Lecture 14: Stabilizer Codes

main ideas:

- quantum code $\mathcal{C}$ is a subspace of say $(\mathbb{C}^2)^{\otimes n} = \mathcal{H}$
- the error spaces form a decomposition of $\mathcal{H}$

$\Rightarrow$ use some observables / operators to define / identify these spaces

Stabilizer codes are joint eigenspaces of a commuting (Abelian) subgroup of the group generated by tensor products of Pauli matrices and identity.

14.1 Connection to classical codes

every tensor product of Pauli matrices can be written as

$$\gamma \cdot X^{\underline{a}} Z^{\underline{b}} = \gamma \cdot (\sigma_x^{a_1} \cdot \sigma_z^{b_1}) \otimes \ldots \otimes (\sigma_x^{a_n} \sigma_z^{b_n})$$

with $\underline{a}, \underline{b} \in \mathbb{F}_2^n$, $\gamma \in \{\cancel{1}, i, -1, -i\}$

$\Rightarrow$ consider the vector $(\underline{a} | \underline{b}) \in \mathbb{F}_2^{2n}$

- multiplication of matrices $\hat{=}$ addition of vectors (up to phases)
- two operator $\gamma X^{\underline{a}} Z^{\underline{b}}$ and $\gamma' X^{\underline{c}} Z^{\underline{d}}$ commute iff $\underline{a} \cdot \underline{d} - \underline{b} \cdot \underline{c} = 0$

weight of an operator: number of factors different of identity

$\Rightarrow \quad \mathrm{wgt}(\gamma \cdot X^{\underline{a}} Z^{\underline{b}}) = \#\{i \in \{1,\ldots,n\} : a_i \neq 0 \vee b_i \neq 0\}$

use vectors over the field $\mathbb{F}_4 \cong GF(4)$

define: $\underline{c} := \underline{a} + \omega \cdot \underline{b}$ where $\omega^2 = \omega + 1$

$\Rightarrow$ vector of length n over $GF(4)$

$\mathrm{wgt}_H(\underline{c}) = \mathrm{wgt}(\gamma \cdot X^{\underline{a}} Z^{\underline{b}})$

multiplication of operators $\hat{=}$ addition of vectors over $GF(4)$ (up to phase)

Correspondences:

operators	binary vectors	elements of $GF(4)$
I	$(0,0)$	0
σ_x	$(1,0)$	1
σ_y	$(1,1)$	$1+\omega = \omega^2$
σ_z	$(0,1)$	ω

3

symplectic ~~inner~~ product on $\mathbb{F}_2^{2n}$

$\Rightarrow$ vanishes, iff the operators commute

Definition: trace of elements of finite fields

here: tr: $GF(4) \to GF(2)$

$$x \mapsto x + x^2 = x + \bar{x}$$

x	$tr(x)$
0	$0+0=0$
1	$1+1=0$
ω	$\omega+\omega^2=1$
ω^2	$\omega^2+\omega^4=1$

$\omega^3 = 1$

symplectic inner product on $GF(4)^n$

$$u * v = \sum_{i=1}^{n} tr(u_i \cdot \bar{v}_i)$$

$$= \sum_{i=1}^{n} u_i \bar{v}_i + \bar{u}_i v_i$$

where $\bar{x} := x^2$

one can show that for $u = a + \omega \cdot b$, $v = c + \omega \cdot d$

$$u * v = a \cdot d - b \cdot c$$

$\Rightarrow$ commutative subgroups of the Pauli matrices correspond to additively closed subsets C of $GF(4)^n$ such that

Commutative subgroups of n-qubit Pauli matrices correspond to additively closed subsets C of $GF(4)^n$ such that

$$\forall c, d \in C: \quad c * d = 0.$$

Note that in general C is not a $GF(4)$-vector space, i.e. not closed under multiplication by ω.

