An introduction to quantum cryptography, computation and error correction.

Colloquium of the Physics Department, ENS-Paris
October 23, 2018

Pierre Rouchon
Centre Automatique et Systèmes, Mines ParisTech, PSL Research University
Quantic Research Team (ENS, Inria, Mines)

Quantum cryptography and computation

- RSA public-key system
- Quantum mechanics from scratch
- BB84 quantum key distribution protocol
- Shor's factorization algorithm based on quantum Fourier transform

Quantum error correction (QEC)

- Classical error correction
- QEC in discrete-time
- Continuous-time QEC and measurement-based feedback
- Autonomous QEC and coherent feedback

Appendix: two key quantum systems

- Qubit (half-spin)
- Harmonic oscillator (spring)

• Invented by Rivest, Shamir and Adleman in 1977, this protocole relies on the factorization difficulty of RSA integer $n = pq$ with p and q large prime numbers (typically $\log_2(n) \sim 2048$).
• 3-step protocol based on the public key (n, e), with e invertible modulo $(p-1)(q-1)$ and the secrete key d, inverse of e modulo $(p-1)(q-1)$:

1. Encryption of M by Alice: $M \mapsto A = M^e \mod (n)$ (efficient exponentiation by squaring $\leq \log_2(e)$ multiplications $\mod (n)$)
2. Alice sends A to Bob on a public classical communication channel (possibly spied by the bad Oscar)
3. Decryption of A by Bob: $M = A^d$ where d is known only by Bob [1]

[1] Euler-Fermat theorem combined with Chinese-remainder theorem ensures that for arbitrary integers M and k, $M^{k\varphi(n)+1} = M \mod (n)$ where $\varphi(n) = \varphi(pq) = (p-1)(q-1)$ is the Euler's totient function (use $ed = 1 + r\varphi(n)$ for some integer r).

- To recover M from knowing A, e and n, the bad Oscar has to solve $A = M^e \mod (n)$. Specialists conjecture that there do-not exist C and $k > 0$ and an algorithm starting with input (n, e, A) providing M with less that $C\big(\log n\big)^k$ evaluations of universal classical gates **AND**, **XOR** and **NOT** (RSA problem conjectured outside complexity class **P**).
- If one has access to the factorization $pq = n$, one recovers the secret key d as the inverse of e modulo $(p-1)(q-1)$ (Euclidean polynomial algorithm providing the greatest common divisor).
- Factorization, which is in the complexity class **NP**, is guessed to be outside complexity class **P**: conjecture $\mathbf{P} \subsetneq \mathbf{NP}$.

Issues around quantum cryptography and computation:

1. **unconditionally secure key distribution:** BB84 quantum protocol (commercially available, see `https://www.idquantique.com/`).
2. **factorization in " polynomial time"** via Shor algorithm (success probability $O(1)$ with $O\Big((\log n)^3\Big)$ operations)
   (quantum computer with $3\log_2 n + c$ logical qubits, far from being available yet for 2048-bit RSA numbers n).

Quantum cryptography and computation

- RSA public-key system
- Quantum mechanics from scratch
- BB84 quantum key distribution protocol
- Shor's factorization algorithm based on quantum Fourier transform

Quantum error correction (QEC)

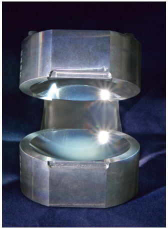
- Classical error correction
- QEC in discrete-time
- Continuous-time QEC and measurement-based feedback
- Autonomous QEC and coherent feedback

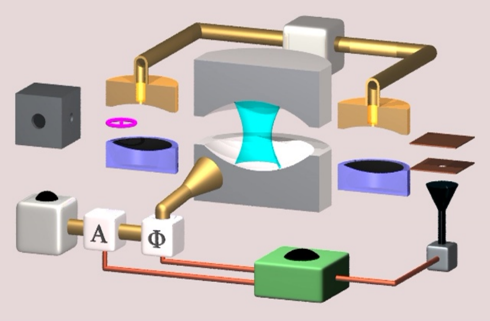
Appendix: two key quantum systems

- Qubit (half-spin)
- Harmonic oscillator (spring)

The first experimental realization of a quantum-state feedback:

microwave photons
(10 GHz)





Theory: I. Dotsenko, . . . : Quantum feedback by discrete quantum non-demolition measurements: towards on-demand generation of photon-number states. Physical Review A, **2009**, 80: 013805-013813.
Experiment: C. Sayrin, . . . , **S. Haroche**:
Real-time quantum feedback prepares and stabilizes photon number states. Nature, **2011**, 477, 73-77.

1. Schrödinger: wave funct. $|\psi\rangle \in \mathcal{H}$,

$$\frac{d}{dt}|\psi\rangle = -\frac{i}{\hbar}\boldsymbol{H}|\psi\rangle, \quad \boldsymbol{H} = \boldsymbol{H}_0 + u\boldsymbol{H}_1,$$

2. Origin of dissipation: collapse of the wave packet induced by the measurement of observable $\boldsymbol{O}$ with spectral decomp. $\sum_\mu \lambda_\mu \boldsymbol{P}_\mu$:
   - measurement outcome μ with proba. $\mathbb{P}_\mu = \langle\psi|\boldsymbol{P}_\mu|\psi\rangle$ depending on $|\psi\rangle$, just before the measurement
   - measurement back-action if outcome $\mu = y$:

$$|\psi\rangle \mapsto |\psi\rangle_+ = \frac{\boldsymbol{P}_y|\psi\rangle}{\sqrt{\langle\psi|\boldsymbol{P}_y|\psi\rangle}}$$

3. Tensor product for the description of composite systems (S, M):
   - Hilbert space $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_M$
   - Hamiltonian $\boldsymbol{H} = \boldsymbol{H}_S \otimes \boldsymbol{I}_M + \boldsymbol{H}_{int} + \boldsymbol{I}_S \otimes \boldsymbol{H}_M$
   - observable on sub-system M only: $\boldsymbol{O} = \boldsymbol{I}_S \otimes \boldsymbol{O}_M$.

[2] S. Haroche and J.M. Raimond. *Exploring the Quantum: Atoms, Cavities and Photons.* Oxford Graduate Texts, 2006.

- System S corresponds to a quantized harmonic oscillator:

$$\mathcal{H}_S = \left\{ \sum_{n=0}^{\infty} \psi_n \; |n\rangle \;\middle|\; (\psi_n)_{n=0}^{\infty} \in l^2(\mathbb{C}) \right\},$$

where $|n\rangle$ is the photon-number state with n photons ($\langle n_1|n_2\rangle = \delta_{n_1,n_2}$).

- Meter M is a qubit, a 2-level system:

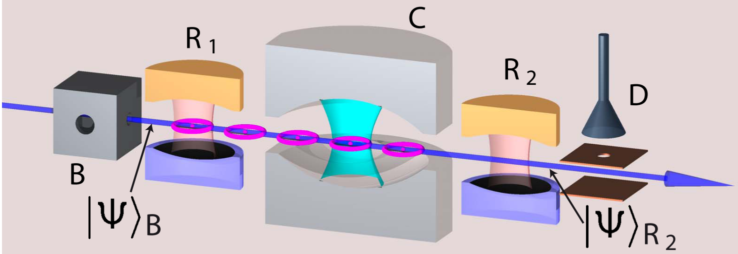
$$\mathcal{H}_M = \left\{ \psi_g \; |g\rangle + \psi_e \, |e\rangle \;\middle|\; \psi_g, \psi_e \in \mathbb{C} \right\},$$

where $|g\rangle$ (resp. $|e\rangle$) is the ground (resp. excited) state ($\langle g|g\rangle = \langle e|e\rangle = 1$ and $\langle g|e\rangle = 0$)

- **State of the composite system $|\boldsymbol{\Psi}\rangle \in \mathcal{H}_S \otimes \mathcal{H}_M$:**

$$\begin{aligned} |\boldsymbol{\Psi}\rangle &= \sum_{n\geq 0} \Big(\Psi_{ng} \; |n\rangle \otimes |g\rangle + \Psi_{ne} \; |n\rangle \otimes |e\rangle \Big) \\ &= \left(\sum_{n\geq 0} \Psi_{ng} \; |n\rangle \right) \otimes |g\rangle + \left(\sum_{n\geq 0} \Psi_{ne} \; |n\rangle \right) \otimes |e\rangle, \quad \Psi_{ne}, \Psi_{ng} \in \mathbb{C}. \end{aligned}$$

Ortho-normal basis: $\big(|n\rangle \otimes |g\rangle \, , |n\rangle \otimes |e\rangle \big)_{n\in\mathbb{N}}$.



