2 Die WALSH-Transformation

Gegenstand der Betrachtung sind jetzt zunächst *reellwertige* Funktionen $\varphi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$. Diese Funktionen bilden die $\mathbb{R}$-Algebra $\mathcal{C}_n = \mathbb{R}^{\mathbb{F}_2^n}$.

2.1 Definition der WALSH-Transformation

Die folgende Konstruktion ist trotz ihrer Einfachheit das Zaubermittel, das die Theorie der BOOLEschen Funktionen und Abbildungen einfach und elegant macht.

Definition 1 Die **WALSH-Transformation** (oder HADAMARD-WALSH-Transformation)

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

ist definiert durch

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

Dabei ist $u \cdot x$ das kanonische Skalarprodukt in $\mathbb{F}_2^n$.

Bemerkungen

1. Es ist unmittelbar ersichtlich, dass Φ eine $\mathbb{R}$-lineare Abbildung ist.

2. Φ ist ein Spezialfall der diskreten FOURIER-Transformation. Im allgemeinen Fall würde man statt -1 die komplexe N-te Einheitswurzel $\zeta = e^{2\pi i/N}$ verwenden und komplexwertige Funktionen über dem Ring $\mathbb{Z}/N\mathbb{Z}$ transformieren – oder Funktionen auf $\mathbb{Z}^n$, die in jeder Variablen die Periode N haben. [Eine weitere Verallgemeinerung sind Charakter-Summen.]

3. Klar ist $\hat{0} = 0$ für die konstante Funktion $0 \in \mathcal{C}_n$. Für die konstante Funktion 1 ist $\hat{1}$ die „Punktmasse“ in 0:

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

Das ergibt sich aus dem folgenden Hilfssatz:

Hilfssatz 1 *Für $u \in \mathbb{F}_2^n$ gilt*

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

Beweis. Falls $u = 0$, sind alle Exponenten 0, alle Summanden 1, und davon gibt es 2^n Stück.

Falls $u \neq 0$, sei H die Hyperebene $\{x \in \mathbb{F}_2^n \mid x \cdot u = 0\}$. Dann ist $\bar{H} = \{x \in \mathbb{F}_2^n \mid x \cdot u = 1\}$ das Komplement, also $\mathbb{F}_2^n = H \bigcup \bar{H}$, $H \bigcap \bar{H} = \emptyset$, und $\#H = \#\bar{H} = 2^{n-1}$. Für $x \in H$ ist der Summand 1, für $x \in \bar{H}$ jeweils -1. Also ist die Summe 0. $\diamond$

Definition 2 Für eine BOOLEsche Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ heißt die transformierte Funktion $\hat{\chi_f} : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ der Charakter-Form χ_f das (WALSH-) **Spektrum** von f. Die Größe $\max |\hat{\chi_f}|$ heißt **Spektralradius** von f (DOBBERTIN FSE 94).

Es ist

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

Bezeichnet man die erste dieser Mengen mit

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

so ist gezeigt:

Korollar 1 *Für eine* BOOLE*sche Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist das Spektrum gleich*

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

Insbesondere ist $\hat{\chi}_f(u)$ stets gerade und

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

Dabei wird die untere Grenze für $f(x) = u \cdot x + 1$, die obere für $f(x) = u \cdot x$ angenommen. Das Spektrum „misst“ also die Übereinstimmung bzw. Abweichung zwischen einer BOOLEschen Funktion und allen linearen und affinen Funktionen.

Korollar 2 *Ist α die Linearform $\alpha(x) = u \cdot x$, so ist*

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

Speziell ist

$$\hat{\chi}_f(0) = 2^n - 2 \cdot d(f, 0) = 2^n - 2 \cdot \mathrm{wt}(f).$$

Bemerkungen

4. $\hat{\chi}_{f+1} = -\hat{\chi}_f$ für alle f.

5. Allgemeiner sei g eine affine Funktion, $g(x) = v \cdot x + c$. Dann ist

$$\hat{\chi}_{f+g}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+v\cdot x+c+u\cdot x} = (-1)^c \cdot \hat{\chi}_f(u+v).$$

   Die Addition einer affinen Funktion bewirkt also bis aufs Vorzeichen eine Permutation des Spektrums.

6. Ist $g \in GL_n(\mathbb{F}_2)$, so ist

$$\begin{aligned} \hat{\chi}_{f\circ g}(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(g(x))+u\cdot x} = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+u\cdot g^{-1}(y)} \\ &= \hat{\chi}_f(g^*(u)) \end{aligned}$$

   für alle $u \in \mathbb{F}_2^n$. Insbesondere permutiert g das Spektrum von f.

7. Ist $g(x) = f(x+z)$ mit fester Verschiebung z, so ist

$$\begin{aligned} \hat{\chi}_g(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x+z)+u\cdot x} = (-1)^{u\cdot z} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)+u\cdot y} \\ &= (-1)^{u\cdot z} \hat{\chi}_f(u); \end{aligned}$$

   Bei Translation im Argumentraum ändern sich die Werte des Spektrums also höchstens um das Vorzeichen.

