Quantum Codes From Generalized AG Codes

José Ignacio Iglesias Curto
Universidad de Salamanca

Zurich - July 12, 2022

Qubits and Pauli operators

Qubit is the usual system in quantum computation. Its quantum states may be represented as vectors in a 2 dimensional Hilbert space $\mathcal{H}$.
Operators on $\mathcal{H}$ may be written as a linear combination of I and the three Pauli operators, X, Y, Z,

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

verifiying

$$\begin{aligned} X^2 = Y^2 = Z^2 &= Id \\ XY = -YX &= iZ \\ YZ = -ZY &= iX \\ ZX = -XZ &= iY \end{aligned}$$

In particular, they anticommute and have eigenvalues ± 1.

Qubits and Pauli operators

We consider n-**qubits**, (or **quantum words**). Their states are vectors from a 2^n-dimensional Hilbert spaces $\mathcal{H}_n = \mathcal{H} \otimes \overset{n}{\ldots} \otimes \mathcal{H}$.

Definition

The Pauli group on n-qubits is the set of tensor products of n either Pauli operators or Identity

$$\mathcal{G}_n := \langle \{I, X, Y, Z\}^{\otimes n} \rangle$$

with componentwise product.

For the sake of symplicity $\bar{\mathcal{G}}_n = \{O_1 O_2 \ldots O_n\}_{O_i = I,X,Y,Z}$.

Definition

The weigth of a Pauli n-operador is

$$w(O_1 O_2 \ldots O_n) := \sharp\{i \mid O_i \neq I\}\,.$$

Quantum information, errors, coding

Evaluate the state of a qubit $\Rightarrow$ decoherence
BUT
meassuring: determine in which subspace $\leftarrow$ is possible

Quantum information, errors, coding

Evaluate the state of a qubit $\Rightarrow$ decoherence
BUT
meassuring: determine in which subspace $\leftarrow$ is possible
An error occurs if the n-qubit's state "changes" to another subspace.
Such change is due to a Pauli n-operator.
Hence, an error is on operator $O_1 O_2 \dots O_n$, where

$$O_i = \begin{cases} I & \text{(no error)} \\ X & \text{(bit flip)} \\ Z & \text{(phase flip)} \\ Y & \text{(both } X, Z\text{)} \end{cases}$$

Detection: determine the error operator
Correction: apply the same operator.

Stabilizer codes

In order to *detect* errors one can use a set of "control" operators.

Definition

A stabilizer group is a subgroup $S \subseteq \mathcal{G}_n$ of **commuting** operators.
$S = \langle \mathbf{g}_1, \ldots \mathbf{g}_r \rangle$.

Definition

The $[[n, k, d]]$ **quantum stabilizer code** associated to
$S = \langle \mathbf{g}_1, \ldots \mathbf{g}_{n-k} \rangle$ is the intersection subspace of the eigenvector subspaces of eigenvalue 1 for all operators in S.
$d =$ minimum weigth among operators (not in S) that commute with all the ones in S.

Error detection: the n-qubit has eigenvalue -1 for some $\mathbf{g}_i$.
$\mathbf{E} \in \mathcal{G}_n$ is an error operator if it doesn't commute with some element from S.

Classical code associated to the stabilizer group

There is a group isomorphism $L : \bar{\mathcal{G}}_1 \longrightarrow \mathbb{F}_4$

$$I \longrightarrow 0$$
$$X \longrightarrow \alpha$$
$$Y \longrightarrow 1$$
$$Z \longrightarrow \alpha^2$$

extendable to $L : \bar{\mathcal{G}}_n \longrightarrow \mathbb{F}_4^n$

$$L(O_1 O_2 \dots O_n) = \big(L(O_1), L(O_2), \dots L(O_n)\big) .$$

Classical code associated to the stabilizer group

There is a group isomorphism $L : \bar{\mathcal{G}}_1 \longrightarrow \mathbb{F}_4$

