# Encoding a qudit in an oscillator

Daniel Gottesman
Alexei Kitaev
John Preskill

# Encoding a qudit in an oscillator

-- Classical information can be either analog or digital.
Digital classical information is more robust.

-- Quantum information can be carried by either a finite-dimensional system (two-level atom, electron spin, . .) or an infinite-dimensional system (harmonic oscillator, rotor, . .).

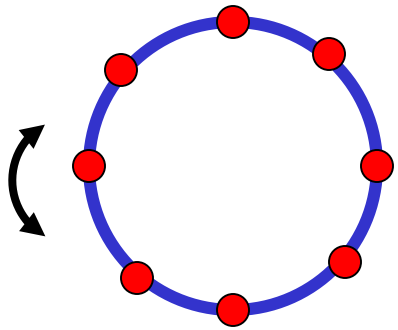
-- Although a qubit is in a sense continuous (vector in a Hilbert space), a qubit like a classical bit, if cleverly encoded, can be protected from the gradual accumulation of small errors, or from decoherence due to interactions with the environment.

-- Can we also protect the quantum state of a system described by *continuous quantum variables*?

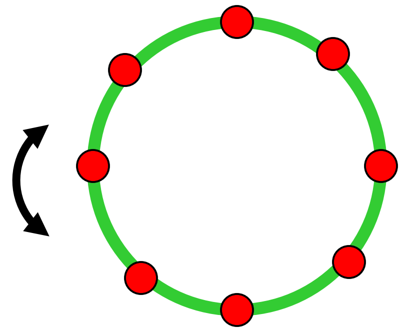
-- Probably not. But we can use the continuous variable systems available in the physics laboratory to encode a robust finite-dimensional system. ("*Encoding a qudit in an oscillator*")

# Error model: shifts in amplitude and phase

Consider a *d*-dimensional system ("qudit"):

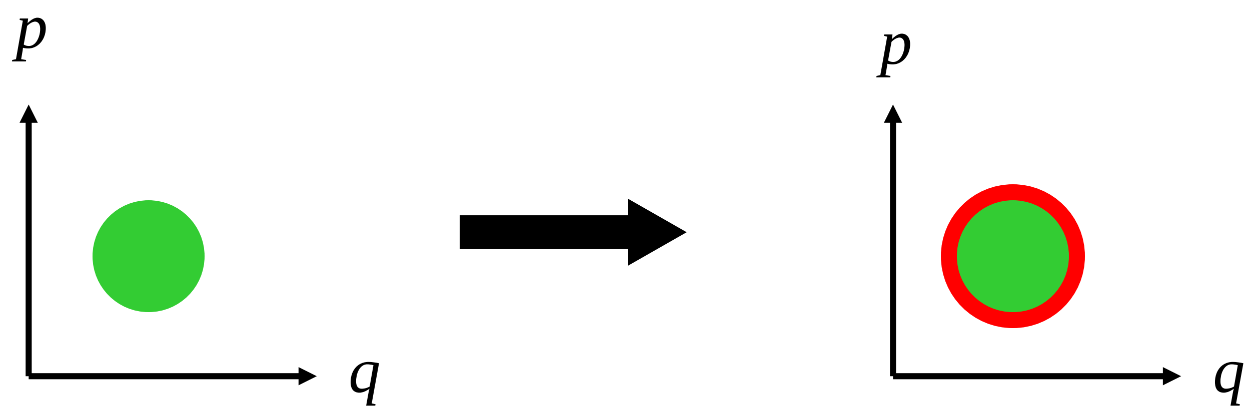


amplitude
shift



phase
shift

Or the "quantum diffusion" of a particle:



# Qudit

Basis: $|j\rangle, \quad j = 0,1,2,\ldots,(d-1)$

Operators: $\omega = \exp(2\pi i/d)$ (amplitude shift)

$Z: \quad |j\rangle \rightarrow \omega^j |j\rangle,$ (phase shift)

$X: \quad |j\rangle \rightarrow |j+1\rangle,$

Commutator: $ZX = \omega XZ$

Pauli Operator Basis: $X^a Z^b, \quad a,b = 0,1,2,\ldots,(d-1)$

Can we correct errors with $|a|, |b| << d$?

