Math 480A: Algebraic Complexity Theory, Spring Quarter 2019
Jarod Alper
Homework 2
Due: Friday, April 26

**Problem 2.1.** Show that $\{0,1\}^*$ is countable.

**Problem 2.2.** A *commutative ring* is a set $R$ endowed with two binary options

$$+\colon R \times R \to R \qquad \text{(addition)}$$
$$\times\colon R \times R \to R \qquad \text{(multiplication)}$$

satisfying the following properties for all $a, b, c \in R$.

| | |
|---|---|
| (1) $(a+b)+c = a+(b+c)$ | (addition + is associative) |
| (2) $a+b = b+a$ | (addition + is commutative) |
| (3) There is a $0 \in R$ with $a+0=a$. | (there is an additive identity 0) |
| (4) For each $x \in R$, there exists $y \in R$ with $x+y=0$ | (there is an additive inverse of $x$ which we usually as '$-x$'.) |
| (5) $(a \times b) \times c = a \times (b \times c)$ | (multiplication $\times$ is associative) |
| (6) $a \times b = b \times a$ | (multiplication $\times$ is commutative) |
| (7) There is a $1 \in R$ with $a \times 1 = a$ | (There is a multiplicative identity 1) |
| (8) $a \times (b+c) = a \times b + a \times c$ | (Multiplication distributes over addition). |

Let $k$ be $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ and define

$$k[x_1, \dots, x_n] := \text{set of all polynomials } f(x_1, \dots, x_n) \text{ with coefficients in } k$$

Show that $k[x_1, \dots, x_n]$ is a commutative ring where $+$ and $\times$ are the usual addition and multiplication of polynomials.

**Problem 2.3.** Let $n$ be a positive integer. Define $\mathbb{Z}/n := \{0, 1, 2, \dots, n-1\}$. If $a \in \mathbb{Z}$, we define $a$ *modular* $n$, which we denote by $a \mod n$, as the the unique integer $a' \in \mathbb{Z}/n$ such that $a - a'$ is divisible by $n$. Define addition (resp. multiplication) in $\mathbb{Z}/n$ by taking the usual addition (resp. multiplication) and then taking it modular $n$.

(a) Compute $73 \mod 13$.
(b) Show that $\mathbb{Z}/n$ is a commutative ring.
(c) Show that the map of sets $f\colon \mathbb{Z} \to \mathbb{Z}/n$ which maps $a \mapsto a \mod n$ satisfies the following three properties: (i) $f(x+y) = f(x)+f(y)$, (ii) $f(x \times y) = f(x) \times f(y)$ and $f(1) = 1$. A map between rings satisfying these three properties is called a *ring homomorphism*.
(d) Convince yourself that your argument for Problem 2.2 also shows that the set $\mathbb{Z}/n[x_1, \dots, x_n]$ of polynomials $f(x_1, \dots, x_n)$ with coefficients in $\mathbb{Z}/n$ is also a ring. *(You need not write anything down here.)*

**Problem 2.4.** A *field* is a commutative ring $R$ satisfying the additional property

(9) For each nonzero $x \in R$, there exists $y \in R$ with $x \times y = 1$ (there is a multiplicative inverse of $x$ which we usually write it as '$x^{-1}$'.)

Examples of fields include $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. Show that if $p > 1$ is a prime integer, then $\mathbb{Z}/p$ is a field.

**Problem 2.5.** Let $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}/p$ (or more generally any field).

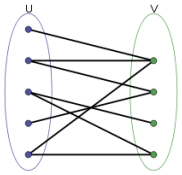
(1) For integers $d$ and $n$, what is the dimension of the vector space $k[x_1, \ldots, x_n]_{\leq d}$ consisting of all polynomials in variables $x_1, \ldots, x_n$ of degree $\leq d$?
(2) What is the dimension of the vector space $k[x_1, \ldots, x_n]_d$ of homogeneous polynomials in $x_1, \ldots, x_n$ of degree $d$?
(3) What is the dimension of the vector space of homogeneous polynomials $f$ in $x_1, \ldots, x_n$ of degree $d$ in which all of the exponents of every monomial appearing in $f$ are either 0 or 1? For example, $x_1x_2x_4x_5$ would be in the vector space but $x_1^2x_4x_5$ would not be.

**Problem 2.6.** Show that the language CLIQUE is NP-complete.

**Problem 2.7.** Define the language $ROOTS \subset \{0,1\}^*$ to be the set of polynomials $f(x_1, \ldots, x_n)$ (not necessarily homogeneous) with coefficients in $\mathbb{Z}/2$ which have a root (i.e., there exists $(a_1, \ldots, a_n) \in (\mathbb{Z}/2)^n$ with $f(a_1, \ldots, a_n) \cong 0 \mod 2$). Show that ROOTS is NP-complete.

**Problem 2.8.** Problem 7.29 about 3COLOR from Sipser, 3rd edition (It is Problem 7.34 in the 1st and 2nd edition and Problem 7.38 from the international version of the 3rd edition).

**Problem 2.9.** A *bipartite graph* is a graph $G = (W, E)$ where the set vertices $W$ is decomposed into two disjoint sets $U$ and $V$ such that every edge connects a vertex from $U$ to a vertex from $V$. An example:




From wikipedia

A *perfect matching* is a collection of edges in $G$ such that each vertex is contained in exactly one edge. Consider the language PERFECT consisting of bipartite graphs that contain a perfect matching. Show that PERFECT is NP-complete.

**Problem 2.10.** Define the Boolean operation NAND by $x \,\text{NAND}\, y := \overline{x \wedge y}$ (i.e., $x \,\text{NAND}\, y$ is the opposite of $x$ AND $y$). Show that any Boolean expression can be written using only NAND operations.