NEW PARAMETERS FOR BENT FUNCTIONS

Jacques Wolfmann

IMATH (GRIM)

Université du Sud Toulon-Var

France

$\mathbb{F}_q$9

Dublin, july 2009

Definition: A k-*variable boolean function* is a map f from $\mathbb{F}_2^k$ into $\mathbb{F}_2$.
Weight: $w(f) = \sharp\{v \in \mathbb{F}_2^k \mid f(v) = 1\}$.

Distance: $d(f,g) = \sharp\{v \in \mathbb{F}_2^k \mid f(v) \neq g(v)\}$.

Vector: If $\mathbb{F}_2^k = \{v_0, v_1, \ldots, v_{2^k-1}\}$
$V(f) = \Big(f(v_0), f(v_1), \ldots, f(v_{2^k-1})\Big)$

Polynomial represent.: $P_f(x) = \sum_{i=0}^{2^k-1} f(v_i)x^i$

Walsh coefficients: For every $v \in \mathbb{F}_2^m$:
$c_v = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x) \oplus <v,x>}$
with $<,>$: usual inner product.

Algebraic Normal Form (ANF)
$F(X_0, X_1, \ldots, X_{k-1})$ in
$\mathbb{F}_2[X_0, X_1, \ldots, X_{k-1}]/(X_0^2 - X_0, X_1^2 - X_1, \ldots, X_{k-1}^2 - X_{k-1})$
such that: if $u = (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_2^k$ then $f(u) = F(u_0, u_1, \ldots, u_{k-1})$.

Degree: $\deg(f)$ is the degree of the ANF.

Derivative: If $e \in \mathbb{F}_2^k$: $D_e(x) = f(x) + f(x+e)$

A special representation

We identify $\mathbb{F}_2^k$ with $\mathbb{F}_2 \times \mathbb{F}_2^{k-1}$
and $\mathbb{F}_2^{k-1}$ with $\mathbb{F}_{2^{k-1}} = \mathbb{F}_2(\alpha)$
$n = 2^{k-1} - 1$, f: k-boolean function:

<u>A special order:</u>

$\mathbb{F}_{2^k} = \{v_0, v_1, \ldots, v_n, \ldots, v_{2n+1}\}$ with:

$v_0 = (0,1)$, $v_1 = (0,\alpha)$, $\quad v_2 = (0,\alpha^2) \ldots\ldots v_{n-1} = (0,\alpha^{n-1})$,
$v_n = (1,1), v_{n+1} = (1,\alpha), v_{n+2} = (1,\alpha^2) \ldots v_{2n-1} = (1,\alpha^{n-1})$,
$v_{2n} = (0,\underline{0}), v_{2n+1} = (1,\underline{0})$

$V(f) = \big(f(v_0), \ldots, f(v_{n-1}), f(v_n), \ldots, f(v_{2n-1}), f(0,\underline{0}), f(1,\underline{0})\big)$

Two $(k-1)$-boolean functions:
$u \in \mathbb{F}_{2^{k-1}}$: $f_p(u) = f(0,u)$, $f_q(u) = f(1,u)$.

Polynomial represent.

$P_f(x) = p(x) + x^n q(x) + f_p(\underline{0}) x^{2n} + f_q(\underline{0}) x^{2n+1}$

with

$p(x) = \sum_{i=0}^{n-1} f_p(\alpha^i) x^i$,$q(x) = \sum_{i=0}^{n-1} f_q(\alpha^i) x^i$.

BENT FUNCTIONS

$\mathcal{F}(k)$: set of k-variable boolean functions.
$\mathcal{A}(k)$: subset of affine functions, (deg≤ 1).

Definition 1
$f \in \mathcal{F}(k)$ is a bent function if:

$$d(f, \mathcal{A}(k)) = \max_{g \in \mathcal{F}(k)} d(g, \mathcal{A}(k))$$

From now on $k = 2t$, $t \geq 2$.

Proposition 2 *(classical)*
Let $f \in \mathcal{F}(k)$, $k = 2t$, c_v: Walsh coeff. of f.

1) f is a bent function if and only if:
$\forall v \in \mathbb{F}_2^k \quad | c_v | = 2^t$.

2) $\exists \epsilon \in \{-1, +1\}$ such that:
$w(f) = 2^{2t-1} + \epsilon 2^{t-1}$.

A useful lemma

Lemma 3
f: k-bent function,
$e \in \mathbb{F}_2^k$, $e \neq 0$.
g: linear form of $\mathbb{F}_2^k$ such that $g(e) = 1$.

