Constructing Generalized Bent Functions from Trace Forms over Galois Rings

Xiaoming Zhang

Key Laboratory of Mathematics Mechanization, CAS

Oct. 26, 2012, Beijing

Joint work with Zhuojun Liu, Baofeng Wu and Qingfang Jin

Outline of this talk

Outline of this talk

- A constant-amplitude code is a code that reduces the peak-to-average power ratio (PAPR) in multicode code-division multiple access (MC-CDMA) systems to the favorable value 1.
- Kai-Uwe Schmidt showed the conncetion between codes with PAPR equal to 1 and functions from the binary m-tuples to $\mathbb{Z}_4$ having the bent property.
- Kai-Uwe Schmidt proposed a technique to consturct generalized bent functions using trace form over Galois rings.

Outline of this talk

Boolean function

Let $f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$, then f is called a Boolean function with m variables.

- f can be represented as a polynomial in $\mathbb{F}_2[x_1, x_2, \cdots, x_m]/(x_1^2 + x_1, x_2^2 + x_2, \cdots, x_m^2 + x_m)$.

Walsh Transform

The Walsh transform of a Boolean function f at u is defined by

$$W_f(u) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x) + x \cdot u}$$

where $x \cdot u = \sum_{1 \leq i \leq m} x_i u_i$ for $x = (x_1, x_2, \cdots, x_m)$, $u = (u_1, u_2, \cdots, u_m) \in \mathbb{F}_2^m$.

Walsh Transform

The Walsh transform of a Boolean function f at u is defined by

$$W_f(u) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+x\cdot u}$$

where $x \cdot u = \sum_{1\le i\le m} x_i u_i$ for $x = (x_1, x_2, \cdots, x_m)$, $u = (u_1, u_2, \cdots, u_m) \in \mathbb{F}_2^m$.

Bent function

$f : \mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ is called a Bent function if $|W_f(u)| = 2^{m/2}$ for all $u = (u_1, u_2, \cdots, u_m) \in \mathbb{F}_2^m$.

- The number of variables m must be even.

Generalized Boolean function

A generalized Boolean function is defined as a map $f : \mathbb{F}_2^m \longrightarrow \mathbb{Z}_{2^h}$, where h is a positive integer.

- Write $k = (k_1, k_1, ..., k_m)$ for $k \in \{0, 1\}^m$, every such function can be uniquely expressed in the polynomial form

$$f(x) = f(x_1, ..., x_m) = \sum_{k\in\{0,1\}^m} c_k \prod_{j=1}^{m} x_j^{k_j},\ c_k \in \mathbb{Z}_{2^h}$$

Generalized Walsh Transform

For $f : \mathbb{F}_2^m \longrightarrow \mathbb{Z}_{2^h}$, the generalized Walsh transform of f is given by $\hat{f} : \mathbb{F}_2^m \longrightarrow \mathbb{C}$ with

$$\hat{f}(u) = \sum_{x \in \mathbb{F}_2^m} \omega^{f(x)}(-1)^{x \cdot u}$$

where "$\cdot$" denotes the scalar product in $\mathbb{F}_2^m$ and ω is a primitive 2^h-th root of unity in $\mathbb{C}$.

Generalized Bent function

A function $f : \mathbb{F}_2^m \longrightarrow \mathbb{Z}_{2^h}$ is called a generalized Bent function if $|\hat{f}(u)| = 2^{m/2}$ for all $u \in \mathbb{F}_2^m$.

- The number of variables m can be even or odd.

Outline of this talk

Notations:

- Define

$$\begin{array}{cccc} \mu: & \mathbb{Z}_{2^h} & \longrightarrow & \mathbb{F}_2, \\ & \sum_{i=0}^{h-1} a_i 2^i & \longmapsto & a_0 \end{array}$$

-

$$\begin{array}{cccc} \mu: & \mathbb{Z}_{2^h}[x] & \longrightarrow & \mathbb{F}_2[x] \\ & \sum_{i=0}^{m} b_i x^i & \longmapsto & \sum_{i=0}^{m} \mu(b_i) x^i \end{array}$$

- A polynomial $p(x) \in \mathbb{Z}_{2^h}[x]$ is called monic basic irreducible if $p(x)$ is monic and its projection $\mu(p(x))$ is irreducible over $\mathbb{F}_2$.

Galois ring

The Galois ring $\mathcal{R}_{h,m}$ is defined by $\mathcal{R}_{h,m} \cong \mathbb{Z}_{2^h}[x]/(p(x))$, where $p(x)$ is a basic irreducible polynomial over $\mathbb{Z}_{2^h}$ of degree m.

- Let $\xi \in \mathcal{R}_{h,m}$ be a root of $p(x)$, then

$$\mathcal{R}_{h,m} \cong \mathbb{Z}_{2^h}[x]/(p(x)) \cong \mathbb{Z}_{2^h}[\xi].$$

- The map μ can be extended to $\mathcal{R}_{h,m}$.

