Perfectly Balanced Functions in Symbolic Dynamics*

Oleg A. Logachev[1], Alexei A. Salnikov[2], Stanislav V. Smyshlyaev[3] and Valery V. Yashchenko[4]

Abstract: In the present paper we study properties of perfectly balanced Boolean functions. Based on the concept of Boolean function barrier, we propose a novel approach to construct large classes of perfectly balanced Boolean functions.

Keywords: Symbolic dynamics, code, filter generator, perfectly balanced function, barrier.

Introduction

A nonfeedback shift register with nonlinear filtering function (finite memory encoder [1, 2]) implements a convolution transformation of binary sequences. A finite memory encoder feeded with linear recurrence sequence turns out to be a filter generator. One of the aims of studying such shift registers is to provide for acceptable statistical properties of output sequences. The best statistical properties of output sequences are reached when using perfectly balanced functions [3, 4].

The paper is organized as follows. In Section 1 we remind some basic concepts of symbolic dynamics. Properties of perfectly balanced Boolean functions in the general case are studied in Section 2. Binary case is treated in Section 3. In Section 4 we propose based on the concept of Boolean function barrier a novel approach to construct large classes of perfectly balanced Boolean functions. In Appendix we present a classification of perfectly balanced Boolean functions of $n = 4$ and $n = 5$ variables.

1 Background

In the present section we give some background on symbolic dynamics. For a more detailed exposition, the reader is referred to [5, 6].

Let I denote the set of all integers. For $i \in \mathrm{I}$, let $\mathrm{I}_i = \{j \in \mathrm{I} \,|\, j \geq i\}$. The cardinality of a set E will be denoted by $\operatorname{card} \mathrm{E}$.

Let $p \in \mathrm{I}_2$. In what follows, the set $\mathcal{A}_p = \{0, 1, \ldots, p-1\}$ is treated as the set of symbols. A bisequence over $\mathcal{A}_p$ is a mapping from I to $\mathcal{A}_p$.

Let $\Sigma_p = \{x = (\ldots x_{-1}x_0x_1\ldots) \,|\, x_i \in \mathcal{A}_p,\ i \in \mathrm{I}\}$ be the set of all bisequences over $\mathcal{A}_p$. For any $x \in \Sigma_p$ and any $i \in \mathrm{I}$ let $(x)_i = x_i$.

A metrics d on Σ_p is defined as follows. Let $x, y \in \Sigma_p$. Then

$$d(x,y) = \begin{cases} 0 & \text{if } x = y, \\ (1+k)^{-1} & \text{if } x \neq y, \end{cases},$$

where $k = \max\{m \in \mathrm{I}_0 \,|\, x_i = y_i \text{ for } |i| < m\}$.

It is easily verified that the metric topology induced by d coincides with the product topology induced by discrete topology of $\mathcal{A}_p$. Therefore Σ_p is a compact, totally disconnected, perfect, metric space and hence is homeomorphic

*The work was partially supported by the Russian Foundation for Basic Research (grant no. 07-01-00154 for the first, second and fourth author and grant no. 09-01-00653 for the first and third author).

[1]Information Security Institute, Lomonosov University, Moscow, Russia; E-mail: logol@iisi.msu.ru

[2]Information Security Institute, Lomonosov University, Moscow, Russia; E-mail: orfeo@rambler.ru

[3]Computer Science Department, Lomonosov University, Moscow, Russia; E-mail: smyshsv@gmail.com

[4]Information Security Institute, Lomonosov University, Moscow, Russia; E-mail: iisi@iisi.msu.ru

to the Cantor discontinuum. The shift transformation σ acts on Σ_p bijectively. The shift σ takes $x \in \Sigma_p$ to $y \in \Sigma_p$, where for any $i \in \mathrm{I}$

$$y_i = (y)_i = [\sigma(x)]_i = x_{i+1}.$$

The shift σ is a homeomorphism of Σ_p.

A symbolic dynamical system is a pair (S, σ), where S is a closed and shift-invariant (i.e., $\sigma(S) = S$) subset of Σ_p. Such a system is called also subshift. For example, (Σ_p, σ) is a symbolic dynamical system, often called the full shift, as opposed to all other shift, which are called subshifts and define embeddings into Σ_p.

Let S be a closed nonempty σ-invariant subset of Σ_p. Then the restriction of σ to S is a homeomorphism of S onto S. It is clear that S is a compact totally disconnected metric space.

Let (S_i, σ), $i = 1, 2$, be two subshifts ($S_i \subset \Sigma_{p_i}$, $i = 1, 2$). A continuous mapping $C\colon S_1 \to S_2$ is a code if $\sigma \circ C = C \circ \sigma$. An injective code is an embedding; a bijective code defines a topological conjugacy of subshifts is called isomorphism. In the case $S_1 = S_2 = S$ the code C is an endomorphism of the dynamical system (S, σ).

Let $n \in \mathrm{I}_1$. An n-block (word) over $\mathcal{A}_p$ is an ordered set $x_1 x_2 \dots x_n$, where $x_i \in \mathcal{A}_p$ ($i = 1, 2, \dots, n$). Let $\mathcal{B}_{n,p}$ denote the set of all n-blocks over $\mathcal{A}_p$.

Let $f\colon \mathcal{B}_{n,p} \to \mathcal{B}_{1,p} = \mathcal{A}_p$. The set of all such mappings for a given $n \in \mathrm{I}_1$ will be denoted by $\mathcal{F}_{n,p}$. Note that $\operatorname{card} \mathcal{B}_{n,p} = p^n$ and $\operatorname{card} \mathcal{F}_{n,p} = p^{p^n}$.

For any $f \in \mathcal{F}_{n,p}$, left $f_\infty\colon \Sigma_p \to \Sigma_p$ be a mapping of the form

$$f_\infty(x) = y, \quad y_i = f(x_i x_{i+1} \dots x_{i+n-1}),$$

where $x, y \in \Sigma_p$, $x_i, y_i \in \mathcal{A}_p$, $i \in \mathrm{I}$. It is easily verified that a mapping f_∞ is a code for $S_1 = S_2 = \Sigma_p$. It is usually called an n-block code.

In the case $S = \Sigma_p$ denote by $\mathcal{E}_p$ the set of all endomorphisms (codes) of symbolic dynamical system (Σ_p, σ).

Let $\mathcal{F}_p$ denote the set $\bigcup_{n=1}^{\infty} \mathcal{F}_{n,p}$ and let $\mathcal{F}_p^* = \{\sigma^m f_\infty \mid m \in \mathrm{I},\ f \in \mathcal{F}_p\}$.

The structure of endomorphism (code) set of full shift (Σ_p, σ) and its subshifts was described by Curtis, Hedlund, and Lyndon and can be summarized in the next theorem.

Theorem 1 ([7]). $\mathcal{E}_p = \mathcal{F}_p^*$.

2 Perfectly Balanced Functions

In what follows, we use the term "function" for elements of the set $\mathcal{F}_p$ only as opposed to all other mappings. This section recalls the general properties of perfectly balanced functions. We also need some notation and definitions.

Let $f \in \mathcal{F}_{n,p}$ and $m \in \mathrm{I}_1$. Define a mapping

$$f_m\colon \mathcal{B}_{m+n-1,p} \to \mathcal{B}_{m,p}$$

as follows:

$$f_m(b_1 b_2 \dots b_{m+n-1}) = a_1 a_2 \dots a_m,$$

where

$$a_i = f(b_i b_{i+1} \dots b_{i+n-1}), \quad i = 1, 2, \dots, m. \tag{1}$$

Let

$$J(f, m) = \{y \in \mathcal{B}_{m,p} \mid \forall\, x \in \mathcal{B}_{m+n-1,p}\ f_m(x) \neq y\}.$$

It is evident that $\operatorname{card} J(f, m) = \operatorname{Def}_m(f)$.