- When atom comes out B, the quantum state $|\boldsymbol{\Psi}\rangle_B$ of the composite system is separable: $|\boldsymbol{\Psi}\rangle_B = |\psi\rangle \otimes |g\rangle$.
- Just before the measurement in D, the state is in general entangled (not separable):

$$|\boldsymbol{\Psi}\rangle_{R_2} = \boldsymbol{U}_{SM}\Big(|\psi\rangle \otimes |g\rangle \Big) = \Big(\boldsymbol{M}_g |\psi\rangle \Big) \otimes |g\rangle + \Big(\boldsymbol{M}_e |\psi\rangle \Big) \otimes |e\rangle$$

where $\boldsymbol{U}_{SM} = \boldsymbol{U}_{R_2}\boldsymbol{U}_C\boldsymbol{U}_{R_1}$ is a unitary transformation (Schrödinger propagator) defining the measurement operators $\boldsymbol{M}_g$ and $\boldsymbol{M}_e$ on $\mathcal{H}_S$. Since $\boldsymbol{U}_{SM}$ is unitary, $\boldsymbol{M}_g^\dagger \boldsymbol{M}_g + \boldsymbol{M}_e^\dagger \boldsymbol{M}_e = \boldsymbol{I}$.

Just before detector D the quantum state is **entangled**:

$$|\boldsymbol{\Psi}\rangle_{R_2} = (\boldsymbol{M}_g |\psi\rangle) \otimes |g\rangle + (\boldsymbol{M}_e |\psi\rangle) \otimes |e\rangle$$

Just after outcome y, the state becomes **separable** [3]:

$$|\boldsymbol{\Psi}\rangle_D = \left(\frac{\boldsymbol{M}_y}{\sqrt{\langle \psi | \boldsymbol{M}_y^\dagger \boldsymbol{M}_y | \psi \rangle}} |\psi\rangle \right) \otimes |y\rangle .$$

Outcome y obtained with probability $\mathbb{P}_y = \langle \psi | \boldsymbol{M}_y^\dagger \boldsymbol{M}_y | \psi \rangle$..

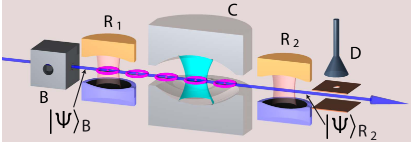
Quantum trajectories (Markov chain, stochastic dynamics):

$$|\psi_{k+1}\rangle = \begin{cases} \frac{\boldsymbol{M}_g}{\sqrt{\langle \psi_k | \boldsymbol{M}_g^\dagger \boldsymbol{M}_g | \psi_k \rangle}} |\psi_k\rangle, & y_k = g \text{ with probability } \langle \psi_k | \boldsymbol{M}_g^\dagger \boldsymbol{M}_g | \psi_k \rangle; \\ \frac{\boldsymbol{M}_e}{\sqrt{\langle \psi_k | \boldsymbol{M}_e^\dagger \boldsymbol{M}_e | \psi_k \rangle}} |\psi_k\rangle, & y_k = e \text{ with probability } \langle \psi_k | \boldsymbol{M}_e^\dagger \boldsymbol{M}_e | \psi_k \rangle; \end{cases}$$

with state $|\psi_k\rangle$ and measurement outcome $y_k \in \{g, e\}$ at time-step k:

[3] Measurement operator $\boldsymbol{O} = \boldsymbol{I}_S \otimes (|e\rangle\langle e| - |g\rangle\langle g|)$.

$$|\boldsymbol{\Psi}\rangle_{R_2} = \boldsymbol{U}_{R_2}\boldsymbol{U}_C\boldsymbol{U}_{R_1}\big(\,|\psi\rangle \otimes |g\rangle\,\big)$$



$$\boldsymbol{U}_{R_1} = \boldsymbol{I}_S \otimes \left(\left(\frac{|g\rangle+|e\rangle}{\sqrt{2}}\right)\langle g| + \left(\frac{-|g\rangle+|e\rangle}{\sqrt{2}}\right)\langle e|\right)$$

$$\boldsymbol{U}_C = e^{-i\frac{\phi_0}{2}\boldsymbol{N}} \otimes |g\rangle\langle g| + e^{i\frac{\phi_0}{2}\boldsymbol{N}} \otimes |e\rangle\langle e|$$

$$\boldsymbol{U}_{R_2} = \boldsymbol{U}_{R_1}$$

$$\boldsymbol{U}_{R_1}\big(\,|\psi\rangle \otimes |g\rangle\,\big) = \tfrac{1}{\sqrt{2}}\left(|\psi\rangle \otimes |g\rangle + |\psi\rangle \otimes |e\rangle\right)$$

$$\boldsymbol{U}_C\boldsymbol{U}_{R_1}\big(\,|\psi\rangle \otimes |g\rangle\,\big) = \tfrac{1}{\sqrt{2}}\Big(\Big(e^{-i\frac{\phi_0}{2}\boldsymbol{N}}|\psi\rangle\Big) \otimes |g\rangle + \Big(e^{i\frac{\phi_0}{2}\boldsymbol{N}}|\psi\rangle\Big) \otimes |e\rangle\Big)$$

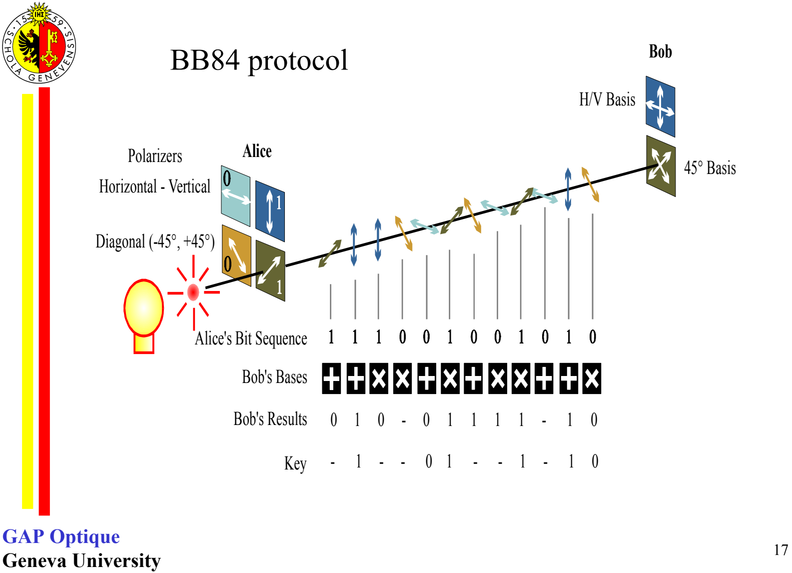
$$|\boldsymbol{\Psi}\rangle_{R_2} = \tfrac{1}{2}\Big(\Big(e^{-i\frac{\phi_0}{2}\boldsymbol{N}}|\psi\rangle\Big) \otimes (|g\rangle + |e\rangle) + \Big(e^{i\frac{\phi_0}{2}\boldsymbol{N}}|\psi\rangle\Big) \otimes (-|g\rangle + |e\rangle)\Big)$$

$$= \Big(-i\sin(\tfrac{\phi_0}{2}\boldsymbol{N})\,|\psi\rangle\Big) \otimes |g\rangle + \Big(\cos(\tfrac{\phi_0}{2}\boldsymbol{N})\,|\psi\rangle\Big) \otimes |e\rangle$$

Thus $\boldsymbol{M}_g = -i\sin(\frac{\phi_0}{2}\boldsymbol{N})$ and $\boldsymbol{M}_e = \cos(\frac{\phi_0}{2}\boldsymbol{N})$.

Quantum Monte-Carlo simulations with MATLAB: `QNDphoton.m`

[4] M. Brune, . . . : Manipulation of photons in a cavity by dispersive atom-field coupling: quantum non-demolition measurements and generation of "Schrödinger cat" states . Physical Review A, 45:5193-5214, 1992.


BB84 protocol
Bob
H/V Basis
45° Basis
Polarizers
Alice
Horizontal - Vertical
0
1
Diagonal (-45°, +45°)
0
1
Alice's Bit Sequence 1 1 1 0 0 1 0 0 1 0 1 0
Bob's Bases + + × × + × + × × + + ×
Bob's Results 0 1 0 - 0 1 1 1 1 - 1 0
Key - 1 - - 0 1 - - 1 - 1 0
GAP Optique
Geneva University
17

A first quantum sequence via a quantum communication channel:

1. Alice sends to Bob a large number N of linearly polarized photons (i.e. qubits $|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$) along 4 possible directions:
   - horizontal ($|0\rangle$) or vertical ($|1\rangle$).
   - $+\pi/4$ ($\frac{|0\rangle+|1\rangle}{\sqrt{2}}$) or $-\pi/4$ ($\frac{|0\rangle-|1\rangle}{\sqrt{2}}$).
2. For each photon received from Alice, Bob chooses a measurement
   - H/V: $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$
   - $\pm\pi/4$: $X = |1\rangle\langle 0| + |0\rangle\langle 1| = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0|+\langle 1|}{\sqrt{2}}\right) - \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0|-\langle 1|}{\sqrt{2}}\right)$

A second classical sequence via a public communication channel:

1. For each photon, Alice and Bob exchange the type of chosen polarization Z or X (but not its value).
2. For 50% of the photons sharing the same polarization (around $N/4$), Alice and Bob exchange their values (H/V or $\pm\pi/4$).
3. For 50% of the photons with same polarization (around $N/4$), Alice and Bob keep secret their values

If the exchanged values (H/V or $\pm\pi/4$) coincide, Alice and Bob are convinced that the quantum communication was not spied by the bad Oscar. The remaining values (around N/4 and kept secret) will then form a coding key exploited by Alice and Bob in a classical cryptographic protocol.

