Class 2 Exercises

CS250/EE387, Winter 2022

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?

   Solution

   No, this is not a field. For example, there are not inverses. For example, $(0,1)\times(1,0)=(0,0)$ But then if $(0,1)$ had an inverse, we'd have $(1,0)=(0,1)^{-1}\times(0,0)=(0,0)$, and that's not true.

   (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?

   Solution

   Yes, this is a field! The "zero" element is $(0,0)$ and the "one" element is $(0,1)$. By looking at the grid we can see that $(0,0)\times(a,b)=(0,0)$ for all (a,b), and $(0,1)\times(a,b)=(a,b)$ for all (a,b). Also we can see that $\times$ is symmetric, since the grid above is symmetric about the diagonal. (You can also check that it's associative, though it's a bit tedious). Also there are inverses! This can be seen since every row/column except for $(0,0)$'s has one $(0,1)$ in it.

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 $\mathcal{C}$?

Solution

The dimension of $\mathcal{C}$ is 3, since G has full rank. A parity-check matrix is given by

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

(This can be verified because $HG = 0$). The distance is 2. This can be seen because the parity-check matrix has two columns which are linearly dependent (in this case, the same), but no one column is 0.

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.

Solution

(a) As we saw in class, it suffices to show that there are 3 linearly dependent columns, but no pair of columns that are linearly dependent (and no zero column). There are lots of pairs of 3 linearly dependent columns (for example any three vectors $x, y, x \oplus y$), and no two columns are linearly dependent since no two are the same (and there is no zero column).

(b) The dimension is $k = 2^r - 1 - r$, since $n = 2^r - 1$, and the parity-check matrix has rank r.

(c) The volume of the Hamming ball of radius $\lfloor (3-1)/2 \rfloor = 1$ is $n + 1 = 2^r$. The Hamming bound says that $n - k \geq \log_2(2^r) = r$, and indeed we have $k = 2^r - 1 - r = n - r$.

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.

Solution

In order to meet the Hamming bound for $d = 3$, we need to have

$$\log_2(\mathrm{Vol}(\lfloor (d-1)/2 \rfloor, n)) = n - k$$

or plugging in $d = 3$,

$$\log_2(n+1) = n - k.$$

In particular, $\log_2(n+1)$ needs to be an integer, which means that n needs to be of the form $2^r - 1$. So we need to be in the same parameter regime as the Hamming codes.

Now, suppose we have some linear code C of length $n = 2^r - 1$ and dimension $n - r$. The parity-check matrix H for C is then $r \times n$. Since C should have distance 3, that means that no two columns of the parity-check matrix should be the same, and all columns need to be nonzero. But the only way that $H \in \mathbb{F}_2^{r \times (2^r - 1)}$ can have all distinct nonzero columns is if each column shows up exactly once. This is precisely the Hamming code (or some coordinate permutation of it).

5. (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 $\mathcal{C}_{r+1} = \mathcal{H}_{r+1}$.

Solution

Let H_r be the parity-check matrix for $\mathcal{H}_r$. Consider the matrix

$$H_{r+1} = \begin{pmatrix} 111\cdots111 & 000\cdots000 & 1 \\ & & 0 \\ H_r & H_r & \vdots \\ & & 0 \end{pmatrix}.$$

On the one hand, this matrix contains every non-zero vector of length $r+1$ as a column, and thus is indeed H_{r+1}, the parity-check matrix for $\mathcal{H}_{r+1}$ (which is why I have called it H_{r+1}). On the other hand, we claim that H_{r+1} is also a parity-check matrix for $\mathcal{C}_{r+1}$. We can see that for any $c \in \mathcal{C}_{r+1}$, we have $H_{r+1}c = 0$. Indeed, the first coordinate of $H_{r+1}c$ is given by

$$\sum_{i=1}^{n} x_i + \sum_{i=1}^{n} x_i = 0$$

and the last r columns are given by

$$H_r\mathbf{x} + H_r(\mathbf{h} + \mathbf{x}) = H_r\mathbf{x} + H_r\mathbf{x} = 0,$$

