Journey into differential and graph theoretical properties of (generalized) Boolean function

Pante Stănică
(includes joint work with T. Martinsen, W. Meidl, A. Pott, C. Riera, P. Solé)

Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943, USA; pstanica@nps.edu

The objects of the investigation: (Generalized) Boolean functions I

- Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$
- *Generalized Boolean function* $f : \mathbb{F}_2^n \to \mathbb{Z}_q$ $(q \geq 2)$; its set $\mathcal{GB}_n^q$; when $q = 2$, $\mathcal{B}_n$;
- *(Generalized) Walsh-Hadamard transform*:
$$\mathcal{H}_f^{(q)}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \zeta_q^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}},\ \zeta_q = e^{\frac{2\pi i}{q}};\ \text{(use } \mathcal{W}_f\text{, if } q = 2\text{)}$$
- Fourier transform: $\mathcal{F}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} f(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}}$
- Let $2^{k-1} < q \leq 2^k$. Then $\mathcal{GB}_n^q \ni f \longleftrightarrow \{a_i\}_{0 \leq i \leq k-1} \subset \mathcal{B}_n$:
$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x}), \forall \mathbf{x} \in \mathbb{F}_2^n.$$

Characterizing generalized bent $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$

- $f : \mathcal{GB}_n^q$ is *generalized bent* (*gbent*) if $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}, \forall \mathbf{u}$.

Theorem (Various Authors 2015–'17)

Let $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-2}a_{k-2}(\mathbf{x}) + 2^{k-1}a_{k-1}(\mathbf{x})$ be a function in $\mathcal{GB}_n^{2^k}$, $k > 1$, $a_i \in \mathcal{B}_n$, $0 \le i \le k-1$, and $\tilde{f} \in a_{k-1} \oplus \langle a_0, a_1, \ldots a_{k-2} \rangle$. Then f is gbent iff $\tilde{f}$ is bent (n even), respectively, semibent (n odd), with an (explicit) extra condition on the Walsh-Hadamard coeff.

Differential properties of generalized Boolean functions I

- $\mathbf{u} \in \mathbb{F}_2^n$ is a *linear structure* of $f \in \mathcal{GB}_n^q$ if the derivative $D_{\mathbf{u}} f(\mathbf{x}) := f(\mathbf{x} \oplus \mathbf{u}) - f(\mathbf{x}) = c \in \mathbb{Z}_q$ constant, for all $\mathbf{x} \in \mathbb{F}_2^n$.
- Let $S_f = \{\mathbf{x} \in \mathbb{F}_2^n \,|\, \mathcal{H}_f(\mathbf{x}) \neq 0\} \neq \emptyset$ (gen.WH support)

Theorem (Martinsen–Meidl–Pott–S., 2018)

Let $f \in \mathcal{GB}_n^{2^k}$, with $f(\mathbf{x}) = \sum_{i=0}^{k-1} 2^i a_i(\mathbf{x})$, $a_i \in \mathcal{B}_n$. The following are equivalent:

(*i*) $\mathbf{a}$ *is a linear structure for* f.

(*ii*) $\mathbf{a}$ *is a linear structure for* a_i, *s.t.* $a_i(\mathbf{a}) = a_i(\mathbf{0}), 0 \leq i < k-1$.

(*iii*) $\mathbf{a}$ *satisfies* $\zeta^{f(\mathbf{a})-f(\mathbf{0})} = (-1)^{\mathbf{a}\cdot\mathbf{w}}$, *for all* $\mathbf{w} \in S_f$.

Differential properties of generalized Boolean functions II

- We say that $f \in \mathcal{GB}_n^{2^k}$ satisfies the (*generalized*) *propagation criterion of order ℓ* ($1 \le \ell \le n$), $gPC(\ell)$, iff the autocorrelation $\mathcal{C}_f(\mathbf{v}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x}) - f(\mathbf{x} \oplus \mathbf{v})} = 0$, for all vectors $\mathbf{v} \in \mathbb{F}_2^n$ of weight $0 < wt(\mathbf{v}) \le \ell$.
- f is gbent $\iff gPC(n)$.

