Construction of Boolean functions with lots of flat spectra

Gaofei Wu
Joint work with Matthew Parker and Constanza Riera

Selmer Center
Department of Informatics
University of Bergen, Norway

September 6, 2014
BFA Workshop, Rosendal, Norway

Outline

Each mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called an *n*-variable Boolean function. Any *n*-variable Boolean function $f(x)$ can be generally represented by its algebraic normal form (ANF):

$$f(x_0, x_1 \cdots, x_{n-1}) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=0}^{n-1} x_i^{u_i}),$$

where $\lambda_u \in \mathbb{F}_2, u = (u_0, u_1, \cdots, u_{n-1}) \in \mathbb{F}_2^n$.

f is *bent*: it has a flat spectrum w.r.t. $H^{\otimes n}$, where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Walsh-Hadamard kernel, and $\bigotimes$ is the tensor product. (equiv. def.: $f(x) + f(x+a)$ is balanced for all nonzero $a \in \mathbb{F}_2^n$.)

Riera and Parker [1] introduced some generalized bent criteria for Boolean functions. They considered Boolean functions that have flat spectrum with respect to the $\{I, H, N\}^n$ set or subsets thereof, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$.

- f is bent$_4$: flat w.r.t. at least one $U \in \{H, N\}^n = \{\bigotimes_{i=0}^{n-1} U_i \mid U_i \in \{H, N\}\}$. (equiv. def.: $f(x) + f(x+a) + a \cdot (s * x)$ is balanced for **all** nonzero $a \in \mathbb{F}_2^n$ for **some** $s \in \mathbb{F}_2^n$, $a * x = (a_0x_0, \cdots, a_{n-1}x_{n-1})$)
- f is *negabent*: flat w.r.t $N^{\bigotimes n}$. (equiv. def.: $f(x) + f(x+a) + a \cdot x$ is balanced for all nonzero $a \in \mathbb{F}_2^n$.)

[1] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions", IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4142-4159, Sep. 2006.

Riera and Parker [1] introduced some generalized bent criteria for Boolean functions. They considered Boolean functions that have flat spectrum with respect to the $\{I, H, N\}^n$ set or subsets thereof, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$.

- f is bent$_4$: flat w.r.t. at least one $U \in \{H, N\}^n = \{\bigotimes_{i=0}^{n-1} U_i \mid U_i \in \{H, N\}\}$. (equiv. def.: $f(x) + f(x+a) + a \cdot (s * x)$ is balanced for **all** nonzero $a \in \mathbb{F}_2^n$ for **some** $s \in \mathbb{F}_2^n$, $a * x = (a_0 x_0, \cdots, a_{n-1} x_{n-1})$)
- f is *negabent*: flat w.r.t $N^{\bigotimes n}$. (equiv. def.: $f(x) + f(x+a) + a \cdot x$ is balanced for all nonzero $a \in \mathbb{F}_2^n$.)

[1] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions", IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4142-4159, Sep. 2006.

Riera and Parker [1] introduced some generalized bent criteria for Boolean functions. They considered Boolean functions that have flat spectrum with respect to the $\{I, H, N\}^n$ set or subsets thereof, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$.

- f is bent$_4$: flat w.r.t. at least one $U \in \{H, N\}^n = \{\bigotimes_{i=0}^{n-1} U_i \mid U_i \in \{H, N\}\}$. (equiv. def.: $f(x) + f(x+a) + a \cdot (s * x)$ is balanced for **all** nonzero $a \in \mathbb{F}_2^n$ for **some** $s \in \mathbb{F}_2^n$, $a * x = (a_0 x_0, \cdots, a_{n-1} x_{n-1})$)
- f is *negabent*: flat w.r.t $N^{\bigotimes n}$. (equiv. def.: $f(x) + f(x+a) + a \cdot x$ is balanced for all nonzero $a \in \mathbb{F}_2^n$.)

[1] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions", IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4142-4159, Sep. 2006.

Interesting Problems

- Construct *bent-negabent* functions (Boolean functions which are both bent and negabent, two flat spectra) with optimal degree;
- Construct Boolean functions which have lots of flat spectra w.r.t. $\{I, H, N\}^n$ or subsets thereof.

Interesting Problems

- Construct *bent-negabent* functions (Boolean functions which are both bent and negabent, two flat spectra) with optimal degree;
- Construct Boolean functions which have lots of flat spectra w.r.t. $\{I, H, N\}^n$ or subsets thereof.

Interesting Problems

- Construct *bent-negabent* functions (Boolean functions which are both bent and negabent, two flat spectra) with optimal degree;
- Construct Boolean functions which have lots of flat spectra w.r.t. $\{I, H, N\}^n$ or subsets thereof.

State of the art (1)

- In 2007, Parker and Pott [1] showed that quadratic bent-negabent functions exist for all even m, and gave a powerful connection between bent and negabent functions.
- In 2008, Schmidt, Parker, and Pott [2] presented a construction of bent-negabent functions in $2mn$ variables $(m > 1)$ and of degree at most n.
- In 2012, Stănică et al. [3] proved that the maximum degree of an n variables negabent functions is $\lceil \frac{n}{2} \rceil$. They also gave a construction of bent-negabent functions of degree $\frac{n}{4} + 1$ by using complete permutation polynomials.

[1] M. G. Parker and A. Pott, "On Boolean functions which are bent and negabent," Sequences, Subsequences, Consequences, Lecture Notes Comput. Sci., vol. 4893, pp. 9-23, 2007.
[2] K.-U. Schmidt, M. G. Parker, and A. Pott, "Negabent functions in the Maiorana-McFarland class," in Proc. Sequ. Appl., 2008, vol. LNCS 5203, pp. 390-402.
[3] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, and S. Maitra, "Investigations on bent and negabent functions via the nega-Hadamard transform," IEEE Trans. Inf. Theory, vol. 58, no. 6, pp. 4064-4072, 2012.

State of the art (1)

- In 2007, Parker and Pott [1] showed that quadratic bent-negabent functions exist for all even m, and gave a powerful connection between bent and negabent functions.
- In 2008, Schmidt, Parker, and Pott [2] presented a construction of bent-negabent functions in $2mn$ variables $(m > 1)$ and of degree at most n.
- In 2012, Stănică et al. [3] proved that the maximum degree of an n variables negabent functions is $\lceil \frac{n}{2} \rceil$. They also gave a construction of bent-negabent functions of degree $\frac{n}{4} + 1$ by using complete permutation polynomials.

[1] M. G. Parker and A. Pott, "On Boolean functions which are bent and negabent," Sequences, Subsequences, Consequences, Lecture Notes Comput. Sci., vol. 4893, pp. 9-23, 2007.
[2] K.-U. Schmidt, M. G. Parker, and A. Pott, "Negabent functions in the Maiorana-McFarland class," in Proc. Sequ. Appl., 2008, vol. LNCS 5203, pp. 390-402.
[3] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, and S. Maitra, "Investigations on bent and negabent functions via the nega-Hadamard transform," IEEE Trans. Inf. Theory, vol. 58, no. 6, pp. 4064-4072, 2012.

