

Decompositions of negabent functions and related properties

Aleksandr Kutsenko

Novosibirsk State University

The 14th Workshop on
Current Trends in Cryptology (CTCrypt 2025)
Veliky Novgorod, June 3–6, 2025

Some representation of Boolean functions

Some representation of Boolean functions

Vector of values (in the lexicographic order):

$$\mathbf{f} = (f_0, f_1, \dots, f_{2^n-1})$$

Characteristic vector (in the lexicographic order):

$$(-1)^{\mathbf{f}} = \left((-1)^{f_0}, (-1)^{f_1}, \dots, (-1)^{f_{2^n-1}} \right)$$

Some representation of Boolean functions

Vector of values (in the lexicographic order):

$$\mathbf{f} = (f_0, f_1, \dots, f_{2^n-1})$$

Zhegalkin polynomial's (algebraic normal form), real polynomial's, Fourier coefficients

$$\mathbf{f} \longrightarrow M\mathbf{f}$$

Characteristic vector (in the lexicographic order):

$$(-1)^{\mathbf{f}} = \left((-1)^{f_0}, (-1)^{f_1}, \dots, (-1)^{f_{2^n-1}} \right)$$

Walsh–Hadamard coefficients

$$(-1)^{\mathbf{f}} \longrightarrow M(-1)^{\mathbf{f}}$$

Some representation of Boolean functions

Vector of values (in the lexicographic order):

$$\mathbf{f} = (f_0, f_1, \dots, f_{2^n-1})$$

Zhegalkin polynomial's (algebraic normal form), real polynomial's, Fourier coefficients

$$\mathbf{f} \longrightarrow M\mathbf{f}$$

Matrix M of order $2^n \times 2^n$ usually is a tensor product (Kronecker product) of some **basic** matrices.

Characteristic vector (in the lexicographic order):

$$(-1)^{\mathbf{f}} = \left((-1)^{f_0}, (-1)^{f_1}, \dots, (-1)^{f_{2^n-1}} \right)$$

Walsh–Hadamard coefficients

$$(-1)^{\mathbf{f}} \longrightarrow M(-1)^{\mathbf{f}}$$

In quantum mechanics there are known the **Pauli matrices**

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The set $\{I, \sigma_x, \sigma_y, \sigma_z\}$ forms a basis in a real space of 2×2 Hermitian matrices and a basis in a complex space of 2×2 complex matrices.

- real space of 2×2 Hermitian matrices — **density matrix** of a two-level quantum-mechanical system, in particular, density matrix of a single qubit;
- complex space of 2×2 complex matrices — **all unitary operators** acting on a single qubit, including any local error that could act on a qubit.

In quantum mechanics there are known the **Pauli matrices**

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The **Pauli group** P_1 on 1 qubit is generated by these matrices with some global phase equal to ± 1 or $\pm i$:

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm \sigma_x, \pm i\sigma_x, \pm \sigma_y, \pm i\sigma_y, \pm \sigma_z, \pm i\sigma_z\} = \langle \sigma_x, \sigma_y, \sigma_z \rangle.$$

The n -qubit **Pauli group** P_n is generated by n -fold Kronecker products of Pauli matrices with some global phase equal to ± 1 or $\pm i$. Its order is equal to 4^{n+1} .

The **local Clifford group** $\mathbf{C}_1$ is defined as a subgroup of order 192 of the normalizer¹ of the Pauli group in unitary group $\mathbf{U}(2)$ that is generated by the Sylvester–Hadamard matrix $\mathcal{H}_1$ of order 1 and nega-Hadamard kernel matrix $\mathcal{N}_1$:

$$\mathcal{H}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathcal{N}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}.$$

The group $\mathbf{C}_1$ is the normalizer of $\mathbf{P}_1$ in the unitary group $\mathbf{U}(2)$ up to overall phase factors $\pm 1, \pm i$.

¹It holds $ghg^{-1} \in H$ for any $g \in G$ and $h \in H$.

