A Whirlwind Tour of Quantum Error Correction (with some emphasis on Bosonic codes)

Ronak Ramachandran

University of Texas at Austin

June 28, 2022

Disclaimer

This slide deck is a bit messy since it was cobbled together from multiple sources last minute. If you're reading this to learn, and feel something major is missing, please email ronak dot ramachandran at gmail dot com with any questions you have.

Outline of talk

1. Classical error correction: linear binary codes
2. An unnecessary detour into group theory
3. Stabilizer formalism: stabilizer codes
4. Bosonic quantum computing: Fock-basis codes
5. Continuous Variable (CV) quantum computing: GKP codes

Table of Contents

What is a code?

Definition

A **code** of block length n over an alphabet Σ is a subset of Σ^n. Typically, we will use q to denote $|\Sigma|$.

Definition

The **dimension** of a code $C \subseteq \Sigma^n$ is given by $k := \log_q(|C|)$

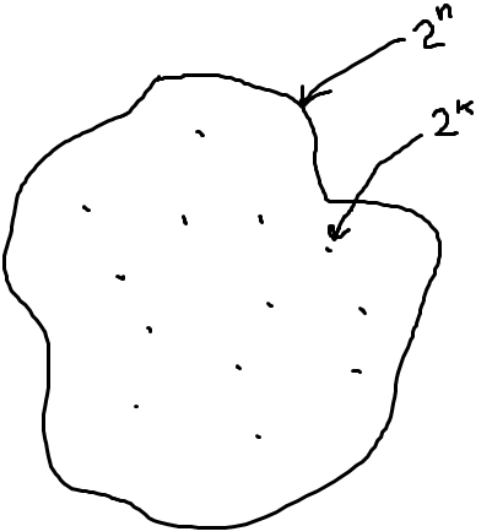
Definition

The **rate** of a code with block length n and dimension k is $R := \frac{k}{n}$

Source: GRS Coding Theory Textbook

In the case of binary codes...

$\Sigma = \{0,1\}$, $\Sigma^n = \{0,1\}^n$, $k = \log_2(|C|)$



Distance

Definition

Given two vectors $u, v \in \Sigma^n$, the **Hamming distance** between u and v, denoted by $\Delta(u, v)$, is the number of positions in which u and v differ.

Definition

Let $C \subseteq \Sigma^n$. The minimum distance (or just **distance**) of C, denoted $\Delta(C)$ (or just d), is defined to be $\Delta(C) = \min_{c_1 \neq c_2 \in C} \Delta(c_1, c_2)$.

Definition

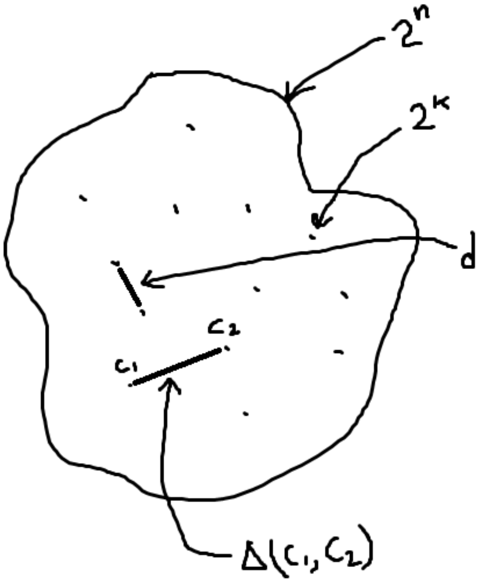
The **relative distance** of a code is given by $\delta := \frac{d}{n}$.

Codes: Block length, dimension, and distance, $[n, k, d]$.

Families of codes: rate and distance $[R, \delta]$.

Source: GRS Coding Theory Textbook

And that looks something like...

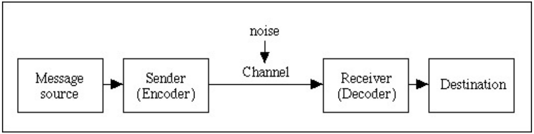


The repetition code

$C = \{000, 111\}$

$n = 3$, $k = 1$, $d = 3$, so we say this is a $[3, 1, 3]$ code.

I don't see any errors...