Beispiele

1. Da $\chi_0 = 1$ konstant, ist

$$\hat{\chi}_0(u) = \begin{cases} 2^n & \text{für } u = 0, \\ 0 & \text{sonst.} \end{cases}$$

2. Sei f affin, also $f(x) = t \cdot x + b$ mit $t \in \mathbb{F}_2^n$ und $b = 0$ oder 1. Dann ist

$$L_f(u) = \{x \in \mathbb{F}_2^n \mid t \cdot x + b = u \cdot x\} = \{x \in \mathbb{F}_2^n \mid (u-t) \cdot x = b\},$$

   und das ist im Fall $u - t \neq 0$ der 1-codimensionale Unterraum $\{u-t\}^\perp$, falls $b = 0$, und die dazu parallele Hyperebene, falls $b = 1$. Insgesamt gibt es also drei Fälle:

$$\#L_f(u) = \begin{cases} 2^n, & \text{falls } u = t,\ b = 0, \\ 0, & \text{falls } u = t,\ b = 1, \\ 2^{n-1}, & \text{falls } u \neq t. \end{cases}$$

Daher ist

$$\hat{\chi}_f(u) = \begin{cases} (-1)^b 2^n, & \text{falls } u = t, \\ 0, & \text{falls } u \neq t. \end{cases}$$

3. Sei $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$ gegeben durch das Polynom T_1T_2, also $f(x_1, x_2) = x_1x_2$. Die Wertetabelle von f und den vier Linearformen sieht dann so aus:

		$u =$			
x	$f(x)$	00	01	10	11
00	0	0	0	0	0
01	0	0	1	0	1
10	0	0	0	1	1
11	1	0	1	1	0

Daraus ergibt sich die Wertetafel

u	00	01	10	11
$\#L_f(u)$	3	3	3	1
$\hat{\chi}_f(u)$	2	2	2	-2

Insbesondere ist $\hat{\chi}_f = 2 \cdot \chi_f$, also 2 Eigenwert und χ_f Eigenvektor der WALSH-Transformation.

4. Für die anisotrope quadratische Form $f = T_1T_2 + T_1 + T_2$ berechnet man genauso die Tabelle

u	00	01	10	11
$\#L_f(u)$	1	3	3	3
$\hat{\chi}_f(u)$	-2	2	2	2

Also ist $\hat{\chi}_f = -2 \cdot \chi_f$, also -2 Eigenwert und χ_f Eigenvektor der WALSH-Transformation.

Übungsaufgabe 1. Sei $V \leq \mathbb{F}_2^n$ ein Untervektorraum der Dimension r und $b \in \mathbb{F}_2^n$. Zeige:

$$\sum_{x \in b+V} (-1)^{u \cdot x} = \begin{cases} 2^r \cdot (-1)^{u \cdot b}, & \text{falls } u \in V^\perp, \\ 0 & \text{sonst.} \end{cases}$$

Übungsaufgabe 2. Sei $V \leq \mathbb{F}_2^n$ ein Untervektorraum der Dimension r und $\varphi \colon \mathbb{F}_2^n \longrightarrow \mathbb{R}$. Zeige:

$$\sum_{v \in V} \hat{\varphi}(v) = 2^r \cdot \sum_{u \in V^\perp} \varphi(u).$$

2.2 Die Umkehrformel

Was passiert, wenn man auf eine WALSH-Transformierte $\hat{\varphi}$ noch einmal Φ anwendet? Das ist leicht zu berechnen:

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

Damit ist gezeigt, dass $\Phi\circ\Phi(\varphi) = 2^n\varphi$ für alle $\varphi\in\mathcal{C}_n$, also:

Satz 1 (Umkehrformel) *Die* WALSH-*Transformation* $\Phi : \mathcal{C}_n \longrightarrow \mathcal{C}_n$ *ist bijektiv, und ihre Umkehrung ist gegeben durch*

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

Korollar 1

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

Korollar 2 *Für eine* BOOLE*sche Funktion* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *gilt*

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

2.3 Die Faltung

Definition 3 Für $\varphi,\psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ ist die **Faltung** $\varphi * \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ definiert durch

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

Dadurch wird eine bilineare Abbildung $* : \mathcal{C}_n \times \mathcal{C}_n \longrightarrow \mathcal{C}_n$ beschrieben.

Anwendung Berechnen wir für die Charakter-Formen zweier BOOLEscher Funktionen $f, g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ den Wert der Faltung in 0:

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

denn

$$(-1)^{f(x)+g(x)} = \begin{cases} 1, & \text{falls } f(x) = g(x), \\ -1 & \text{sonst;} \end{cases}$$

also sind $d(f,g)$ Summanden $= -1$ und $2^n - d(f,g)$ Summanden $= 1$.

Damit ist folgende Verallgemeinerung von Korollar 2 in 2.1 gezeigt:

Satz 2 *Die* HAMMING*-Distanz zweier* BOOLE*scher Funktionen* $f, g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *ist*

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

Man kann dieses Ergebnis auch durch die **Korrelation**

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

der Funktionen f und g ausdrücken:

Korollar 1 *Die Korrelation der Funktionen* f *und* g *ist*

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

Übungsaufgabe Die Korrelation κ ist ein Skalarprodukt auf dem rellen Funktionenraum $\mathcal{C}_n$. Die Menge $\{\chi_f \mid f \in \mathcal{L}_n\}$ der Charakterformen von Linearformen auf $\mathbb{F}_2^n$ bildet eine Orthonormalbasis von $\mathcal{C}_n$. Die WALSH-Transformation einer Funktion $f \in \mathcal{C}_n$ ist gerade die Basis-Darstellung.