The n -qubit local Clifford group $\mathbf{C}_n$ can be represented by the set of matrices that decompose into a Kronecker product of unitary matrices from the local Clifford group $\mathbf{C}_1$. Matrices from $\mathbf{C}_n$ normalize Kronecker products of the Pauli matrices, and can be generated by the 2^n generators

$$\{\mathcal{H}_1, \mathcal{N}_1\}^n = \prod_{j \in J} \mathcal{H}_1^{(j)} \prod_{k \in K} \mathcal{N}_1^{(k)},$$

where J, K partition $\{0, 1, \dots, n-1\}$ and $A^{(k)} = I \otimes I \otimes \dots \otimes I \otimes \underbrace{A}_{k\text{-th}} \otimes I \otimes \dots \otimes I$.

$$\mathcal{H}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$\mathcal{N}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}.$$

$$\mathcal{H}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

$$\mathcal{N}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}.$$

- Clifford gates $\{\text{CNOT}, H, S\}$, where gate S is defined by the matrix $\mathcal{H}_1\mathcal{N}_1$. **The Gottesman–Knill theorem:** a quantum circuit consisting solely of Clifford gates can be simulated efficiently on a classical computer;
- QECC, stabilizer states and stabilizer generators;
- Action of the gates from $\mathbf{C}_n$ on pure quantum state keeps invariant the distance properties of the state when viewed as a zero-dimensional QECC.

The **Walsh–Hadamard transform** (WHT) of a Boolean function f in n variables is an integer function $W_f : \mathbb{F}_2^n \rightarrow \mathbb{Z}$, defined as

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}, \quad y \in \mathbb{F}_2^n.$$

The **nega-Hadamard transform** of a Boolean function f in n variables is a complex valued function:

$$N_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle} i^{\text{wt}(x)}, \quad y \in \mathbb{F}_2^n.$$

Transforms of Boolean functions

Walsh–Hadamard and nega-Hadamard transforms are characterized by $2^n \times 2^n$ unitary matrices $H_n = \underbrace{H_1 \otimes H_1 \otimes \dots \otimes H_1}_{n \text{ times}}$, where

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and $N_n = \underbrace{N_1 \otimes N_1 \otimes \dots \otimes N_1}_{n \text{ times}}$, where

$$N_1 = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix},$$

correspondingly.

Motivation for nega-Hadamard transform: spectral characteristics

For Boolean function f in n variables one can investigate the value of the **effective nonlinearity** (Parker, 2006):

$$\gamma(f) = 2^{n-1} - 2^{n/2-1} \sqrt{\text{PAR}_{\mathcal{U}}(f)},$$

where peak-to-average power ratio (PAR) is

$$\text{PAR}_{\mathcal{U}}(f) = 2^n \cdot \max_{U \in \mathcal{U}} \left(|P_k|^2 : P = U(-1)^f \right).$$

Motivation for nega-Hadamard transform: spectral characteristics

For Boolean function f in n variables one can investigate the value of the **effective nonlinearity** (Parker, 2006):

$$\gamma(f) = 2^{n-1} - 2^{n/2-1} \sqrt{\text{PAR}_{\mathcal{U}}(f)},$$

where peak-to-average power ratio (PAR) is

$$\text{PAR}_{\mathcal{U}}(f) = 2^n \cdot \max_{U \in \mathcal{U}} \left(|P_k|^2 : P = U(-1)^f \right).$$

For $\mathcal{U} = \{\mathcal{H}_1\}^{\otimes n}$ we have standard nonlinearity.

$\mathcal{U}$	$\{\mathcal{H}_1\}^{\otimes n}$	$\{\mathcal{H}_1, \mathcal{N}_1\}^{\otimes n}$	$\{I, \mathcal{H}_1\}^{\otimes n}$	$\{I, \mathcal{H}_1, \mathcal{N}_1\}^{\otimes n}$
AES S-box	112	97.93	94.06	94.06

The spectrum of Boolean functions with respect to $\mathcal{U} = \{I, \mathcal{H}_1, \mathcal{N}_1\}^{\otimes n}$ was considered in (Danielsen, Gulliver, Parker, 2006; Riera, Parker, 2006).

Motivation for nega-Hadamard transform: quantum state

One can consider characteristic vector of a Boolean function as phases of amplitudes for a n -qubit uniform pure quantum state ([«On Connections Between Graphs, Codes, Quantum States, and Boolean Functions», Danielsen, 2008](#)):

$$|\psi\rangle = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} |x\rangle,$$

Then unitary transforms from $\{I, \mathcal{H}_1\}^{\otimes n}$ correspond to amplitudes after quantum evolutions provided by Hadamard gates are applied. At the same time $\{I, \mathcal{H}_1, \mathcal{N}_1\}^{\otimes n}$ provide the action of all Clifford gates except CNOT-gate.