Definition 1. A function $f \in \mathcal{F}_{n,p}$ is called perfectly balanced if $\operatorname{card}(f_m^{-1})(y) = p^{n-1}$ for any $m \in \mathrm{I}_1$ and for every $y \in \mathcal{B}_{m,p}$.

Definition 2. A function $f \in \mathcal{F}_{n,p}$ is said to be of defect zero if $\operatorname{Def}_m(f) = 0$ for any $m \in \mathrm{I}_1$.

Let $b \in \mathcal{B}_{l,p}$ and $\mathrm{E} = \{j_1, j_2, \dots, j_k\} \subset \{1, 2, \dots, l\}, 1 \leq j_1 < \ldots < j_k \leq l, k \leq l$. We denote by $(b)_\mathrm{E}$ a string of the form $(b_{j_1} b_{j_2} \dots b_{j_k})$.

Definition 3. A function $f \in \mathcal{F}_{n,p}$ is called information-lossless if for any $l > 2n$ there do not exist two different blocks $b, b' \in \mathcal{B}_{l,p}$ such that

$$(b)_{\{1,2,\ldots,n\}} = (b')_{\{1,2,\ldots,n\}}, \quad (b)_{\{l-n+1,l-n+2,\ldots,l\}} = (b')_{\{l-n+1,l-n+2,\ldots,l\}},$$

and

$$f_{l-n+1}(b) = f_{l-n+1}(b').$$

Denote by $\mathcal{E}_p^\circ$ the set of all surjective mappings in $\mathcal{E}_p$. The structure of the set $\mathcal{E}_p^\circ$ is closely related to the set of perfectly balanced functions. The next statement is due to Blankenship, Hedlund, Rothaus, and Sumarokov.

Theorem 2 ([7, 8])**.** *Let $n \in \mathrm{I}_1$ and $f \in \mathcal{F}_{n,p}$. Then the following statements are equivalent:*

1. *f_∞ is a surjective endomorphism of (Σ_p, σ), i.e., $f_\infty \in \mathcal{E}_p^\circ$;*
2. *f is perfectly balanced;*
3. *f is of defect zero;*
4. *f is information-lossless.*

Let $n \in \mathrm{I}_2$ and let $f \in \mathcal{F}_{n,p}$. Let $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n (1 \le i \le n)$ be a collection of fixed elements of $\mathcal{A}_p$. Then

$$g(x_i) = f(a_1 \ldots a_{i-1} x_i a_{i+1} \ldots a_n)$$

defines a function g of $\mathcal{A}_p$ into $\mathcal{A}_p$, i.e., $g \in \mathcal{F}_{1,p}$. If for any $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ the function g is a permutation of $\mathcal{A}_p$, then we call f permutive in x_i. If $n = 1$, then f maps $\mathcal{A}_p$ into $\mathcal{A}_p$. A function f is permutive in x_i if its restriction to $\mathcal{A}_p$ is a permutation of $\mathcal{A}_p$.

Let $f \in \mathcal{F}_{p,n}$. A variable x_i $(1 \le i \le n)$ is called essential if there exist $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n, b, c \in \mathcal{A}_p$ such that $b \ne c$ and $f(a_1 \ldots a_{i-1} b a_{i+1} \ldots a_n) \ne f(a_1 \ldots a_{i-1} c a_{i+1} \ldots a_n)$.

Let M be a subset of $\mathcal{F}_{n,p}$. We denote the subset of all functions in M with essential variables x_1, x_n by $\widetilde{M}$. The subset of all perfectly balanced functions in $\mathcal{F}_{n,p}$ is denoted by $\mathcal{PBF}_{n,p}$. Furthermore, let $\mathcal{L}_{n,p}$ ($\mathcal{R}_{n,p}$) denote the subset of all functions in $\mathcal{F}_{n,p}$ that are permutive in x_1 (resp., x_n). It is easily verified that

$$\widetilde{\mathcal{L}}_{n,p} \subset \widetilde{\mathcal{PBF}}_{n,p}, \quad \widetilde{\mathcal{R}}_{n,p} \subset \widetilde{\mathcal{PBF}}_{n,p}. \tag{2}$$

In the remaining sections we study the structure of the set $\widetilde{\mathcal{PBF}}_{n,p} \setminus \left(\widetilde{\mathcal{L}}_{n,p} \cup \widetilde{\mathcal{R}}_{n,p}\right)$ in case $p = 2$.

3 Perfectly Balanced Boolean Functions

The set $\mathcal{PBF}_{n,2}$ is closed under the next operations on the set $\mathcal{F}_{n,2}$ [8]:

1. $\gamma_0 \colon f(x_1 \ldots x_n) \to f(x_1 \ldots x_n) \oplus 1$;
2. $\gamma_1 \colon f(x_1 \ldots x_n) \to f((x_1 \oplus 1) \ldots (x_n \oplus 1))$;
3. $\gamma_2 \colon f(x_1 \ldots x_n) \to f(x_n \ldots x_1)$.

Let ξ and η be two random variables with support in A and B, respectively, with joint probability distribution $p_{\xi,\eta}(x, y)$, marginal distribution $p_\xi(x)$ and $p_\eta(y)$, respectively, and conditional distribution $p_{\eta|\xi}(y|x)$ and $p_{\xi|\eta}(x|y)$ for $x \in \mathrm{A}$ and $y \in \mathrm{B}$, respectively. The Shannon entropy of ξ is defined by

$$H(\xi) = -\sum_{x \in \mathrm{A}} p_\xi(x) \log p_\xi(x).$$

All logarithms are to the base 2. We assume that $0 \log 0 = 0$. The joint Shannon entropy is defined as follows:

$$H(\xi, \eta) = -\sum_{x \in \mathrm{A}} \sum_{y \in \mathrm{B}} p_{\xi,\eta}(x, y) \log p_{\xi,\eta}(x, y).$$

The conditional Shannon entropy of η given ξ is

$$H(\eta|\xi) = -\sum_{x\in \mathrm{A}}\sum_{y\in \mathrm{B}} p_{\xi,\eta}(x,y)\log p_{\eta|\xi}(y|x).$$

Finally, the mutual information of ξ and η is

$$I(\eta,\xi) = I(\xi,\eta) = H(\xi) + H(\eta) - H(\xi,\eta) = H(\xi) - H(\xi|\eta) = H(\eta) - H(\eta|\xi).$$

Theorem 3 ([9]). *Let $n, m \in I_1$ and $f \in \mathcal{F}_{n,2}$. Let $\{\xi_m\}_{m=1}^{\infty}$ be a sequence of random variables with probability distributions*

$$\Pr[\xi_m = (a_1 \dots a_{m+n-1})] = 2^{-(m+n-1)}$$

for any $(a_1 \dots a_{m+n-1}) \in \mathcal{B}_{m+n-1,2}$ and any $m \in I_1$. A random variable $\eta_m = f_m(\xi_m)$ has a probability distribution

$$\Pr[\eta_m = (b_1 \dots b_m)] = 2^{-m}$$

for any $m \in I_1$ and any $(b_1 \dots b_m) \in \mathcal{B}_{m,2}$ iff $f \in \mathcal{PBF}_{n,2}$.

