Assignment #8

Due **Friday, June 4**

This is a shorter assignment than usual because Monday is a holiday.

Reading: Chapter 14 through p. 234; Chapter 15.

To do but not hand in:

p. 223, Ex's 3, 6;

p. 233, Ex. 1;

p. 241, Ex. 1-(i);

N-4 below.

To hand in:

p. 223, Ex. 1;

p. 243, Ex. 5-(i);

N-1, N-2, N-3 below.

Problem N-1. This problem simplifies the 7-element block design, using $\mathbb{F}_8$. Since $8 = 2^3$, $\mathbb{F}_8$ contains $\mathbb{F}_2$ and is a 3-dimensional vector space over $\mathbb{F}_2$.

So to make the block design we have been studying, instead of using subspaces of $(\mathbb{F}_2)^3$ we can use subspaces of $\mathbb{F}_8$. For this field, just as for other finite fields, there is a generator α for the nonzero elements. There are seven nonzero elements here, so $\mathbb{F}_8 = \{1, \alpha, \alpha^2, \ldots, \alpha^6\}$ and $\alpha^7 = 1$. Another useful fact is that α can be chosen so that $\alpha^3 = \alpha + 1$.

As "vectors", 1 and α are linearly independent since neither is a scalar multiple of the other (over $\mathbb{F}_2$). So one 2-dimensional subspace is $\{0, 1, \alpha, 1+\alpha\}$. But because of the equation satisfied by α we can write this as $\{0, 1, \alpha, \alpha^3\}$.

(a) Multiply the equation $\alpha^3 = 1 + \alpha$ through by α, getting $\alpha^4 = \alpha^2 + \alpha$. This helps to give a description of the subspace generated by α and α^2, in terms of powers of α. What is this description? (Simple.)

(b) Multiply through again and again to get more 2-dimensional subspaces, and list their elements using powers of α. You should find that there are seven in all. (If you get more than that, you have forgotten to use $\alpha^7 = 1$.)

(c) To make our block design, we made blocks correspond to 2-dimensional subspaces and plants correspond to the 1-dimensional subspaces they contain.

The 1-dimensional subspaces are the spans of nonzero vectors and are of the form $\{0, \alpha^i\}$ for $i = 0, 1, \ldots, 6$, so number the plants 0 through 6 and have plant i go with the subspace $\{0, \alpha^i\}$. Therefore our first 2-dimensional subspace $\{0, 1, \alpha, \alpha^3\}$ gives a block with plants $0, 1, 3$. What are the other blocks?

(d) In class it was mentioned that this block design has 168 symmetries. A symmetry is a one-to-one function on plants to plants that preserves the blocks—in other words, three plants in a block go to three plants in a block. Some symmetries come from drawing the design using the triangle picture and then rotating or flipping the triangle. Look instead at the function that takes plant 0 to plant 1, plant 1 to plant 2, plant 2 to plant 3, etc., and plant 7 to plant 0. Is that a symmetry?

Problem N-2. Let p be a prime and consider the 3-dimensional vector space $(\mathbb{F}_p)^3$ over $\mathbb{F}_p$. How many one-dimensional subspaces are there?

(Method: A 1-dimensional subspace consists of all scalar multiples of a nonzero vector. Different nonzero vectors might give the same 1-dimensional subspace. So start with the number of nonzero vectors but then divide by an appropriate factor to take this fact into account. Your final answer should be a polynomial in p. Notice that two distinct 1-dimensional subspaces overlap only at $\mathbf{0}$. Also notice that often we have been dealing with $\mathbb{F}_2$, where there are only two scalars, but here there are p scalars.)

Problem N-3. (a) If m and n are coprime and $m|kn$ then $m|k$. Why?

(b) If m and n are coprime and k is a multiple of both, then $mn|k$. Why?

(c) Suppose that a and b are units in a finite commutative ring and have orders m and n respectively, where m and n are coprime. Show that ab has order mn.

(You may assume the ring is $\mathbb{Z}/\ell\mathbb{Z}$ for some ℓ but that doesn't really matter. Method: We know that the list of powers $1, a, a^2, \ldots$ repeats every m steps, so that $a^i = 1$ precisely when i is a multiple of m. Suppose $(ab)^k = 1$, so that $a^k = b^{-k}$. Take the n-th power of both sides. What happens? Look for opportunities to use (a) and (b) to learn more about k.)

Problem N-4. To see how to design a code that corrects more errors, here is one method that has actually been used in space communications:

A 16×16 *Hadamard matrix* with entries ± 1 is constructed as follows: Let $H_1 = [1]$ (a 1×1 matrix) and for each $k = 2, 4, 8, 16$ let $H_k = \begin{bmatrix} H_{k/2} & H_{k/2} \\ H_{k/2} & -H_{k/2} \end{bmatrix}$.

So $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$, etc. Stop at H_{16}. Then to get bits, replace 1 by 0 and -1 by 1, resulting in the matrix

$$\bar{H}_{16} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&0&1&1&0&1&0&0&1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0 \\ 0&1&1&0&1&0&0&1&0&1&1&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&1&0&1&0&1&0&1&1&0&1&0&1&0&1&0 \\ 0&0&1&1&0&0&1&1&1&1&0&0&1&1&0&0 \\ 0&1&1&0&0&1&1&0&1&0&0&1&1&0&0&1 \\ 0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0 \\ 0&1&0&1&1&0&1&0&1&0&1&0&0&1&0&1 \\ 0&0&1&1&1&1&0&0&1&1&0&0&0&0&1&1 \\ 0&1&1&0&1&0&0&1&1&0&0&1&0&1&1&0 \end{bmatrix}$$

Notice that this matrix has the property that any two rows agree in 8 places and disagree in 8 places.

To transmit 4 bits with this code, treat the rows as numbered from 0 to 15 but in binary (`0000` to `1111`) and send that row. For example, `0110` means row 6, which is the 7th row since we started counting from 0, and so we send `0011110000111100`.

(a) What is the largest number of bit errors that can always be detected, among the 16 bits transmitted? For example, if three of the sixteen bits were transmitted incorrectly, would it be known that something is wrong?

(b) What is the largest number of bit errors that can always be corrected? For example, if two of the sixteen bits were transmitted incorrectly, can it be determined with certainty which row was sent?

(c) Decode the received bits `10011110100111100` and explain why your answer is the best.