# Stabilizer Codes

-- A code is a simultaneous eigenspace of a set of commuting operators $S_i$ , the generators of the code's stabilizer group $\mathcal{S}$.

-- $\{E_a\}$ is a unitary operator basis (e.g., the Pauli operators).

-- $\mathcal{E}$ is the set of "likely" errors that we want to be able to correct.

-- Nondegenerate code: All $E_a$ in $\mathcal{E}$ modify the eigenvalues of the stabilizer generators in distinguishable ways:

$$S_i E_a = \omega_{a,i} E_a S_i \; .$$

We can diagnose the errors, without disturbing the encoded state, by measuring the generators.

-- We usually assume that $\mathcal{E}$ is the set of tensor products of Pauli operators with weight up to $t$, but the same principles allow us to protect against errors with other properties.

# Encoding one oscillator in nine

Braunstein,
Lloyd-Slotine
(Shor)

The code is the simultaneous eigenspace (with eigenvalue 0) of the eight mutually commuting operators:

$$q_1 - q_2 = 0\,, \quad q_4 - q_5 = 0, \quad q_7 - q_8 = 0,$$
$$q_2 - q_3 = 0\,, \quad q_5 - q_6 = 0, \quad q_8 - q_9 = 0,$$

$$(p_1 + p_2 + p_3) - (p_4 + p_5 + p_6) = 0,$$
$$(p_4 + p_5 + p_6) - (p_7 + p_8 + p_9) = 0\,.$$

"Logical" operators that preserve the code space are:

$$\bar{q} = q_1 + q_4 + q_7\ ,$$
$$\bar{p} = p_1 + p_2 + p_3\,.$$

This code is designed to correct errors in which one particle makes a large jump in $p$ or $q$, while the others hold fixed. But it does not protect against small diffusive motions that allow the logical operators to drift.

# A shift-resistant code with $d$=18

The code is the simultaneous eigenspace with eigenvalue 1 of the two stabilizer generators:

$$X^6, \quad Z^6$$

There is an encoded *qubit*; logical operators that commute with the stabilizer (and so preserve the code space) are:

$$\bar{X} = X^3, \quad \bar{Z} = Z^3$$

The commutation relations of the stabilizer generators with the Pauli operators are:

$$(X^a Z^b) X^6 = \omega^{6b} X^6 (X^a Z^b),$$

$$(X^a Z^b) Z^6 = \bar{\omega}^{6a} Z^6 (X^a Z^b).$$

For $a$, $b$ = {-1, 0, 1}, there is a unique syndrome for each error. The code can correct a shift by one unit in amplitude or phase.

# A shift-resistant code with $d$=18

A basis for the code space with $Z^6 = X^6 = 1$ is:

$$|\bar{0}\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |6\rangle + |12\rangle)\,,$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{3}}(|3\rangle + |9\rangle + |15\rangle)\,.$$

Shifts in amplitude by +1 or -1 are corrected by adjusting $|\,j\rangle$ to the nearest multiple of 3. Phase shifts are corrected similarly in the conjugate basis.

The code is "perfect": there are (3) X (3) = 9 possible syndromes for the phase and amplitude errors, and the code space has dimension 2; since (2) X (9) = 18, every possible syndrome is valid.

$d$=18 is the minimal dimension for correcting shifts by one in amplitude and phase.

