Linearitätsmaße für Boolesche Abbildungen

Klaus Pommerening
Fachbereich Mathematik
der Johannes-Gutenberg-Universität
Saarstraße 21
D-55099 Mainz

30. Mai 2000, letzte Revision 3. August 2005

In der Kryptologie dienen Boolesche Funktionen und Abbildungen als Grundbausteine für die Konstruktion von Bitblock- und Bitstrom-Chiffren. Ein wichtiges Kriterium dabei ist die Nichtlinearität: Verschlüsselungsfunktionen (z. B. die S-Boxen in Bitblock-Chiffren) und Bit-Generatoren (z. B. Kombinationen von linearen Schieberegistern) sollen „möglichst wenig linear“ sein. Aber was heisst das? Wie können wir Nichtlinearität quantifizieren?

In den letzten Jahren wurden dafür verschiedene Maße eingeführt, die sich bei der Aufdeckung versteckter Linearität ergänzen. Ist eine Boolesche Abbildung bezüglich eines solchen Maßes zu nahe an der Linearität, so eröffnen sich Angriffsmöglichkeiten auf die Verschlüsselungssysteme, in denen sie verwendet wird. Die bekanntesten Beispiele dafür sind die *lineare* und die *differenzielle Kryptoanalyse* von Bitblock-Chiffren sowie die Korrelationsanalyse von Bitstrom-Chiffren.

Das wichtigste mathematische Werkzeug, um Linearitätsmaße elegant und einheitlich behandeln zu können, ist die Walsh- (oder Hadamard-) Transformation, ein Spezialfall der diskreten Fourier-Transformation. Ihre systematische Verwendung ergibt einen gleichmäßigen, eleganten und effizienten Zugang zur Nichtlinearität; obwohl sie konzeptuell sehr einfach ist, ist sie überraschend stark sowohl für theoretische als auch praktische Zwecke. Es wirkt fast wie Magie, wie viele der Beweise aus der Literatur sich dadurch auf wenige Zeilen reduzieren, und die Berechnung der Linearitätsmaße wird sehr effizient möglich. Dieser Text enthält die systematische und geschlossene Darstellung dieser Theorie, die man auch „Fourier-Analyse Boolescher Abbildungen“ nennen könnte, angereichert mit vielen Beispielen.

1 Die algebraische Normalform

BOOLEsche Abbildungen lassen sich durch Polynome beschreiben – das ist die algebraische Normalform. Der Grad als Polynom ist ein erstes, naheliegendes, Maß für die Nichtlinearität – lineare (allgemeiner: affine) Abbildungen haben den Grad 1.

In diesem Abschnitt wird die Bestimmung der algebraischen Normalform und des Grades aus der Wertetabelle einer Abbildung behandelt sowie die Klassifikation von BOOLEschen Abbildungen bei kleiner Dimension oder kleinem Grad.

1.1 BOOLEsche Funktionen und Abbildungen

Der zweielementige Körper wird mit $\mathbb{F}_2$ bezeichnet. Es wird stets die algebraische Schreibweise verwendet: $+$ bezeichnet die Addition im Körper $\mathbb{F}_2$ und in $\mathbb{F}_2$-Vektorräumen. Das Zeichen $\oplus$ ist für direkte Summen reserviert. In semiformalen Beschreibungen von Algorithmen wird auch die logische Notation XOR verwendet.

Eine **BOOLEsche Funktion** in n Variablen ist eine Funktion

$$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2.$$

Im Falle einer Abbildung

$$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$$

spricht man von einer **BOOLEschen Abbildung** (oder vektorwertigen BOOLEschen Funktion; in der Kryptologie ist auch der Ausdruck „S-Box“ oder „Substitutionsbox“ geläufig).

Mit $\mathcal{F}_n$ soll die Menge aller BOOLEschen Funktionen auf $\mathbb{F}_2^n$ bezeichnet werden; die Menge aller Abbildungen $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist dann auf natürliche Weise mit $\mathcal{F}_n^q$ identifizierbar.

Eine BOOLEsche Funktion lässt sich durch ihre **Wahrheitstafel** beschreiben – das ist ihre Wertetabelle. In der Regel ordnet man sie lexikographisch nach $x \in \mathbb{F}_2^n$; diese Ordnung ist, anders ausgedrückt, die natürliche Ordnung der Zahlen $a = 0, \ldots, 2^n - 1$, wenn diese binär als

$$a = x_1 \cdot 2^{n-1} + \cdots + x_{n-1} \cdot 2 + x_n$$

dargestellt und mit den Vektoren $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$ identifiziert werden.

Die logische Negation der Funktion $f \in \mathcal{F}_n$ ist die Funktion $\bar{f} = f + 1$.

Mit $\mathcal{L}_n$ sei die Menge aller Linearformen, also der Dualraum von $\mathbb{F}_2^n$, bezeichnet. Sei $\{e_1, \ldots, e_n\}$ die kanonische Basis von $\mathbb{F}_2^n$ und $\cdot$ das kanonische Skalarprodukt. Die Zuordnung der Linearform $x \mapsto u \cdot x$ zum Vektor $u \in \mathbb{F}_2^n$ ergibt den (Basiswahl-abhängigen) Vektorraum-Isomorphismus $\mathbb{F}_2^n \cong \mathcal{L}_n$.

Ferner sei $\mathcal{A}_n$ die Menge der affinen Funktionen $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. Davon gibt es 2^{n+1} Stück, nämlich die linearen und deren Negationen, anders ausgedrückt, die

$$f(x) = \alpha(x) + c \qquad \text{mit } \alpha \in \mathcal{L}_n \text{ und } c \in \mathbb{F}_2.$$

Sei $\chi : \mathbb{F}_2 \longrightarrow \mathbb{C}^\times$ der einzige nichttriviale Gruppenhomomorphismus („Charakter"), also $\chi(0) = 1$, $\chi(1) = -1$, oder zusammengefasst $\chi(a) = (-1)^a = 1 - 2a$, letzteres „par abus de notation" (índem nämlich $0, 1 \in \mathbb{F}_2$ mit $0, 1 \in \mathbb{R}$ identifiziert werden). Insbesondere ist χ reellwertig. Damit wird zu jeder BOOLEschen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ die **Charakter-Form** als $\chi_f := \chi \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{R}^\times \subseteq \mathbb{C}^\times$ definiert, also

$$\chi_f(x) = (-1)^{f(x)}.$$

Klar, dass $\chi_{f+g} = \chi_f \chi_g$. Etwas komplizierter ist die Formel für das Produkt zweier BOOLEscher Funktionen. Aus der Tabelle

a	b	$a+b$	ab	$\chi(a)$	$\chi(b)$	$\chi(a+b)$	$\chi(ab)$
0	0	0	0	1	1	1	1
0	1	1	0	1	−1	−1	1
1	0	1	0	−1	1	−1	1
1	1	0	1	−1	−1	1	−1

folgt die Formel

$$\chi(a+b) + 2\chi(ab) = 1 + \chi(a) + \chi(b) \quad \text{für alle } a, b \in \mathbb{F}_2.$$

Also gilt für $f, g \in \mathcal{F}_n$ die Produktformel

$$2\chi_{fg} = 1 + \chi_f + \chi_g - \chi_f \chi_g.$$

Definition 1 Für zwei BOOLEsche Funktionen $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ ist die HAMMING-**Distanz** definiert als die Anzahl der Stellen, an denen sie nicht übereinstimmen:

$$d(f, g) := \#\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\};$$

anders ausgedrückt: die Anzahl der Einsen in der Wahrheitstafel von $f + g$. Das HAMMING-**Gewicht** $\mathrm{wt}(f) := d(f, 0)$ gibt die Anzahl der Argumente $x \in \mathbb{F}_2^n$ an, an denen f den Wert 1 annimmt.

Bemerkungen

1. d ist eine Metrik auf $\mathcal{F}_n$. Die Transitivität von d folgt dabei für $f, g, h \in \mathcal{F}_n$ so: Ist $f(x) \neq h(x)$, so $f(x) \neq g(x)$ oder $g(x) \neq h(x)$; also

$$\begin{aligned} d(f, g) + d(g, h) &= \#\{x \mid f(x) \neq g(x)\} + \#\{x \mid g(x) \neq h(x)\} \\ &\geq \#\{x \mid f(x) \neq h(x)\} = d(f, h). \end{aligned}$$

2. Ist $\bar{g} = g + 1$ die Negation von g, so ist $d(f, \bar{g}) = 2^n - d(f, g)$, und das ist die Anzahl der Stellen, an denen f und g übereinstimmen.

3. Die Anzahl der Nullstellen von f ist $d(f, 1) = 2^n - \mathrm{wt}(f)$.

1.2 Boolesche Linearformen

Für $u, x \in \mathbb{F}_2^n$ lässt sich das kanonische Skalarprodukt schreiben als

$$u \cdot x = \sum_{i=1}^{n} u_i x_i = \sum_{u_i=1} x_i = \sum_{i \in \mathrm{Supp}(u)} x_i$$

mit der „Trägermenge“ von u,

$$\mathrm{Supp}(u) = \{i = 1, \ldots, n \mid u_i \neq 0\} = \{i = 1, \ldots, n \mid u_i = 1\}.$$

Das Skalarprodukt mit einem festen Vektor u ist also die Teilsumme über die Koordinaten von x in der Trägermenge $I \subseteq \{1, \ldots, n\}$ von u oder auch die **Parität** von x über I. Da jede Linearform auf einem endlich-dimensionalen Vektorraum eine Darstellung als Skalarprodukt mit einem festen Vektor hat, ist gezeigt:

Satz 1 *Die Linearformen auf $\mathbb{F}_2^n$ sind genau die Paritätsfunktionen über den Teilmengen $I \subseteq \{1, \ldots, n\}$.*

Anders ausgedrückt hat jede Linearform die Gestalt

$$\alpha_I(x) = \sum_{i \in I} x_i \qquad \text{für alle } x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$$

mit einer Teilmenge $I \subseteq \{1, \ldots, n\}$. Dadurch ist eine natürliche bijektive Abbildung zwischen der 2^n-elementigen Menge $\mathcal{L}_n$ und der Potenzmenge $\mathfrak{P}(\{1, \ldots, n\})$ hergestellt.

Andere übliche Schreibweisen sind für $I = \{i_1, \ldots, i_r\}$:

$$\alpha_I(x) = x[I] = x[i_1, \ldots, i_r] = x_{i_1} + \cdots + x_{i_r}.$$

1.3 Funktionen und Polynome

Sei $T = (T_1, \ldots, T_n)$ ein n-Tupel von Unbestimmten. Dann definiert jedes Polynom $p \in \mathbb{F}_2[T]$ eine Funktion $\Psi(p) \in \mathcal{F}_n$ durch Einsetzen:

$$\Psi(p)(x_1, \ldots, x_n) := p(x_1, \ldots, x_n).$$

Der **Einsetzungshomomorphismus**

$$\Psi : \mathbb{F}_2[T] \longrightarrow \mathcal{F}_n,$$

ist ein Homomorphismus der $\mathbb{F}_2$-Algebren.

Hilfssatz 1 Ψ *ist surjektiv.*

Beweis. (Induktion über n) Der Induktionsanfang $n = 0$ ist trivial – die beiden konstanten Polynome entsprechen den beiden konstanten Funktionen. Sei also jetzt $n \geq 1$. Für $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ wird abgekürzt geschrieben: $x' = (x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$.

Sei nun eine Funktion $f \in \mathcal{F}_n$ gegeben. Für $b = 0, 1$ ist aufgrund der Induktionsannahme

$$f(x', b) = p_b(x') \qquad \text{für alle } x' \in \mathbb{F}_2^{n-1}$$

mit Polynomen $p_0, p_1 \in \mathbb{F}_2[T_1, \ldots, T_{n-1}]$; im Fall $n = 1$ sind das Konstanten. Dann ist

$$f(x', x_n) = (1 + x_n)p_0(x') + x_n p_1(x') \qquad \text{für alle } x \in \mathbb{F}_2^n.$$

Also ist $f = \Psi(p)$ mit $p = p_0 + (p_0 + p_1)T_n$. $\diamond$

Anmerkung. Dieser Hilfssatz gilt analog über einem beliebigen endlichen Körper; der Beweis ist im allgemeinen Fall etwas komplizierter und verwendet Interpolation. [Auch diese Verallgemeinerung ist kryptologisch relevant: sie ist – über dem endlichen Körper $\mathbb{F}_{2^n}$ – der Ausgangspunkt für „Interpolations-Angriffe“ auf Bitblock-Chiffren.] Auch der folgende Satz 2 lässt sich entsprechend verallgemeinern.

Was kann man über den Kern des Homomorphismus Ψ sagen? Da $b^2 = b$ für alle $b \in \mathbb{F}_2$, liegen die Polynome $T_1^2 - T_1, \ldots, T_n^2 - T_n$ sicher im Kern, also auch das von ihnen erzeugte Ideal

$$\mathfrak{a} \trianglelefteq \mathbb{F}_2[T].$$

Der induzierte Homomorphismus auf der Restklassen-Algebra,

$$\bar{\Psi} : \mathbb{F}_2[T]/\mathfrak{a} \longrightarrow \mathcal{F}_n,$$

ist immer noch surjektiv. Jedes Element der Algebra $\mathbb{F}_2[T]/\mathfrak{a}$ lässt sich offensichtlich als Linearkombination der Monome schreiben, die in jedem T_i den Grad ≤ 1 haben. Davon gibt es 2^n Stück, nämlich die Produkte

$$T^I := T_{i_1} \cdots T_{i_r}$$

für beliebige Teilmengen

$$I = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}.$$

Auf der linken Seite von $\bar{\Psi}$ steht also ein $\mathbb{F}_2$-Vektorraum der Dimension $\leq 2^n$. Seine Dimension muss also $= 2^n$ und $\bar{\Psi}$ ein Isomorphismus sein. Damit ist gezeigt:

Satz 2 (Algebraische Normalform, ANF) *Jede* Boolesche *Funktion*

$$f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$$

lässt sich eindeutig als Polynom in n Unbestimmten schreiben, das in jeder Unbestimmten einzeln vom Grad ≤ 1 ist:

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} a_I x^I,$$

wobei das Monom x^I das Produkt

$$x^I = \prod_{i \in I} x_i$$

ist, und $a_I = 0$ oder 1.

Eine alternative Herleitung der algebraischen Normalform, die aber nicht auf andere endliche Körper übertragbar ist, geht über die Normalisierung von Booleschen Ausdrücken mit Hilfe der de Morganschen Regeln.

Korollar 1 *Jede* Boolesche *Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ wird durch ein q-Tupel von Polynomen $(p_1, \ldots, p_q) \in \mathbb{F}_2[T_1, \ldots, T_n]$ beschrieben, deren sämtliche partiellen Grade ≤ 1 sind.*

(Mit „partiellem Grad“ ist dabei der Grad in einer einzelnen Unbestimmten T_i gemeint.)

Korollar 2 *Jede* Boolesche *Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ lässt sich eindeutig in der Form*

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} x^I a_I$$

mit Koeffizienten $a_I \in \mathbb{F}_2^q$ schreiben.

Übungaufgabe. Zeige, dass sich die Koeffizienten a_I der algebraischen Normalform ausdrücken lassen als

$$a_I = \sum_{\mathrm{Supp}(u) \subseteq I} f(u).$$

Definition 2 Der Grad einer Booleschen Abbildung als Polynom,

$$\mathrm{Grad}\, f = \max\{\#I \mid a_I \neq 0\},$$

wird als **algebraischer Grad** bezeichnet.

Bemerkungen

1. Allgemein ist $\operatorname{Grad} f \leq n$.

2. f ist affin $\Leftrightarrow \operatorname{Grad} f \leq 1$.

3. Sind $g\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ und $h\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^q$ bijektive affine Abbildungen, so hat $h \circ f \circ g$ den gleichen Grad wie f, d. h., der algebraische Grad ist unter affinen Transformationen in Bild und Urbild invariant.

4. Der Grad einer BOOLEschen Abildung f ist das Maximum der Grade der Komponenten-Polynome $p_1, \ldots, p_q$.

5. Ist $n = 1$, so $\operatorname{Grad} f \leq 1$, d. h., alle Abbildungen $\mathbb{F}_2 \longrightarrow \mathbb{F}_2^q$ sind affin.

6. Ein Untervektorraum $C \leq \mathbb{F}_2^N$ heißt linearer Code der Länge N und der Dimension $r := \operatorname{Dim} C$; die Elemente von C nennt man in diesem Kontext – der Codierungstheorie – die Codewörter.

   Identifiziert man den Raum $\mathcal{F}_n$ der BOOLEschen Funktionen über die Wahrheitstafel mit $\mathbb{F}_2^N$, $N = 2^n$, so bildet der Unterraum $\mathcal{F}_n^{(}d)$ der Funktionen vom algenraischen Grad $\leq d$ den sogenannten REED-MULLER-Code $\mathcal{R}(d, n)$ der Ordnung d. Seine Länge ist 2^n.

Übungsaufgabe. Bestimme die Dimension des REED-MULLER-Codes $\mathcal{R}(d, n)$.

Anmerkung. REED-MULLER-Codes sind nicht optimal bezüglich ihrer fehlerkorrigierenden Eigenschaften, bieten aber sehr effiziente Codierungs- und Decodierungsalgorithmen, und sind daher von praktischer Bedeutung: der Code $\mathcal{R}(1, 5)$ wurde z. B. um 1970 von der Mars-Sonde MARINER 9 zur Bildübertragung verwendet.

Der algebraische Grad ist ein erstes Maß für die Nichtlinearität von f. Ein hoher algebraischer Grad erschwert im allgemeinen die Bestimmung der Nullstellen von f bzw. das Lösen von Gleichungen, in denen f vorkommt. Allerdings bedeutet ein hoher algebraischer Grad nicht notwendig eine hohe Komplexität, wie das Beispiel der Funktion $f(x) = x_1 \cdots x_n$ zeigt; z. B. ist die Bestimmung der Nullstellenmenge $\mathbb{F}_2^n - \{(1, \ldots, 1)\}$ dieser Funktion trivial.

Die Anzahl der Koeffizienten $\neq 0$ in der algebraischen Normalform ist übrigens kein gutes Komplexitätsmaß. Sie ist nicht einmal unter affinen Transformationen invariant, und so wird die „komplexe“ Funktion

$$f(x) = \sum_{I \subseteq \{1,\ldots,n\}} x^I$$

mit der Maximalzahl von 2^n Koeffizienten $\neq 0$ durch die affine Transformation $x_i \mapsto x_i + 1$ – also das „Umkippen“ aller Bits – zu der „einfachen“

Funktion $f(x) = x_1 \cdots x_n$; dabei ist die umgekehrte Richtung leichter zu sehen, denn

$$(x_1 + 1) \cdots (x_n + 1) = \sum_{I \subseteq \{1,\ldots,n\}} x^I.$$

Beispiele

1. Die vier Funktionen $\mathbb{F}_2 \longrightarrow \mathbb{F}_2$ werden durch die Polynome 0, 1, T und $T+1$ in der einen Unbestimmten T beschrieben. Insbesondere sind sie alle affin.

2. Die 16 Funktionen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$ werden durch die Polynome 0, 1, T_1, T_2, T_1+T_2, $1+T_1$, $1+T_2$, $1+T_1+T_2$, T_1T_2, $1+T_1T_2$, $T_1+T_1T_2$, $T_2+T_1T_2$, $T_1+T_2+T_1T_2$, $1+T_1+T_1T_2$, $1+T_2+T_1T_2$ und $1+T_1+T_2+T_1T_2$ beschrieben.

3. Es gibt genau $2^8 = 256$ Funktionen $\mathbb{F}_2^3 \longrightarrow \mathbb{F}_2$ und allgemein 2^{2^n} Funktionen $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. Die Anzahl $\#\mathcal{F}_n$ wächst also superexponentiell mit n – jedes zusätzliche Bit führt zu einer Quadrierung der Anzahl. (Allerdings ist es meist sinnvoll, $N = 2^n$ als Bezugsgröße, also als Größe des Inputs, zu betrachten; dann wächst $\#\mathcal{F}_n$ exponentiell in N.)

1.4 Die Auswertung der algebraischen Normalform

Der Vorteil der algebraischen Normalform ist, dass der algebraische Grad direkt ablesbar ist; auch die „Struktur“ einer BOOLEschen Funktion ist gut zu erkennen, und wir werden in 1.5 sehen, dass sich mit Hilfe der algebraischen Normalform relativ leicht die Bahnen unter affinen Transformationen bestimmen und „reduzierte“ Normalformen herstellen lassen.

Andererseits hat die Wahrheitstafel (also der „Graph“ der Funktion) den Vorteil, dass man das „Verhalten“ der Funktion leicht überblicken kann, z. B. das HAMMING-Gewicht leicht ablesen; auch versteckte Linearität wird sich von hier ausgehend leicht bestimmen lassen.

Daher ist es wünschenswert, zwischen beiden Darstellungen wechseln zu können. Der Übergang von der algebraischen Normalform zur Wahrheitstafel ist einfach die Reihe der Polynom-Auswertungen an allen Stellen; die Umkehrtransformation ist die Interpolation wie im Beweis von Satz 2. Hierfür wird noch ein sehr effizienter Algorithmus angegeben.

Die naive Auswertung einer BOOLEschen Funktion $f \in \mathcal{F}_n$, also einer Funktion $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, an allen Stellen $x \in \mathbb{F}_2^n$ bedeutet 2^n Auswertungen $f(x)$ mit je maximal 2^n Summanden à maximal $n-1$ Multiplikationen. Der Aufwand liegt also in der Größenordnung $n \cdot 2^n \cdot 2^n$; da die Größe des Inputs $N = 2^n$ ist, ist der Aufwand also im wesentlichen quadratisch: $N^2 \cdot {}^2\log(N)$. Wie so oft wird auch hier eine binäre Rekursion, also eine Aufteilung in

zwei Teilprobleme von halber Inputgröße, zu einem wesentlich effizienteren Algorithmus führen.

Zunächst schreiben wir die algebraische Normalform in etwas modifizierter Gestalt:

$$f = \sum_{u \in \mathbb{F}_2^n} \alpha_f(u) T^{(u)} \qquad \text{mit dem Monom} \quad T^{(u)} = \prod_{i \in \mathrm{Supp}(u)} T_i.$$

Die **Koeffizienten-Darstellung** von f ist die Funktion $\alpha_f \in \mathcal{F}_n$. Auf der anderen Seite wird die Wahrheitstafel durch die Familie $(f(x))_{x \in \mathbb{F}_2^n}$, also einfach durch $f \in \mathcal{F}_n$ selbst repräsentiert. Mit dieser Interpretation ist die Auswertung dann die Abbildung

$$\Theta_n \colon \mathcal{F}_n \longrightarrow \mathcal{F}_n, \qquad \alpha_f \mapsto f.$$

Die verschiedenen Interpretationen eines binären Vektors $u \in \mathbb{F}_2^n$ und die „kanonischen“ Zuordnungen zwischen ihnen sind in Tabelle 1 exemplarisch wiedergegeben. Denkt man sich zum Beispiel die acht Bits

$$(00101101)$$

als algebraische Normalform einer Funktion $f \in \mathcal{F}_3$, so ist dies zu interpretieren als

$$\alpha_f(000) = 0,\ \alpha_f(001) = 0,\ \alpha_f(010) = 1,\ \alpha_f(011) = 0,$$

$$\alpha_f(100) = 1,\ \alpha_f(101) = 1,\ \alpha_f(110) = 0,\ \alpha_f(111) = 1,$$

also als das Polynom

$$0 \cdot 1 + 0 \cdot T_3 + 1 \cdot T_2 + 0 \cdot T_2T_3 + 1 \cdot T_1 + 1 \cdot T_1T_3 + 0 \cdot T_1T_2 + 1 \cdot T_1T_2T_3.$$

Die zugehörige Wahrheitstafel ist dann

$$f(000) = 0,\ f(001) = 0,\ f(010) = 1,\ f(011) = 1,$$

$$f(100) = 1,\ f(101) = 0,\ f(110) = 0,\ f(111) = 0,$$

und das wird wieder kurz geschrieben als die Bitfolge

$$(00111000).$$

Die binäre Rekursion startet mit der eindeutigen Zerlegung

$$f = f_0 + T_1 f_1 \qquad \text{mit} \quad f_0, f_1 \in \mathbb{F}_2[T_2, \ldots, T_n],$$

die auch schon beim Beweis von Hilfssatz 1, wenn auch mit anderer Nummerierung, verwendet wurde. Für $y \in \mathbb{F}_2^{n-1}$ gilt dann

$$\begin{aligned} f(0,y) &= f_0(y), \\ f(1,y) &= f_0(y) + f_1(y). \end{aligned}$$

$k \in \mathbb{N}$	$u \in \mathbb{F}_2^3$	$I \subseteq \{1,2,3\}$	Monom
0	000	$\emptyset$	1
1	001	$\{3\}$	T_3
2	010	$\{2\}$	T_2
3	011	$\{2,3\}$	T_2T_3
4	100	$\{1\}$	T_1
5	101	$\{1,3\}$	T_1T_3
6	110	$\{1,2\}$	T_1T_2
7	111	$\{1,2,3\}$	$T_1T_2T_3$

Tabelle 1: Verschiedene Deutungen eines binären Vektors, Beispiel $n = 3$

Allgemein sei $0 \leq i \leq n$, $u \in \mathbb{F}_2^{n-i}$ und $f_u \in \mathbb{F}_2[T_{n-i+1}, \ldots, T_n]$ definiert durch

$$f_u := \sum_{v \in \mathbb{F}_2^i} \alpha_f(u,v) T^{(v)}.$$

Dann ist im Fall $i = n$ und $u = 0 \in \mathbb{F}_2^0$

$$f_u = \sum_{v \in \mathbb{F}_2^n} \alpha_f(v) T^{(v)} = f.$$

Auf der anderen Seite, im Fall $i = 0$ und $u \in \mathbb{F}_2^n$, ist

$$f_u = \alpha_f(u) \quad \text{konstant},$$

und dazwischen, für $1 \leq i \leq n$ und $u \in \mathbb{F}_2^{n-i}$, gilt

$$f_u = f_{(u,0)} + T_{n-i+1} f_{(u,1)}.$$

Die Auswertung folgt daher für $y \in \mathbb{F}_2^{i-1}$ der Rekursionsformel

$$\begin{aligned} f_u(0,y) &= f_{(u,0)}(y), \\ f_u(1,y) &= f_{(u,0)}(y) + f_{(u,1)}(y). \end{aligned}$$

Daraus wird jetzt eine iterative Prozedur gemacht. Dazu wird eine Folge von Vektoren $x^{(i)} = (x_u^{(i)})_{u \in \mathbb{F}_2^n}$ mit Koeffizienten in $\mathbb{F}_2$ so definiert: Der Startvektor sei

$$x^{(0)} := (\alpha_f(u))_{u \in \mathbb{F}_2^n},$$

und für $i = 1, \ldots, n$ sei, wenn man den n-Bit-Index zerlegt in $u\xi v$ mit $n - i$ Bits u, einem Bit ξ und $i - 1$ Bits v, rekursiv definiert

$$\begin{aligned} x_{u0v}^{(i)} &:= x_{u0v}^{(i-1)}, \\ x_{u1v}^{(i)} &:= x_{u0v}^{(i-1)} + x_{u1v}^{(i-1)}. \end{aligned}$$

Durch Induktion folgt dann:

Satz 3 *Für die wie oben rekursiv definierte Folge* $(x^{(i)})$ *gilt*

$$x^{(i)}_{(u,y)} = f_u(y) \qquad \textit{für alle} \quad u \in F_2^{n-i}, y \in \mathbb{F}_2^i;$$

insbesondere ist

$$x^{(n)} = (f(u))_{u \in \mathbb{F}_2^n}$$

die Wahrheitstafel von f.

Da die Iterationsformel umgekehrt genauso aussieht:

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

erfolgt die Umkehrabbildung von Θ_n, also die Gewinnung der Koeffizienten-Darstellung aus der Wahrheitstafel, nach dem gleichen Algorithmus, ist also mit Θ_n identisch:

Korollar 1 *Die Auswertungsabbildung* Θ_n *ist eine Involution.*

Insbesondere *wird durch die umgekehrte Anwendung von* Θ_n *auch der algebraische Grad einer* BOOLE*schen Funktion bestimmt*, die durch ihre Wahrheitstafel gegeben ist.

Zur konkreten Programmierung der Auswertungsprozedur werden die Indizes noch wie in 1.1 und Tabelle 1 als ganze Zahlen $k = \sum k_{n-i} 2^i$ in $[0 \ldots 2^n - 1]$ gedeutet. Dann ist in der Iterationsvorschrift $u1v = u0v + 2^i$, und die Gleichungen werden zu

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

für $k = 0, \ldots, 2^n - 1$. Das Bit k_{n-i} lässt sich aus k nach der Formel

$$k_{n-i} = \left\lfloor \frac{k}{2^i} \right\rfloor \bmod 2 = (k \gg i) \bmod 2$$

extrahieren, wobei $k \gg i$ die Verschiebung um i Bits nach rechts bedeutet. Der gesamte Algorithmus sieht also so aus:

Prozedur [REV] (Rekursive Evaluation)
Ein- und Ausgabeparameter: Vektor x der Länge 2^n,
$x[0], \ldots, x[2^n - 1]$.

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

Dabei sind x und y Vektoren über $\mathbb{F}_2$, also Bitketten, die Addition in $\mathbb{F}_2$ ist daher in die BOOLEsche Programmiersprachen-Operation XOR übergegangen.

Der *Aufwand* beträgt $n \cdot 2^n$ Schleifendurchläufe mit je einer binären Addition, einer Bit-Verschiebung und einer Einzelbit-Komplementierung, also insgesamt $3n \cdot 2^n$ „elementare“ Operationen. Benötigt wird dabei im wesentlichen Speicherplatz für $2 \cdot 2^n$ Bits. Wird der Aufwand als Funktion der Größe $N = 2^n$ der Eingabe ausgedrückt, ist er fast linear: $3N \cdot {}^2\log N$.

Das entsprechende C-Programm befindet sich als Quelltext im Anhang (Prozedur `rev`).

1.5 Gruppenoperationen

In vielen Fällen ist es von Interesse zu wissen, ob bestimmte Größen unter bestimmten Transformationen invariant sind; z. B. sollte ein sinnvolles Linearitätsmaß unter affinen Transformationen in Bild und Urbild invariant sein. Weiterhin ist es von Interesse, ob sich Funktionen oder Abbildungen durch geeignete Transformationen auf besonders einfache, d. h., einfach zu berechnende und zu analysierende, „reduzierte“ algebraische Normalformen bringen lassen. Die hier relevanten Transformationsgruppen liegen in

$$\mathcal{G}_n = \mathrm{Bij}(\mathbb{F}_2^n) \qquad \text{und} \qquad \mathcal{G}_n \times \mathcal{G}_q.$$

Wichtige Untergruppen von $\mathcal{G}_n$ sind die lineare Gruppe $GL(\mathbb{F}_2^n)$ und die Gruppe $GA(\mathbb{F}_2^n)$ der affinen Transformationen.

Die Gruppe $\mathcal{G}_n \times \mathcal{G}_q$ operiert auf der Menge $\mathcal{F}_n^q = \mathrm{Abb}(\mathbb{F}_2^n, \mathbb{F}_2^q)$ aller Abbildungen von $\mathbb{F}_2^n$ nach $\mathbb{F}_2^q$ durch die Vorschrift

$$\omega_{(g,h)} f := h \circ f \circ g^{-1} \qquad \text{für } g \in \mathcal{G}_n, h \in \mathcal{G}_q, f \in \mathcal{F}_n^q.$$

Bei g steht der Exponent -1, damit bei der konventionellen Nacheinanderausführung von Abbildungen $\omega_{(g,h)(g',h')} = \omega_{(g,h)} \circ \omega_{(g',h')}$ ist. Ist g eine lineare Abbildung mit zugehöriger Matrix $A \in GL_n(\mathbb{F}_2)$ und wird $\mathcal{L}_n$ kanonisch mit $\mathbb{F}_2^n$ identifiziert, so ist zu beachten, dass g dann als Multiplikation mit der „kontragredienten Matrix“ $A^* = (A^t)^{-1}$ operiert: Das Skalarprodukt ist in Matrix-Schreibweise $u \cdot x = u^t x =: \alpha(x)$, und $\omega_g(\alpha)$ ist gegeben durch

$$\omega_g(\alpha)(x) = \alpha(g^{-1}x) = u^t A^{-1} x = \left[(A^t)^{-1} u\right]^t x = [A^* u] \cdot x.$$

Im folgenden wird meist, in der Hoffnung, dass die Verwechslung nicht zu Verwirrung führt, die Transformationsgruppe $GL(\mathbb{F}_2^n)$ mit der Matrizengruppe $GL_n(\mathbb{F}_2)$ identifiziert.

Achtung: Die Operation von $GL_n(\mathbb{F}_2)$ auf $\mathcal{F}_n$ ist *nicht homogen* bezüglich des Grades: Ist z. B. $f(x_1, x_2) = x_1x_2$ und $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so $f \circ g^{-1}(x_1, x_2) = f(x_1 + x_2, x_2) = x_1x_2 + x_2$. [Dies ist eine Besonderheit der Charakteristik 2 des Grundkörpers $\mathbb{F}_2$.]

Beispiele

1. Ist (im Fall $q = 1$) $(g, h) \in \mathcal{G}_n \times \mathcal{G}_q$, so ist

   $$d(h \circ f_1 \circ g^{-1}, h \circ f_2 \circ g^{-1}) = d(f_1, f_2);$$

   d. h., die HAMMING-Distanz ist unter allen bijektiven Transformationen in Bild und Urbild invariant.

2. Wie bereits bemerkt, ist der algebraische Grad einer Funktion f unter $GA(\mathbb{F}_2^n) \times GA(\mathbb{F}_2^q)$ invariant, d. h., unter allen affinen Transformationen, wie es sich für ein sinnvolles Linearitätsmaß gehört.

3. Im Fall $n = q = 1$ haben $\mathcal{G}_n$ und $\mathcal{G}_q$ jeweils die Ordnung 2; das nichttriviale Gruppenelement σ vertauscht 0 und 1 und ist affin: $\sigma(x) = x+1$. Die vier Abbildungen $\mathbb{F}_2 \longrightarrow \mathbb{F}_2$ verteilen sich daher unter $\mathcal{G}_n$ auf die drei Bahnen $\{0\}, \{1\}, \{T, T + 1\}$, unter $\mathcal{G}_q$ – und somit auch unter $\mathcal{G}_n \times \mathcal{G}_q$ – auf die zwei Bahnen $\{0, 1\}, \{T, T + 1\}$.

4. Allgemeiner lässt sich jede Abbildung $f : \mathbb{F}_2 \longrightarrow \mathbb{F}_2^q$, die ja nach Bemerkung 5 in 1.3 affin ist, mit affinen Transformationen im Urbild, also unter der Gruppe $GA(\mathbb{F}_2^q)$, in die Gestalt 0 – falls f konstant ist – oder $(T_1, 0, \ldots, 0)$ – falls f nicht konstant ist – bringen.

5. Im Fall $n = 2$, $q = 1$, besteht $\mathcal{G}_q$ aus $\mathbf{1}$ (der identischen Abbildung) und σ wie im Beispiel 3.

   Da $\#\mathbb{F}_2^2 = 4$, ist $\mathcal{G}_n \cong \mathfrak{S}_4$ und hat $4! = 24$ Elemente. Die Gruppe $GL_2 = GL_2(\mathbb{F}_2)$ besteht aus den sechs Matrizen

   $$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

   Die affinen Permutationen erhält man, indem man jede davon mit den vier möglichen Verschiebungen in $\mathbb{F}_2^2$ kombiniert, so dass $GA_2 = GA(\mathbb{F}_2^2)$ aus 24 Transformationen besteht. Insbesondere ist $GA_2 = \mathcal{G}_n$, d. h., alle Permutationen von $\mathbb{F}_2^2$ sind affin.

   Da σ auf Funktionen als $f \mapsto f + 1$ operiert, verteilen sich die 16 Funktionen in $\mathcal{F}_2$ auf acht $\mathcal{G}_q$-Bahnen der Länge 8.

Die Operation von $\mathcal{G}_n$ erhält den Grad und lässt insbesondere die Konstanten 0 und 1 fest. Die Funktionen vom Grad 1 bilden unter $GL_2(\mathbb{F}_2)$ die beiden dreielementigen Bahnen $\{T_1, T_2, T_1+T_2\}$ und $\{T_1+1, T_2+1, T_1+T_2+1\}$, die unter $GA_2 = \mathcal{G}_n$ zu einer sechselementigen zusammenfallen.

Bei den quadratischen Funktionen verwendet man, dass die lineare Abbildung zur Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ die Funktion T_1T_2 in $T_1T_2 + bdT_1 + acT_2$ transformiert. Daher gibt es unter GL_2 je zwei Bahnen der Längen 1 und 3:

$$\{T_1T_2, T_1T_2+T_1, T_1T_2+T_2\}, \{T_1T_2+T_1+T_2\},$$

$$\{T_1T_2+1, T_1T_2+T_1+1, T_1T_2+T_2+1\}, \{T_1T_2+T_1+T_2+1\}.$$

Da die Verschiebung um den Vektor $\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)$ die Transformation $T_1T_2 \mapsto T_1T_2+T_1+T_2+1$ bewirkt, fallen diese unter $GA_2 = \mathcal{G}_n$ zu zwei Bahnen der Länge vier zusammen:

$$\{T_1T_2, T_1T_2+T_1, T_1T_2+T_2, T_1T_2+T_1+T_2+1\},$$

$$\{T_1T_2+1, T_1T_2+T_1+1, T_1T_2+T_2+1, T_1T_2+T_1+T_2\},$$

und unter $\mathcal{G}_n \times \mathcal{G}_q$ gibt es schließlich nur noch eine Bahn der Länge acht. Also sind im Fall $n = 2$, $q = 1$, alle quadratischen Abbildungen affin ineinander transformierbar.

6. Ähnlich, aber natürlich mit etwas mehr Aufwand, zeigt man, dass die 256 Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ unter affinen Transformationen in Bild und Urbild, also unter der vollen Gruppe $\mathcal{G}_n \times \mathcal{G}_q$, in 5 Bahnen zerfallen, die von den folgenden Abbildungen repräsentiert werden – hier durch Polynompaare beschrieben:

$$\binom{0}{0}, \binom{T_1}{0}, \binom{T_1}{T_2}, \binom{T_1T_2}{0}, \binom{T_1T_2}{T_2}.$$

Diese Klassifikation wird in 1.6 in etwas allgemeinerer Form hergeleitet.