Security: Oscar cannot clone the photon emitted by Alice.

Assume that exists a quantum machine copying the original qubit onto a second clone qubit. The initial wave function of the composite system (original qubit, clone qubit, quantum machine) reads

$$|\Xi\rangle_{t=0} = |\psi\rangle \otimes |b\rangle \otimes |f_b\rangle \,.$$

where $|\psi\rangle \in \mathbb{C}^2$ is the original state, $|b\rangle$ the initial state of the clone (b for blank) and $|f_b\rangle$ the initial state of the cloning machine.
The cloning process is associated to a unitary transformation $\boldsymbol{U}_T$ independent of $|\Xi\rangle_{t=0}$ and satisfying

$$\forall\, |\psi\rangle \,, \quad |\psi\rangle \otimes |\psi\rangle \otimes \left|f_{|\psi\rangle}\right\rangle = \boldsymbol{U}_T\big(|\psi\rangle \otimes |b\rangle \otimes |f_b\rangle \big).$$

In particular

$$|0\rangle \otimes |0\rangle \otimes \left|f_{|0\rangle}\right\rangle = U_T\left(|0\rangle \otimes |b\rangle \otimes |f_b\rangle\right)$$

$$\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \otimes \left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \otimes \left|f_{\frac{|0\rangle+|1\rangle}{\sqrt{2}}}\right\rangle = U_T\left(\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \otimes |b\rangle \otimes |f_b\rangle\right)$$

Impossible with $|\Xi\rangle = |0\rangle \otimes |b\rangle \otimes |f_b\rangle$ and $|\Lambda\rangle = \left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \otimes |b\rangle \otimes |f_b\rangle$

$$\tfrac{1}{\sqrt{2}} = \left|\, \langle\Xi|\Lambda\rangle \,\right| \;>\; \tfrac{1}{2} \;\geq\; \left|\, \langle\Xi|\, U_T^\dagger U_T \,|\Lambda\rangle \,\right|$$

since U_T preserves Hermitian product:

- Input: composite odd number n.
- Output: a non trivial factor a of n in $O\big((\log n)^2(\log\log n)(\log\log\log n)\big)$ universal classical/quantum operations.
- Algorithm:

1. Check whether $n = a^b$ with $a, b > 1$ (polynomial classical algorithm); possible return of a and stop.
2. Otherwise, choose randomly $x \in \{2, \ldots, n-1\}$. If $a = \gcd(x, n) > 1$ (Euclidian division), return a and stop.
3. Otherwise **determine with a quantum computer the order r of x modulo n** (the smallest $r > 1$ such that $x^r = 1 \mod (n)$) [5]
   - If r even and $1 < \gcd(x^{r/2} \pm 1, n) < n$, then return $a = \gcd(x^{r/2} \pm 1, n)$ and stop.
   - Otherwise (probability $\leq \eta < 1$ independent of n) goto step 2.

[5] Shor's algorithm is detailed in Chapter 5 of M.A. Nielsen, I.L. Chuang: Quantum Computation and Quantum Information. Cambridge University Press, 2000.

- The canonical ℓ-qubit basis (basis of $\mathbb{C}^{2^\ell} \equiv (\mathbb{C}^2)^{\otimes^\ell}$) is labelled by $\{0,\dots 2^\ell - 1\} \ni j \equiv (j_1,\dots,j_\ell) \in \{0,1\}^\ell$ with $|j\rangle = |j_1 j_2 \dots j_\ell\rangle = |j_1\rangle \otimes |j_2\rangle \otimes \dots \otimes |j_\ell\rangle$ and $j = \sum_{s=1}^{\ell} j_s 2^{\ell-s}$.
- To the data $1 < x < n < 2^\ell$ with $\gcd(x,n) = 1$ is associated $\boldsymbol{U}$ a unitary transformation on ℓ-qubits (permutation between vectors $|j\rangle$)

$$\text{if } y \le n-1,\ \boldsymbol{U}\,|y\rangle = |xy \bmod(n)\rangle\,,\ \text{otherwise } \boldsymbol{U}\,|y\rangle = |y\rangle\,.$$

- For r the order of x mod(n) and any $s \in \{0,\dots,r-1\}$ the ℓ-qubit state

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2i\pi\, sk}{r}} \left|x^k \bmod(n)\right\rangle \quad \text{satisfies } \boldsymbol{U}\,|u_s\rangle = e^{\frac{-2i\pi\, s}{r}}\,|u_s\rangle$$

and $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$.
- Modular exponentiation algorithm to compute $\boldsymbol{U}$ with $O(\ell^3)$ 1-qubit gates [6] and **CNOT** 2-qubit gates [7] (non trivial quantum algorithm...)

[6] Unitary $e^{\imath\theta} e^{-\imath\alpha \boldsymbol{Z}/2} e^{-\imath\beta \boldsymbol{X}/2} e^{-\imath\gamma \boldsymbol{Z}/2}$ with $(\theta,\alpha,\beta,\gamma) \in [0,2\pi]$.

[7] **CNOT** $|y_1 y_2\rangle = |y_1 z_2\rangle$ where $\{0,1\} \ni z_2 = y_1 + y_2 \mod (2)$.

- Computations of the usual discrete Fourier transform
$\mathbb{C}^{2^\ell} \ni (x_0, \ldots, x_{2^\ell-1}) \mapsto (y_0, \ldots, y_{2^\ell-1}) \in \mathbb{C}^{2^\ell}$

$$y_j = \frac{1}{2^{\ell/2}} \sum_{j=0}^{2^\ell-1} e^{\frac{2i\pi\, jk}{2^\ell}} x_k; \quad x_k = \frac{1}{2^{\ell/2}} \sum_{j=0}^{2^\ell-1} e^{\frac{-2i\pi\, jk}{2^\ell}} y_j$$

requires $\boldsymbol{O(\ell 2^\ell)}$ additions and multiplications (FFT).

- It is also a unitary transformation of $\mathbb{C}^{2^\ell} \equiv (\mathbb{C}^2)^{\otimes \ell}$, the quantum Fourier transform (QFT)

$$|j_1\rangle \ldots |j_\ell\rangle = |j\rangle \mapsto \frac{\sum_{k=0}^{2^\ell-1} e^{\frac{2i\pi\, jk}{2^\ell}} |k\rangle}{2^{\ell/2}}$$

with the binary decomposition $j = \sum_{s=1}^{\ell} j_s 2^{\ell-s}$.

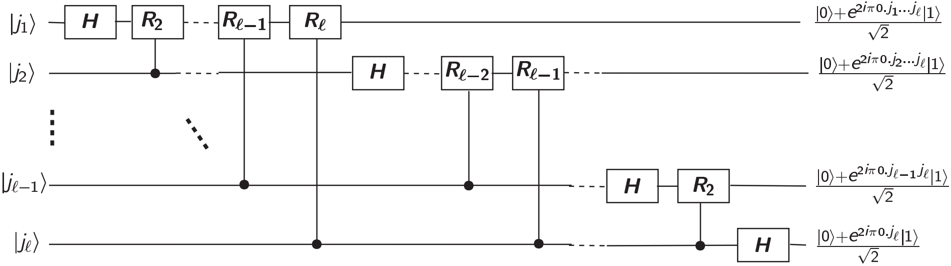
- The identity underlying the quantum circuit implementing the QFT with $\boldsymbol{O(\ell^2)}$ 1-qubit gates and 2-qubit gates:

$$\frac{\sum_{k=0}^{2^\ell-1} e^{\frac{2i\pi\, jk}{2^\ell}} |k\rangle}{2^{\ell/2}} = \frac{\left(|0\rangle + e^{2i\pi\, 0.j_\ell} |1\rangle\right)\left(|0\rangle + e^{2i\pi\, 0.j_{\ell-1} j_\ell} |1\rangle\right) \ldots \left(|0\rangle + e^{2i\pi\, 0.j_1 \ldots j_\ell} |1\rangle\right)}{2^{\ell/2}}$$

with binary fraction notations $0.j_s j_{s+1}\, j_m = j_s/2 + j_{s+1}/4 + \ldots + j_m/2^{m-s+1}$.

