On one class of discrete functions, constructed from several linear recurrence sequences over primal residue rings

Kamlovskii O.V., Pankov K.N.

Moscow Technical University of Communication and Informatics

Goals

Let p be a prime number, $P = GF(p)$ a finite field of p elements, $R = \mathbb{Z}_{p^n}$ the residue ring modulo p^n.

Problem 1. Construct a function $f : P^m \to P$, that is sufficiently distant from the class of affine functions
$A_m(P) = \{c_0 + c_1x_1 + \ldots + c_mx_m : c_0, c_1, \ldots, c_m \in P\}$.

Problem 2. Construct a large class of functions $f : P^m \to P$, sufficiently distant from the class $A_m(P)$.

Feature in solving our goals: we will use linear shift registers over the ring R when constructing functions.

Previously known results

Nonlinearity of functions and permutations built from linear recurrent sequences over prime fields (Shparlinski I.E., Winterhof A., 2006).
Codes built from linear recurrent sequences over the ring $\mathbb{Z}_{2^n}$ that are sufficiently distant from Reed-Muller codes of the first order (Lathtonen L., Ling S., Sole P., Zinoviev D., 2004).
Boolean functions built from one linear recurrent sequence over the ring $\mathbb{Z}_{2^n}$ (Bylkov D.N., Kamlovskii O.V., 2012).
Rule for building a Boolean function from one linear recurrent sequence (idea of Nechaev A.A.; Bylkov D.N., 2014).
Functions over finite fields built from one linear recurrent sequence (Bugrov A.D., Kamlovskii O.V., 2018).
Boolean functions built from many linear recurrent sequences (Gruba A.A., 2023).

The factor ring $\bar{R} = R/pR$ of the ideal pR is a field of p elements.
For convenience purposes denote $\bar{R} = P$.
Let $\bar{a}$ be the image of $a \in R$ under the natural epimorphism of rings $R \to \bar{R}$.
For a polynomial $A(x) \in R[x]$, such that $A(x) = \sum_{i=0}^{m} a_i x^i \in R[x]$ define $\bar{A}(x) = \sum_{i=0}^{m} \bar{a}_i x^i \in P[x]$.

Definition

A polynomial $A(x) \in R[x]$ is called monic, if $a_m = 1$, and reversible, if a_0 is a unit of R.

Theorem of Nechaev A.A., 1977

Definition

A reversible monic polynomial $G(x) \in R[x]$ is called marked, if the periods of polynomials $G(x)$ and $\bar{G}(x)$ are equal.

Theorem

For every reversible monic irreducible polynomial $F(x) \in P[x]$ there exists a unique marked polynomial $G(x) \in R[x]$, such that $\bar{G}(x) = F(x)$.

Let $F(x)$ and $G(x)$ be polynomials such as in the theorem, $m = \deg F(x) = \deg G(x)$,

$$T = T(G) = T(F) = (p^m - 1)/d,$$

where d is a divisor of $p^m - 1$.

Linear recurrent sequences

Let $L_R(G)$ denote the set of all linear recurrent sequences (LRS) u over the ring R with a characteristic polynomial $G(x)$, so $u = (u(i))_{i=0}^{\infty}$