Definition 4 Die **Autokorrelation** einer BOOLEschen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ bezüglich der Verschiebung $x \in \mathbb{F}_2^n$ ist

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

Es folgt

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

also

Hilfssatz 2 *Die Autokorrelation von f ist*

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

Bestimmen wir nun die WALSH-Transformation einer Faltung:

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

Satz 3 (Faltungssatz) *Für $\varphi, \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ ist $\widehat{\varphi * \psi} = \hat{\varphi}\hat{\psi}$.*

Korollar 1 *$\mathcal{C}_n$ ist mit der Multiplikation $*$ eine $\mathbb{R}$-Algebra $\mathcal{C}_n^*$; insbesondere ist $*$ kommutativ und assoziativ, und $\Phi : \mathcal{C}_n \longrightarrow \mathcal{C}_n^*$ ist ein Homomorphismus der $\mathbb{R}$-Algebren.*

Da $\Phi^{-1} = \frac{1}{2^n}\Phi$, ist Φ bis auf den Faktor 2^n auch Homomorphismus $\mathcal{C}_n^* \longrightarrow \mathcal{C}_n$, d. h.:

Korollar 2 *Für $\varphi, \psi \colon \mathbb{F}_2^n \longrightarrow \mathbb{R}$ ist $\widehat{\varphi\psi} = \frac{1}{2^n} \cdot \hat{\varphi} * \hat{\psi}$.*

Korollar 3 *Für $f, g \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gilt*

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

Korollar 4 *Für die Autokorrelation κ_f gilt $\hat{\kappa}_f = \frac{1}{2^n}\hat{\chi}_f^2$.*

Den Wert einer Faltung an der Stelle 0 kann man auf zwei verschiedene Arten berechnen; erstens:

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

Andererseits nach dem Korollar 1 zur Umkehrformel (Satz 1):

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

Damit ist gezeigt:

Satz 4 (PARSEVAL-Gleichung) *Für $\varphi, \psi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ gilt*

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

2.4 Krumme Funktionen

Wendet man die PARSEVAL-Gleichung auf die Charakter-Form einer BOOLEschen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ an, so folgt:

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

da in der letzten Summe alle Summanden = 1 sind. Insbesondere muss in der ersten Summe mindestens einer der 2^n Summanden $\hat{\chi}_f(u)^2 \geq 2^n$ sein. Es folgt:

Satz 5 *Für eine BOOLEsche Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist der Spektralradius*

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

und die Gleichheit gilt genau dann, wenn $\hat{\chi}_f^2 = 2^n$ konstant ist.

Solche Funktionen sind in der Kombinatorik schon lange bekannt:

Definition 5 (ROTHAUS, ca. 1965, veröffenticht 1976) Eine BOOLEsche Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ heißt **krumm** (Bent-Funktion), wenn $(\hat{\chi}_f)^2 = 2^n$ konstant ist, d. h., wenn der Spektralradius den minimal möglichen Wert $2^{n/2}$ hat.

Insbesondere kann das Spektrum $\hat{\chi}_f$ für eine krumme Funktion f nur die Werte $\pm 2^{n/2}$ annehmen; diese müssen aber ganzzahlig sein:

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

Korollar 1 *Wenn eine krumme Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ existiert, muss n gerade sein.*

Beispiele

1. Ist f affin, so $\max|\hat{\chi}_f| = 2^n$, also f sicher nicht krumm.
2. Für $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, ist $(\hat{\chi}_f)^2 = 4$ konstant, diese Funktion ist also krumm.

Bemerkungen

1. Die Größen $\max|\hat{\chi}_f|$ – der Spektralradius – und $\max \hat{\chi}_f^2$ sowie die Eigenschaft „krumm“ sind unter affinen Transformationen, also unter der gesamten affinen Transformationsgruppe $GA(\mathbb{F}_2^n) \times GA(\mathbb{F}_2)$ invariant. Insbesondere ist f genau dann krumm, wenn das Komplement $f + 1$ krumm ist.
2. Ist f krumm und g affin, so ist $f + g$ krumm. Der Spektralradius ist nämlich der gleiche.
3. Die Korrelation einer BOOLEschen Funktion f mit der durch $u \in \mathbb{F}_2^n$ gegebenen Linearform α ist

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

   Bei der Konstruktion von Stromchiffren (oder Pseudozufallsgeneratoren) durch Kombination von linearen Schieberegistern möchte man Korrelationen mit linearen Funktionen vermeiden. Da die Quadratsumme über alle solchen Korrelationen aber konstant = 1 ist, erreicht man die Korrelation 0 nur, wenn man höhere Korrelation mit anderen Linearformen in Kauf nimmt. Besser ist es, alle diese Korrelationen gleichmäßig zu minimieren, also den Spektralradius $\max|\hat{\chi}_f|$, und das wird ja gerade von den krummen Funktionen geleistet.
4. Ist f krumm, so

$$\frac{1}{2^{n/2}} \hat{\chi}_f(u) = \pm 1 = (-1)^{g(u)} = \chi_g(u)$$

   für alle $u \in \mathbb{F}_2^n$ mit einer Funktion $g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. Da umgekehrt $\hat{\chi}_g = 2^{n/2} \chi_f$, nimmt auch $\hat{\chi}_g$ nur die Werte $\pm 2^{n/2}$ an. Also:

Korollar 2 *Ist f krumm, so $\hat{\chi}_f = 2^{n/2} \chi_g$ mit einer krummen Funktion $g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$.*

Es besteht also eine natürliche Dualität zwischen krummen Funktionen.

