2 The Walsh Transformation

For the moment we consider *real valued* functions $\varphi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$. These make up the $\mathbb{R}$-algebra $\mathcal{C}_n = \mathbb{R}^{\mathbb{F}_2^n}$.

2.1 Definition of the Walsh transformation

Definition 1 The **Walsh Transformation** (or Hadamard-Walsh-Transformation)

$$\Phi : \mathcal{C}_n \longrightarrow \mathcal{C}_n, \qquad \varphi \mapsto \hat{\varphi},$$

is defined by the formula

$$\hat{\varphi}(u) := \sum_{x \in \mathbb{F}_2^n} \varphi(x) \cdot (-1)^{u \cdot x}$$

(where $u \cdot x$ is the canonical dot product in $\mathbb{F}_2^n$).

Remarks

1. Obviously Φ is a $\mathbb{R}$-linear map.
2. Φ is a special case of the discrete Fourier transformation. In the general case, instead of -1 in the formula one takes the complex N-th root of unity $\zeta = e^{2\pi i/N}$, and transforms complex valued functions over the ring $\mathbb{Z}/N\mathbb{Z}$—or functions on $\mathbb{Z}^n$, that have period N in each variable. [Character sums are a further generalization.]
3. Clearly $\hat{0} = 0$ for the constant function $0 \in \mathcal{C}_n$. The other constant function 1 tranforms to $\hat{1}$ = the "point mass" in 0:

$$\begin{aligned} \hat{1}(0) &= 2^n, \\ \hat{1}(u) &= 0 \quad \text{else.} \end{aligned}$$

This follows from the next lemma:

Lemma 1 *For $u \in \mathbb{F}_2^n$ we have*

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} = \begin{cases} 2^n, & \text{if } u = 0, \\ 0 & \text{else.} \end{cases}$$

Proof. If $u = 0$, then all exponents are 0, all summands 1, and we have 2^n of them.

For $u \neq 0$ let H be the hyperplane $\{x \in \mathbb{F}_2^n \mid x \cdot u = 0\}$. Then $\bar{H} = \{x \in \mathbb{F}_2^n \mid x \cdot u = 1\}$ is its complement, hence $\mathbb{F}_2^n = H \bigcup \bar{H}$, $H \bigcap \bar{H} = \emptyset$, and $\#H = \#\bar{H} = 2^{n-1}$. For $x \in H$ the summand is 1, for $x \in \bar{H}$ it's -1. Therefore the sum is 0. $\diamond$

Definition 2 For a Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ the transformed function $\hat{\chi_f} : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ of the character form χ_f is called the **(Walsh) spectrum** of f.

We have

$$\begin{aligned}\hat{\chi}_f(u) &= \sum_{x\in\mathbb{F}_2^n} \underbrace{(-1)^{f(x)+u\cdot x}}_{\begin{cases}1, & \text{if } f(x)=u\cdot x,\\ -1, & \text{if } f(x)\neq u\cdot x,\end{cases}} \\ &= \#\{x \mid f(x)=u\cdot x\} - \#\{x \mid f(x)\neq u\cdot x\}.\end{aligned}$$

If we denote the first of these sets by

$$L_f(u) := \{x \mid f(x) = u \cdot x\}$$

then we have shown:

Corollary 1 *The spectrum of a Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ equals*

$$\hat{\chi}_f(u) = 2 \cdot \#L_f(u) - 2^n.$$

In particular $\hat{\chi}_f(u)$ is always even, and

$$-2^n \leq \hat{\chi}_f(u) \leq 2^n.$$

The lower bound is taken for $f(x) = u \cdot x + 1$, the upper one for $f(x) = u \cdot x$. In general the spectrum reflects the coincidence or deviation between a Boolean function and all linear and affine functions.

Corollary 2 *Let α be the linear form $\alpha(x) = u \cdot x$ corresponding to u. Then*

$$d(f, \alpha) = 2^n - \#L_f(u) = 2^{n-1} - \frac{1}{2}\,\hat{\chi}_f(u).$$

Remarks

4. $\hat{\chi}_{f+1} = -\hat{\chi}_f$ for all f.

Exercise 1 How does the spectrum change under an affine transformation of the argument space?

Exercise 2 Calculate the spectrum of an affine function and of the function $f(x_1, x_2) = x_1x_2$ of two variables.

