Generalized partially bent functions and cocyclic Butson matrices

J.A. Armario*, R. Egan†, D. L. Flannery‡

*Depart. Matemática Aplicada I, Universidad de Sevilla, Spain
†School of Mathematical Sciences, Dublin City University, Ireland
‡School of Mathematics, Statistics and Applied Mathematics, NUI Galway, Ireland

19 – 21 October, 2022

17th RECSI, Santander, Spain

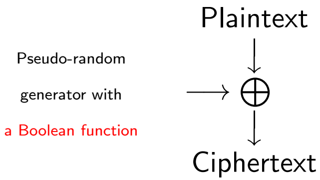
Outline

Index

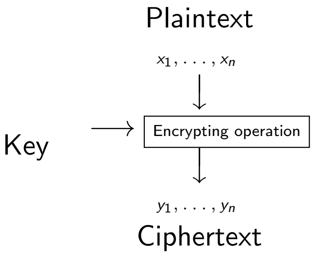
Boolean functions $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ in Cryptography

Symmetric Criptography

Stream ciphers



Block ciphers



outputs of Boolean functions

Cryptographic Boolean functions

Some Cryptographic criteria for Boolean functions in order to design "secure" cryptosystems

1. Balanced
2. Higher-order nonlinearity: Bent functions.
3. Correlation immunity
4. etc.

Some of these criteria are antagonistic ! Tradeoffs between all these criteria must be found.

Cryptographic Boolean functions

Main problems to study:

- Interests are in four aspects:
  1. Characterization
  2. Constructions
  3. Classifications
  4. Enumerations

- Extensions of this theory to:
  1. Vectorial Boolean functions
  2. Generalized functions
  3. etc.

Our motivation.

B. Schmidt. A survey of group invariant Butson matrices..., Radon Ser. Comput. Appl. Math. 23 (2019), 241–251.

Theorem 1

Let $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ be a map. The following are equivalent:

(1) f is a Generalized Bent Function (GBF);

(2) $\left[\zeta_h^{f(x-y)}\right]_{x,y\in\mathbb{Z}_q^m} \in \mathrm{BH}(q^m,h)$ is equivalent to a coboundary matrix $M_{\partial f}$;

(3) f is a perfect h-ary $(q,\ldots,q)$-array.

Additionally, if h is prime and divides q^m, then (1)–(3) are equivalent to

(4) $\{(f(x),x) \mid x \in \mathbb{Z}_q^m\}$ is a splitting $(q^m,h,q^m,q^m/h)$-relative difference set in $\mathbb{Z}_h \times \mathbb{Z}_q^m$.

Definitions

Let q, m, h be positive integers, and let ζ_k be the complex k^{th} root of unity $\exp\left(2\pi\sqrt{-1}/k\right)$. Schmidt defines a map

$$f : \mathbb{Z}_q^m \to \mathbb{Z}_h$$

to be a generalized bent function (GBF) if

$$\Big|\sum_{x\in\mathbb{Z}_q^m} \zeta_h^{f(x)}\zeta_q^{-vx^\top}\Big|^2 = q^m \text{ for all } v \in \mathbb{Z}_q^m,$$

where $|z|$ as usual denotes the modulus of $z \in \mathbb{C}$.

Example of GBF

$$\begin{array}{rccc} f: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 \\ & (x_1, x_2) & \mapsto & x_1 \cdot x_2 \end{array}$$

v	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$\sum_{x \in \mathbb{Z}_2^2} (-1)^{f(x)+vx^\top}$	2	2	2	-2

Bent functions are of interest in cryptography, coding theory,...

Example of GBF (nonlinearity of Boolean functions)

$$\begin{array}{cccc} f: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 \\ & (x_1, x_2) & \mapsto & x_1 \cdot x_2 \end{array}$$

(x_1, x_2)	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$f(x_1, x_2)$	0	0	0	1
x_2	0	1	0	1
$x_1 + x_2$	0	1	0	0

The Hamming distance of f to the 8 affine Boolean functions is either 1, 2 or 3. Therefore the nonlinearity of f is 1.