Bent and negabent functions

A Boolean function f in n variables is said to be **bent** if

$$|W_f(y)| = 2^{n/2}, \quad y \in \mathbb{F}_2^n.$$

The minimal possible maximal absolute value $2^{n/2}$ of the nega-Hadamard spectrum is provided by the **nega-Parseval's identity** (Stănică et al., 2012)

$$\sum_{y \in \mathbb{F}_2^n} |N_f(y)|^2 = 2^{2n}.$$

A Boolean function f in n variables is said to be **negabent** if

$$|N_f(y)| = 2^{n/2}, \quad y \in \mathbb{F}_2^n.$$

Bent-negabent functions

A Boolean function is called **bent-negabent** if it is both bent and negabent that is it has flat both Walsh–Hadamard and nega-Hadamard magnitude spectrums.

	$ \mathcal{B}_n $	$ \mathcal{NB}_n $	$ \mathcal{B}_n \cap \mathcal{NB}_n $
$n = 1$	0	4	0
$n = 2$	8	8	0
$n = 3$	0	64	0
$n = 4$	896	896	384
$n = 5$	0	802 816	0

Dual bent-negabent functions

For every bent function its **dual** Boolean function is uniquely defined. The condition $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ for any $x \in \mathbb{F}_2^n$ gives the Boolean function $\tilde{f}$ that is said to be **dual** of f

In the same way as for bent functions, we define the dual function $\tilde{f}$ of bent-negabent function f . Moreover, dual of bent-negabent function is again bent-negabent ([Parker, Pott, 2007](#)).

Connection between bent and negabent functions

For even number of variables negabent functions are **strongly related** to bent functions:
the mapping

$$f(x) \longrightarrow f(x) \oplus \bigoplus_{1 \leq i < j \leq n} x_i x_j$$

defines an isometry between the sets of bent and negabent functions in even number $n \geq 2$ of variables.

Negabent functions: current state

- Any affine function is negabent (Parker, Pott, 2007);
- Spectrum values for a negabent function f in even (Schmidt, Parker, Pott, 2008) and odd (Su, Pott, Tang, 2013) number of variables;
- Possible values and tight upper bound $\lceil \frac{n}{2} \rceil$ of the algebraic degree of negabent functions (Stănică et al., 2012);
- Study of negabent functions defined over finite fields and characterization of negabent quadratic monomial functions (Sarkar, 2012);
- Necessary and sufficient conditions for negabentness of Boolean functions in odd number of variables (Su, Pott, Tang, 2013);
- Constructions of families of quadratic and cubic monomial negabent functions, together with several sporadic examples (Zhou, Qu, 2017);
- Generalization of the notion of bent-negabentness for vectorial Boolean functions (Pasalic, Kudin, Polujan, Pott, 2022).

Bent-negabent functions: current state

- Some constructions of Boolean functions which are simultaneously bent and negabent ([Parker, Pott, 2007](#); [Zhang, Wei, Pasalic, 2015](#));
- Transforms that leave the bent-negabent property invariant ([Schmidt, Parker, Pott, 2008](#));
- The conjecture that there doesn't exist bent-negabent rotation symmetric Boolean functions was studied and it was proved that it is true for almost all the cases ([Mandal et al., 2018](#); [Sun, Shi, Liu, Fu, 2022](#));
- Generalization of the notion of bent-negabentness for vectorial Boolean functions ([Pasalic, Kudin, Polujan, Pott, 2022](#));
- Several secondary methods for constructing bent-negabent functions under the frameworks of the indirect sum construction together with its modified version and Rothaus' construction ([Guo, Wang, Gong, 2023](#)).

Decomposition of vector of values

Let $\mathbf{f}$ be a vector of values of a Boolean function f in n variables

$$\mathbf{f} = (f_0, f_1, \dots, f_{2^k-1}),$$

where f_i are vectors of values of Boolean functions in $n - k$ variables.

Decomposition of vector of values

Let $\mathbf{f}$ be a vector of values of a Boolean function f in n variables

$$\mathbf{f} = (f_0, f_1, \dots, f_{2^k-1}),$$

where f_i are vectors of values of Boolean functions in $n - k$ variables.