where we have used the fact that $H_r\mathbf{h} = 0$ since $\mathbf{h} \in \mathcal{H}_r$.
This shows that $\mathcal{C}_{r+1} \subseteq \mathrm{Ker}(H_{r+1})$. To show that H_{r+1} is a parity-check matrix for $\mathcal{C}_{r+1}$, it remains to show that they are equal. We can do this by counting dimensions. $\mathrm{Ker}(H_{r+1})$ has dimension $(2^{r+1} - 1) - (r+1) = 2^{r+1} - r - 2$. Meanwhile, $\mathcal{C}_{r+1}$ has dimension

$$\begin{aligned} (\text{dim of } \mathbf{x}\text{'s to choose from}) + (\text{dim of } \mathbf{h}\text{'s to choose from}) &= n + (n - r) \\ &= (2^r - 1) + (2^r - 1 - r) \\ &= 2^{r+1} - r - 2, \end{aligned}$$

which is the same.
Thus, $\mathcal{H}_{r+1}$ and $\mathcal{C}_{r+1}$ share a parity-check matrix, so they are the same.

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

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

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.

Solution

We need to show that $\mathcal{D}_{r+1}$ has distance 3. To do this, we will rule out pairs of codewords at distance 1 or 2. Consider any two distinct codewords, $\mathbf{c}$ and $\mathbf{c}'$, given by $(\mathbf{x}, \mathbf{h})$ and

by $(\mathbf{x}', \mathbf{h}')$ respectively in the definition of $\mathcal{D}_{r+1}$. Observe that from the definition,

$$\Delta(\mathbf{c}, \mathbf{c}') = \mathrm{wt}(\mathbf{x} - \mathbf{x}') + \mathrm{wt}((\mathbf{x} - \mathbf{x}') + (\mathbf{h} - \mathbf{h}')) + \mathrm{Int}(\sum_i (x_i - x_i') + f(\mathbf{h})). \quad (1)$$

(Above, "Int" is just casting the element of $\mathbb{F}_2$ as 0 or 1 in $\mathbb{Z}$, and wt counts the number of ones in a vector).
We will go through a bunch of cases and use (1) to see that the distance is always at least 3. These bunch of cases are a bit tedious. If you see a cleaner proof, please let me know!

- CASE 1: $\mathbf{x} = \mathbf{x}'$. In this case, we must have $\mathbf{h} \neq \mathbf{h}'$, and by the distance of the Hamming code, $\Delta(\mathbf{h}, \mathbf{h}') \geq 3$. Then (1) implies that

$$\Delta(\mathbf{c}, \mathbf{c}') = \mathrm{wt}(\mathbf{h} - \mathbf{h}') + \mathrm{Int}(f(\mathbf{h})) \geq \mathrm{wt}(\mathbf{h} - \mathbf{h}') \geq 3.$$

- CASE 2: $\mathbf{x} \neq \mathbf{x}'$, and $\mathbf{h} = \mathbf{h}'$. Then:
  - CASE 2a: $\mathrm{wt}(\mathbf{x} - \mathbf{x}') = 1$. Then (1) says that

$$\Delta(\mathbf{c}, \mathbf{c}') = 1 + 1 + 1 = 3.$$

  - CASE 2b: $\mathrm{wt}(\mathbf{x} - \mathbf{x}') = 2$. Then (1) says that

$$\Delta(\mathbf{c}, \mathbf{c}') = 2 + 2 + 0 = 4 \geq 3.$$

  - CASE 2c: $\mathrm{wt}(\mathbf{x} - \mathbf{x}') \geq 3$. Then (1) says that

$$\Delta(\mathbf{c}, \mathbf{c}') \geq 3 + (\text{stuff}) + (\text{stuff}) \geq 3.$$

