# TA session — Day 3

**Exercise 1.** Compute the stabilizers for Shor's nine qubit code. What are the logical operators $\overline{X}$ and $\overline{Z}$? Prove that it indeed corrects any Pauli Error of weight 1.

*Hint: Start with the 3 qubit repitition code which is only resilient to $X$ errors. What are the stabilizers for this code and what is $\overline{X}$? Why is there no logical $\overline{Z}$ operator? Similarly, what is the 3 qubit repitition code that is resilient to $Z$ errors? Recall that the 9 qubit code is the 3 qubit $Z$-resistent code applied to an encoded 3 qubit $X$-resistent code.*

**Exercise 2** (Constant depth quantum circuits)**.** Suppose that $U$ is a quantum circuit of depth $d$ composed of one- and two-qubit gates. In class we discussed a relation problem that can be solved by a constant depth $U$ but cannot be solved with high probability by a classical constant depth circuit. In this exercise we will see that such a separation is not possible in the context of computing a function (rather than a relation). We shall write $|\psi_x\rangle = U|x\rangle$.

1. Show that for any $i = 1, \dots, n$ the expected value $\langle \psi_x | Z_i | \psi_x \rangle$ can be computed by a classical circuit of constant size. (Hint: First show that it can be computed by a *quantum* circuit of constant size.)

2. Fix a function $f : \{0,1\}^n \to \{0,1\}^n$. Suppose $U$ computes $f$ deterministically , i.e., $\|\langle z|\psi_x\rangle\|^2 = 1$ if $z = f(x)$ and $\|\langle z|\psi_x\rangle\|^2 = 0$ otherwise. Use the result of 1. to show that $f$ can be computed by a constant depth classical circuit with bounded fan in gates.

3. (Optional) Suppose that $U$ computes $f$ with high probability, say $\|\langle z|\psi_x\rangle\|^2 \geq 1 - \frac{1}{n}^2$. Show that $f$ can be computed (deterministically!) by a constant depth classical circuit with bounded fan-in gates. *(Hint: estimate the probabilities of the measurement outcomes.*

**Exercise 3.** (Global entanglement in QECC states) Suppose that $|\psi\rangle$ is a state in the code space of a quantum error correcting code, which corrects more than a constant number of errors. We will show that $|\psi\rangle$ cannot be generated by constant depth quantum circuits (that is, it has global entanglement).

1. First show that if $U$ is a constant depth quantum circuit, and $A$ is an operator acting on one qubit, then $UAU^\dagger$ acts nontrivially only on a constant number of qubits.

2. Show, using the above, that if a state $|\alpha\rangle$ can be generated by applying on $|0^n\rangle$ a constant depth quantum circuit, then $|\alpha\rangle$ is a unique groundstate of a local Hamiltonian. *(Hint: the locality depends on the constant in part 1.)*

3. Deduce using the properties of the code that the code state $|\psi\rangle$ cannot be generated by a constant depth quantum circuit.

**Exercise 4** (Efficient classical simulation of depth 2 circuits (Terhal and Divincenzo 2002))**.** Consider a depth 2 quantum circuit of a special form where in the first time step two-qubit gates are applied between qubits $(2,3),(4,5),....$ In the second step two qubit gates are applied between $(1,2)$, $(3,4)$, ... ,. Our goal is to show that a classical algorithm can efficiently sample from the output distribution of this circuit, which we denote $p(z)$ below. (Notice that this is different than what was achieved in problem 1; there we made an assumption on the output distribution of the circuit.)

1. First show that the marginal distribution $p(z_1, z_2)$ of the first two output bits can be computed efficiently. (This is similar to 1. from the previous exercise). The classical algorithm first samples these values $z_1, z_2$ from this marginal distribution.

2. Next observe that the conditional distribution $p(z_3, z_4|z_1, z_2)$ can be computed efficiently in a similar way. The second step of the classical algorithm is to sample $z_3, z_4$ from this conditional distribution.

3. Finish the description of the classical simulation algorithm. Then convince yourself that a variant of this algorithm works for arbitrary depth-2 circuits (i.e., without the special form above).

# Quantum games and rigidity

**Exercise 5** (Clause-vs-variable game)**.** Let $\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ be a 3SAT formula over $n$ variables $x_1, \ldots, x_n$, i.e. each clause $C_j$ has the form $C_j = x_{i_1} \vee x_{i_2} \vee \overline{x_{i_3}}$, where any variable can be negated.

Consider the following two-player game associated to $\varphi$. The referee selects a clause $C_j$ at random, but does not tell the players. To Alice, he sends the labels of the three variables appearing in $C_j$. To Bob, he sends the label of only one of the three variables in $C_j$, chosen at random. For example, if $C_j = x_{i_1} \vee x_{i_2} \vee \overline{x_{i_3}}$ then Alice's question is $(x_{i_1}, x_{i_2}, x_{i_3})$, and Bob's question could be just $x_{i_3}$.