Motivation:

- several examples of secondary constructions of bent functions, including iterative constructions, are based on such decompositions ([Preneel et al., 1991](#); [Tokareva, 2011](#));
- some lower and upper bounds for (self-dual) bent functions were obtained upon characteristic vectors analysis;
- some known metrical properties of Boolean functions are based on the characteristic vectors properties.

Decomposition of vector of values: $k = 1$

Let $\mathbf{f}$ be a vector of values of a Boolean function f in n variables

$$\mathbf{f} = (f_0, f_1),$$

where f_i are vectors of values of Boolean functions in $n - 1$ variables.

In (Stănică et al., 2012) just the same subfunctions of a negabent function in n variables were studied: it was proved that if $f(x, y) = f_0(x)(1 \oplus y) \oplus f_1(x)y$, then the following statements are equivalent:

- 1) f is negabent;
- 2) f_0 and f_1 have complementary nega-autocorrelation that is $C_{f_0}^{nega}(y) + C_{f_1}^{nega}(y) = 0$ for any nonzero $y \in \mathbb{F}_2^{n-1}$, and $C_{f_0, f_1}^{nega}(y) = 0$ for all y with odd Hamming weight;
- 3) $|\mathcal{N}_{f_0}(y)|^2 + |\mathcal{N}_{f_1}(y)|^2 = 2$ for all $y \in \mathbb{F}_2^{n-1}$ and $\frac{\mathcal{N}_{f_0}(y)}{\mathcal{N}_{f_1}(y)}$ is a real number whenever $|\mathcal{N}_{f_0}(y)| \cdot |\mathcal{N}_{f_1}(y)| \neq 0$.

Decomposition of vector of values: $k = 2$

Let $\mathbf{f}$ be a vector of values of a Boolean function f in n variables

$$\mathbf{f} = (f_0, f_1, f_2, f_3),$$

where f_i are vectors of values of Boolean functions in $n - 2$ variables.

Such decompositions were investigated in (Canteaut, Carlet, Charpin, Fontaine, 2001; Canteaut, Charpin, 2003).

Bent functions that are concatenations of four bent functions were also studied in (Preneel et al., 1991) and (Tokareva, 2011) from the point of view of obtaining lower bounds on the cardinality of the set of bent functions. They were referred to as **bent iterative** functions.

Concatenation constructions were also considered in recent papers (Hodžić, Pasalic, Wei, 2020; Bapić, Pasalic, Zhang, Hodžić, 2022).

Gram matrices of negabent functions

Gram matrices of negabent functions

Consider inner products $g_{ij} = \langle F_i, F_j \rangle$, where $F_k = (-1)^{f_k}$.

Gram matrices of negabent functions

Consider inner products $g_{ij} = \langle F_i, F_j \rangle$, where $F_k = (-1)^{f_k}$.

The form of the Gram matrix of negabent functions is characterized by

Proposition

The Gram matrix of any negabent function, say f , in n variables has form

$$\text{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & c & a \\ b & 2^{n-2} & a & d \\ c & a & 2^{n-2} & e \\ a & d & e & 2^{n-2} \end{pmatrix}$$

for some even integers a, b, c, d, e .

Proposition

Let f be a negabent function in n variables, then if at least one of its subfunctions f_0, f_1, f_2, f_3 is negabent, the rest of them are also negabent.

Gram matrices of bent-negabent functions: bent functions impact

In (A.K., 2023) it was proved that the Gram matrices of any bent function f , in n variables and its dual bent function $\tilde{f}$ have form

$$\text{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & c & -a \\ b & 2^{n-2} & a & -c \\ c & a & 2^{n-2} & -b \\ -a & -c & -b & 2^{n-2} \end{pmatrix}, \quad \text{Gram}(\tilde{f}) = \begin{pmatrix} 2^{n-2} & c & b & -a \\ c & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -c \\ -a & -b & -c & 2^{n-2} \end{pmatrix}$$

for some even integers a, b, c such that

$$-2^{n-2} + |b + c| \leq a \leq 2^{n-2} - |b - c|.$$

Theorem

The Gram matrices of any bent-negabent function, say f , in n variables and its dual bent-negabent function $\tilde{f}$ have form