$$\begin{aligned} I &\longrightarrow 0 \\ X &\longrightarrow \alpha \\ Y &\longrightarrow 1 \\ Z &\longrightarrow \alpha^2 \end{aligned}$$

extendable to $L : \bar{\mathcal{G}}_n \longrightarrow \mathbb{F}_4^n$

$$L(O_1 O_2 \dots O_n) = \big(L(O_1), L(O_2), \dots L(O_n)\big) .$$

If $S = \langle \mathbf{g}_1, \dots \mathbf{g}_r \rangle$ is a stabilizer group, $L(S) = \langle L(\mathbf{g}_1), \dots L(\mathbf{g}_r) \rangle$ is a $[n, r/2]_4$-linear code.

Definition

$L(S)$ is the quaternary stabilizer code with stabilizer group S.

Classical code associated to the stabilizer group

There is a group isomorphism $L : \bar{\mathcal{G}}_1 \longrightarrow \mathbb{F}_4$

$$\begin{aligned} I &\longrightarrow 0 \\ X &\longrightarrow \alpha \\ Y &\longrightarrow 1 \\ Z &\longrightarrow \alpha^2 \end{aligned}$$

extendable to $L : \bar{\mathcal{G}}_n \longrightarrow \mathbb{F}_4^n$

$$L(O_1 O_2 \dots O_n) = \big(L(O_1), L(O_2), \dots L(O_n)\big) .$$

If $S = \langle \mathbf{g}_1, \dots \mathbf{g}_r \rangle$ is a stabilizer group, $L(S) = \langle L(\mathbf{g}_1), \dots L(\mathbf{g}_r \rangle)$ is a $[n, r/2]_4$-linear code.

Definition

$L(S)$ is the quaternary stabilizer code with stabilizer group S.

The commuting condition on the operators in S means that the quaternary code is self-ortogonal.

Generalized AG codes

X a projective curve over $\mathbb{F}_q$.
For $i = 1, \ldots, s$

- $P_i \in X$, $\deg P_i = k_i$
- $\mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \simeq \mathbb{F}_{q^{k_i}} \simeq \mathbb{F}_q^{k_i}$
- $\mathcal{C}_i$ a $[n_i, k_i, d_i]$ linear code
- a $\mathbb{F}_q$-linear isomorphism $\pi_i : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \to \mathcal{C}_i$

F a divisor with none of the P_i on its support.

Generalized AG codes

X a projective curve over $\mathbb{F}_q$.
For $i = 1, \ldots, s$

- $P_i \in X$, $\deg P_i = k_i$
- $\mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \simeq \mathbb{F}_{q^{k_i}} \simeq \mathbb{F}_q^{k_i}$
- $\mathcal{C}_i$ a $[n_i, k_i, d_i]$ linear code
- a $\mathbb{F}_q$-linear isomorphism $\pi_i : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \to \mathcal{C}_i$

F a divisor with none of the P_i on its support.
We can define

$$\begin{aligned} \pi : \mathcal{L}(F) &\longrightarrow \mathbb{F}_q^n \\ f &\longmapsto (\pi_1(f(P_1)), \ldots, \pi_s(f(P_s))) \end{aligned}$$

Generalized AG codes

Definition

The generalized AG code defined by $\{(P_i, \mathcal{C}_i, \pi_i)\}_i$ and F is the image of π.

Proposition

If $\deg(F) < \sum_i k_i$, *the GAG code is of type* $[n, k, d]$, *with*

$$k = \dim \mathcal{L}(F) \geq \deg(F) + 1 - g, \qquad d \geq \tilde{d}\,.$$

Quantum codes from GAG codes

X a projective curve over $\mathbb{F}_4$ ($\mathbb{P}^1_{\mathbb{F}_4}$).
For $i = 1, \ldots, s$

- $P_i \in X$, $\deg P_i = k_i$
- S_i stabilizer group, $L(S_i)$ a $[n_i, k_i, d_i]_4$ quaternary stabilizer code, ($\sharp$ gen of $S_i = 2k_i$).
- $\pi_i : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \xrightarrow{\sim} L(S_i)$, $\pi_i^L : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \xrightarrow{\sim} S_i$

F a divisor with none of the P_i on its support.

