- $G_1 = \{\pm 1, \pm i\} \times \{\mathbb{1}, X, Y, Z\}$

- $G_n = \{\pm 1, \pm i\} \times \{\mathbb{1}, X, Y, Z\}^{\otimes n}$ PAULI GROUP $\left(|G_n| = 4^n \cdot 4 \right)$

phases necessary to be a group.

PROPERTIES OF G_n (@)

A) - $P_A, P_B \in G_n \Rightarrow P_A P_B = P_B P_A$ or $P_A P_B = - P_B P_A$. (Commute or anticommute)

B) - $P \in G_n \Rightarrow P$ is unitary $P P^\dagger = \mathbb{1}$.

C) - $P \in G_n \setminus \{\pm \mathbb{1}, \pm i \mathbb{1}\} \Rightarrow \mathrm{tr}(P) = 0$

D) - $P \in G_n : P = \pm 1 \cdot \hat{P}, \hat{P} \in \{\mathbb{1}, X, Y, Z\}^{\otimes n} \Rightarrow P^2 = \mathbb{1}, P = P^\dagger$, eigenv. $= \pm 1$

$P \in G_n : P = \pm i \cdot \hat{P}, \hat{P} \in \{\mathbb{1}, X, Y, Z\}^{\otimes n} \Rightarrow P^2 = -\mathbb{1}, P^\dagger = -P$, eigenval $= \pm i$.

E) - $P \in G_n \Rightarrow |\langle \psi | P | \psi \rangle| \leq 1$

(WRITE P in the eigendecomposition)

F) - $P \in G_n \Rightarrow |\langle \psi | P | \psi \rangle| = 1 \Rightarrow |\psi\rangle$ eigenstate of P.

- DEF (1):

Given $S \subseteq G_n$ subgroup, we define V_S the set of n-qubit state $|\psi\rangle$ such that $S_i |\psi\rangle = + |\psi\rangle \quad \forall S_i \in S$.

- OBS (2): V_S is a vector space.

- DEF (3) V_S is called "vector space stabilized by S".

- DEF (4): Given $S \subseteq G_n$ subgroup, we indicate $S = \langle S_1, \dots, S_\ell \rangle$

if $Gen(S) := \{S_1, \dots, S_\ell\}$ are generators for S (i.e. $\forall P \in S$, P can be written as product of elements taken from $\{S_1, \dots, S_\ell\}$.)

EXAMPLE (5) $S = \langle \mathbb{1}, X_1 X_2 \rangle = \{ \mathbb{1}, X_1 X_2 \}$

- $\mathbb{1}|\psi\rangle = |\psi\rangle$
- $X_1 X_2 |\psi\rangle = |\psi\rangle$

$\iff V_S = \mathrm{Span}\left(\left\{ \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \right\} \right)$

- OBS (6): $\dim(V_S) > 0 \Rightarrow$ A) $-\mathbb{1} \notin S$

  B) $S_i, S_j \in S \Rightarrow [S_i, S_j] = 0$

PROOF:

(A) - Assume $-\mathbb{1} \in S$.

$|\psi\rangle \in V_S \Rightarrow -\mathbb{1}|\psi\rangle = |\psi\rangle \Rightarrow |\psi\rangle = 0 \Rightarrow \dim(V_S) = 0 \Rightarrow$ ABSURD.

(B) - Assume that $\exists\, S_i, S_j \in S : [S_i, S_j] \neq 0 \Rightarrow$

S_i, S_j Paulis or Commute or anti Commute.

- $|\psi\rangle \in V_S \Rightarrow |\psi\rangle = S_i S_j |\psi\rangle = -S_j S_i |\psi\rangle$

$= -|\psi\rangle \Rightarrow |\psi\rangle = 0$

$\Rightarrow \dim(V_S) = 0 \Rightarrow$ ABSURD.

- COR (7). $\dim(V_S) > 0 \Rightarrow$ A) $-\mathbb{1} \notin S$

  B) $S_i, S_j \in \mathrm{Gen}(S) \Rightarrow [S_i, S_j] = 0$

- FACT (8): We will prove that also the converse is true.

