Tilla Schade
Fachbereich Automatisierung und Informatik

Bericht über meine Forschungstätigkeit im Wintersemester 2013 / 2014

Ich habe mich in meinem Forschungssemester mit *Bent Funktionen* beschäftigt. Diese besonderen Boole'schen Funktionen werden in der Codierungstheorie und Kryptographie angewendet.

1 Bent Funktionen

Sei V_n ein n-dimensionaler Vektorraum über dem Körper $GF(2)$.

Definition 1 *Eine Boole'sche Funktion f ist eine Abbildung $f : V_n \to GF(2)$ des Vektorraums V_n in die Menge $\{0, 1\}$.*
Mit Hilfe der lexikographischen Ordnung der Elemente von V_n können wir f durch die Folge der Funktionswerte angeben:

$$(f(v_0), f(v_1), \ldots, f(v_{2^n-1})).$$

Dieser Vektor mit 2^n Einträgen $\in \{0, 1\}$ heißt die Wahrheitstabelle von f.
Die Menge $supp(f)$ aller Elemente von V_n, für die f den Wert 1 hat, heißt der Träger von f, die Mächtigkeit dieser Menge wird mit $card(f)$ bezeichnet.
Eine Boole'sche Funktion heißt balanciert, wenn sie die Funktionswerte 0 und 1 gleich häufig annimmt, d.h.

$$card(f) = 2^{n-1}.$$

Da wir den 2^n Elementen von V_n beliebig die Werte 0 oder 1 als Funktionswerte zuordnen können, gibt es insgesamt $2^{(2^n)}$ Boole'sche Funktionen.

Definition 2 (Bent Funktion) *Eine Boole'sche Funktion f heißt Bent, wenn für jeden Vektor $v \in V_n,\ v \neq 0$ die Funktion*

$$g_v(x) := f(x + v) + f(x) \qquad \forall x \in V$$

balanciert ist (d.h. $card(g_v) = 2^{n-1}$).

Bent Funktionen erfüllen offensichtlich das in der Kryptographie wichtige **Strict Avalanche Criterion (SAC)** (siehe z.B. [1]).

Definition 3 (Strict Avalanche Criterion) *Eine Boole'sche Funktion f erfüllt das Strict Avalanche Criterion, wenn sich bei Änderung eines Bits des Eingabevektors der Funktionswert mit Wahrscheinlichkeit $\frac{1}{2}$ ändert.*
Das heißt: Betrachten wir für einen festen Vektor $x \in V_n$ die Funktionswerte $f(x + e_i)$ (wobei e_i der i-te Einheitsvektor aus V_n ist, also der Vektor, der als i-ten Eintrag 1 hat und sonst Einträge 0) für $i = 1, \ldots, n$, so erhalten wir genau $\frac{n}{2}$ mal die 0 und $\frac{n}{2}$ mal die 1.

Bent Funktionen können auch durch andere charakteristische Eigenschaften definiert werden:

1. Der (Hamming-) Abstand einer Boole'schen Funktion f von der Menge $\mathcal{A}_n$ der affinen Funktionen auf V_n ist definiert als

   $$d(f, \mathcal{A}_n) := \min\{d(f, g) \mid g \in \mathcal{A}_n\}.$$

   Bent Funktionen sind genau diejenigen Boole'schen Funktionen, für die dieser Abstand maximal ist (nämlich $2^{n-1} - 2^{\frac{n}{2}-1}$). In diesem Sinne sind Bent Funktionen also „so nichtlinear wie möglich" (daher der Name).