$$u(i+m) = a_0 u(i) + a_1 u(i+1) + \ldots + a_{m-1} u(i+m-1), \quad i \geq 0,$$

$$G(x) = x^m - a_{m-1}x^{m-1} - \ldots - a_1 x - a_0.$$

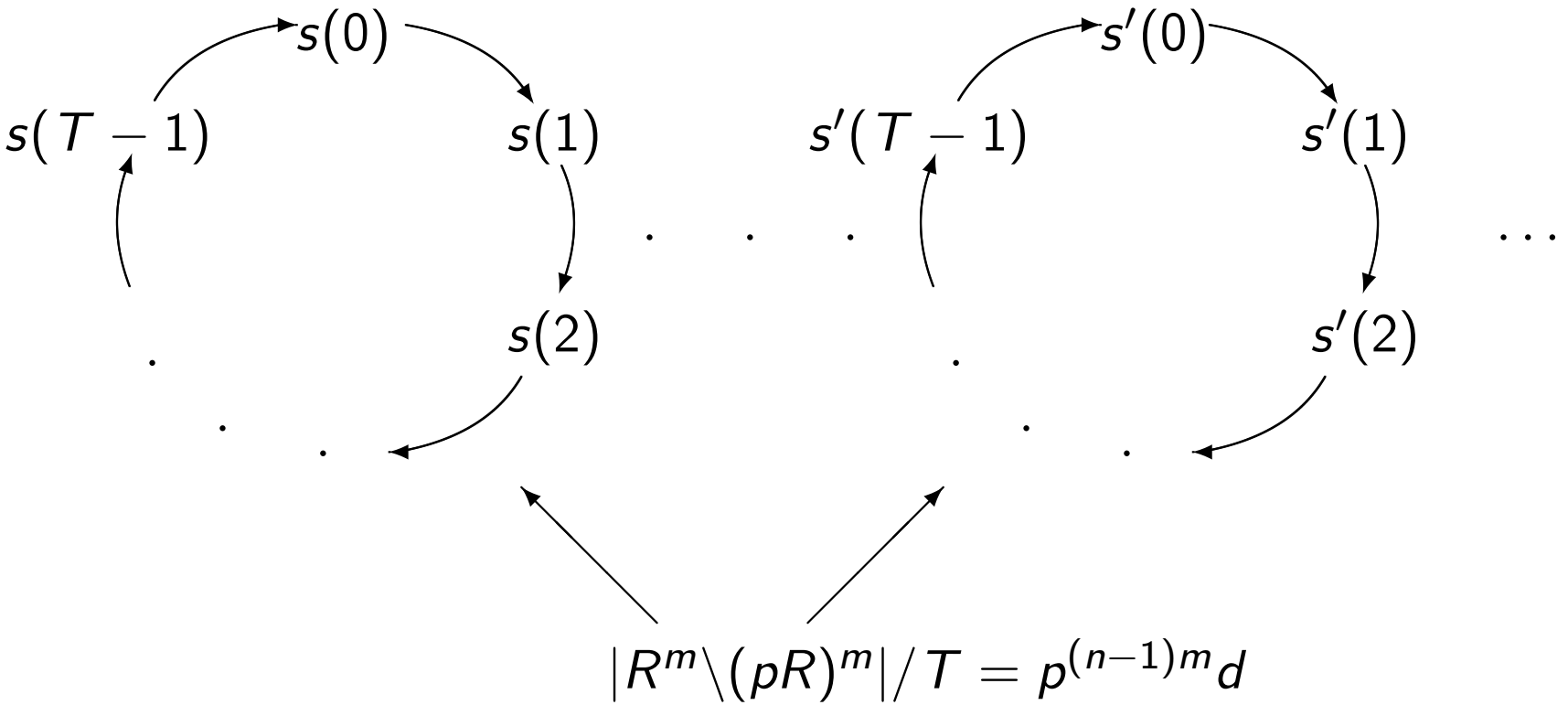
Let $L_R(G)^*$ denote the set of LRS $u \in L_R(G)$, such that $(u(0), \ldots, u(m-1)) \in R^m \backslash (pR)^m$.

Proposition

If $u \in L_R(G)^*$, then $\bar{u} = (\bar{u}(0), \bar{u}(1), \ldots) \in L_P(F)$ is a nonzero LRS.