2.2 The inversion formula

Let's apply the Walsh transformation Φ again to an already transformed function $\hat{\varphi}$:

$$\begin{aligned}
\hat{\hat{\varphi}}(w) &= \sum_{u\in\mathbb{F}_2^n} \hat{\varphi}(u)\cdot(-1)^{u\cdot w} \\
&= \sum_{u\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n} \varphi(x)\cdot(-1)^{u\cdot x}\cdot(-1)^{u\cdot w} \\
&= \sum_{x\in\mathbb{F}_2^n} \varphi(x) \underbrace{\left[\sum_{u\in\mathbb{F}_2^n}(-1)^{u\cdot(x+w)}\right]}_{=\begin{cases}2^n, & \text{if } x+w=0,\\ 0 & \text{else,}\end{cases}} \\
&= 2^n\varphi(w).
\end{aligned}$$

We have shown, that $\Phi\circ\Phi(\varphi) = 2^n\varphi$ for all $\varphi\in\mathcal{C}_n$:

Proposition 1 *The Walsh transformation $\Phi:\mathcal{C}_n\longrightarrow\mathcal{C}_n$ is bijective, and it's inverse transformation is given by*

$$\Phi^{-1} = \frac{1}{2^n}\Phi.$$

Corollary 1

$$\varphi(0) = \frac{1}{2^n}\sum_{u\in\mathbb{F}_2^n}\hat{\varphi}(u).$$

Corollary 2 *For every Boolean function $f:\mathbb{F}_2^n\longrightarrow\mathbb{F}_2$ we have*

$$\sum_{u\in\mathbb{F}_2^n}\hat{\chi}_f(u) = \begin{cases}2^n, & \text{if } f(0)=0,\\ -2^n & \text{else.}\end{cases}$$

2.3 The convolution

Definition 3 For $\varphi,\psi:\mathbb{F}_2^n\longrightarrow\mathbb{R}$ the **convolution** $\varphi*\psi:\mathbb{F}_2^n\longrightarrow\mathbb{R}$ is defined by

$$\varphi*\psi(w) := \sum_{x\in\mathbb{F}_2^n}\varphi(x)\psi(w-x).$$

This gives a bilinear map $*:\mathcal{C}_n\times\mathcal{C}_n\longrightarrow\mathcal{C}_n$.

Let's calculate the value at 0 for the convolution of the character forms of two Boolean functions $f, g\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$:

$$\begin{aligned}\chi_f * \chi_g(0) &= \sum_{x\in\mathbb{F}_2^n} \chi_f(x)\chi_g(x)\\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+g(x)}\\ &= 2^n - 2\cdot d(f,g),\end{aligned}$$

because

$$(-1)^{f(x)+g(x)} = \begin{cases}1, & \text{if } f(x)=g(x),\\ -1 & \text{else.}\end{cases}$$

Therefore $d(f,g)$ summands are $=-1$, and $2^n - d(f,g)$ summands are $=1$. We have shown the following generalization of corollary 2 in 2.1:

Proposition 2 *The Hamming distance of two Boolean functions f, g on $\mathbb{F}_2^n$ is*

$$d(f,g) = 2^{n-1} - \frac{1}{2}\,\chi_f * \chi_g(0).$$

Another way to express this result is in terms of the **correlation**,

$$\begin{aligned}\kappa(f,g) &:= \frac{1}{2^n}\left[\#\{x \mid f(x)=g(x)\} - \#\{x \mid f(x)\neq g(x)\}\right]\\ &= \frac{1}{2^{n-1}}\left[\#\{x \mid f(x)=g(x)\}\right] - 1.\end{aligned}$$

Corollary 1 *The correlation of the functions f and g is*

$$\kappa(f,g) = \frac{1}{2^n}\cdot \chi_f * \chi_g(0).$$

Exercise Show: The correlation κ is a scalar product on the real function space $\mathcal{C}_n$. The set $\{\chi_f \mid f \in \mathcal{L}_n\}$ of the character forms of the linear forms on $\mathbb{F}_2^n$ is an orthonormal basis of $\mathcal{C}_n$. The Walsh transformation of a function $f \in \mathcal{C}_n$ is its representation in this basis.