Example of GBF (Cryptography)

Boolean functions with large nonlinearity are difficult to approximate by linear functions and so provide resistance against linear cryptanalysis.

Result

The largest nonlinearity of a Boolean function on $\mathbb{Z}_2$ is $2^{n-1} - 2^{n/2-1}$ for n even. The functions attaining this bound, are called bent functions.

Definitions

Let H be a square matrix of order n with entries in $\langle \zeta_k \rangle = \{\zeta_k^l : l = 0, \ldots, k-1\}$. We say that H is a Butson Hadamard matrix if

$$HH^* = nI_n$$

where I_n is the $n \times n$ identity matrix and H^* is the complex conjugate transpose of H. We denote by $H \in \mathrm{BH}(n, k)$.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad HH^* = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

Definitions: Cocyclic Butson matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

indexing the rows and columns of H with the element of $\mathbf{Z}_2^2 = \{(0,0),(0,1),(1,0),(1,1)\}$. We have

$$\psi(x,y) = H_{x,y}, \quad x, y \in \mathbf{Z}_2^2$$

satisfies that

$$\psi(x,y)\psi(xy,z) = \psi(x,yz)\psi(y,z), \ \forall x,y,z \in \mathbf{Z}_2^2$$

- ψ is a cocycle and H is a cocyclic Butson matrix.
- The "simplest" cocycles are the coboundaries.

Example of GBF: Butson Hadamard matrix

$$\begin{array}{cccc} f: & \mathbb{Z}_2^2 & \rightarrow & \mathbb{Z}_2 \\ & (x_1, x_2) & \mapsto & x_1 \cdot x_2 \end{array}$$

$$M = [\zeta_2^{f(x-y)}]_{x,y\in\mathbb{Z}_2^2} = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}$$

Observe

$$H = PMQ^T, \quad \text{with} \quad P = Q = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

Definitions

Let E be a group with a normal subgroup N of order m and index v. A (v, m, k, λ)-*relative difference set in E relative to N* (the *forbidden subgroup*) is a k-subset R of a transversal for N in E such that

$$|R \cap xR| = \lambda \quad \forall x \in E \setminus N.$$

That is, x can be written as $r_1 r_2^{-1}$ for λ different pairs $(r_1, r_2) \in R^2$.

We call R *abelian* if E is abelian, and *splitting* if N is a direct factor of E.

Example of GBF: relative difference set

$$\begin{array}{cccc} f: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 \\ & (x_1, x_2) & \mapsto & x_1 \cdot x_2 \end{array}$$

$$R = \{(0,\, 0, 0),\ (0,\, 0, 1),\ (0,\, 1, 0),\ (1,\, 1, 1)\} \subset \mathbb{Z}_2 \times \mathbb{Z}_2^2$$

$$E = \mathbb{Z}_2^3 \quad \text{and} \quad N = \{(0,\, 0, 0), (1,\, 0, 0)\}$$

$x \setminus y^{-1}$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(1,1,1)$
$(0,0,0)$		$(0,0,1)$	$(0,1,0)$	$(1,1,1)$
$(0,0,1)$	$(0,0,1)$		$(0,1,1)$	$(1,1,0)$
$(0,1,0)$	$(0,1,0)$	$(0,1,1)$		$(1,0,1)$
$(1,1,1)$	$(1,1,1)$	$(1,1,0)$	$(1,0,1)$	

R is a $(4, 2, 4, 2)$-RDS in $\mathbb{Z}_2 \times \mathbb{Z}_2^2$.

Definitions

Let $\mathbf{s} = (s_1, \ldots, s_m)$ be an m-tuple of integers $s_i > 1$, and let $G = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_m}$. A *$h$-ary $\mathbf{s}$-array* is merely a set map

$$\phi \colon G \to \mathbb{Z}_h.$$

When $h = 2$, the array is *binary*.

For $w \in G$, we define the periodic autocorrelation at shift w of an array ϕ, denoted $AC_\phi(w)$, by

$$AC_\phi(w) = \sum_{g \in G} \zeta_h^{\phi(g) - \phi(g+w)}.$$

If $AC_\phi(w) = 0$ for all $w \neq 0$, then ϕ is called perfect.