Theorem 4. *Let $f \in \mathcal{F}_{n,2}$. Under conditions of Theorem 3, let $i_m(f) = m^{-1}I(\eta_m, \xi_m)$. Then*

1. *f is perfectly balanced iff $i_m(f) = 1$ for any $m \in I_1$;*
2. *for any $g \in \mathcal{F}_{n,2}$ one has $i_m(g) \le i_m(f)$.*

Proof. Let $f \in \mathcal{F}_{n,2}$. Under conditions of Theorem 3 we have

$$\begin{aligned}
p_a &= \Pr[\xi_m = a] = 2^{-(m+n-1)} \quad \text{for any } a \in \mathcal{B}_{m+n-1,2};\\
p_{b/a} &= \Pr[\eta_m = b \,|\, \xi_m = a] = \begin{cases} 1 & \text{if } a \in f_m^{-1}(b),\\ 0 & \text{if } a \notin f_m^{-1}(b);\end{cases}\\
p_{b,a} &= \Pr[\eta_m = b,\, \xi_m = a] = p_a p_{b/a} = \begin{cases} 2^{-(m+n-1)} & \text{if } a \in f_m^{-1}(b),\\ 0 & \text{if } a \notin f_m^{-1}(b);\end{cases}\\
q_b &= \Pr[\eta_m = b] = 2^{-(m+n-1)}\operatorname{card} f_m^{-1}(b)
\end{aligned}$$

for any $b \in \mathcal{B}_{m,2}$. Then one has

$$\begin{aligned}
i_m(f) &= m^{-1}I(\eta_m,\xi_m) = m^{-1}[H(\eta_m) - H(\eta_m|\xi_m)]\\
&= m^{-1}\sum_{b\in\mathcal{B}_{m,2}}\sum_{a\in f_m^{-1}(b)} p_{b,a}[\log p_{b/a} - \log q]\\
&= m^{-1}\sum_{b\in\mathcal{B}_{m,2}}\sum_{a\in f_m^{-1}(b)} 2^{-(m+n-1)}[(m+n-1) - \log(\operatorname{card} f_m^{-1}(b))]\\
&= m^{-1}\sum_{b\in\mathcal{B}_{m,2}} \operatorname{card} f_m^{-1}(b) 2^{-(m+n-1)}[(m+n-1) - \log(\operatorname{card} f_m^{-1}(b))]\\
&= m^{-1}\Bigg[(m+n-1)\\
&\qquad - 2^{-(m+n-1)}\sum_{b\in\mathcal{B}_{m,2}} \operatorname{card} f_m^{-1}(b)\log(\operatorname{card} f_m^{-1}(b))\Bigg]. \qquad (3)
\end{aligned}$$

1. Let $f \in \mathcal{PB}_{n,2}$. Then $\operatorname{card} f_m^{-1}(b) = 2^{n-1}$ for any $b \in \mathcal{B}_{m,2}$ and any $m \in I_1$. From (3) one has $i_m(f) = 1$ for any $m \in I_1$.

To prove the opposed implication, let $f \in \mathcal{F}_{n,2}$ and $i_m(f) = 1$ for any $m \in I_1$. Then (3) implies

$$2^{-(m+n-1)}\sum_{b\in\mathcal{B}_{m,2}} \operatorname{card} f_m^{-1}(b)\log(\operatorname{card} f_m^{-1}(b)) = n-1.$$

Hence,

$$-\sum_{b\in\mathcal{B}_{m,2}}\frac{\operatorname{card} f_m^{-1}(b)}{2^{m+n-1}}\log\left(\frac{\operatorname{card} f_m^{-1}(b)}{2^{m+n-1}}\right)=m. \tag{4}$$

Moreover,

$$\sum_{b\in\mathcal{B}_{m,2}}\frac{\operatorname{card} f_m^{-1}(b)}{2^{m+n-1}}=1 \tag{5}$$

Thus (4) holds if and only if $\operatorname{card} f_m^{-1}(b)/2^{m+n-1}=2^{-m}$ for any $b\in\mathcal{B}_{m,2}$ [10]. For an arbitrary positive integer m one has $\operatorname{card} f_m^{-1}(b)=2^{n-1}$ for any $b\in\mathcal{B}_{m,2}$ and any $m\in I_1$. Thus $f\in\mathcal{PBF}_{n,2}$.

2. Let $g\in\mathcal{F}_{n,2}$ and $f\in\mathcal{PBF}_{n,2}$. Then

$$\begin{aligned}
&i_m(f)-i_m(g)\\
&\quad=m^{-1}[2^{-(m+n-1)}\sum_{b\in\mathcal{B}_{m,2}}\operatorname{card} g_m^{-1}(b)\log(\operatorname{card} g_m^{-1}(b))-(n-1)]\\
&\quad=m^{-1}\left[\sum_{b\in\mathcal{B}_{m,2}}\frac{\operatorname{card} g_m^{-1}(b)}{2^{m+n-1}}\log(\operatorname{card} g_m^{-1}(b))\right.\\
&\qquad\qquad\left.-\sum_{b\in\mathcal{B}_{m,2}}\frac{\operatorname{card} g_m^{-1}(b)}{2^{m+n-1}}\log(2^{n-1})\right]\\
&\quad=m^{-1}\left[\sum_{b\in\mathcal{B}_{m,2}}\frac{\operatorname{card} g_m^{-1}(b)}{2^{m+n-1}}\log\left(\frac{\operatorname{card} g_m^{-1}(b)}{2^{m+n-1}}\Big/\frac{2^{n-1}}{2^{m+n-1}}\right)\right].
\end{aligned} \tag{6}$$

The next inequality is well-known (see [10]). Let $\alpha_j,\beta_j,j=1,\dots,s$ be nonnegative real numbers such that $\sum_{j=1}^s\alpha_j=\sum_{j=1}^s\beta_j=1$. Then

$$\sum_{j=1}^s\alpha_j\log\alpha_j\ge\sum_{j=1}^s\alpha_j\log\beta_j \tag{7}$$

Combining (5), (6) for Boolean function g, and (7), one gets $i_m(f)-i_m(g)\ge 0$. □

For a pair of positive integers m,k, a mapping $\Xi_{m,k}\colon\mathcal{F}_{m,2}\times\mathcal{F}_{k,2}\to\mathcal{F}_{m+k-1,2}$ is defined as follows:

$$\Xi_{m,k}(g,h)=g[h]=f\in\mathcal{F}_{m+k-1,2},\quad g\in\mathcal{F}_{m,2},\ h\in\mathcal{F}_{k,2}, \tag{8}$$

where

$$\begin{aligned}
f(x_1\dots x_{m+k-1})&=g[h](x_1\dots x_{m+k-1})\\
&=g(h(x_1\dots x_k)h(x_2\dots x_{k+1})\dots h(x_m\dots x_{m+k-1})).
\end{aligned}$$

Theorem 5 ([11]). *Let $g\in\mathcal{F}_{m,2}$, $h\in\mathcal{F}_{k,2}$. The function $f=g[h]\in\mathcal{F}_{m+k-1,2}$ is perfectly balanced iff g and h are perfectly balanced.*

Theorem 5 allows one to generate functions in $\mathcal{PBF}_{n,2}\setminus(\mathcal{L}_{n,2}\cup\mathcal{R}_{n,2})$.

We consider integer sequences $\gamma=(\gamma_1\dots\gamma_n)$ such that

$$\gamma_1=0,\quad\forall\, i\in\{1,\dots,n-1\}\ \gamma_{i+1}>\gamma_i,\quad N=\gamma_n+1.$$

These sequences correspond to tapping sequences of filter generators. For any $f\in\widetilde{\mathcal{F}}_{n,2}$, let $f_\gamma(x_1\dots x_N)\equiv f(x_{N-\gamma_n}x_{N-\gamma_{n-1}}\dots x_{N-\gamma_1})$.