State of the art (1)

- In 2007, Parker and Pott [1] showed that quadratic bent-negabent functions exist for all even m, and gave a powerful connection between bent and negabent functions.
- In 2008, Schmidt, Parker, and Pott [2] presented a construction of bent-negabent functions in $2mn$ variables $(m > 1)$ and of degree at most n.
- In 2012, Stănică et al. [3] proved that the maximum degree of an n variables negabent functions is $\lceil \frac{n}{2} \rceil$. They also gave a construction of bent-negabent functions of degree $\frac{n}{4} + 1$ by using complete permutation polynomials.

[1] M. G. Parker and A. Pott, "On Boolean functions which are bent and negabent," Sequences, Subsequences, Consequences, Lecture Notes Comput. Sci., vol. 4893, pp. 9-23, 2007.
[2] K.-U. Schmidt, M. G. Parker, and A. Pott, "Negabent functions in the Maiorana-McFarland class," in Proc. Sequ. Appl., 2008, vol. LNCS 5203, pp. 390-402.
[3] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, and S. Maitra, "Investigations on bent and negabent functions via the nega-Hadamard transform," IEEE Trans. Inf. Theory, vol. 58, no. 6, pp. 4064-4072, 2012.

State of the art (1)

- In 2007, Parker and Pott [1] showed that quadratic bent-negabent functions exist for all even m, and gave a powerful connection between bent and negabent functions.
- In 2008, Schmidt, Parker, and Pott [2] presented a construction of bent-negabent functions in $2mn$ variables $(m > 1)$ and of degree at most n.
- In 2012, Stănică et al. [3] proved that the maximum degree of an n variables negabent functions is $\lceil \frac{n}{2} \rceil$. They also gave a construction of bent-negabent functions of degree $\frac{n}{4} + 1$ by using complete permutation polynomials.

[1] M. G. Parker and A. Pott, “On Boolean functions which are bent and negabent,” Sequences, Subsequences, Consequences, Lecture Notes Comput. Sci., vol. 4893, pp. 9-23, 2007.
[2] K.-U. Schmidt, M. G. Parker, and A. Pott, “Negabent functions in the Maiorana-McFarland class,” in Proc. Sequ. Appl., 2008, vol. LNCS 5203, pp. 390-402.
[3] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, and S. Maitra, “Investigations on bent and negabent functions via the nega-Hadamard transform,” IEEE Trans. Inf. Theory, vol. 58, no. 6, pp. 4064-4072, 2012.

State of the art (2)

- In 2013, Su, Pott, and Tang [1] gave sufficient and necessary conditions for a Boolean function to be negabent, and determined the nega spectrum distribution of negabent functions. They also presented a construction of bent-negabent functions in $2m$-variable of degree ranging from 2 to m.
- In 2013, Gangopadhyay, Pasalic, and Stănică [2] gave a relationship between bent, semibent, and $bent_4$ functions, and showed that the maximum possible degree of a $bent_4$ function of n-variable is $\lceil \frac{n}{2} \rceil$.
- In 2014, Sarkar [3] considered negabent functions over finite fields. They gave a link between bent and negabent functions via a quadratic function, and gave a construction for negabent functions with trace representation that have optimal degree.

[1] W. Su, A. Pott, X. Tang, "Characterization of Negabent Functions and Construction of Bent-Negabent Functions with Maximum Algebraic Degree", IEEE Trans. Inf. Theory 59(6) (2013) 3387-3395.
[2] S. Gangopadhyay, E. Pasalic, P. Stanica, "A Note on Generalized Bent Criteria for Boolean Functions, " IEEE Trans. Inf. Theory 59(5) (2013) 3233-3236.
[3] S. Sarkar, Some Results on Bent-Negabent Boolean Functions, arXiv: 1406.1036.

State of the art (2)

- In 2013, Su, Pott, and Tang [1] gave sufficient and necessary conditions for a Boolean function to be negabent, and determined the nega spectrum distribution of negabent functions. They also presented a construction of bent-negabent functions in $2m$-variable of degree ranging from 2 to m.
- In 2013, Gangopadhyay, Pasalic, and Stănică [2] gave a relationship between bent, semibent, and $bent_4$ functions, and showed that the maximum possible degree of a $bent_4$ function of n-variable is $\lceil \frac{n}{2} \rceil$.
- In 2014, Sarkar [3] considered negabent functions over finite fields. They gave a link between bent and negabent functions via a quadratic function, and gave a construction for negabent functions with trace representation that have optimal degree.

[1] W. Su, A. Pott, X. Tang, "Characterization of Negabent Functions and Construction of Bent-Negabent Functions with Maximum Algebraic Degree", IEEE Trans. Inf. Theory 59(6) (2013) 3387-3395.
[2] S. Gangopadhyay, E. Pasalic, P. Stanica, "A Note on Generalized Bent Criteria for Boolean Functions, " IEEE Trans. Inf. Theory 59(5) (2013) 3233-3236.
[3] S. Sarkar, Some Results on Bent-Negabent Boolean Functions, arXiv: 1406.1036.

State of the art (2)

- In 2013, Su, Pott, and Tang [1] gave sufficient and necessary conditions for a Boolean function to be negabent, and determined the nega spectrum distribution of negabent functions. They also presented a construction of bent-negabent functions in $2m$-variable of degree ranging from 2 to m.
- In 2013, Gangopadhyay, Pasalic, and Stănică [2] gave a relationship between bent, semibent, and $bent_4$ functions, and showed that the maximum possible degree of a $bent_4$ function of n-variable is $\lceil \frac{n}{2} \rceil$.
- In 2014, Sarkar [3] considered negabent functions over finite fields. They gave a link between bent and negabent functions via a quadratic function, and gave a construction for negabent functions with trace representation that have optimal degree.

[1] W. Su, A. Pott, X. Tang, "Characterization of Negabent Functions and Construction of Bent-Negabent Functions with Maximum Algebraic Degree", IEEE Trans. Inf. Theory 59(6) (2013) 3387-3395.
[2] S. Gangopadhyay, E. Pasalic, P. Stanica, "A Note on Generalized Bent Criteria for Boolean Functions, " IEEE Trans. Inf. Theory 59(5) (2013) 3233-3236.
[3] S. Sarkar, Some Results on Bent-Negabent Boolean Functions, arXiv: 1406.1036.

State of the art (2)

- In 2013, Su, Pott, and Tang [1] gave sufficient and necessary conditions for a Boolean function to be negabent, and determined the nega spectrum distribution of negabent functions. They also presented a construction of bent-negabent functions in $2m$-variable of degree ranging from 2 to m.
- In 2013, Gangopadhyay, Pasalic, and Stǎnicǎ [2] gave a relationship between bent, semibent, and $bent_4$ functions, and showed that the maximum possible degree of a $bent_4$ function of n-variable is $\lceil \frac{n}{2} \rceil$.
- In 2014, Sarkar [3] considered negabent functions over finite fields. They gave a link between bent and negabent functions via a quadratic function, and gave a construction for negabent functions with trace representation that have optimal degree.