OBS (9) $S = \langle S_1, \dots, S_l \rangle$. $[S_i, S_j] = 0$ with $S_i, S_j \in \mathrm{Gen}(S) \iff S$ is abelian.

PROOF:

- $(\Leftarrow)$ OK. - $(\Rightarrow)$ $\forall\, g_1, g_2 \in S \Rightarrow g_1$ and g_2 can be written as product of $\mathrm{Gen}(S)$ elements $\Rightarrow$ II.

- OBS (10): $-\mathbb{1} \notin S \Rightarrow \left(S_i, S_j \in \mathrm{Gen}(S) \Rightarrow [S_i, S_j] = 0 \right)$

PROOF:

Suppose that $\exists\, g$ and $h \in \mathrm{Gen}(S) : hg = -gh$.

If $h^2 = -\mathbb{1}$ or $g^2 = -\mathbb{1}$ $\Rightarrow$ ok. If $h^2 = \mathbb{1}$, $g^2 = \mathbb{1}$ $\Rightarrow$ $(gh)^2 = ghgh = -g^2h^2 = -\mathbb{1} \in S$

$\Rightarrow$ ABSURD.

OBS: (1.1) $-\mathbb{1} \notin S \Rightarrow \forall P \in S \quad P = \pm Q$ with $Q \in \{\mathbb{1}, X, Y, Z\}^{\otimes n}$

$(P \neq \pm i Q)$

$\Rightarrow \forall P \in S, \quad P^2 = \mathbb{1}.$

PROOF:

If $P = (\pm i\, Q) \in S \Rightarrow P^2 = -\mathbb{1} \in S$.

COR. (1.2) $\dim(V_S) > 0 \Rightarrow -\mathbb{1} \notin S \Rightarrow$ A) $\cdot$ S is abelian (Gen(S) also).

B) $\cdot$ $\forall P \in S$, $P = \pm Q$, $P = P^+$

$Q \in \{\mathbb{1}, X, Y, Z\}^{\otimes n}$

C) $\cdot$ $\forall P \in S$, $P^2 = \mathbb{1}$, eigenvalues: ± 1.

EXAMPLE (1.3) $\cdot$ $S = \langle \mathbb{1}, iP \rangle \Rightarrow V_S = \{0\}$

$iP \in S \Rightarrow (iP)^2 = -\mathbb{1}$

$\cdot$ $S = \langle \mathbb{1}, X_1, Y_1 \rangle \Rightarrow V_S = \{0\}$

$X_1 Y_1 = -Y_1 X_1$

TH (1.4): $\cdot$ The projector on V_S is given by $P_S := \frac{1}{|S|} \sum_{g \in S} g$

PROOF:

$\cdot$ If $-\mathbb{1} \in S \Rightarrow$ if $g \in S \Rightarrow -\mathbb{1}g = -g \in S \Rightarrow P_S = 0$. OK!

$\cdot$ If $-\mathbb{1} \notin S \Rightarrow \cdot\, P_S = P_S^+$, $P_S^2 = P_S \Rightarrow$ PROJECTOR.

(1.2)

$$P_S^2 = \left(\frac{1}{|S|}\sum_{g\in S} g\right)\left(\frac{1}{|S|}\sum_{g'\in S} g'\right) = \frac{1}{|S|^2}\sum_{g}\underbrace{\left(\sum_{g'} gg'\right)}_{\left(\sum_{g'} g'\right)} = \frac{1}{|S|^2}\underbrace{\left(\sum_{g} 1\right)}_{|S|}\cdot\left(\sum_{g'} g'\right) = P_S$$