Krumme Funktionen können keinen allzuhohen algebraischen Grad haben. Dazu zunächst zwei Hilfssätze:

Hilfssatz 3 *Ist* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *durch die algebraische Normalform*

$$f = \sum_{I \subseteq \{1,\ldots,n\}} a_I T^I$$

gegeben, so ist die Anzahl $\nu_f(0)$ *der Nullstellen von* f *genau dann gerade, wenn der Leitkoeffizient* $a_{1\ldots n} = 0$*, d. h.* $\operatorname{Grad} f \leq n-1$ *ist.*

Beweis. Es ist

$$\sum_{x \in \mathbb{F}_2^n} f(x) = \#\{x \mid f(x) = 1\} \bmod 2 = [2^n - \nu_f(0)] \bmod 2 = \nu_f(0) \bmod 2.$$

Andererseits ist für jede Teilmenge $I \subseteq \{1,\ldots,n\}$, da die Koordinaten außerhalb von I nicht ausgewertet werden,

$$\begin{aligned} \sum_{x \in \mathbb{F}_2^n} x^I &= 2^{n-\#I} \cdot \sum_{\operatorname{Supp}(x) \subseteq I} \underbrace{x^I}_{\begin{cases} 0, & \text{wenn } \operatorname{Supp}(x) \subset I, \\ 1, & \text{wenn } \operatorname{Supp}(x) = I, \end{cases}} \bmod 2 \\ &= 2^{n-\#I} \bmod 2 = \begin{cases} 0, & \text{wenn } \#I < n, \\ 1, & \text{wenn } I = \{1,\ldots,n\}, \end{cases} \end{aligned}$$

also

$$\sum_{x \in \mathbb{F}_2^n} f(x)$$

und daraus folgt die Behauptung. $\diamond$

Hilfssatz 4 *Sei* $n = r + s$*, und zu* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *sei* $g\colon \mathbb{F}_2^r \longrightarrow \mathbb{F}_2$ *mit*

$$g(x) = f(x, 0) \quad \textit{für } x \in \mathbb{F}_2^r$$

gebildet. Dann ist

$$2^{n-r} \hat{\chi}_g(w) = \sum_{v \in \mathbb{F}_2^s} \hat{\chi}_f(w, v) \quad \textit{für alle } w \in \mathbb{F}_2^r.$$

Beweis. Für $w \in \mathbb{F}_2^r$ ist

$$\begin{aligned}
\hat{\chi}_g(w) &= \sum_{x\in\mathbb{F}_2^r} \chi_g(x)(-1)^{w\cdot x} = \sum_{x\in\mathbb{F}_2^r} \chi_f(x,0)(-1)^{w\cdot x} \\
&= \sum_{x\in\mathbb{F}_2^r} \left[\frac{1}{2^n}\cdot \sum_{u\in\mathbb{F}_2^r}\sum_{v\in\mathbb{F}_2^s} \hat{\chi}_f(u,v)(-1)^{u\cdot x+v\cdot 0}\right](-1)^{w\cdot x} \\
&= \frac{1}{2^n}\cdot \sum_{v\in\mathbb{F}_2^s}\sum_{u\in\mathbb{F}_2^r} \hat{\chi}_f(u,v)\cdot \underbrace{\sum_{x\in\mathbb{F}_2^r}(-1)^{(u+w)\cdot x}}_{\begin{cases} 2^r, & \text{wenn } u=w, \\ 0 & \text{sonst,}\end{cases}} \\
&= \frac{1}{2^{n-r}}\cdot \sum_{v\in\mathbb{F}_2^s} \hat{\chi}_f(w,v),
\end{aligned}$$

wie behauptet. $\diamond$

Satz 6 (Rothaus) *Ist* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *krumm und* $n \geq 4$*, dann ist* $\operatorname{Grad} f \leq \frac{n}{2}$.

Beweis. Die Zahl der Nullstellen von f ist

$$\nu_f(0) = \#L_f(0) = 2^{n-1} + \frac{1}{2}\hat{\chi}_f(0) = 2^{n-1} \pm 2^{\frac{n}{2}-1}.$$

Für gerades $n \geq 4$ ist diese Anzahl gerade, also der Leitkoeffizient $a_{1\ldots n} = 0$ nach Hilfssatz 3.

Sei nun r mit $\frac{n}{2} < r < n$ beliebig und g wie in Hilfssatz 4 gebildet. Dann ist die Anzahl der Nullstellen von g

$$\begin{aligned}
\nu_g(0) &= 2^{r-1} + \frac{1}{2}\hat{\chi}_g(0) = 2^{r-1} + \frac{1}{2^{n-r+1}}\cdot \sum_{v\in\mathbb{F}_2^{n-r}} \hat{\chi}_f(0,v) \\
&= 2^{r-1} + \sum_{v\in\mathbb{F}_2^{n-r}} (\pm 2^{r-\frac{n}{2}-1}).
\end{aligned}$$

Falls $r \geq \frac{n}{2}+2$, ist das gerade. Falls $r = \frac{n}{2}+1$, besteht die letzte Summe aus $2^{n-r} = 2^{\frac{n}{2}-1}$ Summanden ± 1, ist also auch gerade. Also ist der Leitkoeffizient von g Null: $a_{1\ldots r} = 0$. Durch Umnummerierung der Variablen folgt genauso, dass $a_I = 0$ für $\#I > \frac{n}{2}$. Also ist $\operatorname{Grad} f \leq \frac{n}{2}$. $\diamond$

Satz 7 (MAIORANA-MCFARLAND-Konstruktion) *Sei $n = 2m \geq 2$ gerade. Sei $\pi : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$ bijektiv und $g : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ beliebig. Dann ist die Funktion*

$$f : \mathbb{F}_2^n = \mathbb{F}_2^m \times \mathbb{F}_2^m \longrightarrow \mathbb{F}_2, \quad f(x,y) = \pi(x) \cdot y + g(x),$$

krumm.

