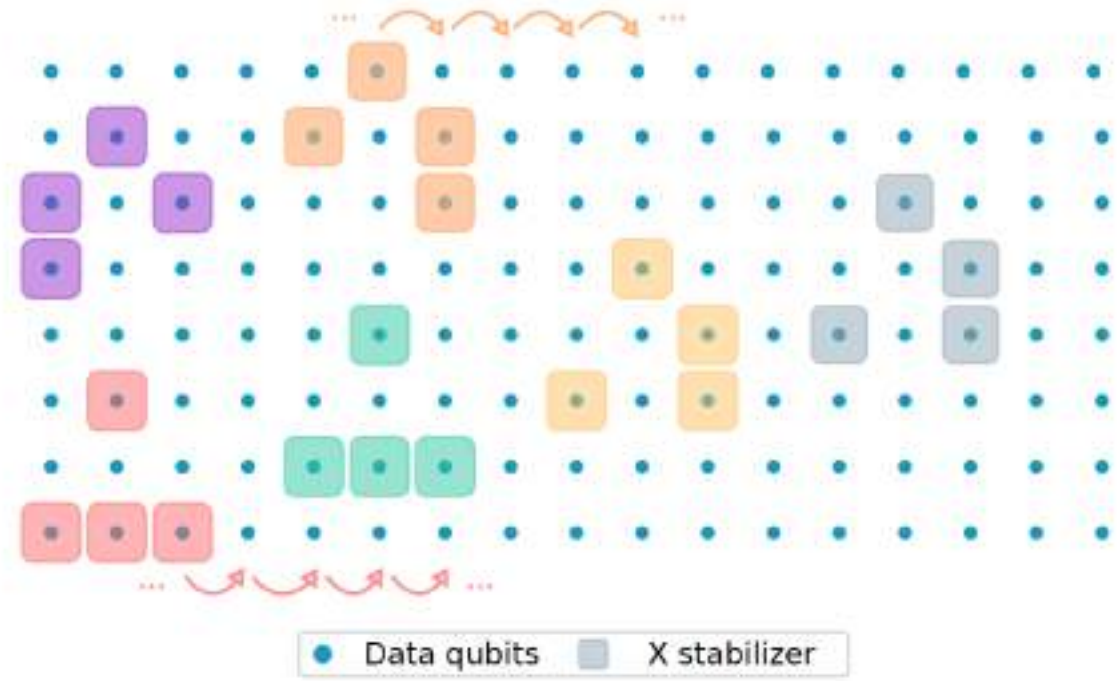
Double the number of logical qubits

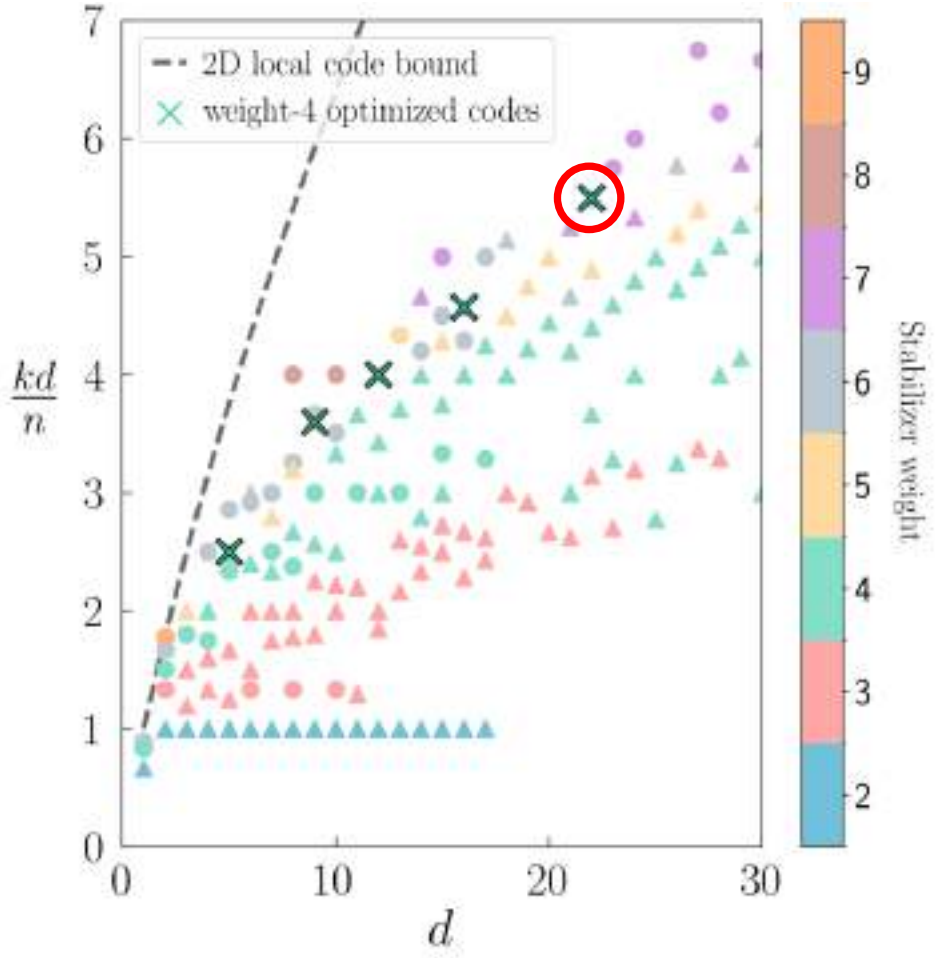


Reduce the distance

Overall, the overhead reduction factor kd/n is improved

Cellular automaton codes

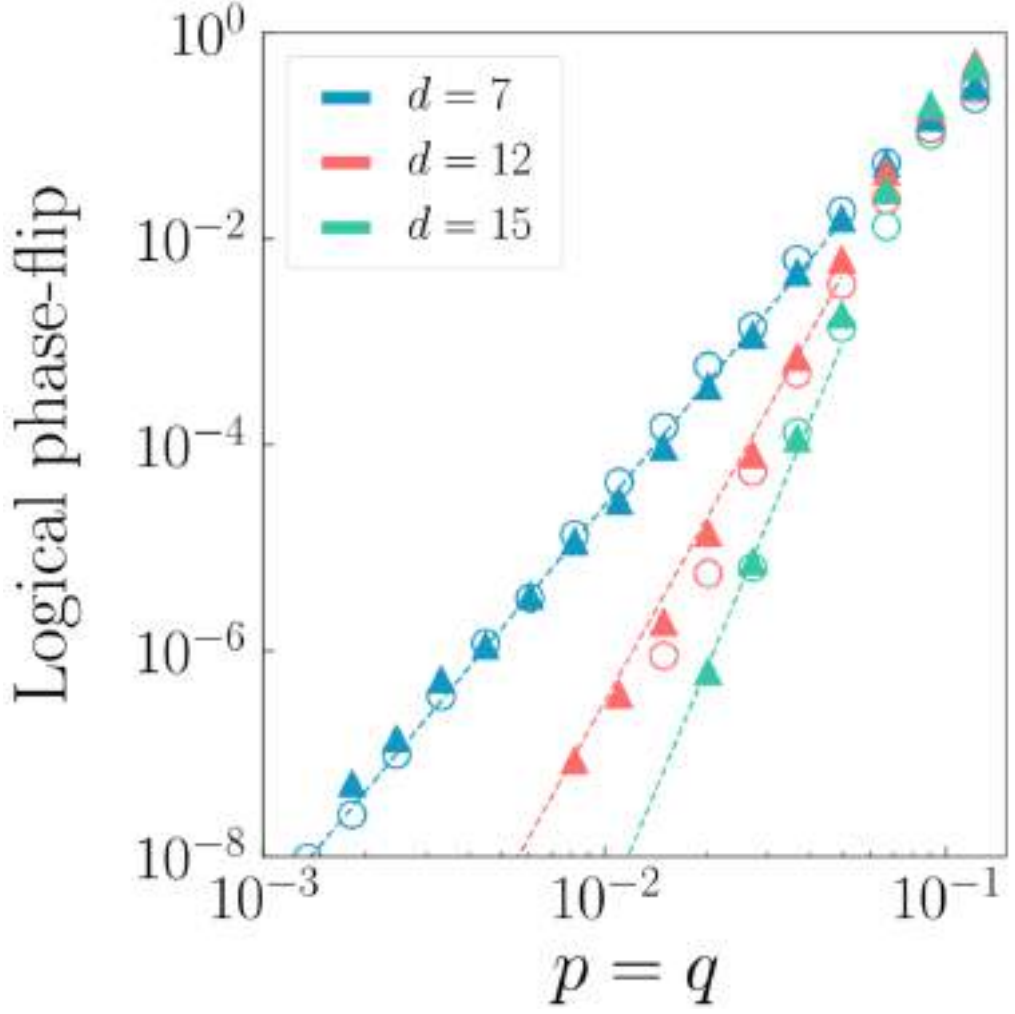




$\rightarrow d = 22$ with only 4 physical qubits per logical qubits

→ 100 logical qubits with 758 cat qubits (including ancilla) vs 4300 for the repetition code

Logical Z error – phenomenological noise

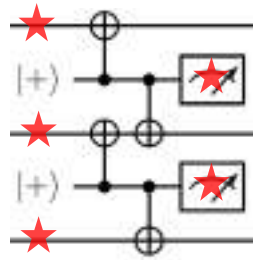


○ Repetition codes

▲ LDPC codes

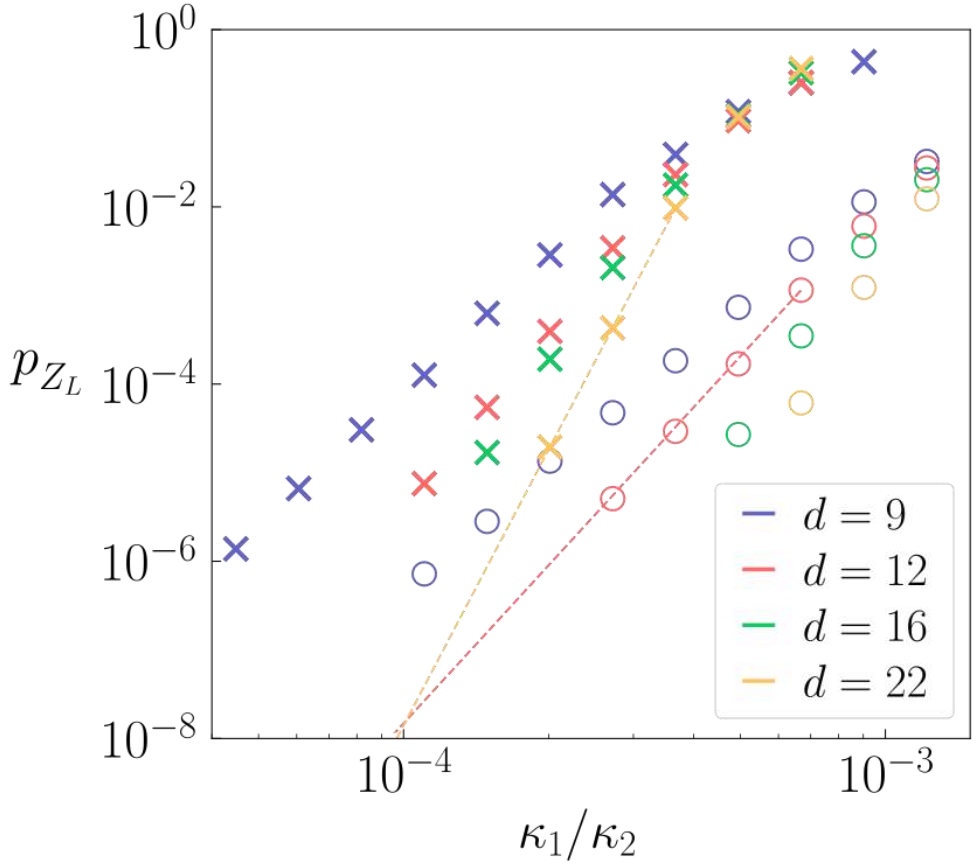


Phenomenological model



Essentially the same threshold and scaling below threshold

Logical Z error – circuit level noise



○ Repetition codes

× LDPC codes

Circuit level model

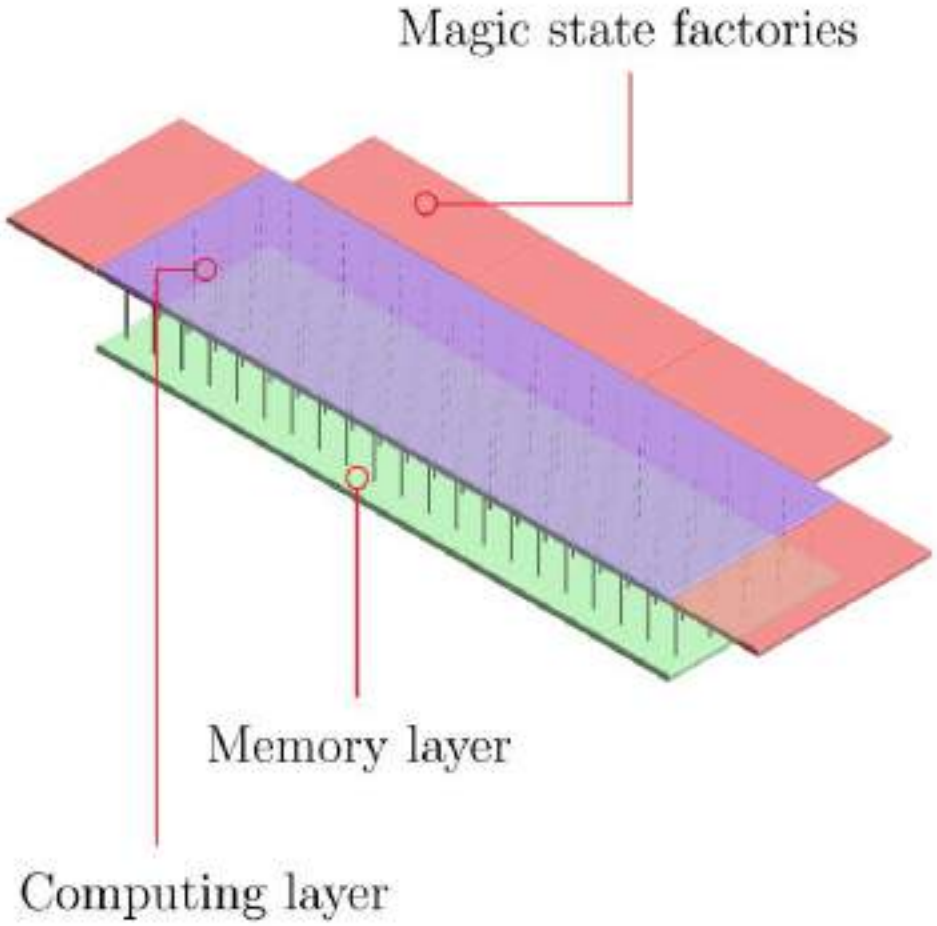


- Lower threshold in circuit level
- Overhead is $/3$ at $\kappa_1/\kappa_2 = 10^{-4}$ to achieve 10^{-8} logical error level
- BP+OSD decoder quantumgizmos/bp_osd