- $P_S|\psi\rangle = |\psi\rangle \Leftrightarrow |\psi\rangle \in V_S.$

SUBPROOF:

$$P_S|\psi\rangle = |\psi\rangle \Rightarrow 1 = \langle\psi|P_S|\psi\rangle = \frac{1}{|S|}\sum_g \langle\psi|g|\psi\rangle \leq \frac{1}{|S|}\sum_g |\langle\psi|g|\psi\rangle| \underset{\text{Q.F.}}{\leq} \frac{1}{|S|}\sum_g 1 = 1$$

$$\Rightarrow \langle\psi|g|\psi\rangle = 1 \underset{\text{Q.F.}}{\Rightarrow} g|\psi\rangle = +|\psi\rangle\ \forall g\in S \Rightarrow |\psi\rangle \in V_S,$$

- TH (15)
  - $S = \langle s_1, \dots, s_\ell\rangle$ where $Gen(S) = \{s_1, \dots, s_\ell\}$ are indipendent generators.

If $-I \in S \Rightarrow \dim(V_S) = 0$

If $-I \notin S \Rightarrow \begin{cases} \cdot\ P_S := \dfrac{1}{2^\ell}\displaystyle\sum_{g\in S} g = \prod_{k=1}^{\ell}\left(\dfrac{1+S_k}{2}\right) \\ \cdot\ \dim(V_S) = 2^{n-\ell} \end{cases}$

PROOF:

- If $-\mathbb{1} \in S \Rightarrow$ if $g\in S \Rightarrow -\mathbb{1}g = -g \in S \Rightarrow P_S = 0$. OK!
- If $-\mathbb{1} \notin S \Rightarrow P_S := \dfrac{1}{|S|}\displaystyle\sum_{g\in S} g \underset{\substack{\cdot\ \text{COR (12)} \Rightarrow S \text{ is abelian}\\ \text{and } g^2 = \mathbb{1},\\ \forall g\in S.}}{=} \dfrac{1}{|S|}\prod_{k=1}^{\ell}(1+\underset{\text{generators}}{g_k}) =$

$$\underset{(|S| = 2^\ell)}{=} \frac{1}{2^\ell}\prod_{k=1}^{\ell}\left(\frac{1+S_k}{2}\right)$$

- $\dim(V_S) = Tr(P_S) = \dfrac{1}{2^\ell}\, Tr\left(\displaystyle\sum_{g\in S} g\right) \underset{Tr(g) = 0\ \forall g \neq \mathbb{1}}{=} \dfrac{2^n}{2^\ell} = 2^{n-\ell}.$

TH 16 • $S = \langle s_1, \dots, s_n \rangle$ with $s_1, \dots, s_n$ indipendent generators such that $-\mathbb{1} \notin S$. $\Rightarrow \dim(V_S) = 1$

PROOF: Follows by 15.

FACT 17

• Given $Gen(S) = \{s_1, \dots, s_\ell\}$, how do we verify that $-\mathbb{1} \notin S$?

$$\left.\begin{array}{l} \bullet \text{ If } s_1, \dots, s_\ell \text{ commute} \\ \bullet\ s_1, \dots, s_\ell \text{ are indipendent removing phase factors.} \\ \bullet\ s_i^2 = \mathbb{1} \quad \forall s_i \in Gen(S) \\ \bullet\ s_i \neq -\mathbb{1} \quad \forall s_i \in Gen(S) \end{array}\right\} \Rightarrow -\mathbb{1} \notin S$$

$s_i = \pm P$ with $P \in \{\mathbb{1}, X, Y, Z\}^{\otimes n}$

PROOF:

• $-\mathbb{1} \in S \Rightarrow -\mathbb{1} = s_1^{x_1} \cdots s_\ell^{x_\ell}$ for some $x_1, \dots, x_\ell \Rightarrow -\mathbb{1} = \tilde{s}_1 \cdots \tilde{s}_m$

considering only $s_i^{x_i}$: $x_i \neq 0$.

• Here $m > 1$, since if $m = 1 \Rightarrow -\mathbb{1} = \tilde{s}_1 \in Gen(S)$, $\Rightarrow$ ABSURD.