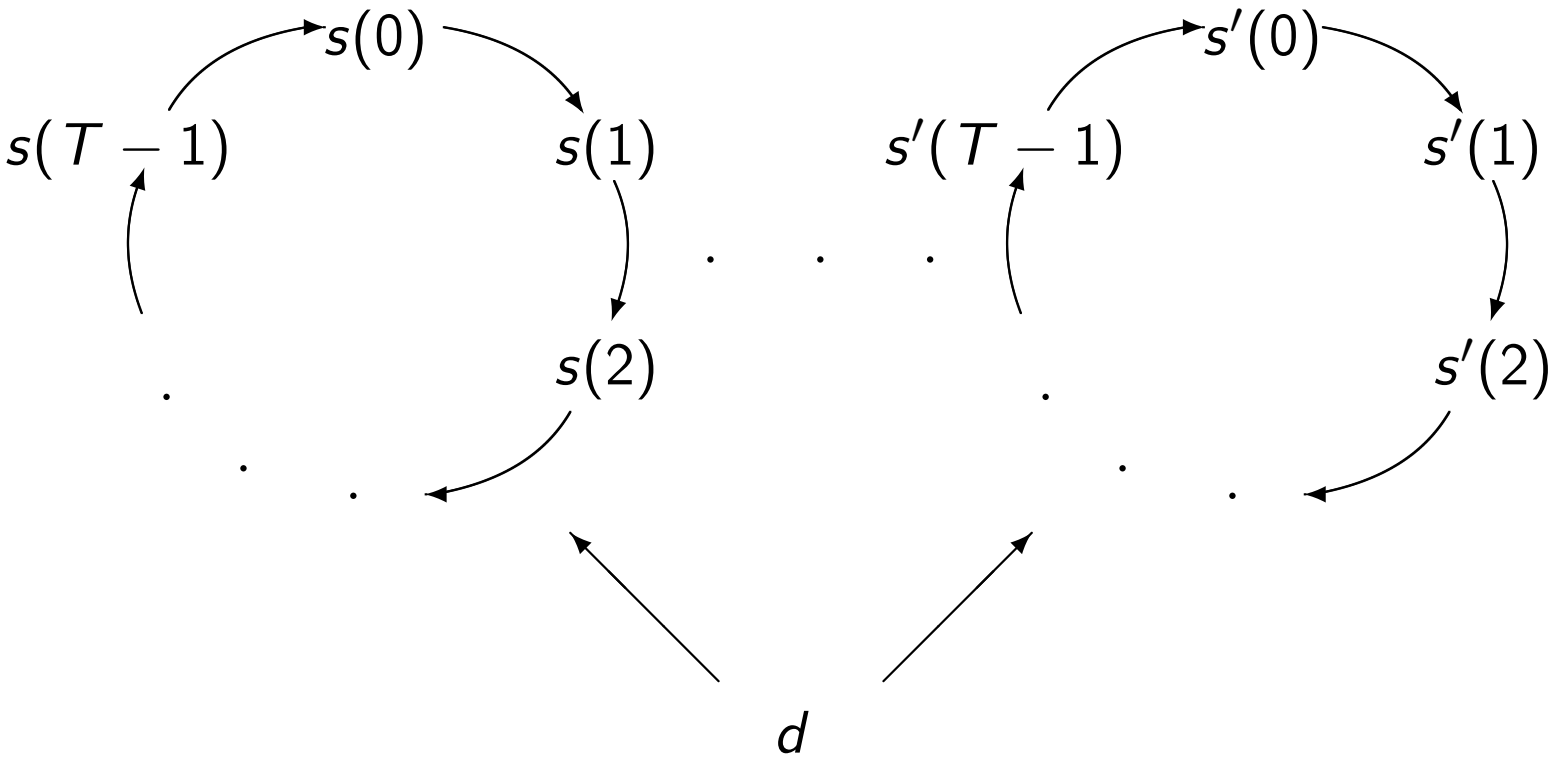
Graph of a linear shift register over the ring R with a characteristic polynomial $G(x)$

Initial states $s(0), \ldots, s'(0)$ are chosen from $R^m \backslash (pR)^m$.



Graph of a linear shift register over the field P with a characteristic polynomial $F(x)$

Initial states $s(0), \ldots, s'(0)$ are chosen from P^m.



Construction of functions

Let $\psi_0 : R \to P, \ldots, \psi_{d-1} : R \to P$ be arbitrary maps.
Choose LRS $v_0, \ldots, v_{d-1}$ with a chracteristic polynomial $G(x)$, such that the vectors

$$(\bar{v}_0(i), \ldots, \bar{v}_0(i+m-1)), \ldots, (\bar{v}_{d-1}(i), \ldots, \bar{v}_{d-1}(i+m-1)),$$

where $i = 0, 1, \ldots T-1$, run through the set $P^m \backslash \{\vec{0}\}$.
Initial segments of LRS $\bar{v}_0, \ldots, \bar{v}_{d-1}$ are representatives of distinct cycles in the graph of a linear shift register with a characteristic polynomial $F(x)$.

