A family of crooked functions

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

September 10, 2007

It has been proved in [3] that binomial functions $aX^i + bX^j$ on a finite field $F = \mathbb{F}_{2^r}$ can be crooked only if both exponents i, j have 2-weight at most 2. In the meantime several families of quadratic binomials have been constructed. The first examples arose from computer experiments [7]. Infinite families were constructed in [4, 5, 6]. In these families either $r = 3k$ or $r = 4k$. In the present paper we simplify and generalize these constructions. The two infinite families are really only one family. A brief construction is given in Section 2. Aside of this family only one sporadic example of a binomial crooked function is known. It has $r = 10$. We describe this sporadic example and prove its crookedness. The proof is in terms of a smooth trigonal algebraic curve of genus 3. For general background on trigonal curves see [1].

Here is a description of the infinite family. Let $F = GF(q^k)$, where $q = 2^s$. Consider the trace and norm $T, N : F \longrightarrow \mathbb{F}_q$, let $q' = 2^i$. Choose $\mu \in F$ such that $N(\mu) = 1$ and the function $f : F \longrightarrow F$ defined by

$$f(x) = x^{q'+1} + \mu x^{qq'+q^{k-1}}.$$

Our result is the following:

Theorem 1. *The function $f(x)$ above is crooked when the following are satisfied:*

- $r = ks, k \in \{3, 4\}$.
- *The integers k, s, i are pairwise coprime and $k \mid i + s$.*

- *$\mu = \epsilon^e$, where ϵ is a primitive element of $F = GF(2^r), e$ is a multiple of $2^s - 1$ and coprime to $2^k - 1$.*

An alternative terminology is $f(x) = g_0(x)g_i(x) + \mu g_{i+s}(x)g_{(k-1)s}(x)$ where g_i the field automorphism mapping $x \mapsto x^{2^i}$. Applying g_{-i}, g_{-i-s} or g_s yields equivalent functions. In particular crooked functions of the form $g_0(x)g_j(x) + \mu' g_{j-s}(x)g_s(x)$ are obtained as well.

The sporadic example is defined on $F = \mathbb{F}_{2^{10}}$ as

$$f(x) = x^3 + \mu x^{36}$$

where μ is an element of order 3. Its crookedness is proved in Section 3.

In the next section we start by reviewing general facts concerning crooked binomials.

1 Generalities

Let $F = GF(2^r)$ and $f(x) = xg_i(x) + \mu g_j(x)g_k(x)$. In this quadratic case the notions of an APN function and of a crooked function coincide. Recall that function $f(x)$ as above is **crooked** if for every $0 \neq a \in F$ the additive derivative δ_a defined by $\delta_a(x) = f(x+a) + f(x)$ is two-to-one: each $b \in F$ has either 0 or 2 preimages under δ_a.

Theorem 2. *Let $f(x) = xg_i(x) + \mu g_j(x)g_k(x)$, where $0 \neq \mu \in F = GF(2^r)$. Define $m = 2^j + 2^k - 2^i - 1, d = gcd(2^r - 1, m)$ and let U be the subgroup of order $(2^r - 1)/d$. Then $f(x)$ is APN (crooked) if and only if the following hold:*

- *$i, j - k, r$ do not have a common divisor.*
- *No element of the coset $u \in \mu U$ is representable in the form*

$$u = \frac{x + g_i(x)}{g_j(x) + g_k(x)}$$

When the first condition is satisfied, the second is equivalent with the following: for each $t \in U$ the equation

$$\mu t(g_j(x) + g_k(x)) + x + g_i(x) = 0$$

has only solutions $x \in \mathbb{F}_2$.

