Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

11. Exercise sheet
Hand in solutions until Monday, 26 January 2015, 13:59

Exercise 11.1 (Walsh trivia and combining correlations). (11+5 points)

Recall that the Walsh transform of a function $f\colon \mathbb{F}^j \to \mathbb{F}_2$ (or the Fourier transform of $(-1)^{f(\cdot)}$) is given by

$$\widetilde{f}\colon \begin{array}{ccc} \check{\mathbb{F}}_2^j & \longrightarrow & \mathbb{F}_2, \\ a & \longmapsto & \widetilde{f}(a) = \frac{1}{2^j}\sum_{\xi\in\mathbb{F}_2^j}(-1)^{\langle a\,|\,\xi\rangle}\cdot(-1)^{f(\xi)} \end{array}$$

and the correlation is defined by

$$\mathrm{corr}(f) = \mathrm{prob}\,(f(X)=0) - \mathrm{prob}\,(f(X)=1)$$

(i) Prove that f is completely determined by $\widetilde{f}$, namely [2]

$$(-1)^{f(x)} = \sum_{\alpha\in\check{\mathbb{F}}_2^j}\widetilde{f}(\alpha)(-1)^{\langle\alpha\,|\,x\rangle}.$$

Hint: Consider $\sum_{\alpha\in\check{\mathbb{F}}_2^j}(-1)^{\langle\alpha\,|\,x\rangle}(-1)^{\langle\alpha\,|\,\xi\rangle}$ in case $x=\xi$ and in case $x\neq\xi$.

(ii) For two functions $f_1, f_2\colon \mathbb{F}_2^j \to \mathbb{F}_2$ prove that [2]

$$\mathrm{corr}(f_1-f_2) = \frac{\left\langle (-1)^{f_1}\,\middle|\,(-1)^{f_2}\right\rangle}{\|(-1)^{f_1}\|\cdot\|(-1)^{f_2}\|}.$$

Hint: $\left\|(-1)^{f_1}\right\| = \sqrt{\left\langle (-1)^{f_1}\,\middle|\,(-1)^{f_1}\right\rangle} = 2^{\frac{j}{2}}$.

In other words: the correlation is the cosine of the angle between the two real (or complex) vectors $(-1)^{f_1}$ and $(-1)^{f_2}$.

In again other words: $\mathrm{corr}(f) = \frac{1}{2^j}\sum_{x\in\mathbb{F}_2^j}(-1)^{f(x)}$.

Thus $\mathrm{corr}(f) = \widetilde{f}(0)$.

(iii) Prove $\left\|\widetilde{f}\right\|^2 = 1$ (Parseval's identity). [2]

Hint: Just plug in the definition of $\widetilde{f}$.

2 (iv) For two functions $f_1, f_2 \colon \mathbb{F}_2^j \to \mathbb{F}_2$ and their XOR $f = f_1 + f_2$ prove that

$$\widetilde{f}(a) = \sum_{a_1+a_2=a} \widetilde{f}_1(a_1)\widetilde{f}_2(a_2).$$

Hint: Rewrite $(-1)^{f_1(a_1)} \cdot (-1)^{f_2(a)}$ using the equation in (i) and notice that $\widetilde{f}$ is determined by that very equation.

1 (v) Check that for $c_1, c_2 \in \{1, -1\}$ we have

$$\begin{aligned} c_1 c_2 &= 1 - 2 \cdot \frac{1-c_1}{2} \cdot \frac{1-c_2}{2} \\ &= \frac{1}{2}\left(1 + c_1 + c_2 - c_1 c_2\right). \end{aligned}$$

2 (vi) For two functions $f_1, f_2 \colon \mathbb{F}_2^j \to \mathbb{F}_2$ and their AND $f = f_1 \cdot f_2$ prove that

$$\widetilde{f}(a) = \frac{1}{2}\left(\delta(a) + \widetilde{f}_1(a) + \widetilde{f}_2(a) + \widetilde{f_1 + f_2}(a)\right).$$

Here, $\delta(0) = 1$ and $\delta(a) = 0$ for $a \neq 0$.

For a function $g \colon \mathbb{F}_2^k \to \mathbb{F}_2^\ell$ and $a \in \check{\mathbb{F}}_2^k$, $b \in \check{\mathbb{F}}_2^\ell$ we consider $f_{a,b} \colon \mathbb{F}_2^k \to \mathbb{F}_2$ with $f_{a,b}(x) = \langle a \,|\, x \rangle + \langle b \,|\, g(x) \rangle$. Define the correlation matrix $C(g) := [\mathrm{corr}(f_{a,b})]_{a,b}$ as the matrix of correlations when a, b run over all values.

+2 (vii) Prove that

$$(-1)^{\langle b \,|\, g(x) \rangle} = \sum_a C(h)_{a,b} \cdot (-1)^{\langle a \,|\, x \rangle}.$$

Hint: Use (i).

This is a reinterpretation of the correlation matrix.

+3 (viii) Consider such a function g and a function $h \colon \mathbb{F}_2^\ell \to \mathbb{F}_2^n$. Then

$$C(h \circ g) = C(h) \cdot C(g).$$