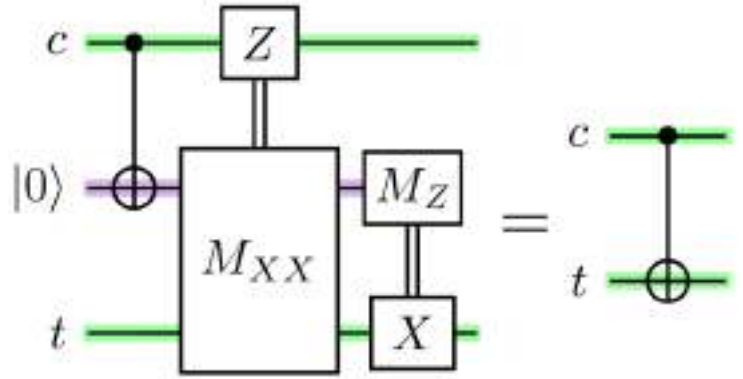
P. Panteleev *et al*, Quantum 585, 2021

J. Roffe *et al*, PRR 2, 2020

Universal set of logical gates



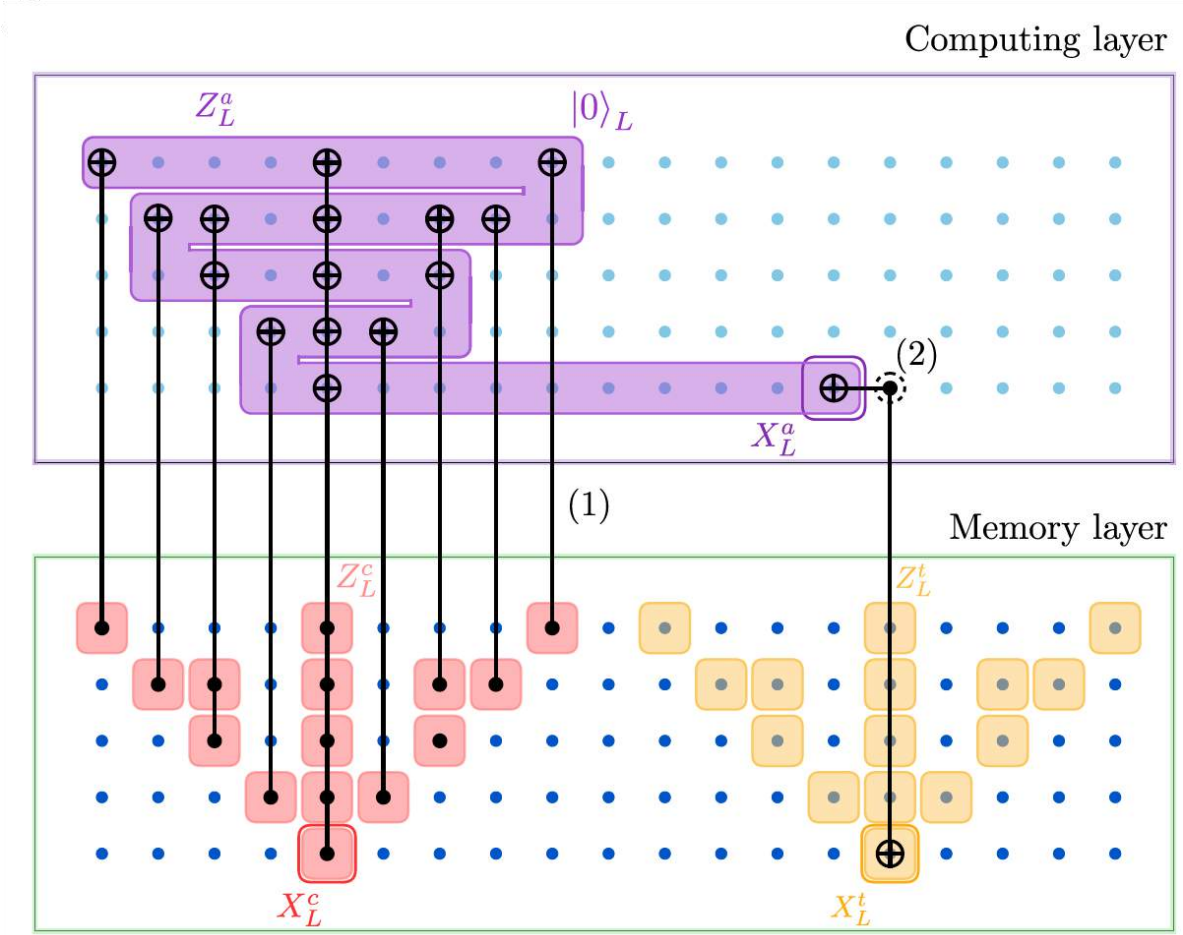
Intra-block CNOT using lattice surgery

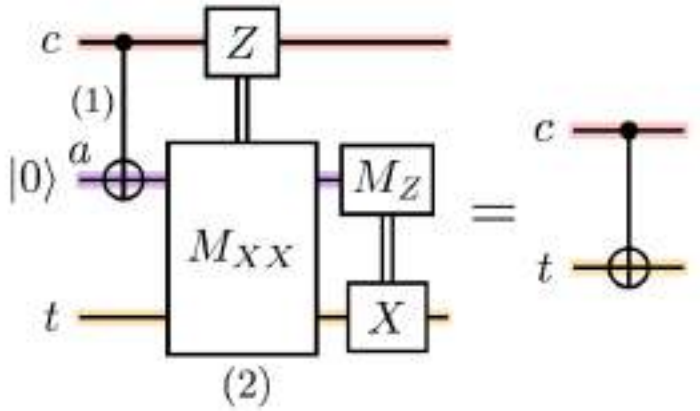


- Parallelizable for almost all logical qubits
- Flip chip architecture

D. Horsman et al, NJP 14.12, 2012

(Intra-block) CNOT gate with lattice surgery





- Parallelizable for almost all logical qubits
- Flip-chip architecture

D. Horsman et al, NJP 14.12, 2012

06

Resource estimation

Counting to validate

Shor’s algorithm: textbook version

Shor's algorithm: factoring by period finding

Problem

$N = pq$, p and q prime numbers

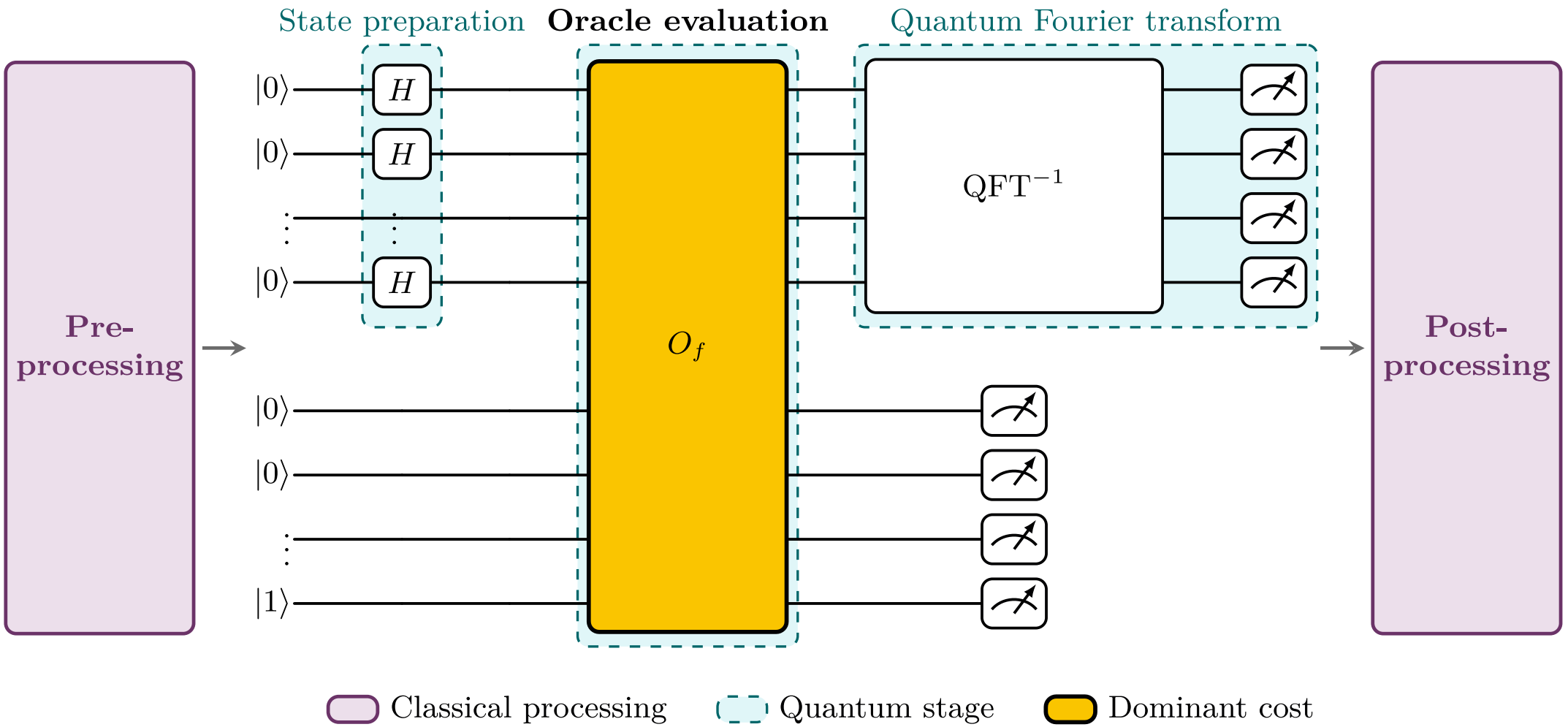
Principle

- pick up $g \in \mathbb{Z}_N^*$ randomly
- find the period r of $e \mapsto g^e \bmod N$
- hypothesis r even and $g^{r/2} \not\equiv -1 \bmod N$
- $g^r \equiv 1 \bmod N, \left(g^{r/2} - 1\right)\left(g^{r/2} + 1\right) \equiv 0 \bmod N$
- $p, q = \gcd\left[g^{r/2} - 1, N\right], \gcd\left[g^{r/2} + 1, N\right]$

Run on quantum hardware

1. prepare
   $$\frac{1}{\sqrt{2^{n_e}}} \sum_{x=0}^{2^{n_e}-1} |x\rangle$$
   with n_e the number of bits of the exponent
2. compute $e \mapsto g^e \bmod N$
3. quantum Fourier transform to recover r

Textbook Shor algorithm



Destructive interferences

Before the Fourier transform

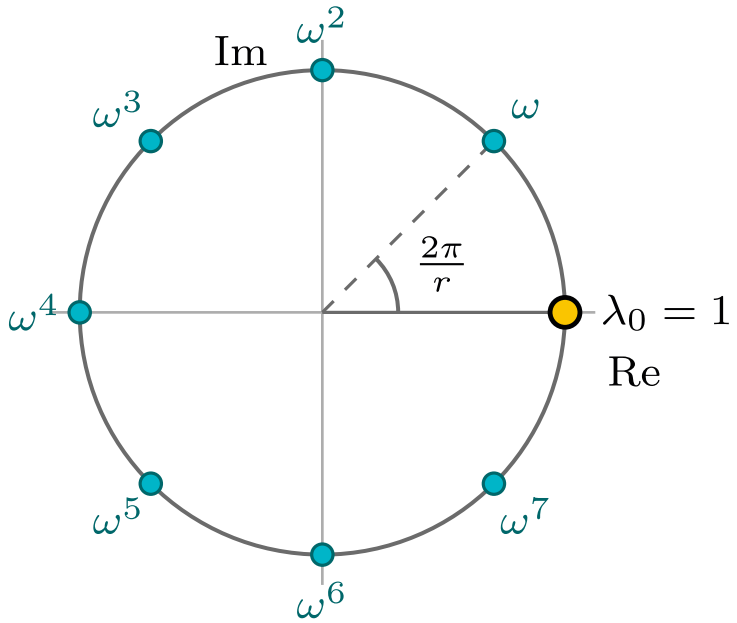
$$|\psi\rangle = \frac{1}{\sqrt{2^{n_e}}} \sum_{x=0}^{2^{n_e}-1} |x\rangle |g^x \bmod N\rangle$$

After the Fourier transform

$$|\psi'\rangle = \frac{1}{2^{n_e}} \sum_{x,y=0}^{2^{n_e}-1} e^{2\pi i x y / 2^{n_e}} |y\rangle |g^x \bmod N\rangle$$

$$= \sum_{y=0}^{2^{n_e}-1} \sum_{k=0}^{r-1} \left[\frac{1}{2^{n_e}} \sum_{x:\, g^x \equiv g^k} e^{2\pi i x y / 2^{n_e}} \right] |y\rangle |g^k \bmod N\rangle$$

The bracket is the amplitude of $|y\rangle|g^k \bmod N\rangle$: its phases cancel unless $ry/2^{n_e}$ is close to an integer.



Eigenvalues $\lambda_\mu = \omega^\mu$,
$\omega = e^{2\pi i/r}$ (here $r = 8$)

Uniform sum of eigenvectors

$|v_0\rangle$

$|v_1\rangle$

$\vdots$

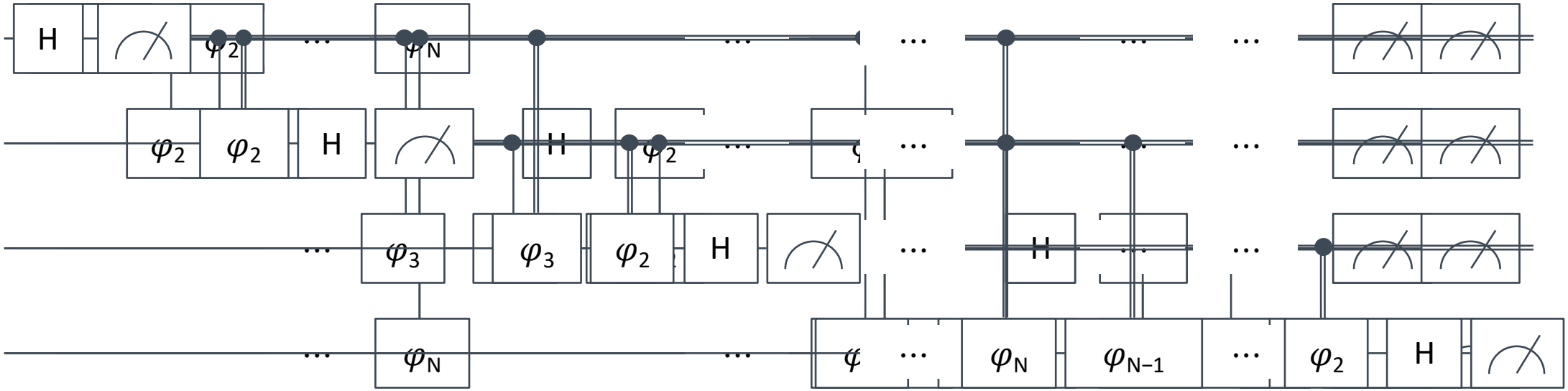
$|v_{r-1}\rangle$

$\frac{1}{\sqrt{r}} \sum_\mu |v_\mu\rangle =$

$|1\rangle$

all phases cancel except on $|1\rangle$

Semi-classical Fourier transform

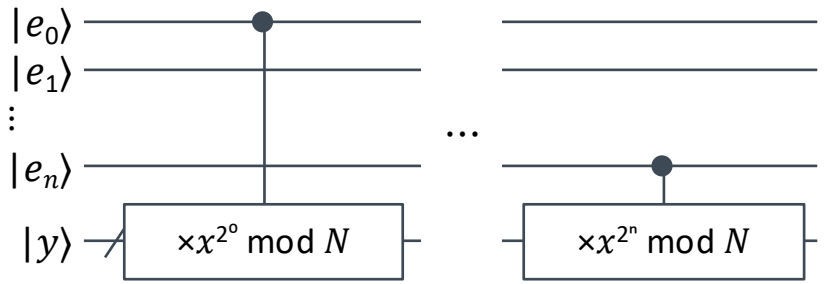


with gate φ_k: $\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$

Standard implementation complexity

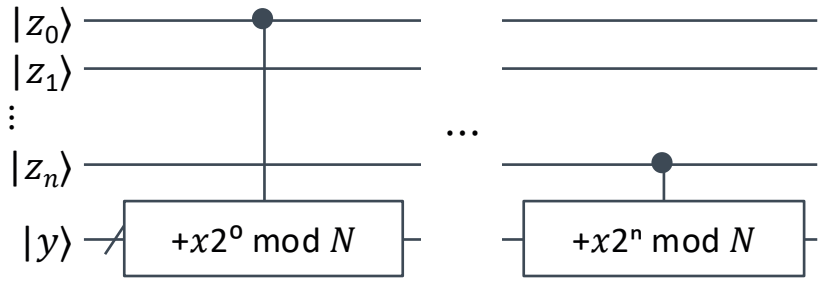
Exponentiation: $|e\rangle|y\rangle \mapsto |e\rangle|y \times x^e \bmod N\rangle$

$$x^e = x^{\sum_i 2^i e_i} = \prod_i \left[x^{2^i}\right]^{e_i}$$



Multiplication: $|z\rangle|y\rangle \mapsto |z\rangle|y + x \times z \bmod N\rangle$

$$xz = x\sum_i 2^i z_i = \sum_i \left(x2^i\right) z_i$$



Addition: $|x\rangle|y\rangle \mapsto |x\rangle|x + y \bmod N\rangle$

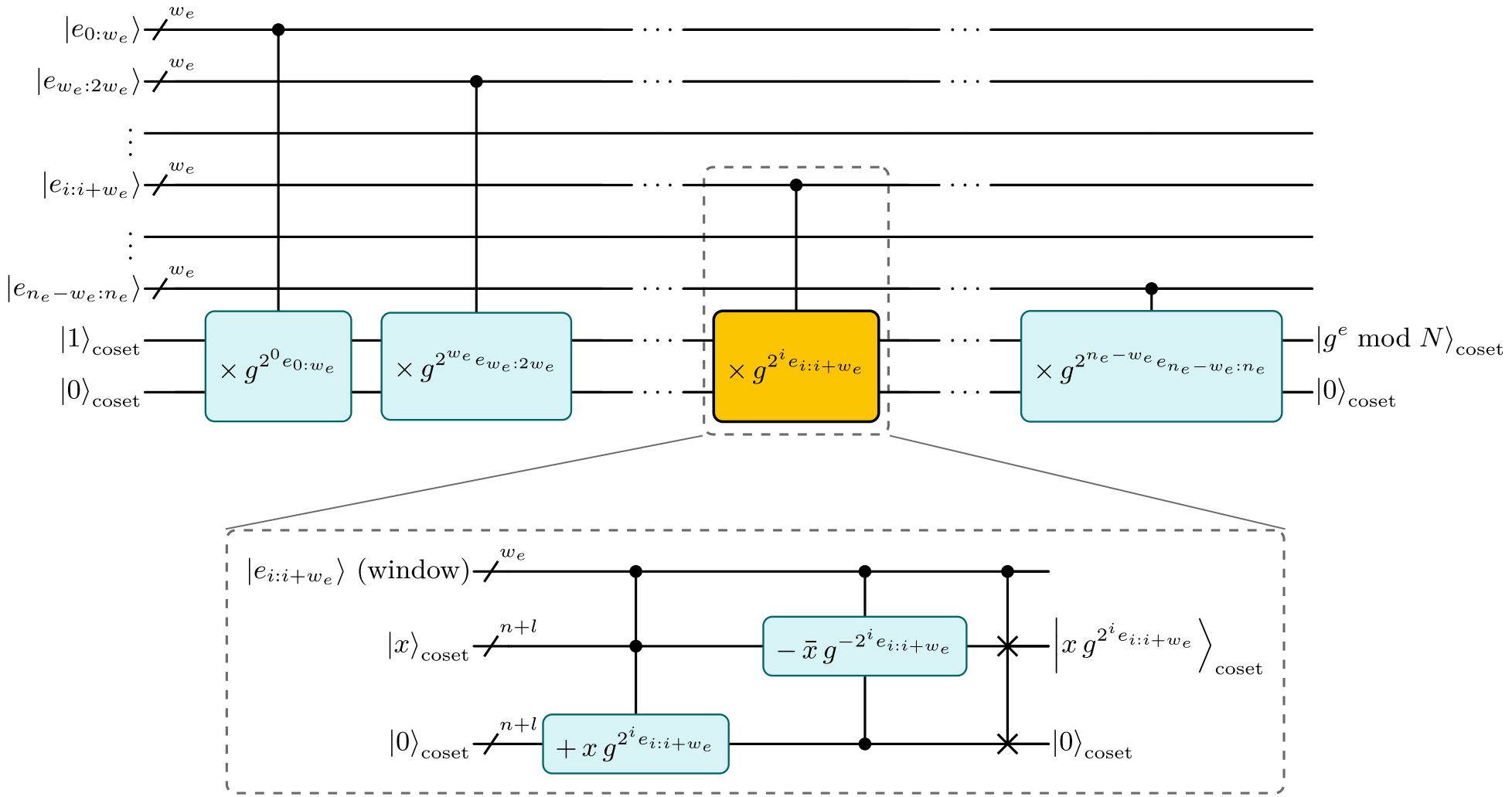
$O(n)$ with carry-ripple addition[1]

Modular addition: addition, comparison, controlled correction and clean-up of ancillary qubits: $O(n)$

Complexity: modular exponentiation in $O(n^3)$

[1] S. A. Cuccaro et al., "A new quantum ripple-carry addition circuit", 2004

Modular exponentiation and inplace multiplication



What is an addition?

Decimal addition

$$\begin{array}{r} {\scriptstyle 1\quad\ 1\ 1\ \ } \\ 23167 \\ +\ \ 9267 \\ \hline 32434 \end{array}$$

Binary addition

$$\begin{array}{r} {\scriptstyle 1\ 1\ 1\ 1\ 1\ 1\ 1\ \ } \\ 1011010011111111 \\ +\ \ 1001000011001101 \\ \hline 1111101011001010 \end{array}$$

How to compute the carries?