# Shift-resistant codes

Suppose that $d = rsn$ , where *r, s, n are integers.*

A basis for the *n*-dimensional code space is:

$$|\bar{0}\rangle = \frac{1}{\sqrt{s}}(|0\rangle + |nr\rangle + |2nr\rangle + \cdots + |(s-1)nr\rangle),$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{s}}(|r\rangle + |(n+1)r\rangle + |(2n+1)r\rangle + \cdots + |[(s-1)n+1]r\rangle),$$

$$\vdots \qquad\qquad \vdots$$

$$|\overline{n-1}\rangle = \frac{1}{\sqrt{s}}(|(n-1)r\rangle + |(2n-1)r\rangle + |(3n-1)r\rangle + \cdots + |(sn-1)r\rangle).$$

Similar in the conjugate (Fourier transformed) basis, but with *r* and *s* interchanged.

This code can correct all shifts that satisfy:

$$|a| \le (r-1)/2, \quad |b| \le (s-1)/2$$

# The limit $d \to \infty$

We cannot scale $d \to \infty$ while holding $r/d$ and $s/d$ fixed, since

$$\frac{r}{d} = \frac{1}{ns}, \quad \frac{s}{d} = \frac{1}{nr}$$

Nevertheless interesting codes are obtained in the limit of continuous variables, because the ranges of $q$ and $p$ are unbounded.

(Alternatively, we can take $d \to \infty$ with $r/d$ fixed and obtain a periodically identified *rotor* with quantized but unbounded angular momentum.)

Stabilizer generators: $\exp(2\pi i q/\alpha), \quad \exp(inp\alpha)$

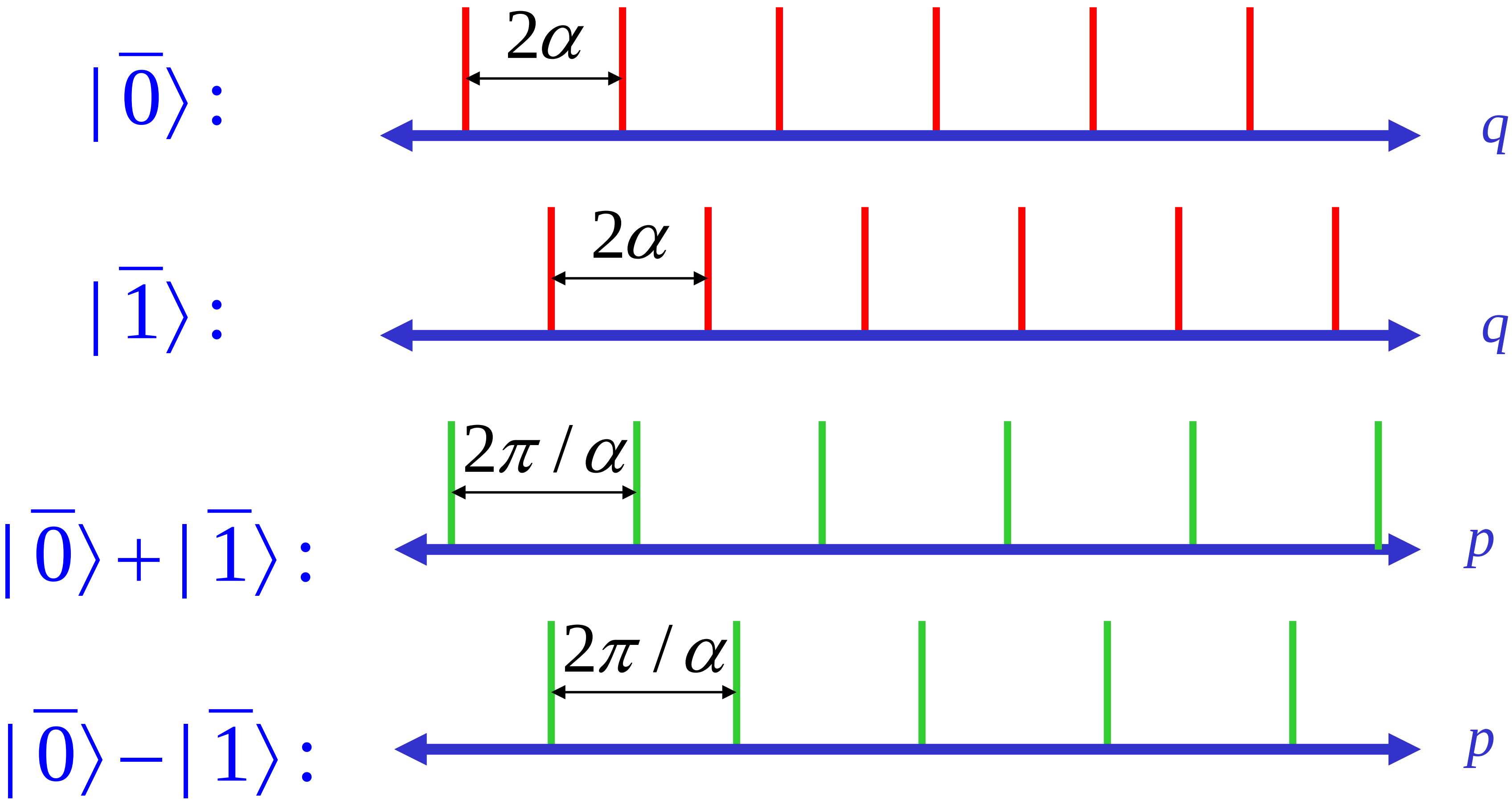
Encoded operators: $\bar{Z} = \exp(2\pi i q / n\alpha), \quad \bar{X} = \exp(ip\alpha)$

