HS 2009 Prof. Dr. Roger Wattenhofer, Philipp Sommer, Johannes Schneider

Ad Hoc And Sensor Networks
Sample Solution to Exercise 7

Assigned: November 2, 2009
Due: November 9, 2009

1 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

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

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

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

2 Walsh Codes

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:

$c_0^{(0)} = (+1)$
$c_0^{(1)} = (+1, +1)$ $c_1^{(1)} = (+1, -1)$
$c_0^{(2)} = (+1, +1, +1, +1)$ $c_1^{(2)} = (+1, +1, -1, -1)$ $c_2^{(2)} = (+1, -1, +1, -1)$ $c_3^{(2)} = (+1, -1, -1, +1)$
$\ldots$

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

a) $c_i^{(k)}|c_i^{(k)}$ and $c_i^{(k)}|\overline{c_i^{(k)}}$: For the inner product, we have

$$c_i^{(k)}|c_i^{(k)} \cdot c_i^{(k)}|\overline{c_i^{(k)}} = c_i^{(k)} \cdot c_i^{(k)} + c_i^{(k)} \cdot \overline{c_i^{(k)}} = c_i^{(k)} \cdot c_i^{(k)} + c_i^{(k)} \cdot (-c_i^{(k)}) = 0.$$

b) $c_i^{(k)}|c_i^{(k)}$ and $c_j^{(k)}|c_j^{(k)}$: By the induction hypothesis, we know that $c_i^{(k)} \cdot c_j^{(k)} = 0$.

c) $c_i^{(k)}|c_i^{(k)}$ 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.

d) For similar arguments as in cases 2 and 3, case 4 follows from the induction hypothesis.

2.1 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 ($(+1, +1, \ldots, +1) \in \mathcal{C}$). 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.