[1] W. Su, A. Pott, X. Tang, "Characterization of Negabent Functions and Construction of Bent-Negabent Functions with Maximum Algebraic Degree", IEEE Trans. Inf. Theory 59(6) (2013) 3387-3395.
[2] S. Gangopadhyay, E. Pasalic, P. Stanica, "A Note on Generalized Bent Criteria for Boolean Functions, " IEEE Trans. Inf. Theory 59(5) (2013) 3233-3236.
[3] S. Sarkar, Some Results on Bent-Negabent Boolean Functions, arXiv: 1406.1036.

Our contributions

- Two constructions of Boolean functions which have two flat spectra with respect to $\{H, N\}^n$ are proposed. Some known results about bent-negabent functions can be seen as special cases of our results.
- Develop recursive formulae for the numbers of flat spectra of some structural quadratics.

Our contributions

- Two constructions of Boolean functions which have two flat spectra with respect to $\{H, N\}^n$ are proposed. Some known results about bent-negabent functions can be seen as special cases of our results.
- Develop recursive formulae for the numbers of flat spectra of some structural quadratics.

Our contributions

- Two constructions of Boolean functions which have two flat spectra with respect to $\{H, N\}^n$ are proposed. Some known results about bent-negabent functions can be seen as special cases of our results.
- Develop recursive formulae for the numbers of flat spectra of some structural quadratics.

Outline

Notations

- $\sigma = \bigoplus_{0 \le i < k \le n-1} x_i x_k$ is the clique function;
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, $S \subseteq \mathbb{Z}_n$, and $\sigma_S = \bigoplus_{i,k \in S, i<k} x_i x_k$.
- $\mathbf{x_{a,b}} = (x_a, x_{a+1}, \ldots, x_{b-1})$, for any integers $a < b$;
- $U_S = \bigotimes_{i=0}^{n-1} U_i$, where $U_i = N$ if $i \in S$, and $U_i = H$ otherwise.
- $GL(n, \mathbb{F}_2)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_2$, and $O(n, \mathbb{F}_2)$ is the orthogonal group of $n \times n$ binary matrices over $\mathbb{F}_2$, i.e., $O(n, \mathbb{F}_2) = \{E \in GL(n, \mathbb{F}_2) \mid EE^T = I\}$.

Notations

- $\sigma = \bigoplus_{0 \le i < k \le n-1} x_i x_k$ is the clique function;
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, $S \subseteq \mathbb{Z}_n$, and $\sigma_S = \bigoplus_{i,k \in S, i<k} x_i x_k$.
- $\mathbf{x_{a,b}} = (x_a, x_{a+1}, \ldots, x_{b-1})$, for any integers $a < b$;
- $U_S = \bigotimes_{i=0}^{n-1} U_i$, where $U_i = N$ if $i \in S$, and $U_i = H$ otherwise.
- $GL(n, \mathbb{F}_2)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_2$, and $O(n, \mathbb{F}_2)$ is the orthogonal group of $n \times n$ binary matrices over $\mathbb{F}_2$, i.e., $O(n, \mathbb{F}_2) = \{E \in GL(n, \mathbb{F}_2) \mid EE^T = I\}$.

Notations

- $\sigma = \bigoplus_{0 \le i < k \le n-1} x_i x_k$ is the clique function;
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, $S \subseteq \mathbb{Z}_n$, and $\sigma_S = \bigoplus_{i,k \in S, i<k} x_i x_k$.
- $\mathbf{x_{a,b}} = (x_a, x_{a+1}, \ldots, x_{b-1})$, for any integers $a < b$;
- $U_S = \bigotimes_{i=0}^{n-1} U_i$, where $U_i = N$ if $i \in S$, and $U_i = H$ otherwise.
- $GL(n, \mathbb{F}_2)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_2$, and $O(n, \mathbb{F}_2)$ is the orthogonal group of $n \times n$ binary matrices over $\mathbb{F}_2$, i.e., $O(n, \mathbb{F}_2) = \{E \in GL(n, \mathbb{F}_2) \mid EE^T = I\}$.

Notations

- $\sigma = \bigoplus_{0 \leq i < k \leq n-1} x_i x_k$ is the clique function;
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, $S \subseteq \mathbb{Z}_n$, and $\sigma_S = \bigoplus_{i,k \in S, i<k} x_i x_k$.
- $\mathbf{x_{a,b}} = (x_a, x_{a+1}, \ldots, x_{b-1})$, for any integers $a < b$;
- $U_S = \bigotimes_{i=0}^{n-1} U_i$, where $U_i = N$ if $i \in S$, and $U_i = H$ otherwise.
- $GL(n, \mathbb{F}_2)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_2$, and $O(n, \mathbb{F}_2)$ is the orthogonal group of $n \times n$ binary matrices over $\mathbb{F}_2$, i.e., $O(n, \mathbb{F}_2) = \{E \in GL(n, \mathbb{F}_2) \,|\, EE^T = I\}$.

Notations

- $\sigma = \bigoplus_{0 \leq i < k \leq n-1} x_i x_k$ is the clique function;
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, $S \subseteq \mathbb{Z}_n$, and $\sigma_S = \bigoplus_{i,k \in S, i<k} x_i x_k$.
- $\mathbf{x_{a,b}} = (x_a, x_{a+1}, \ldots, x_{b-1})$, for any integers $a < b$;
- $U_S = \bigotimes_{i=0}^{n-1} U_i$, where $U_i = N$ if $i \in S$, and $U_i = H$ otherwise.
- $GL(n, \mathbb{F}_2)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_2$, and $O(n, \mathbb{F}_2)$ is the orthogonal group of $n \times n$ binary matrices over $\mathbb{F}_2$, i.e., $O(n, \mathbb{F}_2) = \{E \in GL(n, \mathbb{F}_2) \mid EE^T = I\}$.

Notations

- $\sigma = \bigoplus_{0 \le i < k \le n-1} x_i x_k$ is the clique function;
- $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, $S \subseteq \mathbb{Z}_n$, and $\sigma_S = \bigoplus_{i,k \in S, i<k} x_i x_k$.
- $\mathbf{x_{a,b}} = (x_a, x_{a+1}, \ldots, x_{b-1})$, for any integers $a < b$;
- $U_S = \bigotimes_{i=0}^{n-1} U_i$, where $U_i = N$ if $i \in S$, and $U_i = H$ otherwise.
- $GL(n, \mathbb{F}_2)$ is the group of all invertible $n \times n$ matrices over $\mathbb{F}_2$, and $O(n, \mathbb{F}_2)$ is the orthogonal group of $n \times n$ binary matrices over $\mathbb{F}_2$, i.e., $O(n, \mathbb{F}_2) = \{E \in GL(n, \mathbb{F}_2) \,|\, EE^T = I\}$.

It is shown in [1] that for n even, $f + \sigma$ is bent if and only if f is negabent, and this had been extended in [2] to the following:

Lemma 1

For n even, $f \oplus \sigma_S$ is bent if and only if $U_S(-1)^f$ is flat.