There exists a k-bent function $f^\dagger$ in $\{f, f \oplus 1, f \oplus g, f \oplus g \oplus 1\}$ such that $f^\dagger(0) = f^\dagger(e) = 0$.

Strategy:
We can restrict the study to bent functions f such that $f(0) = f(e) = 0$.

We choose $e = (1, 0, \ldots, 0) = (1, \underline{0})$.

Special bent functions

Definition 4
$\mathcal{B}_0(k)$ is the set of k-bent functions f such that: $f(0,\underline{0}) = f(1,\underline{0}) = 0$.

If $f \in \mathcal{B}_0(k)$, its (special) polynomial representation is:
$P_f(x) = p(x) + x^n q(x) + f_p(\underline{0})x^{2n} + f_q(\underline{0})x^{2n+1}$

$$P_f(x) = p(x) + x^n q(x)$$

$n = 2^{k-1} - 1$
$p(x) = \sum_{i=0}^{n-1} p_i x^i$ and $q(x) = \sum_{i=0}^{n-1} q_i x^i$.
$p_i = f_p(\alpha^i) = f(0, \alpha^i)$, $q_i = f_q(\alpha^i) = f(1, \alpha^i)$.

Remark:
$p(x)$ and $q(x)$ are in $\mathbb{F}_2[x]/(x^n - 1)$.
They are the polynomial representations of the $(k-1)$-boolean functions f_p and f_q.

Special divisors of $x^{2^{k}-1}-1$

Definition:
If $i=\sum_{j=0}^{r-1}\epsilon_j 2^j \in \mathbb{N}$ then $w_2(i)$ is the weight of $(\epsilon_0, \epsilon_1, \ldots, \epsilon_j, \ldots, \epsilon_{r-1})$.
(**binary weight** of i).
$37 = 1 + 2^2 + 2^5$, $w_2(37) = 3$.

Remark: i and $(2^j)i$ calculated modulo 2^m-1 have the same binary weight.
Notations:

α: primitive root of $\mathbb{F}_{2^m}$.
$m_i(x)$: minimal polynomial of α^i.
$M_j(x)$: product, without repetition, of the $m_i(x)$ such that $1 \leq w_2(i) \leq j$.

Example: $m = 5$.

$$x^{31}-1 = m_0(x)m_1(x)m_3(x)m_5(x)m_7(x) m_{11}(x)m_{15}(x).$$

If $w_2(i) = 1 : i = 1$. If $w_2(i) = 2 : i = 3, 5$.
If $w_2(i) = 3 : i = 7, 11$. If $w_2(i) = 4 : i = 15$.

$M_1(x) = m_1(x),\ M_2(x) = m_1(x)m_3(x)m_5(x)$.
$M_3(x) = m_1(x)m_3(x)m_5(x)m_7(x)m_{11}(x)$.

Notation: $n = 2^{2t-1} - 1$

$g(x)$: divisor of $x^n - 1$ in $\mathbb{F}_2[x]$.

$< g(x) >_2^n = \{$multiples modulo $x^n - 1$ of $g(x)\}$.

(ideal generated by $g(x)$ = polynomial representation of a cyclic code).

A chain of ideals in $\mathbb{F}_2[x]/(x^n - 1)$:

$$< (x-1)M_{t-2}(x) >_2^n \supset < (x-1)M_{t-1}(x) >_2^n$$

$$\supset < (x-1)M_t(x) >_2^n \supset < (x-1)M_{t+1}(x) >_2^n$$

$$\supset \ \ldots\ldots \ \supset < (x-1)M_j(x) >_2^n \supset \ldots\ldots\ldots\ldots$$

$$< (x-1)M_{2t-3}(x) >_2^n \supset < (x-1)M_{2t-2}(x) >_2^n = \{0\}$$

Remark:

$M_i(x)$ is the generator of $\mathcal{R}(m-i-1, m)^*$ (punctured Reed-Muller code)

The main result

Theorem 5
$f \in \mathcal{B}_0(k)$, $k = 2t$, $n = 2^{2t-1} - 1$.
$w(f) = 2^{2t-1} + \epsilon 2^{t-1}$ *with* $\epsilon \in \{-1, +1\}$.
$P_f(x) = p(x) + x^n q(x)$
Define $r(x) = p(x) \oplus q(x)$.
1)

$w(p(x)) = w(r(x)) = 2^{2t-2}$.
$w(q(x)) = 2^{2t-2} + \epsilon 2^{t-1}$.

or

$w(p(x)) = 2^{2t-2} + \epsilon 2^{t-1}$.
$w(q(x)) = w(r(x)) = 2^{2t-2}$.

