15-354: CDM **K. Sutner**

Assignment 9 Due: **April 30, 2021**.

1. Shrinking Dimension (30)

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, it may be better to build a tower of subfields

$$\mathbb{F}_p \subseteq \mathbb{K} \subseteq \mathbb{F}$$

and then to interpret $\mathbb{F}$ as a lower-dimensional vector space over $\mathbb{K}$. 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) ℓ 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 $\mathbb{K}$ is a subfield of $\mathbb{F}$ then $\mathbb{K}$ is (isomorphic to) $\mathbb{F}_{p^\ell}$ where ℓ divides k.

C. Show that if ℓ 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.

2. Redundant Field Representations (30)

Background

Here is another, somewhat surprising way to represent a finite field: we can embed $\mathbb{F}_{2^k}$ in a quotient ring $\mathbb{K} = \mathbb{F}_2[x]/(x^n + 1)$ that fails to be a field itself. In other words, we pick elements in $\mathbb{K}$ that behave just like $\mathbb{F}_{2^k}$ with respect to addition and multiplication.

For example, $\mathbb{F}_4$ can be embedded into $\mathbb{K} = \mathbb{F}_2[x]/(x^3 + 1)$ by using the elements $0, x^2 + x, x + 1, x^2 + 1$. Make sure to figure out which element is the multiplicative generator. This is computationally useful since the reduction in $\mathbb{K}$ is easier than in the classical construction. .

For this method to be of any practical use, the least n such that that $\mathbb{F}_2[x]/(x^n + 1)$ embeds $\mathbb{F}_{2^k}$ cannot be much larger than k. Let's write $\eta(k)$ for this "embedding number". For example, it turns out that $\eta(8) = 17$. The following lemma can be found in an otherwise excellent paper from 1998.

Lemma: $\eta(k) = \min\big(\, n > k \mid k = \text{ order of 2 in } {\mathbb{Z}_n}^\star \,\big)$

Recall that $\mathbb{F}_{2^k}$ is a subfield of $\mathbb{F}_{2^\ell}$ if, and only if, k divides ℓ.

Task

A. Compute $\eta(5)$ and $\eta(10)$ according to this lemma.

B. Conclude that the lemma is false.

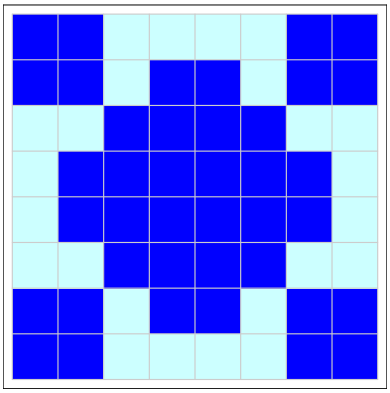
C. Fix the lemma.

3. Chessboards and Lights (40)

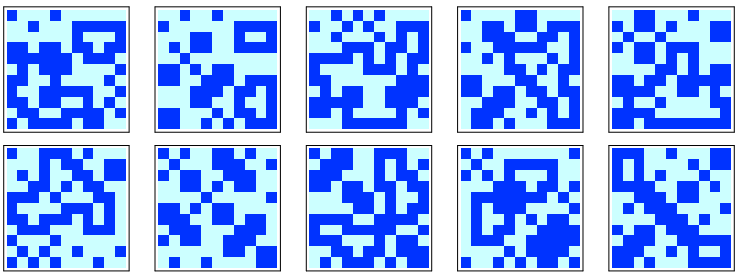
Background

Suppose the squares of chessboard can be illuminated from below, each individually. Tapping a square toggles the corresponding light (on to off, off to on) and also the neighboring squares (north/east/south/west, not diagonally). Initially, all lights are off. So pushing a square in the middle will light up 5 squares.

The goal is to turn on all the lights. One can show that this is always possible, for arbitrary $n \times n$ boards, for rectangular boards $n \times m$, and even for arbitrary undirected graphs (for infinite graphs the vertex degrees need to be finite). Here is a solution for the 8×8 board, which turns out to be unique (disregarding the order in which the squares are tapped):



In general, solutions are not unique. For example, on the 11×11 board there are 64 solutions. If we count modulo rotations and reflections (the natural action of D_4 on the board), only 10 patterns remain:



Note that on the $n \times n$ board there are 2^{n^2} possible configurations. So a little care is needed when one tries to compute solutions. In particular, a brute-force search over the huge space $\mathbf{2}^{n \times n}$ is out.

Task

1. Give a simple description of a solution in terms of the underlying grid graph.
2. Find an algorithm that computes the solutions for the $n \times n$ board using only a search over $\mathbf{2}^n$.
3. Find a fast algorithm to compute the number of solutions for the $n \times n$ board.
4. Find a fast algorithm to compute an actual solution the $n \times n$ board.

Comment

Fast definitely means not exponential in n. Think vector spaces over the two-element field and use linear algebra. Exploit the geometry of a $n \times n$ grid.

Extra Credit 1: Find a solution for the 40 by 40 grid (plot a picture, it's easy to check visually whether your solution is correct).

Extra Credit 2: Prove the existence theorem.