[1] M. G. Parker and A. Pott, "On Boolean functions which are bent and negabent," Sequences, Subsequences, Consequences, Lecture Notes Comput. Sci., vol. 4893, pp. 9-23, 2007.
[2] S. Gangopadhyay, E. Pasalic, P. Stanica, "A Note on Generalized Bent Criteria for Boolean Functions, " IEEE Trans. Inf. Theory 59(5) (2013) 3233-3236.

Outline

1. Background
2. Preliminaries
3. **Constructions of Boolean functions with two flat spectra**
   - Construction 1
   - Construction 2
4. Boolean functions with lots of flat spectra
5. Questions and Future work

Construction 1 (1)

- $\theta : \mathbb{F}_2^m \to \mathbb{F}_2^m$ and $\theta(\mathbf{x_{0,m}}) \oplus \mathbf{x_{0,m}}$: permutations;
- $n = 2m + t$, t even;
- $S = \{0, 1, \ldots, 2m-1\}$, $\sigma_S(\mathbf{x_{0,n}}) = \bigoplus_{i,k \in S, i<k} x_i x_k$, $h(\mathbf{x_{0,n}}) = \mathbf{x_{0,m}} \cdot \mathbf{x_{m,2m}}$;
- there exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that

$$\sigma_S(\mathbf{x_{0,n}}) = h(\mathbf{x_{0,n}} A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x} \oplus \epsilon.$$

Construction 1 (2)

Theorem 1

Let $g(\mathbf{x_{0,n}}) = \mathbf{x_{0,m}} \cdot \theta(\mathbf{x_{m,2m}}) \oplus r(\mathbf{x_{m,n}})$, for any r such that g is bent. Let $f(\mathbf{x}) = g(\mathbf{x}A \oplus \mathbf{b})$. Then, for $S = \{0, 1, \ldots, 2m-1\}$, both f and $f \oplus \sigma_S$ are bent. Thus, $f(\mathbf{x})$ is flat with respect to the Hadamard transform $H^{\bigotimes n}$, and the $2^n \times 2^n$ unitary, $U = NN \ldots NHH \ldots H$, where there are $2m$ N's and t H's.

Transforms preserve the bent$_4$ property

$E_S(E_{\overline{S}})$: $|S| \times |S|$ $(|\overline{S}| \times |\overline{S}|)$ binary matrix obtained from E by deleting all rows and columns with indices in $\overline{S}$ (S), where $\overline{S} = Z_n \setminus S$.

Lemma 2

Let x, b, $u \in \mathbb{F}_2^n$, $\epsilon \in \mathbb{F}_2$, and $S \subseteq \mathbb{Z}_n$. Let $f(x)$ be an n-variable Boolean function such that $U_S(-1)^{f(x)}$ is flat. Define $f'(x) = f(xE \oplus b) \oplus u \cdot x \oplus \epsilon$, where E is an $n \times n$ binary matrix satisfying the following three conditions:

- **a)** *E_S is an orthogonal matrix, i.e., $E_S \in O(|S|, \mathbb{F}_2)$.*
- **b)** *$E_{\overline{S}} = I$.*
- **c)** *$E_{j,k} = 0$, for all $j \in S$, $k \in \overline{S}$ and for all $j \in \overline{S}$, $k \in S$.*

Then $U_S(-1)^{f'(x)}$ is also flat.

Transforms preserve the bent$_4$ property

$E_S(E_{\overline{S}}) : |S| \times |S|$ ($|\overline{S}| \times |\overline{S}|$) binary matrix obtained from E by deleting all rows and columns with indices in $\overline{S}$ (S), where $\overline{S} = Z_n \setminus S$.

Lemma 2

Let x, b, $u \in \mathbb{F}_2^n$, $\epsilon \in \mathbb{F}_2$, and $S \subseteq \mathbb{Z}_n$. Let $f(x)$ be an n-variable Boolean function such that $U_S(-1)^{f(x)}$ is flat. Define $f'(x) = f(xE \oplus b) \oplus u \cdot x \oplus \epsilon$, where E is an $n \times n$ binary matrix satisfying the following three conditions:

a) *E_S is an orthogonal matrix, i.e., $E_S \in O(|S|, \mathbb{F}_2)$.*

b) *$E_{\overline{S}} = I$.*

c) *$E_{j,k} = 0$, for all $j \in S$, $k \in \overline{S}$ and for all $j \in \overline{S}$, $k \in S$.*

Then $U_S(-1)^{f'(x)}$ is also flat.

Denote by $O_S(n, \mathbb{F}_2)$ the set of matrices that satisfy the three conditions in Lemma 2.

Corollary 1

Let $f(\mathbf{x_{0,n}}A \oplus \mathbf{b})$ be a bent Boolean function constructed in Theorem 1. Then by Lemma 2, for any $E \in O_S(n, \mathbb{F}_2)$, and any $\alpha, \beta \in \mathbb{F}_2^n, \gamma \in \mathbb{F}_2$, $f(\mathbf{x_{0,n}} \cdot E \cdot A \oplus \alpha) \oplus \beta \cdot \mathbf{x_{0,n}} \oplus \gamma$ also has flat spectrum with respect to the transform U_S.

Denote by $O_S(n, \mathbb{F}_2)$ the set of matrices that satisfy the three conditions in Lemma 2.

Corollary 1

Let $f(\mathbf{x_{0,n}}A \oplus \mathbf{b})$ *be a bent Boolean function constructed in Theorem 1. Then by Lemma 2, for any* $E \in O_S(n, \mathbb{F}_2)$, *and any* $\alpha, \beta \in \mathbb{F}_2^n$, $\gamma \in \mathbb{F}_2$, $f(\mathbf{x_{0,n}} \cdot E \cdot A \oplus \alpha) \oplus \beta \cdot \mathbf{x_{0,n}} \oplus \gamma$ *also has flat spectrum with respect to the transform* U_S.

Construction 2 (1)

- $n = 2m$, $S \subset \mathbb{Z}_n$, $|S|$ even. $S(i) < S(j)$ if $i < j$;
- Let q be the first positive integer such that $S(q) \geq m$, i.e., $S(i) < m$ for all $0 \leq i \leq q-1$, and $S(q) \geq m$, $1 \leq q \leq \frac{|S|}{2}$;
- $\sigma_S(\mathbf{x_{0,n}}) = \bigoplus_{i,k \in S, i<k} x_i x_k$,
  $h_S(\mathbf{x_{0,n}}) = \sum_{i=0}^{|S|/2-1} x_{S(i)} x_{S(i+\frac{|S|}{2})}$;
- There exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that $\sigma_S(\mathbf{x_{0,n}}) = h_S(\mathbf{x_{0,n}} A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x_{0,n}} \oplus \epsilon$.

Construction 2 (1)

- $n = 2m$, $S \subset \mathbb{Z}_n$, $|S|$ even. $S(i) < S(j)$ if $i < j$;
- Let q be the first positive integer such that $S(q) \geq m$, i.e., $S(i) < m$ for all $0 \leq i \leq q-1$, and $S(q) \geq m$, $1 \leq q \leq \frac{|S|}{2}$;
- $\sigma_S(\mathbf{x_{0,n}}) = \bigoplus_{i,k \in S, i<k} x_i x_k$,
  $h_S(\mathbf{x_{0,n}}) = \sum_{i=0}^{|S|/2-1} x_{S(i)} x_{S(i+\frac{|S|}{2})}$;
- There exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that $\sigma_S(\mathbf{x_{0,n}}) = h_S(\mathbf{x_{0,n}} A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x_{0,n}} \oplus \epsilon$.