Eine weitere sinnvolle Gruppenoperation erhalten wir durch Translationen mit affinen Abbildungen $r \in \mathcal{A}_n^q$; eine solche wirkt als $f \mapsto f + r$. Diese Operation erhält den Grad, sofern er ≥ 2 ist; auf den Abbildungen vom Grad ≤ 1, also auf $\mathcal{A}_n^q$, hat sie offensichtlich genau eine Bahn.

Anmerkung. Man kann das leicht zu einer Operation eines geeignet definierten semidirekten Produkts $[\mathcal{G}_n \times GA_q] \ltimes \mathcal{A}_n^q$ zusammensetzen. Wie sich später zeigen wird, ist die darin enthaltene Untergruppe $[GA_n \times GA_q] \ltimes \mathcal{A}_n^q$ eine sehr natürliche Transformationsgruppe auf $\mathcal{F}_n^q$, wenn es um die Untersuchung von Nichtlinearität geht.

Auch ohne die Definition des semidirekten Produkts explizit hinzuschreiben [**Übungsaufgabe**], können wir die von $GA_n \times GA_q$ und $\mathcal{A}_n^q$ zusammen erzeugte Untergruppe G aller Bijektionen von $\mathcal{F}_n^q$ betrachten und definieren:

Definition 3. Zwei Abbildungen $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißen äquivalent, wenn sie in derselben Bahn unter G liegen.

Beispiele. In $\mathcal{F}_1^q$ sind alle Abbildungen zueinander äquivalent. In $\mathcal{F}_2$ und $\mathcal{F}_2^2$ gibt es jeweils zwei Äquivalenzklassen: die affinen Abbildungen und die (echt) quadratischen.

Die Zahl der Äquivalenzklassen sieht in diesen Beispielen beeindruckend klein aus. Eine grobe Überschlagsrechnung zeigt allerdings, dass dieser Effekt nur für kleine Dimensionen wirksam ist: $GA_n(\mathbb{F}_2)$ hat höchstens $2^{2n} + 2^n \leq 2^{2n+1}$ Elemente, die ganze Gruppe G also höchstens $2^{nq+2n+2q+2}$. Der Raum, auf dem sie operiert, $\mathcal{F}_n^q$, hat dagegen 2^{q2^n} Elemente. Es gibt also mindestens $2^{q2^n-nq-2n-2q-2} \approx 2^{q2^n}$ Bahnen. Für $n = 3$ ist diese Unterschranke $= 2^{3q-8}$, für $n = 4$ schon $= 2^{10q-10}$, also spätestens für $q = 5$ außerhalb der Reichweite einer vollständigen Aufzählung aller Äquivalenzklassen. Für $n = 5$ lässt uns die Schranke 2^{25q-12} allerspätestens bei $q = 3$ resignieren, und für $n = 6$, $q = 1$ gibt es mindestens 2^{42} Äquivalenzklassen.

1.6 Quadratische Abbildungen

Eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, vom Grad ≤ 2 soll hier als **quadratische Abbildung** bezeichnet werden; darin sind also auch die affinen eingeschlossen. Eine solche quadratische Abbildung hat in algebraischer Normalform die Gestalt

$$f = \sum_{i=1}^{n} a_{ii} T_i + \sum_{1 \leq i < j \leq n} a_{ij} T_i T_j + b$$

mit Koeffizienten $a_{ij}, b \in \mathbb{F}_2^q$.

Bemerkungen

1. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ quadratische Abbildung und $(e_1, \ldots, e_n)$ die kanonische Basis von $\mathbb{F}_2^n$, so

   (i) $b = f(0)$,

   (ii) $a_{ii} = f(e_i) - f(0)$ für $i = 1, \ldots n$,

   (iii) $a_{ij} = f(e_i + e_j) - f(e_i) - f(e_j) + f(0)$ für $1 \leq i < j \leq n$.

   Das folgt direkt durch Einsetzen von e_i bzw. $e_i + e_j$ in die algebraische Normalform.

2. Die zu f gehörige bilineare Abbildung

$$\beta_f : \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$$

ist gegeben durch

$$\begin{aligned}\beta_f(x,y) &= f(x+y) - f(x) - f(y) + f(0) \\ &= \sum_{i=1}^{n} a_{ii}[x_i + y_i - x_i - y_i] \\ &\quad + \sum_{1\le i<j\le n} a_{ij}[(x_i+y_i)(x_j+y_j) - x_ix_j - y_iy_j] \\ &= \sum_{1\le i<j\le n} a_{ij}(x_iy_j + y_ix_j).\end{aligned}$$

Es ist offensichtlich

(i) $\beta_f(x,x) = 0$ für alle $x \in \mathbb{F}_2^n$,

(ii) $\beta_f(x,y) = \beta_f(y,x)$ für alle $x, y \in \mathbb{F}_2^n$,

also β_f „symplektisch“.

Definition 4 Das **Radikal** der quadratischen Abbildung $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist der Unterraum

$$\mathrm{Rad}_f := \{u \in \mathbb{F}_2^n \mid \beta_f(u,x) = 0 \text{ für alle } x \in \mathbb{F}_2^n\}.$$

Der **Rang** von f ist $\mathrm{Rang}\, f := n - \mathrm{Dim}(\mathrm{Rad}_f)$. Die quadratische Abbildung f heißt **nichtausgeartet**, wenn $\mathrm{Rang}\, f = n$ oder, äquivalent dazu, $\mathrm{Rad}_f = 0$.

Bemerkungen

3. Genau dann ist $u \in \mathrm{Rad}_f$, wenn $f(u+x)+f(0) = f(u)+f(x)$ für alle $x \in \mathbb{F}_2^n$. Insbesondere ist f auf Rad_f affin.

4. Sind $f_1, \ldots, f_q\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ die Komponenten der quadratischen Abbildung $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, so ist

$$\mathrm{Rad}_f = \bigcap_{i=1}^{q} \mathrm{Rad}_{f_i};$$

insbesondere ist f genau dann nichtausgeartet, wenn mindestens eine Komponente f_i nichtausgeartet ist.

5. $\beta_f = 0$ konstant $\Leftrightarrow \mathrm{Rad}_f = \mathbb{F}_2^n \Leftrightarrow f$ affin.

6. Im Fall der Dimension $n = 1$ sind alle quadratischen Abbildungen affin.

7. **Basiswechsel:** Sei $h \in GL_n(\mathbb{F}_2)$ und $v_i = he_i$ für $i = 1, \ldots, n$. Dann ist auch $\tilde{f} := f \circ h$ eine quadratische Abbildung und

$$\begin{aligned}\mathrm{Rad}_{\tilde{f}} &= \{u \in \mathbb{F}_2^n \mid f \circ h(x+u) - f \circ h(x) - f \circ h(u) + f \circ h(0) = 0 \\ &\quad \text{für alle } x \in \mathbb{F}_2^n\} \\ &= \{u \in \mathbb{F}_2^n \mid f(y+hu) - f(y) - f(hu) + f(0) = 0 \quad \text{für alle } y\} \\ &= \{u \in \mathbb{F}_2^n \mid hu \in \mathrm{Rad}_f\} = h^{-1}(\mathrm{Rad}_f).\end{aligned}$$

8. Weiter ist bei einem Basiswechsel h:

$$\begin{aligned}f(\xi_1 v_1 + \cdots + \xi_n v_n) &= f \circ h(\xi_1 e_1 + \cdots + \xi_n e_n) = f \circ h(\xi_1, \ldots, \xi_n) \\ &= \sum_{i=1}^{n} \tilde{a}_{ii}\xi_i + \sum_{1 \le i < j \le n} \tilde{a}_{ij}\xi_i\xi_j + b\end{aligned}$$

   mit $\tilde{a}_{ij} \in \mathbb{F}_2^q$ für $1 \le i \le j \le n$, und zwar

$$\tilde{a}_{ii} = f(v_i) - f(0), \quad \tilde{a}_{ij} = f(v_i + v_j) - f(v_i) - f(v_j) + f(0) \quad \text{für } i \neq j.$$

9. Sei $(v_1, \ldots, v_r, v_{r+1}, \ldots, v_n)$ eine Basis von $\mathbb{F}_2^n$, so dass $v_{r+1}, \ldots, v_n$ eine Basis von Rad_f bilden. Dann ist $\tilde{a}_{ij} = f(v_i+v_j)-f(v_i)-f(v_j)+f(0) = \beta_f(v_i, v_j) = 0$ für $j > r$, also

$$\begin{aligned}f \circ h(\xi_1, \ldots, \xi_n) &= f(\xi_1 v_1 + \cdots + \xi_n v_n) \\ &= \sum_{i=1}^{n} \tilde{a_{ii}}\xi_i + \sum_{1 \le i < j \le r} \tilde{a_{ij}}\xi_i\xi_j + b \\ &= \left[\sum_{i=1}^{r} \tilde{a}_{ii}\xi_i + \sum_{1 \le i < j \le r} \tilde{a}_{ij}\xi_i\xi_j + b\right] + \sum_{i=r+1}^{n} \tilde{a_{ii}}\xi_i.\end{aligned}$$

   Der Vektorraum $\mathbb{F}_2^n$ zerfällt also in die direkte Summe $\mathbb{F}_2^r \oplus \mathbb{F}_2^{n-r}$ von Unterräumen, so dass $f \circ h$ auf dem ersten nichtausgeartet, auf dem zweiten linear ist.

Damit ist gezeigt:

Satz 4 *Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine quadratische Abbildung vom Rang $r \le n-1$. Dann gibt es ein $h \in GL_n(\mathbb{F}_2)$, eine nichtausgeartete quadratische Abbildung $g\colon \mathbb{F}_2^r \longrightarrow \mathbb{F}_2^q$ und eine lineare Abbildung $l\colon \mathbb{F}_2^{n-r} \longrightarrow \mathbb{F}_2^q$, so dass*

$$f \circ h(x_1, \ldots, x_n) = g(x_1, \ldots, x_r) + l(x_{r+1}, \ldots, x_n)$$

für alle $x \in \mathbb{F}_2^n$, und $\mathrm{Rad}_{f\circ h}$ wird von $e_{r+1}, \ldots, e_n$ aufgespannt.

Insbesondere ist $r \geq 2$, wenn f nicht affin ist.

Bemerkungen

10. Sei $a \in \mathbb{F}_2^n$ und $\tilde{f}(x) = f(x+a)$ (Verschiebung im Urbildraum). Für $u \in \mathrm{Rad}_f$ gilt dann

$$\begin{aligned} \tilde{f}(x+u) &- \tilde{f}(x) - \tilde{f}(u) + \tilde{f}(0) \\ &= f(x+a+u) - f(x+a) - f(u+a) + f(a) \\ &= f(u) - f(0) - f(u) + f(0) = 0. \end{aligned}$$

    Also ist $\mathrm{Rad}_f \subseteq \mathrm{Rad}_{\tilde{f}}$. Da die umgekehrte Inklusion natürlich genauso gilt, folgt $\mathrm{Rad}_{\tilde{f}} = \mathrm{Rad}_f$.

11. Bei einer affinen Transformation im Bildraum bleibt das Radikal trivialerweise ungeändert. Zusammengenommen folgt:

Satz 5 *Der Rang einer quadratischen Abbildung ist unter affinen Transformationen in Bild und Urbild invariant.*

Versuchen wir nun die Klassifikation der Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^q$ unter affinen Transformationen, also unter $GA(\mathbb{F}_2^2) \times GA(\mathbb{F}_2^q)$ – diese sind ja alle quadratisch. Jede solche Abbildung hat also die Gestalt

$$f(x_1, x_2) = a_{12}x_1x_2 + a_{11}x_1 + a_{22}x_2 + b$$

mit $a_{11}, a_{12}, a_{22}, b \in \mathbb{F}_2^q$.

Ist f affin, also $a_{12} = 0$, so ist $f - b$ linear, also $W := f(\mathbb{F}_2^n) - b$ ein Unterraum von $\mathbb{F}_2^q$. Ist $\mathrm{Dim}\, W = 0$, so f konstant $= b$. Ist $\mathrm{Dim}\, W = 1$, so ist mit $GL_q(\mathbb{F}_2)$, also einer linearen Transformation im Bild, $W = \mathbb{F}_2 e_1$ zu erreichen, ebenso $W = \mathbb{F}_2 e_1 + \mathbb{F}_2 e_2$ in Fall $\mathrm{Dim}\, W = 2$. Durch Verschiebung im Bildraum erreicht man außerdem $b = 0$.

Im Fall $\mathrm{Dim}\, W = 0$ ist f also auf die Nullabbildung 0 reduziert. Im Fall $\mathrm{Dim}\, W = 1$ reduziert man die erste Komponente von f weiter durch eine lineare Transformation im Urbild auf $f_1 = T_1$, im Fall $\mathrm{Dim}\, W = 2$ die ersten beiden auf $f_1 = T_1$, $f_2 = T_2$. Die Bahnen von affinen Abbildungen werden also durch die Normalformen

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} T_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} T_1 \\ T_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

repräsentiert, letztere nur im Fall $q \geq 2$.

Sei nun f nicht affin, also $a_{12} \neq 0$. Eine lineare Transformation im Bild bildet dann a_{12} auf den ersten kanonischen Basisvektor e_1 ab; f hat dann die Form

$$f(x_1, x_2) = \begin{pmatrix} x_1 x_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + a_{11}x_1 + a_{22}x_2 + b = \begin{pmatrix} f_1(x_1, x_2) \\ f_2(x_1, x_2) \end{pmatrix}$$

mit $f_1 \colon \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$ vom Grad 2 und $f_2 \colon \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^{q-1}$ affin. Eine Verschiebung im Bildraum $\mathbb{F}_2^q$ annulliert b.

Im Fall $f_2 = 0$ lässt sich f_1 mit einer linearen Transformation im Urbild nach Beispiel 5 in 1.5 auf die Gestalt T_1T_2 bringen.

Ist $q \geq 2$ und $f_2 \neq 0$, so bringen wir es auf die Gestalt (zeilenweise geschrieben) $(T_1, 0, \ldots, 0)$ oder , falls $q \geq 3$, auch $(T_1, T_2, 0, \ldots, 0)$.

Im ersten dieser Fälle hat f_1 die Gestalt $T_1T_2 + a_{11}T_1 + a_{22}T_2$. Ist $a_{11} = a_{22} = 1$, so bewirkt die Addition der ersten beiden Komponenten, also ein lineare Transformation des Bildraums, dass f_1 zu $T_1T_2 + T_2$ wird. Die affine Transformation $T_1 \mapsto T_1 + 1$ im Urbild macht daraus T_1T_2; der dadurch entstehende konstante Summand 1 in der zweiten Komponente wird wieder durch eine Verschiebung im Bild annulliert. Die Kette der eben durchgeführten Transformationen sah also auf den ersten beiden Komponenten so aus:

$$\begin{pmatrix} T_1T_2 + T_1 + T_2 \\ T_1 \end{pmatrix} \mapsto \begin{pmatrix} T_1T_2 + T_2 \\ T_1 \end{pmatrix} \mapsto \begin{pmatrix} T_1T_2 \\ T_1 + 1 \end{pmatrix} \mapsto \begin{pmatrix} T_1T_2 \\ T_1 \end{pmatrix}$$

In dieser Kette sind auch die Fälle $a_{11} = 0$, $a_{22} = 1$ sowie $a_{11} = a_{22} = 0$ enthalten, die daher keine neuen Bahnen ergeben.

Ist $a_{11} = 1$, $a_{22} = 0$, also $f_1 = T_1T_2 + T_1$, so landen wir durch die erste Transformation der Kette schon gleich am Endpunkt: also auch keine weitere Bahn.

Es bleibt der Fall $q \geq 3$, $f_2 = (T_1, T_2, 0, \ldots, 0)$. Durch Addition, je nach Bedarf, der Zeilen 2 und 3 zur ersten, also durch eine lineare Transformation im Bild, lässt sich dann f_1 auf die Gestalt T_1T_2 bringen.

Insgesamt haben wir also höchstens drei nicht-affine Bahnen, die durch

$$\begin{pmatrix} T_1T_2 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} T_1T_2 \\ T_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} T_1T_2 \\ T_1 \\ T_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

repräsentiert werden, wobei die zweite nur bei $q \geq 2$, die dritte nur bei $q \geq 3$ vorkommt.

Satz 6 (i) *Jede* BOOLE*sche Funktion* $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$ *ist unter affinen Transformationen äquivalent zu einer der Normalformen*

$$0, \quad T_1, \quad T_1T_2.$$

(ii) *Jede* BOOLE*sche Funktion* $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ *ist unter affinen Transformationen äquivalent zu einer der Normalformen (Komponenten in Zeilen angeordnet)*

$$(0,0), \quad (T_1,0), \quad (T_1,T_2), \quad (T_1T_2,0), \quad (T_1T_2,T_1).$$

(iii) *Jede* BOOLE*sche Funktion* $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^q$ *mit* $q \geq 3$ *ist unter affinen Transformationen äquivalent zu einer der Normalformen (Komponenten in Zeilen angeordnet)*

$$(0,\ldots,0), \quad (T_1,0,\ldots,0), \quad (T_1,T_2,0,\ldots,0),$$

$$(T_1T_2,0,\ldots,0), \quad (T_1T_2,T_1,0,\ldots,0), \quad (T_1T_2,T_1,T_2,0,\ldots,0).$$

(iv) *Es gibt in* $\mathcal{F}_2^q$ *genau zwei Äquivalenzklassen: die affinen Abbildungen und die (echt) quadratischen.*

1.7 Klassifikation der BOOLEschen quadratischen Formen

Definition 5 Eine **BOOLEsche quadratische Form** in n Variablen ist eine Funktion $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ vom algebraischen Grad 2 mit $f(0) = 0$.

(Der Zusammenhang mit dem üblichen Begriff einer quadratischen Form über einem beliebigen Körper entsteht dadurch, dass in $\mathbb{F}_2$ stets $x^2 = x$ gilt.)

(*Anmerkung:* Für quadratische Formen in Charakteristik 2 wird die Nichtausgeartetheit oft etwas schwächer als in 1.6 definiert.)

Bemerkungen

1. Die zu f gehörige symplektische Bilinearform

$$\beta_f : \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$$

ist gegeben durch $\beta_f(x,y) = f(x+y) - f(x) - f(y)$.

2. Geht man von der Koeffizientendarstellung in 1.6 aus und setzt man $a_{ij} = 0$ für $i > j$, so bilden die Koeffizienten a_{ij} eine $n \times n$-Matrix A mit

$$f(x) = x^t Ax \quad \text{für alle } x \in \mathbb{F}_2^n,$$

und es ist

$$\begin{aligned} \beta_f(x,y) &= f(x+y) - f(x) - f(y) \\ &= (x+y)^t A(x+y) - x^t Ax - y^t Ay \\ &= x^t Ay + y^t Ax = x^t(A + A^t)y. \end{aligned}$$

3. Für eine quadratische Form f ist $\mathrm{Rad}_f = \mathrm{Kern}(A + A^t)$:

$$u^t(A + A^t)x = 0 \quad \text{für alle } x \in \mathbb{F}_2^n \iff u^t(A + A^t) = 0$$

$$\iff (A + A^t)u = 0.$$

Also ist $\mathrm{Rang}\, f = \mathrm{Rang}(A + A^t)$.

4. Im Fall der Dimension $n = 1$ sind alle quadratischen Formen linear.

5. Satz 4 lässt sich hier verschärfen: Falls $f \circ h$ nicht sowieso schon 0 ist, lässt sich durch einen weiteren Basiswechsel noch erreichen, dass $f \circ h$ eine Koordinatenprojektion ist, also z. B. $\tilde{a}_{r+1,r+1} = 1$, $\tilde{a}_{ii} = 0$ für $i \geq r + 2$.

Damit ist gezeigt:

Satz 7 *Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ eine quadratische Form vom Rang $r \leq n-1$. Dann gibt es ein $h \in GL_n(\mathbb{F}_2)$, ein $a \in \mathbb{F}_2$ und eine nichtausgeartete quadratische Form $g\colon \mathbb{F}_2^r \longrightarrow \mathbb{F}_2$, so dass*

$$f \circ h(x_1, \ldots, x_n) = g(x_1, \ldots, x_r) + a x_{r+1}$$

für alle $x \in \mathbb{F}_2^n$, und $\mathrm{Rad}_{f\circ h}$ wird von $e_{r+1}, \ldots, e_n$ aufgespannt.

Definition 6 Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ eine quadratische Form. Ein **hyperbolisches Paar** (u, v) für f ist ein Paar von Vektoren $u, v \in \mathbb{F}_2^n$ mit $f(u) = f(v) = 0$, $f(u + v) = 1$ (also $\beta_f(u, v) = 1$).

Hilfssatz 2 *Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ eine quadratische Form und $u \in \mathbb{F}_2^n - \mathrm{Rad}_f$ ein Vektor mit $f(u) = 0$. Dann gibt es einen Vektor $v \in \mathbb{F}_2^n$, so dass (u, v) ein hyperbolisches Paar für f ist.*

Beweis. Es gibt v mit $\beta_f(u, v) \neq 0$, also $= 1$. Falls $f(v) = 0$, sind wir fertig. Andernfalls sei $w := u + v$. Dann ist

$$\beta_f(u, w) = \beta_f(u, u + v) = f(v) + f(u) + f(u + v) = \beta_f(u, v) = 1,$$

$$f(w) = f(u + v) = \beta_f(u, v) + f(u) + f(v) = 1 + 0 + 1 = 0,$$

also (u, w) hyperbolisches Paar für f. $\diamond$

Welche BOOLEschen quadratischen Formen gibt es im Fall der Dimension $n = 2$?

a) Die linearen.

b) Ist f nichtlinear, so

$$f(x) = a_{11}x_1 + a_{22}x_2 + a_{12}x_1x_2 \quad \text{mit } a_{12} = \beta_f(e_1, e_2) = 1.$$

Insbesondere ist f nichtausgeartet. Ist $f(e_1) = 0$ oder $f(e_2) = 0$, so findet man ein hyperbolisches Paar für f, also eine Transformation $h \in GL_n(\mathbb{F}_2)$ mit $f \circ h = T_1T_2$ in algebraischer Normalform.

Es bleibt der Fall $f(e_1) = f(e_2) = 1$. Dann ist

$$f(e_1 + e_2) = \beta_f(e_1, e_2) + f(e_1) + f(e_2) = 1,$$

und wir sind im „anisotropen“ Fall

$$f = T_1 + T_2 + T_1T_2.$$

Damit ist die Klassifikation unter linearen Transformationen aus Beispiel 5 in 1.5 auf andere Weise hergeleitet.

Sei nun $n \geq 3$ und f nichtlineare quadratische Form. Der Unterraum $U \subseteq \mathbb{F}_2^n$ sei direktes Komplement zu Rad_f, so dass f auf U nichtausgeartet ist, insbesondere $\mathrm{Dim}\, U = r \geq 2$. Sei $u \in U - \{0\}$ beliebig gewählt. Dann ist $f(u) = 0$ oder 1. Im zweiten Fall wählen wir im $(r-1)$-dimensionalen Unterraum $\{v \in U \mid \beta_f(u, v) = 0\}$ ein $v \neq 0$. Dann ist $f(v) = 0$ oder $f(u + v) = \beta_f(u, v) + f(u) + f(v) = 0$ – das klappt, außer wenn $r = 2$, also nur $v = u$ möglich ist. Also:

Hilfssatz 3 *Ist $n \geq 3$ und $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ eine nichtlineare quadratische Form vom Rang $r \geq 3$, so gibt es*

(i) *ein $u \in \mathbb{F}_2^n - \mathrm{Rad}_f$ mit $f(u) = 0$,*

(ii) *ein hyperbolisches Paar (u, v) für f.*

Sei nun (u, v) hyperbolisches Paar und $U := \mathbb{F}_2u + \mathbb{F}_2v = \{0, u, v, u + v\}$ der davon aufgespannte Unterraum, ferner

$$V = \{x \in \mathbb{F}_2^n \mid \beta_f(u, x) = \beta_f(v, x) = 0\}$$

der zu U bezüglich β_f orthogonale Unterraum. Dann ist $\mathrm{Dim}\, V \geq n - 2$ und $U \cap V = 0$, denn $u, v, u + v \notin V$. Also ist $\mathbb{F}_2^n = U \oplus V$ direkte Summe dieser beiden Unterräume.

Es gibt also einen Basiswechsel $h \in GL_n(\mathbb{F}_2)$, so dass

$$f \circ h(x) = x_1x_2 + g(x_3, \ldots, x_n)$$

mit einer quadratischen Form $g \colon \mathbb{F}_2^{n-2} \longrightarrow \mathbb{F}_2$. Durch Induktion folgt:

Satz 8 *Sei $f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ eine quadratische Form, die nicht linear ist. Dann gibt es eine lineare Transformation $h \in GL_n(\mathbb{F}_2)$, so dass $f \circ h$ in algebraischer Normalform eine der folgenden Gestalten hat:*

$(Q_I(m))$ $T_1T_2 + \cdots T_{2m-1}T_{2m}$ mit $1 \leq m \leq \frac{n}{2}$,

$(Q_{II}(m))$ $T_1T_2 + \cdots T_{2m-1}T_{2m} + T_{2m-1} + T_{2m}$ mit $1 \leq m \leq \frac{n}{2}$,

$(Q_{III}(m))$ $T_1T_2 + \cdots T_{2m-1}T_{2m} + T_{2m+1}$ mit $1 \leq m \leq \frac{n-1}{2}$.

Insbesondere ist $\mathrm{Rang}\, f = 2m$ *gerade.*

Unter affinen Transformationen in Bild und Urbild liegen $Q_I(m)$ und $Q_{II}(m)$ in derselben Bahn.

Die folgenden algebraischen Normalformen repräsentieren also jeweils ein vollständiges Vertretersystem der Bahnen von $GL_n(\mathbb{F}_2)$ auf den BOOLEschen Funktionen $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ vom Grad 2 mit $f(0) = 0$:

Beispiele

1. $n = 2$: T_1T_2, $T_1T_2 + T_1 + T_2$.
2. $n = 3$: T_1T_2, $T_1T_2 + T_1 + T_2$, $T_1T_2 + T_3$.
3. $n = 4$: Die gleichen wie bei $n = 3$ und zusätzlich $T_1T_2 + T_3T_4$, $T_1T_2 + T_3T_4 + T_3 + T_4$.
4. $n = 5$: Die gleichen wie bei $n = 3$ und zusätzlich $T_1T_2 + T_3T_4 + T_5$.

Im allgemeinen Fall sind es $\lfloor \frac{3n-1}{2} \rfloor$ solcher Bahnen.

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.*]

3 Approximation durch lineare Relationen

In diesem Abschnitt suchen wir nach verstecker Linearität einer Boolеschen Abbildung, indem wir nach Linearkombinationen der Output-Bits Ausschau halten, die von einer Linearkombination der Input-Bits linear abhängen – zumindest für einige Argumente.

3.1 Transformation von Indikatorfunktionen

Definition 1 Für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt $\vartheta_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$,

$$\vartheta_f(x,y) := \begin{cases} 1, & \text{wenn } y = f(x), \\ 0 & \text{sonst,} \end{cases}$$

Indikatorfunktion von f.

Bestimmen wir die Walsh-Transformation einer solchen; dabei kommt die Menge

$$L_f(u,v) := \{x \in \mathbb{F}_2^n \mid u \cdot x = v \cdot f(x)\}$$

vor, wo die Funktion $v \cdot f$ mit der durch u bestimmten Linearform übereinstimmt. Je größer die Menge $L_f(u,v)$, desto enger ist die „Approximation“ von f durch die Linearformen zu u und v.

$$\begin{aligned} \hat{\vartheta}_f(u,v) &= \sum_{x\in\mathbb{F}_2^n} \sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)(-1)^{u\cdot x+v\cdot y} \\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{u\cdot x+v\cdot f(x)} \\ &= \#L_f(u,v) - (2^n - \#L_f(u,v)). \end{aligned}$$

Damit ist gezeigt:

Satz 1 *Für eine* Boolesche *Abbildung* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *ist die* Walsh-*Transformation der Indikatorfunktion gegeben durch*

$$\hat{\vartheta}_f(u,v) = \sum_{x\in\mathbb{F}_2^n} (-1)^{u\cdot x+v\cdot f(x)} = 2\cdot \#L_f(u,v) - 2^n.$$

Insbesondere ist $-2^n \le \hat{\vartheta}_f \le 2^n$*, und alle Werte von* $\hat{\vartheta}_f$ *sind gerade.*

Die Herleitung des Satzes ergibt als Zwischenschritt:

Korollar 1 *Ist* $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ *die durch* v *definierte Linearform, so ist*

$$\hat{\vartheta}_f(u,v) = \hat{\chi}_{\beta\circ f}(u).$$

Definition 2 Für eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt die reellwertige Funktion $\hat{\vartheta_f} : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{R}$ (WALSH-) **Spektrum** von f. Das Maximum

$$\max_{(\mathbb{F}_2^n \times \mathbb{F}_2^q) - \{0\}} |\hat{\vartheta}_f|$$

heißt **Spektralradius** von f.

Man stellt sich das Spektrum $\hat{\vartheta}_f$ von f als $2^n \times 2^q$-Matrix vor, deren Zeilen mit $u \in \mathbb{F}_2^n$ und deren Spalten mit $v \in \mathbb{F}_2^q$ indiziert sind. Die Spalten sind nach dem Korollar 1 gerade die Spektren der BOOLEschen Funktionen $\beta \circ f$ für alle Linearformen $\beta \in \mathcal{L}_q$.

Bemerkungen

1. Da $L_f(0,0) = \mathbb{F}_2^n$, ist $\hat{\vartheta}_f(0,0) = 2^n$. Die obere Grenze in Satz 1 wird also für jedes f angenommen; die untere Grenze wird nur von geeigneten f angenommen.

2. Für $u \neq 0$ ist dagegen

$$\hat{\vartheta}_f(u,0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x} = 0.$$

Die erste Spalte des Spektrums, die „Spalte 0“, hat also die Gestalt $(2^n, 0, \ldots, 0)$.

Korollar 2 (Spaltensummen des Spektrums) *Ist $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ die durch v definierte Linearform, so ist*

$$\begin{aligned} \sum_{u \in \mathbb{F}_2^n} \hat{\vartheta}_f(u,v) &= \begin{cases} 2^n, & \textit{wenn } \beta \circ f(0) = 0, \\ -2^n & \textit{sonst,} \end{cases} \\ \sum_{u \in \mathbb{F}_2^n} \hat{\vartheta}_f(u,v)^2 &= 2^{2n}. \end{aligned}$$

Beweis. Das folgt aus Korollar 2 zur Umkehrformel in 2.2 bzw. aus Korollar 1 und der PARSEVAL-Gleichung (Satz 4 in 2.3). $\diamond$

Aus Satz 5 in 2.4 folgt ferner

$$\max |\hat{\vartheta}_f(\bullet, v)| = \max |\hat{\chi}_{\beta \circ f}| \geq 2^{n/2} \qquad \text{für jeden Vektor } v \in \mathbb{F}_2^q$$

mit Gleichheit genau dann, wenn $\beta \circ f$ krumm ist. Also:

Korollar 3 *Für den Spektralradius einer* BOOLE*schen Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ gilt*

$$\max_{(\mathbb{F}_2^n \times \mathbb{F}_2^q) - \{0\}} |\hat{\vartheta}_f| \geq 2^{\frac{n}{2}},$$

mit Gleichheit genau dann, wenn $\beta \circ f$ für jede Linearform $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$, krumm ist.

Definition 3 (NYBERG, EUROCRYPT 91) Eine Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt **krumm**, wenn ihr Spektralradius gleich $2^{n/2}$ ist.

Bemerkungen

3. Ist f bijektiv (also insbesondere $q = n$), so ist offensichtlich $\vartheta_{f^{-1}}(y,x) = \vartheta_f(x,y)$ für alle $x, y \in \mathbb{F}_2^n$. Die Menge

$$L_{f^{-1}}(v,u) = \{y \in \mathbb{F}_2^n \mid v \cdot y = u \cdot f^{-1}(y)\}$$

ist das Bild unter f von $L_f(u,v)$; insbesondere ist sie gleich groß. Daher ist auch

$$\hat{\vartheta}_{f^{-1}}(v,u) = \hat{\vartheta}_f(u,v)$$

für alle $u, v \in \mathbb{F}_2^n$. Das Spektrum $\hat{\vartheta}_{f^{-1}}$ ist also transponiert zum Spektrum $\hat{\vartheta}_f$.

4. Im Fall $q = 1$ ist $\hat{\chi}_f(u) = \hat{\vartheta}_f(u,1)$ nach Korollar 1 in 2.1. Insgesamt gilt im Fall $q = 1$ also:

$$\hat{\vartheta}_f(u,v) = \begin{cases} 2^n, & \text{wenn } u = 0,\ v = 0, \\ 0, & \text{wenn } u \neq 0,\ v = 0, \\ \hat{\chi}_f(u), & \text{wenn } v = 1. \end{cases}$$

5. Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ direkte Summe von $g\colon \mathbb{F}_2^r \longrightarrow \mathbb{F}_2^q$ und $h\colon \mathbb{F}_2^s \longrightarrow \mathbb{F}_2^q$. Dann ist für jede Linearform $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ auch $\beta \circ f = \beta \circ g \oplus \beta \circ h$. Es folgt

$$\hat{\vartheta}_f(u,v,w) = \hat{\chi}_{\beta\circ f}(u,v) = \hat{\chi}_{\beta\circ g}(u) \cdot \hat{\chi}_{\beta\circ h}(v) = \hat{\vartheta}_g(u,w) \cdot \hat{\vartheta}_h(v,w)$$

für alle $u \in \mathbb{F}_2^r, v \in \mathbb{F}_2^s, w \in \mathbb{F}_2^q$, wenn β die zu w gehörige Linearform ist.

6. Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ affin, also $f(x) = Ax + b$ mit $A \in M_{n,q}(\mathbb{F}_2)$ und $b \in \mathbb{F}_2^q$. Dann ist

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

und das ist der Kern der Linearform $u^t - v^t A$, falls $v^t b = 0$, und parallel dazu, falls $v^t b = 1$. Es gibt also die Fälle

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

Daraus folgt

$$\hat{\vartheta}_f(u,v) = 2 \cdot \#L_f(u,v) - 2^n = \begin{cases} 2^n, & \text{falls } v^t A = u^t \text{ und } v^t b = 0, \\ -2^n, & \text{falls } v^t A = u^t \text{ und } v^t b = 1, \\ 0, & \text{falls } v^t A \neq u^t. \end{cases}$$

Das Spektrum enthält also in jeder Spalte (d. h. bei konstantem v) genau einen Eintrag $\pm 2^n$ und sonst lauter Nullen.

7. Hat umgekehrt das Spektrum von f diese Gestalt, so $\beta \circ f$ affin für alle Linearformen $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$. Also ist f affin. Damit ist gezeigt:

Satz 2 *Die Abbildung $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist genau dann affin, wenn jede Spalte des Spektrums $\hat{\vartheta}_f$ von f genau einen Eintrag $\neq 0$ hat.*

Beispiele

1. Für $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, erhalten wir mit Bemerkung 4 das Spektrum

	$v =$	
$\hat{\vartheta}_f(u,v)$	0	1
$u = 00$	4	2
01	0	2
10	0	2
11	0	-2

2. Ebenso ergibt sich für $f \in \mathcal{F}_4$, gegeben durch das Polynom $T_1T_2+T_3T_4$, die Wertetabelle

$\hat{\vartheta}_f(u,v)$	$v=$ 0	1
$u=0000$	16	4
0001	0	4
0010	0	4
0011	0	−4
0100	0	4
0101	0	4
0110	0	4
0111	0	−4
1000	0	4
1001	0	4
1010	0	4
1011	0	−4
1100	0	−4
1101	0	−4
1110	0	−4
1111	0	4

3. Und für $f \in \mathcal{F}_3$, gegeben durch das Polynom $T_1T_2 + T_1T_3 + T_2T_3$:

$\hat{\vartheta}_f(u,v)$	$v=$ 0	1
$u=000$	8	0
001	0	4
010	0	4
011	0	0
100	0	4
101	0	0
110	0	0
111	0	−4

4. Ebenso erhalten wir die Werte für die Polynome $T_1 \cdots T_n$ und $(T_1+1)\cdots(T_n+1)$ aus den Beispielen 3 und 4 in 2.7.

5. Der „Halbaddierer“ ist die Abbildung $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ mit den Komponenten-Polynomen $f_1 = T_1T_2$ und $f_2 = T_1 + T_2$. Er ergibt die Wertetabellen

$\vartheta_f(x,y)$	$y=$ 00	01	10	11
$x=00$	1	0	0	0
01	0	1	0	0
10	0	1	0	0
11	0	0	1	0

$\hat{\vartheta}_f(u,v)$	$v=$ 00	01	10	11
$u=00$	4	0	2	−2
01	0	0	2	2
10	0	0	2	2
11	0	4	−2	2

6. Der „Volladdierer“ ist die Abbildung $f : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2^2$ mit den Komponenten-Polynomen $f_1 = T_1T_2 + T_1T_3 + T_2T_3$ und $f_2 = T_1 + T_2 + T_3$. Er ergibt die Wertetabellen

	$y =$			
$\vartheta_f(x,y)$	00	01	10	11
$x = 000$	1	0	0	0
001	0	1	0	0
010	0	1	0	0
011	0	0	1	0
100	0	1	0	0
101	0	0	1	0
110	0	0	1	0
111	0	0	0	1

	$v =$			
$\hat{\vartheta}_f(u,v)$	00	01	10	11
$u = 000$	8	0	0	-4
001	0	0	4	0
010	0	0	4	0
011	0	0	0	4
100	0	0	4	0
101	0	0	0	4
110	0	0	0	4
111	0	8	-4	0

Satz 3 *Für die Komposition zweier* Boole*scher Abbildungen* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, $h\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$ *gilt:*

$$\hat{\vartheta}_{h\circ f}(u,w) = \frac{1}{2^q} \cdot \sum_{v\in\mathbb{F}_2^q} \hat{\vartheta}_f(u,v)\hat{\vartheta}_h(v,w).$$

Beweis. Das ist eine einfache Umsummierung:

$$\begin{aligned}
\sum_{v\in\mathbb{F}_2^q} \hat{\vartheta}_f(u,v)\hat{\vartheta}_h(v,w) &= \sum_{v\in\mathbb{F}_2^q}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} (-1)^{u\cdot x+v\cdot f(x)+v\cdot y+w\cdot h(y)} \\
&= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} (-1)^{u\cdot x+w\cdot h(y)} \cdot \underbrace{\sum_{v\in\mathbb{F}_2^q} (-1)^{v\cdot[f(x)+y]}}_{\begin{cases} 2^q, & \text{falls } y = f(x), \\ 0 & \text{sonst,}\end{cases}} \\
&= 2^q \cdot \sum_{x\in\mathbb{F}_2^n} (-1)^{u\cdot x+w\cdot h(f(x))} \\
&= 2^q \cdot \hat{\vartheta}_{h\circ f}(u,w)
\end{aligned}$$

wie behauptet. $\diamond$

Bemerkungen

8. Ist $h \in GL(\mathbb{F}_2^q)$ eine lineare Transformation des Bildraums, so entsteht $\hat{\vartheta}_{h\circ f}$ aus $\hat{\vartheta}_f$ durch Multiplikation der Wertetabelle von rechts mit einer Permutationsmatrix.