Theorem (Martinsen–Meidl–Pott–S., 2018)

Let $f \in \mathcal{GB}_n^{2^k}$, and $A_j^{(\mathbf{w})} = (D_{\mathbf{w}} f)^{-1}(j) = \{\mathbf{x} | f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x}) = j\}$. Then f is $gPC(\ell)$ if and only if, for $1 \le wt(\mathbf{w}) \le \ell$,

$$|A_0^{(\mathbf{0})}| = 2^n, |A_j^{(\mathbf{0})}| = 0, |A_j^{(\mathbf{w})}| = |A_{j+2^{k-1}}^{(\mathbf{w})}|, \ \forall\, 0 \le j \le 2^{k-1} - 1.$$

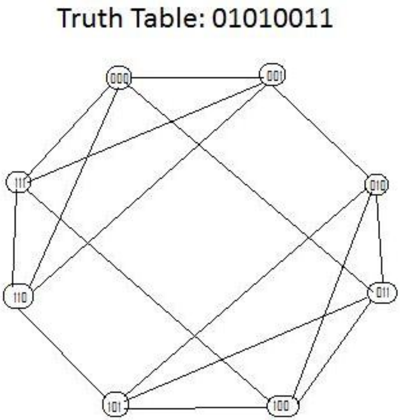
Can one "visualize" some cryptographic properties of a Boolean function?

- *Cayley graph* of $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $G_f = (\mathbb{F}_2^n, E_f)$,

$$E_f = \{(\mathbf{w}, \mathbf{u}) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \,:\, f(\mathbf{w} \oplus \mathbf{u}) = 1\}.$$

- Adjacency matrix $A_f = \{a_{i,j}\}$, $a_{i,j} := f(\mathbf{i} \oplus \mathbf{j})$ (where $\mathbf{i}$ is the binary representation as an n-bit vector of the index i);
- *Spectrum* of G_f is the set of eigenvalues of A_f (G_f).
- Cayley graph G_f has eigenvalues $\lambda_i = \mathcal{W}_f(\mathbf{i})$, $\forall i$.

Cayley graph example: $f(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_3$



Strongly regular graphs

- A graph is regular of degree r (or r-regular) if every vertex has degree r;
- The Cayley graph of a Boolean function is always a regular graph of degree $wt(f)$.
- We say that an r-regular graph G with v vertices is a strongly regular graph (SRG) with parameters (v, r, e, d) if $\exists$ integers $e, d \geq 0$ s.t. for all vertices $\mathbf{u}, \mathbf{v}$:
  - the number of vertices adjacent to both $\mathbf{u}, \mathbf{v}$ is e if $\mathbf{u}, \mathbf{v}$ are adjacent,
  - the number of vertices adjacent to both $\mathbf{u}, \mathbf{v}$ is d if $\mathbf{u}, \mathbf{v}$ are nonadjacent.
- We assume throughout that G_f is connected (in fact, one can show that all connected components of G_f are isomorphic).

Bernasconi-Codenotti correspondence

- Shrikhande & Bhagwandas '65: A connected r-regular graph is strongly regular iff $\exists$ exactly three distinct eigenvalues $\lambda_0 = r, \lambda_1, \lambda_2$
  (also, $e = r + \lambda_1\lambda_2 + \lambda_1 + \lambda_2$, $d = r + \lambda_1\lambda_2$).
- The parameters satisfy $r(r - e - 1) = d(v - r - 1)$.
- The adjacency matrix A satisfies (J is the all 1 matrix)

$$A^2 = (d - e)A + (r - e)I + eJ.$$

- Bernasconi-Codenotti correspondence: Bent functions exactly correspond to strongly regular graphs with $e = d$.