Quantum codes from GAG codes

X a projective curve over $\mathbb{F}_4$ ($\mathbb{P}^1_{\mathbb{F}_4}$).
For $i = 1, \ldots, s$

- $P_i \in X$, $\deg P_i = k_i$
- S_i stabilizer group, $L(S_i)$ a $[n_i, k_i, d_i]_4$ quaternary stabilizer code, ($\sharp$ gen of $S_i = 2k_i$).
- $\pi_i : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \xrightarrow{\sim} L(S_i)$, $\pi_i^L : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \xrightarrow{\sim} S_i$

F a divisor with none of the P_i on its support.
We define

$$\begin{aligned} \pi : \mathcal{L}(F) &\longrightarrow \bar{\mathcal{G}}_n \\ f &\longmapsto \pi_1^L(f(P_1)) \otimes \ldots \otimes \pi_s^L(f(P_s)) \end{aligned}$$

Quantum codes from GAG codes

Definition

The quantum generalized AG code defined by $\{(P_i, S_i, \pi_i^L)\}_i$ and F is the QECC stabilized by $\mathrm{Im}\ \pi$.

Quantum codes from GAG codes

Definition

The quantum generalized AG code defined by $\{(P_i, S_i, \pi_i^L)\}_i$ and F is the QECC stabilized by $\mathrm{Im}\ \pi$.

Proposition

If $\deg(F) < \sum_i k_i$ *and* $\deg(F) - g \geq k_i - 1 \, \forall i$, *the QGAG code is of type* $[[n, n-2k, d]]$, *with*

$$n = \sum_i n_i, \quad k = \dim \mathcal{L}(F) \geq \deg(F) + 1 - g, \quad d \geq \min\{d_i\}\,.$$

Quantum codes from GAG codes

Example

$X = \mathbb{P}^1_{\mathbb{F}_4}$

$P_1, P_2 \in \mathbb{P}^1_{\mathbb{F}_4}$ of degrees 2, 3.

- S_1 stabilizer of $[[5, 1, 3]]$-QEC
- S_2 stabilizer of $[[10, 4, 3]]$-QEC

π_i^L appropriate isomorphisms

$F = 2P_\infty$, $\dim \mathcal{L}(F) = 3$.

$S = \mathrm{Im}\ \pi$ has 6 generators and is the stabilizer of a $[[15, 9, 3]]$ QEC code.

Quantum Convolutional Codes (QCC)

As in classical Information Theory we can add a convlutional structure by considering all information blocks as just one single sequence.
Let

$$
\begin{aligned}
L : \bar{\mathcal{G}}_\infty &\longrightarrow \mathbb{F}_4[D]^n \\
O_1 O_2 \dots O_n &\longrightarrow \big(L(O_1), L(O_2), \dots L(O_n)\big) \\
&\dots \\
I^{\otimes n \cdot r} O_1 O_2 \dots O_n &\longrightarrow D^r \big(L(O_1), L(O_2), \dots L(O_n)\big)
\end{aligned}
$$

Stabilizer group $S \subset \mathcal{G}_\infty$ verifies: $O \in S \Rightarrow I^{\otimes n} O \in S$.

Definition

The QCC with stabilizer group S is the subespace $\mathcal{H}_\infty$ stabilized by S.

Generalized AG convolutional codes

X a projective curve over $\mathbb{F}_q(z)$.
For $i = 1, \ldots, s$

- $P_i \in X$, $\deg P_i = k_i$
- $\mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \simeq \mathbb{F}_q(z)^{k_i}$
- $\mathcal{C}_i$ a $[n_i, k_i, \delta_i, d_i]$ convolutional code
- a $\mathbb{F}_q(z)$-linear isomorphism $\pi_i : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \to \mathcal{C}_i$

F a divisor with none of the P_i on its support.

