Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

WS 2005-2006 Roger Wattenhofer, Nicolas Burri, Pascal von Rickenbach, Yves Weber, and Andreas Wetzel

Mobile Computing
Exercise 4 , Sample Solution

1 Walsh Codes

1.1 Orthogonality

We use induction over the length of the code to prove that the the code words of a Walsh code are pairwise orthogonal. We denote code words of a Walsh code of length 2^k by $c_i^{(k)}$ for $0 \leq i \leq k-1$. Therefore, we have:

$$
\begin{array}{llll}
c_0^{(0)} = (+1) & & & \\
c_0^{(1)} = (+1,+1) & c_1^{(1)} = (+1,-1) & & \\
c_0^{(2)} = (+1,+1,+1,+1) & c_1^{(2)} = (+1,+1,-1,-1) & c_2^{(2)} = (+1,-1,+1,-1) & c_3^{(2)} = (+1,-1,-1,+1) \\
\dots & & &
\end{array}
$$

For the basis of the induction, we can easily verify that the three codes above are orthogonal. In the induction step, we have to show that the code words of length 2^{k+1} are pairwise orthogonal given that the code words of length 2^k are pairwise orthogonal. If we write down the code words of length 2^{k+1} in dependence on the code words of length 2^k, we get:

$$c_{2i}^{(k+1)} := c_i^{(k)}|c_i^{(k)}, \quad c_{2i+1}^{(k+1)} := c_i^{(k)}|\overline{c_i^{(k)}} \quad \text{for } 0 \leq i \leq k-1$$

where $c|d$ denotes the concatenation of two code words and $\bar{c}$ is the inverse of code word c, i.e. $\bar{c} := -c$. Among the code words of length 2^{k+1} there are four possible kind of pairs ($i \neq j$).

1. $c_i^{(k)}|c_i^{(k)}$ and $c_i^{(k)}|\overline{c_i^{(k)}}$: For the inner product, we have
$$c_i^{(k)}|c_i^{(k)} \cdot c_i^{(k)}|\overline{c_i^{(k)}} = c_i^{(k)} \cdot c_i^{(k)} + c_i^{(k)} \cdot \overline{c_i^{(k)}} = c_i^{(k)} \cdot c_i^{(k)} + c_i^{(k)} \cdot (-c_i^{(k)}) = 0.$$
2. $c_i^{(k)}|c_i^{(k)}$ and $c_j^{(k)}|c_j^{(k)}$: By the induction hypothesis, we know that $c_i^{(k)} \cdot c_j^{(k)} = 0$.
3. $c_i^{(k)}|c_i^{(k)}$ and $c_j^{(k)}|\overline{c_j^{(k)}}$: We have $c_i^{(k)} \cdot \overline{c_j^{(k)}} = -c_i^{(k)} \cdot c_j^{(k)} = 0$ and therefore this case follows from the induction hypothesis, as well.
4. For similar arguments as in cases 2 and 3, case 4 follows from the induction hypothesis.

$\square$

1.2 Balance of the Code Words

We use the orthogonality of the code words to get a very simple proof for this exercise. From the definition of the Walsh codes, it is clear that the code word with all ones is always a code word ($(+1,+1,\dots,+1) \in \mathcal{C}$). Since this code word has to be orthogonal to all other code words of $\mathcal{C}$, the other code words have to be balanced, i.e. they need to have the same number of +1 and -1 among their components. $\square$

2 Random White Noise and Orthogonal Codes

2.1 Distribution of X

We have to compute the distribution of $X = \pm m + s \cdot N$ where $s \in \{-1, +1\}^m$ and

$$N = \sum_{i=1}^{k} N_i, \qquad N_i = \big(\mathcal{N}(0,\sigma^2), \mathcal{N}(0,\sigma^2), \ldots, \mathcal{N}(0,\sigma^2)\big).$$

We denote the random part of X by $Y := s \cdot N$ and calculate the distribution of Y. We have

$$Y = \sum_{i=1}^{k} s \cdot N_i = \sum_{i=1}^{k}\sum_{j=1}^{m} \pm 1 \cdot \mathcal{N}(0,\sigma^2) = \sum_{i=1}^{k}\sum_{j=1}^{m} \mathcal{N}(0,\sigma^2) = \sum_{i=1}^{k} \mathcal{N}(0, m\sigma^2) = \mathcal{N}(0, km\sigma^2).$$

Note that $+\mathcal{N}(0,\sigma^2) = -\mathcal{N}(0,\sigma^2)$ since the density function of the normal distribution with expectation value 0 is symmetric with respect to the y-axis. We also use the fact that the sum of two independent Gaussian random variables is a Gaussian random variable as well (cf. the hint on the exercise sheet).

For the distribution of X, we therefore get

$$X \sim \begin{cases} \mathcal{N}(m, km\sigma^2) & \text{if } S \text{ sends a 1} \\ \mathcal{N}(-m, km\sigma^2) & \text{if } S \text{ sends a 0.} \end{cases}$$

2.2

To decode a signal, we check if the value of X is positive (decode as a 1) or negative (decode as a 0). For symmetry reasons, we have that

$$\Pr(X \text{ decoded correctly}) = \Pr(X > 0 | S \text{ sends a 1}) = 1 - \Phi\left(\frac{0 - m}{\sqrt{km\sigma^2}}\right) = \Phi\left(\sqrt{\frac{m}{k}}\right).$$

We get that $\Phi(x) \geq 0.99$ for $x \geq 2.326$ (e.g. by using a table for $\Phi(\cdot)$). We therefore have to choose k such that $\sqrt{\frac{m}{k}} \geq 2.326$ which yields $k \leq 0.185m$. For $m = 128$, we then have to choose $k \leq 23$ such that at least 99% of the received signals are decoded correctly.

3 Slotted Aloha

We define the function $P : \mathbb{R}^2 \to \mathbb{R}$ as

$$P(p, n) := \Pr(\text{success}) = n \cdot p(1-p)^{n-1}.$$

For a fixed p, $P(p,n)$ is monotone increasing for $n \leq -1/\ln(1-p)$ and monotone decreasing for $n \geq -1/\ln(1-p)$ and therefore $P(p,n)$ is minimized either at $n = A$ or at $n = B$ for $n \in [A, B]$. Therefore, we have to find

$$p_{\text{opt}} := \max_p \left(\min\left\{P(p, A), P(p, B)\right\}\right).$$

For a fixed n, $P(p,n)$ is monotone increasing for $p \leq 1/n$ and monotone decreasing for $p \geq 1/n$ (for $p \in [0,1]$). Furthermore, $P(1/A, A) \geq P(1/A, B)$ and $P(1/B, B) \geq P(1/B, A)$ for $B \geq A + 1$ and therefore the intersection between $P(p, A)$ and $P(p, B)$ is between the maxima of $P(p, A)$ and $P(p, B)$, respectively. Thus p_{opt} is found where $P(p_{\text{opt}}, A) = P(p_{\text{opt}}, B)$.

$$\begin{aligned} A p_{\text{opt}}(1-p_{\text{opt}})^{A-1} &= B p_{\text{opt}}(1-p_{\text{opt}})^{B-1} \\ \frac{A}{B} &= (1-p_{\text{opt}})^{B-1-(A-1)} = (1-p_{\text{opt}})^{B-A} \\ p_{\text{opt}} &= 1 - \sqrt[B-A]{\frac{A}{B}}. \end{aligned}$$

For $A = 100$ and $B = 200$, we get

$$p_{\text{opt}} = 0.006908 = \frac{1}{144.8}.$$