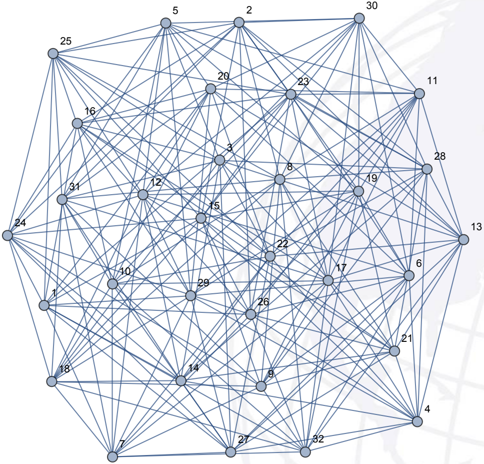
 P.J. Cameron: "*Strongly regular graphs lie on the cusp between highly structured and unstructured. For example, there is a unique srg with parameters* $(36, 10, 4, 2)$*, but there are* 32548 *non-isomorphic srg with parameters* $(36, 15, 6, 6)$*. In light of this, it will be difficult to develop a theory of random strongly regular graphs!*"

Plateaued functions and their Cayley graphs

- $f \in \mathcal{GB}_n^{2^k}$ is called *s-plateaued* if $|\mathcal{H}_f(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{F}_2^n$.
- For $k = 1$: $s = 0$ (n even), f is bent; if $s = 1$ (n odd), or $s = 2$ (n even), we call f semibent.
- Advantages: they can be balanced and highly nonlinear with no linear structures.
- In general, the spectrum of the Cayley graph of an s-plateaued $f : \mathbb{F}_2^n \to \mathbb{F}_2$ will be 4-valued (so, not srg!): if the WH transform of f takes values in $\{0, \pm 2^{\frac{n+s}{2}}\}$, then the Fourier transform of f takes values in $\{wt(f), 0, \pm 2^{\frac{n+s}{2}-1}\}$;

Cayley graphs of plateaued Boolean functions: example

Cayley graph of the semibent
$f(\mathbf{x}) = x_1x_2 \oplus x_3x_4 \oplus x_1x_4x_5 \oplus x_2x_3x_5 \oplus x_3x_4x_5$



Cayley graphs of plateaued Boolean functions with $wt(f) = 2^{(n+s-2)/2}$

There is one case when we do obtain an srg:

Theorem (Riera–Solé–S. 2018)

If $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is s-plateaued and $wt(f) = 2^{(n+s-2)/2}$, then G_f (if connected) is the complete bipartite graph between $\mathrm{supp(f)}$ and $\overline{\mathrm{supp(f)}}$ (if disconnected, it is a union of complete bipartite graphs). Moreover, G_f is strongly regular with $(e, d) = \left(0, 2^{(n+s-2)/2}\right)$.

Strongly walk-regular graphs

- van Dam and Omidi: G is strongly ℓ-walk-regular of parameters $(\sigma_\ell, \mu_\ell, \nu_\ell)$ if there are $\sigma_\ell, \mu_\ell, \nu_\ell$ walks of length ℓ between every two adjacent, every two non-adjacent, and every two identical vertices, respectively.
- Every strongly regular graph of parameters (v, r, e, d) is a strongly 2-walk-regular graph with parameters (e, d, r).

Cayley graphs of plateaued Boolean functions with $wt(f) \neq 2^{(n+s-2)/2}$

Theorem (Riera–Solé–S. 2018)

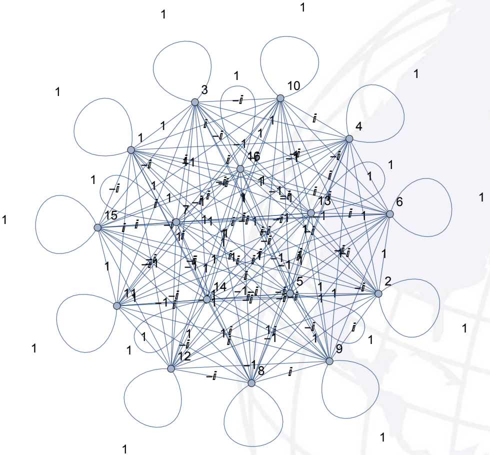
Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, and assume that G_f is connected and $r := wt(f) \neq 2^{(n+s-2)/2}$. Then, f is s-plateaued (with 4-valued spectra) if and only if G_f is strongly 3-walk-regular of parameters $(\sigma, \mu = \nu) = (2^{-n}r^3 + 2^{n+s-2} - 2^{s-2}r, 2^{-n}r^3 - 2^{s-2}r)$.

