MA503: Homework 7

Exercise 7.1. [10pts] Find the Smith normal form of the matrix

$$\begin{bmatrix} 1 & 2 & 1 \\ 3 & 4 & 0 \\ 2 & 1 & -1 \end{bmatrix}$$

Show all steps!

Exercise 7.2. [10pts] Consider the set $\mathbf{Hom}(\mathbb{Z}^n, \mathbb{Z}_2)$ of homomorphisms from $\mathbb{Z}^n$ to $\mathbb{Z}_2$ has 2^n elements. Fix the standard free basis $\{e_1, \ldots, e_n\}$ for $\mathbb{Z}^n$.

(a) Consider any homomorphism $\varphi : \mathbb{Z}^n \to \mathbb{Z}_2$. Let $b_i = \varphi(e_i)$ for $i = 1, \ldots, n$. Let $v = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$. Show that $\varphi(v)$ is uniquely defined by $b_1, \ldots, b_n$, i.e., find a formula for $\varphi(v)$.

(b) Prove that for any $b_1, \ldots, b_n \in \{0, 1\}$ there exists a homomorphism φ satisfying $b_i = \varphi(e_i)$ for every $i = 1, \ldots, n$.

(c) Conclusion. There are 2^n choices of $b_1, \ldots, b_n \in \{0, 1\}$. Each choice defines a unique homomorphism. Hence, there are 2^n homomorphisms.

A **hidden subgroup problem** algorithm is one of the most advanced algorithms in quantum computing. The factorization problem and the dlp problem are particular cases of HSP. The goal of that algorithm is to learn the algebraic structure of some abelian group G "hidden inside an algebraic operator".

- By assumption, we know the generators $x_1, \ldots, x_n$ for G.
- Roughly speaking, each iteration of the algorithm produces a random relation for $x_1, \ldots, x_n$, i.e., a tuple $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ satisfying $\alpha_1 x_1 + \ldots + \alpha_n x_n = 0$.
- It can produce a useless relation, like $(0, \ldots, 0)$.
- It can produce a redundant relation, i.e., one that follows from already found relations.

Exercise 7.3. [10pts] Suppose that G is an abelian group generated by x_1 and x_2. Using a quantum algorithm we learn that x_1 and x_2 are subject to the following relations:

$$r_1 = 6x_1 + 10x_2 = 0$$
$$r_2 = 14x_1 - 2x_2 = 0$$
$$r_3 = -4x_1 + 18x_2 = 0.$$

Assuming that this set of relations is complete (all other relations follow from r_1, r_2, r_3) express G as a direct product of cyclic groups.

Exercise 7.4. [10pts] Suppose that G is an abelian group generated by x_1, x_2, x_3. Using a quantum algorithm we learn that x_1, x_2, x_3 are subject to the following relations:

$$r_1 = 2x_1 + 4x_2 - 4x_3 = 0$$
$$r_2 = -4x_1 + 2x_2 + 8x_3 = 0.$$

Assuming that this set of relations is complete (all other relations follow from r_1, r_2) express G as a direct product of cyclic groups.

Definition 7.1. A ring R is a **commutative** if $\cdot$ is commutative.

All rings in our course are commutative!

Definition 7.2. $a \in R$ is a **unit** if R contains a **multiplicative inverse** for a, i.e., for some $b \in R$, $ab = 1$, denoted by a^{-1}.

Definition 7.3. A **field** is a commutative ring in which **every non-trivial element is a unit**.

Exercise 7.5. [+6pts] Which of the following rings are fields? If R is a field, then find inverses for all nontrivial elements, or a formula to compute the inverse. If R is not a field, then find a nontrivial element that has no inverse (prove that it has no inverse).

(a) $(\mathbb{Z}_5, +, \cdot)$
(b) $(\mathbb{Z}_6, +, \cdot)$
(c) $\{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ with the usual addition and multiplication.