Generalized AG convolutional codes

X a projective curve over $\mathbb{F}_q(z)$.
For $i = 1, \ldots, s$

- $P_i \in X$, $\deg P_i = k_i$
- $\mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \simeq \mathbb{F}_q(z)^{k_i}$
- $\mathcal{C}_i$ a $[n_i, k_i, \delta_i, d_i]$ convolutional code
- a $\mathbb{F}_q(z)$-linear isomorphism $\pi_i : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \to \mathcal{C}_i$

F a divisor with none of the P_i on its support.
We can define

$$\begin{aligned} \pi : \mathcal{L}(F) &\longrightarrow \mathbb{F}_q(z)^n \\ f &\longmapsto (\pi_1(f(P_1)), \ldots, \pi_s(f(P_s))) \end{aligned}$$

Definition

The generalized AG code defined by $\{(P_i, \mathcal{C}_i, \pi_i)\}_i$ and F is the image of π.

QCC from GAG codes

X a projective curve over $\mathbb{F}_4(z)$ $(\mathbb{P}^1_{\mathbb{F}_4(z)})$.
For $i = 1, \ldots, s$

- $P_i \in X$, $\deg P_i = k_i$
- $S_i \subset \mathcal{G}_\infty$ stabilizer group of a QCC, $L(S_i)$ a $[n_i, k_i, \delta_i, d_i]_4$ convolutional code, ($\sharp$ gen of $S_i = 2k_i$).
- $\pi_i^L : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \xrightarrow{\sim} S_i$

F a divisor with none of the P_i on its support.

QCC from GAG codes

X a projective curve over $\mathbb{F}_4(z)$ $(\mathbb{P}^1_{\mathbb{F}_4(z)})$.
For $i = 1, \ldots, s$

- $P_i \in X$, $\deg P_i = k_i$
- $S_i \subset \mathcal{G}_\infty$ stabilizer group of a QCC, $L(S_i)$ a $[n_i, k_i, \delta_i, d_i]_4$ convolutional code, ($\sharp$ gen of $S_i = 2k_i$).
- $\pi_i^L : \mathcal{O}_{P_i}/\mathfrak{m}_{P_i} \xrightarrow{\sim} S_i$

F a divisor with none of the P_i on its support.
Let $n = \sum_i n_i$, and $\forall i \ \pi_i^L(f(P_i)) \overset{\text{not}}{:=} w_i^0 \otimes w_i^1 \otimes \ldots$ with $w_i^j \in \bar{\mathcal{G}}_n$
We define

$$\pi : \mathcal{L}(F) \longrightarrow \bar{\mathcal{G}}_\infty$$

$$f \longmapsto w_1^0 \otimes \ldots \otimes w_s^0 \otimes w_1^1 \otimes \ldots \otimes w_s^1 \otimes \ldots$$

QCC from GAG codes

Definition

The QCGAG code defined by $\{(P_i, S_i, \pi_i^L)\}_i$ and F is the QCC stabilized by

$$S = \{I^{\otimes k \cdot n} O \mid k \in \mathbb{N}, O \in \mathrm{Im}\ \pi\}$$

QCC from GAG codes

Definition

The QCGAG code defined by $\{(P_i, S_i, \pi_i^L)\}_i$ and F is the QCC stabilized by

$$S = \{I^{\otimes k \cdot n} O \mid k \in \mathbb{N}, O \in \operatorname{Im} \pi\}$$

Proposition

If $\deg(F) < \sum_i k_i$ *and* $\deg(F) - g \geq k_i - 1 \, \forall i$, *the QCGAG code is of type* $[[n, n-2k, \delta, d]]$, *with*

$$n = \sum_i n_i, \quad k = \dim \mathcal{L}(F) \geq \deg(F) + 1 - g, \quad d \geq \min\{d_i\}\,.$$

Thank you