Construction 2 (1)

- $n = 2m$, $S \subset \mathbb{Z}_n$, $|S|$ even. $S(i) < S(j)$ if $i < j$;
- Let q be the first positive integer such that $S(q) \geq m$, i.e., $S(i) < m$ for all $0 \leq i \leq q-1$, and $S(q) \geq m$, $1 \leq q \leq \frac{|S|}{2}$;
- $\sigma_S(\mathbf{x_{0,n}}) = \bigoplus_{i,k \in S, i<k} x_i x_k$, $h_S(\mathbf{x_{0,n}}) = \sum_{i=0}^{|S|/2-1} x_{S(i)} x_{S(i+\frac{|S|}{2})}$;
- There exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that $\sigma_S(\mathbf{x_{0,n}}) = h_S(\mathbf{x_{0,n}} A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x_{0,n}} \oplus \epsilon$.

Construction 2 (1)

- $n = 2m$, $S \subset \mathbb{Z}_n$, $|S|$ even. $S(i) < S(j)$ if $i < j$;
- Let q be the first positive integer such that $S(q) \geq m$, i.e., $S(i) < m$ for all $0 \leq i \leq q-1$, and $S(q) \geq m$, $1 \leq q \leq \frac{|S|}{2}$;
- $\sigma_S(\mathbf{x_{0,n}}) = \bigoplus_{i,k \in S, i<k} x_i x_k$, $h_S(\mathbf{x_{0,n}}) = \sum_{i=0}^{|S|/2-1} x_{S(i)} x_{S(i+\frac{|S|}{2})}$;
- There exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that $\sigma_S(\mathbf{x_{0,n}}) = h_S(\mathbf{x_{0,n}} A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x_{0,n}} \oplus \epsilon$.

Construction 2 (1)

- $n = 2m$, $S \subset \mathbb{Z}_n$, $|S|$ even. $S(i) < S(j)$ if $i < j$;
- Let q be the first positive integer such that $S(q) \geq m$, i.e., $S(i) < m$ for all $0 \leq i \leq q-1$, and $S(q) \geq m$, $1 \leq q \leq \frac{|S|}{2}$;
- $\sigma_S(\mathbf{x_{0,n}}) = \bigoplus_{i,k \in S, i<k} x_i x_k$,
  $h_S(\mathbf{x_{0,n}}) = \sum_{i=0}^{|S|/2-1} x_{S(i)} x_{S(i+\frac{|S|}{2})}$;
- There exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that $\sigma_S(\mathbf{x_{0,n}}) = h_S(\mathbf{x_{0,n}} A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x_{0,n}} \oplus \epsilon$.

Construction 2 (2)

Theorem 2

Let $A, \mathbf{b}, S$ *be defined as above. Let* $\pi(\mathbf{x_{m,2m}}) = (\pi_0(\mathbf{x_{m,2m}}), \pi_1(\mathbf{x_{m,2m}}), \cdots, \pi_{m-1}(\mathbf{x_{m,2m}}))$ *be a linear permutation of* $\mathbb{F}_2^m$ *such that*

$$(\pi_0(\mathbf{x_{m,2m}}) \oplus x_{t(0)}, \pi_1(\mathbf{x_{m,2m}}) \oplus x_{t(1)}, \cdots, \pi_{m-1}(\mathbf{x_{m,2m}}) \oplus x_{t(m-1)})$$

is also a linear permutation of $\mathbb{F}_2^m$*, where* $t(i)$ *is defined in (2). Let* $f(\mathbf{x_{0,2m}}) = \mathbf{x_{0,m}}\pi(\mathbf{x_{m,2m}}) \oplus g(\mathbf{x_{m,2m}})$*. Then* $f(\mathbf{x_{0,2m}}A \oplus \mathbf{b})$ *is bent and also flat with respect to the transform* U_S*.*

Lemma 3

For any $v \in \mathbb{F}_2^n$ and $v \neq \mathbf{0}$, let $\Gamma_v = diag(v)$ be an $n \times n$ matrix, where $n > 1$. There always exists an $n \times n$ binary full rank matrix M such that $\Gamma_v \bigoplus M$ is also full rank.

Corollary 2

Let $n > 1$ be a positive integer. Let $\Gamma \neq \mathbf{0}$ be a binary $n \times n$ matrix, where each row and each column has weight less than or equal to 1. Then there always exists an $n \times n$ binary full rank matrix M such that $\Gamma \bigoplus M$ is also full rank.

Lemma 3

For any $v \in \mathbb{F}_2^n$ and $v \neq \mathbf{0}$, let $\Gamma_v = diag(v)$ be an $n \times n$ matrix, where $n > 1$. There always exists an $n \times n$ binary full rank matrix M such that $\Gamma_v \bigoplus M$ is also full rank.

Corollary 2

Let $n > 1$ be a positive integer. Let $\Gamma \neq \mathbf{0}$ be a binary $n \times n$ matrix, where each row and each column has weight less than or equal to 1. Then there always exists an $n \times n$ binary full rank matrix M such that $\Gamma \bigoplus M$ is also full rank.

Proof of theorem 2 (1)

By Lemma 1, it is sufficient to show that

$$\begin{aligned} & f(\mathbf{x_{0,2m}}A \oplus \mathbf{b}) \oplus \sigma_S(\mathbf{x_{0,2m}}) \\ = \quad & f(\mathbf{x_{0,2m}}A \oplus \mathbf{b}) \oplus h_S(\mathbf{x_{0,2m}}A \oplus \mathbf{b}) \oplus \mathbf{u}\mathbf{x_{0,2m}} \oplus \epsilon \end{aligned}$$

is bent. We show that $f(\mathbf{x_{0,2m}}) \oplus h_S(\mathbf{x_{0,2m}})$ is bent. Recall that

$$\begin{aligned} h_S(\mathbf{x_{0,2m}}) &= \bigoplus_{i=0}^{|S|/2-1} x_{S(i)} x_{S(i+\frac{|S|}{2})} \\ &= \bigoplus_{i=0}^{q-1} x_{S(i)} x_{S(i+\frac{|S|}{2})} \oplus \bigoplus_{i=q}^{|S|/2-1} x_{S(i)} x_{S(i+\frac{|S|}{2})}. \end{aligned}$$

Proof of theorem 2 (2)

Then

$$f(\mathbf{x_{0,2m}}) \oplus h_S(\mathbf{x_{0,2m}}) = \bigoplus_{i=0}^{q-1} x_{S(i)} \cdot (\pi_{S(i)}(\mathbf{x_{m,2m}}) \oplus x_{S(i+\frac{|S|}{2})}) \oplus \bigoplus_{i=0, i\notin S}^{m-1} x_i \pi_i(\mathbf{x_{m,2m}}) \oplus g'(\mathbf{x_{m,2m}}), \quad (1)$$

where $g'(\mathbf{x_{m,2m}}) = g(\mathbf{x_{m,2m}}) \oplus \bigoplus_{i=q}^{|S|/2-1} x_{S(i)} x_{S(i+\frac{|S|}{2})}$.
For $0 \leq i \leq m-1$, define

$$t(i) = \begin{cases} -1, & \text{if } i \notin S, \\ S(k + \frac{|S|}{2}), & \text{if } i \in S, \end{cases} \quad (2)$$

where k is an integer such that $S(k) = i$.

