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* BOOLE*sche 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 minimalen Wert* $\Lambda_f = 2^{-n}$.

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

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

(vi) *Die Linearitätsdistanz von* f *hat den maximalen 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* BOOLE*sche 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* BOOLE*sche Funktion.*

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

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

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

Korollar 1 *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 2 *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 „differentielles 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 $f\colon\mathbb{F}_2^n\longrightarrow\mathbb{F}_2^q$ 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 $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ 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 $f\colon \mathbb{F}_2^2 \longrightarrow \mathbb{F}_2^2$.

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

$$u = u_0a + u_1a^2 + \cdots + u_{n-1}a^{2^{n-1}},$$

so verschiebt das Quadrieren den Koeffizientenvektor zyklisch um 1 nach rechts, das Potenzieren mit 4 um 2, also

$$u^4 = u_{n-2}a + u_{n-1}a^2 + u_0a^4 \cdots + u_{n-3}a^{2^{n-1}}.$$

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 $h_{uv} = u^{-1}T + T + u$, 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 $\operatorname{Dim} k = n$, so hat die Inversionsabbildung $f = f_{-1}$ das differenzielle Potenzial*

$$\Omega_f = \begin{cases} \frac{1}{2^{n-1}}, & \textit{wenn } n \textit{ ungerade,} \\ \frac{1}{2^{n-2}}, & \textit{wenn } n \textit{ gerade.} \end{cases}$$

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 $\beta(y) = \mathrm{Tr}(by)$ für alle $y \in K$, und $\beta \circ f(x) = \mathrm{Tr}(bx^{-1}) = \mathrm{Tr}((cx)^{-1})$ mit $c = b^{-1}$ für $x \in K^\times$. Ebenso ist $u \cdot x = \mathrm{Tr}(ax)$ für $u \in K$ mit passendem $a \in K$. Damit gilt für $v \in K^\times$:

$$\begin{aligned}
\hat{\vartheta}_f(u,v) &= = \sum_{x \in K} (-1)^{v \cdot f(x) + u \cdot x} \\
&= 1 + \sum_{x \in K^\times} (-1)^{\mathrm{Tr}((cx)^{-1} + ax)} = 1 + \sum_{y \in K^\times} (-1)^{\mathrm{Tr}(y^{-1} + \frac{a}{c} y)} \\
&= 1 + \kappa(\frac{a}{c}) = 1 + \kappa(ab)
\end{aligned}$$

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*

$$\Lambda_f = \frac{1}{2^{2n}} \cdot \max_{u \in K^\times} |1 + \kappa(u)|^2.$$

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	$\max \lvert 1 + \kappa(u) \rvert$
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*

$$\begin{aligned} \text{(i)} \quad & \max\nolimits_{K^2-\{0\}} |\hat{\vartheta}_f| && = \xi(n), \\ \text{(ii)} \quad & \sigma_f && = 2^{n-1} - \frac{1}{2}\xi(n), \\ \text{(iii)} \quad & \Lambda_f && = \frac{1}{2^{2n}}\xi(n)^2. \end{aligned}$$

Falls $n \geq 2$ gerade, ist $\xi(n) = 2^{n/2+1}$. 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

$$\begin{aligned} \Lambda(n,q) &:= \min\{\Lambda_f \mid f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q\}, \\ \Omega(n,q) &:= \min\{\Omega_f \mid f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q\} \end{aligned}$$

bekannt ist; dazu werden einige Ergänzungen bewiesen.

Hilfssatz 4 *Sei* $g : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^{q+1}$ *zerlegt in* $g = (f_0, f)$ *mit* $f_0 : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ *und* $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^q$. *Dann ist*

(i) $\Lambda_g \geq \Lambda_f$,

(ii) $\Omega_g \leq \Omega_f$.