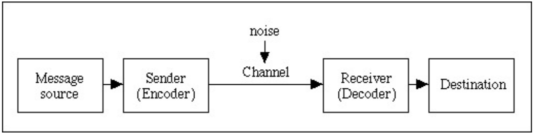
Definition

Let $C \subseteq \Sigma^n$. An equivalent description of the code C is an injective mapping $E : [|C|] \to \Sigma^n$ called the **encoding function**.

Definition

Let $C \subseteq \Sigma^n$ be a code. A mapping $D : \Sigma^n \to [|C|]$ is called a decoding function for C.

The repetition code is SECDED



Imagine noise in the form of bit flips.

The $[3, 1, 3]$ repetition code $C = \{000, 111\}$ can correct 1 error and can detect 2

Single Error Correcting, Double Error Detecting (SECDED)

In general, a code with distance d can correct $\frac{d-1}{2}$ errors and detect $d - 1$ errors.

Linear Binary Codes

$\Sigma = \{0, 1\}$.

If $x, y \in C$, then $x \oplus y \in C$.

Note this implies $x \oplus x = 0 \in C$.

Additionally, if $\Delta(x, y) = d$ (the minimum distance), then $x \oplus y \in C$ and $|x \oplus y| = d$.

The above implies d is the weight of the minimum weight codeword.

Generator Matrices and Parity Check Matrices

A linear binary code can always be specified by a generator matrix and parity check matrix.

Example: The $[7,4,3]$ Hamming code. (Can correct 1 error.)

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Encoder: given $x \in \{0,1\}^4$ (as a row vector), $xG \in C$

Detect error: $Hc^\top = 0$ iff $c \in C$. $Hc^\top$ is called the **syndrome**.

Correct error: find the column of H matching the syndrome.

Table of Contents

Overview of this section

Def'n of a group, examples

Action of a group G on a set X

What stabilizers are in group theory

Action of Pauli gates (a group) on quantum states (a set)

The stabilizer formalism

Some group theory

Definition

A **group** is a set G together with a binary operation $\cdot$ on G such that

(Def'n of "binary operation on G") $\forall a, b \in G$, $a \cdot b \in G$

(Identity) $\exists 1 \in G$ such that $\forall a \in G$, $1 \cdot a = a \cdot 1 = a$

(Associativity) $\forall a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(Inverses) $\forall a \in G$, $\exists b \in G$ such that $a \cdot b = 1$. Such b is denoted a^{-1}.

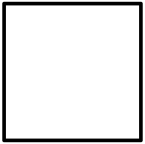
Cheat-sheet version:

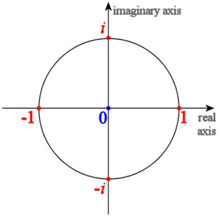
$ab \in G$, $1a = a1 = a$, $a(bc) = (ab)c$, $aa^{-1} = a^{-1}a = 1$.

"Closed under $\cdot$ with an identity, associativity, and inverses."

An example group: C_4

"The cyclic group of order 4" - rotational symmetries on a square.





$C_4 = \{1, x, x^2, x^3\} = \langle x \rangle \leftarrow$ we say x is a **generator** of C_4.

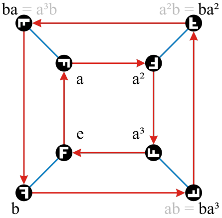
$C_4 = \{1, i, -1, -i\}$.

$$C_4 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}.$$

$\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}_4 = \{0, 1, 2, 3\}$, Group operation: $+$ ("additive" group).

Second example: D_4

"The dihedral group of order 4" - symmetries on a square including rotations and reflections.



	ϵ	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
ϵ	ϵ	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
σ	σ	σ^2	σ^3	ϵ	$\sigma^3\tau$	τ	$\sigma\tau$	$\sigma^2\tau$
σ^2	σ^2	σ^3	ϵ	σ	$\sigma^2\tau$	$\sigma^3\tau$	τ	$\sigma\tau$
σ^3	σ^3	ϵ	σ	σ^2	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	τ
τ	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	ϵ	σ	σ^2	σ^3
$\sigma\tau$	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$	τ	σ^3	ϵ	σ	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma^3\tau$	τ	$\sigma\tau$	σ^2	σ^3	ϵ	σ
$\sigma^3\tau$	$\sigma^3\tau$	τ	$\sigma\tau$	$\sigma^2\tau$	σ	σ^2	σ^3	ϵ

$D_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\} = \langle x, y\rangle$, where $yx = x^{-1}y$.

Note $yx = x^{-1}y = x^3y \neq xy$ (D_4 is non-abelian).

