Journey into differential and graph theoretical properties of generalized Boolean functions

Pante Stănică

Naval Postgraduate School , Department of Applied Mathematics
Monterey, CA 93943–5216, USA; pstanica@nps.edu

In this talk we briefly look at various differential properties of generalized Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$, $k \geq 2$. We characterize linear structures for generalized Boolean functions in terms of their components, we describe the avalanche features of a generalized Boolean function in terms of differentials (mentioned below), and show that a partially generalized bent function (that is, functions with flat generalized Walsh-Hadamard spectrum) is plateaued. We display below an example of a result we will mention. We say that a generalized Boolean $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ satisfies the (*generalized*) *propagation criterion of order* ℓ ($1 \leq \ell \leq n$), denoted by $gPC(\ell)$, if and only if the autocorrelation $\sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x})-f(\mathbf{x}\oplus\mathbf{v})} = 0$, for all vectors $\mathbf{v} \in \mathbb{F}_2^n$ of weight $0 < wt(\mathbf{v}) \leq \ell$. We consequently show that a generalized Boolean $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is $gPC(\ell)$ if and only if

$$|A_0^{(\mathbf{0})}| = 2^n, |A_j^{(\mathbf{0})}| = 0, |A_j^{(\mathbf{w})}| = |A_{j+2^{k-1}}^{(\mathbf{w})}|, \text{ for } 0 \leq j \leq 2^{k-1} - 1, 1 \leq wt(\mathbf{w}) \leq \ell,$$

where $A_j^{(\mathbf{w})} = \{\mathbf{x} | f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x}) = j\}$.

We then define the (edge-weighted) Cayley graph associated to a generalized Boolean function, introduce a notion of strong regularity and give several of its properties. We show some connections between this concept and generalized bent functions, showing, for example the following result. Recall that a *q-Butson Hadamard matrix* (q-BH) of dimension d is a $d \times d$ matrix H with all entries q-th roots of unity such that $HH^* = dI_d$, where H^* is the conjugate transpose of H. When $q = 2$, q-BH matrices are called Hadamard matrices (where the entries are ± 1). We show that a generalized Boolean f is gbent if and only if the adjacency matrix A_f of the (multiplicative) edge-weighted Cayley graph associated to f is a q-Butson Hadamard matrix. Further, we find a complete characterization of quartic generalized bent functions in terms of the strong regularity of their associated Cayley graph.

If time permits, going back to classical Boolean functions, we characterize plateaued Boolean functions in terms of the associated Cayley graphs, extending Bernasconi-Codenotti correspondence between strongly regular graphs and bent functions.