Proof. In the case at hand

$$\delta_a(x) = (x+a)g_i(x+a) + xg_i(x) + ug_j(x+a)g_k(x+a) + ug_j(x)g_k(x).$$

After forgetting constants we obtain

$$d_a(x) = xg_i(a) + ag_i(x) + u(g_j(x)g_k(a) + g_j(a)g_k(x),$$

a linear function. Write $x = ay$. Then

$$d_a(y) = yag_i(a) + g_i(y)ag_i(a) + u(g_j(a)g_k(a)g_j(y) + g_j(a)g_k(a)g_k(y)).$$

We collect terms and see $a = x$ as a variable:

$$d(x,y) = xg_i(x)(y + g_i(y)) + ug_j(x)g_k(x)(g_j(y) + g_k(y)).$$

Our function f is crooked if for every $x \neq 0$ this function as a function of y alone has rank $r-1$. As $d(x,1) = 0$ the condition is that $d(x,y) \neq 0$ whenever $xy \neq 0$ and $y \neq 1$. Equivalently: the equation

$$xg_i(x)(y + g_i(y)) = ug_j(x)g_k(x)(g_j(y) + g_k(y))$$

is satisfied only when $xy = 0$ or $y = 1$. An obvious condition is that the fixed field of g_i and g_{j-k} is $\mathbb{F}_2$. This is the first condition of the theorem. Assume it is satisfied. The remaining condition is that μ is not representable in the form

$$\mu = \frac{xg_i(x)}{g_j(x)g_k(x)} \frac{y + g_i(y)}{g_j(y) + g_k(y)}$$

(with y not in the fixed field of g_i or of g_{j-k}). The factor involving x describes the subgroup U of order $(2^r - 1)/d$, where $d = (2^r - 1, m)$. □

2 The proof of Theorem 1

The first condition of Theorem 2 is $gcd(i, i+2s, ks) = 1$, which is equivalent to

- $gcd(i, s) = 1$ and either i odd or k odd.

The second condition is the following: for each $u \in \mu U$ the only solutions to the equation

$$u(x^{qq'} + x^{q^{k-1}}) + x + x^{q'} = 0$$

are $x \in \mathbb{F}_2$.

As $q-1$ is a divisor of m we have that U is a subgroup of the group of elements of norm 1. We need U to be a proper subgroup. We have $m = (q-1)(q^{k-2}+\cdots+1+q')$. It follows $d = (q-1)d'$, where $d' = (q^{k-1}+\cdots+1, q^{k-1}-q')$ and we need $d' \neq 1$. This implies $g = gcd(ks, (k-1)s - i) \neq 1$. As $(s, i) = 1$ it follows that g is coprime to s and $g = (k, s+i)$. It follows $d' = 2^{(k,s+i)} - 1$.

Lemma 1. *U has index d' in the group of order $(q^k - 1)/(q - 1)$, where $d' = 2^{(k,s+i)} - 1$.*

For a fixed $x \in F$ denote $y = g_i(x) = x^{q'}$ and denote the conjugates under the Galois group $G = G(F \mid \mathbb{F}_q)$ by $x_j = g_{js}(x)$, likewise y_j and u_j. In particular $x_0 = x, y_0 = y, u_0 = u$. Observe $N(u) = u_0 \cdot \ldots u_{k-1} = 1$. Also fix c such that $c^{q-1} = u_0$. With this terminology the basic equation in Theorem 2 is

$$f_0: \ u_0(y_1 + x_{k-1}) + x_0 + y_0 = 0.$$

Recall that u_0 is chosen arbitrary in the coset μU. For each such u_0 we have to prove that the basic equation has no solutions except for $x \in \mathbb{F}_2$.

Let f_j be the conjugates of equation f_0 under G. Here $j = 0, 1, \ldots, k-1$. Let now f_0 be satisfied. Fix $v = v_0 \in F$ with its conjugates v_j and consider $\sum_{j=0}^{k-1} v_j f_j$. This simplifies:

$$T(x(v + u_1 v_1)) = T(y(v + u_{k-1} v_{k-1})).$$

The choice $v = 1/c^q$ yields $v + u_1 v_1 = 0$. The trace on the right has to vanish as well. Likewise for $v = c$ we have $v + u_{k-1}v_{k-1} = 0$ and the trace on the left has to vanish:

Proposition 1. *Assume f_0 is satisfied. For every $v \in F$ we have*

$$T(x(v + u_1 v_1)) = T(y(v + u_{k-1} v_{k-1})).$$

Special cases are

$$T(y(1/g_{-s}(c) + 1/g_s(c)) = 0$$

$$T(x(c + g_{2s}(c)) = T(yg_i(c + g_{2s}(c))) = 0.$$

Lemma 2. *The two $\mathbb{F}_q$-linear conditions on y in Proposition 1 are linearly dependent over $\mathbb{F}_q$ if and only if*

$$1/u_0^{q+q'} = (1 + u_0 u_{k-1})^{(q-1)(qq'-1)}.$$

Proof. Assume they are linearly dependent. Write $a \sim b$ if $a/b \in \mathbb{F}_q$. We have

$$1/g_{-s}(c) + 1/g_s(c) \sim g_i(c + g_{2s}(c))).$$

Factor out $1/c$ on the left and $g_i(c)$ on the right, use $g_{-s}(c)/c = u_{k-1}$:

$$(1 + u_0 u_{k-1})/(cu_0) \sim g_i(c) g_i(1 + u_0 u_1).$$

Raising to power $q - 1$ yields equality:

$$1/u_0^{q+q'} = (1 + u_0 u_{k-1})^{(q-1)(qq'-1)}.$$

□

Case $k = 3$

By Lemma 1 we have $d' \neq 1$ if and only if $s + i$ is a multiple of 3, and $d' = 7$ in this case.

It has to be shown that the basic equation

$$f_0 : \; u_0(x_2 + y_1) + x_0 + y_0 = 0$$

has only $x \in \mathbb{F}_2$ as solutions (equivalently $y \in \mathbb{F}_2$). By Lemma 2 the two linear conditions from Proposition 1 are independent. In fact, the right side of the equation in Lemma 2 is in U, the left is not. The solutions form a 1-dimensional subspace. As $\mathbb{F}_q$ does yield solutions we have $x, y \in \mathbb{F}_q$. The original equation f_0 yields $x(1 + u) = y(1 + u)$, hence $x = y$ and $x \in \mathbb{F}_2$ as $gcd(i, s) = 1$.

Case $k = 4$

We have $r = 4s$. The first necessary condition from Theorem 2 is :$gcd(i, s) = 1$ and i odd. As $d' = 2^{(4,s+i)} - 1 > 1$ we must have that s is odd. It follows $d' = 3$ if $i \equiv s \bmod 4$ and $d' = 15$ if $i \equiv -s \bmod 4$. In either case the two linear conditions of Proposition 1 are independent. The 2-dimensional space of solutions is then $L = GF(q^2)$. Apply f_0 when $y \in L$:

$$x + x^{q'} = u_0(x + x^{q'})^q.$$

If $x = x^{q'}$, then $x \in \mathbb{F}_2$. Otherwise u_0 is a $(q-1)$-st power of an element in L. In particular the order of u_0 divides $q+1$. Recall that we are assuming $i \equiv -s \mod 4$ and the order of μ divisible by the full 3-power contained in $q+1$ and also divisible by 5. Observe that $5|q^2+1$ but 25 does not divide q^2+1. It follows that the order of $u_0 \in \mu U$ will be divisible by 5, which does divide $q+1$, contradiction.

Case $k = 4, r = 12$

As an illustration consider case $k = 4, s = 3$. We have $s \equiv 3 \mod 4$ and therefore $i \equiv 1 \mod 4$. Let $i = 1$. Then $f(x) = x^3 + \mu x^{512+16} = x^3 + \mu x^{528}$. Let ϵ be a primitive element of $F = GF(2^{12})$ and write $\mu = \epsilon^e$. In order for the second case of Theorem 1 to apply we need e to be a multiple of 7 (so that $N(\mu) = 1$) and $gcd(e, 15) = 1$.

3 The sporadic case

Let $r = 2m$, where m is odd and $F = \mathbb{F}_{2^{2m}}, L = \mathbb{F}_{2^m}$ and $f(x) = x^3 + \omega x^{2^m+4}$ where ω is an element of order 3. We have that U is the multiplicative group of L. As $1, \omega$ form a basis of F over L we write elements of F in the form $x = a + b\omega$ and have to show that for $0 \neq c \in L$ the equation

$$\omega c(x + x^2) = g_m(x) + g_2(x)$$

has only $x \in \mathbb{F}_2$ as solutions. As $g_m(x) = a + b\overline{\omega}, g_2(x) = a^4 + b^4\omega, g_1(x) = a^2 + b^2\overline{\omega}$ the equation above is equivalent with

$$a + a^4 + b + (b + b^4)\omega = c\omega(a + a^2 + b^2 + (b + b^2)\omega$$

for some $c \in L$, equivalently

$$a + a^4 + b + (b + b^4)\omega = c(b + b^2) + c(a + a^2 + b)\omega$$

which is equivalent with

$$(a + a^4 + b)(a + a^2 + b) = (b + b^2)(b + b^4)$$

The crookedness condition is that this equation over L has only two solutions: $b = 0, a \in \mathbb{F}_2$. This means that the corresponding curve has only 3 rational points, $(0:0:1), (1:0:1), (1:1:0)$, those defined over $\mathbb{F}_2$.

