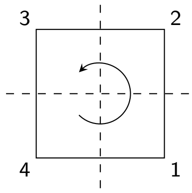
Introduction to Quantum Computing (IN2381) – WS2020/2021 **Sheet 11**

Christian B. Mendl, Irene López Gutiérrez, Keefe Huang due: 3 Feb 2021

Tutorial 11 (Group theory fundamentals[1])
A group $(G, \cdot)$ is a non-empty set G with a binary group operation '$\cdot$', with the following properties:

- *Closure*: $g_1 \cdot g_2 \in G$ for all $g_1, g_2 \in G$.
- *Associativity*: $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ for all $g_1, g_2, g_3 \in G$.
- *Identity*: there exists $e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$.
- *Inverses*: for all $g \in G$, there exists $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.



A simple example of a finite group is the additive group Z_n of integers modulo n, under the operation of modular addition. In this case, the identity would be 0 and the inverse of each element g would be $n - g$. Another more abstract example is the group of geometric transformations that map a square to itself (i.e., 90 degrees rotation, reflection along the vertical or horizontal axis, ...).

(a) Prove that for any element g of a finite group, there always exists a positive integer r such that $g^r = e$.

(b) For a single qubit, the Pauli group is defined to consist of all the Pauli matrices with some multiplicative factors:

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}. \tag{1}$$

G_1 forms a group under matrix multiplication. Argue why the factors ± 1 and $\pm i$ are included, and how this group satisfies the properties of associativity, identity and inverses.

(c) A group G is said to be *Abelian* if $g_1 \cdot g_2 = g_2 \cdot g_1$ for all $g_1, g_2 \in G$. Is the Pauli group Abelian?

Exercise 11.1 (Fidelity of the amplitude damping channel)
The *fidelity* is a distance measure between density operators, defined as

$$F(\rho, \sigma) = \mathrm{tr}\big[\sqrt{\rho^{1/2}\, \sigma\, \rho^{1/2}}\big],$$

where the square-root of a Hermitian matrix is understood to act on the eigenvalues of this matrix, and the products inside the trace are usual matrix multiplications. For the special case of a pure state $\rho = |\psi\rangle\langle\psi|$, it holds that $\rho^{1/2} = \rho$ (since the eigenvalues of ρ are 0 and 1 in this case), and thus

$$F(|\psi\rangle, \sigma) := F(|\psi\rangle\langle\psi|, \sigma) = \mathrm{tr}\big[\sqrt{|\psi\rangle\langle\psi|\sigma|\psi\rangle\langle\psi|}\big] = \sqrt{\langle\psi|\sigma|\psi\rangle}\ \mathrm{tr}\big[|\psi\rangle\langle\psi|\big] = \sqrt{\langle\psi|\sigma|\psi\rangle}. \tag{2}$$

Compute the fidelity $F(|\psi\rangle, \mathcal{E}_{\mathsf{AD}}(|\psi\rangle\langle\psi|))$ when $\mathcal{E}_{\mathsf{AD}}$ is the amplitude damping channel with parameter γ from exercise 12.2, and show that its minimum with respect to $|\psi\rangle$ is $\sqrt{1-\gamma}$.
Hint: Based on the operator-sum representation of $\mathcal{E}_{\mathsf{AD}}$ and Eq. (2), first derive that

$$F\big(|\psi\rangle, \mathcal{E}_{\mathsf{AD}}(|\psi\rangle\langle\psi|)\big) = \sqrt{\sum_k |\langle\psi|E_k|\psi\rangle|^2},$$

and evaluate this expression for a general state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Now parametrize $|\alpha|^2 = \cos(\theta/2)^2$ and $|\beta|^2 = \sin(\theta/2)^2$ for some angle θ, and find the minimum with respect to θ.

Exercise 11.2 (Pauli group and check matrix)
Recall that the *commutator* of two matrices A and B is defined as $[A, B] = AB - BA$, and the so-called *anti-commutator* as $\{A, B\} = AB + BA$. It turns out that the Pauli matrices $\sigma_1 = X$, $\sigma_2 = Y$, $\sigma_3 = Z$ either pairwise commute or anti-commute: for all $\alpha, \beta \in \{1, 2, 3\}$

$$\sigma_\alpha \sigma_\beta = \begin{cases} \sigma_\beta \sigma_\alpha & \text{if } \alpha = \beta \\ -\sigma_\beta \sigma_\alpha & \text{if } \alpha \neq \beta \end{cases} \tag{3}$$

(a) Verify Eq. (3) for all $\alpha < \beta$ by explicit computation. (Note that the case $\alpha = \beta$ is trivial, and the cases $\alpha > \beta$ then follow by symmetry.)