Golić [3] stated the next theorem:

Theorem 6 ([3]). *For a nonlinear filter generator with the filter function f_γ and independent of the tapping sequence γ, the output sequence is purely random given that the input sequence is such if (and only if [not proven]) $f\in(\mathcal{L}_{N,2}\cup\mathcal{R}_{N,2})$.*

The "if" part of Theorem 6 was proven in [3]. The next statement can help to prove the "only if" part.

Theorem 7. *For any $f \in \widetilde{\mathcal{F}}_{n,2}$ which has no linear arguments there exists a sequence γ such that $f_\gamma \notin \mathcal{PBF}_{N,2}$.*

Proof. Consider a sequence γ such that $\gamma_1 = 0$ and $\gamma_{i+1} > 2\gamma_i$ for each $i \in \{1, \dots, n-1\}$. The system of equations

$$\begin{cases} f(x_{N-\gamma_n-1}x_{N-\gamma_{n-1}-1}\dots x_{N-\gamma_2-1}x_{N-\gamma_1-1}) \\ \qquad = f(z_{N-\gamma_n-1}z_{N-\gamma_{n-1}-1}\dots z_{N-\gamma_2-1}z_{N-\gamma_1-1}), \\ f(x_{N-\gamma_n}x_{N-\gamma_{n-1}}\dots x_{N-\gamma_2}x_{N-\gamma_1}) \\ \qquad = f(z_{N-\gamma_n}z_{N-\gamma_{n-1}}\dots z_{N-\gamma_2}z_{N-\gamma_1}), \\ f(x_{N-\gamma_n+1}x_{N-\gamma_{n-1}+1}\dots x_{N-\gamma_2+1}x_{N-\gamma_1+1}) \\ \qquad = f(z_{N-\gamma_n+1}z_{N-\gamma_{n-1}+1}\dots z_{N-\gamma_2+1}z_{N-\gamma_1+1}), \\ \dots \\ f(x_{N-\gamma_1}x_{N-\gamma_1+\gamma_n-\gamma_{n-1}}\dots x_{N-2\gamma_1+\gamma_n}) \\ \qquad = f(z_{N-\gamma_1}z_{N-\gamma_1+\gamma_n-\gamma_{n-1}}\dots z_{N-2\gamma_1+\gamma_n}), \\ f(x_{N-\gamma_1+1}x_{N-\gamma_1+\gamma_n-\gamma_{n-1}+1}\dots x_{N-2\gamma_1+\gamma_n+1}) \\ \qquad = f(z_{N-\gamma_1+1}z_{N-\gamma_1+\gamma_n-\gamma_{n-1}+1}\dots z_{N-2\gamma_1+\gamma_n+1}), \\ x_{N-\gamma_n-1} = z_{N-\gamma_n-1}, \\ x_{N-\gamma_n} = z_{N-\gamma_n}, \\ \dots \\ x_{N-\gamma_1-1} = z_{N-\gamma_1-1}, \\ x_{N-\gamma_1} = 0,\ z_{N-\gamma_1} = 1, \\ x_{N-\gamma_1+1} = z_{N-\gamma_1+1}, \\ x_{N-\gamma_1+2} = z_{N-\gamma_1+2}, \\ \dots \\ x_{N-2\gamma_1+\gamma_n+1} = z_{N-2\gamma_1+\gamma_n+1}. \end{cases} \tag{9}$$

is solvable. Indeed, all equations that do not depend on $x_{N-\gamma_1}$ and $z_{N-\gamma_1}$ evidently hold. Therefore one has to solve the system

$$\begin{cases} f(x_{N-\gamma_n+\gamma_1}x_{N-\gamma_{n-1}+\gamma_1}\dots x_{N-\gamma_2+\gamma_1}0) \\ \qquad = f(x_{N-\gamma_n+\gamma_1}x_{N-\gamma_{n-1}+\gamma_1}\dots x_{N-\gamma_2+\gamma_1}1), \\ f(x_{N-\gamma_n+\gamma_2}x_{N-\gamma_{n-1}+\gamma_2}\dots x_{N-\gamma_3+\gamma_2}0x_{N-\gamma_1+\gamma_2}) \\ \qquad = f(x_{N-\gamma_n+\gamma_2}x_{N-\gamma_{n-1}+\gamma_2}\dots x_{N-\gamma_3+\gamma_2}1x_{N-\gamma_1+\gamma_2}), \\ \dots \\ f(0x_{N-\gamma_{n-1}+\gamma_n}\dots x_{N-\gamma_1+\gamma_n}) \\ \qquad = f(1x_{N-\gamma_{n-1}+\gamma_n}\dots x_{N-\gamma_1+\gamma_n}). \end{cases} \tag{10}$$

Every equation in this system is solvable because f does not have linear arguments. Next, we show that jth and lth equations are independent. This amounts to show:

$$\begin{aligned} &\forall\, i,j,k,l \in \{1,\dots,n\}\ i \neq j,\ k \neq l,\ i \neq k,\ j \neq l \\ &\qquad \Longrightarrow\ N - \gamma_i + \gamma_j \neq N - \gamma_k + \gamma_l. \end{aligned} \tag{11}$$

It can be easily verified that it suffices to show for each $i \in \{1, \dots, n-1\}$, for all $j \leq i$, $k \leq i$, l that $\gamma_{i+1} - \gamma_j > \gamma_k - \gamma_l$ holds. We have chosen a sequence γ such that for each $i \in \{1, \dots, n-1\}$ inequality $\gamma_{i+1} > 2\gamma_i$ holds. Therefore $\gamma_{i+1} - \gamma_j > \gamma_i + (\gamma_i - \gamma_j) \geq \gamma_i \geq \gamma_i - \gamma_l \geq \gamma_k - \gamma_l$.

System (11) has n independent equations each of which is solvable. Thus systems (10) and (9) are solvable. By Theorem 2 one has $f_\gamma \notin \mathcal{PBF}_{N,2}$. □

To prove the "only if" part (the Golić conjecture), one has to handle linear arguments of f and solve "an underlying combinatorial problem" mentioned by Golić.

4 Barriers of Boolean Functions

A barrier of a Boolean function is closely related to the property of perfect balancedness.

Definition 4 ([12]). A Boolean function $f \in \mathcal{F}_{n,2}$ has a right barrier of length b if the system

$$\begin{cases} f(y_1y_2\dots y_n) = f(z_1z_2\dots z_n), \\ f(y_2y_3\dots y_{n+1}) = f(z_2z_3\dots z_{n+1}), \\ \dots \\ f(y_{b-1}y_b\dots y_{b+n-2}) = f(z_{b-1}z_b\dots z_{b+n-2}), \\ y_1 = z_1 = x_1, \dots, y_{n-1} = z_{n-1} = x_{n-1},\ y_n = 0,\ z_n = 1. \end{cases} \tag{12}$$

is solvable, but the system

$$\begin{cases} f(y_1y_2\dots y_n) = f(z_1z_2\dots z_n), \\ f(y_2y_3\dots y_{n+1}) = f(z_2z_3\dots z_{n+1}), \\ \dots \\ f(y_{b-1}y_b\dots y_{b+n-2}) = f(z_{b-1}z_b\dots z_{b+n-2}), \\ f(y_by_{b+1}\dots y_{b+n-1}) = f(z_bz_{b+1}\dots z_{b+n-1}), \\ y_1 = z_1 = x_1, \dots, y_{n-1} = z_{n-1} = x_{n-1},\ y_n = 0,\ z_n = 1. \end{cases} \tag{13}$$

is not solvable.

A Boolean function $f \in \mathcal{F}_{n,2}$ has a left barrier of length b if $f^{\gamma_2}(x_1\dots x_n) \equiv f(x_n\dots x_1)$ has a right barrier of length b.

