1 Polynomials Mod 2 (25)

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 $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ 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.

Comment
It is probably a good idea to distinguish between a polynomial $P(x_1, \ldots, x_n) \in \mathbb{Z}_2[x_1, \ldots, x_n]$ and the corresponding function $\hat{P} : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$.

2 Polynomials Mod $p$ (25)

Background
We have seen many examples of functions $f : A^n \rightarrow A$ over some finite domain $A$ that can be expressed in terms of simple components, yet have useful behavior. Often some sort of algebraic characterization is helpful in analyzing these functions.

One potentially interesting representation is in terms of polynomials: find some multivariate polynomial $P$ such that $f(x) = P(x)$. Of course, in general there may be no such polynomial but for arithmetic modulo a prime it turns out that polynomial functions already include every possible function.

Task

A. Show that any function $f : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p$ can be expressed in terms of a polynomial $P(x_1, \ldots, x_n)$ where $p$ is an arbitrary prime.

B. For $p = 2$, what does this have to do with representations of Boolean functions in terms of negation, conjunctions and disjunctions?

C. How about functions $f : \mathbb{Z}_m^n \rightarrow \mathbb{Z}_m$ in general?
D. Testing whether a single polynomial equation \( P(x_1, \ldots, x_n) = 0 \) over the integers has a solution is undecidable. By contrast, show that over \( \mathbb{Z}_2 \) we can check in polynomial time whether there is a solution. Note: we are not talking about systems of equations here, just a single one.

3 Shrinking Dimension (25)

Background
As we have seen in class, there is a unique finite field \( \mathbb{F} \) of size \( p^k \) for any prime \( p \) and \( k \geq 1 \). In one standard implementation we then think of \( \mathbb{F} \) as a vector space of dimension \( k \) over \( \mathbb{F}_p \), so the field elements are vectors of modular numbers. However, it is sometimes more convenient to deal with a lower-dimensional vector space over a larger ground field. More precisely, we may have a tower of fields

\[
\mathbb{F}_p \subseteq K \subseteq \mathbb{F}
\]

and we can consider \( \mathbb{F} \) as a vector space over \( K \). Alas, this only works under special circumstances which will be described in this problem.
Fix some prime characteristic \( p \) throughout.

Task

A. Show that the following are equivalent, where \( 1 \leq \ell \leq k \):

(a) \( \ell \) divides \( k \)

(b) \( p^\ell - 1 \) divides \( p^k - 1 \)

(c) \( x^\ell - 1 \) divides \( x^k - 1 \) (in the polynomial ring \( \mathbb{F}_p[x] \)).

B. Show that if \( K \) is a subfield of \( \mathbb{F} \) then \( K \) is (isomorphic to) \( \mathbb{F}_{p^\ell} \) where \( \ell \) divides \( k \).

C. Show that if \( \ell \) divides \( k \) then \( \mathbb{F}_{p^\ell} \) is (isomorphic to) a subfield of \( \mathbb{F} \).

Comment
The last item is the hardest; think splitting fields.

4 Building A Finite Field (25)

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 \texttt{xor} (addition) and \texttt{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 $2^{1024}$?