Homomorphisms: 'embedding one group into another'

Definition

A **homomorphism** between two groups $(G, \cdot)$ and $(P, *)$ is a function $\varphi : G \to P$ such that $\varphi(g \cdot h) = \varphi(g) * \varphi(h)$.

Example: For any groups G and P, $\varphi(g) = 1_P$ is a valid homomorphism. (The trivial homomorphism.)

Product Groups

Definition

For any groups G and P, the product group is given by $G \times P = \{(g,p) \mid g \in G, p \in P\}$ with the group operation $(g,p) \cdot (h,q) = (gh, pq)$.

Like a tensor product.

Group G acting on a set X

"A homomorphism from G to Perm(X)."

$$\alpha : G \times X \to X$$
$$\alpha(e, x) = x$$
$$\alpha(g, \alpha(h, x)) = \alpha(gh, x)$$

$g \to [\sigma_g : X \to X]$	$g \to [g : X \to X]$	
$\sigma_e(x) = x$	$e(x) = x$	$ex = x$
$\sigma_g(\sigma_h(x)) = \sigma_{gh}(x)$	$g(h(x)) = gh(x)$	$g(hx) = (gh)x$

Group G acting on a set X

$C_4 = \{1, x, x^2, x^3\}$ acting on a toothpick.

Toothpick has two states: horizontal and vertical, $X = \{|, -\}$.

$1(|) = |$, $1(-) = -$.

$x(|) = -$, $x(-) = |$.

$x^2(|) = |$, $x^2(-) = -$.

$x^3(|) = -$, $x^3(-) = |$.

Definition

We say $g \in G$ **stabilizes** $x \in X$ iff $gx = x$.

Definition

The **stabilizer subgroup** of G with respect to $x \in X$ is $G_x = \{g \in G \mid gx = x\}$.

The stabilizers of $|$ are 1 and x^2.

The Pauli group

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

16 element group:

$P_1 = \langle X, Y, Z \rangle = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$.

Properties:

$$X^2 = Y^2 = Z^2 = 1$$

$$\begin{aligned} XY &= iZ & \qquad YZ &= iX & \qquad ZX &= iY \\ YX &= -iZ & \qquad YZ &= -iX & \qquad ZX &= -iY \end{aligned}$$

n-qubit Paulis

The n-qubit Paulis form a group P_n of order 4×4^n.

For instance, P_2 has $4 \times 16 = 64$ elements. Examples: XI and $-iZZ$.

At the same time, P_n only has $3n$ generators.

For instance, $P_2 = \langle XI, YI, ZI, IX, IY, IZ \rangle$.

We can have the n-qubit Pauli group act on the set of n-qubit states.

The single qubit case

The states stabilized by P_1 are very special:

I stabilizes all $\qquad\qquad$ $-I$ stabilizes none

$$Z|0\rangle = |0\rangle \qquad X|+\rangle = |+\rangle \qquad Y|i\rangle = |i\rangle$$
$$-Z|1\rangle = |1\rangle \qquad -X|-\rangle = |-\rangle \qquad -Y|-i\rangle = |-i\rangle$$

These are the axes of the Bloch sphere.

The stabilizer formalism

Paraphrasing a bit: "The key idea of the stabilizer formalism is to represent a quantum state $|\psi\rangle$, not by a vector of amplitudes, but by a stabilizer group, consisting of unitary matrices that stabilize $|\psi\rangle$. At first stabilizers seem worse than amplitude vectors, since they require about 2^2n parameters to specify instead of about 2^n. Remarkably, though, a large and interesting class of quantum states can be specified uniquely by much smaller stabilizer groups—specifically, the intersection of Stab$(|\psi\rangle)$ with the Pauli group."

Theorem 1 *Given an n-qubit state $|\psi\rangle$, the following are equivalent:*

(i) $|\psi\rangle$ *can be obtained from* $|0\rangle^{\otimes n}$ *by CNOT, Hadamard, and phase gates only.*

(ii) $|\psi\rangle$ *can be obtained from* $|0\rangle^{\otimes n}$ *by CNOT, Hadamard, phase, and measurement gates only.*

(iii) $|\psi\rangle$ *is stabilized by exactly* 2^n *Pauli operators.*

(iv) $|\psi\rangle$ *is uniquely determined by* $S(|\psi\rangle) = \mathrm{Stab}(|\psi\rangle) \cap \mathcal{P}_n$*, or the group of Pauli operators that stabilize* $|\psi\rangle$*.*

The Gottesman-Knill Theorem

Theorem

Any stabilizer circuit—that is, a quantum circuit consisting solely of CNOT, Hadamard, and phase gates—can be simulated efficiently on a classical computer. See paper.