The $n$-dimensional code space is protected against shifts that satisfy:

$$|\Delta q| < \frac{\alpha}{2}, \quad |\Delta p| < \frac{\pi}{n\alpha}.$$

# A qubit encoded in an oscillator

Formally, the basis states for the code space are coherent superpositions of equally spaced states, infinitely squeezed in $p$ and $q$:




This code can correct all shifts that satisfy:

$$|\Delta q|<\frac{\alpha}{2},\quad |\Delta p|<\frac{\pi}{2\alpha}.$$

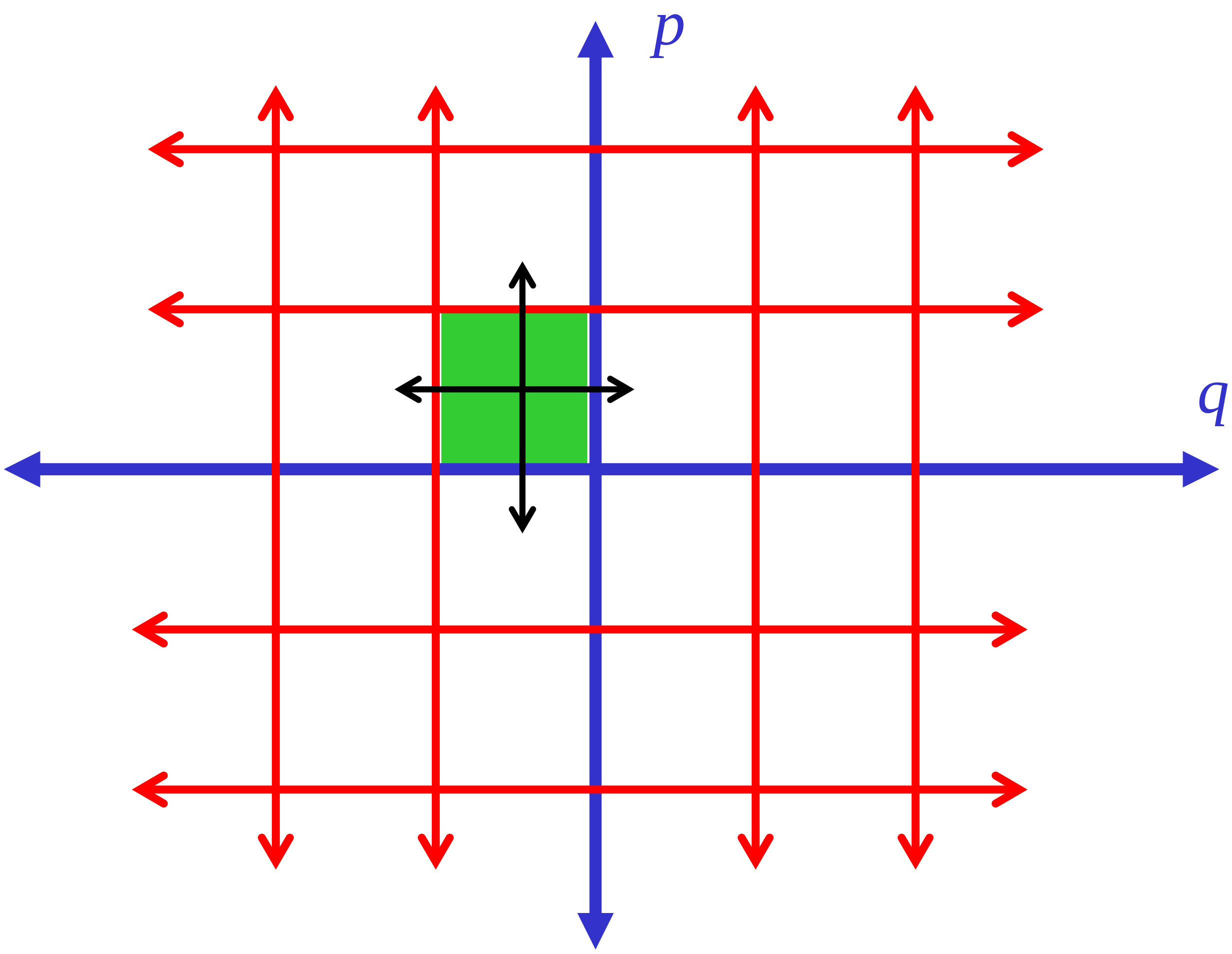
# Stabilizer: a lattice of commuting translations in phase space