$$\text{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & c & 0 \\ b & 2^{n-2} & 0 & -c \\ c & 0 & 2^{n-2} & -b \\ 0 & -c & -b & 2^{n-2} \end{pmatrix}, \quad \text{Gram}(\tilde{f}) = \begin{pmatrix} 2^{n-2} & c & b & 0 \\ c & 2^{n-2} & 0 & -b \\ b & 0 & 2^{n-2} & -c \\ 0 & -b & -c & 2^{n-2} \end{pmatrix}$$

for some even integers b, c such that

$$\max \{|b + c|, |b - c|\} \leq 2^{n-2}.$$

Iterative constructions of negabent functions

Given a negabent function f in n variables, we are to consider the relation $\langle F_0, F_3 \rangle = \langle F_1, F_2 \rangle$ for two extrema cases.

- $\langle F_0, F_3 \rangle = \langle F_1, F_2 \rangle = 2^{n-2}$: from this we obtain characteristic vector $(\mathbf{A}, \mathbf{B}, \mathbf{B}, \mathbf{A})$, where A, B are characteristic vectors of negabent functions in $n - 2$ variables;
- $\langle F_0, F_3 \rangle = \langle F_1, F_2 \rangle = -2^{n-2}$: from this we deduce the vector $(\mathbf{A}, \mathbf{B}, -\mathbf{B}, -\mathbf{A})$, where A, B are characteristic vectors of negabent functions in $n - 2$ variables.

It is worth to note that the proposed constructions **do not** provide bent-negabent functions for any even $n \geq 4$.

Proposition

For any $n \geq 3$ it holds

$$|\mathcal{NB}_n| \geq 2 |\mathcal{NB}_{n-2}|^2.$$

Iterative constructions of negabent functions: bound for cardinality

Proposition

For any $n \geq 3$ it holds

$$|\mathcal{NB}_n| \geq 2 |\mathcal{NB}_{n-2}|^2.$$

	$ \mathcal{B}_n $	$ \mathcal{NB}_n $	$ \mathcal{NB}\mathcal{I}_n $	$2 \mathcal{NB}_{n-2} ^2$
$n = 1$	0	4	—	—
$n = 2$	8	8	—	—
$n = 3$	0	64	64	32
$n = 4$	896	896	512	128
$n = 5$	0	$802\,816 \simeq 2^{19.6}$	$262\,144 = 2^{18}$	$8192 = 2^{13}$
$n = 6$	$\simeq 2^{32.3}$	$\simeq 2^{32.3}$	*	$\simeq 2^{20.6}$

Self-duality of negabent functions

We will study the question of **self-duality** of negabent function that is the existence of such functions that

$$N_f(y) = 2^{n/2}(-1)^{f(y)} \quad (1)$$

for all $y \in \mathbb{F}_2^n$ or

$$N_f(y) = i \cdot 2^{n/2}(-1)^{f(y)} \quad (2)$$

for all $y \in \mathbb{F}_2^n$.

Self-duality of negabent functions

We will study the question of **self-duality** of negabent function that is the existence of such functions that

$$N_f(y) = 2^{n/2}(-1)^{f(y)} \quad (1)$$

for all $y \in \mathbb{F}_2^n$ or

$$N_f(y) = i \cdot 2^{n/2}(-1)^{f(y)} \quad (2)$$

for all $y \in \mathbb{F}_2^n$.

Theorem

There are no negabent functions that possess the property (1) or (2).

Minimal Hamming distance between negabent functions

As it was mentioned in previous sections, the algebraic degree of any negabent function in n variables is at most $\lceil \frac{n}{2} \rceil$, therefore Hamming distance between any pair of distinct negabent functions in n variables is at least $2^{n-\lceil n/2 \rceil} = 2^{\lfloor n/2 \rfloor}$.

Minimal Hamming distance between negabent functions

As it was mentioned in previous sections, the algebraic degree of any negabent function in n variables is at most $\lceil \frac{n}{2} \rceil$, therefore Hamming distance between any pair of distinct negabent functions in n variables is at least $2^{n-\lceil n/2 \rceil} = 2^{\lfloor n/2 \rfloor}$.

In what follows we will provide the minimal distance for the set of negabent functions.

Proposition

The minimal Hamming distance between distinct negabent functions in n variables is equal to $2^{\lfloor n/2 \rfloor}$.

For even n it coincides with the minimal distance between bent functions, while for odd n is equal to $2^{(n-1)/2}$.

Thanks for attention!