9. Bei einer Verschiebung im Bildraum ändern sich einige Spalten des Spektrums im Vorzeichen: Für $b \in \mathbb{F}_2^q$ gilt

$$\begin{aligned} \vartheta_{f+b}(x,y) &= \vartheta_f(x, y-b), \\ \hat{\vartheta}_{f+b}(u,v) &= (-1)^{v\cdot b}\hat{\vartheta}_f(u,v). \end{aligned}$$

10. Ist $g \in GL(\mathbb{F}_2^n)$ eine lineare Transformation des Urbildraums, so entsteht $\hat{\vartheta}_{f\circ g}$ aus $\hat{\vartheta}_f$ durch Multiplikation des Spektrums von links mit einer Permutationsmatrix.

11. Bei einer Verschiebung im Urbildraum ändern sich einige Zeilen des Spektrums im Vorzeichen: Für $a \in \mathbb{F}_2^n$ und $g(x) = f(x+a)$ gilt

$$\begin{aligned} \vartheta_g(x,y) &= \vartheta_f(x+a, y), \\ \hat{\vartheta}_g(u,v) &= (-1)^{u\cdot a}\hat{\vartheta}_f(u,v). \end{aligned}$$

12. Insbesondere ist der Spektralradius und sein Quadrat $\max \hat{\vartheta}_f^2$ auf $\mathbb{F}_2^n \times \mathbb{F}_2^q - \{(0,0)\}$ invariant unter $GA(\mathbb{F}_2^n) \times GA(\mathbb{F}_2^q)$, also unter affinen Transformationen in Bild und Urbild.

3.2 Urbildzähler und balancierte Abbildungen

Bei der zu Bemerkung 2 in 3.1 analogen Gleichung für $\hat{\vartheta}_f(0,v)$, also die erste Zeile des Spektrums, kommt der **Urbildzähler** $\nu_f : \mathbb{F}_2^q \longrightarrow \mathbb{N}$,

$$\nu_f(y) := \#f^{-1}(y) = \#\{x \in \mathbb{F}_2^n \mid f(x) = y\} = \sum_{x\in\mathbb{F}_2^n} \vartheta_f(x,y),$$

vor:

$$\begin{aligned} \hat{\vartheta}_f(0,v) &= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)(-1)^{v\cdot y} \\ &= \sum_{y\in\mathbb{F}_2^q} \nu_f(y)(-1)^{v\cdot y} \\ &= \hat{\nu_f}(v). \end{aligned}$$

Durch Aufsummieren erhält man eine neue Erkenntnis:

$$\sum_{v\in\mathbb{F}_2^q} \hat{\vartheta}_f(0,v) = \sum_{v\in\mathbb{F}_2^q} \hat{\nu}_f(v) = 2^q \cdot \nu_f(0)$$

nach 2.2. Hierbei ist $\nu_f(0)$ die Anzahl der Nullstellen von f. Damit ist bewiesen:

Hilfssatz 1 *Für eine* BOOLE*sche Abbildung* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *gilt:*

$$\begin{aligned} \hat{\vartheta}_f(0, v) &= \hat{\nu}_f(v), \\ \sum_{v \in \mathbb{F}_2^q - \{0\}} \hat{\vartheta}_f(0, v) &= 2^q \cdot \nu_f(0) - 2^n. \end{aligned}$$

Übungsaufgabe. Zeige, dass für jedes $u \in \mathbb{F}_2^n$

$$\sum_{v \in \mathbb{F}_2^q} \hat{\vartheta}_f(u, v) = 2^q \cdot \sum_{x \in V(f)} (-1)^{u \cdot x}$$

ist, wobei $V(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 0\}$ die Nullstellenmenge von f ist.

Eine wichtige Eigenschaft BOOLEscher Abbildungen für kryptologische Anwendungen ist die Balanciertheit – unbalancierte Abbildungen ergeben eine ungleichmäßige Wahrscheinlichkeitsverteilung auf den Geheimtexten und bieten daher einen Ansatz für statistische Angriffe:

Definition 4 Eine Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt **balanciert**, wenn alle Urbildmengen $f^{-1}(y)$ für $y \in \mathbb{F}_2^q$ gleich groß sind.

Bemerkungen

1. f ist genau dann balanciert, wenn der Urbildzähler ν_f konstant ist.

2. Ist f balanciert, so muss f surjektiv sein, insbesondere $n \geq q$, und der Urbildzähler ist konstant $\nu_f = 2^{n-q}$; im Fall $n = q$ sind genau die bijektiven Abbildungen balanciert.

3. Nach Bemerkung 3 in 2.1 und Bemerkung 2 ist f genau dann balanciert, wenn $\hat{\nu}_f(0) = 2^n$ und $\hat{\nu}_f(v) = 0$ für $v \neq 0$, also nach Hilfssatz 1 genau dann, wenn

$$\hat{\vartheta}_f(0, v) = \begin{cases} 2^n & \text{für } v = 0, \\ 0 & \text{sonst.} \end{cases}$$

   Auf diese Weise hängt die Balanciertheit eng mit der ersten Zeile („Zeile 0“) des Spektrums zusammen.

4. Eine BOOLEsche *Funktion* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist balanciert, wenn sie die Werte 0 und 1 beide genau 2^{n-1}-mal annimmt; anders ausgedrückt, wenn ihre Wahrheitstafel genau 2^{n-1} Nullen enthält, also wenn $d(f, 0) = 2^{n-1}$ oder $\mathrm{wt}(f) = 2^{n-1}$. Wendet man Korollar 2 in 2.1 speziell auf die Linearform 0 an, so folgt, dass f genau dann balanciert ist, wenn $\hat{\chi}_f(0) = 0$.

5. Aus Hilfssatz 3 in 2.4 und der Tatsache, dass im Fall $n \geq 2$ die Zahl 2^{n-1} der Nullstellen einer balancierten Funktion gerade ist, folgt, dass sie den Grad $\leq n-1$ hat.

6. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ surjektiv linear, so ist f balanciert, denn die Gleichung $f(x) = 0$ beschreibt den Untervektorraum Kern f der Codimension q, wird also von genau 2^{n-q} Elementen erfüllt. Die anderen Urbildmengen sind die Nebenklassen von Kern f. Allgemeiner ist jede surjektive affine Abbildung balanciert.

7. Für $g \in \mathcal{G}_n, h \in \mathcal{G}_q$ und $\tilde{f} = \omega_{(g,h)} f$ gilt offensichtlich $\nu_{\tilde{f}}(y) = \nu_f(h^{-1}y)$: Beliebige Transformationen von $\mathbb{F}_2^n$ lassen den Urbildzähler ungeändert, Transformationen von $\mathbb{F}_2^q$ permutieren seine Werte.

8. Die Balanciertheit von f ist invariant unter Bijektionen von $\mathbb{F}_2^n$ und $\mathbb{F}_2^q$, also unter der gesamten Gruppe $\mathcal{G}_n \times \mathcal{G}_q$ aus Abschnitt 1.5.

9. Die Funktion $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, ist nicht balanciert, da sie drei Nullstellen hat. Nach Bemerkung 7 und 1.5, Beispiel 4, ist also keine der quadratischen Funktionen in $\mathcal{F}_2$ balanciert. Daher gibt es in $\mathcal{F}_2$ nur sechs balancierte Funktionen: die nichtkonstanten affinen.

10. Da es insgesamt 2^n Urbilder gibt, ist

$$\sum_{y \in \mathbb{F}_2^q} \nu_f(y) = 2^n.$$

11. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ eine *beliebige* BOOLEsche Funktion, so ist die einfache Erweiterung $\breve{f} : \mathbb{F}_2^{n+1} \longrightarrow \mathbb{F}_2$ balanciert. Denn da

$$\breve{f}(1, x_1, \ldots, x_n) = 1 + \breve{f}(0, x_1, \ldots, x_n),$$

werden die Werte 0 und 1 gleich oft angenommen.

12. Eine quadratische Form $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist genau dann balanciert, wenn f vom Typ $Q_{III}(m)$ ist, bzw. wenn $f|_{\mathrm{Rad}_f}$ nicht konstant ist.

Satz 4 (SEBERRY/ZHANG/ZHENG, EUROCRYPT 94) *Eine* BOOLE*sche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist genau dann balanciert, wenn für jede Linearform $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$, die Linearform $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ balanciert ist.*

Beweis. Wenn f balanciert ist, ist offensichtlich jede Komponentenfunktion $f_1, \ldots f_q : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ balanciert. Eine beliebige Linearform $\beta \neq 0$ lässt sich durch einen linearen Automorphismus h von $\mathbb{F}_2^q$ auf die erste Koordinate abbilden; also ist $\beta \circ f$ ebenfalls balanciert.

Umgekehrt ist zu zeigen, dass der Urbildzähler $\nu_f = 2^{n-q}$ konstant ist.

Nach Bemerkung 4 und Korollar 1 zu Satz 1 ist für $v \in \mathbb{F}_2^q - \{0\}$ stets $\hat{\vartheta}_f(0,v) = \hat{\chi}_{v\cdot f}(0) = 0$. Da außerdem $\hat{\vartheta}_f(0,0) = 2^n$, folgt die Behauptung aus Bemerkung 3. $\diamond$

Korollar 1 *Ist* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *balanciert, so* $\operatorname{Grad} f \leq n-1$.

Beweis. Das gilt nach Bemerkung 5 für jede Komponentenfunktion. $\diamond$

Der nächste Satz drückt die Balanciertheit durch das Faltungsquadrat des Urbildzählers ν_f aus:

Satz 5 *Für eine Abbildung* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *sind äquivalent:*
(i) f *ist balanciert.*
(ii) $\nu_f * \nu_f = 2^{2n-q}$ *konstant.*
(iii) $\nu_f * \nu_f(0) = 2^{2n-q}$.

Beweis. „(i) $\Longrightarrow$ (ii)“ ist fast trivial:

$$\nu_f * \nu_f(v) = \sum_{y\in\mathbb{F}_2^q} \nu_f(y)\nu_f(v+y) = 2^q \cdot 2^{n-q} \cdot 2^{n-q} = 2^{2n-q}.$$

„(ii) $\Longrightarrow$ (iii)“ ist die Einschränkung auf einen Spezialfall.
„(iii) $\Longrightarrow$ (i)“: Es ist

$$\begin{aligned} 2^{2n-q} = \nu_f * \nu_f(0) &= \sum_{y\in\mathbb{F}_2^q} \nu_f(y)^2, \\ 2^n &= \sum_{y\in\mathbb{F}_2^q} \nu_f(y). \end{aligned}$$

Die Cauchy-Schwarz-Ungleichung ergibt

$$2^{2n} = \left[\sum_{y\in\mathbb{F}_2^q} 1\cdot\nu_f(y)\right]^2 \leq \sum_{y\in\mathbb{F}_2^q} 1^2 \cdot \sum_{y\in\mathbb{F}_2^q} \nu_f(y)^2 = 2^q \cdot 2^{2n-q}.$$

Die Gleichheit impliziert, dass $\nu_f(y)$ ein konstantes Vielfaches von 1, also konstant ist. $\diamond$

3.3 Krumme Abbildungen

Einige einfache Folgerungen aus der Definition 3 von krummen Abbildungen sind:

Bemerkungen

1. Nach den Korollaren zu Satz 1 ist $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ genau dann krumm, wenn

$$\hat{\vartheta}_f(u,v) = \pm 2^{n/2} \qquad \text{für alle } u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^q - \{0\},$$

   d. h., wenn das Spektrum (ausser in der ersten Spalte) nur die Werte $\pm 2^{n/2}$ annimmt.

2. Wenn eine krumme Abbildung existiert, muss n nach Korollar 1 zu Satz 5 in 2.4 gerade sein.

3. Wie im Fall $q = 1$ gilt auch allgemein: Ist f krumm und g affin, so ist $f + g$ krumm. Für jede Linearform $\beta \neq 0$ auf $\mathbb{F}_2^q$ ist nämlich $\beta \circ f$ krumm, $\beta \circ g$ affin und $\beta \circ (f + g) = \beta \circ f + \beta \circ g$.

4. Nach Bemerkung 12 in 3.1 ist die Eigenschaft „krumm“ invariant unter affinen Transformationen von Bild und Urbild.

5. Nach Satz 6 in 2.4 folgt auch allgemein für krumme Abbildungen, dass der algebraische Grad $\leq \frac{n}{2}$ ist.

6. Sie $f = g \oplus h$ direkte Summe. Dann ist f genau dann krumm, wenn alle $\beta \circ f$ krumm sind, also alle $\beta \circ g$ und $\beta \circ h$, also genau dann, wenn g und h krumm sind. (Nach Satz 9 in 2.8.)

Satz 6 (Nyberg, Eurocrypt 91) *Eine krumme Abbildung $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ existiert genau dann, wenn $n \geq 2q$ und gerade ist.*

Beweis. Es gebe eine krumme Abilsung f. Das Spektrum $\hat{\vartheta}_f$ nimmt für $v \neq 0$ nur die Werte $\pm 2^{n/2}$ an; sei

$$r := \#\{v \in \mathbb{F}_2^q - \{0\} \mid \hat{\vartheta}_f(0,v) = +2^{n/2}\}.$$

Für die Summe $S := \sum_{v \in \mathbb{F}_2^q - \{0\}} \hat{\vartheta}_f(0,v)$ folgt dann

$$S = 2^{n/2} \cdot [r - (2^q - 1 - r)] = 2^{n/2} \cdot [2r - 2^q + 1].$$

Andererseits ist nach dem Hilfssatz 1

$$S = 2^q \cdot \nu_f(0) - 2^n,$$

$$\nu_f(0) = \frac{S + 2^n}{2^q} = 2^{\frac{n}{2}-q} \cdot [2r - 2^q + 2^{n/2} + 1].$$

Da der Faktor in eckigen Klammern ungerade ist, kann $\nu_f(0)$ nur dann eine ganze Zahl sein, wenn $2^{\frac{n}{2}-q}$ ganz, also $\frac{n}{2} \geq q$ ist.

Für die umgekehrte Richtung nehmen wir $n = 2m \geq 2q$ gerade an. Der Vektorraum $\mathbb{F}_2^m$ wird mit einer passenden Multiplikation als Körper

$\mathbb{F}_{2^m}$ interpretiert. Seien $a_1, \ldots, a_q \in \mathbb{F}_2^m$ über $\mathbb{F}_2$ linear unabhängig. Die Komponenten $f_1, \ldots, f_q$ der Abbildung $f\colon \mathbb{F}_2^m \times \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^q$ werden dann so definiert:

$$f_i(x, y) = a_i x \cdot y \quad \text{für } x, y \in \mathbb{F}_2^m,$$

wobei das Produkt $a_i x$ im Körper $\mathbb{F}_{2^m}$ gebildet wird; das ist ein Spezialfall der MAIORANA-MCFARLAND-Konstruktion, Satz 7 in Abschnitt 2.4. Insbesondere sind die f_i krumme Funktionen. Ist nun $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ eine beliebige Linearform $\neq 0$ und $\beta(z) = b_1 z_1 + \cdots + b_q z_q$, so ist

$$\beta \circ f(x, y) = (b_1 a_1 + \cdots b_q a_q) x \cdot y$$

ebenfalls eine MAIORANA-MCFARLAND-Funktion, also krumm. $\diamond$

3.4 Das Linearitätsprofil

Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine BOOLEsche Abbildung. In Abschnitt 3.1 wurden für $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^q$ die Mengen $L_f(u, v)$ eingeführt. Nach dieser Definition und Satz 1 ist

$$\#L_f(u, v) = 2^n - d(\alpha, \beta \circ f) = 2^{n-1} + \frac{1}{2}\,\hat{\vartheta}_f(u, v),$$

wenn α und β die durch das Skalarprodukt mit u bzw. v definierten Linearformen sind. Als Bezeichnungen werden weiterhin verwendet:

$$\begin{aligned} p_f(u, v) &:= \frac{\#L_f(u, v)}{2^n} = 1 - \frac{d(\alpha, \beta \circ f)}{2^n} = \frac{1}{2} + \frac{\hat{\vartheta}_f(u, v)}{2^{n+1}}, \\ \lambda_f(u, v) &:= (2p_f(u, v) - 1)^2 = \frac{1}{2^{2n}} \cdot \hat{\vartheta}_f(u, v)^2. \end{aligned}$$

Definition 5 Die Funktion

$$\lambda_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{Q}$$

heißt **Linearitätsprofil** von f. Die Größen $p_f(u, v)$ und $\lambda_f(u, v)$ heißen **Wahrscheinlichkeit** bzw. **Potenzial** der linearen Relation $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^q$ für f.

Anmerkung. Die Verwendung des Quadrats bei der Definition des Linearitätsprofils wurde von MATSUI 1999 eingeführt und erweist sich als sehr sinnvoll. Nicht üblich, aber, wie sich zeigen wird, ebenfalls sinnvoll, ist die Normierung mit dem Faktor $\frac{1}{2^{2n}}$.

Bemerkungen

1. Es gilt stets
$$0 \leq \lambda_f(u,v) \leq 1,$$
$$p_f(u,v) = \frac{1 \pm \sqrt{\lambda_f(u,v)}}{2},$$
und nach Satz 1 in 3.1 sind alle Werte von λ_f ganzzahlige Vielfache von $\frac{1}{2^{2n-2}}$.

2. Für $v = 0$ gilt $v \cdot f(x) = u \cdot x$ genau dann, wenn x in der durch $u \cdot x = 0$ beschriebenen Hyperebene liegt. Also ist
$$\begin{aligned} \#L_f(u,0) &= \begin{cases} 2^n, & \text{wenn } u = 0, \\ 2^{n-1} & \text{sonst,} \end{cases} \\ p_f(u,0) &= \begin{cases} 1, & \text{wenn } u = 0, \\ \frac{1}{2} & \text{sonst,} \end{cases} \\ \lambda_f(u,0) &= \begin{cases} 1, & \text{wenn } u = 0, \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$
(„Erste Spalte“ des Linearitätsprofils; auch aus 3.1 klar.)

3. Alle „Spaltensummen“ des Linearitätsprofils sind 1:
$$\sum_{u \in \mathbb{F}_2^n} \lambda_f(u,v) = 1.$$
Das folgt aus Korollar 2 zu Satz 1 in 3.1. Insbesondere gibt es zu jedem $v \in \mathbb{F}_2^q$ ein $u \in \mathbb{F}_2^n$ mit $\lambda_f(u,v) \geq \frac{1}{2^n}$.

4. Ebenso folgt aus 3.1, dass die „erste Zeile“ des Linearitätsprofils aus den Einträgen $\hat{\nu}_f(v)^2/2^{2n}$ besteht, und aus 3.2 dass f genau dann balanciert ist, wenn diese Zeile die Form $10\ldots0$ hat. Ferner ist f genau dann krumm, wenn alle Spalten außer der ersten konstant $= \frac{1}{2^n}$ sind.

5. Ist f bijektiv, so folgt aus Bemerkung 3 in 3.1, dass
$$p_{f^{-1}}(v,u) = p_f(u,v), \qquad \lambda_{f^{-1}}(v,u) = \lambda_f(u,v)$$
für alle $u, v \in \mathbb{F}_2^n$. Insbesondere ist das Linearitätsprofil von f^{-1} (als Matrix geschrieben) das Transponierte des Linearitätsprofils von f. Ferner sind auch alle Zeilensummen des Linearitätsprofils einer bijektiven Abbildung f gleich 1; dieses ist also eine doppelt stochastische Matrix.

6. Ist $p_f(u,v) > \frac{1}{2}$, so wird durch das Skalarprodukt $u \cdot x$ die Parität von $v \cdot f(x)$ besser als durch bloßes Raten geschätzt, das mit Wahrscheinlichkeit $\frac{1}{2}$ das richtige Bit trifft. Im Falle $p_f(u,v) < \frac{1}{2}$ ist die Schätzung

schlechter als bloßes Raten, aber dann ergibt die Negation $u \cdot x + 1$ eine überzufällig gute Schätzung. Insgesamt ist eine lineare Relation (u, v) „nutzbar für die lineare Kryptoanalyse“, wenn $p_f(u, v) \neq \frac{1}{2}$, also wenn $\lambda_f(u, v) > 0$.

7. Die Relation $(0, 0)$ hat zwar die Wahrscheinlichkeit 1, ist aber natürlich „nutzlos“; sie sagt nichts über f aus.

8. Nach Bemerkung 12 in 3.1 ändert sich bei affiner Transformation in Bild und Urbild das Linearitätsprofil jeweils um eine Permutation der Spalten bzw. Zeilen.

9. Ist $f = g \oplus h$ direkte Summe, so

$$\lambda_f(x, y, z) = \frac{1}{2^{2n}} \cdot \hat{\vartheta}_f(x, y, z)^2 = \frac{1}{2^{2r}} \cdot \hat{\vartheta}_g(x, z)^2 \cdot \frac{1}{2^{2s}} \cdot \hat{\vartheta}_h(y, z)^2$$
$$= \lambda_g(x, z) \cdot \lambda_h(y, z)$$

für alle $x \in \mathbb{F}_2^r$, $y \in \mathbb{F}_2^s$, $z \in \mathbb{F}_2^q$.

Beispiele

1. Ist f linear, so gibt es zu jedem $v \in \mathbb{F}_2^q$ ein $u \in \mathbb{F}_2^n$ mit $\lambda_f(u, v) = 1$, nämlich den Vektor, der die Linearform $v \cdot f$ definiert. Die anderen Einträge $\lambda_f(u, v)$ dieser Zeile des Linearitätsprofils müssen dann 0 sein.

2. Ist f affin, so gibt es ebenfalls zu jedem $v \in \mathbb{F}_2^q$ ein $u \in \mathbb{F}_2^n$ mit $\lambda_f(u, v) = 1$: Ist $f(x) = Ax + b$, so

$$p_f(u, v) = \begin{cases} 1, & \text{falls } v^t A = u^t \text{ und } v^t b = 0, \\ 0, & \text{falls } v^t A = u^t \text{ und } v^t b = 1, \\ \frac{1}{2}, & \text{falls } v^t A \neq u^t, \end{cases}$$

$$\lambda_f(u, v) = \begin{cases} 1, & \text{falls } v^t A = u^t, \\ 0, & \text{falls } v^t A \neq u^t. \end{cases}$$

3. Umgekehrt folgt, wenn das Linearitätsprofil in jeder Spalte genau einen Wert $\neq 0$ hat, dass f affin sein muss, siehe Satz 2 in 3.1.

4. Für $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, ergibt sich das Linearitätsprofil am einfachsten aus der Gleichung $\lambda_f = \frac{1}{16} \hat{\vartheta}_f^2$:

$\lambda_f(u, v)$	0	1
00	1	$\frac{1}{4}$
01	0	$\frac{1}{4}$
10	0	$\frac{1}{4}$
11	0	$\frac{1}{4}$

5. Weitere Beispiele kann man ebenfalls direkt den Wertetabellen für $\hat{\vartheta}_f$ aus 3.1 entnehmen, so für den Volladdierer:

$\lambda_f(u,v)$	00	01	10	11
000	1	0	0	$\frac{1}{4}$
001	0	0	$\frac{1}{4}$	0
010	0	0	$\frac{1}{4}$	0
011	0	0	0	$\frac{1}{4}$
100	0	0	$\frac{1}{4}$	0
101	0	0	0	$\frac{1}{4}$
110	0	0	0	$\frac{1}{4}$
111	0	1	$\frac{1}{4}$	0

6. Für die „affinen Normalformen“ der Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ aus 1.5,

$$\binom{0}{0}, \binom{T_1}{0}, \binom{T_1}{T_2}, \binom{T_1T_2}{0}, \binom{T_1T_2}{T_2},$$

sind die Linearitätsprofile der Reihe nach:

	00	01	10	11
00	1	1	1	1
01	0	0	0	0
10	0	0	0	0
11	0	0	0	0

	00	01	10	11
00	1	1	0	0
01	0	0	0	0
10	0	0	1	1
11	0	0	0	0

	00	01	10	11
00	1	0	0	0
01	0	1	0	0
10	0	0	1	0
11	0	0	0	1

	00	01	10	11
00	1	1	$\frac{1}{4}$	$\frac{1}{4}$
01	0	0	$\frac{1}{4}$	$\frac{1}{4}$
10	0	0	$\frac{1}{4}$	$\frac{1}{4}$
11	0	0	$\frac{1}{4}$	$\frac{1}{4}$

	00	01	10	11
00	1	0	$\frac{1}{4}$	$\frac{1}{4}$
01	0	1	$\frac{1}{4}$	$\frac{1}{4}$
10	0	0	$\frac{1}{4}$	$\frac{1}{4}$
11	0	0	$\frac{1}{4}$	$\frac{1}{4}$

3.5 Das lineare Potenzial

Die Größe

$$\Lambda_f := \max\{\lambda_f(u,v) \mid u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^q, (u,v) \neq 0\}$$

bezeichnet das maximale Potenzial einer nichttrivialen linearen Relation. Je größer es ist, desto „näher“ an der Linearität ist f. Um „möglichst nichtlineare“ Abbildungen zu konstruieren, wird man also versuchen, Λ_f möglichst klein zu halten. Λ_f ist das Linearitätsmaß der linearen Kryptoanalyse.

Definition 6 Für eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt Λ_f das **lineare Potenzial** von f.

Bemerkungen

1. Es ist stets $0 \leq \Lambda_f \leq 1$. Ist f affin, so ist $\Lambda_f = 1$. Insbesondere ist im Fall $n = 1$, q beliebig, stets $\Lambda_f = 1$.

2. Es ist
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max_{(\mathbb{F}_2^n \times \mathbb{F}_2^q) - \{(0,0)\}} \hat{\vartheta}_f^2.$$
(Das lineare Potenzial ist das umnormierte Quadrat des Spektralradius.) Insbesondere ist Λ_f unter affinen Transformationen von Bild und Urbild invariant.

3. Im Fall $q = 1$ ist
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max \hat{\chi}_f^2.$$

4. Allgemein gilt für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$
$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max_{\beta \in \mathcal{L}_q - \{0\}} \hat{\chi}_{\beta \circ f}^2 = \max_{\beta \in \mathcal{L}_q - \{0\}} \Lambda_{\beta \circ f}.$$

5. Weiter gilt im Fall $q = 1$ für eine direkte Summe $f = g \oplus h$, dass
$$\lambda_f(x, y, a) = \lambda_g(x, a) \cdot \lambda_h(y, a)$$
für $x \in \mathbb{F}_2^r$, $y \in \mathbb{F}_2^s$, $a \in \mathbb{F}_2$. Also ist $\Lambda_f = \Lambda_g \cdot \Lambda_h$. (Die Verallgemeinerung auf höhere Dimensionen q des Bildraums klappt so nicht!)

6. Ist f bijektiv, so $\Lambda_{f^{-1}} = \Lambda_f$.

Aus Korollar 3 zu Satz 1 in 3.1 oder Bemerkung 3 in 3.4 folgt also:

Satz 7 (CHABAUD/VAUDENAY, EUROCRYPT 94) *Für jede* BOOLE*sche Abbildung* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *ist*
$$\Lambda_f \geq \frac{1}{2^n};$$
die Gleichheit gilt genau dann, wenn f *krumm ist.*

Die krummen Abbildungen sind also die „möglichst nichtlinearen“ Abbildungen bezüglich des Maßes Λ_f. Sie existieren allerdings höchstens im Fall $n \geq 2q$ gerade. Im Fall $q < n < 2q$ oder n ungerade ist die Minimierung von Λ_f komplizierter, z. T. sogar noch ein offenes Problem, siehe Kapitel 5.

Korollar 1 *Ist f nicht krumm und $n \geq 2$, so ist*

$$\Lambda_f \geq \frac{1}{2^n} + \frac{1}{2^{2n-2}}.$$

Insbesondere gilt das stets, wenn die Dimension n ungerade oder $n < 2q$ ist.

Beweis. Λ_f muss $> \frac{1}{2^n}$ und ganzzahliges Vielfaches von $\frac{1}{2^{2n-2}}$ sein. $\diamond$

Beispiele

1. Für $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2$, $f(x_1, x_2) = x_1 x_2$, ist $\Lambda_f = \frac{1}{4}$, da f krumm. Das passt auch zum Linearitätsprofil aus 3.4.

2. Wir betrachten die Abbildung

$$f : \mathbb{F}_2^3 \longrightarrow \mathbb{F}_2, \qquad f(x_1, x_2, x_3) = x_1 x_2 + x_1 x_2 x_3 + x_3$$

Die Wahrheitstafel von f und den 8 möglichen Linearformen zu den Vektoren $u \in \mathbb{F}_2^3$ sieht so aus:

		$u =$							
x	$f(x)$	000	001	010	011	100	101	110	111
000	0	0	0	0	0	0	0	0	0
001	1	0	1	0	1	0	1	0	1
010	0	0	0	1	1	0	0	1	1
011	1	0	1	1	0	0	1	1	0
100	0	0	0	0	0	1	1	1	1
101	1	0	1	0	1	1	0	1	0
110	1	0	0	1	1	1	1	0	0
111	1	0	1	1	0	1	0	0	1

Daraus ergeben sich Wahrscheinlichkeiten und Potenziale (hier „zu Fuß“ bestimmt, ohne Verwendung von ϑ_f):

$p_f(u,v)$	0	1
000	1	$\frac{3}{8}$
001	$\frac{1}{2}$	$\frac{7}{8}$
010	$\frac{1}{2}$	$\frac{5}{8}$
011	$\frac{1}{2}$	$\frac{5}{8}$
100	$\frac{1}{2}$	$\frac{5}{8}$
101	$\frac{1}{2}$	$\frac{5}{8}$
110	$\frac{1}{2}$	$\frac{3}{8}$
111	$\frac{1}{2}$	$\frac{3}{8}$

$\lambda_f(u,v)$	0	1
000	1	$\frac{1}{16}$
001	0	$\frac{9}{16}$
010	0	$\frac{1}{16}$
011	0	$\frac{1}{16}$
100	0	$\frac{1}{16}$
101	0	$\frac{1}{16}$
110	0	$\frac{1}{16}$
111	0	$\frac{1}{16}$

Das maximale Potenzial $\Lambda_f = \lambda_f(001, 1) = \frac{9}{16}$ ist also durch die dritte Koordinate gegeben: *Es gilt* $f(x_1, x_2, x_3) = x_3$ *mit Wahrscheinlichkeit* $\frac{7}{8}$. Insbesondere ist f nicht krumm.

3. Beim Halbaddierer und beim Volladdierer ist das lineare Potenzial 1, repräsentiert durch die 1 am Ende der zweiten Spalte des Linearitätsprofils. Das ist aber auch kein Wunder, da beide Abbildungen ja eine lineare Koordinatenfunktion haben: $T_1 + T_2$ bzw. $T_1 + T_2 + T_3$.

4. Ebenso ist für alle reduzierten Normalformen von Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ das lineare Potenzial 1. Daher ist 1 auch der kleinstmögliche Wert von Λ_f für *beliebige* Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$. Man sollte für Bitblock-Chiffren keine 2×2-S-Boxen verwenden.

5. Für alle drei Typen $Q_x(m)$ von quadratischen Formen folgt

$$\Lambda_f = \frac{1}{2^{2m}}.$$

Also gilt:

Satz 8 *Sei* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *quadratische Form vom Rang* r*. Dann ist das lineare Potenzial* $\Lambda_f = \frac{1}{2^r}$.

Ist $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine quadratische Abbildung, so ist für jede Linearform $\beta\colon \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ auch $\beta \circ f$ quadratisch. Sei $r_\beta := \operatorname{Rang} \beta \circ f$. Dann ist

$$\Lambda_f = \max_{\beta \in \mathcal{L}_q - \{0\}} \Lambda_{\beta \circ f} = \max_{\beta \in \mathcal{L}_q - \{0\}} \frac{1}{2^{r_\beta}} = \frac{1}{2^s}$$

mit $s := \min_\beta r_\beta$. Man beachte, dass $\operatorname{Rang} f = \max_\beta r_\beta$.

Satz 9 (i) *Ist* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *eine quadratische Abbildung, so*

$$\Lambda_f = \frac{1}{2^s}$$

mit $0 \le s \le \operatorname{Rang} f \le n$*. Ist* f *nicht krumm, so*

$$\Lambda_f \ge \frac{1}{2^{n-1}}.$$

(ii) *Ist* f *quadratisch und balanciert, so*

$$\Lambda_f \ge \begin{cases} \frac{1}{2^{n-1}} & \text{wenn } n \text{ ungerade,} \\ \frac{1}{2^{n-2}} & \text{wenn } n \text{ gerade.} \end{cases}$$

Beweis. (i) wurde oben gezeigt. (ii) folgt, weil nach Bemerkung 12 in 3.2 alle $\beta \circ f$ vom Typ $Q_{III}(m)$ sind, also insbesondere alle $r_\beta \le n-1$. Ist n gerade, so müssen sogar alle $r_\beta \le n-2$ sein. $\diamond$

3.6 Die Nichtlinearität BOOLEscher Abbildungen

Definition 7 (i) (PIEPRZYK/FINKELSTEIN 1988) Die **Nichtlinearität** einer BOOLEschen Funktion $f: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ ist die HAMMING-Distanz

$$\sigma_f := d(f, \mathcal{A}_n)$$

zum Unterraum der affinen Funktionen.

(ii) (NYBERG 1992) Für eine Abbildung $f : \mathbb{F}_2^n \longrightarrow F_2^q$ ist die **Nichtlinearität** definiert als

$$\sigma_f := \min\{\sigma_{\beta \circ f} \mid \beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2 \text{ affin}, \beta \neq 0\}.$$

Bemerkungen

1. σ_f ist invariant unter affinen Transformationen im Bild- und Urbildbereich, also unter $GA_n \times GA_q$.
2. $\sigma_f = \min\{d(\beta \circ f, \alpha) \mid \alpha \in \mathcal{A}_n, \beta \in \mathcal{A}_q - \{0\}\}$.

Hilfssatz 2 *Die Nichtlinearität einer* BOOLE*schen Funktion* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *ist*

$$\sigma_f = 2^{n-1} - \frac{1}{2} \max |\hat{\chi}_f|.$$

Beweis. Sei α die lineare, $\bar{\alpha}$ die nichtlineare affine Funktion zu $u \in \mathbb{F}_2^n$. Dann gilt nach Korollar 2 in 2.1

$$\begin{aligned} d(f, \alpha) &= 2^{n-1} - \frac{1}{2}\hat{\chi}_f(u), \\ d(f, \bar{\alpha}) &= 1 - d(f, \alpha) = 2^{n-1} + \frac{1}{2}\hat{\chi}_f(u), \\ d(f, \{\alpha, \bar{\alpha}\}) &= 2^{n-1} - \frac{1}{2}|\hat{\chi}_f(u)|. \end{aligned}$$

Daraus folgt die Behauptung. $\diamond$

Satz 10 *Die Nichtlinearität einer* BOOLE*schen Abbildung* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *ist*

$$\sigma_f = 2^{n-1} - \frac{1}{2} \max |\hat{\vartheta}_f|,$$

wobei das Maximum über $\mathbb{F}_2^n \times \mathbb{F}_2^q - \{(0,0)\}$ *gebildet wird.*

Beweis. Das folgt aus Hilfssatz 2 mit dem Korollar 1 in 3.1 und weil die Punkte $(u, 0)$ nichts am Maximum ändern. $\diamond$

Da das Linearitätsprofil $\lambda_f = \frac{1}{2^{2n}}\hat{\vartheta}_f^2$ ist, folgt daraus für das lineare Potenzial:

Korollar 1 (i) $\sigma_f = 2^{n-1} \cdot (1 - \sqrt{\Lambda_f}), \quad \Lambda_f = \left(1 - \frac{1}{2^{n-1}}\sigma_f\right)^2$.

(ii) (Meier/Staffelbach, Eurocrypt 89, im Fall $q = 1$)

$$\sigma_f \leq 2^{n-1} - 2^{\frac{n}{2}-1},$$

mit Gleichheit genau dann, wenn f krumm ist.

(iii) *Ist f bijektiv, so $\sigma_{f^{-1}} = \sigma_f$.*

Insbesondere ist die Nichtlinearität kein wirklich neues Maß. (In Wirklichkeit ist sie das ältere Maß.)

Da σ_f stets ganzzahlig sein muss, ergeben sich für kleine n folgende Schranken (die für beliebiges q gelten):

n	1	2	3	4	5	6	7	8	9
$\sigma_f \leq$	0	1	2	6	13	28	58	120	244

Daraus ergibt sich für $n = 3$ die schärfere untere Schranke $\Lambda_f \geq \frac{1}{4}$. Für $n = 5, 7, \ldots$ werden die entsprechend verschärften unteren Schranken $\frac{9}{256}, \frac{9}{1024}, \ldots$ zunehmend uninteressanter.