2. Die Walsh Transformation einer Boole'schen Funktion f (wobei die Funktionswerte von f als reelle Zahlen 0 und 1 interpretiert werden) ist die Funktion $W(f) : V_n \to \mathbb{R}$, die durch

   $$W(f)(w) := \sum_{x \in V_n} f(x)(-1)^{x \circ w} \qquad \forall w \in V$$

   definiert ist ($x \circ v$ steht für das Skalarprodukt von x und w). (Es handelt sich um einen Spezialfall der diskreten Fouriertransformation.)
   Die Walsh Transformation kann man auch auf die Funktion $\hat{f} : V_n \to \{1, -1\}$ anwenden, die durch $\hat{f}(x) := (-1)^{f(x)}$ definiert ist ($\hat{f}$ bezeichnet man oft als „sign function" von f):

   $$W(\hat{f})(w) := \sum_{x \in V_n} (-1)^{f(x)}(-1)^{x \circ w}$$

   Bent Funktionen haben die charakteristische Eigenschaft, dass die Walsh Transformierte ihrer sign function nur zwei Funktionswerte annimmt, nämlich $\pm 2^{\frac{n}{2}}$.
   Dividiert man die Funktionswerte von $W(\hat{f})(w)$ durch $2^{\frac{n}{2}}$, erhält man eine Funktion g, die wieder nur die Werte ± 1 annimmt. Man kann zeigen, dass g wieder die sign function einer Bent Funktion ist; sie wird als die zu f duale Funktion bezeichnet.

Wie diese Überlegungen zeigen, können Bent Funktionen nur auf Vektorräumen V_n existieren, deren Dimension n gerade ist, d.h. $n = 2m$.
Außerdem lässt sich leicht ableiten, dass für eine Bent Funktion f gilt: $card(f) = 2^{n-1} \pm 2^{m-1}$.

Jede Boole'sche Funktion hat eine eindeutige Darstellung als multivariates Polynom in $GF(2)[x_1, \ldots, n]$, dieses Polynom heißt die algebraische Normalform (ANF) der Funktion.

Beispiel 4 *Sei $n = 4$, also $V_4 = (GF(2)^4)$. Wir definieren die folgende Menge $D \subset V_4$:*

$$D = \{(0,0,1,1), (0,1,1,1), (1,0,1,1), (1,1,0,0), (1,1,0,1), (1,1,1,0)\}$$

Dann ist die Boole'sche Funktion f, die D als Träger hat, eine Bent Funktion. Die ANF, also das zu f gehörende multivariate Polynom lautet

$$F(x_1, x_2, x_3, x_4) \;=\; x_1x_2 + x_3x_4.$$

Es gibt viele Verbindungen von Bent Funktionen zu anderen kombinatorischen Strukturen, wie zum Beispiel Codes, Designs und Graphen. So entsprechen die Bent Funktionen den Nebenklassen des Reed-Muller Codes erster Ordnung, die größtes Minimalgewicht haben. (siehe [3]).

2 Stand der Forschung über Bent Funktionen

Bent Funktionen sind bereits intensiv untersucht worden, die erste Definition stammt bereits von Rothaus ([5]) aus dem Jahr 1976. Einen aktueller Überblick findet man in [4].

Kennt man eine Bent Funktion, kann man durch einfache Transformationen (Komplement, Komposition mit einem Automorphismus des Vektorraums V_n, Addition einer affinen Funktion) weitere Bent Funktionen erzeugen. Bent Funktionen, die durch solche Transformationen ineinander überführt werden können, heißen äquivalent. Daraus ergibt sich die Frage, wie viele nicht-äquivalente Bent Funktionen es über V_n für ein bestimmtes n gibt. Diese Frage ist bisher nur für kleine $n \in \{2, 4, 6\}$ gelöst; für $n \geq 8$ ist die Anzahl nicht-äquivalenter Bent Funktionen bisher unbekannt.

Es gibt mehrere allgemeine Konstruktionen für Bent Funktionen (siehe z.B. [1] oder für Originalarbeiten die Literaturhinweise in [4]). Zwei davon sind besonders wichtig:

1. Die Maiorana-McFarland Konstruktion: Sei $n = 2m$. Wir teilen den Vektorraum V_n in zwei Vektorräume der halben Dimension auf: $V_n = GF(2)^m \times GF(2)^m$. Sei π eine Permutation von $GF(2)^m$ und $\sigma : GF(2)^m \to GF(2)$ irgendeine Boole'sche Funktion. Dann ist die Funktion
$$\begin{array}{rccccc} f: & GF(2)^m & \times & GF(2)^m & \to & GF(2) \\ & (x & , & y) & \to & f(x,y) = x \cdot \pi(y) + \sigma(y) \end{array}$$
eine Bent Funktion auf V_n.