Construction of functions

Table of the function $f : P^m \to P$

$$f(x_1, \ldots, x_m) = f_{v_0,\ldots,v_{d-1},\psi_0,\ldots,\psi_{d-1}}(x_1, \ldots, x_m)$$

x_1	x_2	$\ldots$	x_m	$f(x_1, \ldots, x_m)$
0	0	$\ldots$	0	0
		.		.
		.		.
		.		.
$\bar{v}_k(i)$	$\bar{v}_k(i+1)$	$\ldots$	$\bar{v}_k(i+m-1)$	$\psi_k(v_k(i))$
		.		.
		.		.
		.		.

where $k = 0, 1, \ldots, d-1$, $i = 0, 1, \ldots, T-1$.
We will study the properties of the class

$$D_m(G, \psi_0, \ldots, \psi_{d-1}) = \{f_{v_0,\ldots,v_{d-1},\psi_0,\ldots,\psi_{d-1}}(\vec{x}) : v_0, \ldots, v_{d-1} \in L_R(G)^*\}.$$

Algorithm for constructing a function using one LRS

Let d divide $p-1$, and $(d,m)=1$.
Choose a primitive γ of the field P, and elements $\delta_j \in R$, such that $\bar{\delta}_j = \gamma$, $j = 1, 2, \ldots, d-1$.
Algorithm:
1) choose initial state $(1, \ldots, 1)$ of a shift register with a characteristic polynomial $G(x)$;
2) for every step $i = 0, 1, \ldots, T(G)-1$ of the shift register (in a state $(v_0(i), \ldots, v_0(i+m-1))$) construct d values of f:

$$f(\bar{v}_0(i), \bar{v}_0(i+1), \ldots, \bar{v}_0(i+m-1)) = \psi_0(v_0(i));$$

$$f(\gamma\bar{v}_0(i), \gamma\bar{v}_0(i+1), \ldots, \gamma\bar{v}_0(i+m-1)) = \psi_1(\delta_1 v_0(i));$$

$$\ldots$$

$$f(\gamma^{d-1}\bar{v}_0(i), \gamma^{d-1}\bar{v}_0(i+1), \ldots, \gamma^{d-1}\bar{v}_0(i+m-1)) = \psi_{d-1}(\delta_{d-1} v_0(i)).$$

Digit sets of the ring R

Definition

A subset $K = \{k_0, k_1, \ldots, k_{p-1}\}$ of the ring R, such that $\bar{k}_i \neq \bar{k}_j$ for all $i, j \in \{0, 1, \ldots, p-1\}$, $i \neq j$, is called a digit set.

If K is a digit set of the ring R, then an element $a \in R$ is uniquely represented as

$$a = a_0 + pa_1 + \ldots + p^{n-1}a_{n-1}, \tag{1}$$

where $a_i \in K$, $i = 0, 1, \ldots, n-1$.

Definition

For a digit set K the map $\varkappa_{n-1}^K : R \to P$, such that $\varkappa_{n-1}^K(a) = a_{n-1}$ for all $a \in R$, where a_{n-1} is from the equality (1), is called the highest order digit map.

Digit sets of the ring R that form an arithmetic progression

Definition

A digit set K forms an arithmetic progression, if

$$K = K_{a,t} = \{a, a+t, a+2t, ..., a+(p-1)t\},$$

for some $a, t \in R$, where $a \equiv 0 \,(mod\ p)$, $(t, p) = 1$.

The set $K = K_{0,1} = \{0, 1, \ldots, p-1\}$ is one of them.

Choose digit sets K_{a_s,t_s}, $s = 0, \ldots, d-1$ and maps $\psi_s = \varkappa_{n-1}^{K_{a_s,t_s}}$.

Fourier coefficients of a function

Let L_m denote the set of maps $g : P^m \to \mathbb{C}$.
For arbitrary $g_1, g_2 \in L_m$ let $S : L_m \times L_m \to \mathbb{C}$ denote

$$S(g_1, g_2) = \frac{1}{p^m} \sum_{\vec{x} \in P^m} \psi_1(\vec{x}) \overline{\psi_2(\vec{x})}.$$

Then (L_m, S) is a Euclidean space.
For $\vec{a} = (a_1, \ldots, a_m) \in P^m$ consider a map $\chi_{\vec{a}} : P^m \to \mathbb{C}$, such that

$$\chi_{\vec{a}}(x_1, \ldots, x_m) = e^{2\pi i \frac{a_1 x_1 + \ldots + a_m x_m}{p}}, \quad x_1, \ldots, x_m \in P.$$