Table of Contents

Quantum Error Correcting Codes

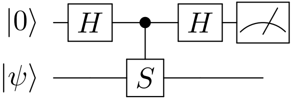
In general, specifying a Quantum Error Correcting Code (QECC) requires 4 steps:

1. Define an error model
2. Specify a codespace through stabilizing operations (syndrome measurements)
3. Show how to perform a universal set of gates on encoded states
4. Show how to prepare and decode codestates.

Stabilizer Codes

Error model: Pauli errors of a certain weight (aka k-qubit bit flips or phase flips). Actually can correct more than just these - syndrome measurements discretize errors.

Codespace: For k dimensional codespace, pick an abelian Pauli subgroup with $n - k$ generators. Make these your stabilizing operations. Perform syndrome measurements:



Gates, encoding, and decoding vary from code to code.

Example: The Steane Code

Click to go to the Steane Code Wiki

Table of Contents

Fock states (Number states)

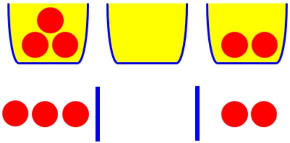
The Fock basis: list of excitation numbers

Excitation numbers can refer to the discrete energy levels of a list of oscillators or the count of photons in a list of modes

Example: 3 photons in 2 modes.

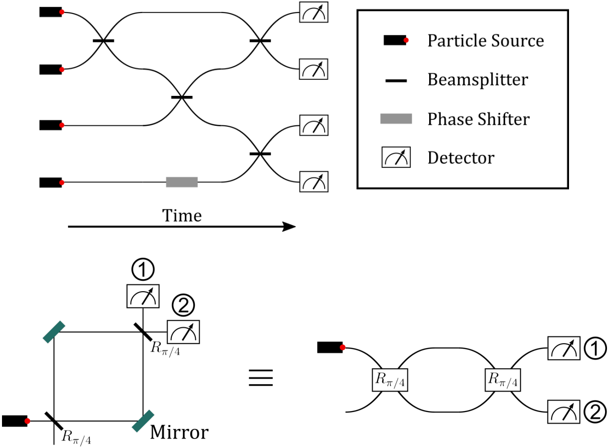
Basis states: $|3,0\rangle$, $|2,1\rangle$, $|1,2\rangle$, $|0,3\rangle$.

In general, for n photons in m modes, Hilbert space has dimension $\binom{n+m-1}{n}$



Bosonic QC

Linear optical networks



Whiteboard time

How do $m \times m$ beamsplitters translate to $M \times M$ unitaries?

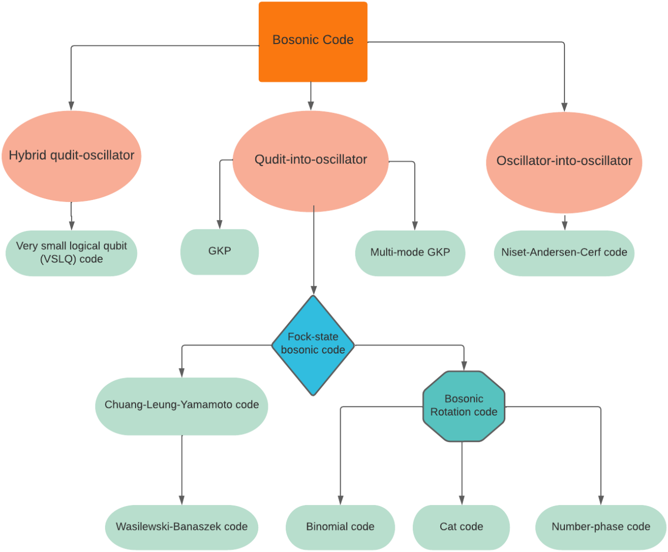
Fock State Codes

Go to paper in progress + wiki for more on these.