Definition 4 The **autocorrelation** of a Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ with respect to the shift $x \in \mathbb{F}_2^n$ is

$$\kappa_f(x) := \frac{1}{2^n}\left[\#\{u \in \mathbb{F}_2^n \mid f(u+x)=f(u)\} - \#\{u \in \mathbb{F}_2^n \mid f(u+x)\neq f(u)\}\right].$$

Therefore we have

$$\kappa_f(x) = \frac{1}{2^n}\cdot \sum_{u\in\mathbb{F}_2^n} (-1)^{f(u+x)+f(u)} = \frac{1}{2^n}\cdot \sum_{u\in\mathbb{F}_2^n} \chi_f(u+x)\chi_f(u),$$

hence

Lemma 2 *The autocorrelation of f is*

$$\kappa_f = \frac{1}{2^n} \cdot \chi_f * \chi_f.$$

Let's calculate the Walsh transform of a convolution:

$$\begin{aligned}
\widehat{\varphi * \psi}(u) &= \sum_{w \in \mathbb{F}_2^n} (\varphi * \psi)(w)(-1)^{u \cdot w} \\
&= \sum_{w \in \mathbb{F}_2^n} \sum_{x \in \mathbb{F}_2^n} \varphi(x)\psi(w+x)(-1)^{u \cdot w} \\
&= \sum_{x \in \mathbb{F}_2^n} \varphi(x) \left[\sum_{w \in \mathbb{F}_2^n} \psi(w+x)(-1)^{u \cdot w} \right] \\
&= \sum_{x \in \mathbb{F}_2^n} \varphi(x) \sum_{v \in \mathbb{F}_2^n} \psi(v)(-1)^{u \cdot (v+x)} \\
&= \sum_{x \in \mathbb{F}_2^n} \varphi(x) \left[\sum_{v \in \mathbb{F}_2^n} \psi(v)(-1)^{u \cdot v} \right] (-1)^{u \cdot x} \\
&= \left[\sum_{x \in \mathbb{F}_2^n} \varphi(x)(-1)^{u \cdot x} \right] \hat{\psi}(u) \\
&= \hat{\varphi}(u)\hat{\psi}(u).
\end{aligned}$$

Proposition 3 (Convolution theorem) *For $\varphi, \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ we have $\widehat{\varphi * \psi} = \hat{\varphi}\hat{\psi}$.*

Corollary 2 *$\mathcal{C}_n$, with $*$ as multiplication is a $\mathbb{R}$-algebra $\mathcal{C}_n^*$; in particular $*$ is commutative and associative, and $\Phi : \mathcal{C}_n \longrightarrow \mathcal{C}_n^*$ is a homomorphism of $\mathbb{R}$-algebras.*

Since $\Phi^{-1} = \frac{1}{2^n}\,\Phi$, up to the factor 2^n also Φ is a homomorphism $\mathcal{C}_n^* \longrightarrow \mathcal{C}_n$, in other words:

Corollary 3 *For $\varphi, \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ we have $\widehat{\varphi\psi} = \frac{1}{2^n} \cdot \hat{\varphi} * \hat{\psi}$.*

Corollary 4 *For $f, g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ we have*

$$\begin{aligned}
\widehat{\chi_{f+g}} &= \widehat{\chi_f \chi_g} = \frac{1}{2^n}\hat{\chi}_f * \hat{\chi}_g, \\
2\widehat{\chi_{fg}} &= \Phi(1 + \chi_f + \chi_g - \chi_f\chi_g) = \hat{1} + \hat{\chi}_f + \hat{\chi}_g - \frac{1}{2^n}\hat{\chi}_f * \hat{\chi}_g.
\end{aligned}$$

Corollary 5 *The Walsh transform of the autocorrelation κ_f is given by $\hat{\kappa}_f = \frac{1}{2^n}\hat{\chi}_f^2$.*

There are two ways to calculate the value of a convolution product at 0; first:

$$\varphi * \psi(0) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)\psi(x).$$

Secondly, by the corollary 1 of the inversion formula (proposition 1):

$$\varphi * \psi(0) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \widehat{\varphi * \psi}(u) = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \hat{\varphi}(u)\hat{\psi}(u).$$

We have shown:

Proposition 4 (Parseval's equation) *For $\varphi, \psi \colon \mathbb{F}_2^n \longrightarrow \mathbb{R}$*

$$\sum_{u \in \mathbb{F}_2^n} \hat{\varphi}(u)\hat{\psi}(u) = 2^n \sum_{x \in \mathbb{F}_2^n} \varphi(x)\psi(x).$$

2.4 Bent functions

Parseval's equation, applied to the character form of a Boolean function $f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ yields:

$$\sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^2 = 2^n \cdot \sum_{x \in \mathbb{F}_2^n} \chi_f(x)^2 = 2^{2n},$$

because in the last sum all summands are $= 1$. Therefore in the first sum there must be at least one of the 2^n summands $\hat{\chi}_f(u)^2 \geq 2^n$. Hence:

Proposition 5 *For every Boolean function $f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ we have*

$$max|\hat{\chi}_f| \geq 2^{n/2},$$

with equality, if and only if $\hat{\chi}_f^2 = 2^n$ constant.

