Boolean Functions and their Applications, Selmer Center, University of Bergen, Norway; July 3–8, 2017

(Generalized) Boolean functions: invariance under some groups of transformations and differential properties

Pantelimon (Pante) Stănică
(Some joint work done with T. Martinsen, W. Meidl, A. Pott)

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

Estimated success of brute force attacks for various key sizes

- 56 bits – 1 million-keys/sec (desktop PC) – 2,283 years
- 56 bits – 1 billion-keys/sec (medium corporate) – 2.3 years
- 56 bits – 100 billion-keys/sec (nations) – 8 days
- 128 bits – 1 bilion-keys/sec (medium corporate) – 10^{22} yrs
- 128 bits – 10^{18} keys/sec (large corp.) – $10,783$ billion yrs
- 128 bits – 10^{32} keys/sec (nations; quantum) – 108 million yrs
- 192 bits – 10^{9} keys/sec (medium corp.) – $2 \cdot 10^{41}$ years
- 192 bits – 10^{18} keys/sec (large corp.) – $2 \cdot 10^{32}$ years
- 192 bits – 10^{23} keys/sec (nations; quantum) – $2 \cdot 10^{27}$ yrs
- 256 bits – 10^{23} keys/sec (nations; quantum) – $3.7 \cdot 10^{46}$ yrs
- 256 bits – 10^{32} keys/sec (nations; quantum) – $3.7 \cdot 10^{37}$ yrs

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

- Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$
- *Generalized Boolean function* $f : \mathbb{V}_n \to \mathbb{Z}_q$ $(q \geq 2)$; its set $\mathcal{GB}_n^q$; when $q = 2$, $\mathcal{B}_n$; $\mathbb{Z}_q$ is the ring of integers modulo q.
- If $2^{k-1} < q \leq 2^k$, for any $f \in \mathcal{GB}_n^q$ we associate a unique sequence of Boolean fcts. $a_i \in \mathcal{B}_n$ $(0 \leq i \leq k-1)$ s.t.

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x}), \forall \mathbf{x} \in \mathbb{V}_n.$$

- For $f : \mathbb{V}_n \to \mathbb{Z}_q$ in $\mathcal{GB}_n^q$ we define the *generalized Walsh-Hadamard transform* to be the complex valued function

$$\mathcal{H}_f^{(q)}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_q^{f(\mathbf{x})} (-1)^{\langle \mathbf{u}, \mathbf{x} \rangle},$$

where $\zeta_q = e^{\frac{2\pi i}{q}}$ and $\langle \mathbf{u}, \mathbf{x} \rangle$ denotes a (nondegenerate) inner product on $\mathbb{V}_n$ (like $\mathbf{u} \cdot \mathbf{x}$ on $\mathbb{F}_2^n$, or $\mathrm{Tr}(ux)$ on $\mathbb{F}_{2^n}$);

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

- For $q = 2$, we obtain the usual *Walsh-Hadamard transform*

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x})}(-1)^{\langle \mathbf{u}, \mathbf{x} \rangle}.$$

- A function $f : \mathbb{V}_n \to \mathbb{Z}_q$ is called *generalized bent* (*gbent*) if $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$.
- It generalizes *bents* f for which $|\mathcal{W}_f(\mathbf{u})| = 2^{n/2}$, $\forall \mathbf{u} \in \mathbb{V}_n$; equivalently, $N_f = 2^{n-1} \pm 2^{\frac{n}{2}-1}$ (distance from the set of all affine functions). These only exists for even n.

Counting bents I

- Bents are hard to construct and/or count: $(2^{n/2})!\, 2^{2^{n/2}} \le \#\,\text{bent} \le 2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$ or the more complicated Carlet-Klapper (2002) bound
- Agievich (bent rectangles, '07); Climent et al. ('08,'14) iterative constructions; better bounds for $n = 12, 14$ but become worse for n larger;
- Natalia (Tokareva) "hypothesizes" that the lower bound might be: $2^{2^{n-2}+\frac{1}{4}\binom{n}{n/2}}$, or perhaps asymptotically,

$$\#\,\text{bent} \sim 2^{2^{n-c}+d\binom{n}{n/2}},$$

for some constants c, d, with $1 \le c \le 2$.