Truth table

a_k	b_k	c_k	c_{k+1}	r_k
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Expression

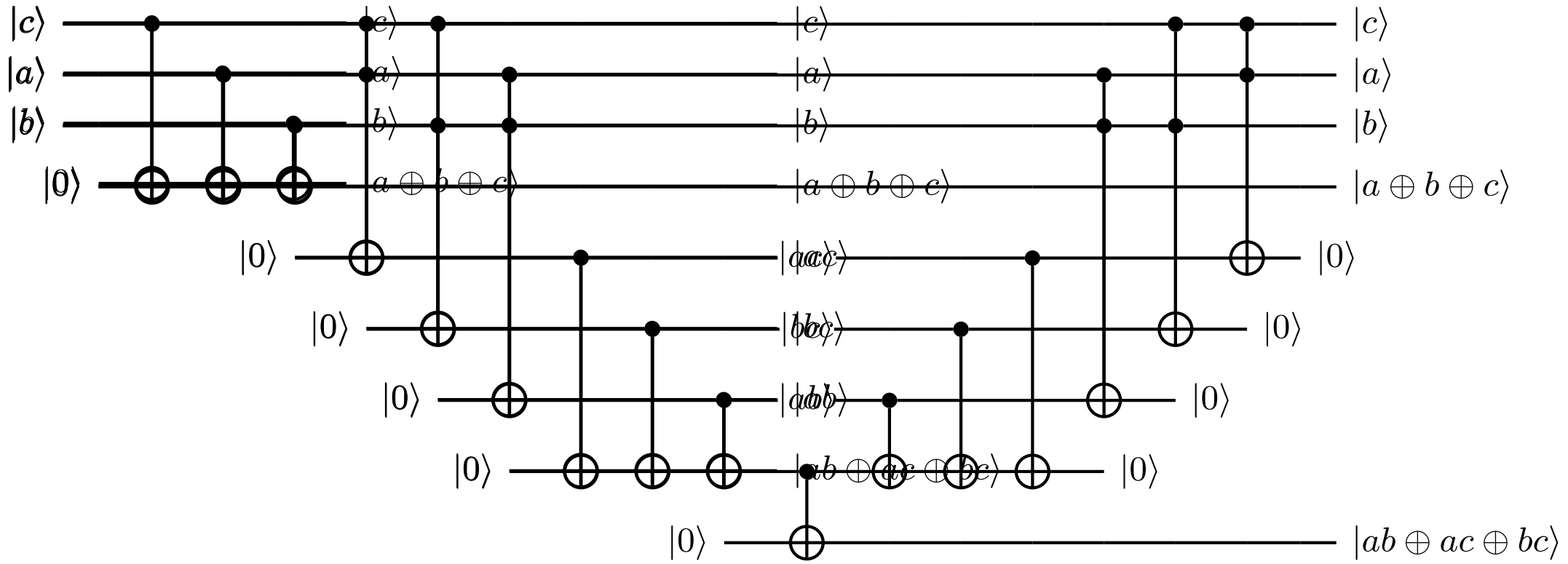
$$c_{k+1} = a_k b_k \oplus b_k c_k \oplus a_k c_k$$

$$r_k = a_k \oplus b_k \oplus c_k$$

Bennet's trick

$$c_{k+1} = a_k b_k \oplus b_k c_k \oplus a_k c_k$$

$$r_k = a_k \oplus b_k \oplus c_k$$



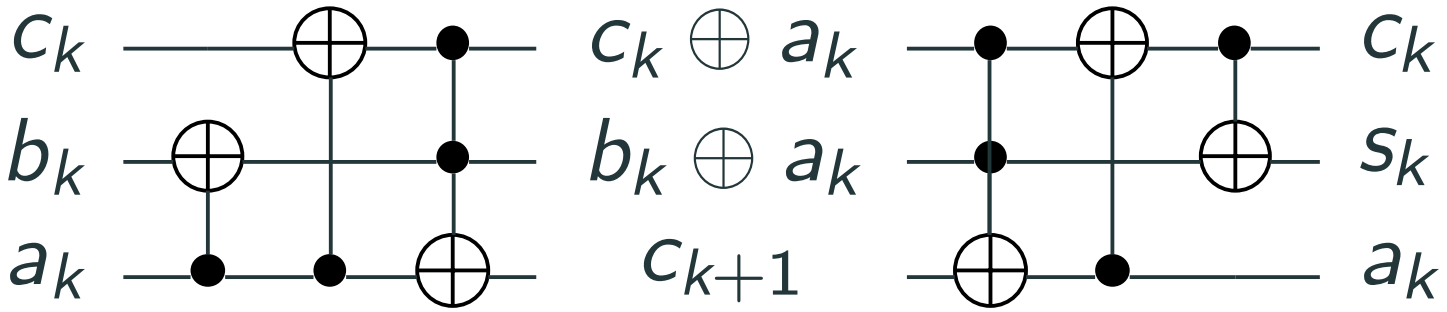
Can we do better?

Simplification

$$c_{k+1} = a_k b_k \oplus b_k c_k \oplus a_k c_k = (a_k \oplus b_k)(a_k \oplus c_k) \oplus a_k$$

$$s_k = a_k \oplus b_k \oplus c_k$$

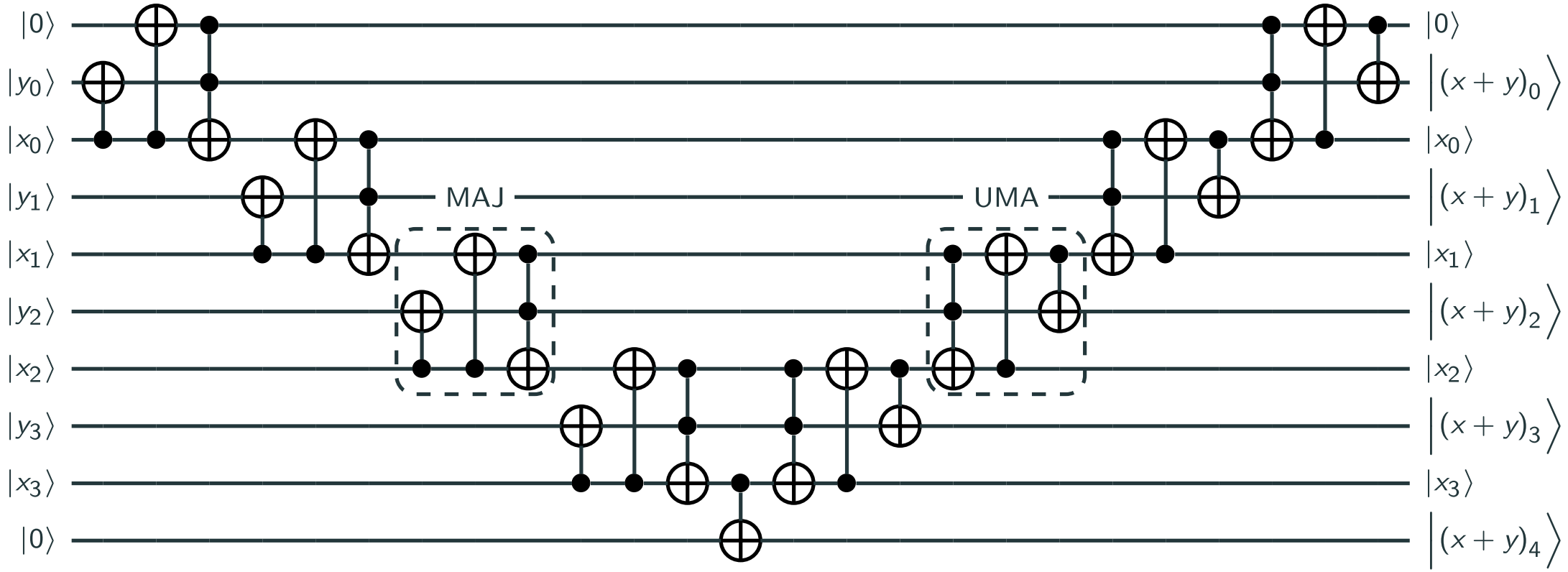
3-bits adder



Convention: left part = MAJ (MAJority); right part = UMA (UnMajority and Add)

Cuccaro et al. 2004. arXiv: quant-ph/0410184

Full Cuccaro's adder



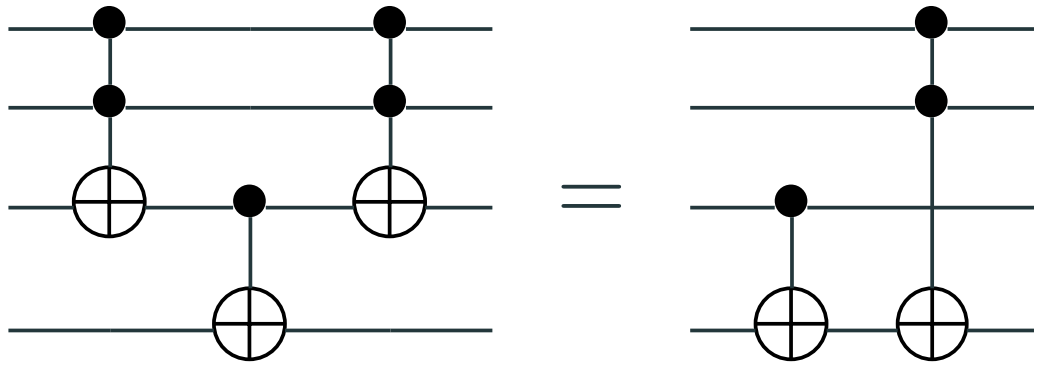
Improvements?

First qubit

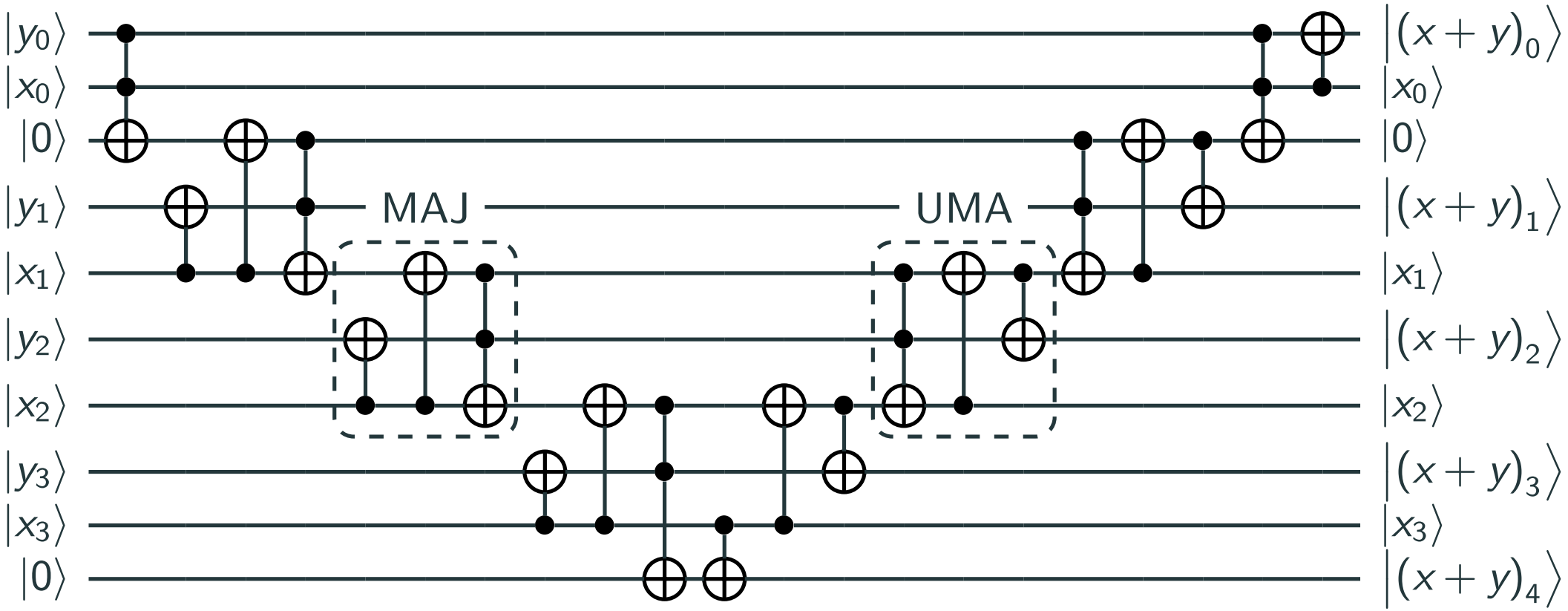
a_0	b_0	c_1	r_0
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

No need for full MAJ

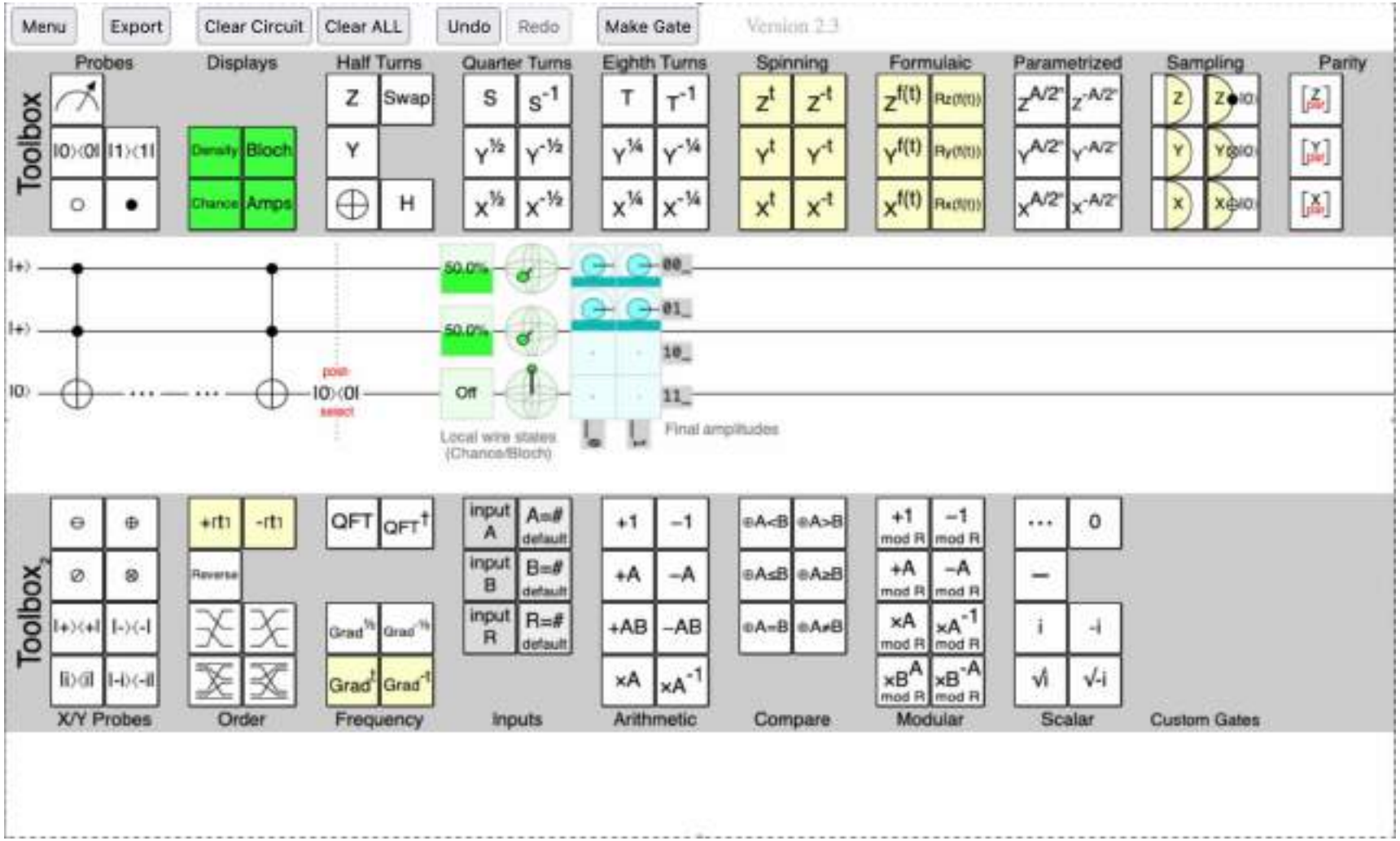
Last qubit



Improved Cuccaro adder

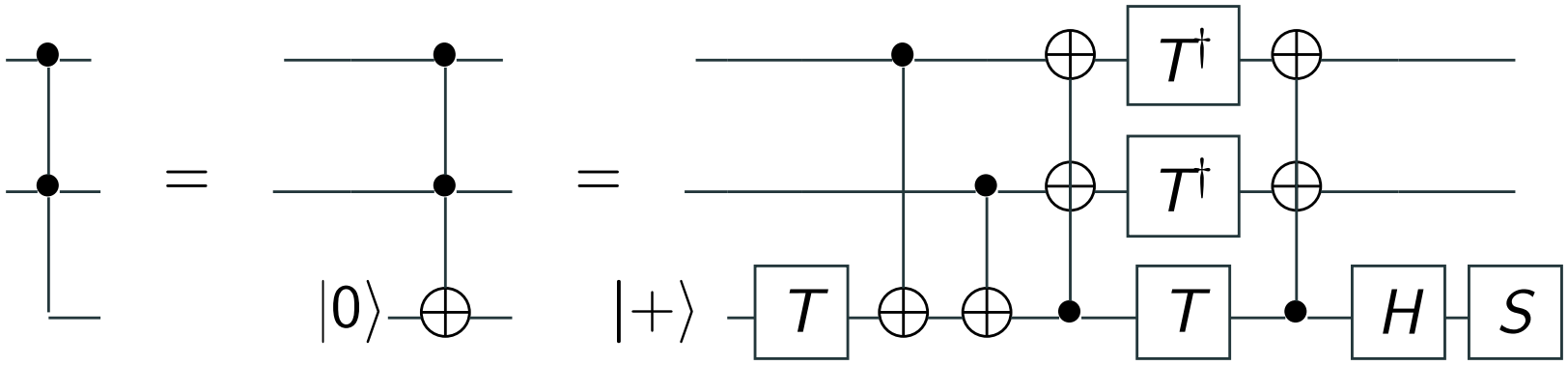


Measurement-based uncomputation

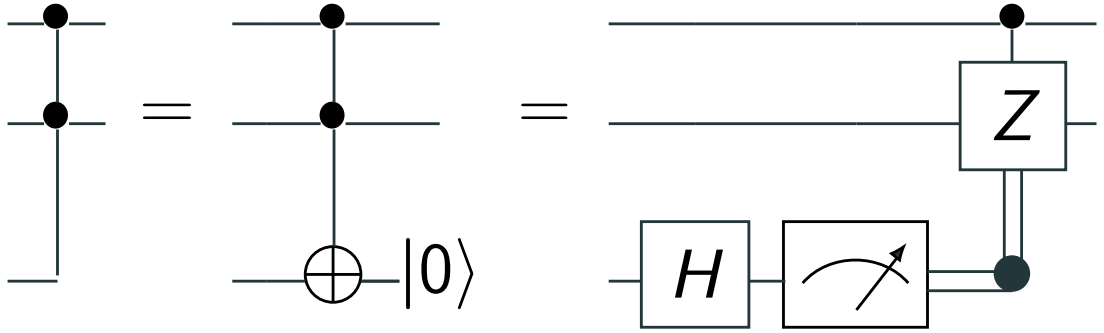


And operation

And: not Clifford



And†: Clifford



Craig Gidney, arXiv:1709.06648

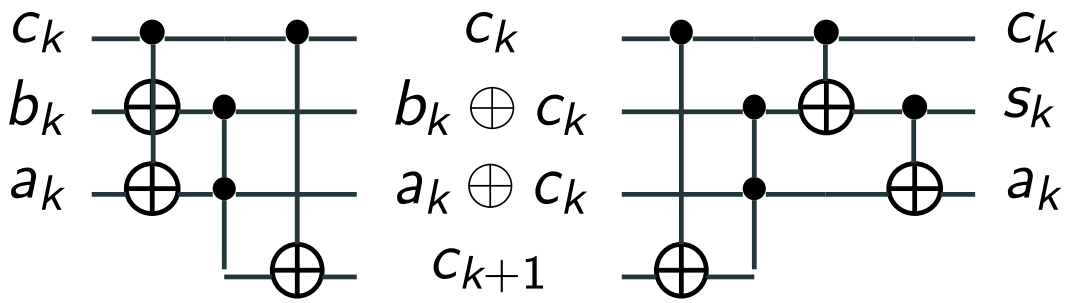
Gidney's adder elementary bloc

Alternative factorization

$$c_{k+1} = a_k b_k \oplus b_k c_k \oplus a_k c_k = (a_k \oplus c_k)(b_k \oplus c_k) \oplus c_k$$