These functions are well-known in combinatorics since many years:

Definition 5 (Rothaus, ca 1965, published in 1976) A Boolean function $f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ is called bent, if $(\hat{\chi}_f)^2 = 2^n$ constant.

In particular the spektrum $\hat{\chi}_f$ of a bent function can only assume the values $\pm 2^{n/2}$; these must be integers:

$$\hat{\chi}_f(u) = \sum_{x \in \mathbb{F}_2^n} \chi_f(x)(-1)^{u \cdot x} \in \mathbb{Z}.$$

Corollary 1 *If a bent function $f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ exists, then n must be even.*

Remarks

1. The correlation of a Boolean function f with the linear form α that corresponds to $u \in \mathbb{F}_2^n$ is

$$\kappa(f, \alpha) = \frac{1}{2^n} \cdot \hat{\chi}_f(u).$$

While constructing stream ciphers (or pseudorandom generators) by combining linear shift registers one tries to avoid correlations with linear functions. But because the sum of squares over all such correlations is constant = 1, the correlation 0 is possible only, if there are higher correlations with other linear forms. It's better to minimize all these correlationen in a uniform way, that means to minimize $\max |\hat{\chi}_f|$. That's what bent functions fulfil.

Exercise 1 Find a bent function of 2 or 4 variables.

Exercise 2 Show that for every bent function f there is a bent function g such that $\hat{\chi}_f = 2^{n/2}\chi_g$. (Duality of bent functions.)

Exercise 3 Let $n = 2m$ be even. Let $\pi : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ be bijective, and $g : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ be any Boolean function. Let $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ be defined by $f(x, y) = \pi(x) \cdot y + g(x)$. Show that f is bent. (Maiorana-McFarland construction.)

2.5 An algorithm for the Walsh transformation

Let $\varphi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ be a function. We assume that φ is given by it's value table—that is, all the values $\varphi(x)$ are known. We want to calculate the value table of the transformed function $\hat{\varphi}$. To this end we construct an algorithm via binary recursion that strongly resembles the algorithm in section 1.4. We start from the observation: For $v \in \mathbb{F}_2^j$, $w \in \mathbb{F}_2^{n-j}$ and $0 \leq j \leq n$

$$\hat{\varphi}(v, w) = \sum_{y \in \mathbb{F}_2^j} (-1)^{v \cdot y} \left[\sum_{z \in \mathbb{F}_2^{n-j}} (-1)^{w \cdot z} \varphi(y, z) \right].$$

We define

$$\varphi^{(j)}(y, w) := \sum_{z \in \mathbb{F}_2^{n-j}} (-1)^{w \cdot z} \varphi(y, z) \quad \text{for } y \in \mathbb{F}_2^j \text{ and } w \in \mathbb{F}_2^{n-j}$$

(**partial Walsh transformation**). Then

$$\begin{aligned} \varphi^{(0)}(w) &= \hat{\varphi}(w) \quad \text{for } w \in \mathbb{F}_2^n, \\ \varphi^{(n)}(y) &= \varphi(y) \quad \text{for } y \in \mathbb{F}_2^n, \end{aligned}$$

and we have:

Lemma 3 *For all $v \in \mathbb{F}_2^j$ and $w \in \mathbb{F}_2^{n-j}$*

$$\hat{\varphi}(v,w) = \sum_{y \in \mathbb{F}_2^j} (-1)^{v \cdot y} \varphi^{(j)}(y,w).$$

This gives a recursion: For $y \in \mathbb{F}_2^{j-1}$, $\eta \in \mathbb{F}_2$, $w \in \mathbb{F}_2^{n-j}$

$$\varphi^{(j-1)}(y,\eta,w) = \sum_{\zeta \in \mathbb{F}_2} \sum_{z \in \mathbb{F}_2^{(n-j)}} (-1)^{\eta\zeta + w \cdot z} \varphi(y,\zeta,z) = \sum_{\zeta \in \mathbb{F}_2} (-1)^{\eta\zeta} \varphi^{(j)}(y,\zeta,w).$$

Therefore:

Proposition 6 (Recursion for the partial Walsh transformation) *For $y \in \mathbb{F}_2^{j-1}$ and $w \in \mathbb{F}_2^{n-j}$*

$$\begin{aligned} \varphi^{(j-1)}(y,0,w) &= \varphi^{(j)}(y,0,w) + \varphi^{(j)}(y,1,w), \\ \varphi^{(j-1)}(y,1,w) &= \varphi^{(j)}(y,0,w) - \varphi^{(j)}(y,1,w). \end{aligned}$$

In order to get an iterative procedure for the Walsh transformation from this formula, we take $i := n - j$. The initial vector $x^{(0)} = (x_u)_{u \in \mathbb{F}_2^n}$ consists of the value table $x_u = \varphi(u)$ of φ. Via the intermediate vectors $x^{(i)}$, $i = 1, \ldots, n-1$, we get the final reasult $x^{(n)}$, the value table of the Walsh transform $\hat{\varphi}$. For the step from $x^{(i)}$ to $x^{(i+1)}$ we decompose the n-bit index as $u\xi v$ with $n-i-1$ bits u, 1 bit ξ, and i bits v; then by proposition 6 we have:

$$\begin{aligned} x^{(i+1)}_{u0v} &= x^{(i)}_{u0v} + x^{(i)}_{u1v} \\ x^{(i+1)}_{u1v} &= x^{(i)}_{u0v} - x^{(i)}_{u1v} \end{aligned}$$

To implement this procedure in a common programming language, as before we interpret the indices as natural numbers $k = \sum k_{n-i} 2^i$ in the integer interval $[0 \ldots 2^n - 1]$ as in table 1. Then in the above equations we have $u1v = u0v + 2^i$ and in analogy with 1.4 get the formula for the iteration:

$$x_k^{(i+1)} = \begin{cases} x_k^{(i)} + x_{k+2^i}^{(i)}, & \text{if } k_{n-i} = 0, \\ x_{k-2^i}^{(i)} - x_k^{(i)}, & \text{if } k_{n-i} = 1, \end{cases}$$

for $k = 0, \ldots, 2^n - 1$. The entire algorithm reads as follows:

Procedure [WT]

Input and output parameters: A vector x of length 2^n, $x[0], \ldots, x[2^n - 1]$.

Local variables: A vector y of length 2^n, $y[0], \ldots, y[2^n - 1]$. Loop counters $i = 0, \ldots, n-1$, and $k = 0, \ldots, 2^n - 1$.

Instructions:

For $i = 0, \ldots, n-1$:
  For $k = 0, \ldots, 2^n - 1$:
    If $(((k \gg i) \bmod 2) = 1)$ then $y[k] := x[k - 2^i] - x[k]$
      else $y[k] := x[k] + x[k + 2^i]$
  For $k = 0, \ldots, 2^n - 1$:
    $x[k] := y[k]$

Of course this procedure makes sense only with exact arithmetic, say with integer vectors. One has to take care of errors by overflow.

Note that, if φ takes values only in a subring of $\mathbb{R}$ (say $\mathbb{Z}$ or $\mathbb{Q}$), then the entire procedure works in this subring.

The expense as function of the input size $N = 2^n$ is—as in 1.4—almost linear: $3N \cdot {}^2\log N$ (as usual for the fast Fourier transform). We need roughly $2N$ memory cells for elements of the base ring (with exact arithmetic).

The corresponding C procedure in the sources is called `wt`.

2.6 An algorithm for the convolution

The naive application of definition 2 requires 2^{2n} products of (complex or integer, depending on the context) numbers: multiply each value of φ with each value of ψ. The expense is quadratic in the input size $N = 2^n$.

Using the convolution theorem we reduce the expense to $N \log N$: Let's denote the intermediate result by $g := \widehat{\varphi * \psi} = \hat{\varphi}\hat{\psi}$. Then $\hat{g} = 2^n \varphi\psi$. Therefore we may use the following algorithm:

1. a) Calculate $\hat{\varphi}$,
   b) Calculate $\hat{\psi}$,
2. Multiply $g = \hat{\varphi}\hat{\psi}$ (for each argument),
3. Transform back $\varphi * \psi = \frac{1}{2^n}\hat{g}$.

The effort essentially consists of 3 Walsh transformations, each with $3n \cdot 2^n$ elementary operations; plus additionally 2^n multiplications in step 2. Togehter we asymptotically need some $9N \cdot {}^2\log N$ elementary operations. For this we essentially need $3N$ memory units.

Note. An analoguous procedure performs the efficient multiplication of polynomials via the fast Fourier transformation.