14.2 Operations on $GF(4)$ or $GF(4)^n$ and the corresponding operations on Pauli matrices:

multiplication by ω

	x	$x \cdot \omega$	
I	0	0	I
σ_x	1	ω	σ_z
σ_z	ω	ω^2	σ_y
σ_y	ω^2	1	σ_x

$\Rightarrow$ cyclic permutation of $\sigma_x, \sigma_y, \sigma_z$

$$\Theta = \frac{1}{2}\begin{pmatrix} i-1 & i+1 \\ i-1 & -(i+1) \end{pmatrix}$$

multiplication with ω over $GF(4)$ corresponds to conjugation of the Pauli matrices by Θ

on vectors over $\mathbb{F}_2^2$:

	x		$x\cdot\omega$		
I	0	00	0	00	I
σ_x	1	10	ω	01	σ_z
σ_z	ω	01	ω^2	11	σ_y
σ_y	ω^2	11	1	10	σ_x

Θ corresponds to a linear mapping on $\mathbb{F}_2^2$:

$(10) \mapsto (01)$ $\qquad (a,b) \mapsto (a,b)\cdot\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

$(01) \mapsto (11)$

$(10)+(01)$ $\quad (11) \mapsto (10) = (01) + (11)$

$(00) \mapsto (00)$

- Hadamard matrix: interchanges σ_x and σ_z

$\Longrightarrow$ mapping on $\mathbb{F}_2^2$ is given by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

(a bit more complicated over $GF(4)$)

- Conjugation over $GF(4)$: $\quad x \mapsto \bar{x} = x^2$

	x	$\bar{x}$	
I	0	0	I
σ_x	1	1	σ_x
σ_y	ω^2	ω	σ_z
σ_z	ω	ω^2	σ_y

$\Longrightarrow$ combination of Θ and H

5a

Summary: The group generated by Θ, H acts via conjugation on the Pauli matrices, i.e. Pauli matrices are mapped to Pauli matrices.
The action corresponds to the symmetric group S_3, i.e. any permutation of the Pauli matrices can be realized.

This corresponds also to ~~multiplicative group~~ full automorphism group of the additive group field $GF(4)$ generated by

$x \mapsto \omega \cdot x$ ~~"inner automorphism"~~

$x \mapsto x^2$ Frobenius automorphism

14.3 Stabilizer codes

additive quantum codes

Let S be an abelian subgroup of the n-qubit Pauli matrices not containing $-I$.
Furthermore, let $C \le GF(4)^n$ be the corresponding additive code over $GF(4)$, i.e.

$$C = (n, 2^{n-k}, d)$$

Then the stabilizer code $\mathcal{C} \le (\mathbb{C}^2)^{\otimes n}$ is ~~the~~ a common eigenspace of the operators in S with parameters $\mathcal{C} = [[n, k, d']]$

where $d' = \min\{\operatorname{wgt}(\underline{c}) : \underline{c} \in C^* \setminus C\}$

where $C^* = \{d : d \in GF(4)^n \mid c * d = 0 \ \forall c \in C\}$

the symplectic dual code of C

7

without loss of generality, let $\mathcal{C}$ be the joint $+1$ eigenspace of the elements in S, i.e.

$$\forall |\psi\rangle \in \mathcal{C}\ \forall s \in S : \quad s|\psi\rangle = |\psi\rangle$$

Let e be any Pauli error, and $|\psi\rangle, |\phi\rangle \in \mathcal{C}$

(*) $\langle\phi|e|\psi\rangle = \langle\phi|es|\psi\rangle = \langle\phi|se|\psi\rangle$

as $s|\psi\rangle = |\psi\rangle$ and $s|\phi\rangle = |\phi\rangle$

and $s^\dagger = s$

(**) $se = (-1)^{\underline{s} * \underline{e}}\ es$ where $\underline{s}, \underline{e} \in GF(4)^n$

$\Rightarrow \langle\phi|es|\psi\rangle = (-1)^{\underline{s} * \underline{e}} \langle\phi|se|\psi\rangle$

assume that $\underline{s} * \underline{e} \neq 0$ for some $s \in S$, $\underline{s} \in C$

(*)
$\Rightarrow$ the $\langle\phi|e|\psi\rangle = 0$
(**)

$\Rightarrow$
- errors that do not commute with some $s \in S$ can be detected
- errors in the stabilizer do not change the state