Beweis. Für beliebige $u, v \in \mathbb{F}_2^m$ gilt

$$\begin{aligned}
\hat{\chi}_f(u,v) &= \sum_{x,y \in \mathbb{F}_2^m} (-1)^{\pi x \cdot y + g(x) + u \cdot x + v \cdot y} \\
&= \sum_{x,y \in \mathbb{F}_2^m} (-1)^{g(x) + u \cdot x + (\pi x + v) \cdot y} \\
&= \sum_{x \in \mathbb{F}_2^m} (-1)^{g(x) + u \cdot x} \cdot \underbrace{\sum_{y \in \mathbb{F}_2^m} (-1)^{(\pi x + v) \cdot y}}_{\begin{cases} 0, & \text{wenn } \pi x \neq v, \\ 2^m, & \text{wenn } \pi x = v, \end{cases}} \\
&= 2^m \cdot (-1)^{g(\pi^{-1} v) + u \cdot \pi^{-1} v} = \pm 2^m.
\end{aligned}$$

Also ist f krumm. $\diamond$

Korollar 3 *Ist n gerade und $2 \leq r \leq \frac{n}{2}$, so gibt es auf $\mathbb{F}_2^n$ eine krumme Funktion vom Grad r.*

2.5 Die Berechnung der WALSH-Transformation

Sei $\varphi : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ eine Funktion. Für die praktische Berechnung der WALSH-Transformierten $\hat{\varphi}$ nehmen wir an, dass die Funktion φ durch ihre Wertetabelle gegeben ist – d. h., alle Werte $\varphi(x)$ sind bekannt – und suchen die Wertetabelle der Transformierten.

In diesem Abschnitt wird ein Algorithmus mittels binärer Rekursion hergeleitet, der dem aus 1.4 ziemlich ähnlich sieht. Er startet mit folgender Beobachtung: Für $v \in \mathbb{F}_2^j$, $w \in \mathbb{F}_2^{n-j}$ und $0 \leq j \leq n$ gilt

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

Setzt man

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

(**partielle** WALSH-**Transformation**), so ist

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

und es gilt:

Hilfssatz 5 *Für alle $v \in \mathbb{F}_2^j$ und $w \in \mathbb{F}_2^{n-j}$ gilt*

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

Daraus lässt sich eine Rekursionformel herleiten: Für $y \in \mathbb{F}_2^{j-1}$, $\eta \in \mathbb{F}_2$, $w \in \mathbb{F}_2^{n-j}$ ist

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

Damit ist bewiesen:

Satz 8 (Rekursionformel für die partielle WALSH-Transformation) *Für $y \in \mathbb{F}_2^{j-1}$ und $w \in \mathbb{F}_2^{n-j}$ gilt*

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

Für die iterative Berechnung der WALSH-Transformation nach dieser Formel setzt man $i := n - j$. Aus dem Startvektor $x^{(0)} = (x_u)_{u \in \mathbb{F}_2^n}$, der Wertetabelle $x_u = \varphi(u)$ von φ, wird also über Zwischenergebnisse $x^{(i)}$, $i = 1, \ldots, n-1$, das Endergebnis $x^{(n)}$, die Wertetabelle der WALSH-Transformierten $\hat{\varphi}$ berechnet. Dabei sieht der Schritt von $x^{(i)}$ nach $x^{(i+1)}$, wenn man den n-Bit-Index zerlegt in $u\xi v$ mit $n-i-1$ Bits u, 1 Bit ξ und i Bits v, nach Satz 8 wie folgt aus:

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

Zum konkreten Programmieren werden die Indizes noch wie in 1.1 als ganze Zahlen in $[0 \ldots 2^n - 1]$ gedeutet; dann ist in den obigen Gleichungen $u1v = u0v + 2^i$, und die Iterationsvorschrift sieht, analog zu 1.4, so aus:

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

für $k = 0, \ldots, 2^n - 1$. Damit lässt sich der gesamte Algorithmus so formulieren:

Prozedur [WT]

Ein- und Ausgabeparameter: Vektor x der Länge 2^n, $x[0], \ldots, x[2^n - 1]$.

lokale Hifsvariablen: Vektor y der Länge 2^n, $y[0], \ldots, y[2^n - 1]$.
Schleifenzähler $i = 0, \ldots, n-1$, und $k = 0, \ldots, 2^n - 1$.

Anweisungen:

Für $i = 0, \ldots, n-1$:
  Für $k = 0, \ldots, 2^n - 1$:
    Falls $(((k \gg i) \bmod 2) = 1)$: $y[k] := x[k - 2^i] - x[k]$
      sonst $y[k] := x[k] + x[k + 2^i]$
  Für $k = 0, \ldots, 2^n - 1$:
    $x[k] := y[k]$

Diese Prozedur ist natürlich nur bei exaktem Rechnen sinnvoll, also etwa mit ganzzahligen Vektoren. Hier ist gegebenenfalls die Fehlersituation durch Überlauf bei der Addition zu berücksichtigen.

Zu bemerken ist noch, dass, wenn φ nur Werte in einem Unterring von $\mathbb{R}$ annimmt (etwa $\mathbb{Z}$ oder $\mathbb{Q}$), die ganze Berechnung in diesem Unterring verläuft.