2) a) There exists l, $t - 2 \leq l \leq 2t - 4$ *s.t:*

- $p(x)$ *and* $q(x)$ *are in* $< (x-1)M_l(x) >_2^n$.

b) Let $\mathfrak{s}$ *be the largest integer s.t.*
$r(x) \in < (x-1)M_{\mathfrak{s}}(x) >_2^n$ *and* $\mathfrak{s} \leq 2t - 3$.

- $P_f(x) \in < (x-1)M_{\mathfrak{s}}(x) >_2^{2n}$.

- $P_{D_e}(x) \in < (x^n - 1)(x-1)M_{\mathfrak{s}}(x) >_2^{2n}$.
  ($e = (1, \underline{0})$*).*

Two parameters

Definition 6
$f \in \mathcal{B}_0(k)$ *with* $P_f(x) = p(x) + x^n q(x)$ *and*
$w(f) = 2^{2t-1} + \epsilon 2^{t-1}$, $\epsilon \in \{-1, +1\}$.

- $\mathfrak{i}$ *is the largest integer* $j \in [t-2, 2t-4]$ *s.t.* $p(x)$ *and* $q(x)$ *belong to* $< (x-1)M_j(x) >_2^n$.

- $\mathfrak{s}$ *is the largest integer* $m \in [\mathfrak{i}, 2t-3]$ *s.t.* $r(x)$ *belongs to* $< (x-1)M_m(x) >_2^n$.

Properties

$w(p(x)) = 2^{2t-2}$ (or $2^{2t-2} + \epsilon 2^{t-1}$).
$p(x) = \mu(x)(x-1)M_{\mathfrak{i}}(x)$.

$w(q(x)) = 2^{2t-2} + \epsilon 2^{t-1}$ (or 2^{2t-2}).
$q(x) = \nu(x)(x-1)M_{\mathfrak{i}}(x)$.

$w(r(x)) = 2^{2t-2}$.
$r(x) = \rho(x)(x-1)M_{\mathfrak{s}}(x)$.

$P_f(x) = \eta(x)M_{\mathfrak{s}}(x)$.

$P_{D_e}(x) = \theta(x)(x^n - 1)(x-1)M_{\mathfrak{s}}(x)$.

New parameters for Bent Functions

Let $\mathcal{L}(k)$ be the set of linear k-boolean functions.

Definition 7
If $f \in \mathcal{B}(k)$ define:

$Z(f) = \{f, f \oplus 1,\ f \oplus g,\ f \oplus g \oplus 1 \mid g \in \mathcal{L}(k), g((1,\underline{0})) = 1\}$

Proposition 8 and definition*.*

a) If $f \in \mathcal{B}(k)$ then there is $f^\dagger$ in $Z(f)$ such that $f^\dagger \in \mathcal{B}_0(k)$

b) All the $f^\dagger$ in $Z(f)$ which are in $\mathcal{B}_0(k)$ have the same parameters $\mathfrak{i}$ and $\mathfrak{s}$.
$\mathfrak{i}$ and $\mathfrak{s}$ are defined as the parameters of f.

Definition 9
$\mathcal{B}(k)[\mathfrak{i}, \mathfrak{s}]$ is the set of k-bent functions f with parameters $\mathfrak{i}$ and $\mathfrak{s}$.

Proposition 10
The non-empty sets $\mathcal{B}(k)[\mathfrak{i}, \mathfrak{s}]$ form a partition of the set of k-bent functions.

Proposition 11
If $f \in \mathcal{B}(k)[\mathfrak{i}, \mathfrak{s}]$ *with* $k = 2t$ *and* $deg(f) = d$, *then*

$$(\mathfrak{i}, \mathfrak{s}) = (k - d - 1, k - d - 1)$$

or

$$(\mathfrak{i}, \mathfrak{s}) = (k-d-2, s) \text{ with } k-d-1 \leq s \leq k-3.$$

Conclusion

Unfortunately ....

Fortunately ....