Counting bents II

n	lower bound	# bent	upper bound	# Boolean
2	8	8	8	16
4	384	896	2,048	65,536
6	$2^{23.3}$	$2^{32.3}$	2^{38}	2^{64}
8	$2^{95.6}$	$2^{106.291}$	$2^{129.2}$	2^{256}
10	$2^{262.16}$	?	2^{612}	2^{1024}

- Preneel (1990), Meng et al. (2006): $B_6 = 5425430528$
- Langevin et al. (Dec. 2007):
  $B_8 = 99270589265934370305785861242880 \sim 2^{106.291}$

Applications of (generalized) Boolean functions

- S-Boxes for block ciphers. e.g. DES, AES
- ’Combiners’ or ’filters’ for Linear Feedback Shift Registers (LFSRs) based stream ciphers: the ’Grain’ family of ciphers (eSTREAM project in Europe), Bluetooth E0, E1, etc.
- Coding theory; e.g. Reed-Muller code
- Spread spectrum communication; e.g., 4G-CDMA=3G-CDMA+OFDM; MC-CDMA=OFDM+CDMA, etc.
- In MC-CDMA systems, the symbol is spread by a user specific spreading sequence, and converted into a parallel data stream, which is then transmitted over multiple carriers.

Peak-to-Power Ratio – System Model I

- Let $n = 2^m$ and H_n be the canonical Walsh-Hadamard matrix of dimension 2^n; $\omega = \exp(2\pi\imath/2^h)$ be a primitive 2^h-th root of unity in $\mathbb{C}$, $h \in \mathbb{Z}^+$;
- Given a word $c = (c_1, \ldots, c_n)$, $c_i \in \mathbb{Z}_{2^h}$, the transmitted MC-CDMA signal can be modeled as

$$S_c(t) = \sum_{j=1}^{n-1} \omega^{c_j} (H_n)_{j,t}, 0 \le t < n,$$

(that is, c_j is used to modulate the j-th row of H_n, and the transmitted signal is the sum of these modulated sequences).

Peak-to-Power Ratio – System Model II

- The PAPR (peak-to-average-power ratio) of a codeword c (and code C) is defined by

$$PAPR(c) = \frac{1}{n} \max_{0 \le t < n} |S_c(t)|^2; \quad PAPR(C) = \max_{c \in C} PAPR(c).$$

The transmit signals in an orthogonal frequency-division multiplexing (OFDM) system can have high peak values in the time domain since many subcarrier components are added via an inverse fast Fourier transformation (IFFT) operation. As a result, OFDM systems are known to have a high peak-to-average power ratio (PAPR) when compared to single-carrier systems. In fact, the high PAPR is one of the most detrimental aspects in an OFDM system as it decreases the signal-to-quantization noise ratio (SQNR) of the analog-digital convertor (ADC) and digital-analog convertor (DAC) while degrading the efficiency of the power amplifier in the transmitter. As a side note, the PAPR problem is more of a concern in the uplink since the efficiency of the power amplifier is critical due to the limited battery power in a mobile terminal.

GOOGLE (Nutaq)

Peak-to-Power Ratio – System Model III

- A major problem to overcome: minimize peak-to-power ratio (PAPR);

Theorem (Schmidt (2009))

Let $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^h}$ be a generalized Boolean function. Then,

$$PAPR(c) = \frac{1}{2^n} \max_{\mathbf{u} \in \mathbb{Z}_2^n} |\mathcal{H}_f^{(2^h)}(u)|^2.$$

In particular, the PAPR of f is 1 if and only if f is gbent.

Existence Results: from $\mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ (the set $\mathcal{GB}_n^{2^k}$)

- Subsets of {S., Gangopadhyay, Martinsen, Singh, Meidl, Mesnager, Pott, Hodžić, Pasalic, Tang, Xiang, Qi, Feng}.: analyzed and constructed large classes of generalized bents; we now have a complete characterization of gbents in terms of their components.