Proof of theorem 2 (3)

Define $x_{-1} = 0$. Then from (1),

$$f(\mathbf{x_{0,2m}}) \oplus h_S(\mathbf{x_{0,2m}}) = \bigoplus_{i=0}^{m-1} x_i(\pi_i(\mathbf{x_{m,2m}}) \oplus x_{t(i)}) \oplus g'(\mathbf{x_{m,2m}}).$$

According to Corollary 2, there exists a linear permutation $\pi(\mathbf{x_{m,2m}})$ such that

$$(\pi_0(\mathbf{x_{m,2m}}) \oplus x_{t(0)}, \pi_1(\mathbf{x_{m,2m}}) \oplus x_{t(1)}, \cdots, \pi_{m-1}(\mathbf{x_{m,2m}}) \oplus x_{t(m-1)})$$

is also a linear permutation of $\mathbb{F}_2^m \Rightarrow$ both $f(\mathbf{x_{0,2m}})$ and $f(\mathbf{x_{0,2m}}) \oplus h_S(\mathbf{x_{0,2m}})$ are bent functions.

By Lemma 2,

Corollary 3

Let $f(\mathbf{x_{0,2m}} A \oplus \mathbf{b})$ *be a Boolean function constructed in Theorem 2. Then by Lemma 2, for any* $E \in O_S(2m, \mathbb{F}_2)$*, and any* α*,* $\beta \in \mathbb{F}_2^{2m}$*,* $\gamma \in \mathbb{F}_2$*,* $f(\mathbf{x_{0,2m}} \cdot E \cdot A \oplus \alpha) \oplus \beta \cdot \mathbf{x_{0,2m}} \oplus \gamma$ *also has flat spectrum with respect to the transform* U_S*.*

Outline

- Bent-negabent functions only have two flat spectra.
- It is of interest to construct Boolean functions of high degree with as many flat spectra as possible with respect to a set of unitary transforms.
- In this section, we give some lower bounds of the numbers of flat spectra w.r.t. $\{H, N\}^n$ of some Boolean functions, and develop some recursive formulae for the numbers of flat spectra of some structural quadratics.

- Bent-negabent functions only have two flat spectra.
- It is of interest to construct Boolean functions of high degree with as many flat spectra as possible with respect to a set of unitary transforms.
- In this section, we give some lower bounds of the numbers of flat spectra w.r.t. $\{H, N\}^n$ of some Boolean functions, and develop some recursive formulae for the numbers of flat spectra of some structural quadratics.

- Bent-negabent functions only have two flat spectra.
- It is of interest to construct Boolean functions of high degree with as many flat spectra as possible with respect to a set of unitary transforms.
- In this section, we give some lower bounds of the numbers of flat spectra w.r.t. $\{H, N\}^n$ of some Boolean functions, and develop some recursive formulae for the numbers of flat spectra of some structural quadratics.

Lower bounds of flat spectra of some Boolean functions

Lemma 4

Let f be a Boolean function of n variables. Then f has at least $n+1$ flat spectra with respect to transforms in $\{I, N\}^{\otimes n}$.

Lemma 5

Let f be a bent Boolean function of n variables. Then f has at least $n+1$ flat spectra with respect to transforms in $\{H, N\}^{\otimes n}$.

Lower bounds of flat spectra of some Boolean functions

Lemma 4

Let f be a Boolean function of n variables. Then f has at least $n+1$ flat spectra with respect to transforms in $\{I, N\}^{\otimes n}$.

Lemma 5

Let f be a bent Boolean function of n variables. Then f has at least $n+1$ flat spectra with respect to transforms in $\{H, N\}^{\otimes n}$.

Lemma 6

Let $f(\mathbf{x_{0,2m}}) = \mathbf{x_{0,m}}\pi(\mathbf{x_{m,2m}}) \oplus \mathbf{g}(\mathbf{x_{m,2m}})$ *be an MM bent function, where* π *is a permutation of* $\mathbb{F}_2^m$*. Then* $f(x)$ *is flat with respect to any transform of the form* $H^{\bigotimes m} \otimes (\bigotimes_{i=0}^{m-1} R_i)$*, where* $R_i \in \{H, N\}$ *for all* $0 \leq i \leq m-1$.

Corollary 4

Let $f(\mathbf{x_{0,2m}}) = \mathbf{x_{0,m}}\pi(\mathbf{x_{m,2m}}) \oplus \mathbf{g}(\mathbf{x_{m,2m}})$ *be an MM bent function, where* π *is a permutation of* $\mathbb{F}_2^m$*. Then* $f(x)$ *has at least* $m + 2^m$ *flat spectra with respect to transforms in* $\{H, N\}^{\otimes n}$.

Lemma 6

Let $f(\mathbf{x_{0,2m}}) = \mathbf{x_{0,m}}\pi(\mathbf{x_{m,2m}}) \oplus \mathbf{g}(\mathbf{x_{m,2m}})$ *be an MM bent function, where* π *is a permutation of* $\mathbb{F}_2^m$*. Then* $f(x)$ *is flat with respect to any transform of the form* $H^{\bigotimes m} \otimes (\bigotimes_{i=0}^{m-1} R_i)$*, where* $R_i \in \{H, N\}$ *for all* $0 \leq i \leq m-1$*.*

Corollary 4

Let $f(\mathbf{x_{0,2m}}) = \mathbf{x_{0,m}}\pi(\mathbf{x_{m,2m}}) \oplus \mathbf{g}(\mathbf{x_{m,2m}})$ *be an MM bent function, where* π *is a permutation of* $\mathbb{F}_2^m$*. Then* $f(x)$ *has at least* $m + 2^m$ *flat spectra with respect to transforms in* $\{H, N\}^{\otimes n}$*.*

Numbers of flat spectra of some quadratic functions

Let $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ be a partition of $\mathbb{Z}_n$.
It is shown in [1] that a quadratic Boolean function will have a flat spectrum w.r.t. a transform in $\{I, H, N\}^n$ iff a certain modification of its adjacency matrix has maximum rank mod 2:

- for $i \in \mathbf{R_I}$, we erase the i^{th} row and column
- for $i \in \mathbf{R_N}$, we substitute 0 for 1 in position $[i, i]$
- for $i \in \mathbf{R_H}$, we leave the i^{th} row and column unchanged,

[1] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions", IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4142-4159, Sep. 2006.