Teichemüler set

The set

$$\mathcal{T}_{h,m} := \{0\} \cup \mathcal{T}^*_{h,m}$$

is called the Teichmüller set of $\mathcal{R}_{h,m}$, where $\mathcal{T}^*_{h,m}$ is the cyclic group generated by ξ.

- $\mu(\xi)$ is a primitive element of $\mathbb{F}_{2^m}$, so $\mu(\mathcal{T}_{h,m}) = \mathbb{F}_{2^m}$.

Every element $z \in \mathcal{R}_{h,m}$ can be uniquely expressed as:

Additive representation

$$z = \sum_{i=0}^{m-1} z_i \xi^i, \; z_i \in \mathbb{Z}_{2^h}$$

2-adic Representation

$$z = \sum_{i=0}^{h-1} z_i 2^i, \; z_i \in \mathcal{T}_{h,m}$$

Frobenius automorphism

For any $z = \sum_{i=0}^{h-1} z_i 2^i, z_i \in \mathcal{T}_{h,m}$, the map $\sigma : \mathcal{R}_{h,m} \longrightarrow \mathcal{R}_{h,m}$ defined by

$$\sigma(z) = \sum_{i=0}^{h-1} z_i^2 2^i$$

is called the Frobenius automorphism of $\mathcal{R}_{h,m}$ with respect to the ground ring $\mathbb{Z}_{2^h}$.

Trace function

The trace function $\mathrm{Tr} : \mathcal{R}_{h,m} \longrightarrow \mathbb{Z}_{2^h}$ is defined to be

$$\mathrm{Tr}(z) = \sum_{i=0}^{m-1} \sigma^i(z).$$

- $\mathrm{Tr}(2r) = 2\mathrm{tr}(\mu(r))$ for any $r \in \mathcal{R}_{h,m}$, where "tr" is the trace function over $\mathbb{F}_{2^m}$.

Outline of this talk

Schmidt's construction

Theorem (K.-U. Schmidt)

Suppose $m \geq 3$ and let $f : \mathcal{T}_{2,m} \longrightarrow \mathbb{Z}_4$ be given by

$$f(x) = \varepsilon + \mathrm{Tr}(ax + 2bx^3), \ \varepsilon \in \mathbb{Z}_4, a \in \mathcal{R}_{2,m}, b \in \mathcal{T}_{2,m}^*.$$

Then $f(x)$ is a generalized Bent function if either of the following conditions holds:

1. $\mu(a) = 0$ *and* $x^3 + \frac{1}{\mu(b)} = 0$ *has no solution in* $\mathbb{F}_{2^m}$*;*
2. $\mu(a) \neq 0$ *and* $x^3 + x + \frac{\mu(b)^2}{\mu(a)^6} = 0$ *has no solution in* $\mathbb{F}_{2^m}$*.*

Here, μ is the modulo 2 reduction map on $\mathcal{R}_{2,m}$.

Question:

1. Can we generalize Schmidt's construction?
2. Can we say something more about the conditions to be satisfied?

Our construction

Theorem

Suppose $m \geq 5$ and let $f(x) = \varepsilon + \mathrm{Tr}(ax + 2bx^{1+2^k})$, where $\varepsilon \in \mathbb{Z}_4, a \in \mathcal{R}_{2,m}, b \in \mathcal{T}^*_{2,m}$. Then $f(x)$ is a generalized Bent function if either of the following conditions holds:

1. $\mu(a) = 0$ and $x^{2^{2k}-1} + \frac{1}{\mu(b)^{2^k-1}} = 0$ has no solution in $\mathbb{F}_{2^m}$;
2. $\mu(a) \neq 0$ and $\mu(b)^{2^k} x^{2^{2k}-1} + \mu(a)^{2^{k+1}} x^{2^k-1} + \mu(b) = 0$ has no solution in $\mathbb{F}_{2^m}$.

- Schmidt's construction is the special case $k = 1$ of ours.

Remark

For any positive integer k, there always exist $a \in \mathcal{R}_{2,m}$ and $b \in \mathcal{T}^*_{2,m}$ such that the function we construct is a generalized Bent function. Hence our construction greatly generalize Schmidt's.

Remark

For any positive integer k, there always exist $a \in \mathcal{R}_{2,m}$ and $b \in \mathcal{T}^*_{2,m}$ such that the function we construct is a generalized Bent function. Hence our construction greatly generalize Schmidt's.

Proof: (sketch) Let γ be a primitive element of $\mathbb{F}_{2^m}$, and let $\alpha = \mu(a)$, $\beta = \mu(b)$.

Condition (1) in the Theorem is equivalent to $\alpha = 0$ and $\beta \notin \langle \gamma^{\frac{2^{(2k,m)}-1}{2^{(k,m)}-1}} \rangle$;
Condition (2) in the Theorem is equivalent to

$$\bigcup_{\beta \in \mathbb{F}^*_{2^m}} h(\langle \gamma^{2^k-1} \rangle) \times \{\beta\} \subsetneqq \mathbb{F}^*_{2^m} \times \mathbb{F}^*_{2^m} = \bigcup_{\beta \in \mathbb{F}^*_{2^m}} \mathbb{F}^*_{2^m} \times \{\beta\},$$

where $h(x) = (\beta^{2^k} x^{2^k} + \frac{\beta}{x})^{\frac{1}{2^k+1}}$. This holds since $h(x)$ will never be a permutation polynomial over $\mathbb{F}_{2^m}$ [5].