Theorem (2016)

Let $f : \mathbb{F}_{2^n} \to \mathbb{Z}_{2^k}$, n even. Then f is a gbent function given as $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$ if and only if, for each $\mathbf{c} \in \mathbb{F}_2^{k-1}$, the Boolean function $f_{\mathbf{c}}$ defined as

$$f_{\mathbf{c}}(x) = c_0 a_0(\mathbf{x}) \oplus c_1 a_1(x) \oplus \cdots \oplus c_{k-2} a_{k-2}(x) \oplus a_{k-1}(x)$$

is a bent function, such that $\mathcal{W}_{f_{\mathbf{c}}}(a) = (-1)^{\mathbf{c}\cdot g(a)+s(a)} 2^{\frac{n}{2}}$, for some $g : \mathbb{F}_{2^n} \to \mathbb{Z}_{2^{k-1}}$, $s : \mathbb{F}_{2^n} \to \mathbb{F}_2$.

Differential properties of generalized Boolean functions I

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

Theorem (2017)

Let $f \in \mathcal{GB}_n^{2^k}$. Then a vector $\mathbf{u}$ is a linear structure for f iff $\zeta^{f(\mathbf{u})-f(\mathbf{0})} = (-1)^{\mathbf{u}\cdot\mathbf{w}}$, for all $\mathbf{w} \in S_f$. As a consequence, if $\mathbf{u}$ is a linear structure for f, then $f(\mathbf{u}) - f(\mathbf{0}) \in \{0, 2^{k-1}\}$.

Differential properties of generalized Boolean functions II

- **Corollary:** *Let $f \in \mathcal{GB}_n^{2^k}$. If $\mathbf{u}$ is a linear structure for f, then either $S_f \subseteq \mathbf{u}^\perp$, or $S_f \subseteq \overline{\mathbf{u}^\perp}$ (the set complement of $\mathbf{u}^\perp$).*

Theorem (2017)

Let $f \in \mathcal{GB}_n^{2^k}$, $k \geq 2$, be given by $f(\mathbf{x}) = \sum_{i=0}^{k-1} 2^i a_i(\mathbf{x})$, $a_i \in \mathcal{B}_n$. Then $\mathbf{u} \in \mathbb{V}_n$ is a linear structure for f iff $\mathbf{u}$ is a linear structure for a_i, $i \geq 0$, such that $a_i(\mathbf{u}) = a_i(\mathbf{0}), 0 \leq i < k-1$.

Differential properties of generalized Boolean functions III

- Using the method of Lechner ('71) and Lai ('95) one can simplify the ANF of a function admitting linear structures.

Theorem (2017)

Let $f \in \mathcal{GB}_n^{2^k}$ and $1 \leq \dim LS_{2^k}(f) = r$. Then, $\exists$ an invertible $n \times n$ matrix A such that

$$f((x_1, \ldots, x_n) \cdot A) = \sum_{i=1}^{r} \alpha_i x_i + g(x_{r+1}, \ldots, x_n),$$

where $\alpha_i \in \mathbb{Z}_{2^k}$ and $g \in \mathcal{GB}_{n-r}^{2^k}$ has no linear structures.

Differential properties of generalized Boolean functions IV

- We say that $f \in \mathcal{GB}_n^{2^k}$ satisfies the (generalized) *strict avalanche criterion* if the autocorrelation $\mathcal{C}_f(\mathbf{e}) = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta^{f(\mathbf{x})-f(\mathbf{x}\oplus\mathbf{e})} = 0$, for all $\mathbf{e}$ of weight 1.