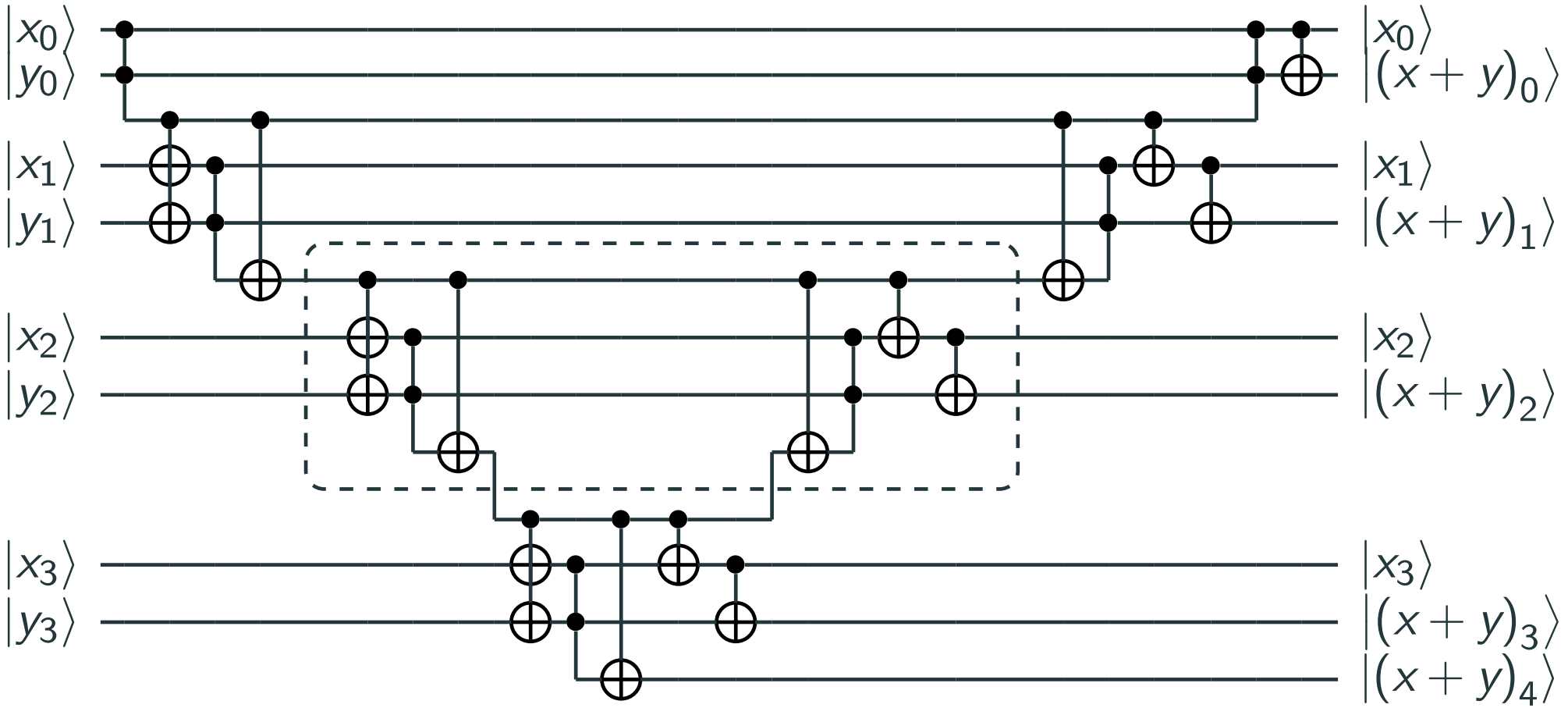
$$s_k = a_k \oplus b_k \oplus c_k$$

3-bit adder



Craig Gidney, arXiv:1709.06648

Gidney's adder



Craig Gidney, arXiv:1709.06648

Shor’s algorithm: 2019 version

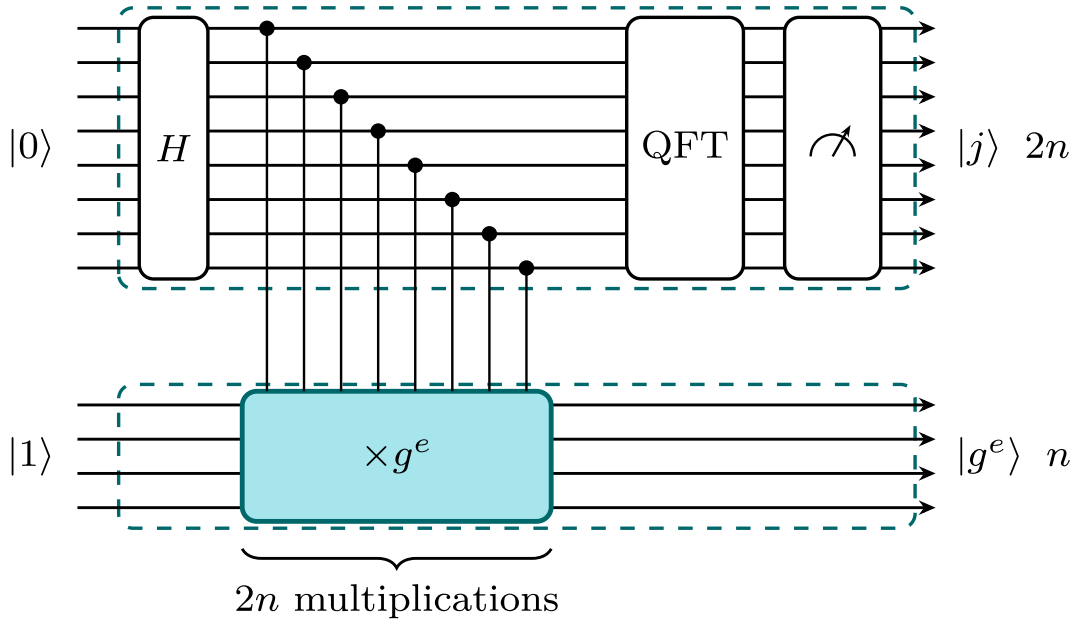
Ekerå and Håstad's algorithm

- pick up $g \in \mathbb{Z}_N^*$ randomly
- let r be the order of g (unknown): $g^r \equiv 1 \bmod N$
- let $h = g^{(N-1)/2}$
- Euler's totient function: $\varphi(N) = (p-1)(q-1)$
- $h \equiv g^{(p+q-2)/2} \bmod N$ (using Euler's theorem)
- hypothesis $r > (p+q-2)/2$
- $\log_g(h) = d \overset{\text{def}}{=} (p+q-2)/2$
- solve $N = p(2d+2-p)$
- take $q = 2d+2-p$

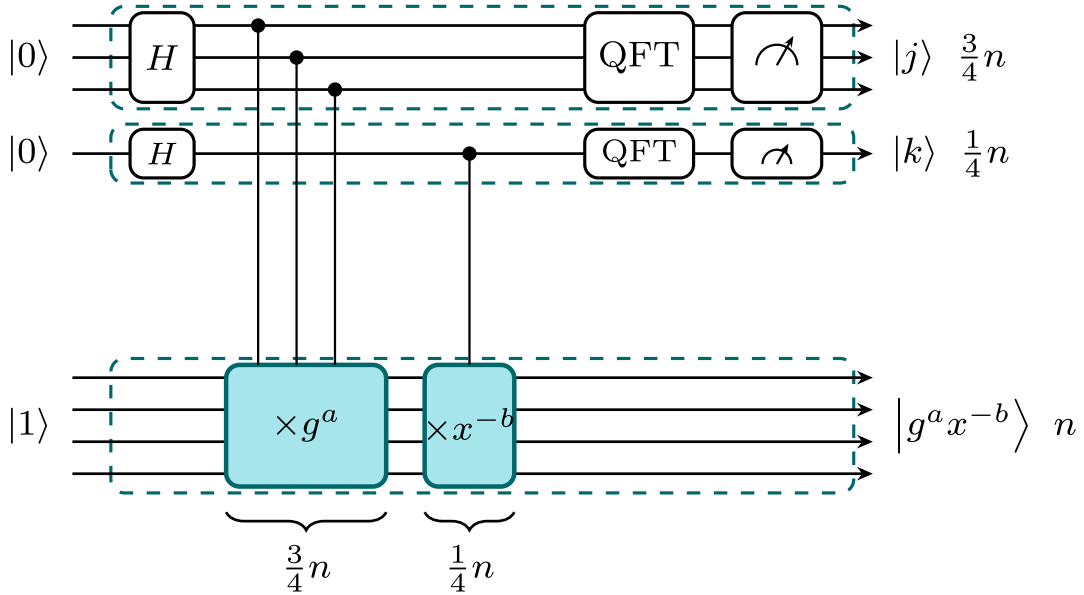
M. Ekerå and J. Håstad, "Quantum algorithms for computing short discrete logarithms and factoring RSA integers", Post-Quantum Cryptography, LNCS vol. 10346, Springer, 2017

Ekerå and Håstad's algorithm

Shor's algorithm



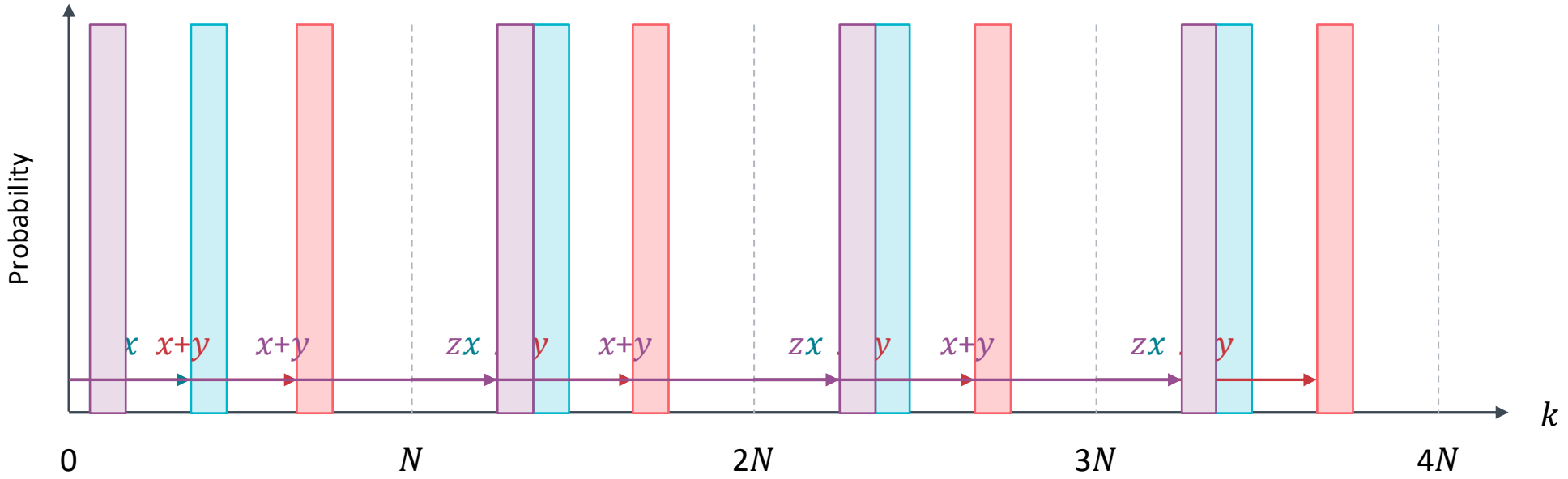
Ekerå and Håstad's algorithm



Coset representation of integers

x represented by

$$\frac{1}{\sqrt{2^c}} \sum_{i=0}^{2^c-1} |x + iN\rangle$$



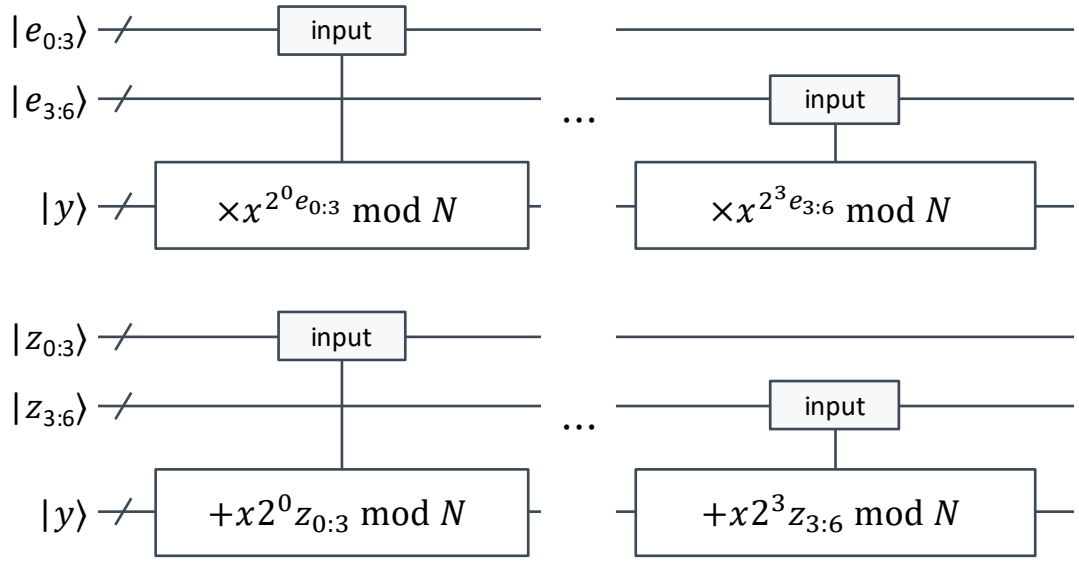
$$z = x + y \bmod N$$

Windowed arithmetic

Exponentiation

$$e = \sum_{0 \le i < n, i \equiv 0 \bmod w} 2^i e_{i:i+w}$$

$$x^e = \prod_{0 \le i < n, i \equiv 0 \bmod w} x^{2^i e_{i:i+w}}$$

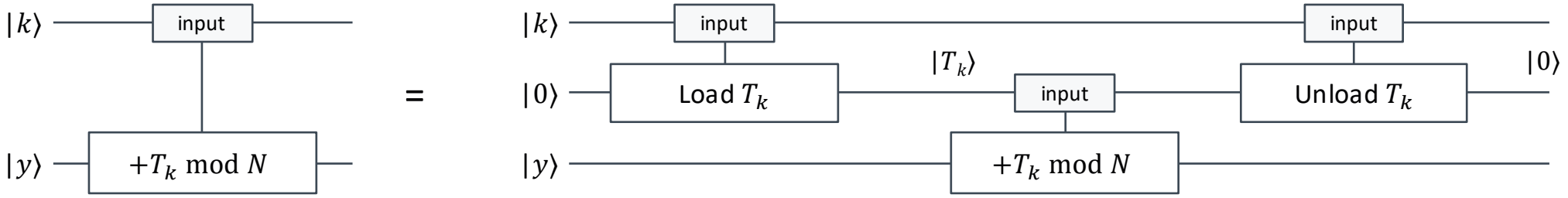


Multiplication

$$z = \sum_{0 \le i < n, i \equiv 0 \bmod w} 2^i z_{i:i+w}$$

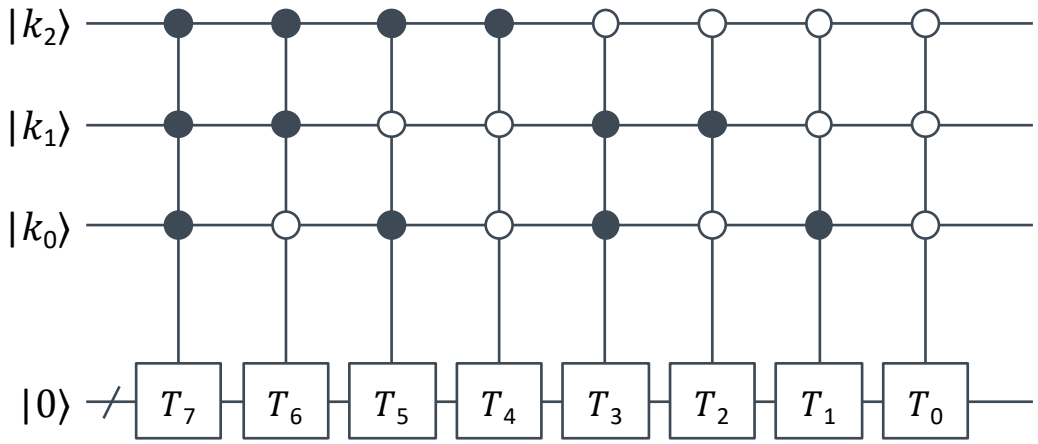
$$xz = \sum_{0 \le i < n, i \equiv 0 \bmod w} x2^i z_{i:i+w}$$

Lookup-addition



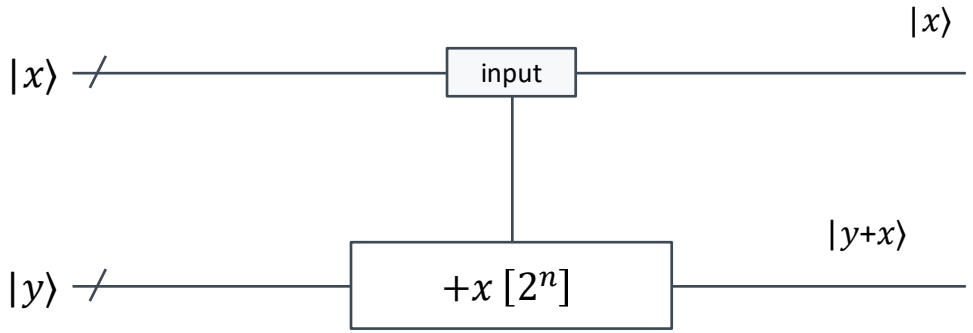
Windowed arithmetic: lookup and addition

Lookup table: $|k\rangle|0\rangle \mapsto |k\rangle|T_k\rangle$



● control on 1, ○ control on 0; each column XORs the classical value T_j into the output register

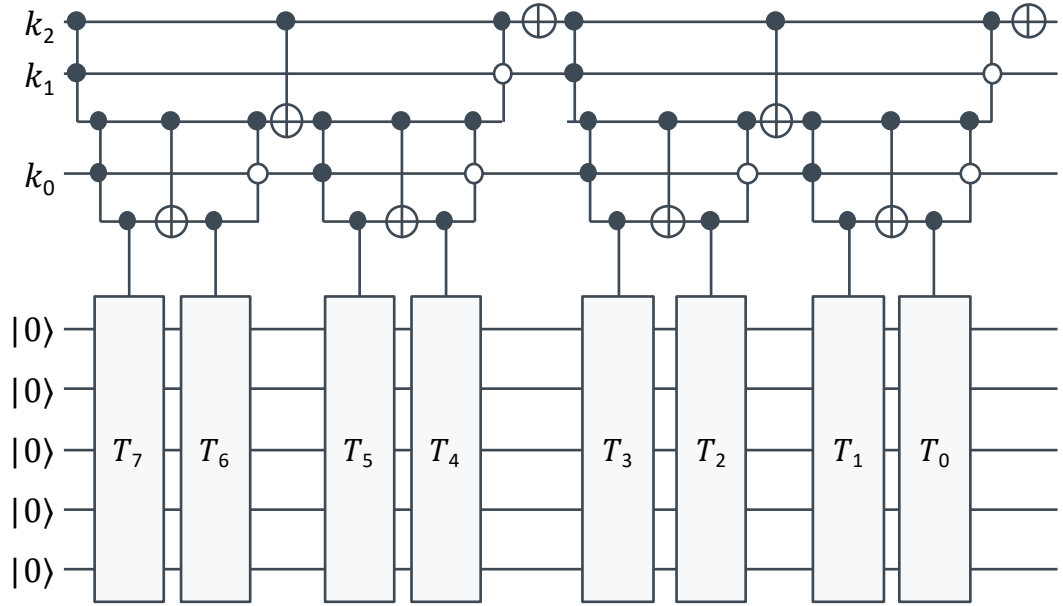
Addition: $|x\rangle|y\rangle \mapsto |x\rangle|x + y\ [2^n]\rangle$



Ripple-carry adder built from AND / de-AND gates (see appendix)

Windowed arithmetic: full lookup and addition circuits

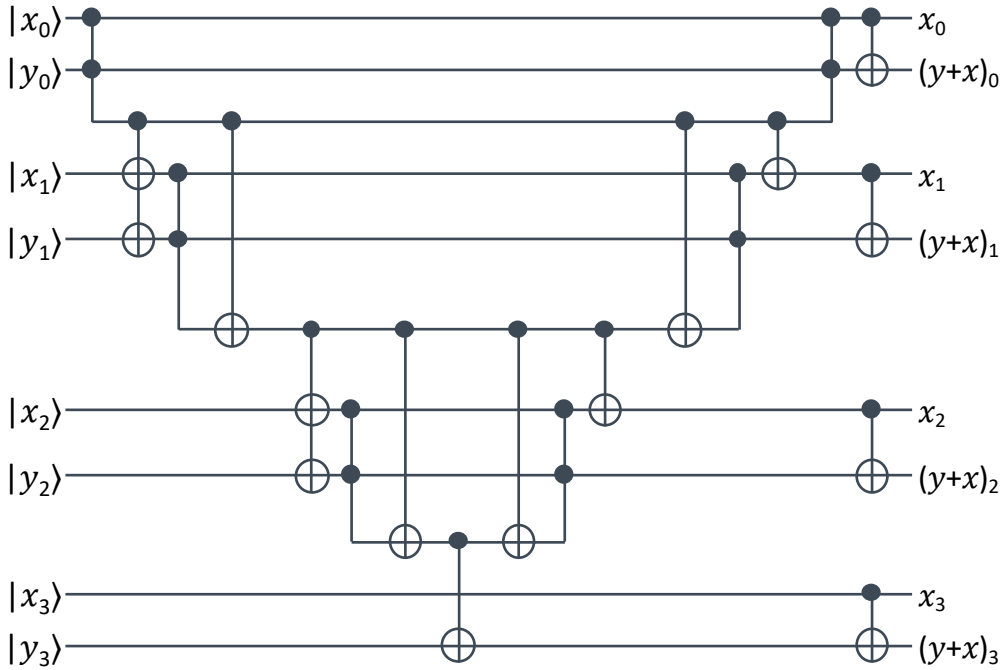
Lookup table: $|k\rangle|0\rangle \mapsto |k\rangle|T_k\rangle$



AND / de-AND notation



Addition: $|x\rangle|y\rangle \mapsto |x\rangle|x + y\ [2^n]\rangle$



T_k boxes stand for the data-dependent CNOTs that write T_k into the output register.

