MATH 1800: Quantum Information Theory with Applications to Cryptography

Bonus 3

Definition. Let p be a prime number. Then we define the **finite field** $\mathbb{F}_p$ via

- $\mathbb{F}_p := \{0, 1, \dots, p-1\}$
- addition and multiplication are performed modulo p.

The following observation follows from the fact that for any $0 \neq a \in \mathbb{F}_p$ one has $\gcd(a, p) = 1$ and an application of (extended) Euclid's algorithm.

Observation. *For all $0 \neq a \in \mathbb{F}_p$, there exists a multiplicative inverse, i.e. $b \in \mathbb{F}_p$ such that $ab \equiv 1 \pmod p$.*

Remark. A **commutative ring** is a set endowed with operations of addition and multiplication, which satisfy a collection of natural axioms (the operations on $\mathbb{F}_p$ defined above can be easily checked to do so). The existence of multiplicative inverses is required for a commutative ring to be a field.

Definition. A **vector space** V **over a field** $\mathbb{F}_p$, is a a collection of elements $v \in \mathbb{F}_p^n := \underbrace{\mathbb{F}_p \times \mathbb{F}_p \times \dots \times \mathbb{F}_p}_{n}$, together with coordinate-wise addition

$$v + w := (v_1 + w_1, v_2 + w_2, \dots, v_n + w_n) \text{ for } v, w \in V$$

and scalar multiplication

$$\lambda v := (\lambda v_1, \lambda v_2, \dots, \lambda v_n) \text{ for } v \in V,\ \lambda \in \mathbb{F}_p.$$

Example. A plane over the field $\mathbb{F}_7$ consists of 49 points.

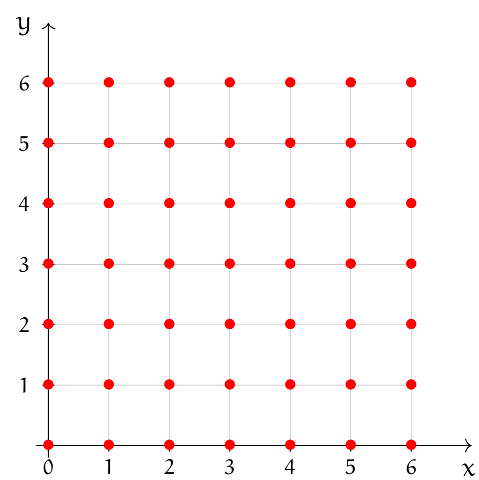

Figure 1: Plane $\mathbb{F}_7^2$

Problem 1. (1 pt) On the picture above circle all points that satisfy the following equations.

(a) $y = 3x + 5$ (a line)

(b) $y = x^2$ (a parabola)

Problem 2. (3 pts)

(a) Let V be an n-dimensional space over $\mathbb{F}_p$ and $W \subset V$ a k-dimensional subspace. Find the probability that a randomly chosen nonzero vector (point) in V does not lie in W.

(b) What is the probability that the linear equation produced by $(k+1)^{\text{st}}$ iteration of Simon's algorithm will be independent from the system of k independent linear equations?

(c) How many different subspaces $W \subset V$ of dimension k are there?[1]

Problem 3. (3 pts) Here is a possible generalization of Simon's problem. Let $W = \mathbb{F}_2^k \subset V = \mathbb{F}_2^n$ be a subspace of the space of all possible strings of n classical bits and $f : \mathbb{B}^n \to \mathbb{B}^n$ a map with the property that $f(x) = f(y)$ iff $x = y \oplus s$ for some $s \in W$.

(a) Suppose you are given a map $f : \mathbb{B}^n \to \mathbb{B}^n$ as in the statement of the problem. What is the minimal number of values of f needed to uniquely recover W?

[1]**Hint:** start by choosing any nonzero vector $v \in V$, then a vector not lying on the line spanned by V, etc. The answer is known as q-binomial coefficient (here $q = p$). You can look it up, but make sure to understand and explain why this formula actually gives the answer.

(b) Let's consider a concrete example with $n = 4$ and $N = 2^4 = 16$. Find (list all vectors in) W given that $f(0000) = f(0101) = f(1010) = 1111$.

(c) Suppose you are given that

$$\begin{aligned} f(0000) &= f(0101) = f(1010) = f(1111) = 1111 \\ f(1000) &= f(1101) = f(0010) = f(0111) = 0110 \\ f(0100) &= f(0001) = f(1110) = f(1011) = 0001 \\ f(1100) &= f(1001) = f(0110) = f(0011) = 1101. \end{aligned}$$

Run Simon's algorithm twice with your own pick of measurement outcomes to obtain two linearly independent vectors in V orthogonal to W.