Ist n gerade und f nicht krumm, so haben wir entsprechend die Schranken

n	2	4	6	8
$\sigma_f \leq$	0	5	27	119
$\Lambda_f \geq$	1	$\frac{9}{64}$	$\frac{25}{1024}$	$\frac{81}{16384}$

Da $\chi_f(u) = \pm 2^{n/2}$, wenn f eine krumme Funktion ist, folgt aus dem Korollar 2 in 2.1:

Korollar 2 *Ist f krumme Funktion, α affin, so*

$$d(f, \alpha) = 2^{n-1} \pm 2^{\frac{n}{2}-1}.$$

Korollar 3 *Ist f krumme Funktion, so hat f genau $2^{n-1} \pm 2^{\frac{n}{2}-1}$ Nullstellen; insbesondere ist f nicht balanciert.*

Beweis. $d(f, 0) = 2^{n-1} \pm 2^{\frac{n}{2}-1} \neq 2^{n-1}$. $\diamond$

Korollar 4 *Ist n gerade, so gibt es eine balancierte Funktion $f \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ mit Nichtlinearität $\sigma_f = 2^{n-1} - 2^{\frac{n}{2}}$ und linearem Potenzial $\Lambda_f = \frac{1}{2^{n-2}}$.*

Beweis. Man nehme eine krumme Funktion und ändere sie an $2^{\frac{n}{2}-1}$ Stellen. Da dann

$$\Lambda_f = \left(1 - \frac{1}{2^{n-1}}\sigma_f\right)^2 = \left(1 - 1 + \frac{1}{2^{\frac{n}{2}-1}}\right)^2 = \frac{1}{2^{n-2}},$$

folgt auch die zweite Aussage. $\diamond$

Beispiele

1. Im Fall $n = 2$, $q = 1$, $f(x_1, x_2) = x_1x_2$, ist $\sigma_f = 2 - 1 = 1$, da f krumm.
2. Im Fall $n = 3$, $f = T_1T_2T_3 + T_1T_2 + T_3$, ist $\sigma_f = 1$.
3. Ist $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form vom Rang r, so

$$\sigma_f = 2^{n-1} \cdot (1 - \frac{1}{2^{r/2}}) = 2^{n-1} - 2^{n-\frac{r}{2}-1}.$$

Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ direkte Summe (siehe 2.8) von $g : \mathbb{F}_2^r \longrightarrow \mathbb{F}_2$ und $h\colon \mathbb{F}_2^s \longrightarrow \mathbb{F}_2$, so ist

$$\begin{aligned} 2^n - 2\sigma_f &= \max|\hat{\chi}_f| = \max|\hat{\chi}_g| \cdot \max|\hat{\chi}_h| = (2^r - 2\sigma_g)(2^s - 2\sigma_h) \\ &= 2^n - 2^r \cdot 2\sigma_h - 2^s \cdot 2\sigma_g + 4\sigma_g\sigma_h. \end{aligned}$$

Korollar 5 *Ist f direkte Summe von g und h, so*

$$\begin{aligned} \sigma_f &= 2^s \cdot \sigma_g + 2^r \cdot \sigma_h - 2\sigma_g\sigma_h, \\ \sigma_f &\geq 2^r \cdot \sigma_h, \\ \sigma_f &\geq 2^s \cdot \sigma_g. \end{aligned}$$

Beweis. Die erste Aussage wurde in der Vorbemerkung gezeigt. Die Abschätzungen folgen, da etwa $2\sigma_g \leq 2^r$. $\diamond$

Bemerkungen

3. Ist f direkte Summe von g und h, und ist h affin, so $\sigma_h = 0$, also $\sigma_f = 2^s\sigma_g$.
4. Als Spezialfall der Bemerkung 3 folgt: Ist $\breve{f} : \mathbb{F}_2^{n+1} \longrightarrow \mathbb{F}_2$ einfache Erweiterung von $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$, so $\sigma_{\breve{f}} = 2\sigma_f$ und $\Lambda_{\breve{f}} = (1 - \frac{1}{2^n}2\sigma_f)^2 = \Lambda_f$.

Startet man für ungerade Dimension n mit einer krummen Funktion $g\colon \mathbb{F}_2^{n-1} \longrightarrow \mathbb{F}_2$, so folgt durch einfache Erweiterung von g:

Korollar 6 *Für jede ungerade Dimension n gibt es eine balancierte Funktion $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ mit $\sigma_f = 2^{n-1} - 2^{\frac{n-1}{2}}$, $\Lambda_f = \frac{1}{2^{n-1}}$.*

4 Approximation durch lineare Strukturen

Die zweite wichtige Methode, versteckte Linearität aufzudecken, beruht auf „linearen Strukturen“. Diese werden durch Differenzenrechnung entdeckt.

4.1 Lineare Strukturen

Definition 1 Für eine Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ und einen Vektor $u \in \mathbb{F}_2^n$ ist die **Differenzenabbildung** $\Delta_u f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ definiert durch

$$\Delta_u f(x) := f(x+u) - f(x) \qquad \text{für alle } x \in \mathbb{F}_2^n.$$

Hilfssatz 1 *Für $f, g \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ und $u \in \mathbb{F}_2^n$ gilt:*

(i) $\Delta_u(f+g) = \Delta_u f + \Delta_u g$,

(ii) $\operatorname{Grad} \Delta_u f \leq \operatorname{Grad} f - 1$.

Beweis. (i) ist trivial.

(ii) Man kann der Reihe nach o. B. d. A. annehmen: $q = 1$, $f = T^I$ Monom, $f = T_1 \cdots T_r$. Dann ist

$$\Delta_u f(x) = (x_1 + u_1) \cdots (x_r + u_r) - x_1 \cdots x_r$$

klar vom Grad $\leq r - 1$. $\diamond$

Korollar 1 *Ist f konstant, so $\Delta_u f = 0$ für alle $u \in \mathbb{F}_2^n$.*

Korollar 2 *Ist f affin, so $\Delta_u f$ konstant für alle $u \in \mathbb{F}_2^n$.*

Bemerkungen

1. $\Delta_{u+v} f(x) = f(x+u+v) - f(x) = f(x+u+v) - f(x+v) + f(x+v) - f(x) = \Delta_u f(x+v) + \Delta_v f(x)$.

2. (Produktregel) In der Situation

   $$\mathbb{F}_2^n \xrightarrow{(f,g)} \mathbb{F}_2^q \times \mathbb{F}_2^r \xrightarrow{\gamma} \mathbb{F}_2^s$$

   mit einer bilinearen Abbildung γ sei $h := \gamma \circ (f, g) \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^s$. Dann ist

   $$\begin{aligned}
   \Delta_u h(x) &= \gamma(f(x+u), g(x+u)) - \gamma(f(x), g(x)) \\
   &= \gamma(f(x+u), g(x+u)) - \gamma(f(x+u), g(x)) \\
   &+ \gamma(f(x+u), g(x)) - \gamma(f(x), g(x)) \\
   &= \gamma(f(x+u), g(x+u) - g(x)) + \gamma(f(x+u) - f(x), g(x)) \\
   &= \gamma(f(x+u), \Delta_u g(x)) + \gamma(\Delta_u f(x), g(x))
   \end{aligned}$$

3. Ist $g : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$ linear, so $\Delta_u(g \circ f) = g \circ \Delta_u f$.

Definition 2 (Evertse, Eurocrypt 87) Ein Vektor $u \in \mathbb{F}_2^n$ heißt **lineare Struktur** von $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, wenn $\Delta_u f$ konstant ist.

Bemerkungen

4. Ist f affin, so ist jeder Vektor eine lineare Struktur von f.

5. 0 ist stets eine lineare Struktur von f.

6. Mit u und v ist auch $u + v$ lineare Struktur wegen Bemerkung 1. Die linearen Strukturen von f bilden also einen Untervektorraum von $\mathbb{F}_2^n$. Auf diesem ist f affin. Insbesondere gilt in Bemerkung 4 auch die Umkehrung.

7. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine Abbildung mit $f(0) = 0$, so ist $u \in \mathbb{F}_2^n$ genau dann lineare Struktur von f, wenn $f(x + u) - f(x)$ konstant, etwa $= c \in \mathbb{F}_2^q$ ist. Da dann $c = f(u) - f(0) = f(u)$, ist u in diesem Fall genau dann lineare Struktur von f, wenn

$$f(x + u) = f(x) + f(u) \quad \text{für alle } x \in \mathbb{F}_2^n.$$

8. Falls $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form mit zugehöriger Bilinearform β_f ist, so ist u genau dann lineare Struktur, wenn $\beta_f(u, x) = f(x + u) - f(x) - f(u) = 0$ für alle x, also wenn $u \in \mathrm{Rad}_f$. Das Radikal ist also in diesem Fall der Vektorraum der linearen Strukturen von f, und seine Dimension ist $n - \mathrm{Rang}\, f$. Insbesondere ist nach dem Korollar 2 in 2.8 f genau dann krumm, wenn $\mathrm{Rad}_f = 0$, also wenn die Linearitätsdimension $= 0$ ist im Sinne der folgenden Definition.

Definition 3 Für eine Boolesche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ wird der Vektorraum der linearen Strukturen als das **Radikal** Rad_f bezeichnet, seine Dimension als **Linearitätsdimension** von f und seine Codimension als **Rang** von f, $\mathrm{Rang}\, f$.

Bemerkungen

9. Ist $f = g \oplus h$ direkte Summe, so ist (u, v) für $u \in \mathbb{F}_2^r$ und $v \in \mathbb{F}_2^s$ genau dann lineare Struktur von f, wenn u lineare Struktur von g und v lineare Struktur von h ist. Insbesondere ist

$$\mathrm{Rad}_f = \mathrm{Rad}_g \oplus \mathrm{Rad}_h\,.$$

4.2 Das Differenzenprofil

Für eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ und $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^q$ sei

$$D_f(u,v) := \{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = v\},$$

$$\delta_f(u,v) := \frac{1}{2^n} \# D_f(u,v).$$

Definition 4 (CHABAUD/VAUDENAY, EUROCRYPT 94) Die Funktion $\delta_f : \mathbb{F}_2^n \times \mathbb{F}_2^q \longrightarrow \mathbb{Q}$ heißt **Differenzenprofil** von f.

(Die Normierung mit dem Faktor $\frac{1}{2^n}$ erweist sich als zweckmäßig. In der Literatur wird die Matrix $\# D_f(u,v)$ auch als Differenzentabelle bezeichnet.)

Bemerkungen

1. Ist f affin, $f(x) = Ax + b$, so $\Delta_u f(x) = Au$, also

$$D_f(u,v) = \{x \in \mathbb{F}_2^n | Au = v\} = \begin{cases} \mathbb{F}_2^n, & \text{falls } Au = v, \\ \emptyset & \text{sonst,} \end{cases}$$

$$\delta_f(u,v) = \begin{cases} 1, & \text{falls } Au = v, \\ 0 & \text{sonst.} \end{cases}$$

   (Jede Zeile des Differenzenprofils enthält genau eine 1 und sonst nur Nullen.)

2. Es sind äquivalent:

$$\begin{aligned} u \text{ lineare Struktur von } f &\iff D_f(u,v) = \begin{cases} \mathbb{F}_2^n & \text{für ein } v, \\ \emptyset & \text{sonst,} \end{cases} \\ &\iff \delta_f(u,v) = \begin{cases} 1 & \text{für ein } v, \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

   (Die „Zeile u“ des Differenzenprofils ist 0 außer genau einem Eintrag 1.)

3. Für beliebiges f, aber $u = 0$ gilt

$$\delta_f(0,v) = \begin{cases} 1, & \text{falls } v = 0, \\ 0 & \text{sonst} \end{cases}$$

   („erste Zeile“ des Differenzenprofils).

4. $\sum_{v \in \mathbb{F}_2^q} \delta_f(u,v) = 1$ („Zeilensummen“ des Differenzenprofils). Insbesondere gibt es für jeden Vektor $u \in \mathbb{F}_2^n$ ein $v \in \mathbb{F}_2^q$ mit $\delta_f(u,v) \geq \frac{1}{2^q}$.

Damit ist klar:

Satz 1 *Für eine Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ sind äquivalent:*

(i) *f ist affin.*

(ii) *Jeder Vektor $u \in \mathbb{F}_2^n$ ist lineare Struktur von f.*

(iii) *Jede Zeile des Differenzenprofils enthält genau einen Eintrag $\neq 0$.*

Bemerkungen

5. $x \in D_f(u,v) \Leftrightarrow x + u \in D_f(u,v)$.

6. Alle Werte $\#D_f(u,v)$ sind gerade: Für $u = 0$ folgt das aus Bemerkung 3, sonst aus Bemerkung 5. Daher sind alle $\delta_f(u,v)$ ganzzahlige Vielfache von $\frac{1}{2^{n-1}}$.

7. Was passiert bei Addition eines konstanten Vektors im Bild? Ist $g(x) = f(x) + b$, so $g(x+u) = f(x+u) + b$ und $g(x) + v = f(x) + b + v$, also $D_g(u,v) = D_f(u,v)$, insbesondere $\delta_g = \delta_f$.

8. Was passiert bei Addition eines konstanten Vektors im Urbild? Ist $h(x) = f(x+a)$, so

$$\begin{aligned} D_h(u,v) &= \{x \mid h(x+u) = h(x) + v\} \\ &= \{y - a \mid f(y+u) = f(y) + v\} = D_f(u,v) - a, \end{aligned}$$

   insbesondere $\delta_h = \delta_f$.

9. Was passiert bei linearen Transformationen im Bildraum? Ist $h \in GL_q(\mathbb{F}_2)$, so ist

$$\begin{aligned} D_{h \circ f}(u,v) &= \{x \mid h \circ f(x+u) = h \circ f(x) + v\} \\ &= \{x \mid f(x+u) = f(x) + h^{-1}(v)\} = D_f(u, h^{-1}(v)), \end{aligned}$$

   insbesondere werden die Spalten von δ_f permutiert.

10. Was passiert bei linearen Transformationen im Urbildraum? Ist $g \in GL_n(\mathbb{F}_2)$, so ist

$$\begin{aligned} D_{f \circ g}(u,v) &= \{x \mid f \circ g(x+u) = f \circ g(x) + v\} \\ &= \{g^{-1}(y) \mid f(y + g(u)) = f(y) + v\} = g^{-1}(D_f(g(u), v), \end{aligned}$$

    insbesondere werden die Zeilen von δ_f permutiert.

Die letzten vier Bemerkungen zusammen zeigen:

Satz 2 *Das Differenzenprofil δ_f einer* Boole*schen Abbildung f wird unter beliebigen affinen Transformationen von Bild und Urbild permutiert.*

Bemerkungen

11. Ist f bijektiv, so ist die Menge

$$D_{f^{-1}}(v,u) = \{y \in \mathbb{F}_2^n \mid f^{-1}(y+v) = f^{-1}(y) + u\}$$

für beliebige $u, v \in \mathbb{F}_2^n$ das Bild unter f von $D_f(u,v)$. Insbesondere sind beide Mengen gleich groß, und es folgt

$$\delta_{f^{-1}}(v,u) = \delta_f(u,v).$$

Das Differenzenprofil von f^{-1} ist – als Matrix geschrieben – also transponiert zum Differenzenprofil von f; insbesondere sind auch alle Spaltensummen des Differenzenprofils von f gleich 1. Dieses ist also, wie das Linearitätsprofil, ebenfalls eine doppelt stochastische Matrix und hat in der ersten Spalte oben eine 1, dann lauter Nullen.

12. Im Fall $q = 1$ lässt sich die Autokorrelation nach ihrer Definition als

$$\kappa_f(x) = \delta_f(x,0) - \delta_f(x,1)$$

ausdrücken.

Beispiele

1. Im Fall $n = 2$, $q = 1$, $f(x_1, x_2) = x_1x_2$, ist

$$D_f(u,v) = \{(x_1,x_2) \mid u_2x_1 + u_1x_2 = u_1u_2 + v\}.$$

Daraus bestimmt man

$\#D_f(u,v)$	0	1
00	4	0
01	2	2
10	2	2
11	2	2

$\delta_f(u,v)$	0	1
00	1	0
01	$\frac{1}{2}$	$\frac{1}{2}$
10	$\frac{1}{2}$	$\frac{1}{2}$
11	$\frac{1}{2}$	$\frac{1}{2}$

2. Ist $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form mit zugehöriger Bilinearform β_f, so $\Delta_u f(x) = f(x+u) - f(x) = f(u) + \beta_f(x,u)$. Also gilt

$$x \in D_f(u,v) \Longleftrightarrow \Delta_u f(x) = v \Longleftrightarrow \beta_f(x,u) = v - f(u).$$

Falls $f(u) = v$, gilt also $x \in D_f(u,v) \iff \beta_f(x,u) = 0$, falls $f(u) \neq v$, ist $x \in D_f(u,v) \iff \beta_f(x,u) = 1$. Daher gilt im Fall $u \in \mathrm{Rad}_f$:

$$D_f(u,v) = \begin{cases} \mathbb{F}_2^n & \text{falls } v = f(u), \\ \emptyset & \text{sonst.} \end{cases}$$

Falls $u \notin \mathrm{Rad}_f$, ist $H := \{x \mid \beta_f(u,x) = 0\}$ ein 1-codimensionaler Unterraum von $\mathbb{F}_2^n$ und $\bar{H} = \{x \mid \beta_f(u,x) = 1\}$ die dazu parallele Hyperebene. Daher ist

$$D_f(u,v) = \begin{cases} H & \text{falls } v = f(u), \\ \bar{H} & \text{sonst.} \end{cases}$$

Für das Differenzenprofil folgt

$$\delta_f(u,v) = \begin{cases} 1, & \text{wenn } u \in \mathrm{Rad}_f \text{ und } v = f(u), \\ 0, & \text{wenn } u \in \mathrm{Rad}_f \text{ und } v \neq f(u), \\ \frac{1}{2} & \text{wenn } u \notin \mathrm{Rad}_f, \end{cases}$$

und für die Autokorrelation

$$\kappa_f(x) = \delta_f(x,0) - \delta_f(x,1) = \begin{cases} \pm 1 & \text{für } x \in \mathrm{Rad}_f \\ 0 & \text{sonst.} \end{cases}$$

3. Sei $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ quadratisch mit zugehöriger bilinearer Abbildung

$$\beta_f(x,y) = f(x+y) - f(x) - f(y) + f(0).$$

Dann ist

$$D_f(u,v) = \{x \mid f(x+u) - f(x) = v\} = \{x \mid \alpha_{f,u}(x) = v - f(u) + f(0)\}$$

mit der linearen Abbildung $\alpha_{f,u}\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, $\alpha_{f,u}(x) = \beta_f(x,u)$. Daher gilt

$$D_f(u,v) = \mathrm{Kern}\,\alpha_{f,u}, \quad \text{falls } v = f(u) - f(0);$$

ist allgemeiner $v - f(u) + f(0)$ im Bild von $\alpha_{f,u}$, so ist $D_f(u,v)$ eine Nebenklasse des Unterraums $\mathrm{Kern}\,\alpha_{f,u}$, ansonsten $D_f(u,v) = \emptyset$. Setzt man $s_u := \mathrm{Dim}\,\mathrm{Bild}\,\alpha_{f,u}$, so ist $1 \leq s_u \leq q$ und

$$\#D_f(u,v) = \begin{cases} 2^{n-s_u} & \text{falls } v - f(u) + f(0) \in \mathrm{Bild}(\alpha_{f,u}), \\ 0 & \text{sonst.} \end{cases}$$

4.3 Effiziente Berechnung des Differenzenprofils

Grundlage für die effiziente Berechnung von Differenzenprofilen ist der folgende Hilfssatz:

Hilfssatz 2 *Für jede* Boolesche *Abbildung* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *gilt*

$$\delta_f = \frac{1}{2^n}\vartheta_f * \vartheta_f.$$

Beweis. Das folgt aus der Gleichungskette

$$\begin{aligned}\vartheta_f * \vartheta_f(u,v) &= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q}\vartheta_f(x,y)\vartheta_f(x+u,y+v)\\ &= \sum_{x\in\mathbb{F}_2^n}\vartheta_f(x+u,f(x)+v)\\ &= \#\{x\in\mathbb{F}_2^n \mid f(x+u)=f(x)+v\}.\diamond\end{aligned}$$

Aus dem Faltungssatz folgt damit direkt

$$\hat{\delta}_f = \frac{1}{2^n}\hat{\vartheta}_f^2 = 2^n\lambda_f,$$

also:

Hauptsatz 1 *Das Differenzenprofil ist bis auf einen konstanten Faktor die* Walsh*-Transformierte des Linearitätsprofils:*

$$\lambda_f = \frac{1}{2^n}\hat{\delta}_f, \qquad \delta_f = \frac{1}{2^q}\hat{\lambda}_f.$$

Mit der Gleichung von Parseval folgt unmittelbar:

Korollar 1 *Für jede* Boolesche *Abbildung* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *gilt*

$$2^n \cdot \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q}\lambda_f(u,v)^2 = 2^q \cdot \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q}\delta_f(x,y)^2.$$

Korollar 2 *Zwei* Boolesche *Abbildungen* $\mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *haben genau dann das gleiche Linearitätsprofil, wenn sie das gleiche Differenzenprofil haben.*

Das Differenzenprofil der Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ lässt sich also nach folgendem Algorithmus berechnen, der das Linearitätsprofil als Zwischenergebnis liefert:

1. Bestimmung von $\hat{\vartheta}_f$.

2. Quadrieren $\omega := \hat{\vartheta}_f^2$, $\lambda_f = \frac{1}{2^{2n}} \cdot \omega$.

3. Rücktransformation $\delta_f = \frac{1}{2^q}\hat{\lambda}_f = \frac{1}{2^{2n+q}}\hat{\omega}$.

Der Aufwand, wenn man $\hat{\lambda}_f$ schon berechnet hat, besteht aus weiteren $3N \cdot {}^2\log(N)$ „elementaren Operationen“, insgesamt also im wesentlichen aus $6N \cdot {}^2\log(N)$ solchen Operationen plus N Quadrierungen, wobei $N = 2^{n+q}$ die Größe des Inputs ist.

Beispiele

1. Ist f durch das Polynom $T_1T_1 + T_3T_4$ gegeben, so

$$\omega(x,y) = \begin{cases} 256 & \text{für } x = 0,\ y = 0, \\ 0 & \text{für } x \neq 0,\ y = 0, \\ 16 & \text{für } y = 1, \end{cases}$$

$$\delta_f(u,v) = \begin{cases} 1 & \text{für } u = 0,\ v = 0, \\ 0 & \text{für } u = 0,\ v = 1, \\ \frac{1}{2} & \text{sonst.} \end{cases}$$

2. Ebenso folgt für $T_1T_2 + T_1T_3 + T_2T_3$:

$$\delta_f(u,v) = \begin{cases} 1 & \text{für } u = 0,\ v = 0 \text{ und für } u = 111,\ v = 1, \\ 0 & \text{für } u = 0,\ v = 1 \text{ und für } u = 111,\ v = 0, \\ \frac{1}{2} & \text{sonst.} \end{cases}$$

3. Für $T_1 \cdots T_n$ folgt

$$\delta_f(u,v) = \begin{cases} 1 & \text{für } u = 0,\ v = 0, \\ 0 & \text{für } u = 0,\ v = 1, \\ 1 - \frac{1}{2^{n-1}} & \text{für } u \neq 0,\ v = 0, \\ \frac{1}{2^{n-1}} & \text{für } u \neq 0,\ v = 1. \end{cases}$$

   Für $(T_1 + 1) \cdots (T_n + 1)$ ist das Ergebnis das gleiche.

4. Für die fünf Normalformen von Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ erhalten wir für δ_f der Reihe nach die Tabellen:

	00	01	10	11
00	1	0	0	0
01	1	0	0	0
10	1	0	0	0
11	1	0	0	0

	00	01	10	11
00	1	0	0	0
01	1	0	0	0
10	0	0	1	0
11	0	0	1	0

	00	01	10	11
00	1	0	0	0
01	0	1	0	0
10	0	0	1	0
11	0	0	0	1

	00	01	10	11
00	1	0	0	0
01	$\frac{1}{2}$	0	$\frac{1}{2}$	0
10	$\frac{1}{2}$	0	$\frac{1}{2}$	0
11	$\frac{1}{2}$	0	$\frac{1}{2}$	0

	00	01	10	11
00	1	0	0	0
01	0	$\frac{1}{2}$	0	$\frac{1}{2}$
10	$\frac{1}{2}$	0	$\frac{1}{2}$	0
11	0	$\frac{1}{2}$	0	$\frac{1}{2}$

5. Für den Volladdierer – siehe 3.1 – erhalten wir ebenso:

δ_f	00	01	10	11
000	1	0	0	0
001	0	$\frac{1}{2}$	0	$\frac{1}{2}$
010	0	$\frac{1}{2}$	0	$\frac{1}{2}$
011	$\frac{1}{2}$	0	$\frac{1}{2}$	0
100	0	$\frac{1}{2}$	0	$\frac{1}{2}$
101	$\frac{1}{2}$	0	$\frac{1}{2}$	0
110	$\frac{1}{2}$	0	$\frac{1}{2}$	0
111	0	0	0	1

Hilfssatz 3 *Für jede* BOOLE*sche Abbildung* $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *gilt*

$$\sum_{u\in\mathbb{F}_2^n} \delta_f(u,v) = \frac{1}{2^n}\nu_f * \nu_f(v)$$

für alle $v \in \mathbb{F}_2^q$.

Beweis. Durch Aufsummieren in Hilfssatz 2 folgt

$$\begin{aligned}
2^n \sum_{u\in\mathbb{F}_2^n} \delta_f(u,v) &= \sum_{u\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)\vartheta_f(u+x,v+y) \\
&= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q} \vartheta_f(x,y)\cdot\left[\sum_{u\in\mathbb{F}_2^n} \underbrace{\vartheta_f(u+x,v+y)}_{\nu_f(v+y)\text{-mal 1, sonst 0}}\right] \\
&= \sum_{y\in\mathbb{F}_2^q}\left[\sum_{x\in\mathbb{F}_2^n} \underbrace{\vartheta_f(x,y)}_{\nu_f(y)\text{-mal 1, sonst 0}}\right]\cdot\nu_f(v+y) \\
&= \sum_{y\in\mathbb{F}_2^q} \nu_f(y)\cdot\nu_f(v+y) \\
&= \nu_f * \nu_f(v).\diamond
\end{aligned}$$

Aus Hilfssatz 3 und Satz 5 in 3.2 folgt sofort die folgende Verallgemeinerung von Bemerkung 11 in 4.2:

Satz 3 (Zhang/Zheng, SAC '96) *Für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ sind folgende Aussagen äquivalent:*

(i) *f ist balanciert.*

(ii) $\sum_{u \in \mathbb{F}_2^n} \delta_f(u, v) = 2^{n-q}$ *für alle $v \in \mathbb{F}_2^q$ (alle „Spaltensummen" des Differenzenprofils).*

(iii) $\sum_{u \in \mathbb{F}_2^n} \delta_f(u, 0) = 2^{n-q}$ *(1. „Spaltensumme" des Differenzenprofils).*

4.4 Das differenzielle Potenzial

Definition 5 (Nyberg, Eurocrypt 93) Für eine Boolesche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt

$$\Omega_f := \max\{\delta_f(u, v) \mid u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^q, (u, v) \neq 0\}$$

differenzielles Potenzial von f.

Anmerkung. In der Literatur wird der maximale Eintrag der Differenzentabelle (außer bei $(0, 0)$) als differenzielle Uniformität bezeichnet.

Bemerkungen

1. Ω_f ist invariant unter affinen Transformationen von $\mathbb{F}_2^n$ und $\mathbb{F}_2^q$.

2. Wegen Bemerkung 4 in 4.2 folgt

$$\frac{1}{2^q} \leq \Omega_f \leq 1.$$

3. Die untere Grenze $\Omega_f = 2^{-q}$ wird genau dann angenommen, wenn für $u \neq 0$ alle $\delta_f(u, v) = 2^{-q}$ sind, d. h., wenn alle Differenzenabbildungen $\Delta_u f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ balanciert (3.2) sind. („Zeile u" des Differenzenprofils konstant.)

4. Hat f eine lineare Struktur $\neq 0$, d. h., ist $\mathrm{Rad}_f \neq 0$, so ist $\Omega_f = 1$.

5. Ist f bijektiv, so $\Omega_{f^{-1}} = \Omega_f$.

6. Da für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ alle Werte des Differenzenprofils δ_f stets Vielfache von $\frac{1}{2^{n-1}}$ sind, ist das differenzielle Potenzial $\Omega_f \geq \frac{1}{2^{n-1}}$.

Beispiele

1. Ist f affin, so $\Omega_f = 1$.
2. Im Fall $n = 2$, $q = 1$, $f(x_1, x_2) = x_1 x_2$, ist $\Omega_f = \frac{1}{2}$.
3. Im Falle einer quadratischen Abbildung folgt aus Beispiel 3 in 4.2 der folgende Satz:

Satz 4 (Seberry, Zhang, Zheng, Eurocrypt 94) *Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ eine quadratische Abbildung.*

(i) *Ist $\mathrm{Rad}_f \neq 0$, so ist $\Omega_f = 1$.*

(ii) *Ist f nichtausgeartet, so ist $\Omega_f = \frac{1}{2^s}$ mit $1 \leq s \leq q$, insbesondere $\Omega_f \leq \frac{1}{2}$. Dabei ist $s = q$ nur möglich, wenn $n = 2q$ und f krumm. In allen anderen Fällen, insbesondere, wenn f balanciert ist, gilt $1 \leq s \leq q-1$.*

Hilfssatz 4 *Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ quadratisch und bijektiv und $u \in \mathbb{F}_2^n - \{0\}$. Dann gibt es mindestens eine Linearform $\beta \in \mathcal{L}_n - \{0\}$, so dass $\beta \circ f$ den Vektor u als lineare Struktur hat.*

Beweis. Es ist $D_f(u, 0) = \emptyset$; insbesondere ist die Differenzenabbildung $\Delta_u f$ nicht balanciert. Also ist mindestens ein $\beta \circ \Delta_u f = \Delta_u(\beta \circ f)$ nicht balanciert. Da diese Differenzenfunktion aber affin ist, muss sie dann konstant sein. Das war zu zeigen. $\diamond$

Satz 5 (Seberry, Zhang, Zheng, Eurocrypt 94) *Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ eine bijektive quadratische Abbildung mit $\Omega_f = \frac{1}{2^{n-1}}$. Dann gilt*

(i) *Jeder Vektor $u \in \mathbb{F}_2^n - \{0\}$ ist lineare Struktur von $\beta \circ f$ für genau eine Linearform $\beta \in \mathcal{L}_n - \{0\}$.*

(ii) *Für jede Linearform $\beta \in \mathcal{L}_n - \{0\}$ hat die quadratische Funktion $\beta \circ f$ den Rang $n - 1$.*

(iii) *n ist ungerade.*

Beweis. (i) Nach Bemerkung 6 in 4.2 sind alle $\delta_f(u, v) = 0$ oder $\frac{1}{2^{n-1}}$. Die Differenzenabbildung $\Delta_u f$ nimmt also genau 2^{n-1} Werte an (jeweils doppelt).

Annahme: u ist für zwei verschiedene Linearformen β_1, β_2 lineare Struktur von $\beta_i \circ f$. Da über dem Grundkörper $\mathbb{F}_2$ zwei verschiedene Vektoren $\neq 0$ stets linear unabhängig sind, lassen sich β_1, β_2 zu einer Basis $\beta_1, \ldots, \beta_n$ von $\mathcal{L}_n$ ergänzen. Dann ist

$$g := \begin{pmatrix} \beta_1 \circ f \\ \vdots \\ \beta_n \circ f \end{pmatrix} = h \circ f \quad \text{mit } h \in GL_n(\mathbb{F}_2),$$

also $\Omega_g = \Omega_f = \frac{1}{2^{n-1}}$. Aber $\Delta_u g$ hat die ersten beiden Komponenten konstant, kann also höchstens 2^{n-2} veschiedene Werte annehmen: Widerspruch.

(ii) Nach (i) besteht eine bijektive Beziehung zwischen Vektoren $u \neq 0$ und Linearformen $\beta \neq 0$. Also hat umgekehrt $\beta \circ f$ für jedes $\beta \in \mathcal{L}_n - \{0\}$ genau eine lineare Struktur $\neq 0$. Also hat jedes $\beta \circ f$ den Rang $n-1$.

(iii) Da der Rang einer quadratischen Funktion nach Satz 8 in 1.7 stets gerade ist, muss n ungerade sein. $\diamond$

Korollar 1 *Sei $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ eine bijektive quadratische Abbildung. Dann ist $\Omega_f \geq \frac{1}{2^{n-1}}$, wenn n ungerade, und $\Omega_f \geq \frac{1}{2^{n-2}}$, wenn n gerade.*

Beweis. Die erste Aussage gilt nach Bemerkung 6 viel allgemeiner. Die zweite folgt, da Ω_f nicht $\frac{1}{2^{n-1}}$ sein kann. $\diamond$

Definition 6 (Nyberg, Eurocrypt 93) Eine Boolesche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt **perfekt nichtlinear**, wenn das differenzielle Potenzial den minimalen Wert $\Omega_f = 2^{-q}$ hat.

Bemerkungen

7. Das ist nach Bemerkung 3 in 4.1 und Satz 4 in 3.2 genau dann der Fall, wenn $\beta \circ f$ für jede Linearform $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$, $\beta \neq 0$ perfekt nichtlinear ist.

8. Perfekt nichtlineare Abbildungen $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ haben insbesondere keine linearen Strukturen $u \neq 0$.

Aus Bemerkung 3 folgt:

Satz 6 *Genau dann ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ perfekt nichtlinear, wenn das Differenzenprofil δ_f auf $(\mathbb{F}_2^n - \{0\}) \times \mathbb{F}_2^q$ konstant $= 2^{-q}$ ist.*

Beispiele

3. Für die fünf Normalformen von Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$ ist Ω_f der Reihe nach 1, 1, 1, $\frac{1}{2}$, $\frac{1}{2}$. Insbesondere ist $\frac{1}{2}$ der kleinstmögliche Wert für Abbildungen $\mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$.

4. Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form, so ist nach Beispiel 2 in 4.2

$$\Omega_f = \begin{cases} \frac{1}{2}, & \text{wenn Rang } f = n, \\ 1 & \text{sonst.} \end{cases}$$

4.5 Gute Diffusion

Definition 7 Eine BOOLEsche Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ hat **gute Diffusion** bezüglich $u \in \mathbb{F}_2^n$, wenn die Differenzenabbildung $\Delta_u f$ balanciert ist.

Bemerkungen

1. Im Fall $q = 1$ bedeutet das $f(x+u)-f(x) = 0$ oder 1 für jeweils genau 2^{n-1} Vektoren $x \in \mathbb{F}_2^n$. Bezeichnet man die Anzahl der Nullstellen der Differenzenfunktion mit

$$\eta_f(u) := \#\{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = 0\} = 2^n \delta_f(u, 0),$$

   so ist die gute Diffusion bezüglich u äquivalent zu $\eta_f(u) = 2^{n-1}$.

2. Für allgemeines q bedeutet die gute Diffusion, dass $\#D_f(u, v) = 2^{n-q}$ bzw. $\delta_f(u, v) = \frac{1}{2^q}$ für jedes $v \in \mathbb{F}_2^q$, dass also die „Zeile u“ des Differenzenprofils konstant ist.

3. Bezüglich 0 hat keine Abbildung gute Diffusion.

4. Affine Abbildungen haben für keinen Vektor u gute Diffusion.

5. Eine BOOLEsche Abbildung f ist genau dann perfekt nichtlinear, wenn sie gute Diffusion bezüglich *aller* Vektoren $u \in \mathbb{F}_2^n - \{0\}$ hat, wie im Beispiel $f(x_1, x_2) = x_1 x_2$.

Definition 8 (WEBSTER/TAVARES, CRYPTO 85) Eine BOOLEsche *Funktion* f erfüllt das **Lawinenkriterium** (SAC = ‘strict avalanche criterion’), wenn f gute Diffusion für alle kanonischen Basisvektoren hat.

Das bedeutet: Das „Umkippen“ eines Input-Bits ändert genau die Hälfte aller Werte von f.

Bemerkungen

6. Jede perfekt nichtlineare Funktion erfüllt das Lawinenkriterium.

Gute Diffusion einer BOOLEschen Funktion f lässt sich auch durch die Faltung der Charakter-Form χ_f mit sich selbst ausdrücken:

$$\chi_f * \chi_f(u) = 2^n \kappa_f(u) = 2^n[\delta_f(u, 0) - \delta_f(u, 1)] = 2\eta_f(u) - 2^n,$$

wobei κ_f die Autokorrelation ist. Also:

Hilfssatz 5 *Eine* Boolesche *Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ hat genau dann gute Diffusion bezüglich u, wenn*

$$\chi_f * \chi_f(u) = 0 \qquad bzw. \quad \kappa_f(u) = 0.$$

Genau dann ist u lineare Struktur von f wenn

$$\chi_f * \chi_f(u) = \pm 2^n \qquad bzw. \quad \kappa_f(u) = \pm 1.$$

Speziell für $u = 0$ folgt

$$\chi_f * \chi_f(0) = 2^n,$$

da $\eta_f(0) = 2^n$. Also ist f genau dann perfekt nichtlinear, wenn $\chi_f * \chi_f = \hat{1}$, die Punktmasse in 0, ist, oder wenn $(\hat{\chi}_f)^2 = \widehat{\chi_f * \chi_f} = 2^n$ konstant ist. Das war gerade die Definition einer krummen Funktion. Wir haben also gezeigt:

Korollar 1 (Dillon 1974) *Eine* Boolesche *Funktion f ist genau dann perfekt nichtlinear, wenn sie krumm ist.*

Korollar 2 *Falls es eine perfekt nichtlineare Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gibt, ist n gerade.*

Satz 7 (Nyberg, Eurocrypt 91) *Eine* Boolesche *Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist genau dann perfekt nichtlinear, wenn sie krumm ist.*

Beweis. Beide Eigenschaften sind jeweils äquivalent dazu, dass sie für alle Funktionen $\beta \circ f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gelten, wo $\beta : \mathbb{F}_2^q \longrightarrow \mathbb{F}_2$ eine beliebige Linearform $\neq 0$ ist. $\diamond$

Korollar 3 *Ist die Urbilddimension n ungerade, so $\Omega_f > \frac{1}{2^q}$. Ist zusätzlich $q \leq n-1$, so $\Omega_f \geq \frac{1}{2^q} + \frac{1}{2^{n-1}}$.*

Beweis. Die zweite Aussage folgt, weil Ω_f Vielfaches von $\frac{1}{2^{n-1}}$ sein muss und $\frac{1}{2^q} \geq \frac{1}{2^{n-1}}$. $\diamond$

Korollar 4 *Für $n \geq 3$ und $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^{n-1}$ ist $\Omega_f \geq \frac{1}{2^{n-2}}$.*

Beweis. Das folgt, weil f nicht perfekt nichtlinear sein kann wie bei Korollar 3. $\diamond$

Ein Maß für eine global „möglichst gute“ Diffusion einer Booleschen Funktion ist die **globale Autokorrelation**

$$\tau_f := \sum_{x \in \mathbb{F}_2^n} \kappa_f(x)^2 = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \hat{\kappa}_f(u)^2 = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^4,$$

wobei die Umformung auf der PARSEVAL-Gleichung und Korollar 4 zum Faltungssatz in 2.3 beruht. Insbesondere ist $\tau_f \geq \kappa_f(0)^2 = 1$, und wir wissen schon, dass f genau dann perfekt nichtlinear ist, wenn $\tau_f = 1$.