• $\tilde{s}_m = -\tilde{s}_1 \cdots \tilde{s}_{m-1} \Rightarrow \tilde{s}_m$ and $\tilde{s}_1, \dots, \tilde{s}_{m-1}$ are NOT indipendent removing phase factors. $\Rightarrow$ ABSURD.

TH 18

A) • If $S_1, \dots, S_\ell$ commute

B) • $S_1, \dots, S_\ell$ are indipendent removing phase factors. $\Rightarrow \dim\left(V_{S=\langle S_1,\dots,S_\ell\rangle}\right) = 2^{n-\ell}$

C) • $S_i^2 = \mathbb{1} \quad \forall\, S_i \in Gen(S)$

$S_i = \pm P$ with $P \in \{\mathbb{1}, X, Y, Z\}^{\otimes n}$

D) • $S_i \neq -\mathbb{1} \quad \forall\, S_i \in Gen(S)$

PROOF:

14 + 15 .

FACT 19

If we have $S_1, \dots, S_n$ and we have to verify conditions of TH 18,

C) and D) can be done efficiently. But what about A) and B)?

We need the so-called CHECK-REPRESENTATION tool.

DEF 20 (CHECK-REPRESENTATION)

• We define a 2n-dim. vector representation $R(P)$ of a Pauli $P = \pm P_1 \otimes P_2 \otimes \dots \otimes P_n$

$$P_i = \mathbb{1} \iff (R(P))_i = 0 \quad , \quad (R(P))_{n+i} = 0$$

$$P_i = X \iff (R(P))_i = 1 \quad , \quad (R(P))_{n+i} = 0$$

$$P_i = Z \iff (R(P))_i = 0 \quad , \quad (R(P))_{n+i} = 1$$

$$P_i = Y \iff (R(P))_i = 1 \quad , \quad (R(P))_{n+i} = 1$$

e.g. $P = X \otimes Z \otimes \mathbb{1} \otimes \underset{\overset{\shortparallel}{iZX}}{Y} \Rightarrow R(P) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ \hline 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \begin{matrix} \} X \\ \\ \} Z \end{matrix}$

· We don't consider phases in this representation.

FACT (21) $P^{(A)} P^{(B)} = \pm P^{(C)} \Longrightarrow \left(R(P^{(A)}) + R(P^{(B)}) = R(P^{(C)}) \right) \mod (2)$.

PROOF:

$$P^{(A)} P^{(B)} = \left(P_1^{(A)} \otimes \cdots \otimes P_n^{(A)}\right)\left(P_1^{(B)} \otimes \cdots \otimes P_n^{(B)}\right) = P_1^{(A)} P_1^{(B)} \otimes \cdots \otimes P_n^{(A)} P_n^{(B)}$$

We can verify it case by case.

e.g. $P_s^{(A)} = X$, $P_s^{(B)} = Y$ $\Rightarrow XY = iZ = P_s^{(C)}$

$$\underset{\overset{\shortparallel}{1}}{(R(X))_s} + \underset{\overset{\shortparallel}{1}}{(R(Y))_s} \underset{=}{=} (R(XY))_s = \underset{\overset{\shortparallel}{0}}{(R(Z))_s} \quad \text{ok!}$$

$$\underset{\overset{\shortparallel}{0}}{(R(X))_{s+n}} + \underset{\overset{\shortparallel}{1}}{(R(Y))_{s+n}} \underset{=}{=} (R(XY))_{s+n} = \underset{\overset{\shortparallel}{1}}{(R(Z))_{s+n}} \quad \text{ok!}$$

· (22) More generally:

$Q = \pm S_n^{x_n} \cdots S_1^{x_1}$ with $x_1, \dots, x_n \in \{0,1\} \Rightarrow R(Q) = x_1 R(S_1) + \dots + x_n R(S_n)$

$$R(Q) = x_1 R(S_1) + \dots + x_n R(S_n) = \underbrace{\left(R(S_1) \,\middle|\, R(S_2) \,\middle|\, \cdots \,\middle|\, R(S_n) \right)}_{\substack{\uparrow \\ 2n \times n \text{ matrix} \\ \shortparallel \ \underline{\underline{R}}_S}} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} =: \underline{\underline{R}}_S \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