Der *Aufwand* als Funktion der Größe $N = 2^n$ der Eingabe ist wie in 1.4 fast linear: $3N \cdot {}^2\log N$, wie man es auch von der schnellen FOURIER-Transformation kennt. Dabei werden im wesentlichen $2N$ Speicherplätze für Elemente des Rings R bei exakter Arithmetik benötigt.

Ein C-Programm steht als Quelltext im Anhang (Prozedur `wt`).

2.6 Die Berechnung der Faltung

Die naive Anwendung der Formel in Definition 2 erfordert, dass jeder Wert von φ mit jedem Wert von ψ multipliziert wird, dass also 2^{2n} Multiplikationen von (je nach Anwendungskontext komplexen oder ganzen) Zahlen ausgeführt werden. Der Aufwand dafür ist quadratisch in der Größe $N = 2^n$ der Eingabe.

Durch die Anwendung des Faltungssatzes lässt sich der Aufwand auf den Wert $N \log N$ drücken: Bezeichnen wir das Zwischenergebnis mit $g := \widehat{\varphi * \psi} = \hat{\varphi}\hat{\psi}$, so ist $\hat{g} = 2^n \varphi\psi$. Also können wir folgenden Algorithmus verwenden:

1. a) Bestimmung von $\hat{\varphi}$,
   b) Bestimmung von $\hat{\psi}$,
2. Multiplikation $g = \hat{\varphi}\hat{\psi}$ (punktweise),
3. Rücktransformation $\varphi * \psi = \frac{1}{2^n}\hat{g}$.

Der Aufwand besteht also im wesentlichen aus 3 WALSH-Transformationen zu je $3n \cdot 2^n$ elementaren Operationen; dazu kommen noch die 2^n Multiplikationen im Schritt 2, so dass asymptotisch etwa $9N \cdot {}^2\log N$ elementare Operationen nötig sind. Dabei kommt man im wesentlichen mit $3N$ Speicherplätzen aus.

Anmerkung. Dieses Verfahren wird analog auch bei der effizienten Multiplikation von Polynomen mit Hilfe der schnellen FOURIER-Transformation verwendet.

2.7 Weitere Beispiele

1. Sei $f \in \mathcal{F}_4$ gegeben durch das Polynom $T_1T_2 + T_3T_4$. Dann haben wir folgende Wertetabellen:

x	$f(x)$	$\chi_f(x)$	$\hat{\chi}_f(x)$
0000	0	+1	+4
0001	0	+1	+4
0010	0	+1	+4
0011	1	−1	−4
0100	0	+1	+4
0101	0	+1	+4
0110	0	+1	+4
0111	1	−1	−4
1000	0	+1	+4
1001	0	+1	+4
1010	0	+1	+4
1011	1	−1	−4
1100	1	−1	−4
1101	1	−1	−4
1110	1	−1	−4
1111	0	+1	+4

   Insbesondere ist f krumm.

2. Sei $f \in \mathcal{F}_3$ gegeben durch das Polynom $T_1T_2 + T_1T_3 + T_2T_3$. Dann sehen die Wertetabellen so aus:

x	$f(x)$	$\chi_f(x)$	$\hat{\chi}_f(x)$
000	0	+1	0
001	0	+1	4
010	0	+1	4
011	1	−1	0
100	0	+1	4
101	1	−1	0
110	1	−1	0
111	1	−1	−4

3. Sei $f \in \mathcal{F}_n$ gegeben durch das Polynom $T_1 \cdots T_n$. Dann ist

$$\begin{aligned} f(x) &= \begin{cases} 0 & \text{für } x \neq (1 \ldots 1), \\ 1 & \text{für } x = (1 \ldots 1), \end{cases} \\ \chi_f(x) &= \begin{cases} 1 & \text{für } x \neq (1 \ldots 1), \\ -1 & \text{für } x = (1 \ldots 1), \end{cases} \\ \hat{\chi}_f(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} - 2(-1)^{|u|} \\ &= \begin{cases} 2^n - 2, & \text{falls } u = 0, \\ -2(-1)^{|u|} & \text{sonst}, \end{cases} \end{aligned}$$

wobei für $x = (1 \ldots 1)$ das Skalarprodukt $u \cdot x = u_1 + \cdots + u_n$ das HAMMING-Gewicht $|u|$ von u ist. Insbesondere ist f nur im Fall $n = 2$ krumm.

4. Sei $g \in \mathcal{F}_n$ gegeben durch das Polynom $(T_1 + 1) \cdots (T_n + 1) = \sum_{T \subseteq \{1,\ldots,n\}} T^I$. Dann ist

$$\begin{aligned} g(x) &= \begin{cases} 0 & \text{für } x \neq 0, \\ 1 & \text{für } x = 0, \end{cases} \\ \chi_g(x) &= \begin{cases} 1 & \text{für } x \neq 0, \\ -1 & \text{für } x = 0, \end{cases} \\ \hat{\chi}_g(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)+u \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} - 2 \\ &= \begin{cases} 2^n - 2, & \text{falls } u = 0, \\ -2 & \text{sonst}. \end{cases} \end{aligned}$$

2.8 Konstruktionsmethoden I: Direkte Summen

Definition 6 Sei $n = r + s$ mit $r, s \geq 1$ und seien $g : \mathbb{F}_2^r \longrightarrow \mathbb{F}_2$ und $h \colon \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$ BOOLEsche Funktionen. Dann heißt

$$f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2, \quad f(x, y) = g(x) + h(y) \quad \text{für } x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^s,$$

die **direkte Summe** von g und h, geschrieben $g \oplus h$.