2. Die Partial Spread Konstruktion: Sei wieder $n = 2m$ und $U_i, i \in I$ eine Familie von Unterräumen von V_n mit Dimension m, so dass $U_i \cap U_j = \{0\}$ für $i \neq j$ (ein sogenanntes „partial spread“). Wenn diese Familie $|I| = 2^{m-1}$ solcher Unterräume enthält, setzen wir $D^{(-)} = \cup_{i \in I}(U_i \setminus \{0\})$ und definieren die Funktion $f : V_n \to GF(2)$ durch
$$f(x) = \begin{cases} 1 & \text{falls} \quad x \in D^{(-)} \\ 0 & \text{sonst.} \end{cases}$$
Diese sowie die entsprechende Konstruktion für $|I| = 2^{m-1} + 1$ und $D^{(+)} = \cup_{i \in I} U_i$ liefern Bent Funktionen.

3 Mein Forschungsansatz

Bent Funktionen, die „klassisch“ auf der elementarabelschen Gruppe $(\mathbb{Z}_2)^n$ (der additiven Gruppe des Körpers $GF(2^n)$) definiert sind, wurden bereits intensiv untersucht. Deshalb habe ich mich damit beschäftigt, wie Bent Funktionen aussehen, die auf einer anderen abelschen Gruppe der Ordnung 2^n (wie z.B. auf $(\mathbb{Z}_4)^n$ oder $\mathbb{Z}_2 \times \mathbb{Z}_8$) definiert sind. Mein ursprüngliches Ziel war es, die mit Hilfe der beiden oben angegebenen Konstruktionen (Maiorana-McFarland Konstruktion bzw. Partial Spread Konstruktion) definierten Bent Funktionen auf Äquivalenz zu untersuchen. Allerdings musste ich feststellen, dass die Partial Spread Konstruktion für diese Fälle fast nie angewendet werden kann, da die Partial Spreads nicht genügend Unterräume enthalten (vgl. [2]). Die einzige Ausnahme ist die (relativ kleine) Gruppe $\mathbb{Z}_4 \times \mathbb{Z}_4$.

Mein neues Ziel ist es, alle Bent Funktionen auf kleinen Gruppen (zunächst Ordnung 2^4, dann 2^6), die nicht elementarabelsch sind, per Computer zu konstruieren und zu klassifizieren. Insbesondere interessiert mich, wie viele es gibt, die nicht durch die Maiorana-McFarland Konstruktion erhalten werden können. Auch über die Anzahl nicht-äquivalenter Bent Funktionen in diesen Gruppen ist bisher wenig bekannt. Ich werde dazu Matlab und das Computeralgebrasystem Magma benutzen und erwarte, dadurch im Laufe des nächsten Jahres Resultate für ein oder zwei Veröffentlichungen zu erhalten.

Im Sommersemester 2014 werde ich meine neu erworbenen Kenntnisse über Bent Funktionen (insbesondere den Informatik-Studenten) in einem Vortrag präsentieren.

Literatur

[1] Thomas W. Cusick, Pantelimon Stanica: *Cryptographic Boolean Functions and Applications*, Academic Press (Elsevier), San Diego (2009).

[2] Dieter Jungnickel: *Partial Spreads over* $\mathbb{Z}_q$, Linear Algebra and its Applications 114/115 (1989), p. 95 - 102.

[3] Florence J. MacWilliams, Neil J. A. Sloane: *The Theory of Error-Correcting Codes*, North Holland Mathematical Library Vol. 16, North Holland Publishing Co., Amsterdam (1977).

[4] Gary L. Mullen, Daniel Panario (eds.): *Handbook of Finite Fields*, CRC Press (Chapman & Hall), Taylor & Francis Group, Boca Raton (2013).

[5] O.S. Rothaus: *On „Bent“ Functions*, Journal of Combinatorial Theory, Ser. A 20 (1976), p. 300-305.