Theorem (2017)

Let $f \in \mathcal{GB}_n^{2^k}$, and $A_j^{(\mathbf{w})} = \{\mathbf{x} | f(\mathbf{x}\oplus\mathbf{w}) - f(\mathbf{x}) = j\}$. Then f satisfies the SAC iff $|A_j^{(\mathbf{e})}| = |A_{j+2^{k-1}}^{(\mathbf{e})}|$, for all $0 \le j \le 2^{k-1}-1$, $wt(\mathbf{e}) = 1$. Also, f is gbent if and only if $|A_0^{(\mathbf{0})}| = 2^n, |A_j^{(\mathbf{0})}| = 0, |A_j^{(\mathbf{w})}| = |A_{j+2^{k-1}}^{(\mathbf{w})}|$, $0 \le j \le 2^{k-1}-1, \mathbf{w} \ne 0$.

Correlation Immune Functions I

- A generalized Boolean function $f \in \mathcal{GB}_n^q$ is said to be *correlation immune of order* t, $1 \leq t \leq n$ if for any fixed subset of t variables the probability that, given the value of $f(\mathbf{x})$, the t variables have any fixed set of values, is 2^{-t}.
- An $m \times n$ array $OA(m, n, s, t)$ with entries from a set of s elements is called an *orthogonal array of size m with n constraints, s levels, strength t, and index r*, if any set of t columns of the array contain all s^t possible row vectors exactly r times.

Correlation Immune Functions II

- As expected, there's a connection with orthogonal arrays;

Theorem (2017)

Every order t correlation immune generalized Boolean function, $f \in \mathcal{GB}_n^q$, "involves" a partition of $\mathbb{V}_n$, consisting of q binary orthogonal arrays, each of strength t.

- Nice connections and constructions of SAC, CI, dependent upon labeling of the hypercube are in (my student) Thor Martinsen's PhD thesis.

Correlation Immune Functions III

Table: A CI(1) Generalized Boolean Function, $f \in \mathcal{GB}_4^4$

$\mathbb{F}_2^4$	f
0000	0
0001	3
0010	2
0011	1
0100	1
0101	2
0110	3
0111	0
1000	2
1001	1
1010	0
1011	3
1100	3
1101	0
1110	1
1111	2

Trade-offs for generalized Boolean functions I

- Are there symmetric and gbent generalized Boolean functions ($k > 1$)?
- **Theorem (2017)**: NO! (proof based upon Savicky's symmetric bents and the recent work on gbents)
  ****
- What about balanced and symmetric generalized Boolean functions ($k > 1$)?
- **Theorem (2017)**: NO! (hard to show – dio. eq.)
- Recall $X(d, n) = \sum_{i_1 < i_2 < \cdots < i_d} x_{i_1} x_{i_2} \cdots x_{i_d}$:

Theorem (Cusick-Li-S., 2009)

If t, ℓ are positive integers, then $X(2^t, 2^{t+1}\ell - 1)$ is balanced.

Trade-offs for generalized Boolean functions II

- We conjectured that these are the only balanced elementary symmetric (many cases covered, but still open);
- (Cusick-Li-S. 2009):
  - If $d = 2^t + 1$, $n = 2^{t+1}\ell$, then $wt(X(2^t + 1, 2^{t+1}\ell)) = 2^{n-2}$;
  - If $d = 2^t$, $X(d, n)$ is balanced iff $n = 2^{t+1}\ell - 1$, $t, \ell \in \mathbb{Z}^+$;
  - If $d = 2^{t+1}\ell + r - 1$, $t, \ell > 0$, $0 \le r \le 2^{t+1}$, $2^t < d \le 2^{t+1} - 2$ even, then $X(d, n)$ is not balanced;
- (Ou–Zhao 2012): Let $d = 2^{t+w}(2^{s+1} - 1), n = 2^{t+w+1}(2^{s+1} - 1) + 2^t q + m$, $m \in \{-1, 0\}$. Under some assumption on t, w, s, q, then $X(d, n)$ is not balanced.