Numbers of flat spectra of some quadratic functions

Let $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ be a partition of $\mathbb{Z}_n$.
It is shown in [1] that a quadratic Boolean function will have a flat spectrum w.r.t. a transform in $\{I, H, N\}^n$ iff a certain modification of its adjacency matrix has maximum rank mod 2:

- for $i \in \mathbf{R_I}$, we erase the i^{th} row and column
- for $i \in \mathbf{R_N}$, we substitute 0 for 1 in position $[i, i]$
- for $i \in \mathbf{R_H}$, we leave the i^{th} row and column unchanged,

[1] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions", IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4142-4159, Sep. 2006.

Numbers of flat spectra of some quadratic functions

Let $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ be a partition of $\mathbb{Z}_n$.
It is shown in [1] that a quadratic Boolean function will have a flat spectrum w.r.t. a transform in $\{I, H, N\}^n$ iff a certain modification of its adjacency matrix has maximum rank mod 2:

- for $i \in \mathbf{R_I}$, we erase the i^{th} row and column
- for $i \in \mathbf{R_N}$, we substitute 0 for 1 in position $[i, i]$
- for $i \in \mathbf{R_H}$, we leave the i^{th} row and column unchanged,

[1] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions", IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4142-4159, Sep. 2006.

Numbers of flat spectra of some quadratic functions

Let $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ be a partition of $\mathbb{Z}_n$.
It is shown in [1] that a quadratic Boolean function will have a flat spectrum w.r.t. a transform in $\{I, H, N\}^n$ iff a certain modification of its adjacency matrix has maximum rank mod 2:

- for $i \in \mathbf{R_I}$, we erase the i^{th} row and column
- for $i \in \mathbf{R_N}$, we substitute 0 for 1 in position $[i, i]$
- for $i \in \mathbf{R_H}$, we leave the i^{th} row and column unchanged,

[1] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions", IEEE Trans. Inf. Theory, vol. 52, no. 9, pp. 4142-4159, Sep. 2006.

Some quadratic Boolean functions

- *line function*, $p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c} \cdot \mathbf{x} + d$;
- *clique function* $p_c(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j$;
- *n clique-line-m clique*,
  $$p_{n,m}(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1} x_n + \sum_{n \le i < j \le n+m-1} x_i x_j \;;$$
- (n, r)-star-line function, $p_{(n,r)}(\mathbf{x}) = x_r \sum_{i=0}^{r-1} x_i + \sum_{i=r}^{n-2} x_i x_{i+1}$;
- (n, r) function $\widetilde{p}_{(n,r)}(\mathbf{x})$,
  $\widetilde{p}_{(n,r)}(\mathbf{x}) = (-1)^{\sum_{i=r}^{n-2} x_i x_{i+1}} \prod_{i=0}^{r-1} (x_i + x_r + 1)$;
- m-star-line-n-star function,
  $f_{m,n} = x_{m-1} \sum_{i=0}^{m-2} x_i + x_{m-1} x_m + x_m \sum_{i=m+1}^{n+m-1} x_i$;
- $\widetilde{f}_{m,n} = (-1)^{x_{m-1} x_m} \prod_{i=0}^{m-2} (x_i + x_{m-1} + 1) \prod_{i=m+1}^{n+m-1} (x_i + x_m + 1)$.

Some quadratic Boolean functions

- *line function*, $p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c} \cdot \mathbf{x} + d$;
- *clique function* $p_c(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j$;
- *n clique-line-m clique*, $p_{n,m}(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1} x_n + \sum_{n \le i < j \le n+m-1} x_i x_j$;
- (n,r)-star-line function, $p_{(n,r)}(\mathbf{x}) = x_r \sum_{i=0}^{r-1} x_i + \sum_{i=r}^{n-2} x_i x_{i+1}$;
- (n,r) function $\widetilde{p}_{(n,r)}(\mathbf{x})$, $\widetilde{p}_{(n,r)}(\mathbf{x}) = (-1)^{\sum_{i=r}^{n-2} x_i x_{i+1}} \prod_{i=0}^{r-1} (x_i + x_r + 1)$;
- m-star-line-n-star function, $f_{m,n} = x_{m-1} \sum_{i=0}^{m-2} x_i + x_{m-1} x_m + x_m \sum_{i=m+1}^{n+m-1} x_i$;
- $\widetilde{f}_{m,n} = (-1)^{x_{m-1} x_m} \prod_{i=0}^{m-2} (x_i + x_{m-1} + 1) \prod_{i=m+1}^{n+m-1} (x_i + x_m + 1)$.

Some quadratic Boolean functions

- *line function*, $p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c} \cdot \mathbf{x} + d$;
- *clique function* $p_c(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j$;
- *n clique-line-m clique*, $p_{n,m}(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1} x_n + \sum_{n \le i < j \le n+m-1} x_i x_j$;
- (n, r)-star-line function, $p_{(n,r)}(\mathbf{x}) = x_r \sum_{i=0}^{r-1} x_i + \sum_{i=r}^{n-2} x_i x_{i+1}$;
- (n, r) function $\widetilde{p}_{(n,r)}(\mathbf{x})$, $\widetilde{p}_{(n,r)}(\mathbf{x}) = (-1)^{\sum_{i=r}^{n-2} x_i x_{i+1}} \prod_{i=0}^{r-1} (x_i + x_r + 1)$;
- m-star-line-n-star function, $f_{m,n} = x_{m-1} \sum_{i=0}^{m-2} x_i + x_{m-1} x_m + x_m \sum_{i=m+1}^{n+m-1} x_i$;
- $\widetilde{f}_{m,n} = (-1)^{x_{m-1} x_m} \prod_{i=0}^{m-2} (x_i + x_{m-1} + 1) \prod_{i=m+1}^{n+m-1} (x_i + x_m + 1)$.

Some quadratic Boolean functions

- *line function*, $p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c} \cdot \mathbf{x} + d$;
- *clique function* $p_c(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j$;
- *n clique-line-m clique*,
  $$p_{n,m}(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1} x_n + \sum_{n \le i < j \le n+m-1} x_i x_j \ ;$$
- (n, r)-star-line function, $p_{(n,r)}(\mathbf{x}) = x_r \sum_{i=0}^{r-1} x_i + \sum_{i=r}^{n-2} x_i x_{i+1}$;
- (n, r) function $\widetilde{p}_{(n,r)}(\mathbf{x})$,
  $\widetilde{p}_{(n,r)}(\mathbf{x}) = (-1)^{\sum_{i=r}^{n-2} x_i x_{i+1}} \prod_{i=0}^{r-1} (x_i + x_r + 1)$;
- m-star-line-n-star function,
  $f_{m,n} = x_{m-1} \sum_{i=0}^{m-2} x_i + x_{m-1} x_m + x_m \sum_{i=m+1}^{n+m-1} x_i$;
- $\widetilde{f}_{m,n} = (-1)^{x_{m-1} x_m} \prod_{i=0}^{m-2} (x_i + x_{m-1} + 1) \prod_{i=m+1}^{n+m-1} (x_i + x_m + 1)$.

