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.