With Hadamard gate, $\boldsymbol{H} = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\langle 0| + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\langle 1|$, and

Controlled-$\boldsymbol{R_k}$ gate (2-qubit) where $\boldsymbol{R_k} = |0\rangle\langle 0| + e^{2i\pi/2^k}|1\rangle\langle 1|$, the circuit



followed by a simple swap circuit reversing the order of the ℓ qubits, one gets the QFT:

$$|j_1\ldots j_\ell\rangle \mapsto \frac{\left(|0\rangle + e^{2i\pi\,0.j_\ell}|1\rangle\right)\left(|0\rangle + e^{2i\pi\,0.j_{\ell-1}j_\ell}|1\rangle\right)\ldots\left(|0\rangle + e^{2i\pi\,0.j_1\ldots j_\ell}|1\rangle\right)}{2^{\ell/2}}$$

- Single bit error model: the bit $b \in \{0,1\}$ flips with probability $p < 1/2$ during Δt (for usual DRAM: $\boldsymbol{p/\Delta t \leq 10^{-14}}$ s^{-1}).
- Multi-bit error model: each bit $b_k \in \{0,1\}$ flips with probability $p < 1/2$ during Δt; no correlation between the bit flips.
- Use redundancy to construct with several physical bits b_k of flip probability p, a logical bit b_L with a flip probability $p_L < p$.
- The simplest solution, the 3-bit code (sampling time Δt):

$t = 0$: $b_L = [bbb]$ with $b \in \{0,1\}$

$t = \Delta t$: measure the three physical bits of $b_L = [b_1 b_2 b_3]$ (instantaneous) :

1. if all 3 bits coincide, nothing to do.
2. if one bit differs from the two other ones, flip this bit (instantaneous);

- Since the flip probability laws of the physical bits are independent, the probability that the logical bit b_L (protected with the above error correction code) flips during Δt is $\boldsymbol{p_L = 3p^2 - 2p^3} < p$ since $p < 1/2$.

The 3-qubit bit flip code

- Local bit-flip errors: each physical qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ becomes $\boldsymbol{X}|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$ [8] with probability $p < 1/2$ during Δt. (for actual super-conducting qubit $\boldsymbol{p/\Delta t > 10^3}$ s^{-1}).
- $t = 0$: $|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle \in \mathbb{C}^8$ with $|0_L\rangle = |000\rangle$ and $|1_L\rangle = |111\rangle$.
- $t = \Delta t$: $|\psi_L\rangle$ becomes with

$$\text{1 flip:} \begin{cases} \alpha|100\rangle + \beta|011\rangle \\ \alpha|010\rangle + \beta|101\rangle \\ \alpha|001\rangle + \beta|110\rangle \end{cases} ; \text{ 2 flips:} \begin{cases} \alpha|110\rangle + \beta|001\rangle \\ \alpha|101\rangle + \beta|010\rangle \\ \alpha|011\rangle + \beta|100\rangle \end{cases} ; \text{ 3 flips: } \alpha|111\rangle + \beta|000\rangle .$$

- Key fact: 4 orthogonal planes $\boldsymbol{\mathcal{P}}_c = \mathrm{span}(|000\rangle, |111\rangle)$, $\boldsymbol{\mathcal{P}}_1 = \mathrm{span}(|100\rangle, |011\rangle)$, $\boldsymbol{\mathcal{P}}_2 = \mathrm{span}(|010\rangle, |101\rangle)$ and $\boldsymbol{\mathcal{P}}_3 = \mathrm{span}(|001\rangle, |110\rangle)$.
- Error syndromes: 3 commuting observables $\boldsymbol{S}_1 = \boldsymbol{I} \otimes \boldsymbol{Z} \otimes \boldsymbol{Z}$, $\boldsymbol{S}_2 = \boldsymbol{Z} \otimes \boldsymbol{I} \otimes \boldsymbol{Z}$ and $\boldsymbol{S}_3 = \boldsymbol{Z} \otimes \boldsymbol{Z} \otimes \boldsymbol{I}$ with spectrum $\{-1, +1\}$ and outcomes $(s_1, s_2, s_3) \in \{-1, +1\}$.

$$\text{-1- } s_1 = s_2 = s_3\text{: } \boldsymbol{\mathcal{P}}_c \ni |\psi_L\rangle = \begin{cases} \alpha|000\rangle + \beta|111\rangle & \text{0 flip} \\ \beta|000\rangle + \alpha|111\rangle & \text{3 flips} \end{cases} ; \text{ no correction}$$

$$\text{-2- } s_1 \neq s_2 = s_3\text{: } \boldsymbol{\mathcal{P}}_1 \ni |\psi_L\rangle = \begin{cases} \alpha|100\rangle + \beta|011\rangle & \text{1 flip} \\ \beta|100\rangle + \alpha|011\rangle & \text{2 flips} \end{cases} ; (\boldsymbol{X} \otimes \boldsymbol{I} \otimes \boldsymbol{I})|\psi_L\rangle \in \boldsymbol{\mathcal{P}}_c.$$

$$\text{-3- } s_2 \neq s_3 = s_1\text{: } \boldsymbol{\mathcal{P}}_2 \ni |\psi_L\rangle = \begin{cases} \alpha|010\rangle + \beta|101\rangle & \text{1 flip} \\ \beta|010\rangle + \alpha|101\rangle & \text{2 flips} \end{cases} ; (\boldsymbol{I} \otimes \boldsymbol{X} \otimes \boldsymbol{I})|\psi_L\rangle \in \boldsymbol{\mathcal{P}}_c.$$

$$\text{-4- } s_3 \neq s_1 = s_2\text{: } \boldsymbol{\mathcal{P}}_3 \ni |\psi_L\rangle = \begin{cases} \alpha|001\rangle + \beta|110\rangle & \text{1 flip} \\ \beta|001\rangle + \alpha|110\rangle & \text{2 flips} \end{cases} ; (\boldsymbol{I} \otimes \boldsymbol{I} \otimes \boldsymbol{X})|\psi_L\rangle \in \boldsymbol{\mathcal{P}}_c.$$

[8] $\boldsymbol{X} = |1\rangle\langle 0| + |0\rangle\langle 1|$ and $\boldsymbol{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$.

The 3-qubit phase flip code

- Local phase-flip error: each physical qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ becomes $\boldsymbol{Z}|\psi\rangle = \alpha|0\rangle - \beta|0\rangle$ [9] with probability $p < 1/2$ during Δt.
- Since $X = \boldsymbol{HZH}$ and $Z = \boldsymbol{HXH}$ ($\boldsymbol{H}^2 = \boldsymbol{I}$), use the 3-qubit bit flip code in the frame defined by $\boldsymbol{H}$:

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}} \triangleq |+\rangle\,, \quad |1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}} \triangleq |-\rangle\,, \quad \boldsymbol{X} \mapsto \boldsymbol{HXH} = \boldsymbol{Z} = |+\rangle\langle +| + |-\rangle\langle -|\,.$$

- $t = +$: $|\psi_L\rangle = \alpha|+_L\rangle + \beta|-_L\rangle$ with $|+_L\rangle = |+++\rangle$ and $|-_L\rangle = |---\rangle$.
- $t = \Delta t$: $|\psi_L\rangle$ becomes with

$$\text{1 flip: } \begin{cases} \alpha|-++\rangle + \beta|+--\rangle \\ \alpha|+-+\rangle + \beta|-+-\rangle \\ \alpha|++-\rangle + \beta|--+\rangle \end{cases} ;\ \text{2 flips: } \begin{cases} \alpha|--+\rangle + \beta|++-\rangle \\ \alpha|-+-\rangle + \beta|+-+\rangle \\ \alpha|+--\rangle + \beta|-++\rangle \end{cases} ;\ \text{3 flips: } \alpha|---\rangle + \beta|+++\rangle\,.$$

- Key fact: 4 orthogonal planes $\mathcal{P}_c = \text{span}(|+++\rangle, |---\rangle)$, $\mathcal{P}_1 = \text{span}(|-++\rangle, |+--\rangle)$, $\mathcal{P}_2 = \text{span}(|+-+\rangle, |-+-\rangle)$ and $\mathcal{P}_3 = \text{span}(|++-\rangle, |--+\rangle)$.
- Error syndromes: 3 commuting observables $\boldsymbol{S_1} = \boldsymbol{I} \otimes \boldsymbol{X} \otimes \boldsymbol{X}$, $\boldsymbol{S_2} = \boldsymbol{X} \otimes \boldsymbol{I} \otimes \boldsymbol{X}$ and $\boldsymbol{S_3} = \boldsymbol{X} \otimes \boldsymbol{X} \otimes \boldsymbol{I}$ with spectrum $\{-1, +1\}$ and outcomes $(s_1, s_2, s_3) \in \{-1, +1\}$.

