NDMI011: Combinatorics and Graph Theory 1

Tutorial #9

Irena Penev

January 6, 2022

Exercise 1. *Let $\ell \geq 2$ be an integer, and set $n = 2^\ell - 1$, $k = 2^\ell - \ell - 1$, and $d = 3$. Let C be an $(n, k, d)_2$-code over some two-element alphabet Σ.*[1] *Prove that for all $\mathbf{x} \in \Sigma^n$, there exists a unique codeword $\mathbf{c} \in C$ such that $d(\mathbf{x}, \mathbf{c}) \leq 1$.*

> ***Hint:*** *What is the number of words in Σ^n at Hamming distance at most one from a codeword in C?*

Exercise 2. *Compute the parity check matrix and the generating matrix for the Hamming $[7, 4, 3]_2$ code C constructed in section 3 of Lecture Notes 13.*[2] *Further, for each of the following vectors $\mathbf{x} \in \mathbb{F}_2^7$, compute the unique codeword $\mathbf{c} \in C$ such that $d(\mathbf{x}, \mathbf{c}) \leq 1$ (such a $\mathbf{c}$ exists by Exercise 1):*

(a) $\mathbf{x} = (1, 0, 0, 0, 0, 1, 1)$;

(b) $\mathbf{x} = (1, 1, 0, 1, 0, 1, 1)$;

(c) $\mathbf{x} = (1, 0, 1, 1, 0, 1, 1)$.

Exercise 3. *Consider the alphabet $\Sigma = \{0, 1, 2\}$.*

(a) Show that if a code $C \subseteq \Sigma^4$ ***corrects*** *one error, then $|C| \leq 9$. More precisely, assume that a code $C \subseteq \Sigma^4$ has the property that for all $\mathbf{w} \in \Sigma^4$, there is at most one codeword $\mathbf{x} \in C$ such that $d(\mathbf{w}, \mathbf{x}) \leq 1$.*[3] *Prove that $|C| \leq 9$.*

[1] We constructed such a code in section 3 of Lecture Notes 13. Here, you are not supposed to use that particular construction, though. You should only use the fact that C is some $(2^\ell - 1, 2^\ell - \ell - 1, 3)_2$-code.

[2] So, using the notation from that section, we have $\ell = 3$.

[3] For such a code, if the sender sends codeword $\mathbf{x}$, and at most one error is made during transmission, then the receiver is able to reconstruct the word that was sent.

(b) *Exhibit a code* $C \subseteq \Sigma^4$ *that has at least* 20 *codewords, and that has the property that* C ***recognizes*** *one error. More precisely, exhibit a code* $C \subseteq \Sigma^4$ *that has at least* 20 *codewords, and that has the property that for any* $\mathbf{x} \in C$ *and* $\mathbf{w} \in \Sigma^4$ *such that* $d(\mathbf{w}, \mathbf{x}) = 1$*, we have that* $\mathbf{w} \notin C$.[4]

[4] For such a code, if the sender sends a word $\mathbf{x}$, and exactly one error is made during transmission, the receiver can tell that an error was made, but he might not be able to fix it.