Table of Contents

Overview of this section

Bird's Eye View of Bosonic Codes



Qubits and Qudits

Qubits have 2 basis states: $|0\rangle$ and $|1\rangle$

$X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$

$Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$

$X : |n\rangle \mapsto |n+1\rangle$, with addition in $\mathbb{F}_2$

$Z : |n\rangle \mapsto \omega^n |n\rangle$, where $\omega = e^{2\pi i/2} = -1$

Qudits have d basis states: $|0\rangle, |1\rangle, |2\rangle, \ldots, |d-1\rangle$

$X_d : |n\rangle \mapsto |n+1\rangle$, with addition in $\mathbb{F}_d$

$Z_d : |n\rangle \mapsto \omega^n |n\rangle$, where $\omega = e^{2\pi i/d}$

These “Shift” and “Clock” operators generalize Pauli X and Z

The Fourier Conjugate Basis

For qubits: $H = \mathsf{QFT}_2$

Conjugate basis $H\left|0\right\rangle = \left|+\right\rangle$ and $H\left|1\right\rangle = \left|-\right\rangle$

For qudits, use:

$$\left|\omega^n\right\rangle := \mathsf{QFT}_d \left|n\right\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \omega^{n \cdot m} \left|m\right\rangle$$

"Position" basis: $\left|0\right\rangle, \left|1\right\rangle, \left|2\right\rangle, \ldots, \left|d-1\right\rangle$

"Momentum" basis: $\left|\omega^0\right\rangle, \left|\omega^1\right\rangle, \left|\omega^2\right\rangle, \ldots, \left|\omega^{d-1}\right\rangle$

Note that $Z_d \left|\omega^n\right\rangle = \left|\omega^{n+1}\right\rangle$ and $X_d \left|\omega^n\right\rangle = \omega^{-n} \left|\omega^n\right\rangle$

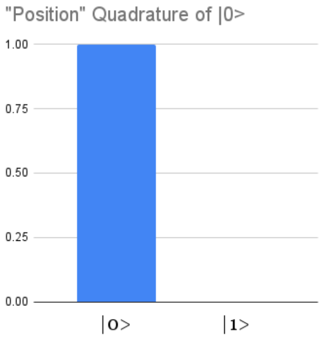
Quadratures

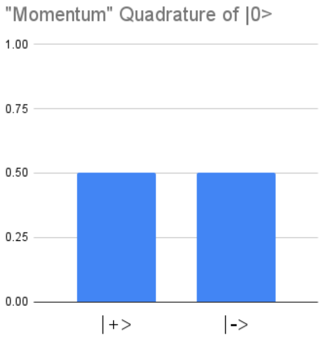
Quadratures $\equiv$ Fourier conjugate bases

Can plot marginal probability distributions for a given state $|\psi\rangle$

"Projections" of $|\psi\rangle$ onto the position and momentum bases

Knowing one quadrature with certainty means you know little about the other





The Wigner Function: A Helpful Visual Tool

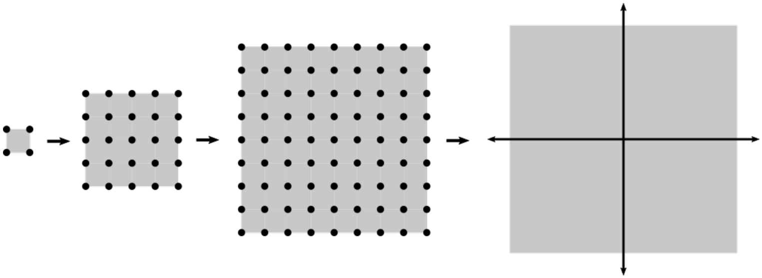
The Wigner Function: Properties

A "Quasiprobability distribution" (can be negative)

To determine the probability of $|n\rangle$, we sum over all spikes with "position" coordinate $|n\rangle$ (same thing for "momentum" basis)

Normalized (all spikes sum to 1)

What happens when we take the limit as $d \to \infty$?



Continuous Variable Quantum Computing (CV)

Infinitely many (position) basis states $|q\rangle$

Note that $|q\rangle$ and $|q+\varepsilon\rangle$ are orthogonal!