-1- $s_1 = s_2 = s_3$: $\mathcal{P}_c \ni |\psi_L\rangle = \begin{cases} \alpha|+++\rangle + \beta|---\rangle & \text{0 flip} \\ \beta|+++\rangle + \alpha|---\rangle & \text{3 flips} \end{cases}$; no correction

-2- $s_1 \neq s_2 = s_3$: $\mathcal{P}_1 \ni |\psi_L\rangle = \begin{cases} \alpha|-++\rangle + \beta|+--\rangle & \text{1 flip} \\ \beta|-++\rangle + \alpha|+--\rangle & \text{2 flips} \end{cases}$; $(\boldsymbol{Z} \otimes \boldsymbol{I} \otimes \boldsymbol{I})|\psi_L\rangle \in \mathcal{P}_c$.

-3- $s_2 \neq s_3 = s_1$: $\mathcal{P}_2 \ni |\psi_L\rangle = \begin{cases} \alpha|+-+\rangle + \beta|-+-\rangle & \text{1 flip} \\ \beta|+-+\rangle + \alpha|-+-\rangle & \text{2 flips} \end{cases}$; $(\boldsymbol{I} \otimes \boldsymbol{Z} \otimes \boldsymbol{I})|\psi_L\rangle \in \mathcal{P}_c$.

-4- $s_3 \neq s_1 = s_2$: $\mathcal{P}_3 \ni |\psi_L\rangle = \begin{cases} \alpha|++-\rangle + \beta|--+\rangle & \text{1 flip} \\ \beta|++-\rangle + \alpha|--+\rangle & \text{2 flips} \end{cases}$; $(\boldsymbol{I} \otimes \boldsymbol{I} \otimes \boldsymbol{Z})|\psi_L\rangle \in \mathcal{P}_c$.

[9] $\boldsymbol{X} = |1\rangle\langle 0| + |0\rangle\langle 1|$, $\boldsymbol{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$ and $\boldsymbol{H} = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\langle 0| + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\langle 1|$.

• Take the phase flip code $|+++\rangle$ and $|---\rangle$. Replace each $|+\rangle$ (resp. $|-\rangle$) by $\frac{|000\rangle+|111\rangle}{\sqrt{2}}$ (resp. $\frac{|000\rangle-|111\rangle}{\sqrt{2}}$). New logical qubit $|\psi_L\rangle = \alpha\,|0_L\rangle + \beta\,|1_L\rangle \in \mathbb{C}^{2^9}$:

$$|0_L\rangle = \frac{\big(|000\rangle+|111\rangle\big)\big(|000\rangle+|111\rangle\big)\big(|000\rangle+|111\rangle\big)}{2\sqrt{2}},\ |1_L\rangle = \frac{\big(|000\rangle-|111\rangle\big)\big(|000\rangle-|111\rangle\big)\big(|000\rangle-|111\rangle\big)}{2\sqrt{2}}$$

• Local errors: each of the 9 physical qubits can have a bit-flip $\boldsymbol{X}$, a phase flip $\boldsymbol{Z}$ or a bit flip followed by a phase flip $\boldsymbol{ZX} = i\boldsymbol{Y}$ [10] with probability p during Δt.
• Denote by $\boldsymbol{X}_k$ (resp. $\boldsymbol{Y}_k$ and $\boldsymbol{Z}_k$), the local operator $\boldsymbol{X}$ (resp. $\boldsymbol{Y}$ and $\boldsymbol{Z}$) acting on physical qubit no $k \in \{1,\ldots,9\}$. Denote by $\boldsymbol{\mathcal{P}}_c = \text{span}(|0_L\rangle, |1_L\rangle)$ the code space. One get a family of the $1+3\times 9 = $ **28 orthogonal planes:**

$$\boldsymbol{\mathcal{P}}_c,\quad \Big(\boldsymbol{X}_k\boldsymbol{\mathcal{P}}_c\Big)_{k=1,\ldots,9},\quad \Big(\boldsymbol{Y}_k\boldsymbol{\mathcal{P}}_c\Big)_{k=1,\ldots,9},\quad \Big(\boldsymbol{Z}_k\boldsymbol{\mathcal{P}}_c\Big)_{k=1,\ldots,9}.$$

• One can always construct error syndromes to obtain, when there is only one error among the 9 qubits during Δt, the number k of the qubit and the error type it has undergone ($\boldsymbol{X}$, $\boldsymbol{Y}$ or $\boldsymbol{Z}$). These 28 planes are then eigen-planes by the syndromes.
• If the physical qubit k is subject to **any kind of local errors** associated to arbitrary operator $\boldsymbol{M} = g\boldsymbol{I} + a\boldsymbol{X} + b\boldsymbol{Y} + c\boldsymbol{Z}$ ($g,a,b,c \in \mathbb{C}$), $|\psi_L\rangle \mapsto \frac{\boldsymbol{M}_k|\psi_L\rangle}{\sqrt{\langle\psi_L|\boldsymbol{M}_k^\dagger\boldsymbol{M}_k|\psi_L\rangle}}$, the syndrome measurements will project the corrupted logical qubit on one of the 4 planes $\boldsymbol{\mathcal{P}}_c$, $\boldsymbol{X}_k\boldsymbol{\mathcal{P}}_c$, $\boldsymbol{Y}_k\boldsymbol{\mathcal{P}}_c$ or $\boldsymbol{Z}_k\boldsymbol{\mathcal{P}}_c$. It is then simple by using either $\boldsymbol{I}$, $\boldsymbol{X}_k$, $\boldsymbol{Y}_k$ or $\boldsymbol{Z}_k$, to recover up to a global phase the original logical qubit $|\psi_L\rangle$.

[10] $\boldsymbol{X} = |1\rangle\langle 0| + |0\rangle\langle 1|$, $\boldsymbol{Z} = |0\rangle\langle 0| - |1\rangle\langle 1|$ and $\boldsymbol{Y} = i\,|1\rangle\,|0\rangle - i\,|0\rangle\,|1\rangle$.

- For a logical qubit relying on n physical qubits, the dimension of the Hilbert has to be larger than $2(1+3n)$ to recover an arbitrary single-qubit error: $2^n \geq 2(1+3n)$ imposing $n \geq 5$.

- Efficient constructions of quantum error-correcting codes: stabilizer codes, surface codes where the physical qubits are located on a 2D-lattice, topological codes, ...

- Fault tolerant computations: computing on encoded quantum states; fault-tolerant operations to avoid propagations of errors during encoding, gates and measurement; concatenation and threshold theorem, ...

- Error rates for a DRAM bit $\leq 10^{-14}$ s^{-1} and for a superconducting qubit $\geq 10^{3}$ s^{-1} : high order error-correcting codes; important overhead (around 1000 physical qubits to encode a logical one[11]); scalability issues; ...

---

[11] A.G. Fowler, M. Mariantoni, J.M. Martinis, A.N. Cleland: Surface codes: Towards practical large-scale quantum computation. Phys. Rev. A,86(3):032324, 2012.

Continuous-time QEC and feedback

- Quantum error correction is a feedback scheme: at each sampling time a measurement is performed and a correction depending only on the measurement outcome is applied.

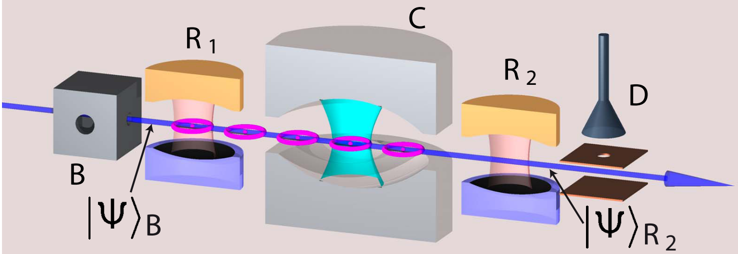
- From a control engineering view point, QEC is based on a static output feedback scheme (feedback without memory) (called also Markovian feedback).

- In usual discrete-time setting, measurement (sensor) and correction (actuator) processes are assumed instantaneous.

- Natural question: how to take into account the finite band-width of the measurement and correction processes.

- Interest of continuous-time formulations for QEC:
  1. measurement and correction are faster than the error rates but not infinitely faster;
  2. qubit errors can occur during the measurement and the correction processes (fault-tolerance issues).

$|\psi\rangle$ replaced by ρ (density operator) obeying to a stochastic master equation (SME).



$$|\boldsymbol{\Psi}\rangle_{R_2} = \boldsymbol{U}_{SM}|\boldsymbol{\Psi}\rangle_B = \boldsymbol{U}_{SM}\big(\,|\psi\rangle \otimes |g\rangle\,\big) = \big(\boldsymbol{M}_g\,|\psi\rangle\,\big) \otimes |g\rangle + \big(\boldsymbol{M}_e\,|\psi\rangle\,\big) \otimes |e\rangle$$

with $\boldsymbol{M}_g^\dagger \boldsymbol{M}_g + \boldsymbol{M}_e^\dagger \boldsymbol{M}_e = \boldsymbol{I}$.