A Boolean function $f \in \mathcal{F}_{n,2}$ has a barrier if it has a right barrier, a left barrier, or both. The length of a Boolean function barrier is defined to be the minimum of the length of its right and left barrier.

Theorem 8. *If a Boolean function has a barrier, then it is perfectly balanced. An opposed implication does not hold.*

Proof. If a function has left or right barrier, then it is easily verified using the definition of barrier and Theorem 6 that the function is perfectly balanced.

Now we give an example of a perfectly balanced function without barrier. Let $f(x_1x_2x_3x_4x_5) = x_1 \oplus x_2 \oplus x_5 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_4x_5 \oplus x_1x_3x_4 \oplus x_2x_3x_4 = g^{\gamma_2}[g]$, where $g(x_1x_2x_3) = x_1 \oplus x_2 \oplus x_3 \oplus x_2x_3$, $g^{\gamma_2}(x_1x_2x_3) \equiv g(x_3x_2x_1)$. The function g has a left barrier of length $k = 1$, hence $g, g^{\gamma_2} \in \mathcal{PBF}_{3,2}$. Using Theorem 5 one concludes that $f \in \mathcal{PBF}_5$. To show that f does not have a barrier, we use next two pairs of binary sequences:

$$\begin{bmatrix} 0001(010100)(010100)(010100)\dots \\ 0001(100010)(100010)(100010)\dots \end{bmatrix}, \tag{14}$$

$$\begin{bmatrix} \dots(00111110)(00111110)(00111110)000100 \\ \dots(11100011)(11100011)(11100011)010100 \end{bmatrix}. \tag{15}$$

For any $k > 0$ one can make pair (14) to have length more than $k + 3$ by repeating periodical parts of the sequences sufficiently many times and then truncating the sequences obtained to exact length. Then one substitutes the sequences in (12) and (13). Eqs. (12) and (13) hold, hence no k can satisfy Definition 4 and f has no right barrier. Similarly one can show that f has no left barrier. □

The next theorem can be used for classification of Boolean functions with a right (left) barrier.

Theorem 9 ([12]). *Let $f \in \mathcal{F}_{n,2}$ be a function with a right (left) barrier of length $b < n$ and $g \in \mathcal{F}_{n-b,2}$ be arbitrary. Then $h(x_1\dots x_n) = f(x_1\dots x_n) \oplus g(x_1\dots x_{n-b})$ (resp., $h(x_1\dots x_n) = f(x_1\dots x_n) \oplus g(x_{b+1}\dots x_n)$) has a right (resp., left) barrier of length b.*

The proof of this theorem is easy and follows from (12) and (13).

Barrier length is a value that characterizes, in a particular way, invertibility of mapping f_m. In the proof of Theorem 8 we show that composition of functions $g^{\gamma_2}[g]$ is a function without barrier. One can show that g does not have a right barrier and g^{γ_2} does not have a left barrier.The next theorem answers the question of existence of right and left barrier of a composition function $g[h]$. We assume that length of a right (left) barrier is $+\infty$ if a function does not have right (left) barrier.

Theorem 10. *Let $h \in \mathcal{F}_{k,2}$, $g \in \mathcal{F}_{m,2}$, $f = g[h]$ and length of right (left) barrier of functions h, g, f are b, c, d, respectively. Then* $\max\{b, c\} \le d \le b + c - 1$

Now we outline ideas behind the proof. Inequalities $d \geq b$ and $d \leq b + c - 1$ (both in the case of finite b, c, d and in the case when some of b, c, d is infinite) are proved by analysing systems produced from (12), (13) by substituting values of h taken on the corresponding vectors into g. In this way we get inequalities $d \geq b$ and $b + c - 1 \geq d$. To prove inequality $d \geq c$ we use Lemma 1 whose proof is based on some special properties of perfectly balanced Boolean functions.

Lemma 1. *Let $f \in \mathcal{PBF}_{n,2}$. Then for any positive integer u and for any binary sequences $z_0, z_1 \in \mathcal{B}_{u,2}$ there exist a positive integer r and binary sequences $x, y \in \mathcal{B}_{r+n-1,2}, z \in \mathcal{B}_{r-u,2}$ such that*

$$x_1 = y_1, \ldots, x_{n-1} = y_{n-1},\ f^*(x) = (z|z_0),\ f^*(y) = (z|z_1).$$

Finally, we show an example of method of a class of perfectly balanced functions without barriers.

Lemma 2. *Functions*

$$\begin{aligned} f = {} & x_1 \oplus x_{m_1^\circ} x_{m_1^\circ+1} \ldots x_{m_1} h_1(x_{m_1+1} x_{m_1+2} \ldots x_{m_k}) \\ & \oplus x_{m_2^\circ} x_{m_2^\circ+1} \ldots x_{m_2} h_2(x_{m_2+1} x_{m_2+2} \ldots x_{m_k}) \oplus \ldots \\ & \oplus x_{m_k^\circ} x_{m_k^\circ+1} \ldots x_{m_k}, \quad 1 < m_1^\circ < m_1 < m_2^\circ < m_2 < \ldots < m_k^\circ < m_k, \end{aligned} \tag{16}$$

where h_i are product terms and k is odd are perfectly balanced functions without right barrier.

Proof. All such functions are in $\mathcal{L}_{n,2}$ and therefore in $\mathcal{PBF}_{n,2}$. To prove that such a function has no right barrier consider for any positive integer b the following pair of binary sequences:

$$\begin{array}{cccccc} \underbrace{\begin{array}{c}00\ldots0\\00\ldots0\end{array}}_{m_k-1} & \underbrace{\begin{array}{c}101\ldots0\\010\ldots1\end{array}}_{m_k^\circ-m_{k-1}^\circ} & \underbrace{\begin{array}{c}000\ldots0\\000\ldots0\end{array}}_{m_{k-1}^\circ-m_{k-2}^\circ} & \underbrace{\begin{array}{c}010\ldots0\\101\ldots1\end{array}}_{m_{k-2}^\circ-m_{k-3}^\circ} & \cdots & \\ \cdots & \underbrace{\begin{array}{c}010\ldots0\\101\ldots1\end{array}}_{m_3^\circ-m_2^\circ} & \underbrace{\begin{array}{c}000\ldots0\\000\ldots0\end{array}}_{m_2^\circ-m_1^\circ} & \underbrace{\begin{array}{c}101\ldots0\\010\ldots1\end{array}}_{m_1^\circ-1} & \underbrace{\begin{array}{c}11\ldots1\\00\ldots0\end{array}}_{b-m_k-m_k^\circ+2} & . \end{array}$$

Substituting this pair of sequences into systems of Definition 4 one can see f has no right barrier of length at most b. Since this holds for any b, f doesn't have right barrier. □

Now using Lemma 2 and Theorem 10 we can describe a large class of perfectly balanced functions without barriers.

Theorem 11. *Let f_1, f_2 be of the form* (16) *or be produced by applying to such functions operations $\gamma_1 \colon f(x_1 \ldots x_n) \to f((x_1 \oplus 1) \ldots (x_n \oplus 1))$. Then $f_1[f_2^{\gamma_2}]$ and $f_1^{\gamma_2}[f_2]$ are perfectly balanced functions without barriers.*

References

[1] F.P. Preparata, Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties, *IEEE Trans. Electron. Comput.* **15**(6) (1966), 898–909.

[2] D. A. Huffman, Canonical forms for information-lossless finite-state logical machines, *IRE Trans. Circuit Theory* **5** (1959), spec. suppl., 41–59.

[3] J.Dj. Golić, On the security of nonlinear filter generators, *Proc. of Fast Software Encryption 1996, Lecture Notes in Computer Science* **1039** (1996), Springer-Verlag, 173–188.