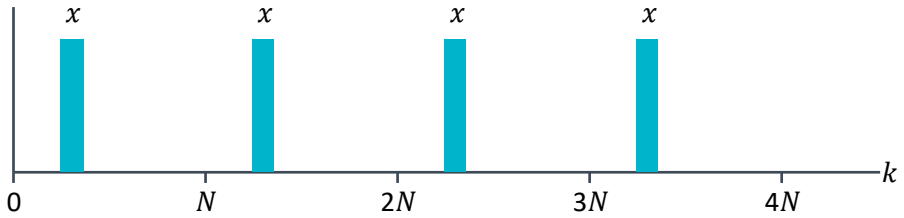
Advanced algorithm complexity

Ekerå and Håstad's algorithm

Size of the exponent: $1.5n$ instead of $2n$ for Shor's algorithm

Modular addition through coset representation

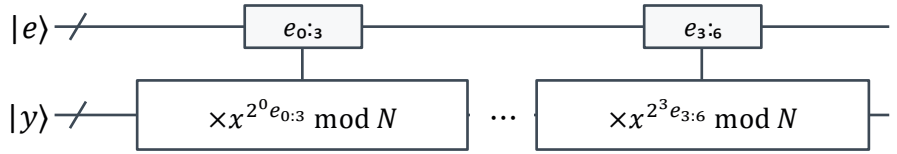
x represented by $\frac{1}{\sqrt{2^c}} \sum_{i=0}^{2^c-1} |x + iN\rangle$



C. Gidney, "Approximate encoded permutations and piecewise quantum adders", 2019

Windowed arithmetic circuits

Exponentiation example: $x^e = \prod_{0 \le i < n, i \equiv 0 \bmod w} x^{2^i e_{i:i+w}}$



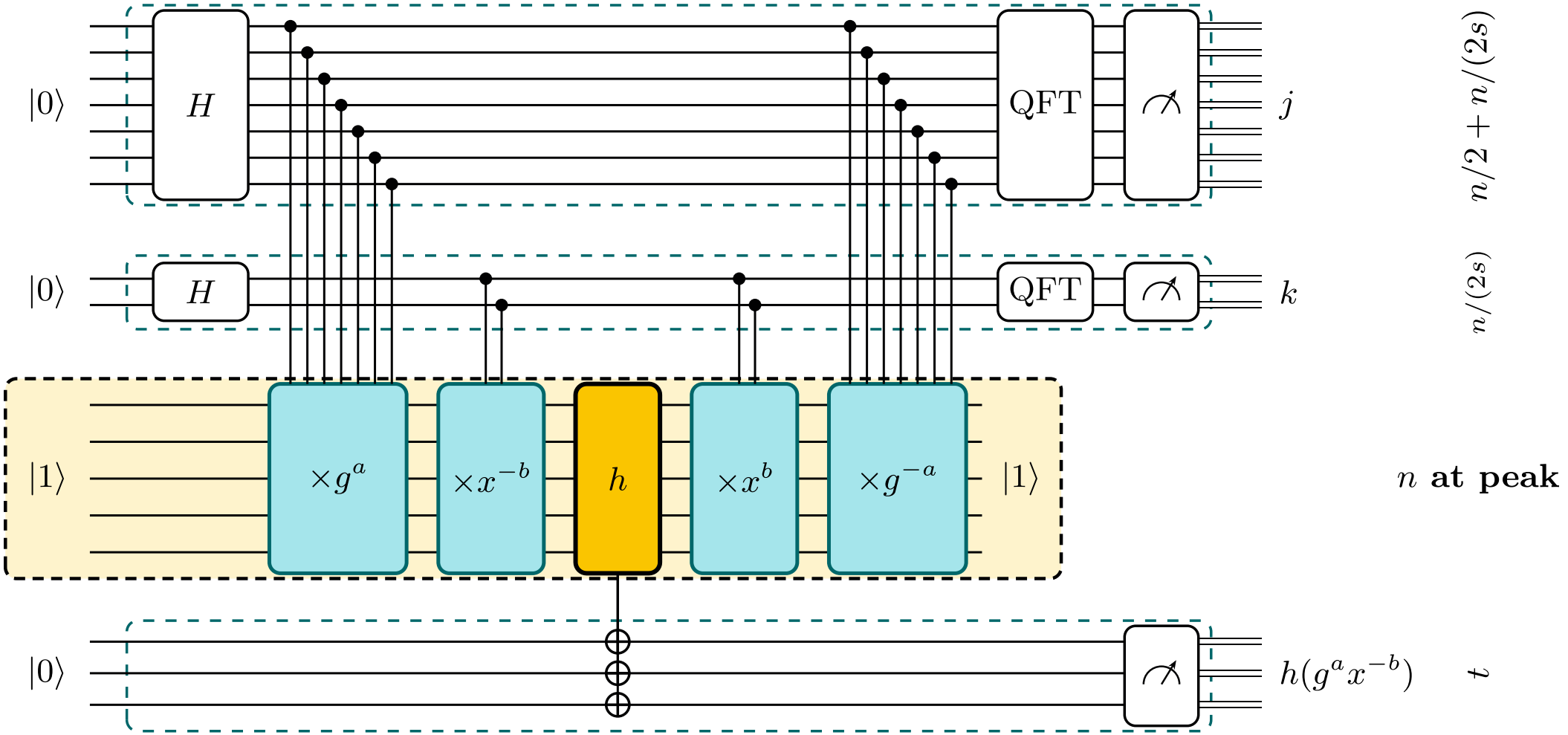
C. Gidney, "Windowed quantum arithmetic", 2019

Complexity: parallel depth $O\left(\frac{n^2(n+2^{2w})}{w^2}\right)$, gates $O\left(\frac{n^3 2^{2w}}{w^2}\right)$; choice: $w = O(1)$

$\Rightarrow O(n^3)$, but better pre-factors than for controlled arithmetic

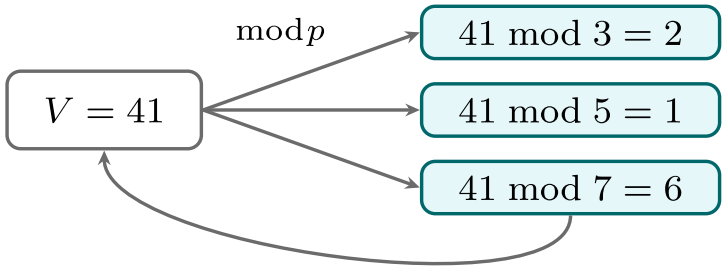
Shor’s algorithm: 2026 version

May–Schlieper algorithm



Chevignard–Fouque–Schrottenloher algorithm

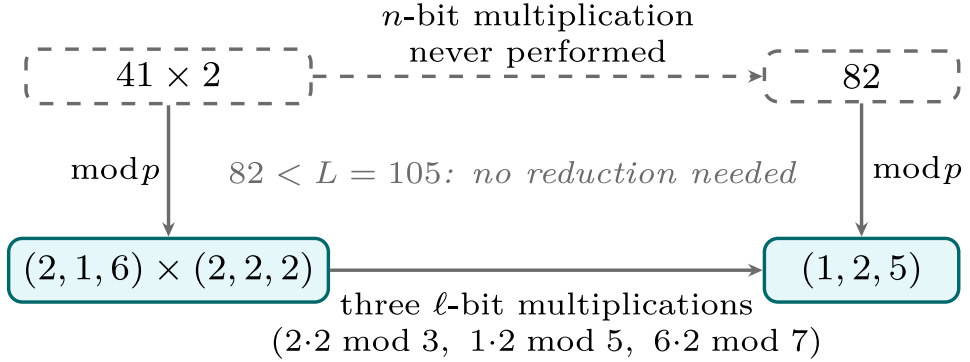
1. Chinese remainder theorem: a number is its residues



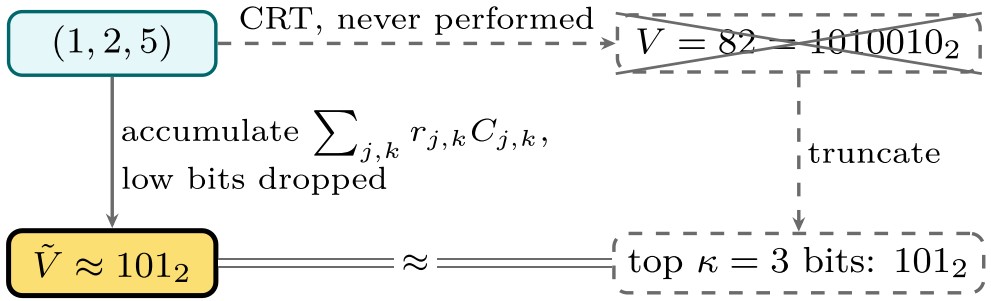
each residue fits in ℓ bits, here $\ell = 3$

back, with the CRT: $V = (2 \cdot 70 + 1 \cdot 21 + 6 \cdot 15) \bmod 105 = 41$

2. Arithmetic runs lane by lane: the diagram commutes



3. Keep only the top bits: the diagram commutes approximately

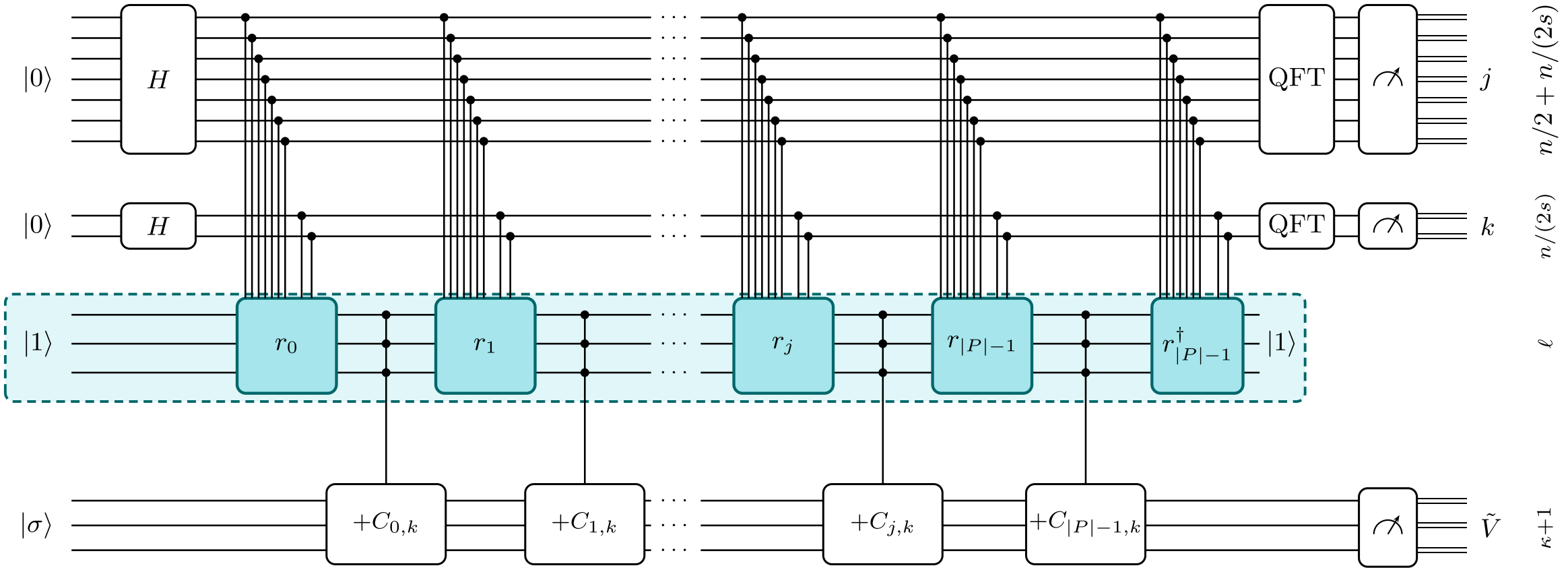


error $O(|P|\,\ell\,2^{-\kappa})$, with $\kappa = O(\log n)$

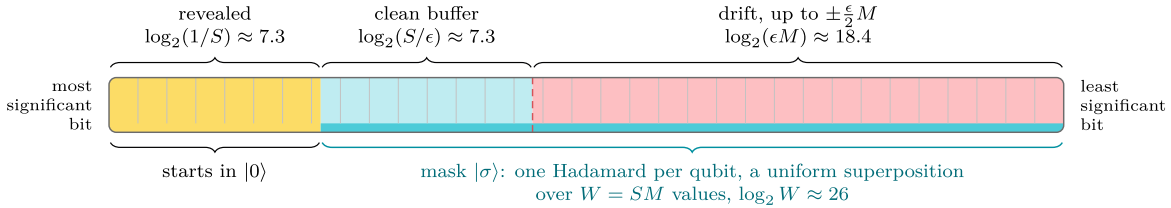
Legend

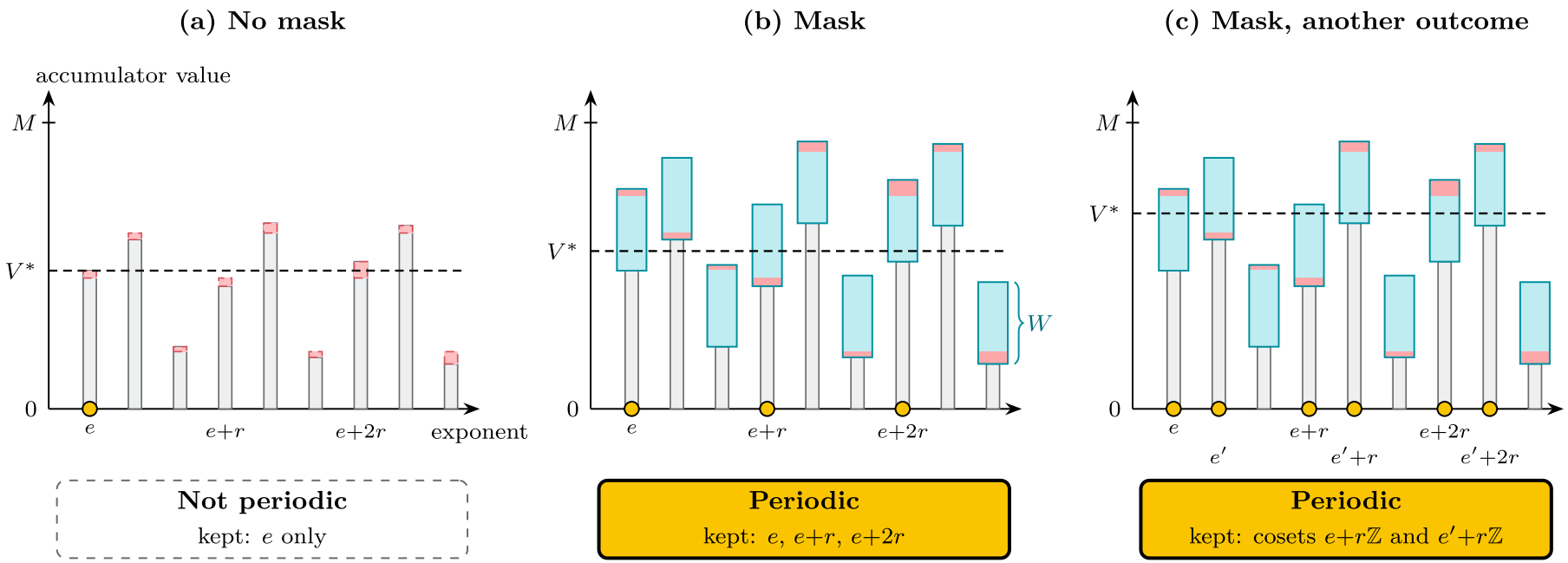
- ℓ-bit residues
- top κ bits, kept
- never formed
- never performed

