15-252

Assignment 6 Due: March 23, 2018.

---

1 Polynomial Equations Mod 2 (50)

Background

We have seen that Diophantine equations are hard: it is undecidable whether a polynomial with integer coefficients has an integer solution. By contrast, modular arithmetic is easy in the sense that one can conduct brute force search over the finitely many possible values. Arithmetic over $\mathbb{Z}_p$, p a prime, is particularly interesting since we are dealing with a field in this case.

Task

1. Show that any function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ can be expressed in terms of a polynomial $P(x_1, \ldots, x_n)$.
2. Show that one can solve a single polynomial equation $P(x_1, \ldots, x_n) = 0$ over $\mathbb{Z}_2$ in polynomial time.

---

2 Building A Finite Field (50)

Background

As we have seen in class, there is a unique finite field of size p^k for any prime p and $k \geq 1$. Needless to say, the case $p = 2$ it is particularly interesting for actual implementations: the prime field can naturally be represented by bits and the arithmetic operations are given by xor (addition) and and (multiplication).

Building a finite field $\mathbb{F}_{2^k}$ requires a little more work.

Task

A. Show how to construct the finite field $\mathbb{F}$ of size 256. What data structures would you use, how would you implement arithmetic in this field.

B. How many primitive elements are there in this field?

C. What are all the subfields of $\mathbb{F}$? Why?

D. If we had constructed a field of size 32, what would the subfields be?

E. What is the main difficulty in doing a similar construction for the field of size 2^{1024}?