Trade-offs for generalized Boolean functions III

- (Castro-Medina 2011) & (Guo-Gao-Zhao 2015): Conjecture 1 is true if n is large enough (dependent upon the degree), $n > -2\left(\log_2 \cos(\pi/2^r)\right)^{-1}$, where $2^{r-1} \le d < 2^r$. In particular, if d is not a power of 2, $X(d,n)$ is not balanced for large n.
- (Su-Tang-Pott 2013): If $d = 2^t$, Conjecture 2 holds in most cases, that is, $wt(X(d,n)) < 2^{n-1}$;
- (Gao-Liu- Zhang 2015): If $n = 2^{t+1}\ell - 1$, ℓ odd, $2^{t+1} \not| d$, $X(d,n)$ balanced iff $d = 2^k$, $1 \le k \le t$;
- (Castro-Gonzales-Medina 2015): More open cases are covered where Conjecture 1 holds.

Bisecting binomial coefficients I

- The existence of balanced elementary symmetric polynomials is related to the problem of bisecting binomial coefficients, that is, *solutions of*

$$\sum_{i=0}^{n} x_i \binom{n}{i} = 0, \quad x_i \in \{-1, 1\}. \tag{1}$$

- *Trivial Solutions*: Obviously, if n is even, then $\pm(1, -1, \ldots, -1, 1)$ are two solutions of (1). If n is odd, then $(\delta_0, \ldots, \delta_{\frac{n-1}{2}}, -\delta_{\frac{n-1}{2}-1}, \ldots, -\delta_0)$ are $2^{\frac{n+1}{2}}$ solutions of (1).

Research Question (Open for the past 25 years)

Find all nontrivial solutions of (1).

Bisecting binomial coefficients II

- There are sporadic cases when non-trivial solutions do appear: e.g., if $n \equiv 2 \pmod 6$, since $\binom{n}{(n+1)/3} = \binom{n}{(n+1)/3-1} + \binom{n}{n-((n+1)/3-1)}$, nontrivial solutions always appear.
- Apart from this, all that was known about the bisection of binomial coefficients was mostly computational.
- (Mitchell, 1990): found the nontrivial solutions for $n = 8, 13$;
- (Cusick & Li, 2005): found all solutions of (1) when $n \leq 28$; nontrivial solutions exist iff $n = 8, 13, 14, 20, 24, 26$.
- (Ionascu-Martinsen-S., 2017): found all nontrivial solutions for $n \leq 51$.

Our approach on the problem I

- The binomial coefficients bisection can be thought of as a subset sum problem. The view we take is the following: a binomial coefficients bisection $\sum_{i\in I}\binom{n}{i} = \sum_{i\in \bar{I}}\binom{n}{i}$ will generate a solution to the Boolean equation

  $$\sum_{i=0}^{n} x_i \binom{n}{i} = 2^{n-1}, x_i \in \{0,1\}$$

  by taking $x_i = 1$ for $i \in I$ and $x_i = 0$, for $i \in \bar{I}$. Certainly, the reciprocal is true, as well, and so, we have an equivalence between these two problems.

Our approach on the problem II

- In general, given a set of positive integers $A = \{a_1, \ldots, a_N\}$ and $b \leq \frac{1}{2}\sum_i a_i$, $b \in \mathbb{N}$, one investigates the Boolean equation
$$\sum_{i=1}^{N} x_i a_i = b,\ x_i \in \{0, 1\}.$$
- The advantage of our approach is that these equations were studied before by analytical number theory methods and much (well, some) is known.
- In general, these problem are well known to be NP-complete [Garey–Johnson, 1979] and have many applications in cryptography, such as the Merkle-Hellman cryptosystem (1978).

Our approach on the problem III

- The density of $\mathcal{S} = \{a_1, \ldots, a_N\}$ is $d(\mathcal{S}) = \dfrac{N}{\log_2\left(\max\limits_{1\le i\le N} a_i\right)}$;

  in terms of knapsack cryptosystems,

  $d(\mathcal{S}) = \dfrac{\text{bit size of the plaintext}}{\text{average bit size of the ciphertext}}$