The function system $\chi_{\vec{a}}$, where $\vec{a} \in P^m$, forms an orthonormal basis of (L_m, S).
For every map $g \in L_m$ there exist unique complex numbers $\nu_g(\vec{a})$, such that

$$g(x_1, \ldots, x_m) = \sum_{\vec{a} \in P^m} \nu_g(\vec{a}) \chi_{\vec{a}}(x_1, \ldots, x_m), \quad x_1, \ldots, x_m \in P.$$

Linear characteristic of a function

Additive characters of the field P consists of homomorphisms

$$\chi_a(x) = e^{2\pi i \frac{ax}{p}}, \quad x \in P, \tag{2}$$

where $a \in P$. The function $f : P^m \to P$ induces $p-1$ maps $f \cdot \chi_a : P^m \to \mathbb{C}$, where $a \in P^*$.

Definition

The linear characteristic of a function $f : P^m \to P$ is defined as

$$\delta(f) = \max_{a \in P^*} \max_{\vec{a} \in P^m} |\nu_{f \cdot \chi_a}(\vec{a})|.$$

If $P = GF(2) = \{0, 1\}$, then

$$\delta(f) = \frac{1}{2^m} \max_{\vec{a} \in P^m} |W_f(\vec{a})|,$$

$$\mathrm{nl}(f) = 2^{m-1} - \frac{1}{2} \max_{\vec{a} \in P^m} |W_f(\vec{a})| = 2^{m-1} - 2^{m-1}\delta(f).$$

Bent functions

Proposition

We have (from Parcevall's identity)

$$\delta(f) \geq p^{-\frac{m}{2}}.$$

Definition

A function f is called bent, if its linear characteristic $\delta(f) = p^{-\frac{m}{2}}$.

Proposition

A function $f : P^m \to P$ is bent if and only if $|\nu_{f \cdot \chi_a}(\vec{a})| = p^{-\frac{m}{2}}$ for all $a \in P^*$, $\vec{a} \in P^m$.

Main result

Theorem

Let $f \in D_m(G, \psi_0, \ldots, \psi_{d-1})$, $T(G) = (p^m - 1)/d$, $n > 1$, $\psi_s = \varkappa_{n-1}^{K_{a_s,t_s}}$, $\psi_s(0) = \bar{0}$ *for all* $s = 0, \ldots, d-1$. *Then*

$$\delta(f) \leq (dp^{n-1} - 1)\left(\frac{2}{\pi}\ln(p^{n-1}) + \frac{13}{40}p + \frac{7}{20}\right)p^{-\frac{m}{2}}.$$

Thus, for fixed n, p, d, and $m \to \infty$ it is proven that $\delta(f) = O(p^{-\frac{m}{2}})$.

Element preimage cardinality for functions from our class

Problem: construct a balanced function f.
For $a \in P$ and a function $f : P^m \to P$ consider the preimage $f^{-1}(a)$ of an element a :

$$f^{-1}(a) = \{(b_1, \ldots, b_m) \in P^m : f(b_1, \ldots, b_m) = a\}.$$

Theorem

Let $f \in D_m(G, \psi_0, \ldots, \psi_{d-1})$, $T(G) = (p^m - 1)/d$, $n > 1$, $\psi_s = \varkappa_{n-1}^{K_{a_s,t_s}}$, $\psi_s(0) = \bar{0}$ for all $s = 0, \ldots, d-1$. Then for an arbitrary $a \in P$ we have

$$\left| |f^{-1}(a)| - p^{m-1} \right| < (dp^{n-1} - 1) \left(\frac{2}{\pi} \ln(p^{n-1}) + \frac{13}{40} p + \frac{7}{20} \right) p^{\frac{m}{2}}.$$

Approach to solving problem 2

Choose fixed LRS $u_0, \ldots, u_{d-1}$ over P with a chracteristic polynomial $F(x)$, such that the vectors

$$(u_0(i), \ldots, u_0(i+m-1)), \ldots, (u_{d-1}(i), \ldots, u_{d-1}(i+m-1)),$$

where $i = 0, 1, \ldots T-1$, run through the set $P^m \backslash \{\vec{0}\}$.
Initial segments of LRS $u_0, \ldots, u_{d-1}$ are representatives of distinct cycles in the graph of a linear shift register with a characteristic polynomial $F(x)$.