- Quantum trajectories (Markov chain, stochastic dynamics):

$$|\psi_{k+1}\rangle = \begin{cases} \dfrac{\boldsymbol{M}_g}{\sqrt{\langle \psi_k|\boldsymbol{M}_g^\dagger \boldsymbol{M}_g|\psi_k\rangle}}\,|\psi_k\rangle\,, & y_k = g \text{ with probability } \langle \psi_k|\boldsymbol{M}_g^\dagger \boldsymbol{M}_g|\psi_k\rangle; \\ \dfrac{\boldsymbol{M}_e}{\sqrt{\langle \psi_k|\boldsymbol{M}_e^\dagger \boldsymbol{M}_e|\psi_k\rangle}}\,|\psi_k\rangle\,, & y_k = e \text{ with probability } \langle \psi_k|\boldsymbol{M}_e^\dagger \boldsymbol{M}_e|\psi_k\rangle; \end{cases}$$

with state $|\psi_k\rangle$ and measurement outcome $y_k \in \{g, e\}$ at time-step k:

Continuous-time quantum trajectories (diffusive case) [12]

- The measurement outcome y_k at discrete-time step k, is replaced by the small among of measurement signal $\boldsymbol{dy_t} \in \mathbb{R}$ obtained during an infinitesimal time interval $[t, t+dt]$.
- The measurement operator $\boldsymbol{M}_{y_k}$ becomes $\boldsymbol{M}_{\boldsymbol{dy_t}}$ close to identity:

$$\boldsymbol{M}_{\boldsymbol{dy_t}} = \boldsymbol{I} + \left(-\tfrac{i}{\hbar}\boldsymbol{H} - \tfrac{1}{2}\left(\boldsymbol{L}^\dagger \boldsymbol{L}\right)\right) dt + \boldsymbol{dy_t}\,\boldsymbol{L}$$

where operator $\boldsymbol{L}$ (not necessarily Hermitian) describes the measurement process and $\boldsymbol{H}$ is the Hamiltonian corresponding to the coherent evolution.

- The measurement backaction reads

$$|\psi\rangle_{t+dt} = \frac{\boldsymbol{M}_{\boldsymbol{dy_t}} |\psi\rangle_t}{\sqrt{\langle\psi|_t \boldsymbol{M}^\dagger_{\boldsymbol{dy_t}} \boldsymbol{M}_{\boldsymbol{dy_t}} |\psi\rangle_t}}$$

- Probability density of $\boldsymbol{dy} \in \mathbb{R}$ knowing $|\psi\rangle_t$: $\frac{e^{-\frac{\boldsymbol{dy}^2}{2dt}}}{\sqrt{2\pi dt}} \langle\psi|_t \boldsymbol{M}^\dagger_{\boldsymbol{dy}} \boldsymbol{M}_{\boldsymbol{dy}} |\psi\rangle_t$.

Coincides up to order $O(dt^{3/2})$ terms to $\boldsymbol{dy} = \langle\psi|_t (\boldsymbol{L} + \boldsymbol{L}^\dagger) |\psi\rangle_t \; dt + dW$ where dW is a Wiener process (Gaussian of zero mean and variance dt).

Quantum Monte-Carlo simulations with MATLAB: `QNDqubit.m` ($\boldsymbol{L} = \boldsymbol{\sigma_z}$, $\boldsymbol{H} = 0$)

[12] For a mathematical exposure: A. Barchielli, M. Gregoratti: Quantum Trajectories and Measurements in Continuous Time: the Diffusive Case. Springer Verlag,2009.

Consider once again the LKB photon-box:

$$|\psi_{k+1}\rangle = \begin{cases} \dfrac{\boldsymbol{M}_g}{\sqrt{\langle\psi_k|\boldsymbol{M}_g^\dagger\boldsymbol{M}_g|\psi_k\rangle}}|\psi_k\rangle, & y_k = g \text{ with probability } \langle\psi_k|\boldsymbol{M}_g^\dagger\boldsymbol{M}_g|\psi_k\rangle; \\ \dfrac{\boldsymbol{M}_e}{\sqrt{\langle\psi_k|\boldsymbol{M}_e^\dagger\boldsymbol{M}_e|\psi_k\rangle}}|\psi_k\rangle, & y_k = e \text{ with probability } \langle\psi_k|\boldsymbol{M}_e^\dagger\boldsymbol{M}_e|\psi_k\rangle; \end{cases}$$

Assume known $|\psi_0\rangle$ and **detector out of order** ($y = \varnothing$): **what about $|\psi_1\rangle$?**

- Expectation value of $|\psi_1\rangle\langle\psi_1|$ knowing $|\psi_0\rangle$: [13]

$$\mathbb{E}\left(|\psi_1\rangle\langle\psi_1| \;\middle|\; |\psi_0\rangle\right) = \boldsymbol{M}_g|\psi_0\rangle\langle\psi_0|\boldsymbol{M}_g^\dagger + \boldsymbol{M}_e|\psi_0\rangle\langle\psi_0|\boldsymbol{M}_e^\dagger.$$

- Set $\boldsymbol{K}(\boldsymbol{\rho}) \triangleq \boldsymbol{M}_g\boldsymbol{\rho}\boldsymbol{M}_g^\dagger + \boldsymbol{M}_e\boldsymbol{\rho}\boldsymbol{M}_e^\dagger$ for any operator $\boldsymbol{\rho}$.
- $\boldsymbol{\rho}_k$ expectation of $|\psi_k\rangle\langle\psi_k|$ knowing $|\psi_0\rangle$:

$$\boldsymbol{\rho}_{k+1} = \boldsymbol{K}(\boldsymbol{\rho}_k) \text{ and } \boldsymbol{\rho}_0 = |\psi_0\rangle\langle\psi_0|.$$

Linear map $\boldsymbol{K}$: trace preserving Kraus map (quantum channel).
Density operators $\boldsymbol{\rho}$: convex space of Hermitian non-negative operators of trace one.

[13] $|\psi\rangle\langle\psi|$: orthogonal projector on line spanned by unitary vector $|\psi\rangle$.

Detector efficiency $\boldsymbol{\eta} \in [0,1]$. Output $y \in \{g, e, \varnothing\}$:

$$\boldsymbol{\rho}_{k+1} = \begin{cases} \dfrac{\boldsymbol{K}_g(\boldsymbol{\rho}_k)}{\operatorname{Tr}(\boldsymbol{K}_g(\boldsymbol{\rho}_k))}, \; y_k = g \text{ with probability } \operatorname{Tr}(\boldsymbol{K}_g(\boldsymbol{\rho}_k)); \\ \dfrac{\boldsymbol{K}_e(\boldsymbol{\rho}_k)}{\operatorname{Tr}(\boldsymbol{K}_e(\boldsymbol{\rho}_k))}, \; y_k = e \text{ with probability } \operatorname{Tr}(\boldsymbol{K}_e(\boldsymbol{\rho}_k)); \\ \dfrac{\boldsymbol{K}_\varnothing(\boldsymbol{\rho}_k)}{\operatorname{Tr}(\boldsymbol{K}_\varnothing(\boldsymbol{\rho}_k))}, \; y_k = \varnothing \text{ with probability } \operatorname{Tr}(\boldsymbol{K}_\varnothing(\boldsymbol{\rho}_k)); \end{cases}$$

with Kraus maps

$$\boldsymbol{K}_g(\boldsymbol{\rho}) = \boldsymbol{\eta} \boldsymbol{M}_g \boldsymbol{\rho} \boldsymbol{M}_g^\dagger, \qquad \boldsymbol{K}_e(\boldsymbol{\rho}) = \boldsymbol{\eta} \boldsymbol{M}_e \boldsymbol{\rho} \boldsymbol{M}_e^\dagger$$
$$\boldsymbol{K}_\varnothing(\boldsymbol{\rho}) = (1-\boldsymbol{\eta}) \left(\boldsymbol{M}_g \boldsymbol{\rho} \boldsymbol{M}_g^\dagger + \boldsymbol{M}_e \boldsymbol{\rho} \boldsymbol{M}_e^\dagger \right).$$

We still have:

$$\mathbb{E}\left(\boldsymbol{\rho}_{k+1} \mid \boldsymbol{\rho}_k\right) \triangleq \boldsymbol{K}(\boldsymbol{\rho}_k) = \boldsymbol{M}_g \boldsymbol{\rho}_k \boldsymbol{M}_g^\dagger + \boldsymbol{M}_e \boldsymbol{\rho}_k \boldsymbol{M}_e^\dagger = \sum_y \boldsymbol{K}_y(\boldsymbol{\rho}_k).$$

Discrete-time quantum trajectories for open quantum systems

Four features:

1. Bayes law: $\mathbb{P}(\mu/y) = \mathbb{P}(y/\mu)\mathbb{P}(\mu) \;/\; \left(\sum_{\mu'} \mathbb{P}(y/\mu')\mathbb{P}(\mu')\right)$,
2. Schrödinger equations defining unitary transformations.
3. Partial collapse of the wave packet: irreversibility and dissipation are induced by the measurement of observables with degenerate spectra.
4. Tensor product for the description of composite systems.