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) 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) $\Omega(n, q) \geq \Omega(n, q+1)$, *d. h.,* Ω *ist bei festem* n *bezüglich* q *monoton fallend.*

(iii) $\Lambda(n, 1) \geq \Lambda(n+1, 1)$, *d. h.,* Λ *ist bei festem* $q = 1$ *bezüglich* n *monoton fallend.*

Beweis. (i) und (ii) folgen direkt aus dem Hilfssatz 4. Für (iii) 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* $f : \mathbb{F}_2^4 \longrightarrow \mathbb{F}_2^4$.

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.
- $\Lambda(1,q) = 1$ 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 $f\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ 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, ist $\Lambda(n,q) \geq \frac{1}{2^n} - \frac{1}{2^{2n-2}}$, siehe Korollar 1 in 3.5. Insbesondere ist
  - $\Lambda(6,q) \geq \frac{17}{1024}$ für alle $q \geq 4$,
  - $\Lambda(8,q) \geq \frac{65}{16384}$ 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. Da $\Lambda(n,n)$ ganzzahliges Vielfaches von $\frac{1}{2^{2n-2}}$ sein muss, folgt

  $$\Lambda(n,n) \geq \frac{2^{n-1}+1}{2^{2n-2}}$$

  für gerades n.
- 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.

Diese Aussagen werden in der folgenden Tabelle 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	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$[\frac{1}{4},1]$	...	...	...	...
4	$\frac{1}{16}$	$[\frac{1}{16},\frac{1}{4}]$	$[\frac{9}{64},\frac{1}{4}]$	...	$[\frac{9}{64},1]$	...	...	...
5	$[\frac{9}{256},\frac{1}{16}]$	...	...	...	$\frac{1}{16}$	$[\frac{1}{16},1]$	...	...
6	$\frac{1}{64}$	$[\frac{1}{64},\frac{49}{256}]$	...	$[\frac{17}{1024},\frac{49}{256}]$	$[\frac{17}{1024},\frac{1}{16}]$	$[\frac{33}{1024},\frac{1}{16}]$	$[\frac{33}{1024},1]$	...
7	$[\frac{9}{1024},\frac{1}{64}]$	...	...	...	...	...	$\frac{1}{64}$	$[\frac{1}{64},1]$
8	$\frac{1}{256}$	$[\frac{1}{256},\frac{1}{64}]$	...	...	$[\frac{65}{16384},\frac{1}{64}]$	...	...	$[\frac{129}{16384},\frac{1}{64}]$

Über $\Omega(n,q)$ ist folgendes bekannt:

- $\frac{1}{2^q} \leq \Omega(n,q) \leq 1$ nach Bemerkung 2 in 4.4.
- $\frac{1}{2^{n-1}} \leq \Omega(n,q)$ nach Bemerkung 6 in 4.4.
- $\Omega(1,q) = 1$ 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 $\frac{1}{4} \leq \Omega(6,4) \leq \Omega(6,5)$.

- $\Omega(n,q) = \frac{1}{2^{n-1}}$ für alle $q \geq n$ nach Korollar 2.

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	$\frac{1}{2}$	$[\frac{1}{4}, \frac{1}{2}]$	$\dots$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$
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	$\frac{1}{2}$	$[\frac{1}{4}, \frac{1}{2}]$	$[\frac{1}{8}, \frac{1}{2}]$	$[\frac{3}{32}, \frac{1}{4}]$	$[\frac{1}{16}, \frac{1}{4}]$	$\frac{1}{32}$	$\frac{1}{32}$	$\frac{1}{32}$
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	$\frac{1}{2}$	$[\frac{1}{4}, \frac{1}{2}]$	$[\frac{1}{8}, \frac{1}{2}]$	$[\frac{1}{16}, \frac{1}{2}]$	$[\frac{5}{128}, \frac{1}{2}]$	$[\frac{3}{128}, \frac{1}{2}]$	$[\frac{1}{64}, \frac{1}{2}]$	$\frac{1}{128}$