Die Charakter-Form einer solchen direkten Summe ist

$$\chi_f(x, y) = \chi_g(x) \cdot \chi_h(y) \quad \text{für } x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^s,$$

folglich das WALSH-Spektrum für $u \in \mathbb{F}_2^r, v \in \mathbb{F}_2^s$:

$$\begin{aligned}\hat{\chi}_f(u,v) &= \sum_{x\in\mathbb{F}_2^r}\sum_{y\in\mathbb{F}_2^s}(-1)^{g(x)+h(y)+u\cdot x+v\cdot y}\\ &= \sum_{x\in\mathbb{F}_2^r}(-1)^{g(x)+u\cdot x}\sum_{y\in\mathbb{F}_2^s}(-1)^{h(y)+v\cdot y}\\ &= \hat{\chi}_g(u)\cdot\hat{\chi}_h(v).\end{aligned}$$

Satz 9 *Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ direkte Summe von $g\colon \mathbb{F}_2^r \longrightarrow \mathbb{F}_2$ und $h\colon \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$. Dann ist*

(i) *$\hat{\chi}_f(u,v) = \hat{\chi}_g(u)\cdot\hat{\chi}_h(v)$ für alle $u \in \mathbb{F}_2^r$ und $v \in \mathbb{F}_2^s$.*
(ii) *$\max|\hat{\chi}_f| = \max|\hat{\chi}_g|\cdot\max|\hat{\chi}_h|$.*
(iii) *f krumm $\Longleftrightarrow$ g und h krumm.*
(iv) *$\kappa_f(x,y) = \kappa_g(x)\kappa_h(y)$ für alle $x \in \mathbb{F}_2^r$ und $y \in \mathbb{F}_2^s$.*

Beweis. (i) wurde oben gezeigt, (ii) und (iii) sind direkte Folgen daraus. Da $\kappa_f = \frac{1}{2^n}\chi_f * \chi_f$, gilt

$$\begin{aligned}\kappa_f(x,y) &= \frac{1}{2^n}\cdot\sum_{u\in\mathbb{F}_2^r}\sum_{v\in\mathbb{F}_2^s}(-1)^{g(u+x)+h(v+y)-g(u)-h(v)}\\ &= \frac{1}{2^r}\cdot\sum_{u\in\mathbb{F}_2^r}(-1)^{g(u+x)-g(u)}\cdot\frac{1}{2^s}\cdot\sum_{v\in\mathbb{F}_2^s}(-1)^{h(v+y)-h(v)},\end{aligned}$$

und daraus folgt (iv). ◇

Korollar 1 *Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ krumm und vom algebraischen Grad $\frac{n}{2}$ mit $n \geq 6$. Dann ist f nicht in eine direkte Summe zerlegbar, auch nicht nach einer affinen Koordinatentransformation.*

Beweis. Da die Eigenschaft „krumm“ bei affiner Koordinatentransformation erhalten bleibt, genügt es, die Behauptung für f selbst zu beweisen. Angenommen, $f = g \oplus h$ mit Funktionen $g\colon \mathbb{F}_2^r \longrightarrow \mathbb{F}_2$, $h\colon \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$, so dass $r + s = n$ und o. B. d. A. $r \geq s \geq 2$. Dann sind g und h ebenfalls krumm, also $\operatorname{Grad} g \leq \frac{r}{2}$ und $\operatorname{Grad} h \leq \frac{s}{2}$, außer wenn $r = s = 2$, also $n = 4$. Also ist $\operatorname{Grad} f \leq \frac{r}{2}$, Widerspruch. ◇

Dass das im Fall $n = 4$ tatsächlich anders ist, zeigt das folgende Beispiel.

Beispiele

1. Wir gehen von der quadratischen Form $f\colon \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$ mit algebraischer Normalform $f = T_1T_2$ aus, von der wir schon wissen, dass sie krumm

ist. Daher ist auch für jedes gerade n die quadratische Form $Q_I(\frac{n}{2})$, also

$$f = T_1T_1 + \cdots + T_{n-1}T_n$$

eine krumme Funktion $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. Weiter folgt durch Induktion aus Beispiel 3 in 2.1, dass

$$\hat{\chi}_f = 2^{\frac{n}{2}}\chi_f,$$

also

$$\hat{\chi}_f(u) = 2^{\frac{n}{2}} \cdot (-1)^{u_1u_2+\cdots+u_{n-1}u_n} \quad \text{für } u \in \mathbb{F}_2^n.$$

Insbesondere sind die quadratischen Formen $Q_I(\frac{n}{2})$ zu sich selbst dual im Sinne von Korollar 2 in 2.4.

2. Für die quadratische Form $Q_{II}(\frac{n}{2})$ gilt analog $f = g \oplus h$, wobei $g\colon \mathbb{F}_2^{n-2} \longrightarrow \mathbb{F}_2$ mit

$$\hat{\chi}_g(u) = 2^{\frac{n}{2}-1}\chi_g(u),$$

und $h\colon \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$ mit

$$\hat{\chi}_h(v) = -2\chi_h(v).$$

Also ist

$$\hat{\chi}_f(u,v) = \hat{\chi}_g(u)\hat{\chi}_h(v) = -2^{\frac{n}{2}}\chi_g(u)\chi_h(v) = -2^{\frac{n}{2}}\chi_f(u,v).$$

Daher ist $\max|\hat{\chi}_f| = 2^{\frac{n}{2}}$ und f krumm.