- For $\mathbf{P}_n = \left\{ \binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n} \right\}$, using $\frac{4^{\lfloor n/2 \rfloor}}{2\lfloor n/2\rfloor+1} \le \binom{n}{\lfloor n/2 \rfloor} \le 4^{\lfloor n/2 \rfloor}$, the density becomes

$$\frac{n+1}{2\lfloor n/2\rfloor - \log_2(2\lfloor n/2\rfloor + 1)} \le d(\mathbf{P}_n) = \frac{n+1}{\log_2(\max_i \binom{n}{i})} = \frac{n+1}{\log_2 \binom{n}{\lfloor n/2\rfloor}} \le \frac{n+1}{2\lfloor n/2\rfloor},$$

and so,

$$d(\mathbf{P}_n) \to 1, \text{ as } n \to \infty.$$

Our approach on the problem IV

- Lagarias and Odlyzko (1985) showed that almost all the subset sum problem with density $d < 0.6463\ldots$ can be solved in polynomial time with a single call to an oracle that can find (in polynomial time with high probability) the shortest vector in a special lattice. Coster et al. (1992) improved the bound to $d < 0.9408\ldots$.
- Since for binomial coefficients, the density is $d = 1$ (as $n \to \infty$), none of these methods are applicable.

The underlying method I

- We recall here the following important result of Freiman (1980) (see also [Buzytsky (1982), Chaimovich, Freiman, Galil (1989)]).

Theorem (Freiman)

Let $A = \{a_1, a_2, \ldots, a_N\}$ and $b \leq \frac{1}{2}\sum_{i=1}^{N} a_i$. The number of Boolean solutions for the equation

$$\sum_{i=1}^{N} a_i x_i = b, \;\; x_i \in \{0, 1\}$$

is precisely $\displaystyle\int_0^1 e^{-2\pi i x b} \prod_{j=1}^{N} \left(1 + e^{2\pi i x a_j}\right) d\,x.$

The underlying method II

- Applying Freiman's paradigm to the bisection of bin. coeff.:

Theorem (Ionascu-Martinsen-S., 2017)

The number of binomial coefficients bisections for fixed n is exactly

$$J_n = \int_0^1 e^{-2^n \pi i x} \prod_{j=0}^{n} \left(1 + e^{2\pi i x \binom{n}{j}}\right) d\,x = 2^{n+1} \int_0^1 \prod_{j=0}^{n} \cos\left(\pi x \binom{n}{j}\right) d\,x.$$

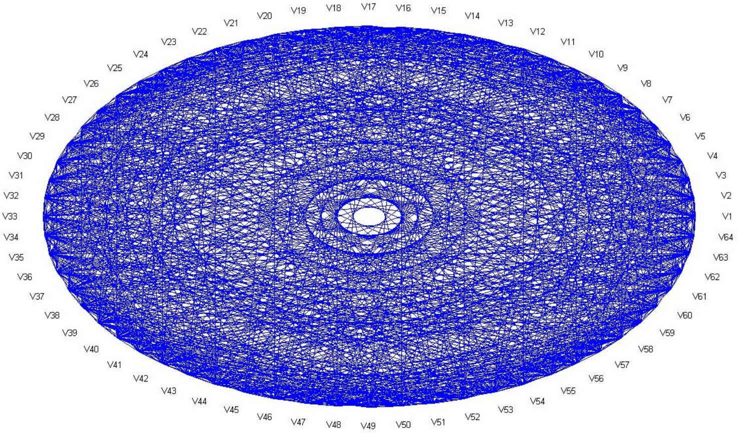
- We constructed infinite families with nontrivial, as well as infinite families with only trivial bisections.
- As a by-product, we got for free two conjectures of Cusick et al. ('05), so there are only four symmetric SAC(k) functions for infinitely many n.

Go2Graphs Go2Tks

Visualizing Boolean functions

- Can one visualize Boolean functions?
- Yes, in several ways, but it becomes very hard to obtain results just based upon graph theoretical tools.
- Nagy graphs, Cayley graphs, etc.
- E.g.: (undirected) Cayley graph – vertices are points of $\mathbb{F}_2^n$ and two points $\mathbf{x}, \mathbf{y}$ are connected by an edge iff $f(\mathbf{x} \oplus \mathbf{y}) = 1$.