Gidney's version



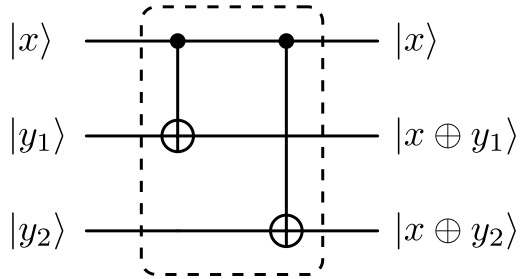
Superposition masking





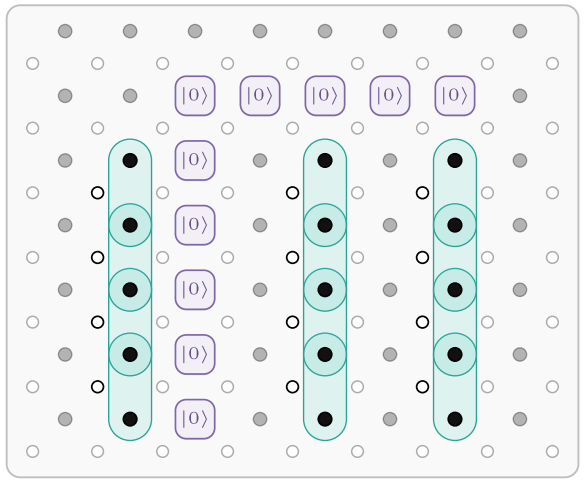
Cat qubits implementation

Multi-target CNOT

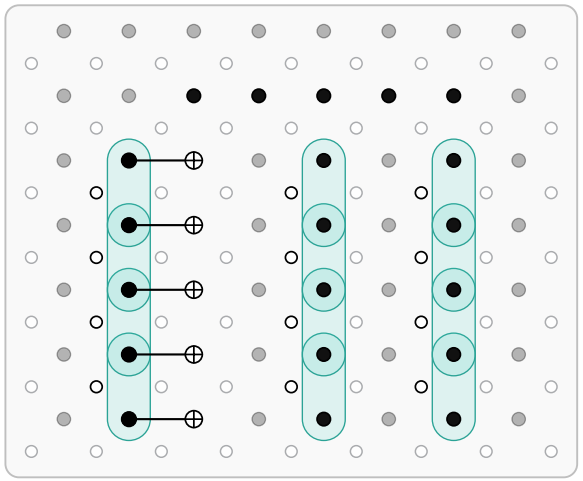


Multi-target CNOT

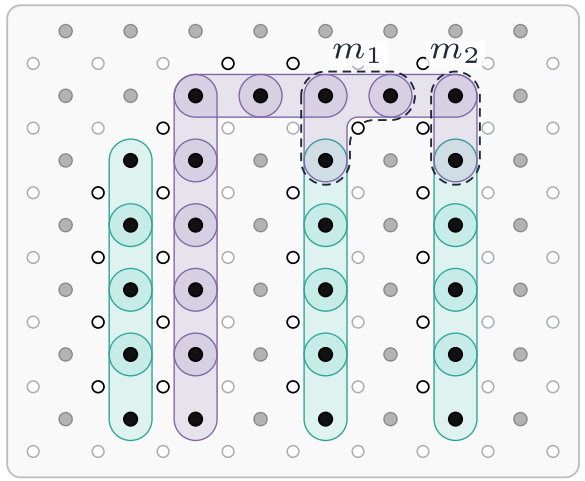
(i) Auxiliary qubits in $|0\rangle_L$



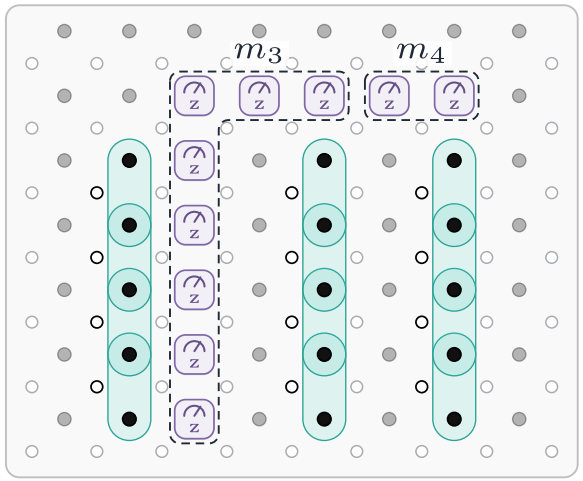
(ii) Transversal CNOT gate



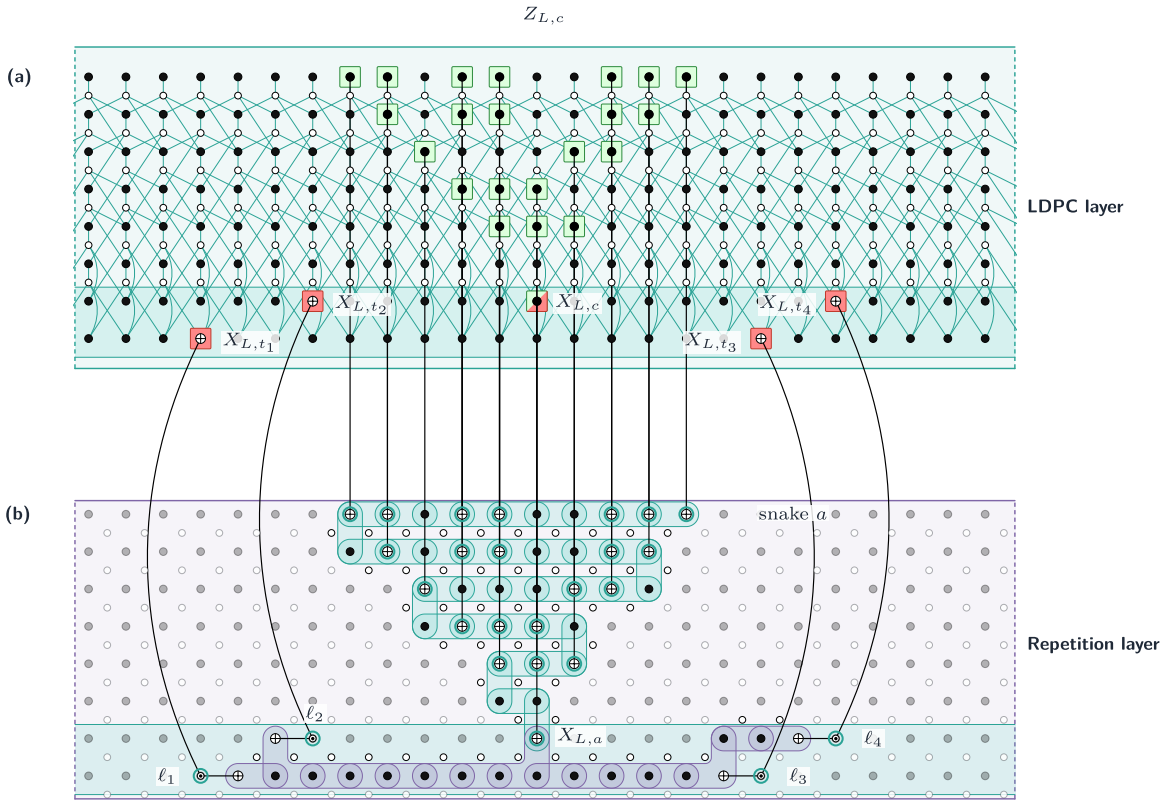
(iii) $M_{X_L X_L X_L} : m_1$, $M_{X_L X_L} : m_2$



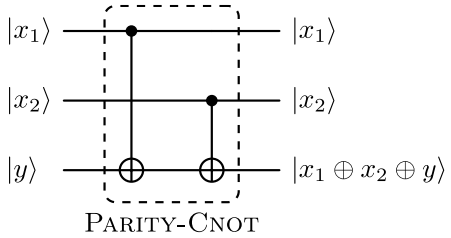
(iv) $M_{Z_L} : m_3$, m_4

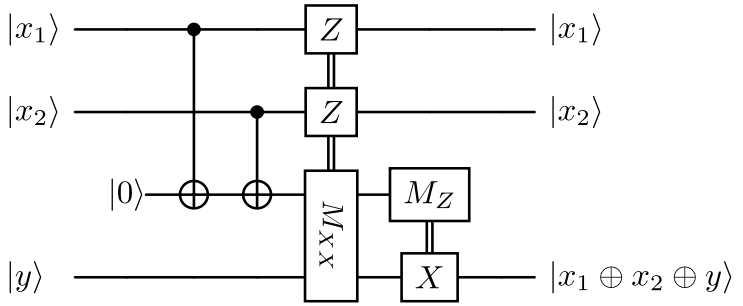


Multi-target CNOT

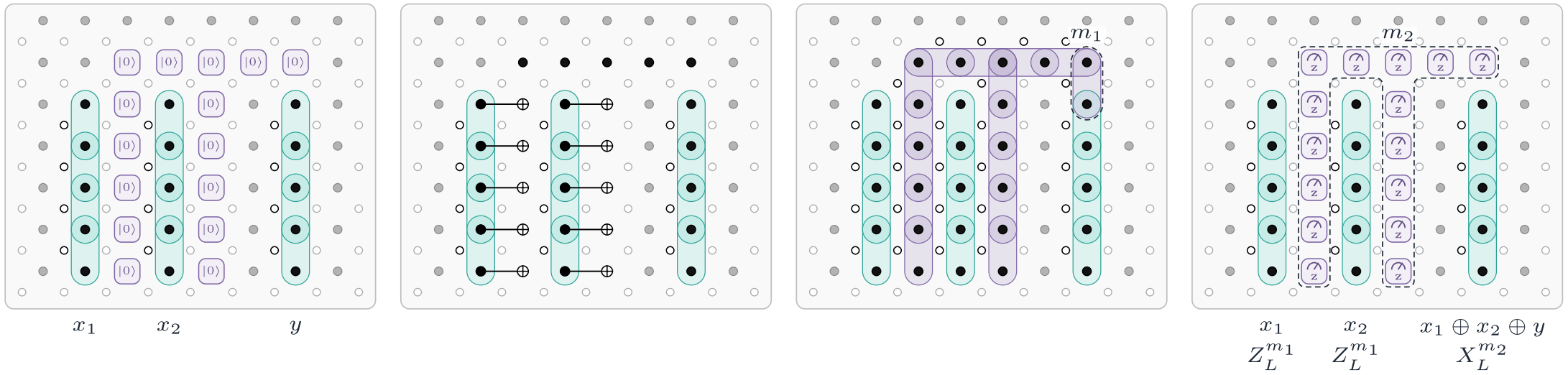


Parity CNOT

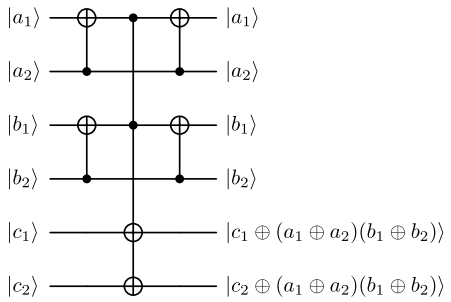


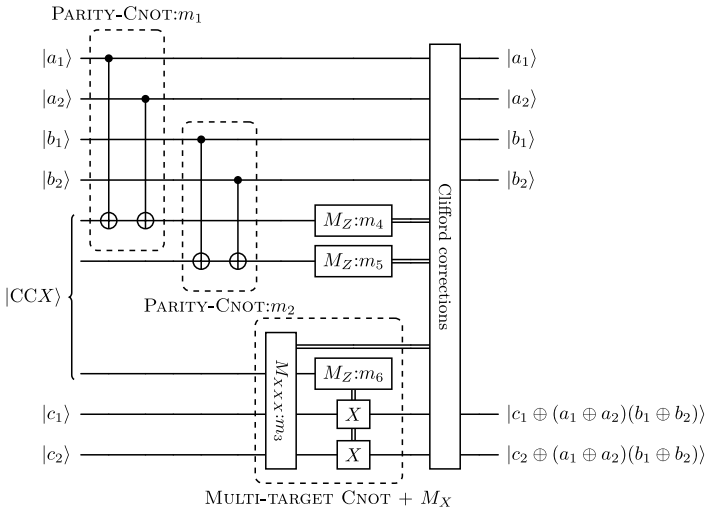


(i) Auxiliary qubit in $|0\rangle_L$ (ii) Transversal Cnot gates (iii) $M_{X_L X_L} : m_1$ (iv) $M_{Z_L} : m_2$

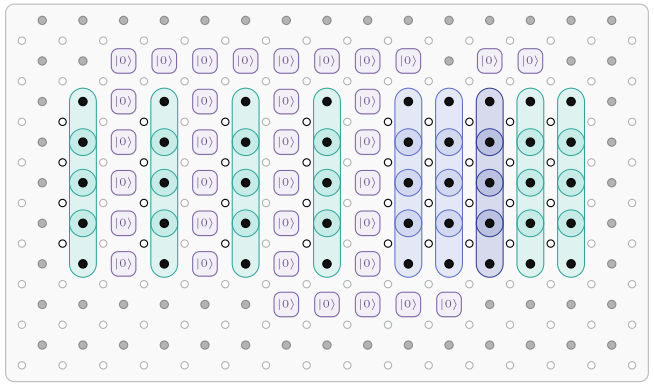


Active injection

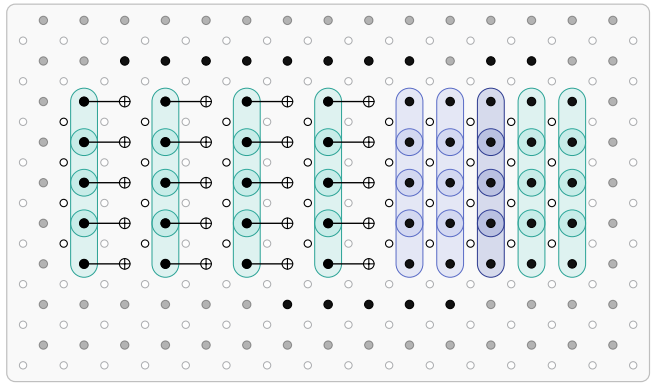




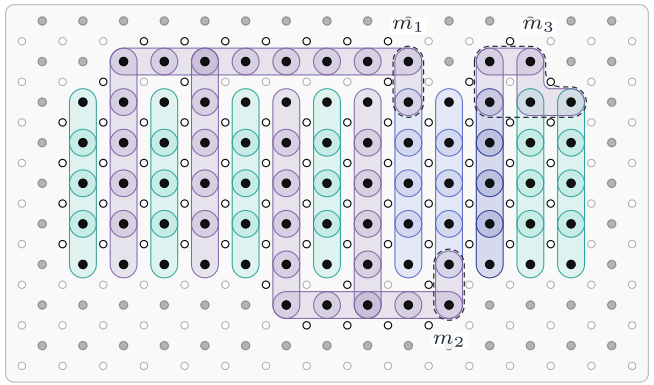
(i) Auxiliary qubits in $|0\rangle_L$



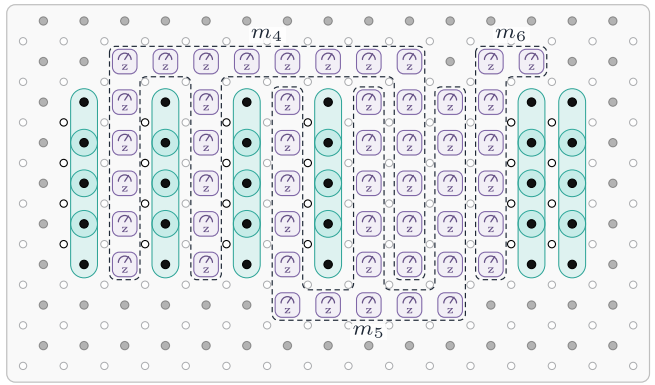
(ii) Transversal Cnot gates



(iii) $M_{X_L X_L}: m_1$, m_2, $M_{X_L X_L X_L}: m_3$



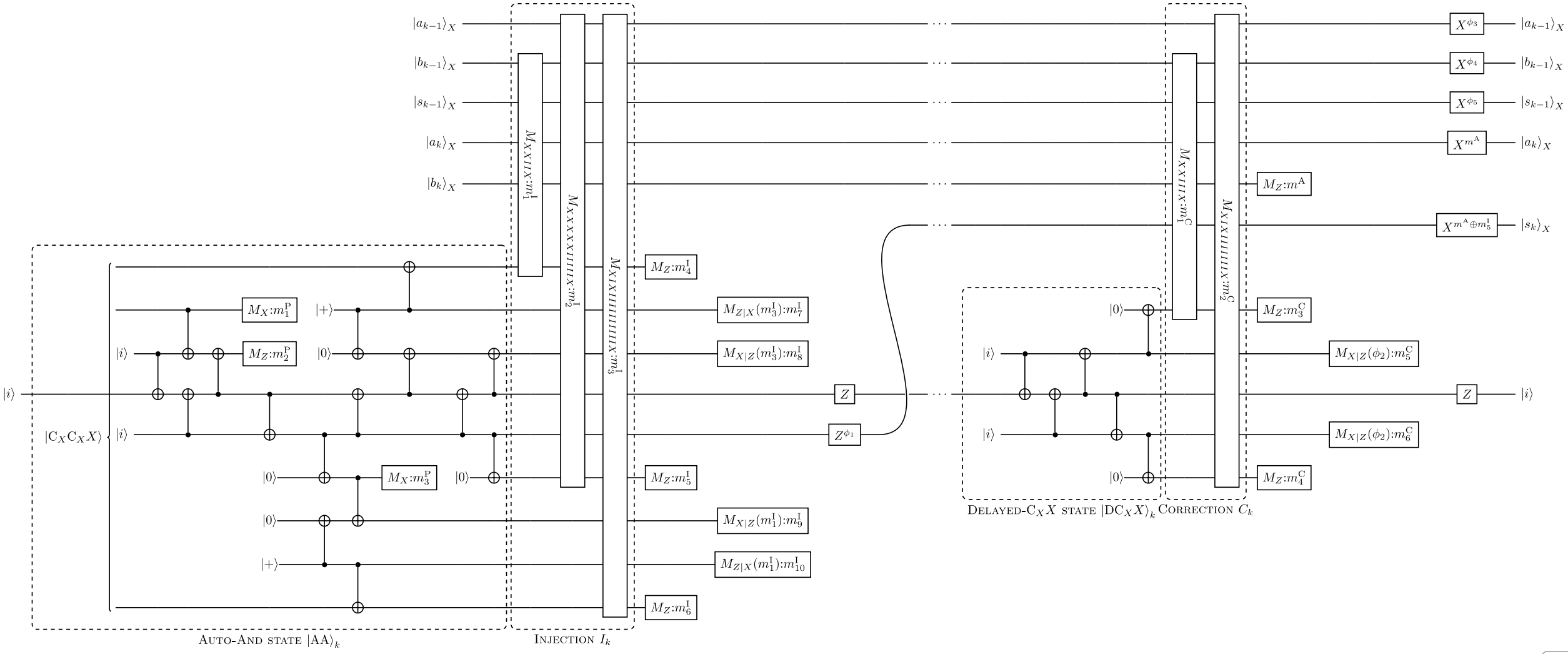
(iv) $M_{Z_L}: m_4$, m_5, m_6



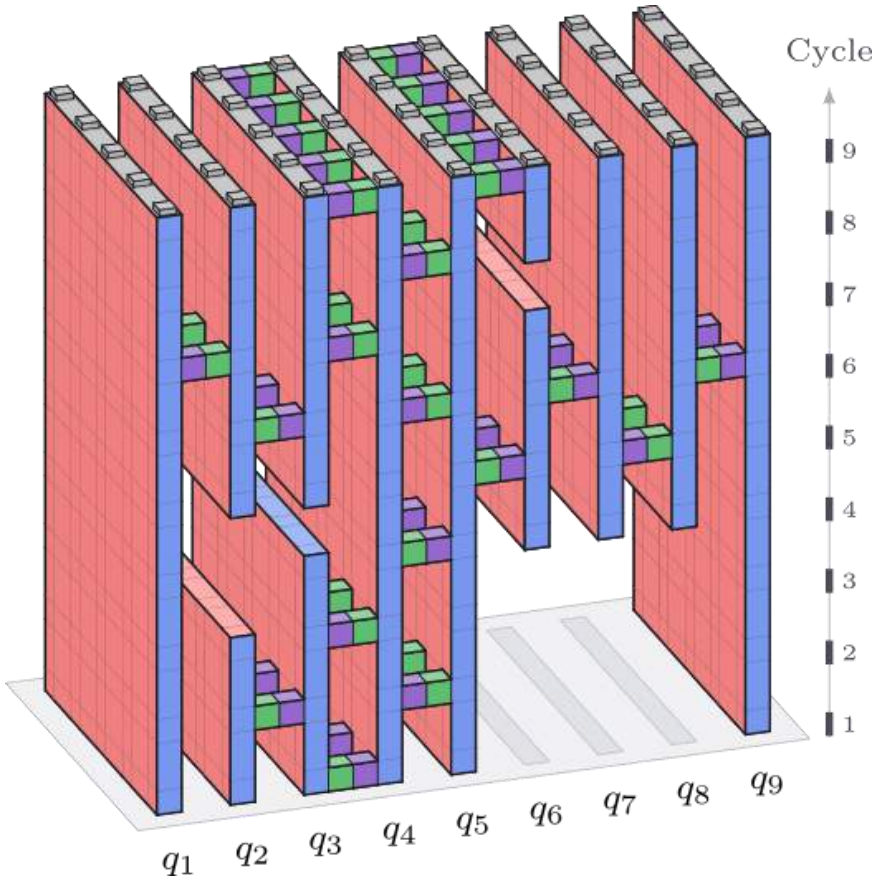
a_1 a_2 b_1 b_2 $c_j \oplus (a_1 \oplus a_2)(b_1 \oplus b_2)$
$Z_L^{m_1}$ $Z_L^{m_1}$ $Z_L^{m_2}$ $Z_L^{m_2}$ $X_L^{m_6}$