(23) To check if $\{s_1, \dots, s_\ell\}$ are indipendent without phases (check-indip.)
we need to see if $\left(R(s_1) \middle| \dots \middle| R(s_\ell) \right) \begin{pmatrix} x_1 \\ \vdots \\ x_\ell \end{pmatrix} = 0$
admit only $x_1 = \dots = x_\ell = 0$ as solution.
These can be solved efficiently in $O(\ell^3)$ time
using Gaussian elimination

(24) How to check if $\{s_1, \dots, s_\ell\}$ commute each other?
I need to check if $[s_i, s_j] = 0 \quad \forall i \neq j$.

$$\frac{n(n-1)}{2}.$$

- Checking if $s_i s_j = s_j s_i$ $(i \neq j)$ can be done also using the check-repres.

FACT (25) $\quad s_i s_j = s_j s_i \iff (R(s_i))^t \begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix} R(s_j) = 0$

PROOF:

- $$\sum_{k=1}^{n} (R(s_i))_k (R(s_j))_{n+k} + \sum_{k=1}^{n} (R(s_i))_{k+n} (R(s_j))_k = 0$$

- $$\sum_{k=1}^{n} \left((R(s_i))_k (R(s_j))_{n+k} + (R(s_i))_{k+n} (R(s_j))_k \right) = 0$$

- $s_i = P_1^i \otimes \dots \otimes P_n^i \quad , s_j = P_1^j \otimes \dots \otimes P_n^j$

- $S_i S_j = P_1^i P_1^j \otimes \dots \otimes P_h^i P_h^j$
- $S_j S_i = P_1^j P_1^i \otimes \dots \otimes P_h^j P_h^i$
- $P_\ell^i P_\ell^j = P_\ell^j P_\ell^i$ or $P_\ell^i P_\ell^j = - P_\ell^j P_\ell^i$

This situation should happen an even number of times to commute.

I have to verify that:

$$(R(S_i))_K (R(S_j))_{h+K} + (R(S_i))_{K+h} (R(S_j))_K = 0 \mod (2) \iff [S_i, S_j] = 0$$

CASE BY CASE:
- If $S_i = \mathbb{1}$ or $S_j = \mathbb{1}$ $\Rightarrow$ ok
- If $S_i = X \Rightarrow$
  - $S_j = X \Rightarrow 1 \cdot 0 + 0 \cdot 1 = 0 \Rightarrow$ ok $\quad [X, X] = 0$
  - $S_j = Y \Rightarrow 1 \cdot 1 + 0 \cdot 1 = 1 \Rightarrow$ ok $\quad \{X, Y\} = 0$
  - $S_j = Z \Rightarrow 1 \cdot 1 + 0 \cdot 0 = 1 \Rightarrow$ ok $\quad \{X, Z\} = 0$
- If $S_i = Z \Rightarrow$
  - $S_j = Y \Rightarrow 1 \Rightarrow$ ok
  - $S_j = Z \Rightarrow 1 \Rightarrow$ ok
- If $S_i = Y \Rightarrow$ $S_j = Y \Rightarrow$ ok

TH (26)

easy to verify

A) If $S_1, \dots, S_\ell$ commute

B) $S_1, \dots, S_\ell$ are check-indipendent

Gauss elimination of check-matrix.

C) $S_i^2 = \mathbb{1} \quad \forall S_i \in Gen(S)$

$S_i = \pm P$ with $P \in \{\mathbb{1}, X, Y, Z\}^{\otimes h}$

D) $S_i \neq -\mathbb{1} \quad \forall S_i \in Gen(S)$

$$\Rightarrow \dim\left(V_{S = \langle S_1, \dots, S_\ell \rangle}\right) = 2^{h-\ell}$$

- Check problem sheet 9 ex. 2.