[1] M. A. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*. Cambridge University Press (2010), Appendix 2

The Kronecker product of matrices satisfies the relation

$$(A_1 \otimes \cdots \otimes A_n) \cdot (B_1 \otimes \cdots \otimes B_n) = (A_1 \cdot B_1) \otimes \cdots \otimes (A_n \cdot B_n) \tag{4}$$

for arbitrary complex matrices A_j and B_j ($j = 1, \dots, n$) with compatible dimensions, such that the matrix products $A_j \cdot B_j$ are well-defined.

In the following, we consider a system of n qubits, and use the notation I_j, X_j, Y_j, Z_j for the identity or one of the Pauli matrices acting on the jth qubit; for example, $X_1 Z_3 \equiv X \otimes I \otimes Z \otimes I \otimes \cdots \otimes I$.

The *Pauli group* G_n on n qubits generalizes Eq. (1) and is defined to consist of all n-fold tensor products of the identity and Pauli matrices, including multiplicative prefactors of ± 1 and $\pm i$ (such that multiplying two elements results again in an element of the group). For example,

$$G_2 = \{\pm I_1 I_2, \pm i I_1 I_2, \pm I_1 X_2, \dots, \pm X_1 I_2, \pm i X_1 I_2, \pm X_1 X_2 \dots, \pm i Z_1 Z_2\}.$$

(To shorten notation, the identity matrix is usually not explicitly listed in tensor products, e.g., $I_1 X_2 \equiv X_2$. Note that here $I_1 I_2$ is simply the 4×4 identity matrix on the 2-qubit system.)

Based on Eqs. (3) and (4), you should convince yourself that any $g, g' \in G_n$ likewise either commute or anti-commute. For example, letting $g = X_1 Z_2 Y_3$ and $g' = Y_1 X_2$, one calculates

$$\begin{aligned} gg' = (X \otimes Z \otimes Y) \cdot (Y \otimes X \otimes I) &= (XY) \otimes (ZX) \otimes Y \\ &= (-YX) \otimes (-XZ) \otimes Y = (YX) \otimes (XZ) \otimes Y = g'g, \end{aligned}$$

that is, $[g, g'] = 0$. As another example, letting $g = Y_1 Z_2$ and $g' = X_1 Z_2$, then g, g' actually anti-commute: $\{g, g'\} = 0$. Note that the allowed prefactors ± 1 and $\pm i$ do not affect the (anti-)commuting property.

(b) Determine whether the following pairs commute or anti-commute:

$$(X_1, Z_1), \quad (X_1, Z_3), \quad (X_1 X_2 X_3, Y_2 Z_3)$$

Given an element $g \in G_n$, we define a row vector of length $2n$, denoted $r(g)$, as follows (again ignoring the allowed prefactor of g):

matrix in g acting on qubit j	jth entry of $r(g)$	$(n+j)$th entry of $r(g)$
I	0	0
X	1	0
Y	1	1
Z	0	1

For example, $n = 5$ and

$$g = i X_2 Y_4 Z_5 \quad \rightsquigarrow \quad r(g) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

For several elements $(g_1, \dots, g_\ell)$, the corresponding *check matrix* is the $\ell \times 2n$ matrix with rows $r(g_1), \dots, r(g_\ell)$:

$$\begin{pmatrix} r(g_1) \\ \vdots \\ r(g_\ell) \end{pmatrix}$$

(c) Compute the check matrix for $n = 5$ and (g_1, g_2, g_3, g_4) the generators of the five qubit code (the meaning of which will be explained later in the lecture):

$$\begin{aligned} g_1 &= X \otimes Z \otimes Z \otimes X \otimes I \\ g_2 &= I \otimes X \otimes Z \otimes Z \otimes X \\ g_3 &= X \otimes I \otimes X \otimes Z \otimes Z \\ g_4 &= Z \otimes X \otimes I \otimes X \otimes Z \end{aligned}$$

(d) Show that $r(g) + r(g') = r(gg')$ for all $g, g' \in G_n$, where the addition is performed bitwise modulo 2.

Hint: Consider the Pauli matrices acting on the jth qubit separately from the rest. The prefactors resulting from products of Pauli matrices, like $XY = iZ$, get absorbed into the global prefactor.

(e) We now define a $2n \times 2n$ matrix Λ by

$$\Lambda = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix},$$

where the off-diagonal identity blocks have size $n \times n$. Show that any $g, g' \in G_n$ commute ($[g, g'] = 0$) if and only if $r(g) \Lambda r(g')^T = 0 \mod 2$.

Hint: Intuitively, $r(g) \Lambda r(g')^T$ counts the number of anti-commuting Pauli matrix pairs. You can use the statement to check (b).