Fourier conjugate basis (momentum): $|p\rangle$

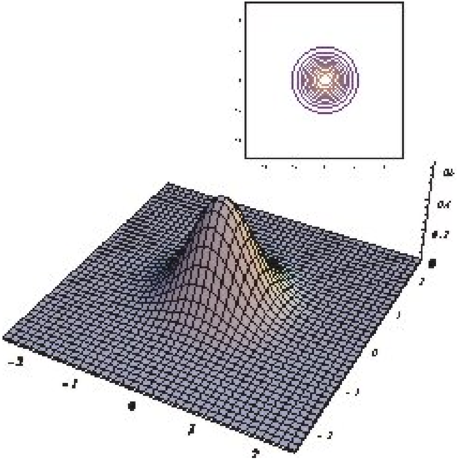
One more basis that's completely new: the number basis, $|n\rangle$

Perfect spikes are no longer feasible, best we can hope for is Gaussians

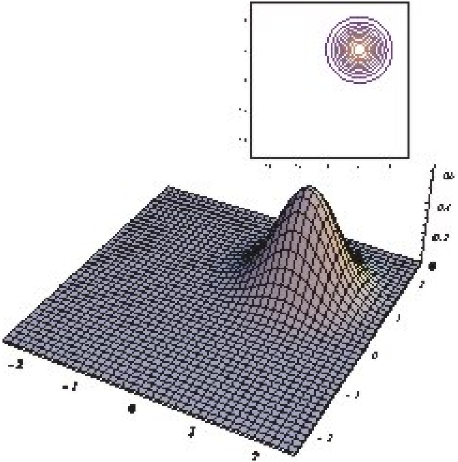
Coherent states:

$$|\alpha\rangle = \frac{1}{\sqrt{e^{|\alpha|^2}}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

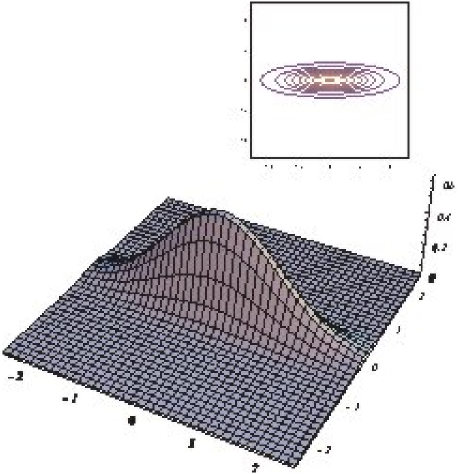
The CV Wigner Function: Vacuum State $|0\rangle$



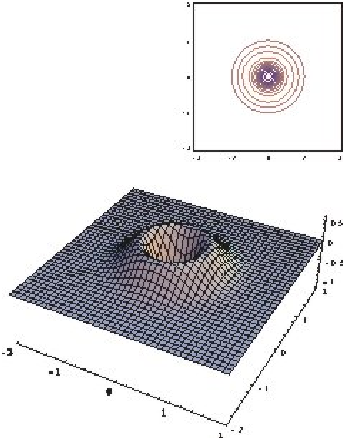
The CV Wigner Function: Coherent State $|\alpha\rangle$

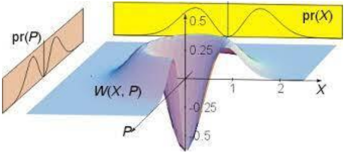


The CV Wigner Function: Squeezed Vacuum

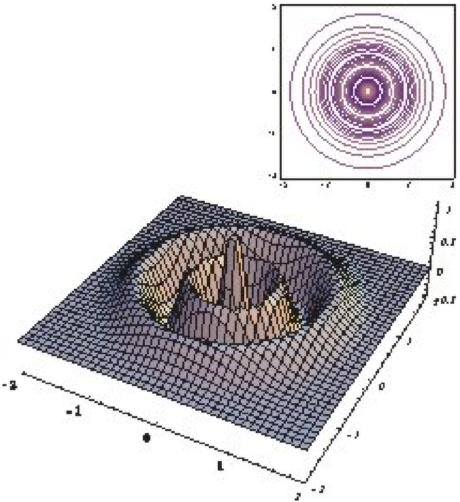


The CV Wigner Function: Fock State $|1\rangle$ (one photon)

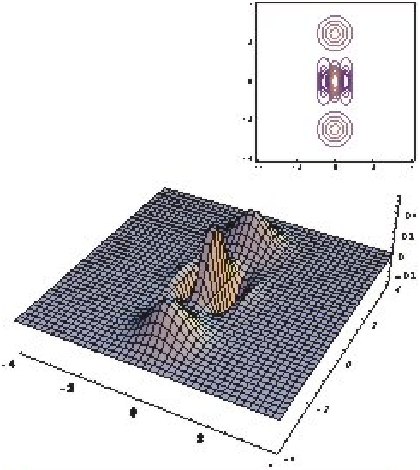




The CV Wigner Function: Fock State $|4\rangle$ (four photons)