A more general construction

Theorem

Let $f(x) = \varepsilon + \mathrm{Tr}(ax + 2bxL(x))$, where $L(x) = \sum_{i=0}^{m-1} a_i x^{2^i} \in \mathcal{T}_{2,m}[x]$, $\varepsilon \in Z_4, a \in \mathcal{R}_{2,m}, b \in \mathcal{T}_{2,m}^*$. Let $\alpha = \mu(a), \beta = \mu(b), \alpha_i = \mu(a_i)$. Then $f(x)$ is a generalized Bent function if

$$\sum_{i=0}^{m-1} (\beta\alpha_i z^{2^i} + (\beta\alpha_i)^{2^{m-i}} z^{2^{m-i}}) + \alpha^2 z$$

is a linearized permutation polynomial over $\mathbb{F}_{2^m}$.

- A polynomial over a finite field $\mathbb{F}_{q^n}$ of the form $B(x) = \sum_{i=0}^{n-1} b_i x^{q^i}$ is called a linearized polynomial.

About linearized permutation polynomials

Theorem (Dickson)

Let $B(x) = \sum_{i=0}^{n-1} b_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ be a linearized polynomial. Then $B(x)$ is a permutation polynomial if and only if the matrix

$$\begin{pmatrix} b_0 & b_1 & \cdots & b_{n-1} \\ b_{n-1}^q & b_0^q & \cdots & b_{n-2}^q \\ \cdots & \cdots & \cdots & \cdots \\ b_1^{q^{n-1}} & b_2^{q^{n-1}} & \cdots & b_0^{q^{n-1}} \end{pmatrix}$$

is nonsingular.

About linearized permutation polynomials

Theorem (B.F. Wu, Z.J. Liu)

$B(x) = \sum_{i=0}^{n-1} b_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ is a linearized permutation polynomial if and only if

$$\mathrm{GCRD}\left(\sum_{i=0}^{n-1} b_i x^i, x^n - 1\right) = 1,$$

where GCRD denotes the greatest common right divisor of two polynomials in $\mathbb{F}_{q^n}[x;\sigma]$ (σ is the Frobenius automorphism of $\mathbb{F}_{q^n}/\mathbb{F}_q$).

- $\mathbb{F}_{q^n}[x;\sigma]$ is known as the skew-polynomial ring, consisting of ordinary polynomials over $\mathbb{F}_{q^n}$ but with a non-commutative multiplication $xc = \sigma(c)x$ for any $c \in \mathbb{F}_{q^n}$;
- For skew-polynomials over $\mathbb{F}_q$, the GCRD degenerates to the ordinary GCD in $\mathbb{F}_q[x]$.

Hence from an algorithmic perspective, to test whether an $L(x) \in \mathcal{T}_{2,m}[x]$ will promise a generalized Bent function in our construction, we need only to test singularity of certain matrix over $\mathbb{F}_{2^m}$, or to compute certain GCRD in $\mathbb{F}_{2^m}[x;\sigma]$. Both can be done in polynomial time.

Hence from an algorithmic perspective, to test whether an $L(x) \in \mathcal{T}_{2,m}[x]$ will promise a generalized Bent function in our construction, we need only to test singularity of certain matrix over $\mathbb{F}_{2^m}$, or to compute certain GCRD in $\mathbb{F}_{2^m}[x;\sigma]$. Both can be done in polynomial time.

Example

Let $f(x) = \varepsilon + \mathrm{Tr}(x + 2xL(x))$, where $L(x) = \sum_{i=0}^{m-1} a_i x^{2^i} \in \mathcal{T}_{2,m}[x]$, $\varepsilon \in Z_4$, $x \in \mathcal{T}_{2,m}$ and $\alpha_i = \mu(a_i) \in \mathbb{F}_2$ for $i = 0, 1, \cdots, m-1$. Then $f(x)$ is a generalized Bent function if $\mathrm{GCD}(\sum_{i=0}^{m-1} \beta_i x^i, x^m - 1) = 1$ where $\beta_0 = 1, \beta_i = \alpha_i + \alpha_{m-i}$ for $i = 0, 1, \ldots, m-1$.

References

[1] K.-U. Schmidt, “On Spectrally-Bounded codes for Multi-Carrier Communications", Vogt Verlag, Dresden, Germany, 2007.

[2] B.R.McDonald, “Finite Rings with Identity", Marcel Dekker, New York, 1974.

[3] R. Lidl, H. Niederreiter “Finite Fields", Cambridge University Press, 1997.

[4] B.F. Wu, Z.J. Liu, “Linearized polynomials over finite fields revisited", Preprint.

[5] Y.Q. Li, M.S. Wang, "Permutation polynomials EA-equivalent to the inverse function over GF (2^n)", Cryptography and Communications 3(3): 175-186, 2011.

Thanks for your attention!