Weiter ist

$$\tau_f = \frac{1}{2^n} \sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^4 \quad \leq \quad \frac{1}{2^n} \left[\sum_{u \in \mathbb{F}_2^n} \hat{\chi}_f(u)^2 \right]^2 ,$$

da alle Summanden ≥ 0 sind, mit Gleichheit genau dann, wenn höchstens ein Summand > 0 ist. Also ist $\tau_f \leq 2^n$, und die Gleichheit gilt genau dann, wenn höchstens ein $\hat{\chi}_f(u)^2 > 0$ ist. Dieses eine muss dann gleich der gesamten Quadratsumme 2^{2n} sein, also $\hat{\chi}_f(u) = \pm 2^n$, also $L_f(u) = \emptyset$ oder $\mathbb{F}_2^n$, also $f(x) = u \cdot x + 1$ oder $f(x) = u \cdot x$ für alle x. Damit ist gezeigt:

Satz 8 *Für die globale Autokorrelation τ_f einer* BOOLE*schen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gilt:*

(i) $1 \leq \tau_f \leq 2^n$.

(ii) $\tau_f = 1 \Longleftrightarrow f$ *perfekt nichtlinear.*

(iii) $\tau_f = 2^n \Longleftrightarrow f$ *affin.*

(iv) *Ist f quadratische Form vom Rang r, so $\tau_f = 2^{n-r}$.*

(v) *Ist $f = g \oplus h$ direkte Summe, so $\tau_f = \tau_g \tau_h$.*

Beweis. Die vierte Aussage folgt, weil

$$\tau_f = \sum_{x \in \mathbb{F}_2^n} \kappa_f(x)^2 = \sum_{x \in \mathrm{Rad}_f} 1$$

nach Beispiel 2 in 4.2, die fünfte direkt aus $\kappa_f(x, y) = \kappa_g(x)\kappa_h(y)$. $\diamond$

Für die Berechnung zweckmäßig ist die folgende Formel:

$$\begin{aligned} \tau_f &= \sum_{x \in \mathbb{F}_2^n} \kappa_f(x)^2 = \sum_{x \in \mathbb{F}_2^n} [\delta_f(x,0) - \delta_f(x,1)]^2 \\ &= \sum_{x \in \mathbb{F}_2^n} \left([\delta_f(x,0) + \delta_f(x,1)]^2 - 4\delta_f(x,0)\delta_f(x,1) \right), \end{aligned}$$

also:

Hilfssatz 6 *Für die globale Autokorrelation τ_f einer* BOOLE*schen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gilt:*

$$\tau_f = 2^n - 4 \cdot \sum_{x \in \mathbb{F}_2^n} \delta_f(x,0)\delta_f(x,1).$$

4.6 Die Linearitätsdistanz

Sei

$$\mathcal{LS}_n := \{f : \mathbb{F}_2^n \to \mathbb{F}_2 \mid f \text{ hat lineare Struktur } \neq 0\}.$$

Das ist die Vereinigung der Untervektorräume zu fester linearer Struktur, aber im allgemeinen selbst kein Untervektorraum.

Definition 9 (Meier/Staffelbach, Eurocrypt 89) Für eine Boolesche Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ heißt die Hamming-Distanz

$$\rho_f := d(f, \mathcal{LS}_n)$$

die **Linearitätsdistanz** von f.

Bemerkungen

1. Die Linearitätsdistanz ist invariant unter affinen Transformationen.
2. $\rho_f = 0 \Leftrightarrow f \in \mathcal{LS}_n$.
3. Da $\mathcal{A}_n \subseteq \mathcal{LS}_n$, ist $\rho_f \leq \sigma_f$, die Nichtlinearität.

Wie groß ist ρ_f sonst? Zur Antwort hilft eine Zählung: Für einen festen Vektor $u \in \mathbb{F}_2^n$ lässt sich $\mathbb{F}_2^n$ in die beiden Mengen

$$\begin{aligned} D_f(u,0) &= \{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = 0\}, \\ D_f(u,1) &= \{x \in \mathbb{F}_2^n \mid \Delta_u f(x) = 1\} \end{aligned}$$

der Größen $n_0 = \eta_f(u) = 2^n \delta_f(u,0)$ und $n_1 = 2^n - \eta_f(u) = 2^n \delta_f(u,1)$ zerlegen.

Nehmen wir zunächst $n_0 \geq n_1$ an. Um f zu einer Funktion mit u als linearer Struktur zu machen, muss man mindestens $\frac{n_1}{2}$ Werte abändern, und damit schafft man es wirklich: Sei nämlich $D_f(u,1) = M_1' \cup M_1''$ irgendwie in zwei gleichgroße Mengen zerlegt mit $x \in M_1' \Leftrightarrow x + u \in M_1''$, $\#M_1' = \#M_1'' = \frac{n_1}{2}$; dann hat die Funktion

$$f'(x) := \begin{cases} f(x) + 1 & \text{für } x \in M_1', \\ f(x) & \text{sonst,} \end{cases}$$

den Vektor u als lineare Struktur:

$$\Delta_u f'(x) = f'(x+u) + f'(x) = \begin{cases} f(x+u) + f(x) & = 0 \quad \text{für } x \in M_0, \\ f(x+u) + f(x) + 1 & = 0 \quad \text{für } x \in M_1', \\ f(x+u) + 1 + f(x) & = 0 \quad \text{für } x \in M_1'', \end{cases}$$

und mit weniger Änderungen ist das nicht zu schaffen.

Falls $n_0 < n_1$, benötigt man analog $\frac{n_0}{2}$ Wertänderungen. Also ist die Distanz von f zu jeder Funktion g, die u als lineare Struktur hat,

$$d(f,g) \geq n_f(u) := \min\{\frac{n_0}{2}, \frac{n_1}{2}\} = 2^{n-1} \cdot \min\{\delta_f(u,0), \delta_f(u,1)\},$$

und für geeignetes g wird dieser Wert angenommen. Es folgt

$$\rho_f = \min\{n_f(u) \mid u \in \mathbb{F}_2^n - \{0\}\}.$$

Da stets $n_0 + n_1 = 2^n$, ist $n_f(u) \leq 2^{n-2}$. Damit ist gezeigt:

Satz 9 (Meier/Staffelbach, Eurocrypt 89) *Für die Linearitätsdistanz einer* Boole*schen Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ gilt*

$$\rho_f \leq 2^{n-2}.$$

Die Gleichheit ist äquivalent dazu, dass f perfekt nichtlinear ist.

Beweis der zweiten Aussage: In der obigen Zählung ist für jeden Vektor $u \in \mathbb{F}_2^n - \{0\}$ stets $n_0 = \delta_f(u,0) = n_1 = \delta_f(u,1) = 2^{n-1}$.$\diamond$

Es folgt weiter

$$\rho_f = 2^{n-1} \cdot \min\{\delta_f(u,v) \mid u \in \mathbb{F}_2^n - \{0\}, v \in \mathbb{F}_2\}.$$

Wird dieses Minimum in (u_0, v_0) angenommen, also $\rho_f = 2^{n-1} \cdot \delta_f(u_0, v_0)$, so ist $\delta_f(u_0, v_0 + 1) = 1 - \delta_f(u_0, v_0)$ maximal, also $= \Omega_f$. Gezeigt ist also:

Satz 10 *Die Linearitätsdistanz ρ_f einer* Boole*schen Funktion f lässt sich durch das differenzielle Potential Ω_f so ausdrücken:*

$$\rho_f = 2^{n-1} \cdot (1 - \Omega_f).$$

Auch die Linearitätsdistanz ist also kein neues Maß für die Nichtlinearität, auch hier gilt, dass sie historisch vor dem differenziellen Potenzial eingeführt wurde.

Ist $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ quadratische Form vom Rang r, so

$$\rho_f = \begin{cases} 2^{n-2}, & \text{wenn } r = n, \\ 0 & \text{sonst,} \end{cases}$$

passend dazu, dass f im ersten Fall krumm ist und im zweiten Fall stets eine lineare Struktur $\neq 0$ hat

5 Optimierung der Nichtlinearität

5.1 Der Hauptsatz über krumme Abbildungen

In diesem Abschnitt werden bereits bewiesene Aussagen über krumme Funktionen und Abbildungen zusammengefasst.

Hauptsatz 1 *Für eine* Boolesche *Funktion* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *sind folgende Aussagen äquivalent:*

(i) f *ist krumm, d. h.,* $\hat{\chi}_f^2 = 2^n$ *konstant.*

(ii) f *ist perfekt nichtlinear, d. h., die Differenzenfunktion* $\Delta_u f$ *ist für alle* $u \in \mathbb{F}_2^n - \{0\}$ *balanciert.*

(iii) *Das lineare Potenzial von* f *hat den kleinstmöglichen Wert* $\Lambda_f = 2^{-n}$.

(iv) *Die Nichtlinearität von* f *hat den größtmöglichen Wert* $\sigma_f = 2^{n-1} - 2^{\frac{n}{2}-1}$.

(v) *Das differenzielle Potenzial von* f *hat den kleinstmöglichen Wert* $\Omega_f = \frac{1}{2}$.

(vi) *Die Linearitätsdistanz von* f *hat den größtmöglichen Wert* $\rho_f = 2^{n-2}$.

Korollar 1 *Ist das der Fall, so gilt weiter:*

(i) n *ist gerade.*

(ii) f *hat keine linearen Strukturen* $\neq 0$.

(iii) f *hat genau* $2^{n-1} \pm 2^{\frac{n}{2}-1}$ *Nullstellen und ist nicht balanciert.*

(iv) f *erfüllt das Lawinenkriterium.*

Hauptsatz 2 *Für eine* Boolesche *Abbildung* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ *sind folgende Aussagen äquivalent:*

(i) f *ist krumm, d. h., für alle Linearformen* $\beta \neq 0$ *auf* $\mathbb{F}_2^q$ *ist* $\beta \circ f$ *krumme* Boolesche *Funktion.*

(ii) *Der Spektralradius ist* $\max_{(\mathbb{F}_2^n \times \mathbb{F}_2^q) - \{(0,0)\}} |\hat{\vartheta}_f| = 2^{n/2}$.

(iii) $\hat{\vartheta}_f^2$ *ist konstant* $= 2^n$ *auf* $\mathbb{F}_2^n \times (\mathbb{F}_2^q - \{0\})$.

(iv) *Das lineare Potenzial hat den kleinstmöglichen Wert* $\Lambda_f = 2^{-n}$.

(v) *Die Nichtlinearität von* f *hat den größtmöglichen Wert* $\sigma_f = 2^{n-1} - 2^{\frac{n}{2}-1}$.

(vi) *f ist perfekt nichtlinear, d. h., das differenzielle Potential hat den kleinstmöglichen Wert $\Omega_f = 2^{-q}$.*

(vii) *Das Differenzenprofil δ_f ist konstant $= 2^{-q}$ auf $(\mathbb{F}_2^n - \{0\}) \times \mathbb{F}_2^q$.*

Korollar 2 *Ist das der Fall, so gilt weiter:*

(i) *n ist gerade und $\geq 2q$.*

(ii) *f hat keine linearen Strukturen $\neq 0$.*

(iii) *f ist nicht balanciert.*

(iv) *Jede Koordinatenfunktion von f erfüllt das Lawinenkriterium.*

Korollar 3 *Eine balancierte Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ ist nicht perfekt nichtlinear, insbesondere ist das differenzielle Potenzial $\Omega_f > 2^{-q}$ und das lineare Potenzial $\Lambda_f > 2^{-n}$.*

Die krummen Abbildungen sind also im Fall n gerade $\geq 2q$ die optimal nichtlinearen Abbildungen bezüglich der Maße „lineares Potenzial“ und „differenzielles Potenzial“. Für andere Kombinationen der Dimensionen n und q von Urbild und Bild ist es wesentlich schwerer, die Minima der beiden Potenziale zu bestimmen; im folgenden werden einige Ergebnisse hergeleitet.

5.2 Die Schranke von Chabaud/Vaudenay

In diesem Abschnitt werden für weitere Dimensionen n und q Bedingungen für optimal nichtlineare Abbildungen hergeleitet. Er folgt (mit einigen Vereinfachungen) dem Artikel von Chabaud/Vaudenay, Eurocrypt 94. Nach Bemerkung 6 in 4.4 ist für jede Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ stets $\Omega_f \geq \frac{1}{2^{n-1}}$.

Definition 1 (Nyberg/Knudsen, Crypto 92) f heißt **fast perfekt nichtlinear**, wenn $\Omega_f = \frac{1}{2^{n-1}}$.

Bemerkungen

1. Da auch stets $\Omega_f \geq \frac{1}{2^q}$, kann eine fast perfekt nichtlineare Abbildung höchstens dann existieren, wenn $\frac{1}{2^{n-1}} \geq \frac{1}{2^q}$, also wenn $q \geq n - 1$.

2. Falls f fast perfekt nichtlinear ist, kann $\delta_f(x, y)$ für $x \neq 0$ nur die Werte 0 oder $\frac{1}{2^{n-1}}$ annehmen. Die entsprechende Zeile im Differenzenprofil enhält also 2^{n-1} Mal den Wert $\frac{1}{2^{n-1}}$ und $2^q - 2^{n-1}$ Mal den Wert 0. Ist $q = n - 1$, so ist f dann also auch perfekt nichtlinear.

3. Perfekt nichtlineare Abbildungen können, wie schon gezeigt, nur im Fall $n = 2q$ existieren. Daher können sowohl perfekt nichtlineare wie auch fast perfekt nichtlineare Abbildungen nur dann existieren, wenn $n = 2$ und $q = 1$. In diesem Fall fallen die beiden Eigenschaften zusammen. Für $n \geq 3$ scheidet die Möglichkeit $q = n - 1$ für fast perfekt nichtlineare Abbildungen dagegen aus.

Satz 1 *Im Fall $n \geq 3$ können fast perfekt nichtlineare Abbildungen höchstens für $q \geq n$ existieren.*

Bemerkungen

4. Es ist $2^{n-1}\delta_f(x,y)^2 \geq \delta_f(x,y)$ mit Gleichheit genau dann, wenn $\delta_f(x,y) = 0$ oder $\frac{1}{2^{n-1}}$. Die Gleichheit für alle $x \in \mathbb{F}_2^n - \{0\}$ und $y \in \mathbb{F}_2^q$ tritt also genau dann ein, wenn f fast perfekt nichtlinear ist. Es folgt

$$\begin{aligned}\sum_{x\in\mathbb{F}_2^n-\{0\}}\sum_{y\in\mathbb{F}_2^q}\delta_f(x,y)^2 &\geq \sum_{x\in\mathbb{F}_2^n-\{0\}}\sum_{y\in\mathbb{F}_2^q}\delta_f(x,y) = \sum_{x\in\mathbb{F}_2^n-\{0\}} 1\\ &= \frac{2^n-1}{2^{n-1}} = 2 - \frac{1}{2^{n-1}},\end{aligned}$$

   und die Gleichheit tritt genau dann ein, wenn f fast perfekt nichtlinear ist.

Als nächstes soll eine alternative untere Schranke für das lineare Potenzial Λ_f hergeleitet werden. Wir starten mit der Beobachtung:

Sind $x_1, \ldots, x_r \in \mathbb{R}$, alle $x_i \geq 0$, $M = \max\{x_1 \ldots, x_r\}$, so ist

$$\sum_{i=1}^{r} x_i^2 \leq M \cdot \sum_{i=1}^{r} x_i$$

mit Gleichheit genau dann, wenn alle $x_i = 0$ oder M sind. Daraus folgt die Abschätzung

$$\Lambda_f \geq \frac{\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q-\{0\}}\lambda_f(u,v)^2}{\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q-\{0\}}\lambda_f(u,v)}$$

mit Gleichheit genau dann, wenn alle $\lambda_f(u,v) = 0$ oder Λ_f für $v \neq 0$.

Definition 2 $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ heißt **fast krumm**, wenn f fast perfekt nichtlinear ist und für alle $(u,v) \neq (0,0)$ gilt $\lambda_f(u,v) = 0$ oder Λ_f.

Definition 3 Die Chabaud-Vaudenay-Schranke ist

$$CV(n,q) := \frac{2^{q+1}(2^n-1) + 2^n(2^q - 2^n)}{2^{2n}(2^q-1)}.$$

Satz 2 *Für $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ gilt*

$$\Lambda_f \geq CV(n,q).$$

Die Gleichheit gilt genau dann, wenn f fast krumm ist.

Beweis. Im Nenner der obigen Ungleichung ist

$$\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q-\{0\}}\lambda_f(u,v) = \sum_{v\in\mathbb{F}_2^q-\{0\}} 1 = 2^q - 1.$$

Im Zähler wird abgeschätzt:

$$\begin{aligned}
\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q-\{0\}}\lambda_f(u,v)^2 &= \sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^q}\lambda_f(u,v)^2 - \sum_{u\in\mathbb{F}_2^n}\lambda_f(u,0)^2 \\
&= \frac{2^q}{2^n}\cdot\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^q}\delta_f(x,y)^2 - 1 \\
&= \frac{2^q}{2^n}\cdot\sum_{x\in\mathbb{F}_2^n-\{0\}}\sum_{y\in\mathbb{F}_2^q}\delta_f(x,y)^2 + \frac{2^q-2^n}{2^n} \\
&\geq \frac{2^q}{2^n}\cdot\frac{2^n-1}{2^{n-1}} + \frac{2^q-2^n}{2^n}.
\end{aligned}$$

Zusammengenommen folgt:

$$\Lambda_f \geq \frac{1}{2^q-1}\cdot\left[\frac{2^q}{2^n}\cdot\frac{2^n-1}{2^{n-1}} + \frac{2^q-2^n}{2^n}\right],$$

und das ist schon die Behauptung. Die Aussage über die Gleichheit folgt aus den Vorbemerkungen. $\diamond$

Da nach der Definition fast krumme Abildungen erst recht fast perfekt nichtlinear sind, können die Eigenschaften „krumm“ und „fast krumm“ ebenfalls höchstens für $n = 2$ und $q = 1$ gleichzeitig vorkommen. In diesem Fall ist in der Tat die Chabaud-Vaudenay-Schranke $= \frac{1}{4}$, also „fast krumm“ zu „krumm“ äquivalent.

Korollar 1 *Falls eine fast krumme Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ existiert, die auch krumm ist, ist $n = 2$, $q = 1$.*

Korollar 2 *Falls eine fast krumme Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ existiert, die nicht krumm ist, ist $q \geq n$.*

Beispiele

1. Für beliebiges q ist

$$CV(1,q) = \frac{2^{q+1} \cdot 1 + 2 \cdot (2^q - 2)}{4 \cdot (2^q - 1)} = \frac{2^{q+2} - 4}{4 \cdot (2^q - 1)} = 1.$$

   Also ist $f : \mathbb{F}_2 \longrightarrow \mathbb{F}_2^q$ genau dann fast krumm, wenn $\Lambda_f = 1$. *Im Fall $n = 1$ sind also alle Abbildungen fast krumm und keine krumm.*

2. Im Fall $q = n$ ist

$$CV(n,n) = \frac{2^{n+1} \cdot (2^n - 1) + 2^n \cdot 0}{2^{2n} \cdot (2^n - 1)} = \frac{1}{2^{n-1}}.$$

   Damit ist gezeigt:

Korollar 3 *Die Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ ist genau dann fast krumm, wenn $\Lambda_f = \frac{1}{2^{n-1}}$.*

Die Existenz solcher Abbildungen wird im folgenden in einigen Fällen durch Beispiele bewiesen. Dabei sei $M_r = 2^r - 1$ die r-te MERSENNE-Zahl.

Beispiele

3. Nach Beispiel 4 in 3.5 gibt es keine fast krummen Abbildungen $f : \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$.

Hilfssatz 1 *Für alle n und q gilt*

$$CV(n,q) = \frac{1}{2^{2n}} \cdot \left[3 \cdot 2^n - 2 - 2 \cdot \frac{M_n M_{n-1}}{M_q} \right].$$

Beweis. Es ist

$$\begin{aligned} CV(n,q) &= \frac{2^{q+1}(2^n - 1) + 2^n(2^q - 2^n)}{2^{2n}(2^q - 1)} \\ &= \frac{1}{2^{2n}(2^q - 1)} \cdot \left[2^q 2^{n+1} - 2 \cdot 2^q + 2^{n+q} - 2^{2n} \right] \\ &= \frac{1}{2^{2n}(2^q - 1)} \cdot \left[(2^q - 1)(3 \cdot 2^n - 2) + 3 \cdot 2^n - 2 - 2^{2n} \right] \\ &= \frac{1}{2^{2n}} \cdot \left[3 \cdot 2^n - 2 - 2 \cdot \frac{(2^n - 1)(2^{n-1} - 1)}{2^q - 1} \right] \end{aligned}$$

wie behauptet. $\diamond$

Hilfssatz 2 [Lemma von CASSAIGNE] *Für $n \geq 2$ und $q \geq n+1$ ist M_q kein Teiler von $M_n M_{n-1}$.*

Beweis. Sei o. B. d. A. $q \leq 2n-1$. Der Ansatz

$$(2^q-1)2^{2n-1-q}-(3\cdot 2^{n-1}-2^{2n-1-q}-1) = 2^{2n-1}-3\cdot 2^{n-1}+1 = (2^n-1)(2^{n-1}-1)$$

ergibt dann die Division

$$M_n M_{n-1} = A \cdot M_q - B$$

mit (negativem) Rest, denn A und B sind ganzzahlig; zu zeigen ist noch: $0 < B < M_q$.

Da $q \geq n+1$, ist $0 < 2^{n-q} < 1$, also $2 < 3 - 2^{n-q} < 3$, also

$$2^n < 2^{n-1} \cdot (3 - 2^{n-q}) = B + 1 < 3 \cdot 2^{n-1} < 2^{n+1} \leq 2^q,$$

also $2^n \leq B \leq 2^q - 2 = M_q - 1$. $\diamond$

Anmerkung. Allgemeiner sagt ein Satz von K. Zsigmondy (*Zur Theorie der Potenzreste*, Monatshefte Mathematik 3 (1892), 265–284), dass jede Mersenne-Zahl M_r für $r \geq 2$ außer M_6 einen Primfaktor hat, der keine Mersenne-Zahl mit kleinerem Index teilt; er wurde unabhängig von E. Artin bewiesen (*The orders of the linear groups*, Communications on Pure and Applied Mathematics VIII(1955), 355–366). Daraus folgt das Lemma von Cassaigne direkt.

Satz 3 *Sei $n \geq 2$, und es gebe eine fast krumme Abbildung $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$, die nicht krumm ist. Dann ist n ungerade und $q = n$, und es gilt $\Lambda_f = \frac{1}{2^{n-1}}$.*

Beweis. Nach dem Korollar 2 zu Satz 2 ist $q \geq n$. Da eine fast krumme Abbildung f existiert, wird $\Lambda_f = CV(n,q)$ angenommen. Da $2^{2n}\Lambda_f$ stets ganzzahlig und Vielfaches von 4 ist, ist nach Hilfssatz 1 $M_q | M_n M_{n-1}$. Nach Hilfssatz 2 muss also sogar $q = n$ sein. Also ist $\Lambda_f = CV(n,n) = \frac{1}{2^{n-1}}$. Weiter muss $2^{2n}\Lambda_f = 2^{n+1}$ ein Quadrat sein; das geht nur, wenn n ungerade ist. $\diamond$

Mit der Konstruktion von fast krummen Abbildungen beschäftigt sich der nächste Abschnitt.

5.3 Potenzabbildungen

Sei $n \geq 2$. In diesem Abschnitt wird ausgenützt, dass der Vektorraum $\mathbb{F}_2^n$ eine Struktur als endlicher Körper $K = \mathbb{F}_{2^n}$ mit 2^n Elementen besitzt. Untersucht werden die Abbildungen

$$f_s\colon K \longrightarrow K, \quad f(x) = x^s,$$

für $s \in \mathbb{Z}$, siehe Anhang A.4. Insbesondere ist f_s für $s = 2^k+1$ und $k \leq n-1$ eine quadratische Abbildung.

Satz 4 *Ist $n \geq k+1$, so gibt es ein r mit $0 \leq r \leq n-1$, so dass f_{2^k+1} das lineare Potenzial $\Lambda_f = \frac{1}{2^r}$ hat.*

Beweis. Das folgt aus Satz 9 in 3.5. $\diamond$

Leichter als das lineare Potenzial lässt sich zunächst, zumindest im Fall $s = 3$, das differenzielle Potenzial bestimmen. Für (o. B. d. A.) $u \neq 0$ ist

$$\begin{aligned} D_f(u,v) &= \{x \in K \mid x^3 + x^2u + xu^2 + u^3 = x^3 + v\} \\ &= \{x \in K \mid x^2 + ux + (u^2 - \frac{v}{u}) = 0\} \\ &= \{x \in K \mid g_{uv}(x) = 0\} \end{aligned}$$

mit dem Polynom $g_{uv} = T^2 + uT + (u^2 - \frac{v}{u}) \in K[T]$. Da die Ableitung $g'_{uv} = u \neq 0$ konstant ist, sind alle Nullstellen einfach, d. h., $\#D_f(u,v) = 0$ oder 2, $\delta_f(u,v) = 0$ oder $\frac{1}{2^{n-1}}$, wobei beide Werte für festes u je 2^{n-1}-mal vorkommen müssen.

Damit ist gezeigt:

Satz 5 *Ist K ein endlicher Körper der Charakteristik 2 mit $\operatorname{Dim} K = n$, so hat die dritte Potenz $f\colon K \longrightarrow K$, $f(x) = x^3$, das differenzielle Potenzial*

$$\Omega_f = \frac{1}{2^{n-1}},$$

ist also fast perfekt nichtlinear.

Für die genauere Bestimmung der linearen Potenzials ist ein Ausflug in die Algebra angesagt; die nötigen Ergebnisse stehen im Anhang A.1 und A.3.

Zunächst betrachten wir die Spur der dritten Potenz,

$$g\colon K \longrightarrow \mathbb{F}_2, \quad g(x) = \operatorname{Tr}(x^3).$$

Dies ist eine quadratische Form, also ist wegen Satz 8 in 3.5 der Rang dieser quadratischen Form oder, äquivalent dazu, die Linearitätsdimension, also die Dimension des Radikals, zu bestimmen. Genau dann liegt $u \in \operatorname{Rad}_g$, wenn

$$\operatorname{Tr}((x+u)^3) - \operatorname{Tr}(x^3) - \operatorname{Tr}(u^3) = \operatorname{Tr}(x^2u) + \operatorname{Tr}(xu^2) = 0$$

für alle $x \in K$, also genau dann, wenn $\operatorname{Tr}(x^2u) = \operatorname{Tr}(xu^2) = \operatorname{Tr}(x^2u^4)$ für alle x (da die Spur unter dem FROBENIUS-Automorphismus $x \mapsto x^2$ invariant ist). Da x^2 mit x alle Elemente von K durchläuft, gilt also

$$\operatorname{Rad}_g = \{u \in K \mid u^4 = u\}.$$

Genauer lässt sich das mit einer Normalbasis $\{a, a^2, \ldots, a^{2^{n-1}}\}$ [siehe Anhang A.3] von K beschreiben. Ist

$$u = u_0 a + u_1 a^2 + \cdots + u_{n-1} a^{2^{n-1}},$$

so verschiebt das Quadrieren den Koeffizientenvektor zyklisch um 1 nach rechts, das Potenzieren mit 4 um 2, also

$$u^4 = u_{n-2} a + u_{n-1} a^2 + u_0 a^4 \cdots + u_{n-3} a^{2^{n-1}}.$$

Also ist $u^4 = u$ genau dann, wenn $u_0 = u_{n-2}$, $u_1 = u_{n-1}$, …; speziell für ungerades n müssen alle Koeffizienten gleich sein. Damit ist gezeigt:

Hilfssatz 3 *Für $g\colon K \longrightarrow \mathbb{F}_2$, $g(x) = \mathrm{Tr}(x^3)$, gilt*

(i) $\mathrm{Rad}_g = \{u \in K \mid u^4 = u\}$.

(ii) *Ist n gerade, so hat g die Linearitätsdimension 2, also den Rang $n-2$.*

(iii) *Ist n ungerade, so hat g die Linearitätsdimension 1, also den Rang $n-1$, und Rad_g wird von dem Vektor $u = a + a^2 + \cdots + a^{2^{n-1}}$ aufgespannt.*

Sei nun $\beta\colon K \longrightarrow \mathbb{F}_2$ eine beliebige Linearform $\neq 0$, also $\beta(y) = \mathrm{Tr}(by)$ für alle $y \in K$ mit einem festen $b \in K^\times$. Das Radikal der quadratischen Form $g_b(x) = \mathrm{Tr}(bx^3)$ besteht genau aus den $u \in K$ mit $\mathrm{Tr}(bux^2) = \mathrm{Tr}(bu^2x) = \mathrm{Tr}(b^2u^4x^2)$ für alle $x \in K$, also mit $bu^4 = u$. Die 0 liegt natürlich immer in $\mathrm{Rad}\, g_b$. Für $u \neq 0$ heißt die Bedingung $u^3 = \frac{1}{b}$. Ist also b keine dritte Potenz, so ist $\mathrm{Rad}\, g_b = 0$. Ist $b = c^3$ dagegen eine dritte Potenz, so $\beta \circ f(x) = \mathrm{Tr}(bx^3) = \mathrm{Tr}((cx)^3)$ für alle $x \in K$, also $\mathrm{Rang}\, g_b = \mathrm{Rang}\, g$.

Genau dann, wenn n ungerade ist, ist jedes $b \in K$ eine dritte Potenz. Damit ist gezeigt:

Hauptsatz 3 *Sei K ein endlicher Körper der Charakteristik 2 mit $\mathrm{Dim}\, K = n$ und $f\colon K \longrightarrow K$, $f(x) = x^3$, die dritte Potenz.*

(i) *Ist n ungerade, so ist f bijektiv und hat das lineare Potenzial*

$$\Lambda_f = \frac{1}{2^{n-1}}$$

sowie die Nichtlinearität

$$\sigma_f = 2^{n-1} - 2^{\frac{n-1}{2}},$$

ist also fast krumm.

(ii) *Ist n gerade, so hat f das lineare Potenzial*

$$\Lambda_f = \frac{1}{2^{n-2}}$$

sowie die Nichtlinearität

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

5.4 Die Inversionsabbildung

Sei $n \geq 2$ und $K = \mathbb{F}_{2^n}$. Für $s = -1$ ist die Potenzabbildung $f_{-1} = f_{2^n-2}$ die Inversionsabbildung

$$f_{-1}\colon K \longrightarrow K, \quad f_{-1}(x) = \begin{cases} x^{-1} & \text{für } x \neq 0, \\ 0 & \text{für } x = 0, \end{cases}$$

siehe Anhang A.4. Sie ist involutorisch, also ihre eigene Umkehrabbildung, insbesondere bijektiv. Nach Satz 6 in A.4 ist (da $n \geq 2$)

$$\operatorname{Grad} f_{-1} = \operatorname{Grad} f_{2^n-2} = \operatorname{wt}(2^n - 2) = n - 1,$$

denn $2^n - 2$ hat die Binärdarstellung

$$2^{n-1} + \cdots + 2^2 + 2.$$

[Im Fall $n = 1$ ist f_{-1} die identische Abbildung auf $\mathbb{F}_2$, also linear, also vom Grad 1.] Nach Korollar 1 zu Satz 4 in 3.2 ist $n - 1$ der maximal mögliche Grad einer Bijektion $K \longrightarrow K$.

Auch hier ist das differenzielle Potenzial wieder leicht zu bestimmen. Seien (o. B. d. A.) $u \neq 0$, $v \neq 0$. Dann ist

$$\begin{aligned} 0 \in D_f(u,v) &\iff u^{-1} = v, \\ u \in D_f(u,v) &\iff 0 = u^{-1} + v \iff u^{-1} = v, \end{aligned}$$

und für $x \neq 0, u$ gilt

$$\begin{aligned} x \in D_f(u,v) &\iff (x+u)^{-1} = x^{-1} + v \iff x = (x+u)(1+xv) \\ &\iff vx^2 + uvx + u = 0 \\ &\iff x \text{ Nullstelle von } h_{uv} := vT^2 + uvT + u \in K[T]. \end{aligned}$$

Dieses Polynom hat nur einfache Nullstellen, also ist $\#D_f(u,v) = 0$ oder 2, wenn $v \neq u^{-1}$, und $\delta_f(u,v) = 0$ oder $\frac{1}{2^{n-1}}$.

Es bleibt der Spezialfall $v = u^{-1}$ genauer zu untersuchen. Hier ist $h_{uv} = u^{-1}T^2 + T + u$, also $h_{uv}(0) = h_{uv}(u) = u \neq 0$, also besteht $D_f(u, u^{-1})$ aus 0, u und den 0 oder 2 Nullstellen von h_{uv}. Nach Satz 8 im Anhang A.5 kommt es auf $\operatorname{Tr}(ac/b^2) = \operatorname{Tr}(1/1) = \operatorname{Tr}(1)$ an. Ist n gerade, so $\operatorname{Tr}(1) = 0$, und h_{uv} hat zwei Nullstellen in K. Ist dagegen n ungerade, so $\operatorname{Tr}(1) = 1$, und h_{uv} hat keine Nullstelle in K. Damit folgt für $u \neq 0$:

$$\begin{aligned} \#D_f(u,u^{-1}) &= \begin{cases} 2, & \text{wenn } n \text{ ungerade}, \\ 4, & \text{wenn } n \text{ gerade}, \end{cases} \\ \delta_f(u,u^{-1}) &= \begin{cases} \frac{1}{2^{n-1}}, & \text{wenn } n \text{ ungerade}, \\ \frac{1}{2^{n-2}}, & \text{wenn } n \text{ gerade}. \end{cases} \end{aligned}$$

Damit ist gezeigt:

Satz 6 *Ist K ein endlicher Körper der Charakteristik 2 mit $\operatorname{Dim} K = n$ über $\mathbb{F}_2$, so hat die Inversionsabbildung $f = f_{-1}$ das differenzielle Potenzial*

$$\Omega_f = \begin{cases} \frac{1}{2^{n-1}}, & \text{wenn } n \text{ ungerade,} \\ \frac{1}{2^{n-2}}, & \text{wenn } n \text{ gerade.} \end{cases}$$

Insbesondere ist f_{-1} genau dann fast perfekt nichtlinear, wenn n ungerade ist.

(Im oben ausgeschlossenen Fall $n = 1$ gilt das trivialerweise auch.)

In der Differenzentabelle $\#D_f$ hat die erste Zeile die Gestalt $(2^n 0 \cdots 0)$. Jede andere Zeile enthält

- je 2^{n-1}-mal die 0 und die 2, wenn n ungerade,
- 1-mal die 4, $(2^{n-1} - 2)$-mal die 2 und $(2^{n-1} + 1)$-mal die 0, wenn n gerade.

Für die Spalten gilt das gleiche; die Tabelle ist ohnehin symmetrisch, da f_{-1} Involution ist.

Zur Bestimmung des linearen Potenzials der Inversionsabbildung $f = f_{-1}$ für beliebige Dimension n braucht man etwas tiefer liegende Ergebnisse aus der Theorie der elliptischen Kurven, die im Anhang A.6 zusammengestellt sind. Zunächst wird eine Formel für das Spektrum hergeleitet:

Für $v \in K = \mathbb{F}_{2^n}$, o. B. d. A. $v \neq 0$, sei $\beta : K \longrightarrow \mathbb{F}_2$ die zugehörige Linearform $\beta(y) = v \cdot y$. Dazu gibt es nach Korollar 3 in Anhang A.1 ein eindeutig bestimmtes $b \in K^\times$ mit $\beta(y) = \operatorname{Tr}(by)$ für alle $y \in K$, und $\beta \circ f(x) = \operatorname{Tr}(bx^{-1}) = \operatorname{Tr}((cx)^{-1})$ mit $c = b^{-1}$ für $x \in K^\times$. Ebenso ist $u \cdot x = \operatorname{Tr}(ax)$ für $u \in K$ mit passendem $a \in K$. Damit gilt für $v \in K^\times$:

$$\begin{aligned} \hat{\vartheta}_f(u,v) &= = \sum_{x \in K} (-1)^{v \cdot f(x) + u \cdot x} \\ &= 1 + \sum_{x \in K^\times} (-1)^{\operatorname{Tr}((cx)^{-1} + ax)} = 1 + \sum_{y \in K^\times} (-1)^{\operatorname{Tr}(y^{-1} + \frac{a}{c} y)} \\ &= 1 + \kappa(\frac{a}{c}) = 1 + \kappa(ab) \end{aligned}$$

mit der Kloosterman-Summe κ, siehe A.6. Daher ist jede Spalte des Spektrums – außer der trivialen ersten – jeweils bis auf eine Permutation und die Addition der Konstanten 1 die Wertetabelle der Kloosterman-Funktion. Insbesondere ist gezeigt:

Satz 7 *Jede Spalte des Spektrums $\hat{\vartheta}_f(u,v)$ (für $v \neq 0$) der Inversionsabbildung $f = f_{-1}$ von $K = \mathbb{F}_{2^n}$ enthält genau die durch 4 teilbaren ganzen Zahlen zwischen $-2^{n/2+1} + 1$ und $2^{n/2+1} + 1$. Für das lineare Potenzial Λ_f gilt*

$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max_{u \in K^\times} |1 + \kappa(u)|^2.$$

Im Beispiel $n = 8$ sind die Grenzen -31 und 33, die angenommenen Werte also $-28, -24, -20, \ldots, 24, 28, 32$, und $\Lambda_f = \frac{1}{64}$.

Falls $n \geq 2$ gerade ist, ist $2^{n/2+1}$ durch 4 teilbar, also $\max|1 + \kappa(u)| = 2^{n/2+1}$, also $\Lambda_f = \frac{2^{n+2}}{2^{2n}} = \frac{1}{2^{n-2}}$.