Some quadratic Boolean functions

- *line function,* $p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c} \cdot \mathbf{x} + d$;
- *clique function* $p_c(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j$;
- *n clique-line-m clique,*
  $$p_{n,m}(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1} x_n + \sum_{n \le i < j \le n+m-1} x_i x_j \ ;$$
- (n,r)-star-line function, $p_{(n,r)}(\mathbf{x}) = x_r \sum_{i=0}^{r-1} x_i + \sum_{i=r}^{n-2} x_i x_{i+1}$;
- (n,r) function $\widetilde{p}_{(n,r)}(\mathbf{x})$,
  $\widetilde{p}_{(n,r)}(\mathbf{x}) = (-1)^{\sum_{i=r}^{n-2} x_i x_{i+1}} \prod_{i=0}^{r-1} (x_i + x_r + 1)$;
- m-star-line-n-star function,
  $f_{m,n} = x_{m-1} \sum_{i=0}^{m-2} x_i + x_{m-1} x_m + x_m \sum_{i=m+1}^{n+m-1} x_i$;
- $\widetilde{f}_{m,n} = (-1)^{x_{m-1} x_m} \prod_{i=0}^{m-2} (x_i + x_{m-1} + 1) \prod_{i=m+1}^{n+m-1} (x_i + x_m + 1)$.

Some quadratic Boolean functions

- *line function*, $p_l(\mathbf{x}) = \sum_{j=0}^{n-2} x_j x_{j+1} + \mathbf{c} \cdot \mathbf{x} + d$;
- *clique function* $p_c(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j$;
- *n clique-line-m clique*,
  $$p_{n,m}(\mathbf{x}) = \sum_{0 \le i < j \le n-1} x_i x_j + x_{n-1} x_n + \sum_{n \le i < j \le n+m-1} x_i x_j \;;$$
- (n, r)-star-line function, $p_{(n,r)}(\mathbf{x}) = x_r \sum_{i=0}^{r-1} x_i + \sum_{i=r}^{n-2} x_i x_{i+1}$;
- (n, r) function $\widetilde{p}_{(n,r)}(\mathbf{x})$,
  $\widetilde{p}_{(n,r)}(\mathbf{x}) = (-1)^{\sum_{i=r}^{n-2} x_i x_{i+1}} \prod_{i=0}^{r-1} (x_i + x_r + 1)$;
- m-star-line-n-star function,
  $f_{m,n} = x_{m-1} \sum_{i=0}^{m-2} x_i + x_{m-1} x_m + x_m \sum_{i=m+1}^{n+m-1} x_i$;
- $\widetilde{f}_{m,n} = (-1)^{x_{m-1} x_m} \prod_{i=0}^{m-2} (x_i + x_{m-1} + 1) \prod_{i=m+1}^{n+m-1} (x_i + x_m + 1)$.

Function	w.r.t. $\{H,N\}^n$ ($\{H,N\}^{n+m}$)	w.r.t. $\{I,H\}^n$ ($\{I,H\}^{n+m}$)	w.r.t. $\{I,H,N\}^n$ ($\{I,H,N\}^{n+m}$)
Line	$\frac{2^{n+1}-(-1)^{n+1}}{3}$	$\frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{n+1}-(\frac{1-\sqrt{5}}{2})^{n+1}]$	$\frac{(1+\sqrt{3})^{n+1}-(1-\sqrt{3})^{n+1}}{2\sqrt{3}}$
Clique	$n+\frac{1+(-1)^n}{2}$	2^{n-1}	$(n+1)2^{n-1}$
n-clique-line-m clique	$3mn-n(\frac{1+(-1)^m}{2})$ $-m(\frac{1+(-1)^n}{2})$ $+3(\frac{1+(-1)^n}{2})(\frac{1+(-1)^m}{2})$	$5\cdot 2^{n+m-4}$	$2^{n+m-3}\cdot$ $(3nm+2n+2m+2)$
(n,r) star line	$(r+1)\frac{2^{n-r+1}}{3}$ $+\frac{2r-1}{3}(-1)^{n-r+1}$	A[1]	B[2]
m-star-line-n star	$(2m-1)(2n-1)+2$	$mn+1$	$(mn+m+n+3)2^{m+n-2}$
Star	$2n-1$	n	$(n+1)2^{n-1}$
$\widetilde{p}_{(n,r)}(\mathbf{x})$	$\frac{2^{n+1}}{3}$ $-\frac{2^r}{3}(-1)^{n-r+1}$	A[1]	B[2]
$\widetilde{f}_{m,n}$	$3\cdot 2^{m+n-2}$	$mn+1$	$(mn+m+n+3)2^{m+n-2}$

[1] $A=K^{IH}_{(n,r)}=\frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{n-r+1}-(\frac{1-\sqrt{5}}{2})^{n-r+1}+r((\frac{1+\sqrt{5}}{2})^{n-r}-(\frac{1-\sqrt{5}}{2})^{n-r})]$.

[2] $B=K^{IHN}_{(n,r)}=\frac{2^{r-1}}{\sqrt{3}}[(r+1+\sqrt{3})(1+\sqrt{3})^{n-r}-(r+1-\sqrt{3})(1-\sqrt{3})^{n-r}]$.

Outline

Questions and Future work

- Exact number or lower bound of the flat spectra w.r.t. transforms in $\{H, N\}^n$ for the Boolean functions in Constructions 1 and 2.
- Over the set of all Boolean functions, does the line function maximize the number of flat spectra w.r.t. $\{H, N\}^n$?
- Construct Boolean functions of degree greater than 2 that have lots of flat spectra w.r.t. $\{H, N\}^n$, $\{I, H\}^n$, $\{I, N\}^n$, or $\{I, H, N\}^n$.
- Construct self-dual bent_4 functions.

Questions and Future work

- Exact number or lower bound of the flat spectra w.r.t. transforms in $\{H, N\}^n$ for the Boolean functions in Constructions 1 and 2.
- Over the set of all Boolean functions, does the line function maximize the number of flat spectra w.r.t. $\{H, N\}^n$?
- Construct Boolean functions of degree greater than 2 that have lots of flat spectra w.r.t. $\{H, N\}^n$, $\{I, H\}^n$, $\{I, N\}^n$, or $\{I, H, N\}^n$.
- Construct self-dual bent$_4$ functions.

Questions and Future work

- Exact number or lower bound of the flat spectra w.r.t. transforms in $\{H, N\}^n$ for the Boolean functions in Constructions 1 and 2.
- Over the set of all Boolean functions, does the line function maximize the number of flat spectra w.r.t. $\{H, N\}^n$?
- Construct Boolean functions of degree greater than 2 that have lots of flat spectra w.r.t. $\{H, N\}^n$, $\{I, H\}^n$, $\{I, N\}^n$, or $\{I, H, N\}^n$.
- Construct self-dual bent$_4$ functions.

Questions and Future work

- Exact number or lower bound of the flat spectra w.r.t. transforms in $\{H, N\}^n$ for the Boolean functions in Constructions 1 and 2.
- Over the set of all Boolean functions, does the line function maximize the number of flat spectra w.r.t. $\{H, N\}^n$?
- Construct Boolean functions of degree greater than 2 that have lots of flat spectra w.r.t. $\{H, N\}^n$, $\{I, H\}^n$, $\{I, N\}^n$, or $\{I, H, N\}^n$.
- Construct self-dual bent$_4$ functions.

Thank you so much for your time :-)