The unit cell of the stabiilzer lattice has area

$$2\pi n\hbar .$$

(one encoded state per area $h$ in phase space).

The encoded operations (commuting with stabilizer) form a finer lattice, whose unit cell has area $2\pi\hbar / n.$

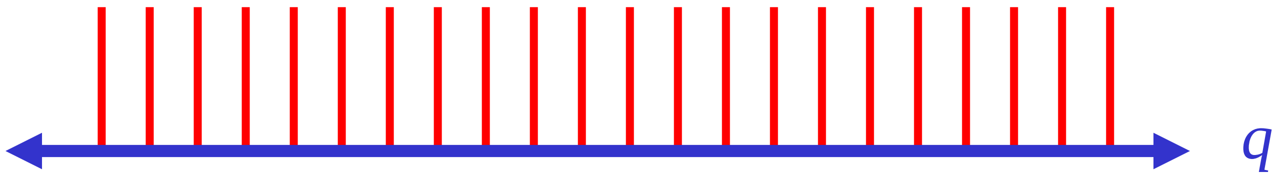



Generalizes to a commuting lattice in $2N$-dimensional phase space.

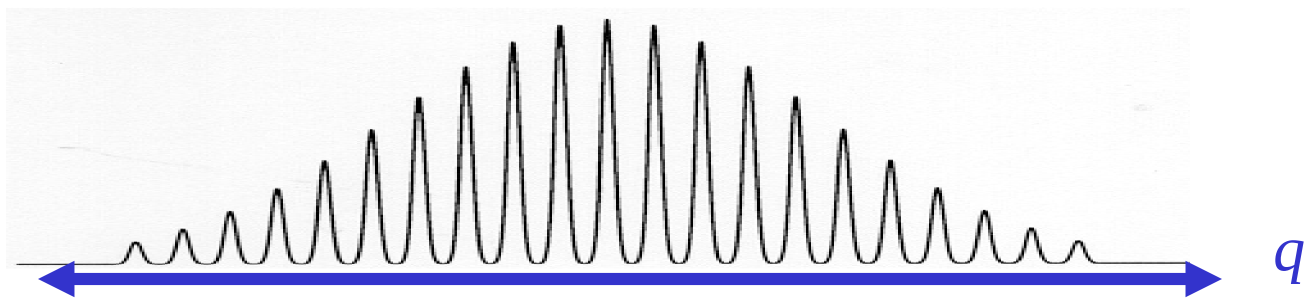
# Finitely squeezed codewords

Realistic codewords are *normalizable*, *finitely squeezed* in $p$ and $q$:

Not



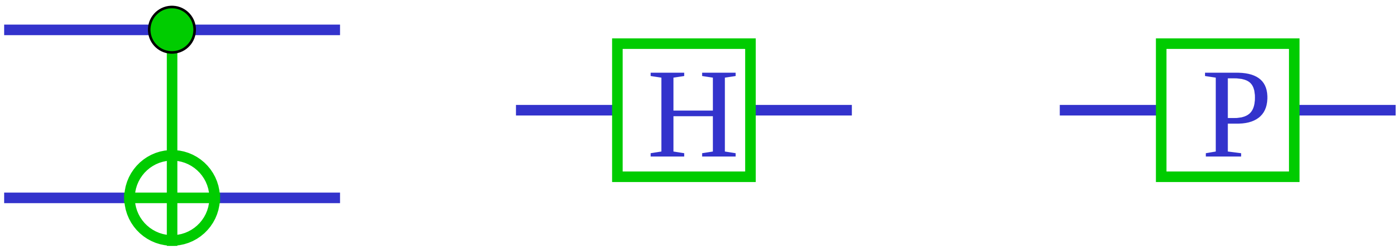

but




Small shifts in $p$ and $q$ can still be detected
and reversed with high fidelity.

# Symplectic operations

Clifford group gates on the code space, generated by:




-- Can be implemented as linear transformations on the *p*'s annd *q*'s (that preserve the canonical commutation relations) -- the *symplectic* transformations. These gates are "easy": they can be implemented with linear optics and squeezing.

Furthermore, the implementation is *fault tolerant*. In this context, fault tolerance means that the gates do not *magnify* errors; e.g., do not turn a (tolerable) small shift in *q* or *p* into a (damaging) large shift.

To complete the universal gate set, we must reach transformations that are not symplectic. This can be achieved via *photon counting*.

# Universal computation via photon counting

-- We can complete the universal gate set by preparing an eigenstate of the single-qubit Hadamard gate:

$$-\boxed{H}- \; = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

-- The Hadamard is implemented on the code space by performing a Fourier transform on *p* and *q*:

$$\exp[i(\pi/2)a^{\dagger}a]: \quad \begin{array}{l} q \to p \\ p \to -q \end{array}$$

-- The eigenvalue of the Hadamard is the photon number modulo 4.

-- We can prepare an entangled state of two encoded qubits, and measure photon number of one of the oscillators, preparing the other oscillator in a Hadamard eigenstate.

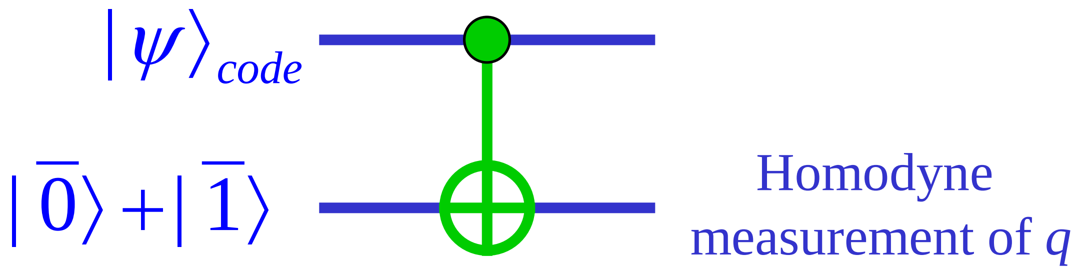
-- The state can then be *purified*.