Cayley graph of first row of S-box 1 of DES



Go2Tks

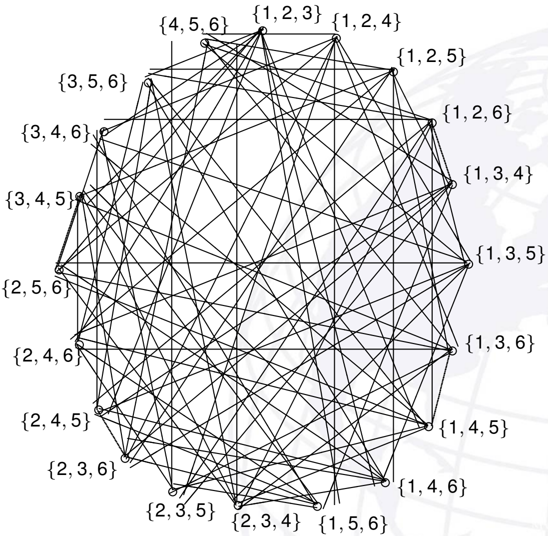
Further Restrictions: invariance under a group of transformations

- On $\mathbb{F}_2^6$, there are 2^{20} cubic homogeneous B.f.
- Among these, $\exists$ 30 homogeneous bent B.f. equivalent to Rothaus ('76): $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$
- Qu-Seberry-Pieprzyk (2000): *There are* $> 30^n\binom{6n}{6}$ *homogeneous bent B.f. on* $\mathbb{F}_2^{6n}$.
- Charnes-Rötteler-Beth (2002):
  The bent functions found by Qu et al. ('00) arise as invariants under the action of the symmetric group on four letters;

Definition (Nagy Graph)

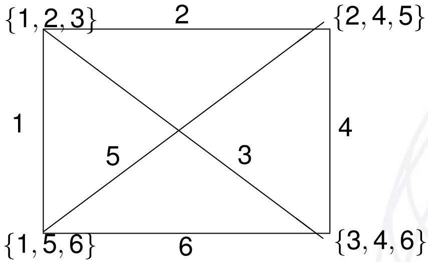
$\Gamma_{(n,k)}$: vertices – the $\binom{n}{k}$ unordered subsets of size k of $\{1,\ldots,n\}$; vertices are joined by an edge whenever the corresponding k-sets intersect in a subset of size one.

Nagy graph $\Gamma_{(6,3)}$



Cliques and Homogeneous Bent Functions

- A *clique* in an undirected graph Γ is a complete subgraph (maximal: not contained in a bigger one); *the clique problem*) is NP-complete.



ptmmn.

Theorem (Charnes-Rötteler-Beth (2002))

The thirty homogeneous bent functions in six variables listed by Qu et al. are in one to one correspondence with the complements of the 30 *(maximal) cliques of* $\Gamma_{(6,3)}$.

Open questions

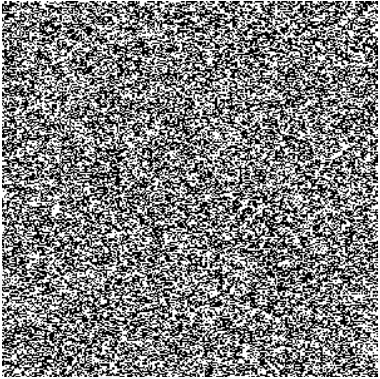
- It is unknown whether there are quartic/quintic/etc. homogeneous bent functions.
- I propose to look at the complements of the maximal cliques of the Nagy graph $\Gamma_{(10,4)}, \Gamma_{(12,4)}$.
- Do the same for $\Gamma_{(12,5)}, \Gamma_{(14,5)}$.

Research Question

Can one find efficiently a (all) clique(s) in $\Gamma_{(2n,k)}$, $k < n$?

- Not a trivial matter, I believe: for instance, $\Gamma_{(10,4)}$ has 210 vertices; $\Gamma_{(12,5)}$ has 792 vertices;

Having some fun: using a gen. Boolean as a combiner



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

Thank you for your attention!

Proof.

None required! $\square$