Falls n ungerade ist, ist das Ergebnis etwas komplizierter zu formulieren. Hier ist

$$2^{\frac{n}{2}+1} = 2^{\frac{n+1}{2}} \cdot \sqrt{2}$$

irrational, und mit der ganzen Zahl

$$\nu(n) := \lfloor 2^{\frac{n}{2}+1} \rfloor$$

gelten für die Einträge $1 + \kappa(u)$ des Spektrums die Grenzen

$$-\nu(n) + 1 \leq 1 + \kappa(u) \leq \nu(n) + 1.$$

Je nach der Restklasse mod4 von $\nu(n)$ sind die Grenzen also:

$\nu(n)$ mod 4	untere Grenze	obere Grenze	$\max\|1 + \kappa(u)\|$
0	$-\nu(n) + 4$	$\nu(n)$	$\nu(n)$
1	$-\nu(n) + 1$	$\nu(n) - 1$	$\nu(n) - 1$
2	$-\nu(n) + 2$	$\nu(n) - 2$	$\nu(n) - 2$
3	$-\nu(n) + 3$	$\nu(n) + 1$	$\nu(n) + 1$

Den Maximalwert kann man also durch die eindeutig bestimmte ganze Zahl $\xi(n) \in \mathbb{Z}$ mit

$$2^{\frac{n}{2}+1} - 3 < \xi(n) \leq 2^{\frac{n}{2}+1} + 1, \quad 4|\xi(n),$$

beschreiben:

Hauptsatz 4 *Für die Inversionsabbildung $f = f_{-1}$ des Körpers $K = \mathbb{F}_{2^n}$ mit $n \geq 2$ gilt*

$$\begin{aligned} &\text{(i)} && \max_{K^2-\{0\}} |\hat{\vartheta}_f| && = \xi(n), \\ &\text{(ii)} && \sigma_f && = 2^{n-1} - \frac{1}{2}\xi(n), \\ &\text{(iii)} && \Lambda_f && = \frac{1}{2^{2n}}\xi(n)^2. \end{aligned}$$

Falls $n \geq 2$ gerade, ist $\xi(n) = 2^{n/2+1}$. Es folgt:

Korollar 1 *Für die Nichtlinearität der Inversionsabbildung f gilt:*

$$\sigma_f = \begin{cases} 2^{n-1} - 2^{n/2}, & \text{wenn } n \text{ gerade,} \\ 2^{n-1} - [2^{n/2} - \frac{1}{2}], & \text{wenn } n \text{ ungerade,} \end{cases}$$

wobei die eckigen Klammern die Rundung zur nächsten ganzen Zahl bedeuten.

Die Ergebnisse für kleine Dimension n werden durch die folgende Tabelle wiedergegeben:

n	2	3	4	5	6	7	8	9	10	11	12
$2^{\frac{n}{2}+1}$	4	5.7	8	11.3	16	22.6	32	45.3	64	90.5	128
$\xi(n)$	4	4	8	12	16	20	32	44	64	88	128
σ_f	0	2	4	10	24	54	112	234	480	980	1984
Λ_f	1	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{9}{64}$	$\frac{1}{16}$	$\frac{25}{1024}$	$\frac{1}{64}$	$\frac{121}{2^{14}}$	$\frac{1}{256}$	$\frac{121}{2^{16}}$	$\frac{1}{1024}$

5.5 Minimierung der Potenziale bei fester Dimension

In diesem Abschnitt wird zusammengesammelt, was aus den vorhergehenden Abschnitten über die Größen

$$\begin{aligned}\Lambda(n,q) &:= \min\{\Lambda_f \mid f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q\},\\ \sigma(n,q) &:= \max\{\sigma_f \mid f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q\},\\ \Omega(n,q) &:= \min\{\Omega_f \mid f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q\}\end{aligned}$$

bekannt ist; dazu werden einige Ergänzungen bewiesen.

Anmerkung. $\sigma(n,1)$ ist in der Codierungstheorie als Überdeckungsradius des Reed-Muller-Codes $\mathcal{R}(1,n)$ bekannt.

Hilfssatz 4 *Sei $g\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^{q+1}$ zerlegt in $g = (f_0, f)$ mit $f_0\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ und $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$. Dann ist*

(i) $\Lambda_g \geq \Lambda_f$,

(ii) $\sigma_g \leq \sigma_f$,

(iii) $\Omega_g \leq \Omega_f$.

Beweis. (i) Für eine Linearform $\beta \in \mathcal{L}_q$ sei $\beta' \in \mathcal{L}_{q+1}$ durch $\beta'(y_0, y) := \beta(y)$ definiert. Dann ist $\beta' \circ g = \beta \circ f$, also

$$\Lambda_f = \max_{\beta \in \mathcal{L}_q - \{0\}} \Lambda_{\beta\circ f} = \max_{\beta \in \mathcal{L}_q - \{0\}} \Lambda_{\beta'\circ g} \leq \max_{\gamma \in \mathcal{L}_{q+1} - \{0\}} \Lambda_{\gamma\circ g} = \Lambda_g.$$

(ii) folgt aus (i) oder durch einen direkten analogen Schluss.
(iii) Ist $v' = (v_0, v)$, so

$$\begin{aligned}D_g(u,v') &= \{x \mid g(x+u) - g(x) = v'\}\\ &= \{x \mid f_0(x+u) - f_0(x) = v_0\} \cap \{x \mid f(x+u) - f(x) = v\}\\ &\subseteq D_f(u,v),\end{aligned}$$

also $\delta_g(u,v') \leq \delta_f(u,v)$, also $\Omega_g \leq \Omega_f$. $\diamond$

Satz 8 *Für alle Dimensionen n und q gilt:*

(i) $\Lambda(n,q) \leq \Lambda(n,q+1)$*, d. h.,* Λ *ist bei festem* n *bezüglich* q *monoton wachsend.*

(ii) $\sigma(n,q) \geq \sigma(n,q+1)$*, d. h.,* σ *ist bei festem* n *bezüglich* q *monoton fallend.*

(iii) $\Omega(n,q) \geq \Omega(n,q+1)$*, d. h.,* Ω *ist bei festem* n *bezüglich* q *monoton fallend.*

(iv) $\Lambda(n,1) \geq \Lambda(n+1,1)$*, d. h.,* Λ *ist bei festem* $q = 1$ *bezüglich* n *monoton fallend.*

Beweis. (i), (ii) und (iii) folgen direkt aus dem Hilfssatz 4. Für (iv) wird verwendet, dass $\Lambda_{\bar{f}} = \Lambda_f$ für die einfache Erweiterung $\bar{f}$ einer BOOLEschen Funktion f nach Bemerkung 4 in 3.6. Wird f mit $\Lambda_f = \Lambda(n,1)$ gewählt, so ist $\Lambda_{\bar{f}} \geq \Lambda(n+1,1)$. $\diamond$

Korollar 1 *Es gibt keine fast krumme Abbildung* $f\colon \mathbb{F}_2^4 \longrightarrow \mathbb{F}_2^4$.

Beweis. Nach Korollar 1 in 3.6 ist $\Lambda(4,4) \geq \Lambda(4,3) \geq \frac{9}{64}$, also insbesondere $> \frac{1}{8}$. $\diamond$

Korollar 2 *Für* $q \geq n$ *gilt* $\Omega(n,q) = \frac{1}{2^{n-1}}$.

Beweis. $\Omega(n,n) = \frac{1}{2^{n-1}}$ für alle n nach Satz 5 in 5.3. Wegen der Monotonie in q ist daher auch $\Omega(n,q) = \frac{1}{2^{n-1}}$ für alle $q \geq n$. $\diamond$

Stellen wir nun zusammen, was über $\Lambda(n,q)$ bekannt ist.

- Stets ist $\frac{1}{2^n} \leq \Lambda(n,q) \leq 1$, siehe Bemerkung 1 und Satz 7 in 3.5. Ist n gerade und $1 \leq q \leq \frac{n}{2}$, so ist $\Lambda(n,q) = \frac{1}{2^n}$, da es krumme Abbildungen gibt.
- $\Lambda(1,q) = 1$ für alle q, denn hier ist jede Abbildung f affin, also $\Lambda_f = 1$, siehe Bemerkung 1 in 3.5.
- $\Lambda(2,2) = 1$ nach Beispiel 4 in 3.5, also wegen der Monotonie auch $\Lambda(2,q) = 1$ für alle $q \geq 2$.
- Wenn es eine krumme Abbildung $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ gibt, ist $\Lambda(n,q) = \frac{1}{2^n}$, siehe Satz 7 in 3.5. Dass eine solche existiert, wissen wir bisher nur für gerade n und $q = 1$. Also $\Lambda(n,1) = \frac{1}{2^n}$ für gerades n.

- Für ungerades n gibt es eine Funktion $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ mit $\Lambda_f = \frac{1}{2^{n-1}}$, siehe Satz 8 in 3.5 oder Korollar 6 in 3.6. Also ist $\Lambda(n,1) \leq \frac{1}{2^{n-1}}$ für ungerades n.

- Wenn es *keine* krumme Abbildung $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ gibt und $n \geq 2$, ist $\Lambda(n,q) \geq \frac{1}{2^n} + \frac{1}{2^{2n-2}}$, siehe Korollar 1 in 3.5, äquivalent dazu ist $\sigma(n,q) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 1$. Insbesondere ist
  - $\sigma(6,q) \leq 27$ und $\Lambda(6,q) \geq \frac{25}{1024}$ für alle $q \geq 4$,
  - $\sigma(8,q) \leq 119$ und $\Lambda(8,q) \geq \frac{81}{16384}$ für alle $q \geq 5$.

- $\Lambda(n,n) = \frac{1}{2^{n-1}}$ für ungerades n, da es dann eine fast krumme Abbildung gibt, siehe Hauptsatz 3 in 5.3. Insbesondere $\Lambda(3,3) = \frac{1}{4}$, $\Lambda(5,5) = \frac{1}{16}$, $\Lambda(7,7) = \frac{1}{64}$.

- $\Lambda(n,n) \leq \frac{1}{2^{n-2}}$ für gerades n nach 5.4. Insbesondere ist $\Lambda(2,4) \leq \Lambda(3,4) \leq \Lambda(4,4) \leq \frac{1}{4}$. Allgemein folgt $\Lambda(n,q) \leq \frac{1}{2^{n-2}}$ für gerades n und $q \leq n$.

- $\Lambda(n,n) > \frac{1}{2^{n-1}}$ für gerades n nach Satz 2, Beispiel 2 und Satz 3 in 5.2, also $\sigma(n,n) < 2^{n-1} - 2^{\frac{n-1}{2}}$, also $\sigma(n,n) \leq 2^{n-1} - \lceil 2^{\frac{n-1}{2}} \rceil$. Daraus folgt
$$\Lambda(n,n) \geq \left(\frac{\lceil 2^{\frac{n-1}{2}} \rceil}{2^{n-1}} \right)^2$$
für gerades n. Das ergibt die Schranken $\sigma(4,4) \leq 5$, $\sigma(6,6) \leq 26$, $\sigma(8,8) \leq 116$, $\Lambda(4,4) \geq \frac{9}{64}$, $\Lambda(6,6) \geq \frac{9}{256}$, $\Lambda(8,8) \geq \frac{9}{1024}$.

- Die explizite Analyse der S-Boxen von DES mit `bma` ergibt für die S-Box S_6 den Wert $\Lambda_f = \frac{49}{256}$. Also ist $\Lambda(6,2) \leq \Lambda(6,3) \leq \Lambda(6,4) \leq \frac{49}{256}$.

- Aus der Ganzzahligkeit der Nichtlinearität folgt (siehe 3.6)
  - $\Lambda(3,q) \geq \frac{1}{4}$ für alle q. Insbesondere $\Lambda(3,1) = \frac{1}{4}$ und wegen der Monotonie auch $\Lambda(3,2) = \frac{1}{4}$.
  - $\Lambda(4,q) \geq \frac{9}{64}$ für alle $q \geq 3$, da es für $q = 3$ keine krumme Abbildung gibt und wegen der Monotonie.
  - $\Lambda(5,q) \geq \frac{9}{256}$ für alle q.
  - $\Lambda(7,q) \geq \frac{9}{1024}$ für alle q.

- Die Chabaud-Vaudenay-Schranke gibt noch für $q = n+1$ interessante Ergebnisse: Es ist $\Lambda(n,n+1) \geq CV(n,n+1)$, also $\sigma(n,n+1) \leq 2^{n-1} \cdot (1 - \sqrt{CV(n,n+1)}$, also $\sigma(n,n+1) \leq 2^{n-1} - \lceil \sqrt{CV(n,n+1)} \rceil$.
  Speziell ist $\sigma(3,4) \leq 1$, $\sigma(4,5) \leq 4$, $\sigma(5,6) \leq 11$, $\sigma(6,7) \leq 25$, $\sigma(7,8) \leq 55$, und dazu passend $\Lambda(3,4) \geq \frac{9}{16}$, $\Lambda(4,5) \geq \frac{1}{4}$, $\Lambda(5,6) \geq \frac{25}{256}$, $\Lambda(6,7) \geq \frac{49}{1024}$, $\Lambda(7,8) \geq \frac{81}{4096}$.

Diese Aussagen werden in den folgenden Tabellen zusammengefasst, wobei die eckigen Klammern abgeschlossene Intervalle und die drei Punkte den gleichen Eintrag wie in der Zelle links davon bedeuten:

$\Lambda(n,q)$	$q=1$	2	3	4	5	6	7	8
$n=1$	1	1	1	1	1	1	1	1
2	$\frac{1}{4}$	1	1	1	1	1	1	1
3	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$[\frac{9}{16},1]$	...	...	...	...
4	$\frac{1}{16}$	$\frac{1}{16}$	$[\frac{9}{64},\frac{1}{4}]$	...	$[\frac{1}{4},1]$	...	...	...
5	$[\frac{9}{256},\frac{1}{16}]$	...	...	...	$\frac{1}{16}$	$[\frac{25}{256},1]$	...	...
6	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$[\frac{25}{1024},\frac{49}{256}]$	$[\frac{25}{1024},\frac{1}{16}]$	$[\frac{9}{256},\frac{1}{16}]$	$[\frac{49}{1024},1]$	...
7	$[\frac{9}{1024},\frac{1}{64}]$	...	...	...	...	...	$\frac{1}{64}$	$[\frac{81}{4096},1]$
8	$\frac{1}{256}$	$\frac{1}{256}$	$\frac{1}{256}$	$\frac{1}{256}$	$[\frac{81}{16384},\frac{1}{64}]$	...	...	$[\frac{9}{1024},\frac{1}{64}]$

$\sigma(n,q)$	$q=1$	2	3	4	5	6	7	8
$n=1$	0	0	0	0	0	0	0	0
2	1	0	0	0	0	0	0	0
3	2	2	2	$[0,1]$	...	...	...	...
4	6	6	$[4,5]$	...	$[0,4]$	...	...	...
5	$[12,13]$	...	...	...	12	$[0,11]$	...	...
6	28	28	28	$[18,27]$	$[8,27]$	$[8,26]$	$[0,25]$	...
7	$[56,58]$	...	...	...	...	...	56	$[0,55]$
8	120	120	120	120	$[112,119]$	...	...	$[112,116]$

Über $\Omega(n,q)$ ist folgendes bekannt:

- $\frac{1}{2^q} \leq \Omega(n,q) \leq 1$ nach Bemerkung 2 in 4.4. Ist n gerade und $1 \leq q \leq \frac{n}{2}$, so ist $\Omega(n,q) = \frac{1}{2^q}$, da es krumme Abbildungen gibt.
- $\frac{1}{2^{n-1}} \leq \Omega(n,q)$ nach Bemerkung 6 in 4.4. Für alle $q \geq n$ ist $\Omega(n,q) = \frac{1}{2^{n-1}}$ nach Korollar 2
- $\Omega(1,q) = 1$ für alle q nach Beipiel 1 in 4.4.
- $\Omega(n,1) = \frac{1}{2}$ für alle geraden n, da dann krumme, also perfekt nichtlineare Funktionen existieren.
- $\Omega(2,2) = \frac{1}{2}$ nach Beispiel 3.
- Ist n ungerade und $\geq q+1$ oder ist n gerade und $q+1 \leq n < 2q$, so ist $\Omega(n,q) \geq \frac{1}{2^q} + \frac{1}{2^{n-1}}$; das folgt, weil es für diese Dimensionen keine perfekt nichtlinearen Abbildungen gibt und jedes Ω_f Vielfaches von $\frac{1}{2^{n-1}}$ sein muss, siehe auch Korollar 3 in 4.5. Insbesondere folgt:
  - $\Omega(3,1) \geq \frac{3}{4}$, $\Omega(3,2) \geq \frac{1}{2}$. Da der Wert $\frac{1}{2}$ vom Volladdierer angenommen wird, siehe Beispiel 5 in 4.3, ist $\Omega(3,2) = \frac{1}{2}$.

- $\Omega(4,3) \geq \frac{1}{4}$.
- $\Omega(5,1) \geq \frac{9}{16}$, $\Omega(5,2) \geq \frac{5}{16}$, $\Omega(5,3) \geq \frac{3}{16}$, $\Omega(5,4) \geq \frac{1}{8}$.
- $\Omega(6,4) \geq \frac{3}{32}$, $\Omega(6,5) \geq \frac{1}{16}$.
- $\Omega(7,1) \geq \frac{33}{64}$, $\Omega(7,2) \geq \frac{17}{64}$, $\Omega(7,3) \geq \frac{9}{64}$, $\Omega(7,4) \geq \frac{5}{64}$, $\Omega(7,5) \geq \frac{3}{64}$, $\Omega(7,6) \geq \frac{1}{32}$.
- $\Omega(8,5) \geq \frac{5}{128}$, $\Omega(8,6) \geq \frac{3}{128}$, $\Omega(8,7) \geq \frac{1}{64}$.

- Für alle S-Boxen von DES gilt nach direkter Analyse $\Omega_f = \frac{1}{4}$. Also ist $\frac{1}{4} \geq \Omega(6,4) \geq \Omega(6,5)$.

Das ergibt die folgende Tabelle:

$\Omega(n,q)$	$q=1$	2	3	4	5	6	7	8
$n=1$	1	1	1	1	1	1	1	1
2	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
3	$[\frac{3}{4},1]$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
4	$\frac{1}{2}$	$\frac{1}{4}$	$[\frac{1}{4},\frac{1}{2}]$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$
5	$[\frac{9}{16},1]$	$[\frac{5}{16},1]$	$[\frac{3}{16},1]$	$[\frac{1}{8},1]$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
6	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$[\frac{3}{32},\frac{1}{4}]$	$[\frac{1}{16},\frac{1}{4}]$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$
7	$[\frac{33}{64},1]$	$[\frac{17}{64},1]$	$[\frac{9}{64},1]$	$[\frac{5}{64},1]$	$[\frac{3}{64},1]$	$[\frac{1}{32},1]$	$\frac{1}{64}$	$\frac{1}{64}$
8	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{16}$	$[\frac{5}{128},\frac{1}{2}]$	$[\frac{3}{128},\frac{1}{2}]$	$[\frac{1}{64},\frac{1}{2}]$	$\frac{1}{128}$

A Endliche Körper

A.1 Die Spur

In diesem Abschnitt werden endliche Erweiterungskörper K des endlichen Körpers $\mathbb{F}_q$ mit q Elementen betrachtet.

Hilfssatz 1 (i) *Die Abbildung*

$$\varphi\colon K \longrightarrow K, \quad \varphi(x) = x^q,$$

ist ein Automorphismus von K, insbesondere $\mathbb{F}_q$-linear. (Man nennt sie den Frobenius-*Automorphismus von K.)*

(ii) *Ein $x \in K$ ist genau dann Fixpunkt von φ, wenn $x \in \mathbb{F}_q$.*

Beweis. (i) Die binomische Formel liefert $(x+y)^q = x^q + y^q$, da q eine Potenz der Charakteristik des Körpers K ist. Die entsprechende multiplikative Relation $(xy)^q = x^q y^q$ ist trivial. Daher ist φ ein Ringhomomorphismus. Da K Körper ist, ist φ injektiv, da K endlich ist, auch surjektiv.

(ii) Das Polynom $T^q - T$ hat die q Elemente von $\mathbb{F}_q$ als Nullstellen. Das müssen daher alle sein. $\diamond$

Sei n die Dimension von K als $\mathbb{F}_q$-Vektorraum. Die **Spur** ist auf K definiert als

$$\mathrm{Tr}\colon K \longrightarrow K, \quad \mathrm{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}} = \sum_{i=0}^{n-1} x^{q^i},$$

also

$$\mathrm{Tr} = \varphi^0 + \varphi + \varphi^2 + \cdots + \varphi^{n-1} = \sum_{i=0}^{n-1} \varphi^i,$$

Anmerkung. Im allgemeinen ist bei einer separablen Körpererweiterung die Spur $\mathrm{Tr}(x)$ die Summe über alle zu x konjugierten Elemente, also aller Bilder unter relativen Automorphismen. Der Zusammenhang entsteht dadurch, dass die Automorphismengruppe von K über $\mathbb{F}_q$ vom Frobenius-Automorphismus φ erzeugt wird und die Ordnung n hat.

Hilfssatz 2 *Für die Spur gilt:*

(i) $\mathrm{Tr}(x) \in \mathbb{F}_q$ *für alle* $x \in K$.

(ii) $\mathrm{Tr}\colon K \longrightarrow \mathbb{F}_q$ *ist $\mathbb{F}_q$-linear.*

(iii) $\mathrm{Tr}(x) = nx$ *für alle* $x \in \mathbb{F}_q$.

Beweis. (i) folgt, weil offensichtlich $\mathrm{Tr}(x)^q = \mathrm{Tr}(x)$. (ii) und (ii) sind trivial. $\diamond$

Satz 1 (ARTINs Lemma von der Unabhängigkeit der Charaktere) *Sei G eine Halbgruppe, K ein Körper und X eine Menge von Homomorphismen $G \longrightarrow K^\times$ („Charaktere"). Dann ist X im K-Vektorraum K^G aller K-wertigen Abbildungen von G linear unabhängig.*

Beweis. Sei

$$a_1\chi_1 + \cdots + a_n\chi_n = 0$$

eine minimale lineare Relation mit verschiedenen $\chi_i \in X$. Dann sind alle $a_i \neq 0$ und, da $\chi_1 \neq 0$, jedenfalls $n \geq 2$. Sei $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$ gewählt. Dann gilt für alle $h \in G$:

$$[a_1\chi_1(g)\chi_1 + \cdots + a_n\chi_n(g)\chi_n](h) = a_1\chi_1(gh) + \cdots + a_n\chi_n(gh) = 0.$$

Also haben wir, zusammen mit der ursprünglichen, die beiden linearen Relationen

$$\begin{aligned} a_1\chi_1(g)\chi_1 + a_2\chi_2(g)\chi_2 + \cdots + a_n\chi_n(g)\chi_n &= 0, \\ a_1\chi_1(g)\chi_1 + a_2\chi_1(g)\chi_2 + \cdots + a_n\chi_1(g)\chi_n &= 0, \end{aligned}$$

deren Differenz eine nichttriviale kürzere lineare Relation ergibt; Widerspruch. ◇

Korollar 1 *Ist $K \supseteq \mathbb{F}_q$ eine endliche Körpererweiterung, so gibt es ein $x \in K$ mit $\mathrm{Tr}(x) \neq 0$.*

Beweis. Ist φ der FROBENIUS-Automorphismus, so ist $\mathrm{Tr} = \varphi^0 + \varphi^1 + \cdots + \varphi^{n-1}$, wobei n die Dimension von K über $\mathbb{F}_q$ ist, und die φ_i sind verschiedene Gruppenhomomorphismen $K^\times \longrightarrow K^\times$. Also sind sie linear unabhängig; insbesondere kann ihre Summe nicht 0 sein. ◇

Die **Spurform** von K ist die bilineare Abbildung

$$\mathrm{Tr}_2 \colon K \times K \longrightarrow \mathbb{F}_q, \quad \mathrm{Tr}_2(x, y) := \mathrm{Tr}(xy).$$

Korollar 2 *Die Spurform ist eine nichtausgeartete Bilinearform.*

Beweis. Sei $x \in K$ gewählt mit $\mathrm{Tr}(x) \neq 0$. Dann ist für $y \in K$, $y \neq 0$,

$$\mathrm{Tr}_2(y, \frac{x}{y}) = \mathrm{Tr}(y \cdot \frac{x}{y}) = \mathrm{Tr}(x) \neq 0,$$

also y nicht im Kern der Bilinearform. ◇

Da die Spurform somit eine Bijektion zwischen K und seinem dualen $\mathbb{F}_q$-Vektorraum herstellt, folgt weiter:

Korollar 3 *Für jede $\mathbb{F}_q$-Linearform $\alpha\colon K \longrightarrow \mathbb{F}_q$ gibt es genau ein $a \in K$ mit*

$$\alpha(x) = \mathrm{Tr}(ax) \quad \textit{für alle } x \in K.$$

Für $x_1, \ldots, x_n \in K$ betrachten wir die Matrix

$$W(x) := \left(x_j^{q^{i-1}}\right)_{1 \le i,j \le n} \in M_{n,n}(K).$$

Es ist

$$W(x)^t\, W(x) = G(x) := (\mathrm{Tr}(x_i x_j))$$

die GRAMsche Matrix bezüglich der Spurform, denn

$$\mathrm{Tr}(x_i x_j) = \sum_{k=1}^{n} x_i^{q^{k-1}} x_j^{q^{k-1}}.$$

Bekanntlich sind $x_1, \ldots, x_n$ genau dann über $\mathbb{F}_q$ linear unabhängig, wenn ihre GRAMsche Matrix invertierbar ist. Damit ist gezeigt:

Hilfssatz 3 *Die Elemente $x_1, \ldots, x_n \in K$ bilden genau dann eine Basis von K über $\mathbb{F}_q$, wenn $n = \mathrm{Dim}_{\mathbb{F}_q} K$ und die Matrix $W(x)$ invertierbar ist.*

A.2 q-Polynome

Eine besondere Rolle spielen bei endlichen Körpern die Polynome, die lineare Funktionen definieren: Die Abbildung

$$\Psi\colon \mathbb{F}_q[T] \longrightarrow \mathbb{F}_q[T], \quad f = \sum_{i=0}^{n} a_i T^i \mapsto F = \sum_{i=0}^{n} a_i T^{q^i}$$

ist $\mathbb{F}_q$-linear; ihre Bilder heißen q-Polynome. Insbesondere sind sie durch T teilbar.

Hilfssatz 4 *Für alle Polynome $f, g \in \mathbb{F}_q[T]$ gilt:*
(i) $\Psi(fg) = \Psi(f)\,(\Psi(g))$ *(Einsetzen eines Polynoms in ein Polynom),*
(ii) $g|f \iff \Psi(g)|\Psi(f)$.
(iii) $\mathrm{ggT}(\Psi(f), \Psi(g)) = \Psi(\mathrm{ggT}(f, g))$.

Beweis. (i) Ist $g = \sum_{j=0}^{n} b_j t^j$, so

$$\begin{aligned} fg &= \sum_{i=0}^{n}\sum_{j=0}^{n} a_i b_j T^{i+j}, \\ \Psi(fg) &= \sum_{i=0}^{n}\sum_{j=0}^{n} a_i b_j \left(T^{q^j}\right)^{q^i} \\ &= \sum_{i=0}^{n} a_i \left(\sum_{j=0}^{n} b_j T^{q^j}\right)^{q^i} = \Psi(f)\,(\Psi(g))\,. \end{aligned}$$

(ii) Sei $f = hg$. Mit dem Polynom $\bar{h} := \frac{1}{T}\Psi(h)$ gilt

$$\Psi(f) = \Psi(hg) = \Psi(h)\,(\Psi(g)) = \Psi(g)\bar{h}\,(\Psi(g))\,.$$

Sei umgekehrt $\Psi(g)|\Psi(f)$. Sei $f = hg + r$ die Division mit Rest r, wobei $\operatorname{Grad} r < \operatorname{Grad} g$ ist. Dann ist auch

$$\Psi(f) = \Psi(hg) + \Psi(r) = \Psi(g)\bar{h}\,(\Psi(g)) + \Psi(r)$$

eine Division mit Rest, denn $\operatorname{Grad}\Psi(r) < \operatorname{Grad}\Psi(g)$. Da diese eindeutig ist und $\Psi(g)|\Psi(f)$, muss $\Psi(r) = 0$, also auch $r = 0$ und $g|f$ sein.

(iii) Sei $h := \mathrm{ggT}(f, g)$. Dann gilt:

$$L = \psi(l)|\Psi(h) \Longleftrightarrow l|h \Longleftrightarrow l|f, g \Longleftrightarrow L|\Psi(f), \Psi(g).$$

Also ist $\Psi(h) = \mathrm{ggT}(\Psi(f), \Psi(g)$. $\diamond$

Da jedes q-Polynom F eine $\mathbb{F}_q$-lineare Abbildung $K \longrightarrow K$ definiert, ist seine Nullstellenmenge V_F ein $\mathbb{F}_q$-Untervektorraum von K mit $\varphi(V_F) = V_F$. Umgekehrt gilt:

Satz 2 *Sei $V \subseteq K$ ein h-dimensionaler $\mathbb{F}_q$-Untervektorraum mit $\varphi(V) = V$. Dann ist*

$$F = F_V := \prod_{v \in V} (T - v) \in K[T]$$

ein q-Polynom, $F = \Psi(f)$ mit $\operatorname{Grad} f = h$; insbesondere ist $F \in \mathbb{F}_q[T]$.

Beweis. Die Koeffizienten von F sind die elementarsymmetrischen Funktionen der $v \in V$, also unter dem FROBENIUS-Automorphismus invariant, also in $\mathbb{F}_q$. Sei $v_1, \ldots v_h$ eine Basis von V. Dann ist die Matrix $W(v) := \left(v_j^{q^{i-1}}\right) \in M_{h,h}(K)$ invertierbar. Also gibt es eine Lösung $a_0, \ldots, a_{h-1} \in K$ des Gleichungssystems

$$v_i^{q^h} + \sum_{j=0}^{h-1} a_j v_i^{q^j} = 0 \quad \text{für } i = 1, \ldots, n.$$

Damit sind $v_1, \ldots, v_h$ Nullstellen des Polynoms

$$G = T^{q^h} + \sum_{j=0}^{h-1} a_j T^{q^j}.$$

Wegen der Linearität sind alle $v \in V$ ebenfalls Nullstellen, und das sind q^h Stück, also sämtliche Nullstellen von G. Daher ist $G = F \in \mathbb{F}_q[T]$. $\diamond$

Korollar 1 *Für jedes $x \in K$ gibt es ein q-Polynom F mit $F(x) = 0$.*

Beweis. Die Potenzen x^{q^i} spannen einen Unterraum $V \subseteq K$ mit $\varphi(V) = V$ auf. Daher ist F_V ein q-Polynom mit x als Nullstelle. $\diamond$

Aus der Konstruktion ist klar, dass F den Leitkoeffizienten 1 hat und jedes andere q-Polynom G mit $G(x) = 0$ teilt. Es heißt daher auch das **q-Minimalpolynom** von x. Umgekehrt heißt x **q-primitive** Nullstelle eines q-Polynoms F, wenn F bis auf einen konstanten Faktor das q-Minimalpolynom von x ist.

Satz 3 *Sei $F = \Psi(f) \in \mathbb{F}_q[T]$ ein q-Polynom mit $f(0) \neq 0$. Dann hat F im algebraischen Abschluss von $\mathbb{F}_q$ eine q-primitive Nullstelle.*

Beweis. Sei $f = f_1^{e-1} \cdots f_r^{e_r}$ die Primzerlegung in $\mathbb{F}_q[T]$; die f_i seien verschieden und vom Grad m_i. Dann ist f vom Grad $m = e_1 m_1 + \cdots + e_r m_r$. Ist $f = a_0 + \cdots a_m T^m$, so $F = a_0 T + \cdots + a_m T^{q^m}$ und die Ableitung $F' = a_0 \neq 0$ konstant. Also sind alle q^m Nullstellen von F einfach.

Nun ist eine Nullstelle x von F genau dann q-primitiv, wenn x nicht Nullstelle eines q-Polynoms $G|F$ von kleinerem Grad ist. Ist $G = \Psi(g)$, so $g|f$, also $g|g_i := \frac{f}{f_i}$ für ein i. Die Nullstellen der $G_i := \Psi(g_i)$ sind also nicht q-primitiv für F. Also ist die Menge der q-primitiven Nullstellen gleich der Nullstellenmenge V_F weniger die Vereinigung der Nullstellenmengen V_{G_i}. Deren Anzahlen sind q^m bzw. q^{m-m_i}. Um das folgende Lemma 5 anwenden zu können, brauchen wir noch die Elementeanzahlen der Durchschnitte $\bigcap_{i \in I} V_{G_i}$ für alle Teilmengen $I \subseteq \{1, \ldots, r\}$. Eine solche gemeinsame Nullstellenmenge ist genau die Nullstellenmenge des

$$\mathrm{ggT}\{G_i \mid i \in I\} = \Psi(\mathrm{ggT}\{g_i \mid i \in I\}).$$

Dieses q-Polynom hat nur einfache Nullstellen und ist vom Grad

$$q^{m - \sum_{i \in I} m_i}.$$

Das ist also auch seine Nullstellenzahl. Also ist die Zahl der q-primitiven Nullstellen von F gleich

$$\begin{aligned} q^m - \sum_{i=1}^{m} q^{m-m_i} + \sum_{1 \leq i < j \leq r} q^{m-m_i-m_j} - \cdots &= q^m \cdot (1 - \frac{1}{q^{m_1}}) \cdots (1 - \frac{1}{q^{m_r}}) \\ &> 0; \end{aligned}$$

insbesondere gibt es q-primitive Nullstellen. $\diamond$

Hilfssatz 5 (DE MOIVRES Ein- und Ausschlussprinzip) *Sei M eine endliche Menge und $M_1, \ldots, M_n \subseteq M$ Teilmengen. Für $I \subseteq \{1, \ldots, n\}$ sei $M_I := \bigcap_{i \in I} M_i$. Dann ist*

$$\# \left(M - \bigcup_{i=1}^{n} M_i \right) = \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{\#I} \# M_I.$$

Beweis. Induktion über n. Der Fall $n = 1$ ist trivial. Sei also jetzt $n \geq 2$. Sei $M' := M - M_1$ und $M_i' := M_i - M_1 \cap M_i$. Weiter sei für $J \subseteq \{2, \ldots, n\}$

$$M_J' := \bigcap_{j \in J} M_j' = \bigcap_{j \in J} M_j - M_1 \cap \bigcap_{j \in J} M_j = M_J - M_{J \cup \{1\}}.$$

Also ist

$$\begin{aligned} \# \left(M - \bigcup_{i=1}^{n} M_i \right) &= \# \left(M' - \bigcup_{i=2}^{n} M_i' \right) \\ &= \sum_{J \subseteq \{2,\ldots,n\}} (-1)^{\#J} \# M_J' \\ &= \sum_{J \subseteq \{2,\ldots,n\}} (-1)^{\#J} \left[\# M_J - M_{J \cup \{1\}} \right] \\ &= \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{\#I} \# M_I, \end{aligned}$$

wie behauptet. $\diamond$

Die Anzahl der q-primitiven Nullstellen aus dem Beweis von Satz 3 lässt sich noch anders beschreiben. Dazu sei für ein Polynom $f \in \mathbb{F}_q[T]$ definiert:

$$\begin{aligned} \Phi_q(f) &:= \{g \in \mathbb{F}_q[T] \mid \operatorname{Grad} g < \operatorname{Grad} f,\ \operatorname{ggT}(f, g) = 1\}, \\ \varphi_q(f) &:= \#\Phi_q(f). \end{aligned}$$

Das ist das „q-Analogon“ zur EULERschen φ-Funktion und hat folgende Eigenschaften:

Hilfssatz 6 (i) *Ist f konstant, so $\varphi_q(f) = 1$.*
(ii) *Sind f und g teilerfremd, so ist $\varphi_q(fg) = \varphi_q(f)\varphi_q(g)$.*
(iii) *Ist $f \in \mathbb{F}_q[T]$ irreduzibel vom Grad n, so ist $\varphi_q(f) = q^n - 1$.*
(iv) *... und $\varphi_q(f^e) = q^{en}(1 - \frac{1}{q^n})$.*
(v) *Ist $f = f_1^{e_1} \cdots f_r^{e_r}$ die Primzerlegung und $n_i = \operatorname{Grad} f_i$, so ist*

$$\varphi_q(f) = q^n \cdot (1 - \frac{1}{q^{n_1}}) \cdots (1 - \frac{1}{q^{n_r}}).$$

(vi) *Hat f in* (v) *nur einfache Nullstellen, so ist*

$$\varphi_q(f) = (q^{n_1} - 1) \cdots (q^{n_r} - 1).$$

Beweis. (i) Nur das Nullpolynom wird gezählt.

(ii) Die Abbildung

$$\Phi_q(fg) \longrightarrow \Phi_q(f) \times \Phi_q(g), \quad h \mapsto (h \bmod f, h \bmod g),$$

ist wohldefiniert, denn ist h zu fg teilerfremd, so auch zu f und g. Nach dem chinesischen Restsatz ist sie bijektiv.

(iii) Es sind alle Polynome von kleinerem Grad zu f teilerfremd außer dem Nullpolynom.

(iv) Die Polynome vom Grad $< en$, die nicht in $\Phi_q(f^e)$ liegen, sind genau die hf mit $\operatorname{Grad} h < en - n$. Also ist $\varphi_q(f^e) = q^{en} - q^{en-n}$.

(v) folgt aus (iv) und (ii), denn $n = e_1 n_1 + \cdots e_r n_r$, und (vi) ist ein Spezialfall davon. $\diamond$

Korollar 1 *Sei $f \in \mathbb{F}_q[T]$ mit $f(0) \neq 0$ und $F = \Psi(f)$ das zugehörige q-Polynom. Dann ist die Anzahl der q-primitiven Nullstellen von F genau gleich $\varphi_q(f)$.*

Beweis. Das war gerade die Formel am Ende des Beweises von Satz 3. $\diamond$

A.3 Normalbasen

Für einen Erweiterungskörper K von $\mathbb{F}_q$ der Dimension n heißt eine Basis der Gestalt x, x^q, …, $x^{q^{n-1}}$ **Normalbasis** von K über $\mathbb{F}_q$, und zwar die von x erzeugte.