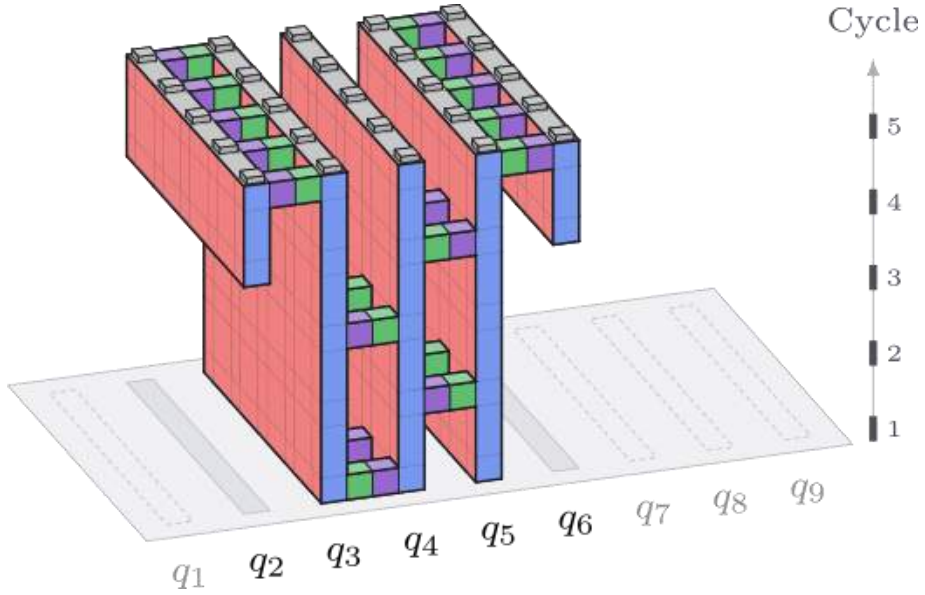


Adder

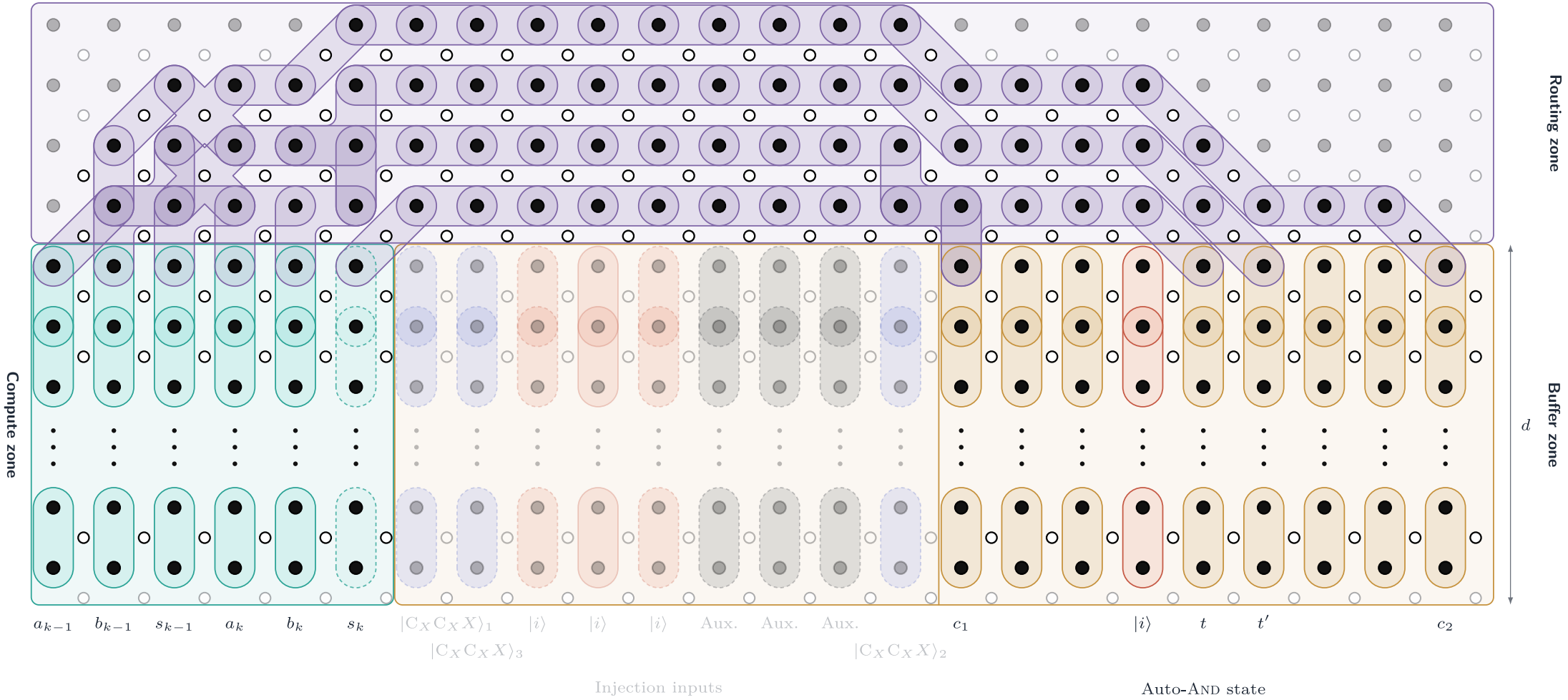

$|a_{k-1}\rangle_X$
$|b_{k-1}\rangle_X$
$|s_{k-1}\rangle_X$
$|a_k\rangle_X$
$|b_k\rangle_X$
$M_{XXIIX}:m_1^{\mathrm{I}}$
$M_{XXXXXXIIIIX}:m_2^{\mathrm{I}}$
$M_{XIXIIIIIIIIX}:m_1^{\mathrm{I}}$
$M_Z:m_4^{\mathrm{I}}$
$M_{Z|X}(m_3^{\mathrm{I}}):m_7^{\mathrm{I}}$
$M_{X|Z}(m_3^{\mathrm{I}}):m_8^{\mathrm{I}}$
Z
Z^{ϕ_1}
$M_Z:m_5^{\mathrm{I}}$
$M_{X|Z}(m_1^{\mathrm{I}}):m_9^{\mathrm{I}}$
$M_{Z|X}(m_1^{\mathrm{I}}):m_{10}^{\mathrm{I}}$
$M_Z:m_6^{\mathrm{I}}$
$|i\rangle$
$|\mathrm{C}_X\mathrm{C}_X X\rangle$
$M_X:m_1^{\mathrm{P}}$
$M_Z:m_2^{\mathrm{P}}$
$M_X:m_3^{\mathrm{P}}$
$|+\rangle$
$|0\rangle$
Auto-And state $|\mathrm{AA}\rangle_k$
Injection I_k
$M_{XXXIIX}:m_1^{\mathrm{C}}$
$M_{XIXIIIIIIIX}:m_2^{\mathrm{C}}$
$M_Z:m^{\mathrm{A}}$
$M_Z:m_3^{\mathrm{C}}$
$M_{X|Z}(\phi_2):m_5^{\mathrm{C}}$
$M_{X|Z}(\phi_2):m_6^{\mathrm{C}}$
$M_Z:m_4^{\mathrm{C}}$
Delayed-$\mathrm{C}_X X$ state $|\mathrm{DC}_X X\rangle_k$
Correction C_k
X^{ϕ_3}
X^{ϕ_4}
X^{ϕ_5}
$X^{m^{\mathrm{A}}}$
$X^{m^{\mathrm{A}}\oplus m_5^{\mathrm{I}}}$

Auto-And and delayed-CXX state

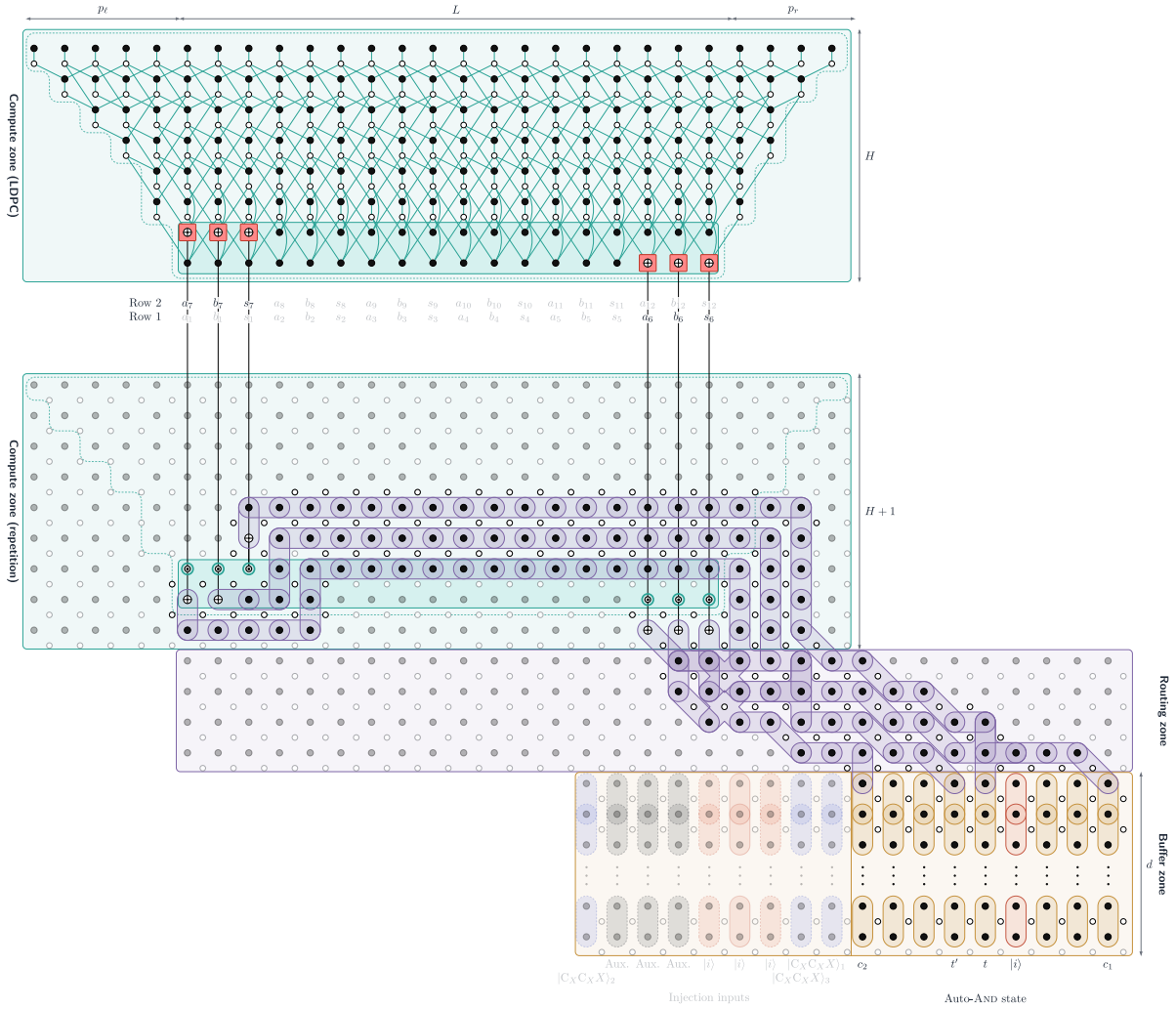




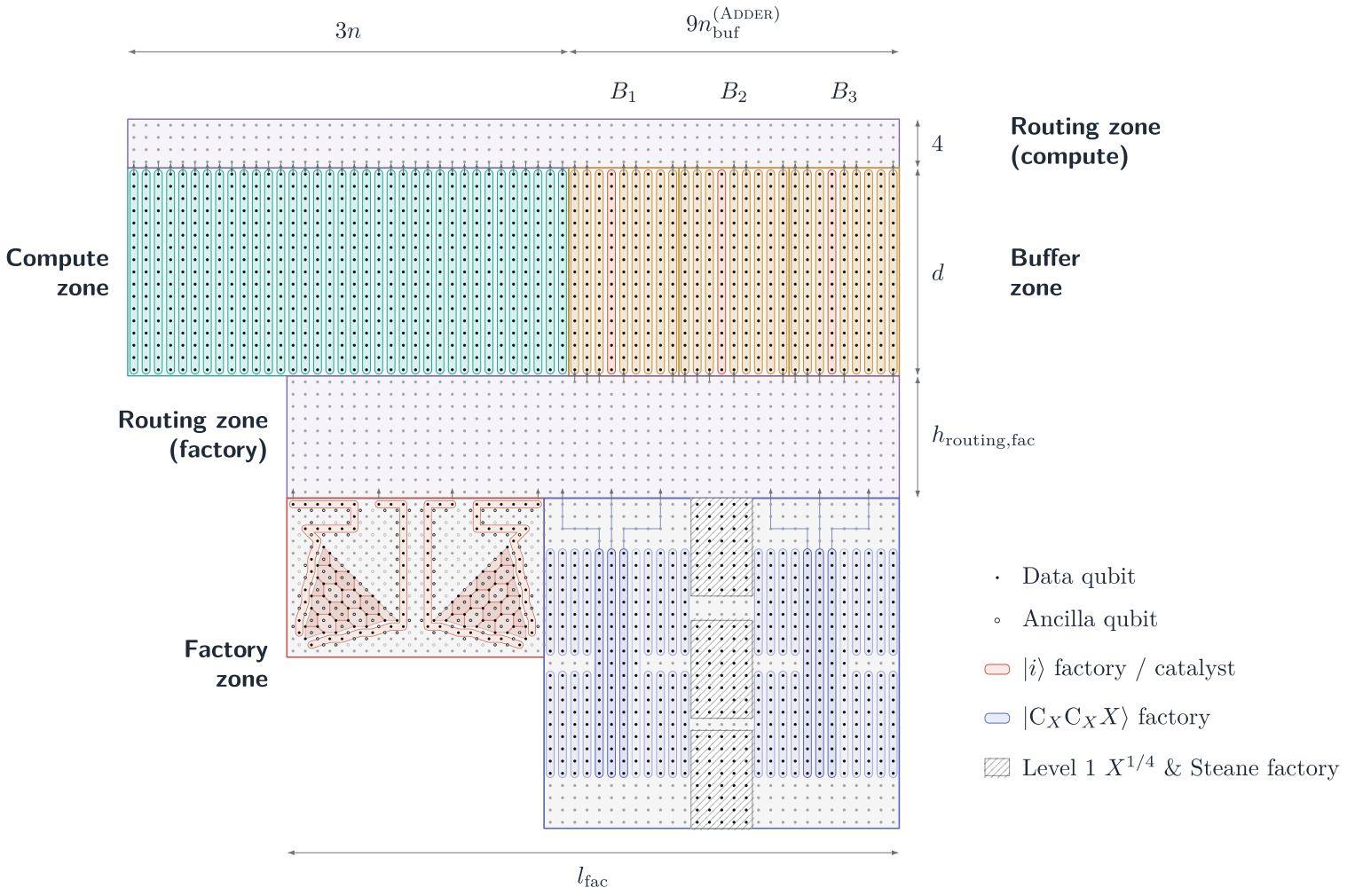
Adder injection



Adder injection for LDPC

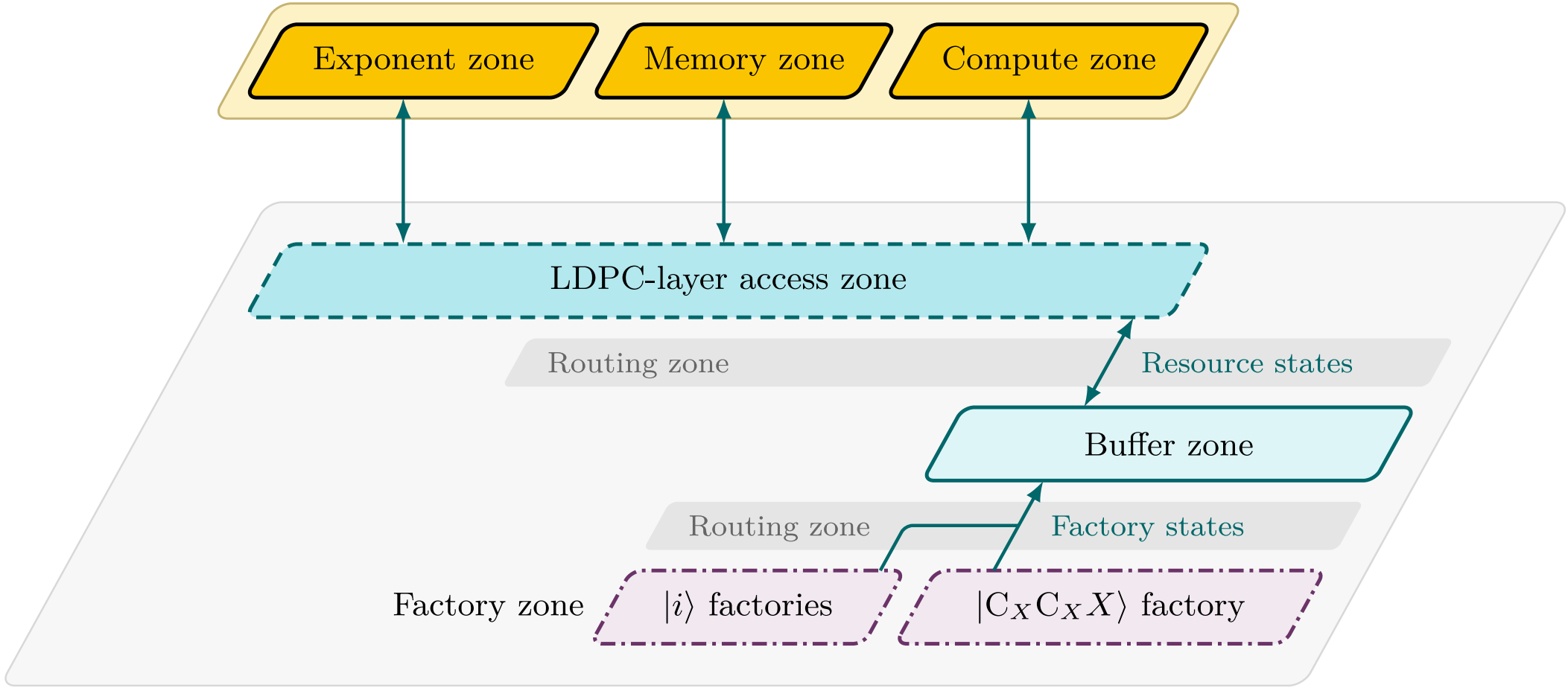


Global layout



Global layout

LDPC layer LDPC-cat code block of distance d_{LDPC} for storing the registers



Repetition layer Repetition codes of distance d_{rep} for access, routing, buffers and factories

arXiv: 2610.37839

Shor's algorithm with cat qubits

Logical and physical resources to break RSA-2048, ECDLP-256 and FFDLP-512

Configuration	RSA-2048 (Factoring)		ECDLP-256[1] (Bitcoin secp256k1)		FFDLP-512 (Baby Shor)	
	Cat qubits	Duration	Cat qubits	Duration	Cat qubits	Duration
Balanced (Reference, compiled in full for RSA)	22 593	3.14 days	29 588	61.8 min	6 656	21.2 min
Less qubits (Smaller, slower magic-state factory)	21 188	8.08 days	28 183	146 min	5 251	58.5 min
Faster[2] (10 machines running in parallel)	610 530	1.25 hours	–	–	66 560	2.6 min
Balanced configuration	Logical resources		Logical resources		Logical resources	
Logical qubits (Encoded in the LDPC-cat code)	1 433		1 462		208	
Toffoli gates (Per shot)	$2^{29.5} \approx 7.6 \times 10^8$		$2^{25.8} \approx 5.8 \times 10^7$		$2^{22.2} \approx 4.8 \times 10^6$	
Time per shot (One run of the circuit)	7.84 h		60 min		2.51 min	
Shots[3] (Expected number of runs)	9.60		1.03		8.44	

[1] Upper bound, reusing the RSA-2048 subroutines. [2] RSA-2048: 10 identical chips, each running 7 residue engines that share one exponent register. FFDLP-512: shots run in parallel on 10 identical chips.
[3] Balanced duration = time per shot × shots. All figures: LDPC-cat architecture, $p_Z = 5 \times 10^{-4}$, negligible bit flips.