$\Rrightarrow$ **Discrete-time Q. traj. :** Markov processes of state ρ, (density op.):
$\rho_{k+1} = \frac{\sum_{\mu=1}^{m} \eta_{y,\mu} \boldsymbol{M}_\mu \rho_k \boldsymbol{M}_\mu^\dagger}{\text{Tr}\left(\sum_{\mu=1}^{m} \eta_{y,\mu} \boldsymbol{M}_\mu \rho_k \boldsymbol{M}_\mu^\dagger\right)}$, with proba. $\mathbb{P}_y(\rho_k) = \sum_{\mu=1}^{m} \eta_{y,\mu} \text{ Tr}\left(\boldsymbol{M}_\mu \rho_k \boldsymbol{M}_\mu^\dagger\right)$
associated to Kraus maps [14] (ensemble average, quantum channel)

$$\mathbb{E}\left(\rho_{k+1}|\rho_k\right) = \boldsymbol{K}(\rho_k) = \sum_\mu \boldsymbol{M}_\mu \rho_k \boldsymbol{M}_\mu^\dagger \quad \text{with} \quad \sum_\mu \boldsymbol{M}_\mu^\dagger \boldsymbol{M}_\mu = \boldsymbol{I}$$

and left stochastic matrices (imperfections, decoherences) $(\eta_{y,\mu})$.

[14] M.A. Nielsen, I.L. Chuang: Quantum Computation and Quantum Information. Cambridge University Press, 2000.

Discrete-time models: Markov chains

$$\rho_{k+1} = \frac{\sum_{\mu=1}^{m} \eta_{y,\mu} \boldsymbol{M}_\mu \rho_k \boldsymbol{M}_\mu^\dagger}{\text{Tr}\left(\sum_{\mu=1}^{m} \eta_{y,\mu} \boldsymbol{M}_\mu \rho_k \boldsymbol{M}_\mu^\dagger\right)}, \text{ with proba. } \mathbb{P}_y(\rho_k) = \sum_{\mu=1}^{m} \eta_{y,\mu} \text{ Tr}\left(\boldsymbol{M}_\mu \rho_k \boldsymbol{M}_\mu^\dagger\right)$$

with ensemble averages corresponding to Kraus linear maps

$$\mathbb{E}\left(\rho_{k+1} | \rho_k\right) = \boldsymbol{K}(\rho_k) = \sum_\mu \boldsymbol{M}_\mu \rho_k \boldsymbol{M}_\mu^\dagger \quad \text{with} \quad \sum_\mu \boldsymbol{M}_\mu^\dagger \boldsymbol{M}_\mu = \boldsymbol{I}$$

Continuous-time models: stochastic differential systems [15]

$$d\rho_t = \left(-\tfrac{i}{\hbar}[\boldsymbol{H}, \rho_t] + \sum_\nu \boldsymbol{L}_\nu \rho_t \boldsymbol{L}_\nu^\dagger - \frac{1}{2}(\boldsymbol{L}_\nu^\dagger \boldsymbol{L}_\nu \rho_t + \rho_t \boldsymbol{L}_\nu^\dagger \boldsymbol{L}_\nu)\right) dt$$
$$+ \sum_\nu \sqrt{\eta_\nu}\left(\boldsymbol{L}_\nu \rho_t + \rho_t \boldsymbol{L}_\nu^\dagger - \text{ Tr}\left((\boldsymbol{L}_\nu + \boldsymbol{L}_\nu^\dagger)\rho_t\right) \rho_t\right) dW_{\nu,t}$$

driven by Wiener processes $dW_{\nu,t}$, with measurements $y_{\nu,t}$,
$dy_{\nu,t} = \sqrt{\eta_\nu} \text{ Tr}\left((\boldsymbol{L}_\nu + \boldsymbol{L}_\nu^\dagger)\rho_t\right) dt + dW_{\nu,t}$, detection efficiencies $\eta_\nu \in [0,1]$ and Lindblad-Kossakowski master equations ($\eta_\nu \equiv 0$):

$$\frac{d}{dt}\rho = -\tfrac{i}{\hbar}[\boldsymbol{H}, \rho] + \sum_\nu \boldsymbol{L}_\nu \rho \boldsymbol{L}_\nu^\dagger - \frac{1}{2}(\boldsymbol{L}_\nu^\dagger \boldsymbol{L}_\nu \rho + \rho \boldsymbol{L}_\nu^\dagger \boldsymbol{L}_\nu)$$

[15] A. Barchielli, M. Gregoratti: Quantum Trajectories and Measurements in Continuous Time: the Diffusive Case. Springer Verlag, 2009.

Positivity-preserving formulation of diffusive SME [16]

With a single imperfect measurement $\boldsymbol{dy_t} = \sqrt{\eta}\ \mathrm{Tr}\left((\boldsymbol{L}+\boldsymbol{L}^\dagger)\,\rho_t\right)\ dt + \boldsymbol{dW_t}$ and detection efficiency $\eta \in [0,1]$, the quantum state ρ_t is usually mixed and obeys to

$$d\rho_t = \left(-\tfrac{i}{\hbar}[\boldsymbol{H},\rho_t] + \boldsymbol{L}\rho_t\boldsymbol{L}^\dagger - \frac{1}{2}(\boldsymbol{L}^\dagger\boldsymbol{L}\rho_t + \rho_t\boldsymbol{L}^\dagger\boldsymbol{L})\right)dt + \sqrt{\eta}\left(\boldsymbol{L}\rho_t + \rho_t\boldsymbol{L}^\dagger - \ \mathrm{Tr}\left((\boldsymbol{L}+\boldsymbol{L}^\dagger)\rho_t\right)\,\rho_t\right)\boldsymbol{dW_t}$$

driven by the Wiener process $\boldsymbol{dW_t}$

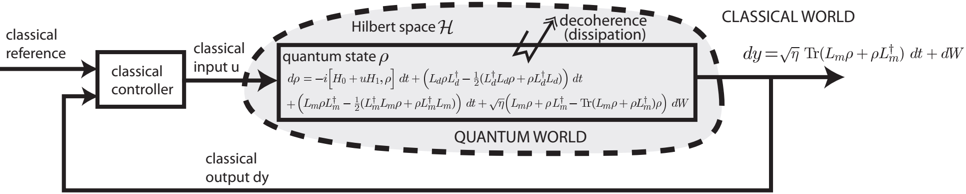
With Itō rules, it can be written as the following "discrete-time" Markov model

$$\rho_{t+dt} = \frac{\boldsymbol{M}_{\boldsymbol{dy_t}}\rho_t\boldsymbol{M}_{\boldsymbol{dy_t}}^\dagger + (1-\eta)\boldsymbol{L}\rho_t\boldsymbol{L}^\dagger dt}{\mathrm{Tr}\left(\boldsymbol{M}_{\boldsymbol{dy_t}}\rho_t\boldsymbol{M}_{\boldsymbol{dy_t}}^\dagger + (1-\eta)\boldsymbol{L}\rho_t\boldsymbol{L}^\dagger dt\right)}$$

with $\boldsymbol{M}_{\boldsymbol{dy_t}} = \boldsymbol{I} + \left(-\frac{i}{\hbar}\boldsymbol{H} - \frac{1}{2}\left(\boldsymbol{L}^\dagger\boldsymbol{L}\right)\right)dt + \sqrt{\eta}\boldsymbol{dy_t}\boldsymbol{L}$.

ρ_0 density operator $\mapsto$ for all $t>0$, ρ_t density operator

[16] Such SME precisely describe cutting-edge experiments with superconducting qubits under homodyne and heterodyne continuous-time measurements. See, e.g., the group of Benjamin Huard at ENS-Lyon: `http://www.physinfo.fr/index.html`.



- How to achieve QEC with the above measurement-based feedback scheme where the controller admits a memory (a dynamical system, possibly stochastic).