Alice replies with three bits, and Bob with one bit. The referee accepts if and only if Alice's three bits are an assignment that satisfies the clause $C_j$ (just that clause), and if Bob's bit is the same as Alice's bit, for the variable that was the same as Bob's question. (In the example, Bob's answer bit should equal Alice's third answer bit.)

Show that the formula $\varphi$ has a satisfying assignment if and only if there is a classical strategy for the players that wins with probability 1.

**Exercise 6.** We need the following two lemmas for the next exercise.

1. Let $|\phi_D\rangle = D^{-1/2} \sum_{i=1}^{D} |i\rangle\,|i\rangle$. Show that $\langle \phi_D | A \otimes B | \phi_D \rangle = D^{-1} \mathrm{Tr} AB^\dagger$.

2. Suppose that $A$ and $B$ anticommute, i.e. $AB = -BA$. Show that $\mathrm{Tr} AB^\dagger = 0$.

**Exercise 7** (Tisrelson's theorem)**.** Show the "hard direction" in Tsirelson's theorem: given an XOR game $G$ and a vector solution to SDP($G$) it is always possible to find a quantum strategy that achieves exactly the same value.

*Hint: Show that for any integer $d$ there exists a $D$ and Hermitian matrices $C_1, \ldots, C_d \in \mathbb{C}^{D \times D}$ that square to identity and pairwise anti-commute. For any vector $u$, consider $u \mapsto C(u) = \sum_i u_i C_i$. What can you say about $C(u)$? And about $\langle \phi_D |\, C(u) \otimes C(v)\, | \phi_D \rangle$, where $|\phi_D\rangle = D^{-1/2} \sum_{i=1}^{D} |i\rangle\,|i\rangle$?*

In exercises 9 and 10, we'll prove special cases of the following theorem, which is useful for certifying optimal strategies in certain games.

**Theorem 8** (Gowers-Hatami)**.** *Let $G$ be a finite group. Let $f : G \to \mathbb{C}^{d\times d}$ be a function such that $f(x)^{-1} = f(x)^\dagger$ and*

$$\mathbb{E}_{x,y\in G}[\|f(x)f(y) - f(xy)\|_2] \leq \varepsilon. \tag{1}$$

*Then there is an isometry $V : \mathbb{C}^d \to \mathbb{C}^D$ and a map $\tau : G \to \mathbb{C}^{D\times D}$ such that*

$$\mathbb{E}_x[f(x) - V^\dagger \tau(x) V] \leq \varepsilon, \tag{2}$$

*and $\tau(x)\tau(y) = \tau(xy)$ for all $x, y \in G$.*

**Exercise 9** (BLR from Gowers-Hatami)**.** Consider the abelian group $G = (\mathbb{Z}_2^n, \oplus)$.

1. Determine all irreducible representations of $G$. *(Hint: Since $G$ is abelian, these are precisely the characters of $G$. The number of characters is equal to the number of elements in the group.)*

2. Prove the Gowers-Hatami theorem for $G$. *[Hint: recall Parseval's formula, and define $V$ from the squared Fourier coefficients $\hat{f}^2(S)$ of $f$]*

3. (Carefully) deduce the following theorem, due to Blum, Luby and Rubinfeld: for any $f : \{0,1\}^n \to \{-1,1\}$ such that $\mathrm{E}_{x,y\in\{0,1\}^n} f(x)f(y)f(x\oplus y) \geq 1-\varepsilon$ for some $\varepsilon > 0$, there is an $u \in \{0,1\}^n$ such that $\mathrm{E}_x f(x)(-1)^{u\cdot x} \geq 1 - O(\varepsilon)$ (here both expectations are under the uniform distribution). In other words, an almost-linear function is always close to an actual linear function.

**Exercise 10** (Gowers-Hatami for the single-qubit Pauli group)**.** Prove the Gowers-Hatami theorem for the case where $G$ is the single-qubit Weyl-Heisenberg group, which is the 8-element matrix group generated by the Pauli $\sigma_X$ and $\sigma_Z$ matrices. *Hint: Consider $V : \mathbb{C}^d \to \mathbb{C}^{d'} \otimes \mathbb{C}^2$, where $\mathbb{C}^{d'} \simeq \mathbb{C}^d \otimes \mathbb{C}^2$, defined by*

$$V|\varphi\rangle = \frac{1}{2}\big((\mathrm{Id}\otimes\mathrm{Id} + A_0\otimes\sigma_X + A_1\otimes\sigma_Z + A_0A_1\otimes\sigma_X\sigma_Z)\otimes\mathrm{Id}\big)\big(|\varphi\rangle\otimes|\phi_2\rangle\big)\,.$$