3. Nach Satz 4 in 1.6 lässt sich jede quadratische Abbildung nach linearer Transformation im Urbild als direkte Summe einer nichtausgearteten quadratischen Abbildung und einer linearen Abbildung schreiben.

Korollar 2 *Eine quadratische Form $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist genau dann krumm, wenn sie zu einem der Typen $Q_I(\frac{n}{2})$ oder $Q_{II}(\frac{n}{2})$ aus 1.7 äquivalent ist, also wenn sie nichtausgeartet ist.*

Als Ziel der Bahn-Klassifikation in 1.5 kann man es ansehen, durch affine Transformationen eine reduzierte algebraische Normalform zu finden, die sich möglichst weit in direkte Summen zerlegen lässt, wie es bei den quadratischen Formen ja gelungen ist.

Korollar 3 *Für jede gerade Dimension n gibt es mindestens eine krumme Funktion $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ vom Grad 2.*

Als Spezialfall der MAIORANA-MCFARLAND-Konstruktion, Satz 7, kann man die krummen Funktionen $Q_I(\frac{n}{2})$ leicht verallgemeinern:

Korollar 4 *Sei $n = 2m$, $g\colon \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ eine beliebige* BOOLE*sche Funktion und $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ definiert durch $f(x,y) = x \cdot y + g(x)$ für alle $x, y \in \mathbb{F}_2^m$. Dann ist f krumm und $\hat{\chi}_f(u,v) = 2^m\chi_f(v,u)$ für alle $u, v \in \mathbb{F}_2^m$.*

Ein einfacher, aber wichtiger Spezialfall der direkten Summe ist:

Definition 7 Für $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ heißt die BOOLEsche Funktion

$$\breve{f}\colon \mathbb{F}_2^{n+1} \longrightarrow \mathbb{F}_2,$$

$$\breve{f}(x_0, x_1, \ldots, x_n) := x_0 + f(x_1, \ldots, x_n),$$

(oder jede, die durch Umnummerierung der Variablen aus $\breve{f}$ entsteht) **einfache Erweiterung** von f.

Da die identische Abbildung $g\colon \mathbb{F}_2 \longrightarrow \mathbb{F}_2$ mit der algebraischen Normalform $g = T_1$ das Spektrum $\hat{\chi}_g(u) = 1 - (-1)^u$, also $\hat{\chi}_g(0) = 0$, $\hat{\chi}_g(1) = 2$, hat, folgt sofort:

Korollar 5 *Ist $\breve{f}$ die einfache Erweiterung von $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, so*

$$\begin{aligned} \hat{\chi}_{\breve{f}}(0,u) &= 0, \\ \hat{\chi}_{\breve{f}}(1,u) &= 2 \cdot \hat{\chi}_f(u) \end{aligned}$$

für $u \in \mathbb{F}_2^n$.

Beispiele

3. Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ die quadratische Form $Q_I(m)$. Dann ist $f = g \oplus 0$ mit $g\colon \mathbb{F}_2^{2m} \longrightarrow \mathbb{F}_2$ und $\hat{\chi}_g = 2^m \chi_g$. Also ist

$$\begin{aligned} \hat{\chi}_f(u,v) &= \hat{\chi}_g(u)\hat{\chi}_h(v) = \begin{cases} 2^{n-2m}\hat{\chi}_g(u), & \text{wenn } v = 0, \\ 0 & \text{sonst,} \end{cases} \\ &= \begin{cases} 2^{n-m}\chi_g(u), & \text{wenn } v = 0, \\ 0 & \text{sonst,} \end{cases} \end{aligned}$$

und $\max|\hat{\chi}_f| = 2^{n-m}$.

4. Der Fall der quadratischen Form $Q_{II}(m)$ geht analog mit dem Ergebnis

$$\hat{\chi}_f(u,v) = \begin{cases} -2^{n-m}\chi_g(u), & \text{wenn } v = 0, \\ 0 & \text{sonst,} \end{cases}$$

und $\max|\hat{\chi}_f| = 2^{n-m}$.

5. Die quadratische Form $Q_{III}(m)$ ist direkte Summe $f = \breve{g} \oplus 0$ mit $g\colon \mathbb{F}_2^{2m} \longrightarrow \mathbb{F}_2$, $\breve{g}\colon \mathbb{F}_2^{2m+1} \longrightarrow \mathbb{F}_2$,

$$\begin{aligned}
\hat{\chi}_{\breve{g}}(u,0) &= 0,\\
\hat{\chi}_{\breve{g}}(u,1) &= 2\hat{\chi}_g(u),\\
\hat{\chi}_f(u,a,v) &= \begin{cases} 2^{n-2m-1}\hat{\chi}_{\breve{g}}(u,a) & \text{wenn } v=0,\\ 0 & \text{sonst,}\end{cases}\\
&= \begin{cases} 2^{n-2m}\hat{\chi}_g(u) & \text{wenn } a=1,\ v=0,\\ 0 & \text{sonst,}\end{cases}\\
&= \begin{cases} 2^{n-m}\chi_g(u) & \text{wenn } a=1,\ v=0,\\ 0 & \text{sonst,}\end{cases}
\end{aligned}$$

und $\max|\hat{\chi}_f| = 2^{n-m}$.

Die letzten drei Beispiele ergeben zusammengefasst:

Korollar 6 *Ist* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *quadratische Form vom Rang* r*, so ist* $\max|\hat{\chi}_f| = 2^{n-\frac{r}{2}}$.

2.9 Konstruktionsmethoden II: Elementare Abänderungen

[*. . . kommt noch.*]