[4] A. Gouget and H. Sibert, Revisiting correlation-immunity in filter generators, *Proc. of SAC 2007, Lecture Notes in Computer Science* **4876** (2007), Springer-Verlag, 378–395.

[5] D. Lind and B. Marcus, *An Introduction to Symbolic Dynamics and Coding*, Cambridge University Press, Cambridge, 1995.

[6] B.R. Kitchens, *Symbolic Dynamics, One-sided, Two-sided, Countable State Markov Shifts*, Springer-Verlag, Berlin, 1998.

[7] G.A. Hedlund, Endomorphisms and automorphisms of the shift dynamical system, *Math. Systems Th.* **3** (1969) 320–375.

[8] S.N. Sumarokov, Functions of defect zero and invertability of some class of finite-memory encoders, *Obozrenie prom. i prikl. mat.* **1**(1) (1994) 33–55 (in Russian).

[9] O.A. Logachev, A.A. Salnikov, and V.V. Yashchenko, *Boolean Functions in Coding Theory and Cryptology*, MCCME, Moscow, 2004 (in Russian).

[10] R. Ash, *Information Theory*, John Wiley and Sons Inc., New York–London–Sydney, 1967.

[11] O.A. Logachev, On perfectly balanced Boolean functions, Cryptology ePrint Archive, Report 2007/022, `http://eprint.iacr.org/`.

[12] O.A. Logachev, S.V. Smyshlyaev, and V.V. Yashchenko, New approach to perfectly balanced functions design, *Discrete Mathematics* **21**(2) (2009), 51-74 (in Russian).

5 Appendix

Sets of $\widetilde{\mathcal{PBF}}_{4,2} \setminus (\mathcal{L}_{4,2} \cup \mathcal{R}_{4,2})$ and $\widetilde{\mathcal{PBF}}_{5,2} \setminus (\mathcal{L}_{5,2} \cup \mathcal{R}_{5,2})$ are divided into classes of equivalence by operations $\gamma_0 - \gamma_2$. These classes are subdivided into subsets by barrier length, which are later classificated by operations noted in Theorem 9. Then we choose one element from each class such that length of barrier is equal to length of right barrier.

$\widetilde{\mathcal{PBF}}_{4,2} \setminus (\mathcal{L}_{4,2} \cup \mathcal{R}_{4,2})$ with barrier of length $k = 3$:

$$
\begin{aligned}
&1\ f(x_1, x_2, x_3, x_4) = x_3 \oplus x_4x_2 \oplus x_4x_2x_1\\
&2\ f(x_1, x_2, x_3, x_4) = x_3 \oplus x_4x_1 \oplus x_4x_2x_1\\
&3\ f(x_1, x_2, x_3, x_4) = x_3 \oplus x_2 \oplus x_4x_2 \oplus x_3x_2 \oplus x_4x_2x_1 \oplus x_3x_2x_1\\
&4\ f(x_1, x_2, x_3, x_4) = x_3 \oplus x_4x_2 \oplus x_3x_2 \oplus x_2x_1 \oplus x_4x_2x_1 \oplus x_3x_2x_1
\end{aligned}
$$

Functions in remaining part of Appendix are presented with ANF coefficients vector.

$\widetilde{\mathcal{PBF}}_{5,2} \setminus (\mathcal{L}_{5,2} \cup \mathcal{R}_{5,2})$ with barrier of length $k = 3$:

f_1 : 00100000000000000000000001000100; f_2 : 00100000000000000000010000000100; f_3 : 00100000000000000100000001000000;
f_4 : 00100000000001000000000000000100; f_5 : 00100100000001000000000010000000; f_6 : 00100000000010000000000001000100;
f_7 : 00100000010001000000000000001000; f_8 : 00100000000000000000000001001100; f_9 : 00100000010001000000000010000000;
f_{10} : 00100000000000000100000001001000; f_{11} : 00100100000001000000000000001000; f_{12} : 00100000000000000000010000001100;
f_{13} : 00100000000000000100100001000000; f_{14} : 00100100000001000000100000000000; f_{15} : 00100000000000000000110000000100;
f_{16} : 00100000000000000000011000001100; f_{17} : 00100000000011000000000000001100; f_{18} : 00100000000000000100100001001000;
f_{19} : 00101000000010000000010000000100; f_{20} : 00101000000001000000100000000100; f_{21} : 00100100000001000000010001000000;
f_{22} : 00100000000011000000100000000100; f_{23} : 00101000000001000000000000001100; f_{24} : 00100000000001000100010001000000;
f_{25} : 00100000000001000000100000001100; f_{26} : 00101000000011000000000000000100; f_{27} : 00100000000010000000000001001100;
f_{28} : 00101000000000000000100001000100; f_{29} : 00100000010011000000000000001000; f_{30} : 00101000010001000000100000000000;
f_{31} : 00101000000001100000000000000110; f_{32} : 00101000011000000000000001100000; f_{33} : 00101000000000000000011000000110;
f_{34} : 00101000000000000000000001100110; f_{35} : 00101000010001000010000000100000; f_{36} : 00101000000000000000100001001100;
f_{37} : 00101000010001000010000000000010; f_{38} : 00101000000010000000100001000100; f_{39} : 00100100000001000000010001001000;
f_{40} : 00100000010001000010100000100000; f_{41} : 00100000011001100000100000000000; f_{42} : 00100000000000000000100001100110;
f_{43} : 00100000010001000010100000000010; f_{44} : 00100000010010100000000001000010; f_{45} : 00100000010011000000000001000100;
f_{46} : 00100000000000000100110001000100; f_{47} : 00100000011000000000100001100000; f_{48} : 00100000000001100000100000000110;
f_{49} : 00101000000010000000110000000100; f_{50} : 00101000000010000000010000001100; f_{51} : 00101100000011000000000000001000;
f_{52} : 00101100001001000000000000100000; f_{53} : 00100000000010000100001001000010; f_{54} : 00100000000010000000011000000110;
f_{55} : 00100000000011100000000000000110; f_{56} : 00100000010000100000000001001010; f_{57} : 00100000000001100000000000001110;
f_{58} : 00100000000011000100010001001000; f_{59} : 00101100001001000000000000101000; f_{60} : 00100000010001000010100000001010;
f_{61} : 00101000010011000010000000000010; f_{62} : 00101000000010000000100001001100; f_{63} : 00100000011001100000100000001000;
f_{64} : 00100000000000000000100001101110; f_{65} : 00101100001001000000100000100000; f_{66} : 00101000000010000000000001100110;