Bezüglich einer Normalbasis ist das Potenzieren mit q, also der Frobenius-Automorphismus sehr einfach auszudrücken; dadurch wird das explizite Rechnen in K in manchen Situationen sehr effizient.

Satz 4 *Sei K ein Erweiterungskörper von $\mathbb{F}_q$. Dann gilt:*

(i) *$x \in K$ erzeugt genau dann eine Normalbasis, wenn x q-primitive Nullstelle von $T^{q^n} - T$ ist.*

(ii) (Hensel) *Es gibt eine Normalbasis von K über $\mathbb{F}_q$.*

(iii) *Es gibt genau*

$$\frac{\varphi_q(T^n - 1)}{n}$$

verschiedene Normalbasen von K über $\mathbb{F}_q$.

(iv) *Die bezüglich der Spurform zu einer Normalbasis duale Basis ist ebenfalls Normalbasis.*

Beweis. (i) K ist die Nullstellenmenge des q-Polynoms $F = T^{q^n} - T \in \mathbb{F}_q[T]$. Sei x eine q-primitive Nullstelle von F. Dann ist K der kleinste Unterraum

von K, der x, x^q, ..., $x^{q^{n-1}}$ enthält. Also wird K von diesen Elementen aufgespannt. Da es n Stück sind, müssen sie linear unabhängig sein.

Erzeugt umgekehrt x eine Normalbasis, so sind die n Elemente x, x^q, ..., $x^{q^{n-1}}$ linear unabhängig, und alle Linearkombinationen von ihnen sind Nullstellen von $T^{q^n} - T$. Also ist dieses das q-Minimalpolynom von x.

(ii) (ORE) Nach Satz 3 hat $T^{q^n} - T$ eine primitive Nullstelle. Alle q^n Nullstellen dieses Polynoms liegen aber in K. Die Behauptung folgt aus (i).

(iii) Jeweils n der q-primitiven Nullstellen erzeugen dieselbe Normalbasis, und die Anzahl der q-primitiven Nullstellen ist $\varphi_q(T^n - 1)$.

(iv) Sei $x, x^q, \ldots, x^{q^{n-1}}$ eine beliebige Normalbasis. Die duale Basis besteht aus den eindeutig bestimmten $y_0, \ldots, y_{n-1} \in K$ mit $\mathrm{Tr}(y_i \cdot x^{q^j}) = \delta_{ij}$. Da die Spur unter dem FROBENIUS-Automorphismus invariant ist, folgt

$$\mathrm{Tr}(y_i^q \cdot x^{q^{j+1}}) = \delta_{ij} = \mathrm{Tr}(y_{i+1} \cdot x^{q^{j+1}}),$$

wobei $y_n := y_0$ gesetzt ist. Daher ist $y_{i+1} = y_i^q$ für alle i, also $y_i = y_0^{q^i}$ für alle i. $\diamond$

Bemerkungen

1. Das Polynom $f = \varphi(T^n - 1)$ hat die Ableitung $f' = n \cdot T^{n-1}$. Alle Nulstellen x von f sind $\neq 0$. Also ist für eine solche

   $$f'(x) = n \cdot x^{n-1} = 0 \Leftrightarrow p|n,$$

   wobei p die Charakteristik von F_q ist. Ist also p kein Teiler von n, so

   $$\varphi_q(T^n - 1) = (q^{n_1} - 1) \cdots (q^{n_r} - 1),$$

   und es sind „nur“ noch die Grade n_i der Primteiler dieses Polynoms zu bestimmen.

2. Ist $q = 2$ und n ungerade, so ist

   $$\varphi_2(T^n - 1) = (2^{n_1} - 1) \cdots (2^{n_r} - 1),$$

   ungerade. Es kann also nicht jede Normalbasis von ihrer dualen Basis verschieden sein – sonst müsste die Gesamtzahl gerade sein. Damit ist gezeigt:

Satz 5 (MACWILLIAMS/SLOANE) *Ist n ungerade, so hat der Körper $\mathbb{F}_{2^n}$ eine zu sich selbst duale Normalbasis.*

Anmerkung. Es ist bekannt, dass $\mathbb{F}_{2^n}$ für gerades n genau dann eine selbstduale Normalbasis hat, wenn $n \equiv 2 \pmod 4$.

A.4 Potenzabbildungen

In diesem Abschnitt werden für den Körper $K = \mathbb{F}_{2^n}$ mit 2^n Elementen die Abbildungen

$$f_s \colon K \longrightarrow K, \quad f_s(x) = x^s, \quad \text{für } s \in \mathbb{Z}$$

untersucht; für $s \leq 0$ wird $f_s(0) = 0$ gesetzt.

Bemerkungen

1. Auf $K^\times$ ist $f_0 = f_{2^n-1} = 1$ konstant.
2. Auf $K^\times$ ist $f_{2^n-2}(x) = x^{-1}$, also f_{2^n-2} die Inversionsabbildung.
3. $f_{2^k} = \varphi^k$ mit dem FROBENIUS-Automorphismus φ.
4. Wie sieht die algebraische Normalform von f_0 aus? Wir kennen sie schon aus Abschnitt 1.3: Bezüglich einer geeigneten Basis von K über $\mathbb{F}_2$ mit 1 als erstem Basisvektor sind alle Komponenten 0 bis auf die erste, die die algebraische Normalform

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

   hat. Insbesondere ist $\operatorname{Grad} f_0 = n$.
5. Für alle $s, t \in \mathbb{Z}$ gilt $f_s f_t = f_{s+t}$, denn $x^s x^t = x^{s+t}$ für alle $x \neq 0$.
6. Insbesondere ist $f_{s+2^n-1} = f_s f_{2^n-1} = f_s$ für alle $s \in \mathbb{Z}$. Die Zuordnung $\mathbb{Z} \longrightarrow K^K$, $s \mapsto f_s$, hat also die Periode $2^n - 1$.
7. $\operatorname{Grad} f_{s+t} \leq \operatorname{Grad} f_s + \operatorname{Grad} f_t$; allgemeiner gilt sogar für $f, g \colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$ beliebig und $\gamma : \mathbb{F}_2^q \times \mathbb{F}_2^q \longrightarrow \mathbb{F}_2^r$ bilinear, dass $\operatorname{Grad} \gamma \circ (f, g) \leq \operatorname{Grad} f + \operatorname{Grad} g$.
8. Für alle $s, t \in \mathbb{Z}$ gilt $f_s \circ f_t = f_{st}$, denn $(x^t)^s = x^{st}$ für alle $x \neq 0$.
9. f_{st} ist genau dann bijektiv, wenn f_s und f_t bijektiv sind. Sind nämlich f_s und f_t bijektiv, so auch $f_{st} = f_s \circ f_t$. Ist f_s nicht bijektiv, so nicht surjektiv, also $f_s \circ f_t$ nicht surjektiv. Ist f_t nicht bijektiv, so nicht injektiv, also $f_s \circ f_t$ nicht injektiv.
10. Ist $s = 2^k t$ mit ungeradem t, so ist $\operatorname{Grad} f_s = \operatorname{Grad} f_t$. Es ist nämlich $f_s = f_{2^k} \circ f_t = \varphi^k \circ f_t$, und φ^k ist als Automorphismus von K linear über dem Grundkörper $\mathbb{F}_2$.

Insbesondere hat f_s dem ersten Anschein zum Trotz im allgemeinen *nicht* den algebraischen Grad s. Man erhält relativ leicht eine obere Schranke. Dazu sei $s \geq 1$ und $s = \sum_{i \in I_s} 2^i$ die Binärdarstellung. Dann heißt

$$\mathrm{wt}(s) := \#I_s$$

das HAMMING-**Gewicht** von s.

Hilfssatz 7 *Sei $s \geq 1$. Dann hat die Potenzabbildung $f_s : K \longrightarrow K$ den algebraischen Grad* $\operatorname{Grad} f_s \leq \mathrm{wt}(s)$.

Beweis. Falls $\mathrm{wt}(s) = 1$, ist $s = 2^k$ für ein k, also $f_s = \varphi^k$ linear und nicht 0, also vom Grad 1.

Für einen Induktionsbeweis wird jetzt $\mathrm{wt}(s) \geq 2$ angenommen. Dann ist $f_s = f_t \varphi^k$, wobei k das größte Element von I_s und $t = s - 2^k$ ist. Mit Bemerkung 7 folgt

$$\operatorname{Grad} f_s \leq \operatorname{Grad} f_t + 1 \leq \mathrm{wt}(t) + 1 = \mathrm{wt}(s)$$

nach Induktionsvoraussetzung. $\diamond$

Um in Hilfssatz 7 die Gleichheit zu beweisen, wird ausgenutzt, dass f_s für $s \leq 2^n - 1$ das Produkt von $\mathrm{wt}(s)$ verschiedenen Automorphismen von K ist. Betrachtet wird also eine Abbildung

$$f = \sigma_1 \cdots \sigma_m$$

mit paarweise verschiedenen $\sigma_i \in \operatorname{Aut} K$ für $i = 1, \ldots, m$. Zunächst zwei Hilfssätze:

Hilfssatz 8 *Seien $\sigma_1, \ldots, \sigma_r \in \operatorname{Aut} K$, $a, u \in K$. Dann ist*

$$\Delta_u(a\sigma_1 \cdots \sigma_r)(x) = a \cdot \sum_{i=1}^{r} \sigma_i(u) \prod_{j \neq i} \sigma_j(x) + h(x)$$

mit $h \colon K \longrightarrow K$ vom Grad $< r$.

Beweis. Das folgt aus der Formel

$$\Delta_u(a\sigma_1 \cdots \sigma_r)(x) = a \cdot \sigma_1(x+u) \cdots \sigma_r(x+u) - a \cdot \sigma_1(x) \cdots \sigma_r(x)$$

mit dem Distributivgesetz. $\diamond$

Hilfssatz 9 *Für $x, u_1, \ldots, u_r \in K$ und $f = \sigma_1 \cdots \sigma_m$ gilt:*

$$\Delta_{u_1 \ldots u_r} f(x) = \sum_{I = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, m\}} \left[\sum_{\pi \in \mathcal{S}_r} \prod_{j=1}^{r} \sigma_{\pi(i_j)}(u_j) \right] \prod_{k \notin I} \sigma_k(x) + h(x)$$

mit $h \colon K \longrightarrow K$ vom Grad $< m - r$.

Beweis. Der Induktionsanfang $r = 0$ ist trivial: Auf der rechten Seite gibt es nur einen Summanden, nämlich für $I = \emptyset$, und der ist $\sigma_1(x) \cdots \sigma_m(x)$

Für den Schluss von r auf $r+1$ wird mit Hilfssatz 8 berechnet

$$\begin{aligned}
\Delta_{u_0 \ldots u_r} f(x) &= \Delta_{u_0}(\Delta_{u_1 \ldots u_r} f)(x) \\
&= \sum_{I=\{i_1,\ldots,i_r\}} \left[\sum_{\pi \in \mathcal{S}_r} \prod_{j=1}^{r} \sigma_{\pi(i_j)}(u_j) \right] \left[\sum_{k \notin I} \sigma_k(u_0) \cdot \prod_{l \notin I \cup \{k\}} \sigma_l(x) \right] \\
&\quad + \Delta_{u_0} h(x) \\
&= \sum_{J=\{i_0,\ldots,i_r\}} \left[\sum_{\pi \in \mathcal{S}_{r+1}} \prod_{j=0}^{r} \sigma_{\pi(i_j)}(u_j) \right] \prod_{l \notin J} \sigma_l(x) + \tilde{h}(x)
\end{aligned}$$

mit $\tilde{h}$ vom algebraischen Grad $< m - r - 1$. $\diamond$

Speziell im Fall $r = m$, also $I = \{1, \ldots, m\}$, folgt

Korollar 1 *Sind die σ_i paarweise verschieden, so ist die Differenzenfunktion*

$$\Delta_{u_1 \ldots u_m} f(x) = \sum_{\pi \in \mathcal{S}_m} \prod_{j=1}^{m} \sigma_{\pi(j)}(u_j)$$

konstant $\neq 0$.

Beweis. Es ist

$$\begin{aligned}
\Delta_{u_1 \ldots u_m} f(x) &= \sum_{\pi \in \mathcal{S}_m} \left[\prod_{j=1}^{m-1} \sigma_{\pi(j)}(u_j) \right] \sigma_{\pi(m)}(u_m) \\
&= \sum_{k=1}^{m} \left[\sum_{\pi \in \mathcal{S}_m, \pi(m)=k} \prod_{j=1}^{m-1} \sigma_{\pi(j)}(u_j) \right] \sigma_k(u_m).
\end{aligned}$$

Wäre das 0 für alle $u_m \in K$, so wäre wegen der linearen Unabhängigkeit der Charaktere, Satz 1,

$$\sum_{\pi \in \mathcal{S}_m, \pi(m)=k} \prod_{j=1}^{m-1} \sigma_{\pi(j)}(u_j) = 0$$

für alle k und $u_1, \ldots, u_{m-1} \in K$. Mit Induktion würde schließlich folgen $\sigma_1(u_1) = \cdots = \sigma_m(u_1) = 0$ für alle $u_1 \in K$, Widerspruch. $\diamond$

Korollar 2 *Sind $\sigma_1, \ldots, \sigma_m$ paarweise verschiedene Automorphismen von K, so ist* $\operatorname{Grad} \sigma_1 \cdots \sigma_m = m$.

Damit ist gezeigt:

Satz 6 *Die Potenzabbildung* $f_s\colon K \longrightarrow K$ *hat für* $1 \le s \le 2^n - 1 = \#K - 1$ *den algebraischen Grad* $\mathrm{wt}(s)$.

Korollar 1 *Die* (2^k+1)*-te Potenz* $f_{2^k+1}\colon K \longrightarrow K$ *hat den algebraischen Grad* 2, *wenn* $n = \operatorname{Dim} K \ge k+1$.

Insbesondere sind f_3, f_5, f_9, f_{17} quadratische Abbildungen, wenn $n \ge 2, 3, 4, 5$ ist, und $f_{-1} = f_{2^n-2}$ hat den Grad $n-1$.

Als nächstes wird untersucht, wann f_s bijektiv ist. Es ist $K^\times$ eine Gruppe der Ordnung $2^n - 1$ und $f_s\colon K^\times \longrightarrow K^\times$ ein Gruppenhomomorphismus. In seinem Kern liegen genau die Elemente $x \in K$ mit $x^s = 1$, also $\operatorname{Ord} x | s$, also $\operatorname{Ord} x | \operatorname{ggT}(s, 2^n - 1)$. Damit ist gezeigt:

Satz 7 *Ist* K *ein endlicher Körper der Charakteristik* 2 *und Dimension* n *über* $\mathbb{F}_2$, *so ist die Potenzabbildung* $f_s\colon K \longrightarrow K$, *genau dann bijektiv, wenn* s *zu* $2^n - 1$ *teilerfremd ist.*

Korollar 1 (i) f_3 *ist genau dann bijektiv, wenn* n *ungerade ist.*
(ii) f_5 *ist genau dann bijektiv, wenn* n *kein Vielfaches von* 4 *ist.*
(iii) f_7 *ist genau dann bijektiv, wenn* n *kein Vielfaches von* 3 *ist.*

Beweis. Das folgt, weil $p = 3, 5, 7$ Primzahl ist und $p | 2^n - 1$ genau dann, wenn $2^n \equiv 1 \pmod{p}$. Und 2 hat mod $3, 5, 7$ die multiplikative Ordnung $2, 4, 3$. $\diamond$

A.5 Quadratische Gleichungen in Charakteristik 2

Sei weiterhin $K = \mathbb{F}_{2^n}$ der Körper mit 2^n Elementen. Wir wollen die Nullstellen des quadratischen Polynoms

$$f = aT^2 + bT + c \in K[T] \quad \text{mit } a \neq 0$$

bestimmen.

Der Fall $b = 0$ ist sehr einfach. Es ist

$$a \cdot f = (aT)^2 + ac = g(aT) \quad \text{mit } g = T^2 + ac \in K[T].$$

Da ac in K ein Quadrat ist, $ac = d^2$, ist

$$g = (T+d)^2 = h(T+d) \quad \text{mit } h = T^2 \in K[T],$$

und f hat genau die eine Nullstelle $\frac{d}{a}$. Zur expliziten Berechnung muss die Quadratwurzel aus ac gezogen werden.

Sei nun $b \neq 0$. Dann ist

$$\frac{a}{b^2} \cdot f = (\frac{a}{b}\,T)^2 + \frac{a}{b}\,T + \frac{ac}{b^2} = g(\frac{a}{b}\,T) \quad \text{mit } g = T^2 + T + d,\ d = \frac{ac}{b^2} \in K.$$

Betrachten wir also die Nullstellen eines solchen Polynoms g. Da die Ableitung konstant 1 ist, hat g in K entweder keine Nullstelle oder zwei verschiedene (einfache) Nullstellen. Sei u eine Nullstelle von g im algebraischen Abschluss von K. Dann ist $u+1$ die andere, und $u(u+1) = d$, also $d = u^2+u$.

Hilfssatz 10 *$g = T^2 + T + d \in K[T]$ hat genau dann eine Nullstelle u in K, wenn $\mathrm{Tr}(d) = 0$. Ist das der Fall, so $g = h(T + u)$ mit $h = T^2 + T$.*

Beweis. „$\Longrightarrow$“: Ist $u \in K$, so ist $\mathrm{Tr}(d) = \mathrm{Tr}(u^2) + \mathrm{Tr}(u) = 0$.

„$\Longleftarrow$“: Sei umgekehrt $\mathrm{Tr}(d) = 0$. Dann ist

$$\begin{aligned} 0 &= \mathrm{Tr}(d) = d + d^2 + \cdots + d^{2^{n-1}} \\ &= (u^2 + u) + (u^4 + u^2) + \cdots + (u^{2^n} + u^{2^{n-1}}) \\ &= u + u^{2^n}, \end{aligned}$$

also $u^{2^n} = u$ und somit $u \in K$.

Der Zusatz ist trivial. $\diamond$

Anmerkung. Der Hilfssatz ist ein Spezialfall des sogenannten Theorem 90 von Hilbert, additive Form. Zur expliziten Bestimmung der Nullstelle hilft er leider gar nicht. Immerhin führt er die Auflösung auf die Auflösung der Gleichung $u^2 + u = ac/b^2$ nach u zurück.

Korollar 1 *$g = T^2+T+d \in K[T]$ ist genau dann irreduzibel, wenn $\mathrm{Tr}(d) = 1$. Ist das der Fall, so $g = h(T+r)$ mit $h = T^2+T+e$, wobei e ein beliebiges Element von K mit Spur $\mathrm{Tr}(e) = 1$ ist und $r \in K$ mit $r^2 + r = d + e$.*

Beweis. g ist in $K[T]$ genau dann irreduzibel, wenn es kein Nullstelle in K hat. Der Zusatz folgt, weil $d + e$ die Spur 0 hat, also von der Form $r^2 + r$ ist. $\diamond$

Damit ist gezeigt:

Satz 8 (Nullstellen) *Sei K ein endlicher Körper der Charakteristik 2 und $f = aT^2 + bT + c \in K[T]$ vom Grad 2. Dann gilt:*

(i) *f hat genau eine Nullstelle in $K \iff b = 0$.*

(ii) *f hat genau zwei Nullstellen in $K \iff b \neq 0$ und $\mathrm{Tr}(\frac{ac}{b^2}) = 0$.*

(iii) *f hat keine Nullstelle in $K \iff b \neq 0$ und $\mathrm{Tr}(\frac{ac}{b^2}) = 1$.*

Satz 9 (Normalform) *Sei K ein endlicher Körper der Charakteristik 2 und $f = aT^2 + bT + c \in K[T]$ vom Grad 2. Dann gibt es ein $e \in K^\times$ und eine affine Transformation $\alpha : K \longrightarrow K$, $\alpha(x) = rx + s$ mit $r \in K^\times$ und $s \in K$, so dass*

$$e \cdot f \circ \alpha = T^2, \quad T^2 + T \quad \text{oder } T^2 + T + d,$$

wobei $d \in K$ ein beliebiges Element mit Spur $\mathrm{Tr}(d) = 1$ ist. Im Fall $n = \mathrm{Dim}\, K$ ungerade ist $e = 1$ wählbar.

Anmerkung. Eine Verallgemeinerung auf einen beliebigen endlichen Grundkörper $\mathbb{F}_q$ statt $\mathbb{F}_2$ und Polynome $T^q - T - d$ ist der Satz von Artin-Schreier, der die zyklischen Körpererweiterungen vom Grad q charakterisiert.

A.6 Elliptische Kurven

Sei K ein Körper und $f \in K[X, Y]$ ein Polynom in zwei Unbestimmten vom Grad $n \geq 1$. Sei $L \supseteq K$ ein Erweiterungskörper. Dann heißt

$$C(L) := \{(x, y) \in L^2 \mid f(x, y) = 0\}$$

die Menge der L-wertigen Punkte der (affinen) ebenen algebraischen Kurve C zu f.

> [Die „Kurve“ C selbst ist die Zuordnung $C : \mathrm{Alg}_K \longrightarrow$ Meng; in der Sprache der Kategorientheorie ist das ein Funktor, in der Sprache der Algebraischen Geometrie speziell ein Schema.]

Eine solche affine Kurve lässt sich zu einer projektiven Kurve erweitern. Dazu betrachtet man die homogenisierte Form von f,

$$F = Z^n \cdot f(\frac{X}{Z}, \frac{Y}{Z}) \in K[X, Y, Z],$$

die ein homogenes Polynom vom Grad n ist, und die projektive Ebene $\mathbb{P}^2$ über K mit

$$\mathbb{P}^2(L) = \{(x : y : z) \mid x, y, z \in L, \text{nicht alle } 0\},$$

wobei die „homogenen Koordinaten“ $(x : y : z)$ die Bahnen von $L^3 - \{0\}$ unter der Operation

$$(x, y, z) \overset{\lambda \in L^\times}{\mapsto} (\lambda x, \lambda y, \lambda z)$$

der multiplikativen Gruppe $L^\times$ repräsentieren. Damit ist

$$\bar{C}(L) = \{(x : y : z) \in \mathbb{P}^2(L) \mid F(x, y, z) = 0\}$$

die Menge der L-wertigen Punkte der (projektiven) ebenen algebraischen Kurve zu F.

„Punkte im Endlichen“ sind die $(x : y : z)$ mit $z \neq 0$, also die $(x : y : 1)$. Es gilt

$$F(x, y, 1) = 0 \Longleftrightarrow f(x, y) = 0,$$

die Punkte der projektiven Kurve im Endlichen sind also (bei kanonischer Identifizierung) die Punkte der affinen Kurve. Die übrigen Punkte von $\mathbb{P}^2$, also die $(x : y : 0)$, heißen „Punkte im Unendlichen“.

Elliptische Kurven sind die Kurven zu den Polynomen

$$f = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \in K[X, Y]$$

in der affinen Version bzw.

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \in K[X, Y, Z]$$

in der projektiven Version.

> [Außerdem verlangt man, dass die elliptische Kurve keine Singularitäten hat; d. h., es gibt in keinem Erweiterungskörper von K eine gemeinsame Nullstelle des Polynoms und aller seiner partiellen Ableitungen.]

Durch lineare Koordinatentransformation lässt sich f

- im Fall $\operatorname{char} K \neq 2, 3$ auf die Normalform

$$Y^2 - X^3 - aX - b \in K[X, Y]$$

- im Fall $\operatorname{char} K = 3$ auf die Normalform

$$Y^2 - X^3 - aX^2 - bX - c \in K[X, Y]$$

bringen (ohne Beweis – **Übungsaufgabe**). Zur Anwendung auf BOOLEsche Abbildungen interessiert der Fall $\operatorname{char} K = 2$. Hier sind zwei Fälle zu unterscheiden, der **gewöhnliche Fall** mit $a_1 \neq 0$ und der **supersinguläre Fall** mit $a_1 = 0$.

Im *gewöhnlichen Fall* geht f nach der Transformation $X \mapsto \frac{X}{a_1} - \frac{a_3}{a_1}$ und anschließender Umbenennung der Koeffizienten über in

$$Y^2 + XY - X^3 - b_2X^2 - b_4X - b_6,$$

nach der weiteren Transformation $Y \mapsto Y + b_4$ in die Normalform

$$Y^2 + XY - X^3 - aX^2 - b.$$

Zu einer andere Version der Normalform kommt man durch die weitere Transformation $Y \mapsto Y + sX$; zunächst erhält man

$$Y^2 + s^2X^2 + XY + sX^2 - X^3 - aX^2 - b.$$

Ist nun $\operatorname{Tr} a = 0$, so kann man nach Hilfssatz 10 ein s wählen mit $s^2 + s = a$, also erhält man die Gestalt $Y^2 + XY - X^3 - b$, die man durch $Y \mapsto Y + t$ mit $t^2 = b$ noch in die alternative Normalform

$$(E_a^+) \qquad\qquad Y^2 + XY - X^3 - aX$$

umformen kann. Ist dagegen $\operatorname{Tr} a = 1$, so $\operatorname{Tr}(a+\tau) = 0$ für ein fest gewähltes $\tau \in K$ mit $\operatorname{Tr} \tau = 1$; also kann man s wählen mit $s^2 + s = a + \tau$ und erhält die Gestalt $Y^2 + XY - X^3 - \tau X^2 - b$, die durch $Y \mapsto Y + t$ wie oben in die Normalform

$$(E_a^-) \qquad Y^2 + XY - X^3 - \tau X^2 - aX$$

umgewandelt wird. In beiden Fällen ist $a \neq 0$, da sonst 0 Singularität der Kurve ist: $\frac{\partial f}{\partial X} = Y - X - a$, $\frac{\partial f}{\partial Y} = X$ in beiden Fällen.

Damit sind die gewöhnlichen elliptischen Kurven im Fall $\operatorname{char} K = 2$ in zwei Scharen klassifiziert, die jeweils durch $a \in K^\times$ parametrisiert werden.

Im *supersingulären Fall* ist notwendig $a_3 \neq 0$, da es sonst wegen $\frac{\partial f}{\partial Y} = 0$ (konstant) Singularitäten gäbe, und durch die Transformation $X \mapsto X - a_2$ kommt man zur Normalform

$$Y^2 + aY - X^3 - bX - c$$

mit $a \in K^\times$. Dieser Fall interessiert im folgenden nicht weiter.

Die Aufgabe, die Anzahl der K-wertigen Punkte einer elliptischen Kurve für einen endlichen Körper K zu bestimmen oder abzuschätzen, gehört zu den ganz prominenten mathematischen Problemen. Ein tiefliegendes Ergebnis ist z. B. der Satz von Hasse:

Satz 10 (Hasse) *Sei K ein endlicher Körper mit q Elementen, E eine über K definierte (projektive) elliptische Kurve und $N = \#E(K)$ die Anzahl ihrer K-wertigen Punkte. Dann gilt:*

$$N = q + 1 + s \quad \textit{mit} \quad |s| \leq 2 \cdot \sqrt{q}.$$

(D. h., N weicht nicht zu stark von q ab.)

Der Beweis wird hier nicht wiedergegeben (siehe [131]); er beruht auf der Untersuchung der Zeta-Funktion der elliptischen Kurve.

Im Fall $q = 2^n$ wird die Formel zu

$$N = 2^n + 1 + s \quad \text{mit} \quad |s| \leq 2^{\frac{n}{2}+1}.$$

Die gewöhnlichen elliptischen Kurven in Charakteristik 2 werden in der projektiven Version durch die Polynome

$$\begin{array}{ll} & Y^2Z + XYZ \quad -X^3 - aXZ^2 \\ \text{bzw.} & Y^2Z + XYZ \quad -X^3 - \tau X^2Z - aXZ^2 \end{array}$$

definiert. Vertauscht man X und Z (das bedeutet geometrisch, eine andere Gerade als „unendlich fern“ zu interpretieren), so werden diese Normalformen zu

$$\begin{array}{ll} (F_a^+) & XY^2 + XYZ - aX^2Z - Z^3 \\ (F_a^-) & XY^2 + XYZ - aX^2Z - \tau XZ^2 - Z^3 \end{array}$$

mit $a \in K^\times$ beliebig.

Zählen wir in dieser Version die K-wertigen Punkte $(x : y : z)$ der zugehörigen elliptischen Kurve für $K = \mathbb{F}_{2^n}$:

Im „Unendlichen“, also für $z = 0$, heißt die Bedingung $xy^2 = 0$, also $x = 0$ oder $y = 0$, also gibt es genau zwei solche Punkte: $(1 : 0 : 0)$ und $(0 : 1 : 0)$.

Im „Endlichen“ können wir $z = 1$ setzen und erhalten für (F_a^+) die Bedingung

$$(x : y : 1) \in E(K) \Longleftrightarrow xy^2 + xy = ax^2 + 1 \Longleftrightarrow y^2 + y = ax + \frac{1}{x},$$

denn mit $x = 0$ gibt es keine Lösung.

- Ist $x \in K^\times$ ein Wert mit $\mathrm{Tr}(ax + \frac{1}{x}) = 0$, so gibt es genau zwei Werte von y, so dass die Bedingung erfüllt ist.
- Ist $x \in K^\times$ ein Wert mit $\mathrm{Tr}(ax + \frac{1}{x}) \neq 0$, also $= 1$, so ist die Bedingung nicht erfüllbar.

Setzt man

$$N_a^+ := \#\{x \in K^\times \mid \mathrm{Tr}(ax + \frac{1}{x}) = 0\},$$

so ist gezeigt:

Satz 11 *Die für $a \in K^\times$ durch (F_a^+) definierte elliptische Kurve über $K = \mathbb{F}_{2^n}$ hat genau*

$$2N_a^+ + 2$$

K-wertige Punkte.

Die gleiche Überlegung für (F_a^-) ergibt die Bedingung

$$(x : y : 1) \in E(K) \Longleftrightarrow xy^2 + xy = ax^2 + 1 + \tau x \Longleftrightarrow y^2 + y = ax + \frac{1}{x} + \tau.$$

Hier gibt es keine Möglichkeit für y, wenn $\mathrm{Tr}(ax + \frac{1}{x}) = 0$, und genau zwei, wenn $\mathrm{Tr}(ax + \frac{1}{x}) = 1$. Mit

$$N_a^- := \#\{x \in K^\times \mid \mathrm{Tr}(ax + \frac{1}{x}) = 1\}$$

folgt also:

Korollar 1 *Die für $a \in K^\times$ durch (F_a^-) definierte elliptische Kurve über $K = \mathbb{F}_{2^n}$ hat genau*

$$2N_a^- + 2$$

K-wertige Punkte.

Hilfssatz 11 *N_a^+ ist ungerade, N_a^- gerade für jedes $a \in K^\times$.*

Beweis. Da $N_a^+ + N_a^- = 2^n - 1$, genügt es, die erste Aussage zu beweisen. Es gibt genau ein $b \in K^\times$ mit $b^2 = a^{-1}$; für dieses ist $ab = b^{-1}$, also $\mathrm{Tr}(ab + b^{-1}) = 0$. Alle anderen Lösungen von $\mathrm{Tr}(ax + x^{-1}) = 0$ kommen paarweise vor: Ist $x \in K^\times - \{b\}$ eine solche, so ist auch $y = a^{-1}x^{-1}$ eine, denn $\mathrm{Tr}(ay + y^{-1}) = \mathrm{Tr}(x^{-1} + ax) = 0$, und $y \neq x$. $\diamond$

Korollar 2 *Sei E eine gewöhnliche elliptische Kurve über $K = \mathbb{F}_{2^n}$ mit $n \geq 2$ und $N = 2^n + 1 + s$ die Anzahl ihrer K-wertigen Punkte. Dann ist s ungerade, und zwar $s = 2N_a^+ + 1 - 2^n \equiv 3 \pmod 4$ im Fall (F_a^+), $s = 2N_a^- + 1 - 2^n \equiv 1 \pmod 4$ im Fall (F_a^-).*

Beweis. $2^n + 1 + s = N = 2N_a^\pm + 2$, und für $n \geq 2$ ist 2^n durch 4 teilbar. $\diamond$

Die relevanten Zahlen $N_a^\pm$ kann man durch Exponential-Summen, sogenannte Kloosterman-Summen, ausdrücken: Die reellwertige Funktion

$$\kappa \colon K^\times \longrightarrow \mathbb{R}$$

sei definiert durch

$$\kappa(u) := \sum_{x \in K^\times} (-1)^{\mathrm{Tr}(ux + x^{-1})}.$$

Klar, dass

$$\kappa(u) = N_u^+ - N_u^- = 2N_u^+ - 2^n + 1 = s,$$

wobei $2^n + 1 + s$ die Anzahl der Punkte der gewöhnlichen elliptischen Kurve vom Typ (F_u^+) ist. Also gilt für $n \geq 2$:

Korollar 3 (i) $\kappa(u) \equiv 3 \pmod 4$ *für alle $u \in K^\times$.*
(ii) $|\kappa(u)| \leq 2^{\frac{n}{2}+1}$ *für alle $u \in K^\times$.*

An dieser Stelle wird ein weiteres tiefliegendes Ergebnis aus der Theorie der elliptischen Kurven ohne Beweis verwendet – siehe [137]:

Satz 12 (HONDA) *Für jede ungerade Zahl $s \in \mathbb{Z}$ mit $|s| \leq 2^{\frac{n}{2}+1}$ gibt es eine gewöhnliche elliptische Kurve über $K = \mathbb{F}_{2^n}$, die genau $2^n + 1 + s$ K-wertige Punkte hat.*

Klar im Fall $n \geq 2$, dass $s \equiv 3 \pmod 4$ genau dann, wenn die Kurve vom Typ (F_a^+) ist. Daraus folgt unmittelbar:

Hauptsatz 1 (LACHAUD/WOLFMANN) *Die* KLOOSTERMAN*-Funktion κ nimmt für $n \geq 2$ genau die Werte $s \in \mathbb{Z}$ mit $|s| \leq 2^{\frac{n}{2}+1}$ und $s \equiv 3 \pmod 4$ an.*

B Die aktuellen Weltrekorde

Über die hier bewiesenen Aussagen hinaus sind für die Optimierung der Nichtlinearität weitere Ergebnisse in der Literatur zu finden. Quellen: [13], [136]. Die „Weltrekorde“ sind in den folgenden Tabellen zusammengestellt. Ferner ist noch erwähenswert, dass $\sigma(15,1) \geq 16276$ nach [107].