1. In fact, we showed that it is ℓ-walk regular for all odd ℓ, and found the parameters explicitly.

Go2OpenQues

Generalized Boolean and their Cayley graphs I

- For $f \in \mathcal{GB}_n^q$, *(gen.) Cayley graph* G_f: $\mathbb{V}_n$ vertices; $(\mathbf{u}, \mathbf{v})$ edge of (multiplicative) weight $\zeta^{f(\mathbf{u} \oplus \mathbf{v})}$ (additively $f(\mathbf{u} \oplus \mathbf{v})$).



Strong regularity for weighted graphs

- Let $X, Y \subseteq \mathbb{Z}_{2^k}$. A weighted regular $G = (V, E, w)$, $V \subseteq \mathbb{V}_n$, $w : E \to \mathbb{Z}_{2^k}$ is a (gen.) *$(X; Y)$-strongly regular* of parameters $(e_{X,Y}, d_{X,Y})$ iff # vertices $\mathbf{c}$ adjacent to both $\mathbf{a}, \mathbf{b}$, with $w(\mathbf{a}, \mathbf{c}), w(\mathbf{b}, \mathbf{c}) \in Y$, is exactly $e_{X,Y}$, if $w(\mathbf{a}, \mathbf{b}) \in X$, resp., $d_{X,Y}$, if $w(\mathbf{a}, \mathbf{b}) \in \bar{X}$.
- One can weaken the condition and define a $(X_1, X_2; Y)$-srg notion, where $X_1 \cap X_2 = \emptyset$, not necessarily a bisection; or even allowing a multi-section, and all of these variations can be fresh areas of research for graph theory experts.
- Note that this is a natural extension of the classical definition: for $q = 2$, and $X = \{1\}$, the classical strongly regular graph is then equivalent to an $(X; X)$-strongly regular graph.

Bernasconi-Codenotti strong regularity for gbents

Theorem (Riera–S.–Gangopadhyay 2018)

Let $f \in \mathcal{GB}_n^4$, n even. Then f is gbent iff G_f is $(X; \bar{X})$-strongly regular with $e_X = d_X$, for both $X = \{0, 1\}$, and $X = \{0, 3\}$.

Theorem (Riera–S.–Gangopadhyay 2018)

If $f = a_0 + 2a_1 + \cdots + 2^{k-1}a_{k-1}$, $k \geq 2$, $a_i \in \mathcal{B}_n$, is gbent (n even) then the associated weighted Cayley graph is $(X_{\mathbf{c}}^0; X_{\mathbf{c}}^1)$-strongly regular with explicit $X_{\mathbf{c}}^0, X_{\mathbf{c}}^1$.

Food for thought

- How do the Cayley graphs for generalized semibent/plateaued look like?
- Can one investigate other cryptographic properties of Boolean functions in terms of their Cayley graphs?
- Investigate the "APN property" for functions $: \mathbb{F}_2^n \to \mathbb{Z}_{2^n}$;
- Construct functions with small differential spectra;
- Look at other functions, like rotation symmetric in the generalized context and their differential properties;
- Define the nonlinearity in that environment;
- Define some of these properties (depending upon the Walsh-Hadamard transform with respect to other characters, and/or combine multiple characters.

Theorem (Pante Stanica: http://faculty/nps.edu/pstanica)

Thank you for your attention!

Proof.

None required, but questions are welcome! □