f_{67} : 00100000000010000000011000001110; f_{68} : 00101000000000000000111000000110; f_{69} : 00100000000010000100001001001010;
f_{70} : 00100100001011000000000000101000; f_{71} : 00100000000010000000111000000110; f_{72} : 00100110000011100000100000000000;
f_{73} : 00101110000001100000000000001000; f_{74} : 00101000000000000000111000001110; f_{75} : 00101000000000000110000001101000;
f_{76} : 00100000000010000100101001000010; f_{77} : 00100000000001000100110001001000; f_{78} : 00100000010011000010100000000010;
f_{79} : 00101000010001000010000000001010; f_{80} : 00100000000010000000100001100110; f_{81} : 00101000000000000000000001101110;
f_{82} : 00101000011001100000000000001000; f_{83} : 00101000010001000010000000101000; f_{84} : 00101000011001100000000010000000;
f_{85} : 00100110000011100000000010000000; f_{86} : 00100000000010000100101001001010; f_{87} : 00100000000011100000100000001110;
f_{88} : 00100000000010000000111000001110; f_{89} : 00100000000010000000100001101110; f_{90} : 00101000011001100010000000000010;
f_{91} : 00101000010000100000100001001010; f_{92} : 00101000011001100010000000100000; f_{93} : 00101000000001100000100000001110;
f_{94} : 00101110000001100000100000001000; f_{95} : 00101000000000000000111000001110; f_{96} : 00101000000000000110100001101000;
f_{97} : 00101000010011000010000000101000; f_{98} : 00100000011001100010100000000010; f_{99} : 00100000010011000010100000001010;
f_{100} : 00101000000010000000000000001101110; f_{101} : 00100100000001000000110001100010; f_{102} : 00101000010011000010000000001010;
f_{103} : 00100000011001100010100000100000; f_{104} : 00100000000001100100110001000010; f_{105} : 00101000000011100000000000001110;
f_{106} : 00101100001001000000001000100010; f_{107} : 00100100001011000000001000100010; f_{108} : 00100110001011100000000000100000;
f_{109} : 00100000000011100100010001000010; f_{110} : 00100000000001100100010001001010; f_{111} : 00101000010010100000100001000010;
f_{112} : 00101000000011100000100000000110; f_{113} : 00100000011001100010100000101000; f_{114} : 00101100001001000000101000100010;
f_{115} : 00101100000011000000110001001000; f_{116} : 00101000011011100010000000000010; f_{117} : 00101100000011000000010001100010;
f_{118} : 00100110001011100000100000100000; f_{119} : 00101100001001000000001000101010; f_{120} : 00100100000001000000110001101010;
f_{121} : 00100100001011000000101000100010; f_{122} : 00101110001001100000000000101000; f_{123} : 00101000011001100010000000101000;
f_{124} : 00101000000001100110011001100000; f_{125} : 00101110000001100000011001100000; f_{126} : 00100000000011100100110001001010;
f_{127} : 00101100000011000000010001101010; f_{128} : 00101000011011100010000000101000; f_{129} : 00100110000011100000111001100000;
f_{130} : 00101110000001100000011001101000; f_{131} : 00101000000001100110111001101000; f_{132} : 00101000000011100110111001100000;

$\widetilde{\mathcal{PBF}}_{5,2} \setminus (\mathcal{L}_{5,2} \cup \mathcal{R}_{5,2})$ with barrier of length $k = 4$:

f_1 : 00100000000000000100000000000100; f_2 : 00100000000000000100000000001100; f_3 : 00100000000000000100000010000100;
f_4 : 00100000000000000100000010001100; f_5 : 00100000100000000100100000000100; f_6 : 00101000000000000110000000000110;
f_7 : 00100000100000000100000000100110; f_8 : 00100000100000000100100010000100; f_9 : 00100000000010000100001000000110;
f_{10} : 00100000100000000100100000001100; f_{11} : 00100000000000000100100000100110; f_{12} : 00100000000000000100100000101110;
f_{13} : 00100000000000000100100010100110; f_{14} : 00100000100010000100001000100100; f_{15} : 00101000000010000110001000000100;
f_{16} : 00100100010100000000000000101010100; f_{17} : 00101000100000000110000000100100; f_{18} : 00100000100000000100000010100110;
f_{19} : 00101000000000000110000000001110; f_{20} : 00100000000010000100101000100100; f_{21} : 00100000000010000100001010000110;
f_{22} : 00101000000000000110100000100100; f_{23} : 00100000000010000100001000001110; f_{24} : 00100000100000000100100010001100;
f_{25} : 00100000100000000100000000101110; f_{26} : 00101000000000000110000010000110; f_{27} : 00101000000000000110000010001110;
f_{28} : 00100000000010000100101010100100; f_{29} : 00100000100000000100000010101110; f_{30} : 00100000000010000100101000101100;
f_{31} : 00101000000000000110100000101100; f_{32} : 00101000011001100001000000010000; f_{33} : 00101000000000000110100010100100;
f_{34} : 00100000000000000100100010101110; f_{35} : 00101000000010000110001010000100; f_{36} : 00100000100010000100001000101100;
f_{37} : 00101000100000000110100000000110; f_{38} : 00101000100000000110000010100100; f_{39} : 00100000100010000100101000000110;
f_{40} : 00101000100000000110000000101100; f_{41} : 00100000000010000100001010001110; f_{42} : 00101000000010000110001000001100;
f_{43} : 00100000100010000100001010100100; f_{44} : 00100000011001100001100000010000; f_{45} : 00100000011001100001100000011000;
f_{46} : 00100000100010000100001010101100; f_{47} : 00100000011001100001100010010000; f_{48} : 00101000100000000110100010000110;
f_{49} : 00101000000010000110001010001100; f_{50} : 00100100110100000000100001010100; f_{51} : 00101000100000000110100000001110;
f_{52} : 00100000100010000100101000001110; f_{53} : 00100000010001000101010001010100; f_{54} : 00100000100010000100101010000110;
f_{55} : 00101100010110000000000000001010100; f_{56} : 00100100010100000000100001011100; f_{57} : 00100100110100000000000011010100;
f_{58} : 00101000011001100001000000011000; f_{59} : 00101000000000000110100010101100; f_{60} : 00101000100000000110000010101100;
f_{61} : 00101000011001100001000010010000; f_{62} : 00101000100010000110101000000100; f_{63} : 00100000000010000100101010101100;
f_{64} : 00100100010100000000100011010100; f_{65} : 00100100110100000000000001011100; f_{66} : 00100100010100000000000011011100;