07

Conclusion

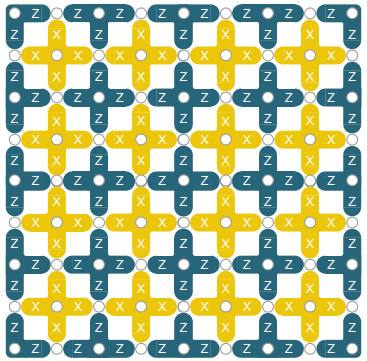
Just the beginning

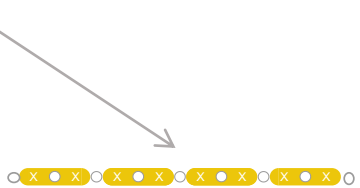
Origin of hardware efficiency

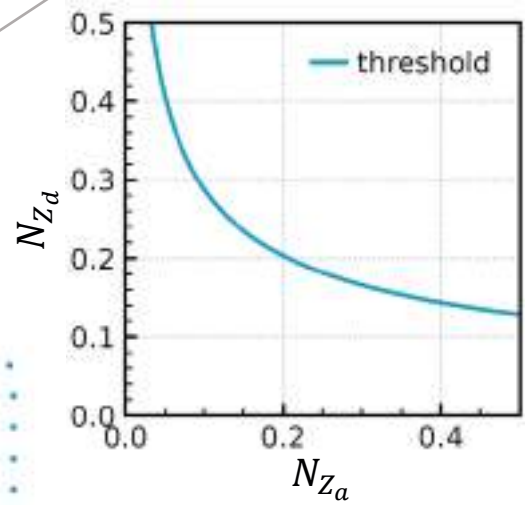
1. Classical codes are sufficient

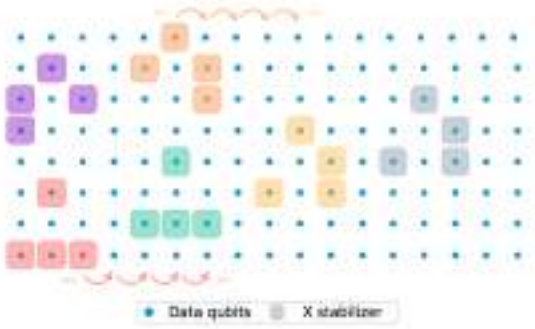
2. High threshold

3. LDPC codes can be local





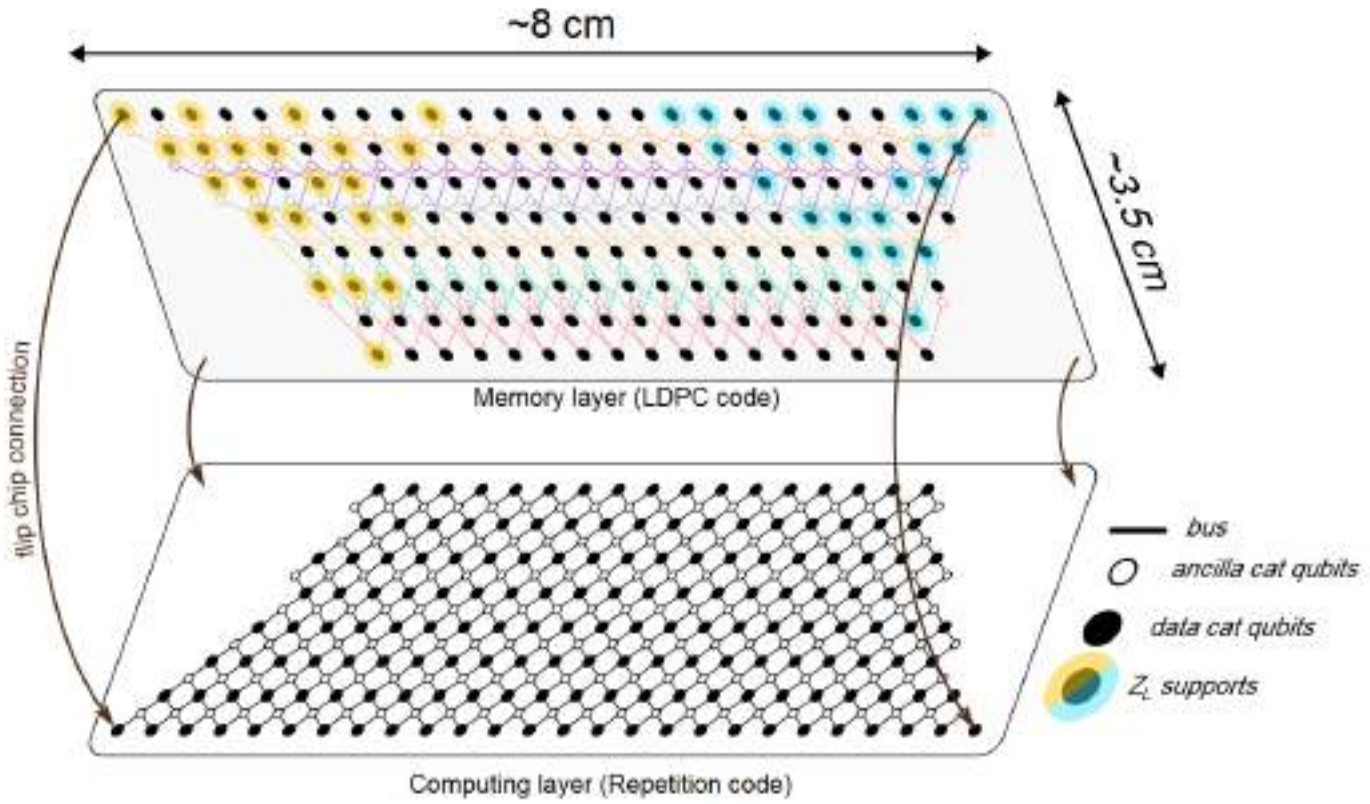




Fowler et al. PRA 86 (2012)
D. Ruiz et al. arXiv:2401.09541 (2024)

Towards a 100 logical qubits processor, And beyond

Flip-chip architecture



100 logical qubits
[429, 100, 22] code
10^{-8} logical error rate

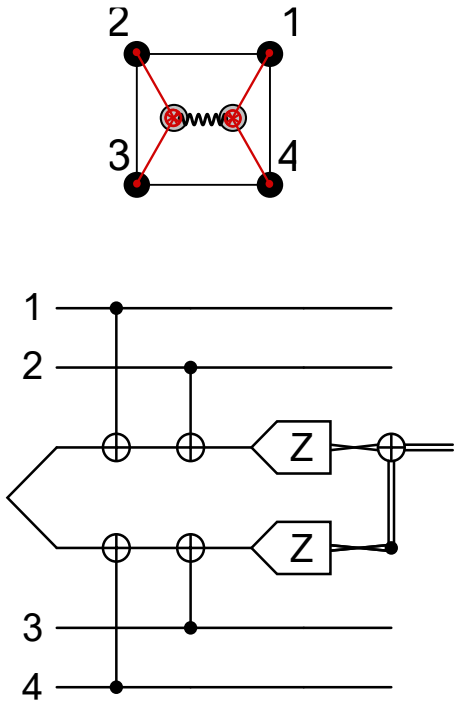
Theoretical targets
$\kappa_1/\kappa_2 = 10^{-4}$
$T_{\text{bit-flip}} = 13$ minutes
Bias-preserving CNOT

Current state of the art
$\kappa_1/\kappa_2 = 6.5\times10^{-3}$
$T_{\text{bit-flip}} = 15$ seconds
CNOT gate WIP

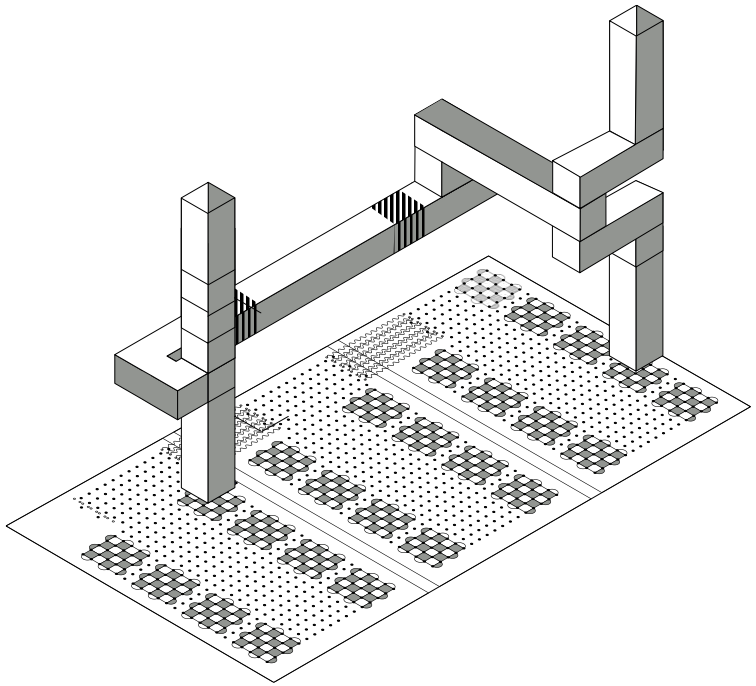
2048-bit factorization
Less than 100 000 cats
[24885, 6214, 22] code

Distributed architecture

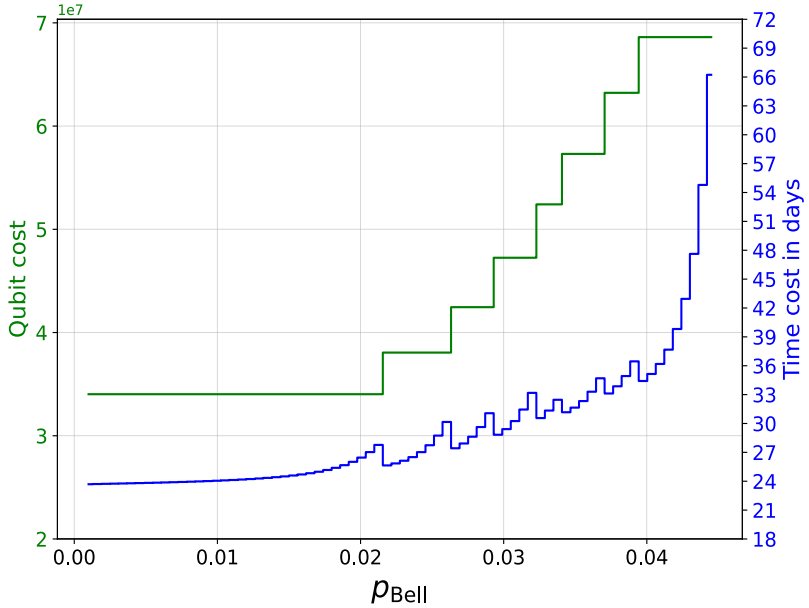
Measurement teleportation:



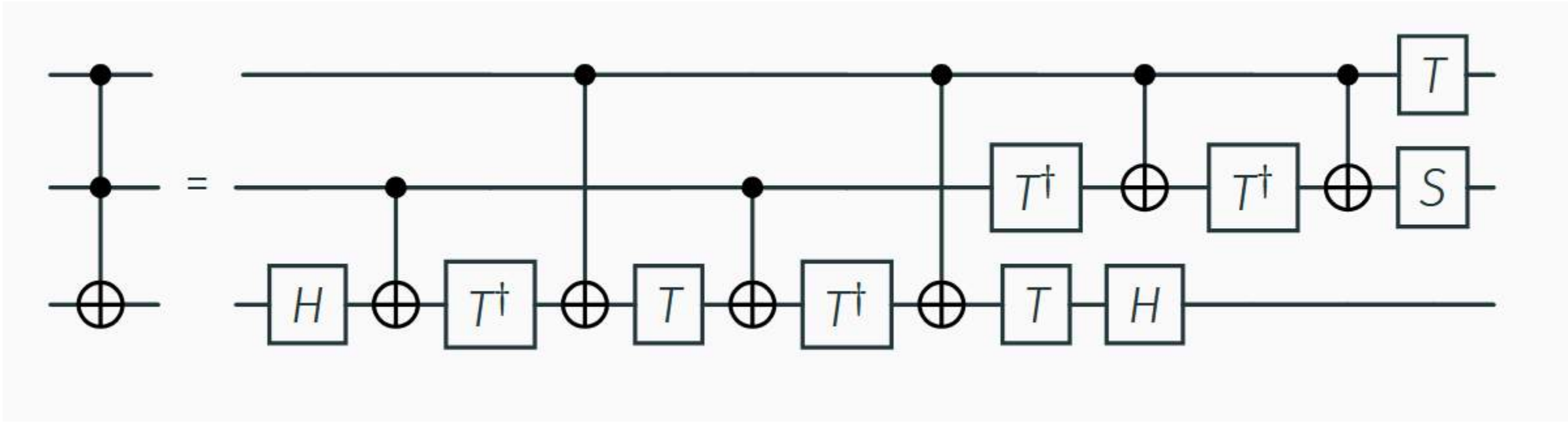
Architecture proposal:



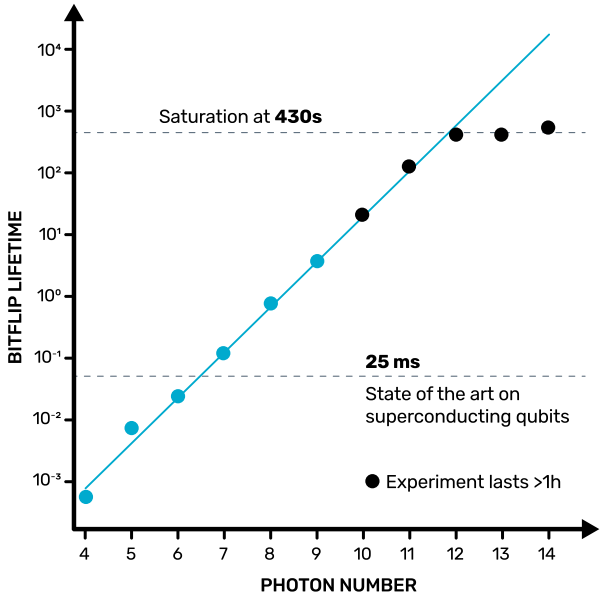
Resource estimation:



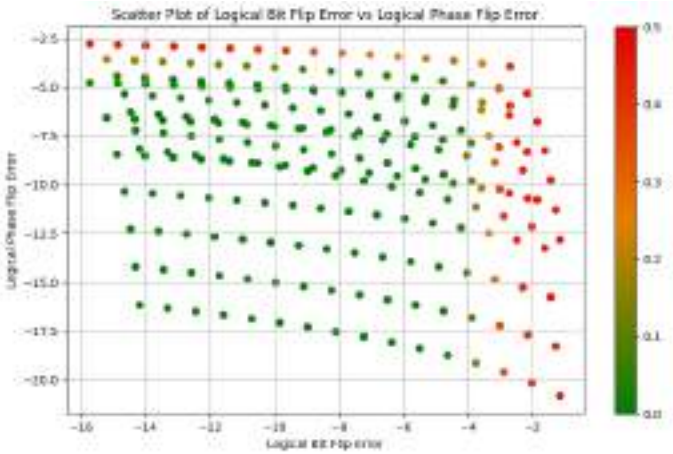
Provably optimal exact gate synthesis from a discrete gate set



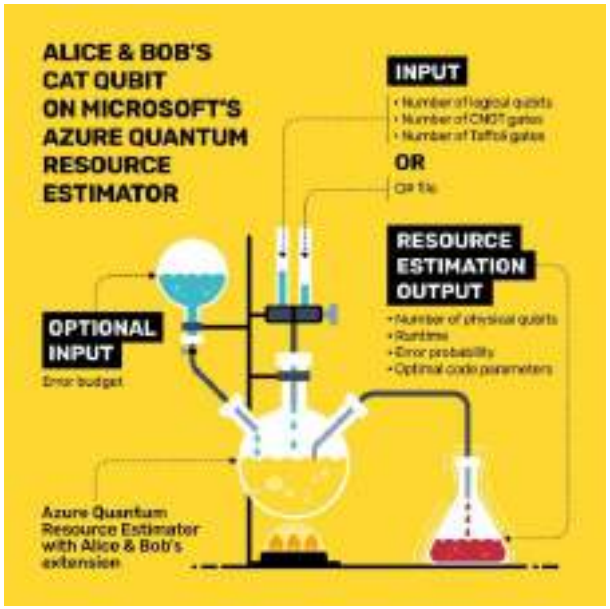
Felis, the software toolbox for cat qubits



Benchmark the Boson 4 chip



Emulate logical qubits based on cat qubits



Estimate resources: # of physical qubits run time

https://github.com/Alice-Bob-SW/qiskit-alice-bob-provider
https://github.com/Alice-Bob-SW/qsharp-alice-bob-resource-estimator

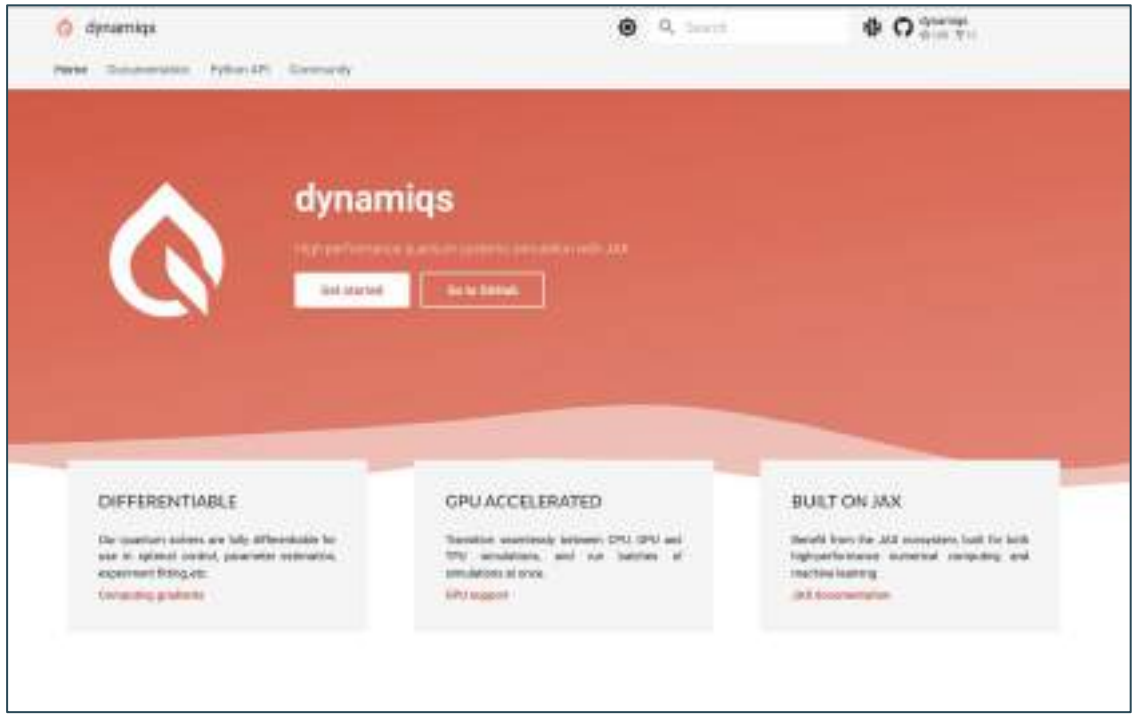
Dynamiqs

An open-source Python library based on JAX, for the simulation of

- the Schrödinger equation
- the Lindblad master equation
- stochastic master equations
- …

With

- CPU and **GPU** support
- **Batching**
- End-to-end **differentiability**
- Tailored **sparse** support
- QuTiP-like **API**



www.dynamiqs.org