Class 2 Exercises

CS250/EE387, Winter 2025

1. Consider the set $F = \{(0,0),(0,1),(1,0),(1,1)\}$. Define addition on F as coordinate-wise addition modulo 2. For example, $(1,0)+(1,1)=(0,1)$.

   (a) Define multiplication on F by $(a,b)\times(c,d)=(a\cdot c, b\cdot d)$. Is F a field under this definition of $+$ and $\times$? Why or why not?

   (b) Define multiplication on F by the following rules:

$\times$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(1,0)$	$(0,0)$	$(1,0)$	$(1,1)$	$(0,1)$
$(1,1)$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,0)$

   Is F a field under this definition of $+$ and $\times$? Why or why not? (You can take for granted that associativity and the distributive law hold; so you just need to check commutivity; identities; and inverses.)

2. Let $\mathcal{C}$ be the binary linear code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

   (a) What is the dimension of $\mathcal{C}$?

   (b) Find a parity-check matrix for $\mathcal{C}$.

   (c) What is the distance of $\mathcal{C}$?

3. Let's talk about **Hamming Codes**!

   Definition 1. *Let $n = 2^r - 1$ for some integer r. The Hamming code $\mathcal{H}_r$ of length n is the code whose parity-check matrix $H_r \in \mathbb{F}_2^{r\times n}$ is the matrix which has every nonzero vector in $\{0,1\}^r$ as its columns.*

   Observe that $\mathcal{H}_3$ is the same as the $(7,4,3)$-Hamming code we defined in Class 1, up to a permutation of the coordinates.

   (a) Show that $\mathcal{H}_r$ has distance 3 for all r. (Hint: We did this in the lecture video for $\mathcal{H}_3$).

   (b) What is the dimension k_r of $\mathcal{H}_r$?

   (c) Confirm that the parameters (n_r, k_r, d_r) of $\mathcal{H}_r$ match the Hamming bound. (That is, that $k_r = n_r - \log_2\left(\mathrm{Vol}_2\left(\left\lfloor\frac{d_r-1}{2}\right\rfloor, n_r\right)\right)$.

4. We say that a code is *perfect* if it meets the Hamming bound. Show that the family of Hamming codes defined above, and coordinate permutations of them, are the only perfect linear binary codes with distance 3.

   [**Hint:** What must the parity-check matrix of such a code look like?]

5. In this problem we will construct a *non-linear* perfect code with distance 3, which is not the same as the Hamming code.

   (a) Let $\mathcal{H}_r$ be the Hamming code of length $n = 2^r - 1$. Consider the code $\mathcal{C}_{r+1} \subseteq \mathbb{F}_2^{2^{r+1}-1}$ given by

   $$\mathcal{C}_{r+1} = \left\{ \mathbf{x} \circ (\mathbf{x} + \mathbf{h}) \circ \sum_{i=1}^{n} x_i \ : \ \mathbf{x} \in \mathbb{F}_2^n, \mathbf{h} \in \mathcal{H}_r \right\},$$

   where $\circ$ denotes concatenation. Show that $\mathcal{C}_{r+1} = \mathcal{H}_{r+1}$.
   (Hint: try to come up with a parity-check matrix for $\mathcal{C}_{r+1}$.)

   (b) Now consider the code $\mathcal{D}_{r+1} \subseteq \mathbb{F}_2^{2^{r+1}-1}$ given by

   $$\mathcal{D}_{r+1} = \left\{ \mathbf{x} \circ (\mathbf{x} + \mathbf{h}) \circ \left(\sum_{i=1}^{n} x_i + f(\mathbf{h}) \right) \ : \ \mathbf{x} \in \mathbb{F}_2^n, \mathbf{h} \in \mathcal{H}_r \right\},$$

   where $f(\mathbf{h})$ is 0 if $\mathbf{h} = \mathbf{0}$, and $f(\mathbf{h}) = 1$ otherwise.

   i. Show that $\mathcal{D}_{r+1}$ is a perfect code.
   (Hint: It suffices to show that $\mathcal{D}_{r+1}$ has distance at least 3 (why?). Can you rule out pairs of codewords at distance 1 or 2 from each other?)
   (Note: This one might get a bit tedious – if you think you see the basic idea, feel free to move on).

   ii. Show that $\mathcal{D}_{r+1}$ is *not* a linear code, for any $r > 1$. In particular it is not the "same" as $\mathcal{H}_{r+1}$, for any reasonable definition of "same."

6. (Not a question for class, just something to think about). The above two problems show that, while Hamming codes are the only *linear* perfect binary codes with distance 3, there are other *non-linear* perfect binary codes of distance 3; it turns out that there are lots of different non-linear perfect binary codes of distance 3.

   You might be wondering about perfect binary codes for other distances. It turns out that there is only one other perfect binary code, discovered by Golay: it happens to be linear, and has length 23 and distance 7. There are no other perfect binary codes, for any distance, linear or not. (This was shown by a line of work in the 1970's—there's a good exposition of it in Van Lint's textbook "Introduction to Coding Theory" if you want to learn more!)

7. (Extra, in case there's time). Let $n = 2k + 1$ for some integer k. Suppose that $C \subseteq \mathbb{F}_2^n$ is a *self-dual* code of length n and dimension k. That is, C is a linear code so that $C \subseteq C^\perp$. Describe $C^\perp \setminus C$.