Let $c = a + a^2$. The equation is then

$$c^3 + c^2(b+1) + b^6 + b^5 + b^3 = 0$$

and the condition is that for each solution in L either $c = 0$ or $tr(c) = 1$ where $tr : L \longrightarrow \mathbb{F}_2$ is the trace.

Let now $x = 1/b, y = c/b^2$ (or $b = 1/x, c = y/x^2$) The equation becomes

$$y^3 + (x^2 + x)y^2 + x^3 + x + 1 = 0$$

and the condition is that for each solution in L with $xy \neq 0$ we have $tr(y/x^2) = 1$.

Definition 1. *Let the projective curve C be defined over $\mathbb{F}_2$ by the affine equation*

$$y^3 + (x^2 + x)y^2 + x^3 + x + 1 = 0.$$

Lemma 3. *The curve C of Definition 1 is smooth of genus $g = 3$. Let N_i be its number of rational points over $\mathbb{F}_{2^i}$. Then*

$$N_1 = 4, N_2 = 10, \ N_3 = 13, N_4 = 18, N_5 = 14.$$

Proof. The corresponding homogeneous polynomial is

$$g(X, Y, Z) = Y^3Z + XY^2Z + X^2Y^2 + X^3Z + XZ^3 + Z^4.$$

We have $F_Y = Y^2Z$. If $Z = 0$, then g shows $XY = 0$. However $F_Z = Y^3 + XY^2 + X^3 + XZ^2$ which cannot vanish under those circumstances. We have $Y = 0$. Then $F_Z = X(X^2 + Z^2), F_X = Z(X^2 + Z^2)$. As $Z \neq 0$ we must have $X = Z$ which contradicts the curve equation. As the curve is smooth of degree 4 its genus is 3.

We have $g(X, Y, 0) = X^2Y^2$. The two points at infinity are therefore $(1:0:0), (0:1:0)$. Write all other points as $P(x, y) = (x : y : 1)$. The two remaining rational points over $\mathbb{F}_2$ are $P(0, 1)$ and $P(1, 1)$. So $N_1 = 4$. When $x \in \mathbb{F}_2$, then $y^3 = 1$. This yields 6 rational points. When $x = \omega$ or $x = \overline{\omega}$ we must have $y = x$. This yields two further rational points over $\mathbb{F}_4$. We have $N_2 = 10$.

Consider $\mathbb{F}_8$. When $x = \epsilon^3$, then $x^3 + x + 1 = 0$ and therefore $y = 0$ or $y = x^2 + x = \epsilon^5$. Considering conjugates this yields 6 rational points. When $x = \epsilon$, then $y = \epsilon^5$. This yields 3 more rational points. We have $N_3 = 4 + 6 + 3 = 13$. The congruence zeta function shows that all numbers N_i are determined by N_1, N_2, N_3. In fact the L-polynomial is

$$L(t) = 1 + t + 3t^2 + 4t^3 + 6t^4 + 4t^5 + 8t^6$$

and the generating function for the numbers $N_i - (2^i + 1)$ is therefore

$$tL'(t)/L(t) = (t+6t^2+12t^3+24t^4+20t^5+48t^6)(1-t-2t^2+t^3+3t^4+4t^5-9t^6 \dots)$$

$$= t + 5t^2 + 4t^3 + t^4 - 19t^5 \dots$$

In particular $N_5 = 33 - 19 = 14$. $\square$

We can now prove the crookedness of the sporadic function in case $r = 10$. Choose $X^5 + X^2 + 1$ as irreducible equation for the field $\mathbb{F}_{32}$. The powers of the corresponding primitive element are the following:

$\epsilon^5 = \epsilon^2 + 1$	$\epsilon^{14} = \epsilon^4 + \epsilon^3 + \epsilon^2 + 1$	$\epsilon^{23} = \epsilon^3 + \epsilon^2 + \epsilon + 1$
$\epsilon^6 = \epsilon^3 + \epsilon$	$\epsilon^{15} = \epsilon^4 + \epsilon^3 + \epsilon^2 + \epsilon + 1$	$\epsilon^{24} = \epsilon^4 + \epsilon^3 + \epsilon^2 + \epsilon$
$\epsilon^7 = \epsilon^4 + \epsilon^2$	$\epsilon^{16} = \epsilon^4 + \epsilon^3 + \epsilon + 1$	$\epsilon^{25} = \epsilon^4 + \epsilon^3 + 1$
$\epsilon^8 = \epsilon^3 + \epsilon^2 + 1$	$\epsilon^{17} = \epsilon^4 + \epsilon + 1$	$\epsilon^{26} = \epsilon^4 + \epsilon^2 + \epsilon + 1$
$\epsilon^9 = \epsilon^4 + \epsilon^3 + \epsilon$	$\epsilon^{18} = \epsilon + 1$	$\epsilon^{27} = \epsilon^3 + \epsilon + 1$
$\epsilon^{10} = \epsilon^4 + 1$	$\epsilon^{19} = \epsilon^2 + \epsilon$	$\epsilon^{28} = \epsilon^4 + \epsilon^2 + \epsilon$
$\epsilon^{11} = \epsilon^2 + \epsilon + 1$	$\epsilon^{20} = \epsilon^3 + \epsilon^2$	$\epsilon^{29} = \epsilon^3 + 1$
$\epsilon^{12} = \epsilon^3 + \epsilon^2 + \epsilon$	$\epsilon^{21} = \epsilon^4 + \epsilon^3$	$\epsilon^{30} = \epsilon^4 + \epsilon$
$\epsilon^{13} = \epsilon^4 + \epsilon^3 + \epsilon^2$	$\epsilon^{22} = \epsilon^4 + \epsilon^2 + 1$	$\epsilon^{31} = 1$

The orbits under the Galois group have representatives $\epsilon, \epsilon^7, \epsilon^{15}$ and $\epsilon^3, \epsilon^5, \epsilon^{11}$. The first three have trace 0, the latter have trace 1. As $N_5 = 14$ and $N_1 = 4$ there are two conjugate classes of rational points defined of $\mathbb{F}_{32}$ but not over $\mathbb{F}_2$. The claim is that $tr(y/x^2) = 1$ for each of the 10 rational points $P(x, y)$ of degree 5. Representatives of the conjugacy classes of points are $P(\epsilon, \epsilon^{12})$ and $P(\epsilon^{21}, \epsilon)$. As $tr(y/x^2) = 1$ in both cases the crookedness is proved. In case $r = 6$ the condition is not satisfied.

4 Conclusion

We have given short descriptions of all the binomial crooked functions that are currently known. They come in an infinite family and one sporadic example. Computer experiments lead us to conjecture that no other crooked binomial functions exist.

References

[1] Daniel Bierbrauer: *Codes auf hyperelliptischen und trigonalen Kurven,* Diplomarbeit, University of Heidelberg 2006.

[2] J. Bierbrauer: *Introduction to Coding Theory,* Chapman and Hall, CRC Press 2004.

[3] J. Bierbrauer and G. M. Kyureghyan: *Crooked binomials,* *Designs, Codes and Cryptography,* to appear.

[4] L. Budaghyan, C. Carlet, P. Felke, G. Leander: *An infinite class of quadratic APN functions which are not equivalent to power mappings, Proceedings of the IEEE International Symposium on Information Theory 2006, Seattle.*

[5] L. Budaghyan, C. Carlet, G. Leander: *A class of quadratic APN binomials inequivalent to power functions,* submitted.

[6] L. Budaghyan, C. Carlet, G. Leander: *Another class of quadratic APN binomials over* $\mathbb{F}_{2^n}$ *: the case n divisible by* 4, manuscript.

[7] Y. Edel, G. Kyureghyan and A. Pott: *A new APN function which is not equivalent to a power mapping,* *IEEE Transactions on Information Theory* **52** (2006), 744-747.