- In [17] QEC is implicitly formulated as feedback stabilization of the code space $\mathcal{P}_c$ under quantum non demolition measurement. Numerical closed-loop simulations indicate promising convergence properties but a precise mathematical convergence analysis is missing. Many open issues such as precise estimates of convergence rates in closed-loop [18]

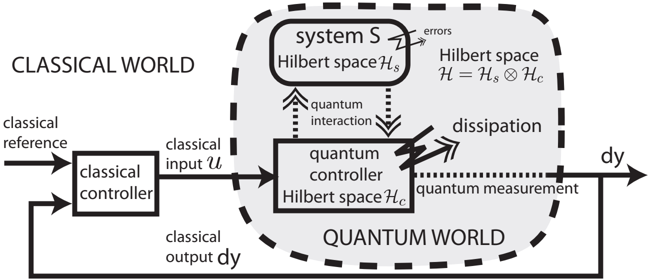
[17] C. Ahn, A. C. Doherty, and A. J. Landahl. Continuous quantum error correction via quantum feedback control. Phys. Rev. A, 65:042301, March 2002.

[18] Preliminary results in, e.g., G. Cardona, A. Sarlette, and PR. Exponential stochastic stabilization of a two-level quantum system via strict Lyapunov control. arXiv:1803.07542.

Outline

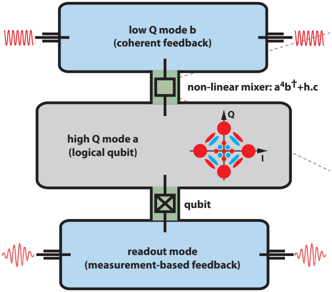
- Quantum analogue of Watt speed governor where a **dissipative** mechanical system controls another mechanical system[19]

- Coherent feedback where the controller is another quantum systems[20]:



[19] J.C. Maxwell: On governors. Proc. of the Royal Society, No.100, 1868.

[20] Optical pumping (**Kastler 1950**), coherent population trapping (Arimondo 1996), dissipation engineering, autonomous feedback: (Zoller, Cirac, Wolf, Verstraete, Devoret, Siddiqi, Lloyd, Viola, Ticozzi, Mirrahimi, Sarlette, ...)



- Quantic in Paris[a]: 3 theoreticians, 1 experimentalist, 4 PhD, 2 PostDocs.
- Development of theoretical methods and experimental devices ensuring robust processing of quantum information.

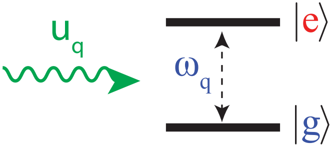
[a] `https://team.inria.fr/quantic/`

- Address Quantum Error Correction (QEC) in a new direction[21]: instead of relying on a large number of physical qubits and collective syndrome measurements to obtain a logical qubit, engineer a logical qubit of tunable high fidelity, localized in a single harmonic oscillator (**cat qubit**), relying on measurement-based and coherent feedback schemes, exploiting typical nonlinearities of Josephson superconducting circuits, and subject essentially to one error channel (finite photon life-time).

[21] M. Mirrahimi, Z. Leghtas, V.V. Albert, S. Touzard, R.J. Schoelkopf, L. Jiang, and M.H. Devoret. Dynamically protected cat-qubits: a new paradigm for universal quantum computation. New Journal of Physics, 16:045014, 2014.

Qubit (2-level system, half-spin) [22]

- Hilbert space:
  $\mathcal{H}_M = \mathbb{C}^2 = \left\{ c_g \left| g \right\rangle + c_e \left| e \right\rangle , \; c_g, c_e \in \mathbb{C} \right\}.$
- Quantum state space:
  $\mathcal{D} = \{\rho \in \mathcal{L}(\mathcal{H}_M), \rho^\dagger = \rho, \; \mathrm{Tr}\left(\rho\right) = 1, \rho \geq 0\} \; .$
- Operators and commutations:
  $\boldsymbol{\sigma_-} = \left| g \right\rangle \left\langle e \right|, \; \boldsymbol{\sigma_+} = \boldsymbol{\sigma_-}^\dagger = \left| e \right\rangle \left\langle g \right|$
  $\boldsymbol{\sigma_x} = \boldsymbol{\sigma_-} + \boldsymbol{\sigma_+} = \left| g \right\rangle \left\langle e \right| + \left| e \right\rangle \left\langle g \right|;$
  $\boldsymbol{\sigma_y} = i\boldsymbol{\sigma_-} - i\boldsymbol{\sigma_+} = i \left| g \right\rangle \left\langle e \right| - i \left| e \right\rangle \left\langle g \right|;$
  $\boldsymbol{\sigma_z} = \boldsymbol{\sigma_+}\boldsymbol{\sigma_-} - \boldsymbol{\sigma_-}\boldsymbol{\sigma_+} = \left| e \right\rangle\left\langle e \right| - \left| g \right\rangle\left\langle g \right|;$
  ${\boldsymbol{\sigma_x}}^2 = \boldsymbol{I}, \; \boldsymbol{\sigma_x}\boldsymbol{\sigma_y} = i\boldsymbol{\sigma_z}, \; [\boldsymbol{\sigma_x}, \boldsymbol{\sigma_y}] = 2i\boldsymbol{\sigma_z}, \; \ldots$

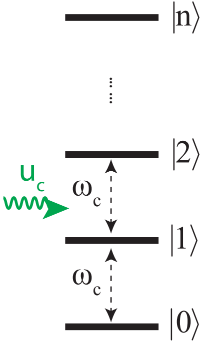


- Hamiltonian: $\boldsymbol{H}_M/\hbar = \omega_q \boldsymbol{\sigma_z}/2 + \boldsymbol{u_q}\boldsymbol{\sigma_x}.$
- Bloch sphere representation:
  $\mathcal{D} = \left\{ \frac{1}{2}\left(\boldsymbol{I} + x\boldsymbol{\sigma_x} + y\boldsymbol{\sigma_y} + z\boldsymbol{\sigma_z}\right) \; \middle| \; (x, y, z) \in \mathbb{R}^3, \; x^2 + y^2 + z^2 \leq 1 \right\}$

[22] See S. M. Barnett, P.M. Radmore: Methods in Theoretical Quantum Optics. Oxford University Press, 2003.

Quantum harmonic oscillator (spring system) [22]

- Hilbert space:
  $\mathcal{H}_S = \left\{ \sum_{n\geq 0} \psi_n \left| n \right\rangle, \; (\psi_n)_{n\geq 0} \in l^2(\mathbb{C}) \right\} \equiv L^2(\mathbb{R}, \mathbb{C})$
- Quantum state space:
  $\mathcal{D} = \{\rho \in \mathcal{L}(\mathcal{H}_S), \rho^\dagger = \rho, \; \mathrm{Tr}\,(\rho) = 1, \rho \geq 0\}$.
- Operators and commutations:
  $\boldsymbol{a} \left| n \right\rangle = \sqrt{n} \left| \boldsymbol{n\text{-}1} \right\rangle$, $\boldsymbol{a}^\dagger \left| n \right\rangle = \sqrt{n+1} \left| n+1 \right\rangle$;
  $\boldsymbol{N} = \boldsymbol{a}^\dagger \boldsymbol{a}$, $\boldsymbol{N} \left| n \right\rangle = n \left| n \right\rangle$;
  $[\boldsymbol{a}, \boldsymbol{a}^\dagger] = \boldsymbol{I}$, $\boldsymbol{a} f(\boldsymbol{N}) = f(\boldsymbol{N} + \boldsymbol{I})\boldsymbol{a}$;
  $\boldsymbol{D}_\alpha = e^{\alpha \boldsymbol{a}^\dagger - \alpha^\dagger \boldsymbol{a}}$.
  $\boldsymbol{a} = \boldsymbol{X} + i\boldsymbol{P} = \frac{1}{\sqrt{2}} \left(x + \frac{\partial}{\partial x} \right)$, $[\boldsymbol{X}, \boldsymbol{P}] = \imath \boldsymbol{I}/2$.
- Hamiltonian: $\boldsymbol{H}_S/\hbar = \omega_c \boldsymbol{a}^\dagger \boldsymbol{a} + \boldsymbol{u_c}(\boldsymbol{a} + \boldsymbol{a}^\dagger)$.
  (associated classical dynamics:
  $\frac{dx}{dt} = \omega_c p, \; \frac{dp}{dt} = -\omega_c x - \sqrt{2} u_c$).



- Classical pure state $\equiv$ coherent state $\left| \alpha \right\rangle$
  $\alpha \in \mathbb{C}: \; \left| \alpha \right\rangle = \sum_{n \geq 0} \left(e^{-|\alpha|^2/2} \frac{\alpha^n}{\sqrt{n!}} \right) \left| n \right\rangle$; $\left| \alpha \right\rangle \equiv \frac{1}{\pi^{1/4}} e^{\imath \sqrt{2} x \Im \alpha} e^{-\frac{(x - \sqrt{2} \Re \alpha)^2}{2}}$
  $\boldsymbol{a} \left| \alpha \right\rangle = \alpha \left| \alpha \right\rangle$, $\boldsymbol{D}_\alpha \left| 0 \right\rangle = \left| \alpha \right\rangle$.