- CASE 3: $\mathbf{x} \neq \mathbf{x}'$ and $\mathbf{h} \neq \mathbf{h}'$. Then $\mathrm{wt}(\mathbf{h} - \mathbf{h}') \geq 3$, so

$$\mathrm{wt}((\mathbf{x} - \mathbf{x}') + (\mathbf{h} - \mathbf{h}')) \geq 3 - \mathrm{wt}(\mathbf{x} - \mathbf{x}')$$

  by the triangle inequality. Using that, along with (1), we get:
  - CASE 3a: $\mathrm{wt}(\mathbf{x} - \mathbf{x}') = 1$. Then (1) says that

$$\Delta(\mathbf{c}, \mathbf{c}') = 1 + (\geq 3 - 1) + (\geq 0) \geq 3.$$

  - CASE 3b: $\mathrm{wt}(\mathbf{x} - \mathbf{x}') = 2$. Then (1) says that

$$\Delta(\mathbf{c}, \mathbf{c}') = 2 + (\geq 3 - 2) + (\geq 0) = \geq 3.$$

  - CASE 3c: $\mathrm{wt}(\mathbf{x} - \mathbf{x}') \geq 3$. Then (1) says that

$$\Delta(\mathbf{c}, \mathbf{c}') \geq 3 + (\text{stuff}) + (\text{stuff}) \geq 3.$$

In all cases, $\Delta(\mathbf{c}, \mathbf{c}') \geq 3$, so this code has distance at least 3.

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

Solution

Let $\mathbf{h} \neq \mathbf{h}'$ be distinct codewords in $\mathcal{H}_r$, and consider the two codewords of $\mathcal{D}_{r+1}$ given

by

$$(\mathbf{0}, \mathbf{0}+\mathbf{h}, \sum_i x_i + f(\mathbf{h})) = (\mathbf{0}, \mathbf{h}, 1)$$

and

$$(\mathbf{0}, \mathbf{0}+\mathbf{h}', \sum_i x_i + f(\mathbf{h}')) = (\mathbf{0}, \mathbf{h}', 1)$$

The sum of these two is

$$(\mathbf{0}, \mathbf{h}+\mathbf{h}', 0).$$

However, this is *not* a codeword in $\mathcal{D}_{r+1}$, because the codeword corresponding to $\mathbf{0}$ and $\mathbf{h}+\mathbf{h}'$ is

$$(\mathbf{0}, \mathbf{h}+\mathbf{h}', f(\mathbf{h}+\mathbf{h}')) = (\mathbf{0}, \mathbf{h}+\mathbf{h}', 1).$$

So the code is not linear.

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!)

Solution

Neat!

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 $C^\perp \setminus C$.

Solution

We have that $C^\perp \setminus C = \{\mathbf{c}+\mathbf{1} : \mathbf{c} \in C\}$. To see this, first note that for any $\mathbf{c} \in C$, we have

$$0 = \mathbf{c}^T\mathbf{c} = \sum_{i=1}^n c_i^2 = \sum_{i=1}^n c_i$$

by definition and by the fact that we are working over $\mathbb{F}_2$. This means that

$$\mathbf{1}^T\mathbf{c} = \sum_{i=1}^n c_i = 0$$

as well for any $\mathbf{c} \in C$. Therefore, $\mathbf{1} \in C^\perp$. Since n is odd, we have $\mathbf{1}^T\mathbf{1} = 1$, and in particular $\mathbf{1} \notin C$. Thus, $\mathbf{1} \in C^\perp \setminus C$.

Counting dimensions, we see that $\dim(C^\perp) = n-k = k+1$ and $\dim(C) = k$, so therefore $C^\perp$ is given by the span of C and $\mathbf{1}$:

$$C^\perp = C + \{\mathbf{0}, \mathbf{1}\} = C \cup \{\mathbf{c}+\mathbf{1} : \mathbf{c} \in C\}.$$

Thus,

$$C^\perp \setminus C = \{\mathbf{c}+\mathbf{1} : \mathbf{c} \in C\},$$

as desired.