Example of GBF: perfect array

$$\begin{array}{cccc} f: & \mathbb{Z}_2^2 & \rightarrow & \mathbb{Z}_2 \\ & (x_1, x_2) & \mapsto & x_1 \cdot x_2 \end{array}$$

can be written as

$$M_f = [f(x,y)]_{x,y \in \mathbb{Z}_2} = \begin{array}{cc} 0 & 0 \\ 0 & 1 \end{array}.$$

Then:

w	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$AC(w)$	4	0	0	0

Example of GBF: perfect array (Cryptography)

The absolute indicator of $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ is

$$\delta(f) = \frac{1}{2^{n/2}} \max_{w \neq 0} |AC_f(w)|$$

This measures the resistance of a Boolean function against differential cryptanalysis.

Index

Our contribution: Cocycles in stead of coboundaries

Theorem 1

Let $f\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ be a map. The following are equivalent:

(1) f is a Generalized Bent Function (GBF);

(2) $\left[\zeta_h^{f(x-y)}\right]_{x,y\in\mathbb{Z}_q^m} \in \mathrm{BH}(q^m, h)$ is equivalent to a coboundary matrix $M_{\partial f}$;

(3) f is a perfect h-ary $(q, \ldots, q)$-array.

Additionally, if h is prime and divides q^m, then (1)–(3) are equivalent to

(4) $\{(f(x), x) \mid x \in \mathbb{Z}_q^m\}$ is a splitting $(q^m, h, q^m, q^m/h)$-relative difference set in $\mathbb{Z}_h \times \mathbb{Z}_q^m$.

Our contribution: Cocycles in stead of coboundaries

Theorem 2

Let h be a prime divisor of q, and let $\phi\colon \mathbb{Z}_q^m \to \mathbb{Z}_h$ be an array with expansion ϕ' of type $\mathbf{z} \neq \mathbf{0}$.

(a) The following are equivalent:

- (i) $\mu_{\mathbf{z}}\partial\phi$ is orthogonal, i.e., $M_{\mu_{\mathbf{z}}\partial\phi} \in \mathrm{BH}(q^m, h)$;
- (ii) ϕ is a $GPhA(q^m)$ of type $\mathbf{z}$;
- (iii) $\{g + K \in E/K \mid \phi'(g) = 0\}$ is a non-splitting $(q^m, h, q^m, q^m/h)$-relative difference set in E/K with forbidden subgroup H/K.

Our contribution in the general case (h-ary arrays)

Theorem 2 (continued)

(b) If $\mathbf{z} = \mathbf{1}$ then (i)–*(iii)* are equivalent to

(iv) ϕ' is a generalized plateaued function, i.e.,

$$\Big| \sum_{x \in \mathbb{Z}_{hq}^m} \zeta_h^{\phi'(x)} \zeta_{hq}^{-v\cdot x} \Big|^2 = \begin{cases} (h^2 q)^m & v \in \mathcal{F} \\ 0 & \text{otherwise,} \end{cases}$$

where $\mathcal{F} = \{v \in \mathbb{Z}_{hq}^m \mid v \equiv \mathbf{1} \mod h\}$.

(c) Let $h = q$ and $\mathbf{z} = \mathbf{1}$. Suppose that, for all $y \in \mathbb{Z}_h^m \setminus \{\mathbf{0}\}$ with $\sum y_i \equiv 0 \mod h$, there exists $x \in \mathbb{Z}_h^m$ satisfying (*). Then (i)–(iv) are equivalent to

(v) ϕ' is a GPBF.

Our contribution in the general case (h-ary arrays)

Remark

If $h = q$ in Theorem 2, then $|L| \cdot |\mathcal{F}| = (hq)^m$. This identity is the condition under which in the literature a map $f : \mathbb{Z}_q^m \to \mathbb{Z}_q$ is called a generalized partially bent function.

Definition

A generalized partially bent function *(GPBF) is a map* $f : \mathbb{Z}_q^m \to \mathbb{Z}_h$ *such that* $|AC_f(x)| \in \{0, q^m\}$ *for all* $x \in \mathbb{Z}_q^m$.