EXAMPLES

The partition of $\mathcal{B}(6)$: (G.Vega).

$$\mathcal{B}(6) = \mathcal{B}(6)[1,2] \cup \mathcal{B}(6)[1,3] \cup \mathcal{B}(6)[2,2] \cup \mathcal{B}(6)[2,3]$$

Degree 3

$| \mathcal{B}(6)[1,2] | = 2^{13}(3^4)(7)(31)(37)$

$| \mathcal{B}(6)[1,3] | = 2^{13}(3^3)(7)(31)$

$| \mathcal{B}(6)[2,2] | = 2^{13}(3^3)(7)(31)$

Degree 2

$| \mathcal{B}(6)[2,3] | = 2^{13}(7)(31)$

Remark: $| \mathcal{B}(6)[1,3] | = | \mathcal{B}(6)[2,2] |$

Duality

The dual of f is the k-boolean function f^* whose support is $\{v \in \mathbb{F}_2^k \mid c_v = -2^t\}$.
f^* is a bent function and $(f^*)^* = f$.

Define $\delta : \mathcal{B}(6) \longrightarrow \mathcal{B}(6)$ such that $\delta(f) = f^*$.
We obtain:

$$\delta(\mathcal{B}(6)[1,2]) = \mathcal{B}(6)[1,2]$$

$$\delta(\mathcal{B}(6)[2,3]) = \mathcal{B}(6)[2,3]$$

$$\delta(\mathcal{B}(6)[1,3]) = \mathcal{B}(6)[2,2]$$

Example 1:

Definition of f:
Let γ be a primitive root of $\mathbb{F}_{64}$ with $\gamma^6 + \gamma + 1 = 0$.

$L = \mathbb{F}_8^* = \{1, \gamma^9, \gamma^{18}, \gamma^{27}, \gamma^{36}, \gamma^{45}, \gamma^{54}, \}$.

The support of f is $L \cup \gamma L \cup \gamma^2 L \cup \gamma^3 L$.
Thus f is a "Partial-Spread Bent Function" (Dillon).
$w(f) = 28$, $\epsilon = -1$.

$(0, \underline{0})$ is the representation of 0 and $(1, \underline{0})$ is the representation of γ^5 but 0 and γ^5 are not in the support of f.
Then $f \in \mathcal{B}^-(6)$.

We find: $P_f(x) = p(x) + x^{31}q(x)$ with:

$$p(x) = x^{28} + x^{26} + x^{25} + x^{24} + x^{23} + x^{21} + x^{16} + x^{15}$$
$$+x^{13} + x^{12} + x^{8} + x^{5} + x^{3} + x^{2} + x + 1$$
$$= \mathbf{A(x)(x-1)M_1(x)} \text{ with}$$
$$A(x) = (x+1)(x^{21} + x^{17} + x^{16} + x^{15} + x^{12} + x^{9} + x^{7}$$
$$+x^{5} + x^{4} + x^{3} + x^{2} + x + 1)$$

$$q(x) = x^{30} + x^{28} + x^{24} + x^{21} + x^{20} + x^{18} + x^{17} + x^{16}$$
$$+x^{13} + x^{12} + x^{11} + x^{4} = \mathbf{B(x)(x-1)M_1(x)} \text{ with}$$
$$B(x) = x^{4}(x+1)(x^{6} + x^{5} + x^{4} + x^{2} + 1)$$
$$(x^{13} + x^{12} + x^{9} + x^{8} + x^{7} + x^{6} + x^{4} + x^{2} + 1)$$

$$r(x) = x^{30} + x^{26} + x^{25} + x^{23} + x^{20} + x^{18} + x^{17} + x^{15}$$
$$+x^{11} + x^{8} + x^{5} + x^{4} + x^{3} + x^{2} + x + 1$$
$$= \mathbf{C(x)(x-1)M_2(x)} \text{ with}$$
$$C(x) = (x+1)^{4}(x^{4} + x^{3} + 1)(x^{6} + x^{4} + x^{2} + x + 1)$$

$$P_f(x) = \mathbf{D(x)(x-1)M_2(x]} \text{ with}$$

$$D(x) =$$
$$(x+1)^{3}(x^{13} + x^{10} + x^{9} + x^{6} + x^{5} + x^{4} + x^{2} + x + 1)$$
$$(x^{9} + x^{8} + x^{6} + x^{5} + x^{3} + x + 1)(x^{3} + x + 1)$$
$$(x^{18} + x^{15} + x^{14} + x^{12} + x^{9} + x^{7} + x^{5} + x^{3} + 1)$$

f belongs to $\mathcal{B}_0(6)[1,2]$,

the degree of f is 3,

$$w(p(x)) = w(r(x)) = 2^{2t-2} = 16$$
$$w(q(x)) = 2^{2t-2} - 2^{t-1} = 12$$

Example 2:

$k = 6$ and f is the nondegenerate quadratic form defined by

$$F(X_0, X_1, X_2, X_3, X_4, X_5) = \sum \sum_{0 \le i < j \le 5} X_i X_j$$

$(0, \underline{0})$ and $(1, \underline{0})$ are not in the support of f and thus f belongs to $\mathcal{B}^{-}(6)$.