The CV Wigner Function: Cat State



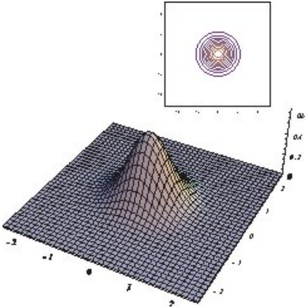
$$\boxed{|\Psi\rangle = |\alpha\rangle + |-\alpha\rangle}$$

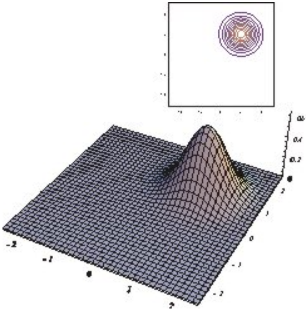
Displacement Operator

Displacement operator: $D(\alpha) = \exp(\alpha\hat{a} - \alpha^*\hat{a}^\dagger)$

$D(\alpha)\left|0\right\rangle = \left|\alpha\right\rangle$

$D(\alpha)\left|\beta\right\rangle = \left|\alpha+\beta\right\rangle$



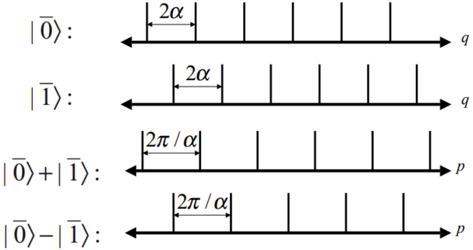


The Ideal GKP Code

Designed to correct small shift errors: $|\delta_q| < \sqrt{\pi}/2$ and $|\delta_p| < \sqrt{\pi}/2$
Note: for large errors, need qubit ECC on top

$$|0_L\rangle \propto \sum_{s=-\infty}^{\infty} \left|q = 2s\sqrt{\pi}\right\rangle$$

$$|1_L\rangle \propto \sum_{s=-\infty}^{\infty} \left|q = (2s+1)\sqrt{\pi}\right\rangle$$



What's the point?

An entirely new kind of error: continuous rather than discrete

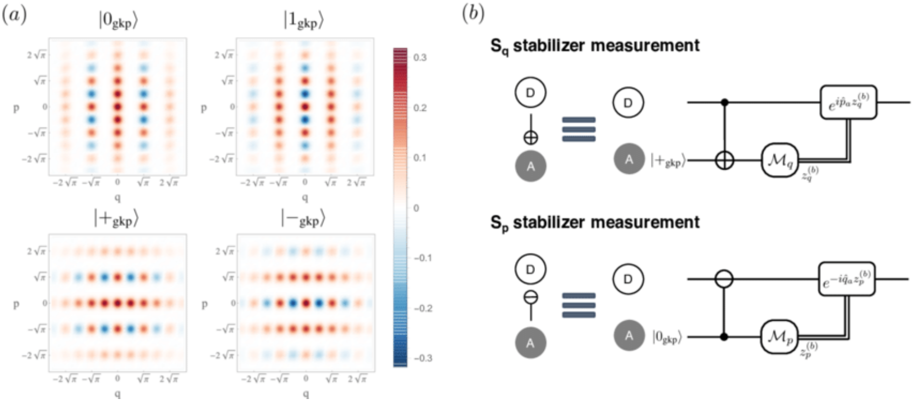
Small deviations lead to orthogonal states, unlike with stabilizer codes

Unlike $\mathbb{F}_d$, has no "wrap-around," so we have to get creative to find states which have simple stabilizers

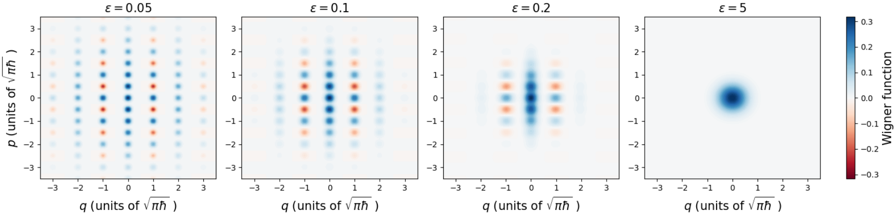
GKP Codes provide a helpful source of non-Gaussianity to Gaussian Optical Computing