Example 1

The map $\phi = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix}$ on $\mathbb{Z}_3^2$ is a GP3A$(3,3)$ of type $\mathbf{z} = (1,1)$.
Its expansion $\phi' \colon \mathbb{Z}_9^2 \to \mathbb{Z}_3$ is defined by

$$\begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\
0 & 1 & 0 & 1 & 2 & 1 & 2 & 0 & 2 \\
2 & 2 & 1 & 0 & 0 & 2 & 1 & 1 & 0 \\
1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 \\
1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 & 0 \\
0 & 0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 \\
2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 \\
2 & 0 & 2 & 0 & 1 & 0 & 1 & 2 & 1 \\
1 & 1 & 0 & 2 & 2 & 1 & 0 & 0 & 2
\end{bmatrix}.$$

We have

$$AC_{\phi'}(v_1, v_2) = \begin{cases} 81\,\zeta_3^{-(v_1+v_2)/3} & v \in L \\ 0 & v \notin L, \end{cases}$$

where

$$L = \{(0,0),(0,3),(0,6),(3,0),(3,3),(3,6),(6,0),(6,3),(6,6)\}.$$

Therefore, ϕ' is a generalized partially bent function.

The cocyclic BH$(9,3)$, $M_{f_z \partial\phi}$, (represented in logarithmic form) is:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 0 & 0 & 2 & 2 & 1 & 2 \\ 0 & 1 & 0 & 2 & 1 & 1 & 2 & 2 & 0 \\ 0 & 2 & 0 & 1 & 2 & 2 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 2 & 1 & 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \\ 0 & 2 & 2 & 0 & 0 & 1 & 1 & 2 & 1 \end{bmatrix}.$$

$$R = \{(0,0)+K, (0,1)+K, (0,2)+K, (1,0)+K, (1,2)+K,$$
$$(1,7)+K, (2,3)+K, (2,4)+K, (2,8)+K\}$$

is a $(9,3,9,3)$-RDS in E/K with forbidden subgroup L/K for $K = \{(0,0),(3,6),(6,3)\}$.

Finally,

$$\mathcal{F} = \{(1,1),(1,4),(1,7),(4,1),(4,4),(4,7),(7,1),(7,4),(7,7)\}$$

and

$$\Big|\sum_{x\in\mathbb{Z}_9^2} \zeta_3^{\phi'(x)} \zeta_9^{-vx^\top}\Big|^2 = \begin{cases} 729 & v \in \mathcal{F} \\ 0 & v \notin \mathcal{F}. \end{cases}$$

Example 2

Let ϕ be the map on $\mathbb{Z}_2^3$ with layers

$$A_0 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad A_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Here A_i is the layer on $\{i\} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and $\phi(i, j, k) = A_i(j, k)$. Then ϕ is a GPBA$(2, 2, 2)$ of type $\mathbf{1}$. In particular, the expansion of ϕ is a GPBF; whereas no GBF $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2$ exists.

Result (By a iterative procedure)

For all $k \geq 3$ there exists a map from $\mathbb{Z}_2^k$ to $\mathbb{Z}_2$ whose expansion is a GPBF; whereas for odd k, no Bent function exists.

Thank you!!!

References

- W. de Launey and D. L. Flannery, *Algebraic design theory*. Math. Surveys. Monogr. 175, American Mathematical Society, Providence, RI (2011).
- S. Mesnager, F. Özbudak, and A. Sınak, *Characterizations of partially bent and plateaued functions over finite fields.* Arithmetic of Finite Fields, 224–241, Lecture Notes in Comput. Sci. 11321, Springer, Cham, 2018.
- S. Mesnager, C. Tang, and Y. Qi, *Generalized plateaued functions and admissible (plateaued) functions.* IEEE Trans. Inf. Theory 63 (2017), no. 10, 6139–6148.
- B. Schmidt, *A survey of group invariant Butson matrices and their relation to generalized bent functions and various other objects.* Radon Ser. Comput. Appl. Math. 23 (2019), 241–251.
- X. Wang, and J. Zhou, *Generalized partially bent functions.* In: Future Generation Communication and Networking (FGCN 2007). vol. 1, pp. 16–21, IEEE (2007).