We find:

$p(x) = \mathbf{A(x)(x-1)M_2(x)}$ with. $A(x) =$
$x^5(x^5 + x^4 + x^2 + x + 1)(x^9 + x^7 + x^5 + x^3 + x^2 + x + 1)$

$q(x) = \mathbf{B(x)(x-1)M_2(x)}$ with
$B(x) = (x-1)(x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^6+x^5+x^2+1)$

$r(x) = \mathbf{(x^2+x+1)(x-1)M_3(x)}$ (in the Simplex Code).

Then f belongs to $\mathcal{B}_0(6)[2, 3]$,

The degree of f is 2,

$w(p(x)) = 2^{2t-2} + 2^{t-1} = 20,$
$w(q(x)) = w(r(x)) = 2^{2t-2} = 16.$

Example 3 (given by G.Leander):

With $\underline{X} = (X_1, X_2, X_3, X_4, X_5)$:

$P(\underline{X}) = X_1X_2 + X_2X_3 + X_3X_4$,
$Q(\underline{X}) = P(\underline{X}) + X_1X_3 + X_5$

Let f be defined by its AFN:
$F(X_0, \underline{X}) = (1 + X_0)P(\underline{X}) + X_0Q(\underline{X})$

One can check by computer that the boolean function f is a bent function. We find :

$$p(x) = x^{28} + x^{27} + x^{23} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{8} = \mathbf{x^8(x+1)^5M_2(x)}$$

$$q(x) = x^{30} + x^{27} + x^{25} + x^{24} + x^{21} + x^{20} + x^{19} + x^{18} + x^{15} + x^{14} + x^{11} + x^{10} + x^{9} + x^{7} + x^{5} + x^{4}$$
$$= \mathbf{x^4(x+1)(x^{10}+x^9+x^8+x^6+x^5+x^4+x^3+x+1)M_2(x)}$$

$$r(x) = x^{30} + x^{28} + x^{25} + x^{24} + x^{21} + x^{17} + x^{16} + x^{13} + x^{11} + x^{10} + x^{9} + x^{8} + x^{7} + x^{5} + x^{4}$$
$$= \mathbf{x^4(x+1)(x^4+x^3+1)(x^6+x+1)M_2(x)}$$

Then f belongs to $\mathcal{B}_0(6)[2,2]$

The degree of f is 3.

$w(p(x)) = 2^{2t-2} + \epsilon 2^{t-1} = 12$,

$w(q(x)) = w(r(x)) = 2^{2t-2} = 16$

Example 4:

f is defined by:
$f_p(x) = tr(\omega x + x^7 + x^{11})$
$f_q(x) = tr((\omega+1)x + x^7 + x^{11})$ with $\omega = \alpha^{-1}$.
We check by computer that f is a bent function. We find:

$$
\begin{aligned}
p(x) = {} & x^{28} + x^{27} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{17} \\
& + x^{16} + x^{13} + x^{11} + x^9 + x^8 + x^5 + x^3 + x^2 \\
& = \mathbf{A(x)(x+1)M_1(x)} \text{ with}
\end{aligned}
$$
$$A(x) = x^2(x^{10} + x^9 + x^8 + x^6 + x^4 + x^2 + 1)m_7(x)m_{11}(x).$$

$$
\begin{aligned}
q(x) = {} & x^{28} + x^{27} + x^{26} + x^{23} + x^{18} + x^{16} + x^{12} + x^{10} \\
& + x^8 + x^6 + x^2 + 1 \\
& = \mathbf{B(x)(x+1)M_1(x)} \text{ with}
\end{aligned}
$$
$$B(x) = (x+1)x^{11} + x^7 + x^3 + x^2 + 1)m_7(x)m_{11}(x).$$

$$
\begin{aligned}
r(x) = {} & x^{26} + x^{24} + x^{22} + x^{21} + x^{20} + x^{18} + x^{17} + x^{13} \\
& + x^{12} + x^{11} + x^{10} + x^9 + x^6 + x^5 + x^3 + 1 \\
& = \mathbf{(x+1)M_3(x)}
\end{aligned}
$$

f belongs to $\mathcal{B}(6)[1,3]$
The degree of f is 3.
Weights:

$$w(q(x)) = 2^{2t-2} - 2^{t-1} = 20$$
$$w(p(x)) = w(r(x)) = 2^{2t-2} = 16$$