$\Lambda(n,q)$	$q=1$	2	3	4	5	6	7	8
$n=1$	1	1	1	1	1	1	1	1
2	$\frac{1}{4}$	1	1	1	1	1	1	1
3	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{9}{16}$	$[\frac{9}{16}, 1]$	...	...	...
4	$\frac{1}{16}$	$\frac{1}{16}$	$[\frac{9}{64}, \frac{1}{4}]$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{9}{16}$	$\frac{9}{16}$
5	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$[\frac{9}{64}, \frac{1}{4}]$	...	$[\frac{49}{256}, \frac{1}{4}]$
6	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$[\frac{25}{1024}, \frac{1}{16}]$	$[\frac{9}{256}, \frac{1}{16}]$	...	$[\frac{49}{1024}, \frac{1}{16}]$	$\frac{1}{16}$
7	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$\frac{1}{64}$	$[\frac{25}{1024}, \frac{1}{16}]$
8	$\frac{1}{256}$	$\frac{1}{256}$	$\frac{1}{256}$	$\frac{1}{256}$	$[\frac{81}{16384}, \frac{1}{64}]$	...	...	$[\frac{9}{1024}, \frac{1}{64}]$

$\sigma(n,q)$	$q=1$	2	3	4	5	6	7	8
$n=1$	0	0	0	0	0	0	0	0
2	1	0	0	0	0	0	0	0
3	2	2	2	1	$[0,1]$	...	...	...
4	6	6	$[4,5]$	4	4	4	2	2
5	12	12	12	12	12	$[8,10]$	...	$[8,9]$
6	28	28	28	$[24,27]$	$[24,26]$	$[24,26]$	$[24,25]$	24
7	56	56	56	56	56	56	56	$[48,54]$
8	120	120	120	120	$[112,119]$	...	...	$[112,116]$

$\Omega(n,q)$	$q=1$	2	3	4	5	6	7	8
$n=1$	1	1	1	1	1	1	1	1
2	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
3	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
4	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$
5	$[\frac{9}{16}, \frac{3}{4}]$	$[\frac{5}{16}, \frac{1}{2}]$	$[\frac{3}{16}, \frac{3}{8}]$	$[\frac{1}{8}, \frac{5}{16}]$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
6	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$[\frac{3}{32}, \frac{1}{4}]$	$[\frac{1}{16}, \frac{1}{4}]$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$
7	$[\frac{33}{64}, \frac{41}{64}]$	$[\frac{17}{64}, \frac{9}{16}]$	$[\frac{9}{64}, \frac{9}{16}]$	$[\frac{5}{64}, \frac{9}{16}]$	$[\frac{3}{64}, \frac{9}{16}]$	$[\frac{1}{32}, \frac{9}{16}]$	$\frac{1}{64}$	$\frac{1}{64}$
8	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{16}$	$[\frac{5}{128}, \frac{1}{2}]$	$[\frac{3}{128}, \frac{1}{2}]$	$[\frac{1}{64}, \frac{1}{2}]$	$\frac{1}{128}$

C Quellcode

```
/*** bma.c *************************************************************/
/*                                                                     */
/* Analysis of Boolean Maps (S-Boxes)  V 0.4                           */
/*                                                                     */
/* Klaus Pommerening                                                   */
/* Institut fuer Medizinische Biometrie, Epidemilogie und              */
/*    Informatik                                                       */
/* Johannes-Gutenberg-Universitaet                                     */
/* D-55101 Mainz                                                       */
/* pom@imsd.uni-mainz.de                                               */
/*     21 August 2001 - last change 15 September 2001                  */
/*                                                                     */
/* Send bug reports and comments by e-mail.                            */
/***********************************************************************/
/*                                                                     */
/* Copyright by the author.                                            */
/* The use of this program code is free for private and                */
/*   educational use.                                                  */
/* Usual disclaimers apply.                                            */
/***********************************************************************/
/*                                                                     */
/* Usage: bma <input >output                                           */
/*   [I. e. use input and output redirection]                          */
/*                                                                     */
/* Input from stdin: Matrix of coefficients of a boolean map in        */
/*   Algebraic Normal Form (ANF) --                                    */
/*     one line per component function.                                */
/*     Let K = Galois Field with 2 elements.                           */
/*     A map f: K^n ---> K^q is given by q components,                 */
/*     each component given by 2^n coefficients in ANF.                */
/*     [Input in lines instead of columns for convenience.]            */
/*                                                                     */
/* Output to stdout:                                                   */
/*   1. ANF -- one column per component function                       */
/*   2. Truth table (one column per component function)                */
/*   3. Characteristic function as a 2^n x 2^q matrix                  */
/*   4. Walsh transform of characteristic function as a 2^n x 2^q      */
/*        matrix                                                       */
/*   5. Linear profile                                                 */
/*   6. Differential profile                                           */
/*   7. Linearity/nonlinearity measures:                               */
/*        linear potential, differential potential, nonlinearity       */
/*                                                                     */
/* The bit string (b_1, ..., b_n) is identified with the integer       */
/*   b_1 2^{n-1} + ... + b_n 2^0.                                      */
/***********************************************************************/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
/* Argument dimension n and image dimension q <= 8               */
/* Increase if needed. The program will allocate 5 arrays of     */
/*   length up to MAXLEN*MAXLEN = 2^{2*MAXDIM}.                  */
/* MAXLEN must be 2^MAXDIM.                                      */
#define MAXDIM 8
#define MAXLEN 256
```

```
/*---------------------------------------------------------------*/
/* getInput: Read component coefficients x from stdin.           */
/*           Set dimension dim1 of argument space and            */
/*           dimension dim2 of image space.                      */
/*           (dim1 = base 2 log of input line length,            */
/*            dim2 = number of input lines.)                     */
/*   Memory for x is allocated inside.                           */
/*   Return codes:                                               */
/*     0 = Input o. K.                                           */
/*     1 = dim1 or dim2 exceeds MAXDIM.                          */
/*     2 = Input line has wrong length.                          */
/*     3 = Input contains value != 0 or 1.                       */
/*---------------------------------------------------------------*/

int getInput(unsigned ***x, unsigned *dim1, unsigned *dim2)
{
  unsigned      i, n;              /* Dimension                  */
  unsigned long m, k, j;           /* Length                     */
  char          buf[MAXLEN+2];
  char          *bufptr;

  i = 0;
  n = 0;
                                    /* 257 = MAXLENGTH + 1       */
  while ((scanf("%257s", buf) != EOF) & (i <= MAXDIM)) {
    if (i == MAXDIM) {
    fprintf(stderr, "bma.getInput: Too many lines.\n");
    return 1;
    }
    m = strlen(buf);
    if (m > MAXLEN) {
      fprintf(stderr, "bma.getInput: Line too long.\n");
      return 2;
      }
    if (i == 0) {                   /* First line                */
      while (m > 1) {               /* Calculate dim1 and 2^dim1 */
        k = m >> 1;
        if ((k << 1) != m) {        /* m not a power of 2 */
          fprintf(stderr, "bma.getInput: Line length not a power of 2.\n");
          return 2;
          }
        n++;
        m = k;
        }                            /* Now n = dim1             */
        *dim1 = n;
        (*x) = (unsigned **) malloc(MAXDIM * sizeof(unsigned *));
        k = 1 << n;                  /* Line length 2^n          */
      }
    else {                           /* Follow-up lines          */
```

```
      if (m != k) {
        fprintf(stderr, "bma.getInput: Line lengths differ.\n");
        return 2;
        }
      } /* Now buf contains a line of good length -----------------*/

    (*x)[i] = (unsigned *) malloc(k * sizeof(unsigned));
    bufptr = buf;                     /* Cursor pointer into buf   */
    for (j = 0; j < k; j++) {
      sscanf(bufptr, "%1u", &((*x)[i][j]));
      if ((*x)[i][j] > 1) {
        fprintf(stderr, "bma.getInput: Input not in range.\n");
        return 3;
        }
      bufptr++;
      }
    i++;
    } /* end while ------------------------------------------------*/

  *dim2 = i;
  return 0;
}
```

```
/*-------------------------------------------------------------------*/
/* rev: Recursive Evaluation of a Boolean function f                 */
/*   Input: Array x of coefficients of Algebraic NF                  */
/*   Output: Truth table y of f                                      */
/* There is no error handling. The input is assumed to be correct.*/
/*-------------------------------------------------------------------*/
void rev(unsigned *x, unsigned *y, unsigned dim)
{
  unsigned      z[MAXLEN];
  unsigned long m, k, mi;
  unsigned      n, i;

  n = dim;
  m = 1 << n;                           /* length of array       */
  for (k = 0; k < m; k++) y[k] = x[k];
  mi = 1;
  for (i = 0; i < n; i++) {
    for (k = 0; k < m; k++)
      if ((k >> i) % 2) z[k] = y[k-mi] ^ y[k];
        else z[k] = y[k];
    for (k = 0; k < m; k++) y[k] = z[k];
    mi *= 2;
    }
  return;
}
```

```
/*-------------------------------------------------------------*/
/* wt: Walsh transform of an integer valued function phi on K^dim */
/*   Input: Array of values of phi                             */
/*   Output: Array of values of Walsh transform                */
/* There is no error handling. The input is assumed to be correct.*/
/*-------------------------------------------------------------*/
void wt(long *x, long *y, unsigned dim)
{
  long          z[MAXLEN*MAXLEN];
  unsigned long m, k, mi;
  unsigned      n, i;

  n = dim;
  m = 1 << n;                 /* Length of truth table          */
  for (k = 0; k < m; k++) y[k] = x[k];
  mi = 1;
  for (i = 0; i < n; i++) {
    for (k = 0; k < m; k++)
      if ((k >> i) % 2) z[k] = y[k-mi] - y[k];
        else z[k] = y[k] + y[k+mi];
    for (k = 0; k < m; k++) y[k] = z[k];
    mi *= 2;
    }
  return;
}
```

```
/*-------------------------------------------------------------------*/
/* printBin: Print the w lowest bits of the number k to stdout.   */
/* There is no error handling. The input is assumed to be correct.*/
/*-------------------------------------------------------------------*/

void printBin(unsigned w, unsigned long k)
{
  unsigned      i, b[MAXDIM];
  unsigned long p, x;
  p = 1;
  for (i = 0; i < w; i++) {
    x = k&p;
    if (x) b[w-i] = 1;
      else b[w-i] = 0;
    p = p*2;
    }
  for (i = 1; i <= w; i++) printf("%1d", b[i]);
}
```

```
/*---------------------------------------------------------------*/
/* reduce: Divide the input vector x of length lt by the highest  */
/*   possible power 2^r of 2.                                    */
/* Return value: The exponent r.                                 */
/* There is no error handling. The input is assumed to be correct.*/
/*---------------------------------------------------------------*/

int reduce(long *x, unsigned long lt)
{
  unsigned long i = 0, j;
  long          z;
  unsigned      r = 0;

  while (x[i] == 0) i++;
  if (i == lt) return 0;           /* All components of x were 0. */
  /* Now x[i] != 0 ------------------------------------------------*/

  z = x[i];                        /* Calculate start value for r */
  while (!(z%2)) {                 /* z is even                   */
    z = z >> 1;
    r++;
    }
  /* Now r = max exponent with 2^r | x[i] ------------------------*/

  if (r == 0) return 0;            /* No sense in continuing      */
  for (j = i+1; j < lt; j++) {
    z = x[j];
    if (((z>>r)<<r) != z) {        /* Else r unchanged            */
      r = 0;                       /* Calculate new value for r   */
      while (!(z%2)) {
        z = z >> 1;
        r++;
        }
      if (r == 0) return 0;
      }
    }
  /* Now r = max exponent with 2^r | x[i], ..., x[lt-1] ----------*/
  /*   and r > 0. ----------------------------------------------*/

  for (j = 0; j < lt; j++) x[j] = x[j] >> r;
  return r;
}
```

```
/*---------------------------------------------------------------*/
/* max: Calculate the maximum entry of the input vector x        */
/*   between indices start and end-1, that is,                   */
/*     max(x[start], x[end-1]).                                  */
/* There is almost no error handling.                            */
/*   If end <= start, the function returns 0.                    */
/*   Otherwise the input is assumed to be correct.               */
/*---------------------------------------------------------------*/

long max(long *x, unsigned long start, unsigned long end)
{
  long          mm;
  unsigned long i;

  if (end <= start) return 0;

  mm = x[start];
  for (i = start+1; i < end; i++)
    if (x[i] > mm) mm = x[i];
  return mm;
}
```

```
/*-----------------------------------------------------------------*/
/* prtTabl0: Print a 2^n x q matrix.                               */
/* There is no error handling. The input is assumed to be correct.*/
/*-----------------------------------------------------------------*/

void prtTabl0(unsigned **x, unsigned dim1, unsigned dim2)
{
  unsigned long length1, length2, k, l;
  unsigned      i;
  length1 = 1 << dim1;
  length2 = dim2;

  for (i = 0; i <= dim1; i++) printf(" ");   /* Table header ...  */
  for (l = 1; l <= length2; l++) printf("%2d", l);
  printf("\n");                              /* ...               */
  for (i = 0; i <= dim1; i++) printf(" ");   /* ...               */
  for (l = 0; l < length2; l++) printf("--");
  printf("\n");                              /* ...               */

  for (k = 0; k < length1; k++) {         /* Print length1 lines: */
    printBin(dim1,k);                        /*   line header ... */
    printf("|");                             /*   ...             */
    for (l = 0; l < dim2; l++) printf(" %d", x[l][k]);
    printf("\n");
    }
}
```

```
/*-----------------------------------------------------------------*/
/* prtTabl1: Print a 2^n x 2^q matrix.                             */
/* There is no error handling. The input is assumed to be correct.*/
/*-----------------------------------------------------------------*/

void prtTabl1(long *x, unsigned dim1, unsigned dim2)
{
  unsigned long length1, length2, k, l;
  unsigned      i;
  length1 = 1 << dim1;
  length2 = 1 << dim2;

  for (i = 0; i <= dim1; i++) printf(" ");   /* Table header ...  */
  for (l = 0; l < length2; l++) {
    printf(" ");                             /* ...               */
    printBin(dim2,l);                        /* ...               */
    }
  printf("\n");                              /* ...               */
  for (i = 0; i <= dim1; i++) printf(" ");   /* ...               */
  for (l = 0; l < length2*dim2+length2; l++) printf("-");
  printf("\n");                              /* ...               */
  for (k = 0; k < length1; k++) {         /* Print length1 lines: */
    printBin(dim1,k);                        /*   line header ... */
    printf("|");                            /*   ...             */
    for (l = 0; l < length2; l++) {
      if (dim2 > 2) for (i = 0; i < dim2-2; i++) printf(" ");
      if (dim2 == 1) printf("%2d", x[(k<<dim2)+l]);
      else printf("%3d", x[(k<<dim2)+l]);
      }
    printf("\n");
    }
}
```

```
/*****************************************************************/
int main()
{
  unsigned      **a = NULL;        /* Array of coefficients       */
  unsigned      **f = NULL;        /* Array of values (truth tbl) */
    /* Note that a and f have their components arranged in rows - */
    /*   that's convenient for input and for calling rev on       */
    /*   the component functions.                                 */
  long          *g = NULL;         /* Characteristic function     */
  long          *c = NULL;         /* Walsh spectrum              */
  long          *lp = NULL;        /* Linear profile              */
  long          *dp = NULL;        /* Differential profile        */
  unsigned      n, q, i, j, n2;
  unsigned long m, p, k, l, y;
  int           rc;
  long          ll, dd, nl, maxnl;
  double        la;

/* Step 1: Algebraic Normal Form ----------------------------------*/

  rc = getInput(&a, &n, &q);
  if (rc) exit(1);
  printf("Argument Dimension = %d\n", n);
  m = 1 << n;                    /* Argument space has m elements */
  printf("Argument space has %d elements.\n", m);
  printf("Image Dimension = %d\n", q);
  p = 1 << q;                    /* Image space has p elements    */
  printf("Image space has %d elements.\n", p);

  printf("\n");
  printf("1. Algebraic Normal Form:\n");
  printf("[Columns = Image components]\n\n");
  prtTabl0(a, n, q);

/* Step 2: Truth Table --------------------------------------------*/

  f = (unsigned **) malloc(q * sizeof(unsigned *));
  for (i = 0; i < q; i++) {
    f[i] = (unsigned *) malloc(m * sizeof(unsigned));
    rev(a[i], f[i], n);          /* calculate truth table         */
    }
  printf("\n");
  printf("2. Truth Table:\n");
  printf("[Columns = Image components]\n\n");
  prtTabl0(f, n, q);
```

```
/* Step 3: Characteristic Function -------------------------------*/

  g = (long *) malloc(m * p * sizeof(long));
  for (k = 0; k < m; k++) {                 /* One line of values */
    for (l = 0; l < p; l++)
      g[(k<<q)+l] = 0;                      /* Set default value  */
    y = 0;                          /* Calculate value of map at k */
    for (i = 0; i < q; i++) y = y + (f[q-1-i][k] << i);
    g[(k<<q)+y] = 1;               /* Here charact. function is 1. */
    }
  printf("\n");
  printf("3. Characteristic Function:\n");
  printf("\n");
  prtTabl1(g, n, q);

/* Step 4: Walsh Spectrum ----------------------------------------*/

  c = (long *) malloc(m * p * sizeof(long));
  wt(g, c, n+q);                  /* calculate Walsh transform     */
  printf("\n");
  printf("4. Walsh Spectrum:\n");
  printf("\n");
  prtTabl1(c, n, q);

/* Step 5: Linear Profile ----------------------------------------*/

  lp = (long *) malloc(m * p * sizeof(long));
  for (k = 0; k < m*p; k++) lp[k] = c[k]*c[k];
  rc = reduce(lp, m*p);
  printf("\n");
  printf("5. Linear Profile:\n");
  printf("[To normalize divide by %d]\n", lp[0]);
  prtTabl1(lp, n, q);

/* Step 6: Differential Profile ----------------------------------*/

  dp = (long *) malloc(m * p * sizeof(long));
  wt(lp, dp, n+q);
  rc = reduce(dp, m*p);
  printf("\n");
  printf("6. Differential Profile:\n");
  printf("[To normalize divide by %d]\n", dp[0]);
  prtTabl1(dp, n, q);
```

```
/* Step 7: Linearity/nonlinearity measures ------------------------*/

  ll = max(lp, 1, m*p);     /* Numerator of linear potential       */
                            /* Denominator is lp[0].               */
  dd = max(dp, 1, m*p);     /* Numerator of differential potential */
                            /* Denominator is dp[0].               */
  la = (double) ll;
  la = la/lp[0];
  la = 1 - sqrt(la);
  la = la * (m >> 1);
  nl = floor(la + 0.5);     /* Nonlinearity                        */
  maxnl = m >> 1;
  if (n <= 1) {
    maxnl = 0;
    }
  else if (!(n%2)) {            /* n is even                       */
    n2 = (n >> 1) - 1;
    maxnl = maxnl - (1 << n2);
    }
  else {                        /* n is odd >=3                    */
    la = 1 << (n-2);
    la = sqrt(la);
    maxnl = floor(maxnl - la);
    }

  printf("\n");
  printf("7. Linearity/nonlinearity measures:\n");
  printf("\n");
  printf("Linear potential: %d/%d\n", ll, lp[0]);
  printf("  [Higher values mean more linearity.]\n");
  printf("  [Theoretical minimum = 1/%d | maximum = 1]\n", m);
  printf("Differential potential: %d/%d\n", dd, dp[0]);
  printf("  [Higher values mean more linearity.]\n");
  printf("  [Theoretical minimum = 1/%d | maximum = 1]\n", p);
  printf("Nonlinearity: %d\n", nl);
  printf("  [Lower values mean more linearity.]\n");
  printf("  [Theoretical minimum = 0 | maximum = %d]\n", maxnl);

/* Finish **************************************************************/
  exit(0);
}
```

Abkürzungen

AAECC =

ACCT = International Workshop on Algebraic and Combinatorial Coding Theory

ACS =

ACSIP = Australian Conference on Security and Information Privacy

ASIACRYPT = Advances in Cryptology Proceedings, Springer Lecture Notes in Computer Science

AUSCRYPT = Advances in Cryptology Proceedings, Springer Lecture Notes in Computer Science

CRYPTO = Advances in Cryptology Proceedings, Springer Lecture Notes in Computer Science

DCC = Designs, Codes and Cryptography

EUROCRYPT = Advances in Cryptology Proceedings, Springer Lecture Notes in Computer Science

FSE = Fast Software Encryption Proceedings, Springer Lecture Notes in Computer Science

ICC = International Conference on Combinatorics, Information Theory and Statistics

ICISC = International Conference on Information Security and Cryptography

IEEE =

IEICE =

INDOCRYPT

ISIT = IEEE International Symposium on Information Theory

LIENS = Laboratoire d'informatique de l'Ecole Normale Supérieure Paris

LMS = London Mathematical Society

SAC = Selected Areas on Cryptography

Literatur

[1] Carlisle Adams, Stafford Tavares: The structured design of cryptographically good S-boxes. Journal of Crytology 3 (1990), 27–41.

[2] Carlisle Adams: Designing DES-like ciphers with guaranteed resistance to differential and linear attacks. SAC 95.

[3] K. G. Beauchamp: *Applications of Walsh and Related Functions.* Academic Press, London 1984.

[4] E. R. Berlekamp, L. R. Welch: Weight distributions of the cosets of the (32,6) Reed-Muller code. IEEE Transactions on Information Theory 18 (1972), 203–207.

[5] Thomas Beth, C. Ding: On almost perfect nonlinear permutations. EUROCRYPT 93, 65–76.

[6] Eli Biham, Adi Shamir: Differential cryptanalysis of DES-like cryptosystems. CRYPTO 90, 2–21.

[7] Eli Biham, Adi Shamir: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4 (1991), 3–72.

[8] Eli Biham, Adi Shamir: Differential cryptanalysis of FEAL and N-Hash. EUROCRYPT 91, 1–16.

[9] Eli Biham, Adi Shamir: Differential cryptanalysis of the full 16-round DES. CRYPTO 92, 487–496.

[10] Eli Biham, Adi Shamir: *Differential cryptanalysis of the Data Encryption Standard.* Springer-Verlag 1993.

[11] Eli Biham: On Matsui's linear cryptanalysis. EUROCRYPT 94, 341–355.

[12] Yuri Borissov, Nickolay Manev, Svetla Nikova: On the non-minimal codewords in the binary Reed-Muller code. ISIT 2001, Washington DC Ju´ne 24–29, 2001.

[13] Brouwer, Verhoeff: An updated table of minimum distance bounds for binary linear codes. IEEE Transactions on Information Theory 39 (1993), 662–677. [Online: `http://www.win.tue.nl/math/dw/voorlincod.html`]

[14] Lawrence Brown, Matthew Kwan, Josef Pieprzyk, Jennifer Seberry: Improving resistance to differential cryptanalysis and the redesign of LOKI. Technical Report CS38/91, Dep.of Computer Science, Canberra.

[15] Paul Camion, Anne Canteaut: Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography. Designs, Codes, and Cryptography 16 (1999), 121–149.

[16] Paul Camion, Claude Carlet, Pascale Charpin, N. Sendrier: On correlation immune functions. CRYPTO 91, 86–100.

[17] Anne Canteaut: Differential cryptanalysis of Feistel ciphers and differentially δ-uniform mappings. SAC 97, 172–184.

[18] Anne Canteaut: Cryptographic functions and design criteria for block ciphers. INDOCRYPT 2001, 1–16.

[19] Anne Canteaut, Pascale Charpin, Hans Dobbertin: A new characterization of almost bent functions. FSE 99, 186–200.

[20] Anne Canteaut, Pascale Charpin, Hans Dobbertin: Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbf{F}_{2^m}$, and crosscorrelation of maximum-length sequences. SIAM J. Discrete Math. 13 (2000), 105–138.

[21] Anne Canteaut, Claude Carlet, Pascale Charpin, Caroline Fontaine: Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. EUROCRYPT 2000, 507–522.

[22] Anne Canteaut, Marion Videau: Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. EUROCRYPT 2002, 518–533.

[23] Claude Carlet: Partially-bent functions. CRYPTO 92, 280–291.

[24] Claude Carlet: Partially-bent functions. Designs, Codes, and Cryptography 3 (1993), 135–145.

[25] Claude Carlet: Two new classes of bent functions. EUROCRYPT 93, 77–101.

[26] Claude Carlet: Hyperbent functions. PRAGOCRYPT 96, 145–155.

[27] Claude Carlet: A construction of bent functions. In: *Finite Fields and their Applications.* LMS Lecture Series 233.

[28] Claude Carlet: A characterization of binary bent functions. ACCT-5/1996.

[29] Claude Carlet: Recent results on bent functions. ICC 97.

[30] Claude Carlet: More correlation immune und resilient functions over Galois fields and Galois rings. EUROCRYPT 97, 422–433.

[31] Claude Carlet: On cryptographic propagation criteria for Boolean functions. Information and Computation 151 (1999), 32–56.

[32] Claude Carlet, Pascale Charpin, V. Zinoviev: Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes, and Cryptography 15 (1998), 125–156.

[33] Claude Carlet, P. Guillot: Une caractérisation des fonctions courbes. C. R. Acad. Sci. Paris (1995).

[34] Claude Carlet, P. Guillot: A characterization of binary bent functions. J. Combinatorial Theory A 76 (1996), 328–335.

[35] Claude Carlet, P. Guillot: A characterization of binary bent functions. ISIT 97, 451–.

[36] Claude Carlet, P. Guillot: An alternate characterization of the bentness of binary functions, with uniqueness. Designs, Codes, and Cryptography 14 (1998), 133–140.

[37] Claude Carlet, P. Guillot: A representation of Boolean functions. AAECC 13/1999.

[38] Claude Carlet, Palash Sarkar: Spectral domain analysis of correlation immune and resilient Boolean functions. Finite Fields Appl. 8 (2002), 120–130.

[39] Claude Carlet, Jennifer Seberry, Xian-Mo Zhang: Comments on „Generating and counting binary bent sequences“. IEEE Trans. Inform. Th. 40 (1994), 600.

[40] Claude Carlet, Yurij Tarannikov: Covering sequences of Boolean functions and their cryptographic significance. DCC 25 (2002), 263–279.

[41] Florent Chabaud, Serge Vaudenay: Links between differential and linear cryptanalysis. Eurocrypt 94, 356–365.

[42] Chris Charnes, Martin Rötteler, Thomas Beth: Homogeneous bent functions, invariants, and designs. DCC 26 (2002), 139–154.

[43] David Chaum, Jan-Hendrik Evertse: Cryptanalysis of DES with a reduced number of rounds Sequences of linear factors in block ciphers. Crypto 85, 192–211.

[44] Jung Hee Cheon: Nonlinear vector resilient functions. Crypto 2001, 458–469.

[45] John A. Clark, Jeremy L. Jacob: Two-stage optimisation in the design of Boolean functions. ACSIP 2000.

[46] John A. Clark, Jeremy L. Jacob, Susan Stepney, Subhamoy Maitra, William Millan: Evolving Boolean functions satisfying multiple criteria. INDOCRYPT 2002.

[47] Jung Hee Cheon, Seongtaek Chee, Choonsik Park: S-boxes with controllable nonlinearity. EUROCRYPT 99, 286–294.

[48] Jung Hee Cheon, Seongtaek Chee: Nonlinearity of Boolean functions and hyperelliptic curves. SIAM J. Discrete Math. 16 (2003), 354–365.

[49] Joan Daemen: *Cipher and hash function design strategies based on linear and differential cryptanalysis.* Dissertation, KU Leuven 1995.

[50] Joan Daemen, Vincent Rijmen: *The Design of Rijndael.* Springer-Verlag, Berlin usw. 2002.

[51] Donald W. Davies: Some regular properties of the DES. CRYPTO 81, 41–41.

[52] Donald W. Davies: Some regular properties of the 'Data Encryption Standard' algorithm. CRYPTO 82, 89–96.

[53] J. F. Dillon: A survey of bent functions. The NSA technical journal 1972, 191–215.

[54] Hans Dobbertin: Almost perfect nonlinear power functions on GF(2^n): the Niho case. Information and Computation 151 (1999), 57–72.

[55] Jan-Hendrik Evertse: Linear structures in block ciphers. EUROCRYPT 87, 249–266.

[56] Eric Filiol, Caroline Fontaine: Highly nonlinear balanced boolean functions with a good correlation-immunity. EUROCRYPT 98, 475–488.

[57] Réjane Forré: The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition. CRYPTO 88, 450–468.

[58] Joanne Fuller, William Millan: On linear redundancy in the AES S-box. Preprint Brisbane 2002.

[59] K. Gopalakrishnan, D. R. Stinson: Three characterizations of non-binary correlation-immune and resilient functions. Designs, Codes and Cryptography 5 (1995), 241–251.

[60] Carlo Harpes, Gerhard G. Kramer, James L. Massey: A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma. EUROCRYPT 95, 24–38.

[61] Howard M. Heys, Stafford E. Tavares: Substitution-permutation networks resistant to differential and linear cryptanalysis. Journal of Cryptology 9 (1996), 1–19.

[62] Howard M. Heys: Modelling avalanche in DES-like ciphers. SAC 96.

[63] Howard M. Heys: A Tutorial on Linear and Differential Cryptanalysis. Memorial University of Newfoundland.

[64] Xiang-Dong Hou: GL(m,2) acting on R(r,m)/R(r-1,m). Discrete Mathematics 149 (1996), 99–122.

[65] Xiang-Dong Hou: Cubic bent functions. Discrete Mathematics 189 (1998), 149–161.

[66] T. Jakobsen: Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree. CRYPTO 98, 212–222.

[67] Burton S. Kaliski Jr., Matt J. B. Robshaw: Linear cryptanalysis using multiple approximations. CRYPTO 94, 26–39.

[68] Yasuyoshi Kaneko, Fumihiko Sano, Kouichi Sakurai: On provable security against differential and linear cryptanalysis in generalized Feistel ciphers with multiple random functions. SAC 97.

[69] Tadao Kasami, Nobuki Tokura: On the weight structure of Reed-Muller codes. IEEE Transactions on Information Theory 16 (1970), 752–759.

[70] Liam Keliher, Henk Meijer, Stafford Tavares: New method for upper bounding the maximum average linear hull probability for SPNs. EUROCRYPT 2001, 420–436.

[71] Lars R. Knudsen: *Block Ciphers – Analysis, Design and Applications.* Aarhus University 1994.

[72] Lars R. Knudsen: Truncated and higher order differentials. FSE 94, 196–211.

[73] Lars R. Knudsen, Matt J. B. Robshaw: Non-linear approximations in linear cryptanalysis. EUROCRYPT 96, 224–236.

[74] Gilles Lachaud, Jacques Wolfmann: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Transactions on Information Theory 36 (1990), 686–692S.

[75] Lai Xuejia: Higher order derivatives and differential cryptanalysis. Proc. Symp. on Communication, Coding and Cryptography in Honour of J. L. Massey, 1994.

[76] Lai Xuejia, James L. Massey: Markov ciphers and differential cryptanalysis. EUROCRYPT 91, 17–38.

[77] Susan K. Langford, Martin E. Hellman: Differential-linear cryptanalysis. CRYPTO 94, 17–25.

[78] R. J. Lechner: A correspondence between equivalence classes of switching functions and group codes. IEEE Transactions on Computers 16 (1967), 621–624.

[79] Rudolf Lidl, Harald Niederreiter: *Finite Fields.* Encyclopedia of Mathematics and its Applications. Addison-Wesley, Reading 1983.

[80] Helger Lipmaa, Shiho Moriai: Efficient algorithms for computing differential properties of addition. FSE 2001.

[81] Sheelagh Lloyd: Counting functions satisfying a higher order strict avalanche criterion. EUROCRYPT 89, 63–74.

[82] Sheelagh Lloyd: Properties of binary functions. EUROCRYPT 90, 124-139.

[83] F. J. MacWilliams, N. J. A. Sloane: *The Theory of Error Correcting Codes.* North-Holland, Amsterdam 1977.

[84] Subhamoy Maitra: Autocorrelation Properties of correlation immune Boolean functions. INDOCRYPT 2001, 242–253.

[85] Subhamoy Maitra: Highly nonlinear balanced Boolean functions with very good autocorrelation property. Elsevier Preprint 2001.

[86] Mitsuru Matsui, Atsuhiro Yamagishi: A new method for known plaintext attack of FEAL cipher. EUROCRYPT 92, 81–91.

[87] Mitsuru Matsui: Linear cryptanalysis method for DES cipher. EUROCRYPT 93, 386–397.

[88] Mitsuru Matsui: The first experimental cryptanalysis of the Data Encryption Standard. CRYPTO 94, 1–11.

[89] Mitsuro Matsui: New structure of block cipos with provable security against differential and linear cryptanalysis. FSE 96, 205–218.

[90] Mitsuro Matsui: On a structure of block ciphers with provable security against differential and linear cryptanalysis: IEICE Trans. Fundamentals E82-A (1999), 117–122.

[91] Willi Meier, Othmar Staffelbach: Fast correlation attacks on stream ciphers. EUROCRYPT 88, 301–314.

[92] Willi Meier, Othmar Staffelbach: Nonlinearity criteria for cryptographic functions. EUROCRYPT 89, 549–562.

[93] William Millan, Andrew Clark, Ed Dawson: Smart hill climbing finds better Boolean functions. SAC 97.

[94] Serge Mister, Carlisle Adams: Practical S-box design. SAC 96.

[95] Pat Morin: Provably secure and efficient block ciphers. SAC 96.

[96] Kaisa Nyberg: Constructions of bent functions and difference sets. EUROCRYPT 90, 151–160.

[97] Kaisa Nyberg: Perfect nonlinear S-boxes. EUROCRYPT 91, 378–386.

[98] Kaisa Nyberg: On the construction of highly nonlinear permutations. EUROCRYPT 92, 92–98.

[99] Kaisa Nyberg: Differentially uniform mappings for cryptography. EUROCRYPT 93, 55–64.

[100] Kaisa Nyberg: Linear approximation of block ciphers. EUROCRYPT 94, 439–444.

[101] Kaisa Nyberg, Lars R. Knudsen: Provable security against differential cryptanalysis. CRYPTO 92, 566–574.

[102] Kaisa Nyberg, Lars R. Knudsen: Provable security against differential cryptanalysis. Journal of Cryptology 8 (1995), 27–37.

[103] Luke O'Connor: On the distribution of characteristics in bijective mappings. Journal of Cryptology 8 (1995), 67–86.

[104] Luke O'Connor: Convergence in differential distributions. EUROCRYPT 95, 13–23.

[105] Katsuo Ohta, Shiho Moriai, Katsumaro Aoki: Improving the search algorithm for the best linear expression. CRYPTO 95, 157–170.

[106] J. D. Olsen, R. A. Scholtz, L. R. Welch: Bent function sequences. IEEE Transactions on Information Theory IT-28 (1982), 858–864.

[107] N. J. Patterson, D. H. Wiedemann: The covering radius of the $[2^{15}, 16]$ Reed-Muller code is at least 16276. IEEE Transactions on Information Theory 29 (1983), 354–356. Correction. IEEE Transactions on Information Theory 36 (1990), 443.

[108] Franz Pichler: On the Walsh-Fourier analysis of correlation immune switching functions. EUROCRYPT 86, 43–44.

[109] Josef P. Pieprzyk, G. Finkelstein: Towards an effective non-linear crypto design. IEEE Proceedings 135 (1988), 325–335.

[110] Josef P. Pieprzyk: Non-linearity of exponent permutations. EUROCRYPT 89, 80–92.

[111] Josef P. Pieprzyk, C. Charnes, Jennifer Seberry: Linear approximation versus nonlinearity. SAC 94.

[112] Bart Preneel, Werner van Leekwijck, Luc van Linden, René Govaerts, Joos Vandevalle: Propagation characteristics of Boolean functions. EUROCRYPT 90, 161–173.

[113] Bart Preneel, René Govaerts, Joos Vandevalle: Boolean functions satisfying higher order propagation criteria. EUROCRYPT 91, 141–152.

[114] Qing Xiang: Maximally nonlinear functions and bent functions. DCC 17 (1999), 211–218.

[115] Qu Chengxin, Jennifer Seberry, Josef Pieprzyk: On the symmetric property of homogeneous Boolean functions. ACISP 99. Lecture Notes in Computer Science 1587 (1999), 26–35.

[116] J. A. Reeds, J. L. Manferdelli: DES has no per round linear factors. CRYPTO 84, 377–394.

[117] Vincent Rijmen: *Cryptanalysis and Design of Iterated Block Ciphers.* Dissertation, KU Leuven 1997.

[118] O. S. Rothaus: On „bent“ functions. J. Combinatorial Theory A 20 (1976),´300–305.

[119] Palash Sarkar, Subhamoy Maitra: Nonlinearity bounds and constructions of resilient Boolean functions. CRYPTO 2000, 515–532.

[120] Palash Sarkar, Subhamoy Maitra: Construction of nonlinear Boolean functions with important cryptographic properties. EUROCRYPT 2000, 485–506.

[121] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Highly nonlinear 0-1-balanced functions satisfying strict avalanche criterion. AUSCRYPT 92, 145–155.

[122] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: On constructions and nonlinearity of correlation immune functions. EUROCRYPT 93, 181–199.

[123] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Nonlinearly balanced Boolean functions and their propagation characteristics. CRYPTO 93, 49–60.

[124] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Relationships among nonlinearity criteria. EUROCRYPT 94, 376–388.

[125] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Pitfalls in designing substitution boxes. CRYPTO 94, 383–396.

[126] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: Nonlinearity characteristics of quadratic substitution boxes. SAC 94.

[127] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: GAC — the criterion for global avalanche characteristics of cryptographic functions. Preprint 1994.

[128] Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng: The relationship between propagation characteristic and nonlinearity of cryptographic functions. Preprint 1994.

[129] Adi Shamir: On the security of DES. CRYPTO 85, 280–281.

[130] Thomas Siegenthaler: Correlation immune polynomials over finite fields. EUROCRYPT 86, 42–42.

[131] J. Silverman: *The Arithmetic of Elliptic Curves.* Springer-Verlag, New York 1986.

[132] D. R. Stinson, J. L. Massey: An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions. J. Cryptology 8 (1995), 167–173.

[133] Yurij Tarannikov: New constructions of resilient Boolean functions with maximal nonlinearity. FSE 2001.

[134] Yurij Tarannikov, Peter Korolev, Anton Botev: Autocorrelation coefficients and correlation immunity of Boolean functions. ASIACRYPT 2001, 460–479.

[135] Serge Vaudenay: Provable security for block ciphers by decorrelation. LIENS–98–8.

[136] Tadashi Wadayama, Toru Hada, Koichiro Wakasugi, Masao Kasahara: Upper and lower bounds on maximum nonlinearity of n-input and m-output Boolean functions. DCC 23 (2001), 23–33.

[137] William C. Waterhouse: Abelian varieties over finite fields. Ann. Sc. ENS 4 (1969), 521–560.

[138] A. F. Webster, Stafford E. Tavares: On the design of S-Boxes. CRYPTO 85, 523–534.

[139] Xiao Guo-Chen, J. Massey: A spectral characterization of correlation immune combining functions. IEEE Transactions on Information Theory 34 (1988), 569-571.

[140] Amr M. Youssef, T. W. Cusick, P. Stănică, Stafford E. Tavares: New bounds on the number of functions satisfying the strict avalanche criterion. SAC 96.

[141] Amr M. Youssef, Guang Gong: Hyper-bent functions. Eurocrypt 2001, 406–419.

[142] Muxiang Zhang, Agnes Chan: Maximum correlation analysis of nonlinear S-Boxes in stream ciphers. Crypto 2000, 501–514.

[143] Xian-Mo Zhang, Yuliang Zheng: Auto-correlations and new bounds on the non-linearity of Boolean functions. Eurocrypt 96, 294–306.

[144] Xian-Mo Zhang, Yuliang Zheng: Difference distribution table of a regular substitution box. SAC 96, 57–60.

[145] Xian-Mo Zhang, Yuliang Zheng: New lower bounds on nonlinearity and a class of highly nonlinear functions. ACISP 97, 147–158.

[146] Xian-Mo Zhang, Yuliang Zheng: The nonhomomorphicity of Boolean functions. SAC98, 280–295.

[147] Xian-Mo Zhang, Yuliang Zheng, Hideki Imai: Non-existence of certain quadratic S-boxes and two bounds on nonlinear characteristics of general S-boxes. SAC 97, 27–39.

[148] Xian-Mo Zhang, Yuliang Zheng, Hideki Imai: Duality of Boolean functions and its cryptographic significance. ICICS 97, 159–169.

[149] Yuliang Zheng, Xian-Mo Zhang: The nonhomomorphicity of S-boxes. ICISC 98, 92–105.

[150] Yuliang Zheng, Xian-Mo Zhang: Strong linear dependence and unbiased distributions of non-propagative vecotrs. SAC 99, 92–105.

[151] Yuliang Zheng, Xian-Mo Zhang: Relationships between bent functions and complimentary plateaued functions. ICISC 99, 60–75.

[152] Yuliang Zheng, Xian-Mo Zhang: Plateaued functions. ICICS 99, 284–300.

[153] Yuliang Zheng, Xian-Mo Zhang: On relationships among avalanche, nonlinearity, and correlation immunity. Asiacrypt 2000, 470–482.

[154] Yuliang Zheng, Xian-Mo Zhang: Non-separable cryptographic functions. Int. Symp. Information Theory and its Applications, Honolulu 2000, 51–58.

[155] Yuliang Zheng, Xian-Mo Zhang: On k-th order nonhomomorphicity of S-Boxes. J. Unic. Comp. Sci. 6 (2000), 830–848.

[156] Yuliang Zheng, Xian-Mo Zhang: Improved upper bound on the nonlinearity of high order correlation immune functions. SAC 2000, 262–274.

[157] Yuliang Zheng, Xian-Mo Zhang: A new property of Maiorana-McFarland functions. Bull. Inst. Comb. Appl. 33 (2001), 13–22.

[158] Yuliang Zheng, Xian-Mo Zhang, Hideki Imai: Connections between nonlinearity and restrictions, terms and hypergraphs of Boolean functions. IEEE Int. Symp. IT 1998, 439.

[159] Yuliang Zheng, Xian-Mo Zhang, Hideki Imai: Restrictions, terms and nonlinearity of Boolean functions. Theor. Comp. Sc. 226 (1999), 207–223.

[160] Anna Zugaj, Karol Górski, Zbigniew Kotulski, Andrzej Paszkiewicz, Janusz Szczepański: New constructions in linear cryptanalysis of block ciphers. ACS 2000, 523–530.