GKP Stabilizers

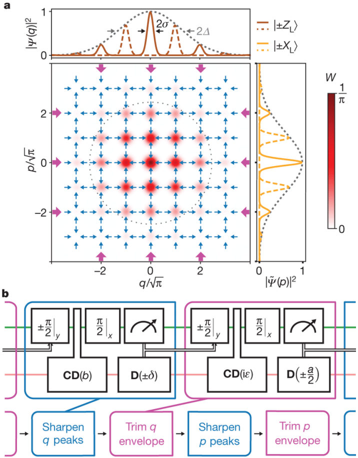
$$S_q = D(i\sqrt{2\pi}),\ S_q = D(\sqrt{2\pi})$$



Why can't it be ideal?



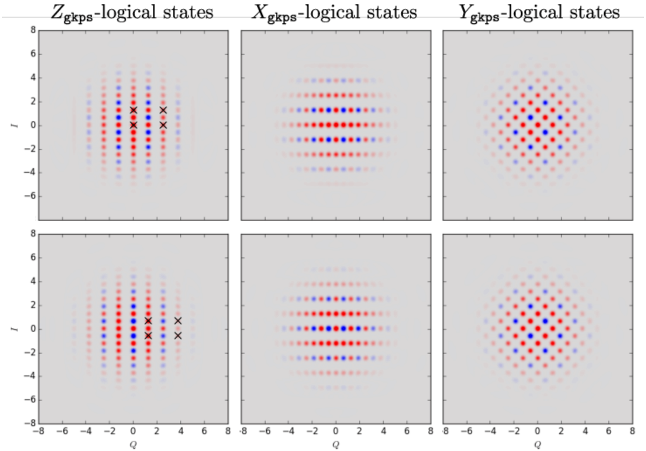
Quadratures, for reference



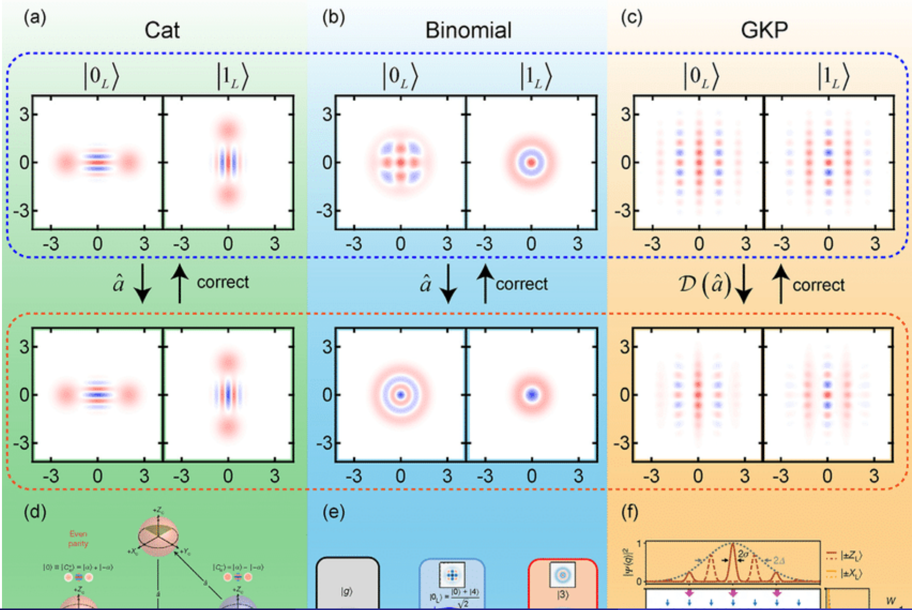
CV Paulis Acting on GKP Code States

$$X = D(i\sqrt{\pi/2}),\ Z = D(\sqrt{\pi/2}),\ Y = D(\sqrt{\pi/2} + i\sqrt{\pi/2})$$

Note: Paulis commute!



Other Notable Bosonic Codes



Applications

Universal Quantum Computation with Continuous-Variable Cluster States https://arxiv.org/pdf/quant-ph/0605198.pdf

All-Gaussian universality and fault tolerance with the Gottesman-Kitaev-Preskill code https://arxiv.org/pdf/1903.00012.pdf

Time-Domain Multiplexed 2-Dimensional Cluster State: Universal Quantum Computing Platform https://arxiv.org/pdf/1903.03918.pdf

Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer https://arxiv.org/pdf/2010.02905v2.pdf