# Error detection and recovery

CNOT is the symplectic transformation:

$$q_1 \rightarrow q_1 \qquad\qquad p_1 \rightarrow p_1 - p_2$$

$$q_2 \rightarrow q_1 + q_2 \qquad\qquad p_2 \rightarrow p_2$$




-- The CNOT propagates the shift in $q$ of the data forward to the ancilla, where it can be read out via a destructive measurement of the $q$ quadrature of the ancilla.

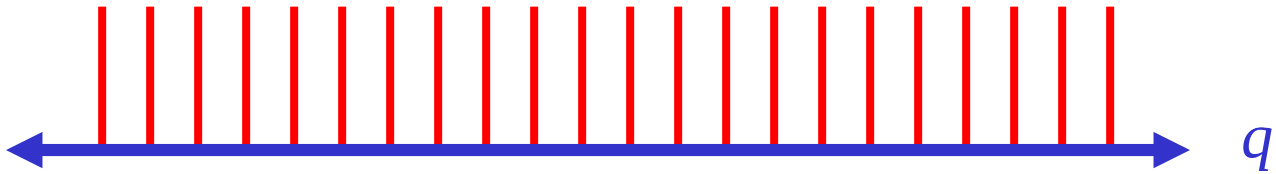
--To recover, apply a shift by -$q$ modulo $\alpha$ to the data.

--Similar procedure corrects shift in $p$.

# Preparing an encoded state

Encoding is the most challenging part of using continuous variable codes. Symplectic operations alone are not adequate for encoding, since each letter must satisfy two independent stabilizer conditions.

To prepare:




Start with $p$ eigenstate:


Then measure $q$ modulo $\alpha$ .

For example: couple the oscillator to a meter $H' = \kappa\, q\, (b^\dagger b)_{meter}$ .

Frequency of the meter shifts by $\Delta\omega_{meter} = \kappa\, q$ .

In time $t = 2\pi / \kappa\alpha$ , phase of meter advances by $\boxed{\theta = 2\pi q / \alpha}$

# Quantum key distribution with squeezed states

Alice

Alice and Bob generate a key bit by transmitting an oscillator, as follows:

1) Alice sends either a $q$ eigenstate or a $p$ eigenstate.

2) Bob measures either $q$ or $p$.

3) Alice broadcasts $q$ modulo $\alpha$, or $p$ modulo $\pi/\alpha$.

Bob

4) Bob subtracts Alice's value from what he measured, and then corrects to the nearest integer multiple of $\alpha$ or $\pi/\alpha$.

5) The key bit is determined by whether the multiple of $\alpha$ or $\pi/\alpha$ is even or odd.

-- Alice and Bob sacrifice some bits for verification. If the error rate is below 11% for both $p$ and $q$ transmissions, then the protocol, enhanced by classical binary error correction and privacy amplification, is provably secure.

-- The proof bounds the eavesdropper's mutual information with the key by invoking the ability of the continuous variable code to correct errors in both $p$ and $q$.

-- $q$ "eigenstates" need to be squeezed to width small compared to $\alpha$, and range of $q$ sampled needs to be $\sim 13\,\alpha$ (or larger). Similar for $p$ (with $\alpha$ replaced by $\pi/\alpha$) .

# Encoding a qudit in an oscillator

• Eventually, continuous variable codes may be used for robust storage and processing of quantum information.

• Some physical realizations:

-- mode of electromagnetic field in a cavity, protected against drift in $p$ and $q$.

-- a superconducting dot, protected against drift in phase $\theta$ and jump in charge $Q$.

-- single electron in a Landau level, protected against drift in $p_x$ and $p_y$.

• Continuous variable codes can be used to demonstrate the security of quantum key distribution protocols using squeezed states. For these protocols, it is necessary only to prepare and transmit states squeezed in $q$ or $p$, and to measure the $q$ or $p$ quadrature.