f_{67} : 0010100010001000011010100000 1100; f_{68} : 0010010011010010000000000 1010110; f_{69} : 0010100010001000011010101000 0100;
f_{70} : 0010111001010110000000000 1010000; f_{71} : 0010100011101110000100000001 0000; f_{72} : 0010100001100110000100001001 1000;
f_{73} : 0010100010001000011000100010 0110; f_{74} : 0010010001010010000000001 1010110; f_{75} : 0010011001010100000000001 1010010;
f_{76} : 0010011011010100000000000 1010010; f_{77} : 0010000011101110000110000001 0000; f_{78} : 0010000001100110000110001001 1000;
f_{79} : 0010000001000100010101000 1011100; f_{80} : 0010000010001000010010101000 1110; f_{81} : 0010100000001000011010100010 0110;
f_{82} : 0010000001000100010101001 1010100; f_{83} : 0010000001100110001110000011 0000; f_{84} : 0010100010000000011010001000 1110;
f_{85} : 0010010001010010000000000 1011110; f_{86} : 0010010001010010000010000 1010110; f_{87} : 0010011001011110000000000 1010000;
f_{88} : 0010010001000110000001000 1001110; f_{89} : 0010110011011000000000001 1010100; f_{90} : 0010000011101110000110001001 0000;
f_{91} : 0010110011110000000000000 1110100; f_{92} : 0010110011011000000000000 1011100; f_{93} : 0010011011010100000000000 1011010;
f_{94} : 0010000011101110000110000001 1000; f_{95} : 0010010011010000000010001 1011100; f_{96} : 0010010011001110000001000 1000110;
f_{97} : 0010000001100110001110000011 1000; f_{98} : 0010000011001100010101000 1010100; f_{99} : 0010000001000100010101001 1011100;
f_{100} : 0010000001100110001110001011 0000; f_{101} : 0010110011011000000010000 1010100; f_{102} : 0010011011010100000010000 1010010;
f_{103} : 0010011001011110000000000 1011000; f_{104} : 0010110001110000000010000 1110100; f_{105} : 0010010001111000000000000 1111100;
f_{106} : 0010110001011000000010000 1011100; f_{107} : 0010011001011110000010000 1010000; f_{108} : 0010111001010110000000000 1011000;
f_{109} : 0010100011101110000100001 0010000; f_{110} : 0010100001100110001100000 0111000; f_{111} : 0010000001101110000110100 0010010;
f_{112} : 0010100010001000011010101 0001100; f_{113} : 0010100000001000011010100 0101110; f_{114} : 0010010011111000000000000 1110100;
f_{115} : 0010100010001000011000101 0100110; f_{116} : 0010100011101110000100000 0011000; f_{117} : 0010100001100110001100001 0110000;
f_{118} : 0010100011100110000100100 0010010; f_{119} : 0010000011100110000110100 0010010; f_{120} : 0010011001010100000000000 1011010;
f_{121} : 0010110001110000000000000 1110100; f_{122} : 0010110001011000000000000 1011100; f_{123} : 0010010001111000000000000 1110100;
f_{124} : 0010110001011000000010001 1010100; f_{125} : 0010011001010100000010001 1010010; f_{126} : 0010111001011100000000000 1010010;
f_{127} : 0010100001100110001100001 0111000; f_{128} : 0010010011010010000000001 1011110; f_{129} : 0010000001101110000110101 0010010;
f_{130} : 0010000011100110000110101 0010010; f_{131} : 0010010011010010000010000 1011110; f_{132} : 0010100010001000011000101 0101110;
f_{133} : 0010100011101110000100001 0011000; f_{134} : 0010010011010010000010001 1010110; f_{135} : 0010111001010110000010000 1011000;
f_{136} : 0010111011011100000000000 1010010; f_{137} : 0010110011011010000000000 1010110; f_{138} : 0010010001010010000010001 1011110;
f_{139} : 0010110001011010000000000 1101010; f_{140} : 0010011011110100000000000 1110010; f_{141} : 0010011001110100000000000 1110010;
f_{142} : 0010100001001100010111000 1010100; f_{143} : 0010100011000100010111000 1010100; f_{144} : 0010100000001000011010101 0101110;
f_{145} : 0010100011100110000100101 0010010; f_{146} : 0010100001101110000100100 0011010; f_{147} : 0010000011101110000110001 0011000;
f_{148} : 0010110001011010000010000 1010110; f_{149} : 0010010001111010000000000 1110110; f_{150} : 0010110001011010000000000 1011110;
f_{151} : 0010110001110010000000000 1110110; f_{152} : 0010011011011110000000000 1101000; f_{153} : 0010011001110100000000000 1111010;
f_{154} : 0010010011111000000010000 1111100; f_{155} : 0010100011100110001100100 0110010; f_{156} : 0010111011011100000010000 1010010;
f_{157} : 0010110011110000000010001 1110100; f_{158} : 0010110011011000000010001 1011100; f_{159} : 0010011011011100000010001 1010000;
f_{160} : 0010110011110000000010000 1111100; f_{161} : 0010011001110100000010001 1110010; f_{162} : 0010000011101110001110000 0111000;
f_{163} : 0010000001101110001110100 0110010; f_{164} : 0010000010011000101011001 1011110; f_{165} : 0010000011100110001110100 0110010;
f_{166} : 0010100011101110001100000 0111000; f_{167} : 0010011011110100000000000 1111010; f_{168} : 0010011011110100000010000 1110010;
f_{169} : 0010111011111100000000000 1110010; f_{170} : 0010010011111010000000000 1111110; f_{171} : 0010010011111010000000000 1111010;
f_{172} : 0010110011011010000010000 1011110; f_{173} : 0010011011110100000010000 1111010; f_{174} : 0010110011110010000010000 1110110;
f_{175} : 0010110011011010000010001 1010110; f_{176} : 0010010011111010000010000 1110110; f_{177} : 0010111001111100000000000 1110010;
f_{178} : 0010010001111010000000000 1111110; f_{179} : 0010110001110010000010001 1110110; f_{180} : 0010110011110010000000000 1111110;
f_{181} : 0010010001111010000010001 1110110; f_{182} : 0010110001110010000000000 1111110; f_{183} : 0010000011100110001101010 1100010;
f_{184} : 0010100011100110001100101 0110010; f_{185} : 0010100001101110001100100 0111010; f_{186} : 0010110011011010000000000 1011110;
f_{187} : 0010110001110010000010000 1111110; f_{188} : 0010110011110010000000000 1110110; f_{189} : 0010010001111010000010000 1111110;
f_{190} : 0010100001101110001100101 0111010; f_{191} : 0010110011110010000010001 1111110; f_{192} : 0010010011111010000010001 1111110;

$\widetilde{\mathcal{PBF}}_{5,2} \setminus (\mathcal{L}_{5,2} \cup \mathcal{R}_{5,2})$ with barrier of length $k = 5$:

f_1 : 0000100000000000000010000000 10000; f_2 : 0000100001010000000000000 01010000; f_3 : 0000100000000000010010000 10010000;
f_4 : 0000100011010000000000000 10000000; f_5 : 0000100010000000000000000 11010000; f_6 : 0000100000000000010010010000 10010;
f_7 : 0000100000000000000010010 10010010; f_8 : 0000100010000000000000000 00011110; f_9 : 0000100000000000000000000 10111100;

f_{10} : 0000100001010000001000 1010000000; f_{11} : 0000100011010000000000000 11010000; f_{12} : 0000100000000000010000000 10011110;
f_{13} : 0000100010000000010000000000 111100; f_{14} : 0011101000110010000000000 10000000; f_{15} : 0000100000000000000110010 10110010;
f_{16} : 0000100000000000010110010 00110010; f_{17} : 0000100010000000010000000 01111010; f_{18} : 0000100000000000010000000 11111010;
f_{19} : 0000100010000000011010100 01010100; f_{20} : 0000100010000000010101001 1010100; f_{21} : 0000100011010100100000000 1010100;
f_{22} : 0000100001010100100000000 11010100; f_{23} : 0000100010000000010101100 1010110; f_{24} : 0000100001010110000000000 11010110;
f_{25} : 0011000010111010100010100 0001000; f_{26} : 0011000010111010000010101 0001000; f_{27} : 0001110010010100100101 0100001 01000;
f_{28} : 0000100011010100011111001 0101000; f_{29} : 0000100010000000011111100 1111110; f_{30} : 0000100001111110000000000 11111110;

$\widetilde{\mathcal{PBF}}_{5,2} \setminus (\mathcal{L}_{5,2} \cup \mathcal{R}_{5,2})$ without barrier:

f_1 : 00001000100100100000000010000000; f_2 : 01011000010100000000000010000000; f_3 : 01011000101000000000000010000000;
f_4 : 01011000000000000010001010000000; f_5 : 00011010000001100000000010000000; f_6 : 01011000000001100000000010000000;
f_7 : 01010010010001001000000010000000; f_8 : 01011100100001000000000010000000; f_9 : 01011100001001000000000000100000;
f_{10} : 01111000001000000000000011010000; f_{11} : 00010110100000000000000000011110; f_{12} : 00111010000011100000000010000000;
f_{13} : 00011010100000101000001010000000; f_{14} : 00111000100010000000101010000000; f_{15} : 00100101110110001000100010000000;
f_{16} : 00101011001100101000001010000000; f_{17} : 00011001101100101000001010000000; f_{18} : 01011110001010000000000010101000;
f_{19} : 01011000010100000000000011010110; f_{20} : 01111010100000000010001011010000; f_{21} : 01010010010001001000000010011110;
f_{22} : 01011100110101000000000011010000; f_{23} : 01010010001010101010010010000100; f_{24} : 00001000001111000011001010110010;
f_{25} : 00101011001100011011000110110000; f_{26} : 00101000000011011101110111010000; f_{27} : 01011110011111100000000011111110;