Second construction of functions (problem 2)

Table of the function $f : P^m \to P$

$$f(x_1, \ldots, x_m) = \tilde{f}_{v_0,\ldots,v_{d-1},\psi_0,\ldots,\psi_{d-1}}(x_1, \ldots, x_m)$$

x_1	x_2	$\ldots$	x_m	$f(x_1, \ldots, x_m)$
0	0	$\ldots$	0	0
		.		.
		.		.
		.		.
$u_k(i)$	$u_k(i+1)$	$\ldots$	$u_k(i+m-1)$	$\psi_k(v_k(i))$
		.		.
		.		.
		.		.

where $k = 0, 1, \ldots, d-1$, $i = 0, 1, \ldots, T-1$.

Proposition

Theorems on upper bounds of $\delta(f)$ and $\left||f^{-1}(a)| - p^{m-1}\right|$ remain true.

Computational experiments for $d = 1$

The case $R = \mathbb{Z}_{2^n}$, $d = 1$, $\psi_0 = \varkappa_{n-1}^{\{0,1\}}$ was studied.
Fix m and polynomials $G(x) \in R[x]$, $\deg G(x) = m$,
$F(x) = \bar{G}(x) \in P[x]$.
Choose LRS $u_0 \in L_P(F)$ with an initial state
$(u_0(0), \ldots, u_0(m-1)) = (0, \ldots, 0, 1)$.
Choose a random initial vector of an LRS $v_0 \in L_R(G)^*$ and construct $\tilde{f}_{v_0,\psi_0}(x_1, \ldots, x_m)$.
Compute the parameters $\mathrm{nl}(f)$, $\deg f$, and $bal(f)$ for the constructed function.
In the following table an entry $(\mathrm{nl}, \deg, \mathrm{bal}) - N$ constitutes that N functions with nonlinearity nl, algebraic degree deg, and balance bal ($\mathrm{bal} = 0$ — not balanced, $\mathrm{bal} = 1$ — balanced) were found.

Computational experiments for $d = 1$

d	n	$G(x)$	$(\mathrm{nl}, \deg, \mathrm{bal}) - N$
1	2	$x^8 + 3x^7 + 2x^6 + x^5 + 3x^3 + 1$	$(120, 2, 0) - 65280$
	3	$x^8 + 2x^7 + 3x^6 + 5x^5 + 2x^4 + 5x^3 + 2x^2 + 4x + 1$ Random sample	$(110, 4, 0) - 32$, $(106, 4, 0) - 6493$ $(102, 4, 0) - 4968$, $(98, 4, 0) - 1424$ $(94, 4, 0) - 112$
	4	$x^8 + 2x^7 + 11x^6 + 5x^5 + 11x^4 + 6x^3 + 10x^2 + 4x + 1$ Random sample	$(111, 8, 0) - 58$, $(109, 8, 0) - 2593$ $(107, 8, 0) - 20290$, $(105, 8, 0) - 32043$ $(103, 8, 0) - 26128$, $(101, 8, 0) - 14802$ $(99, 8, 0) - 7355$, $(97, 8, 0) - 2470$ $(95, 8, 0) - 666$, $(93, 8, 0) - 378$ $(91, 8, 0) - 85$

Computational experiments for $d > 1$

The case $R = \mathbb{Z}_{2^n}$, $d \in \{3, 5\}$, $\psi_0 = \ldots = \psi_{d-1} = \varkappa_{n-1}^{\{0,1\}}$ was studied.

Fix m and polynomials $G(x) \in R[x]$, $\deg G(x) = m$, $F(x) = \bar{G}(x) \in P[x]$.

Choose random initial vectors of LRS $v_0 \in L_R(G)^*$, ..., $v_{d-1} \in L_R(G)^*$ and construct $f_{v_0,\ldots,v_{d-1},\psi_0,\ldots,\psi_{d-1}}(x_1, \ldots, x_m)$.

Compute the parameters $\mathrm{nl}(f)$, $\deg f$, and $bal(f)$ for the constructed function.

In the following table an entry $(\mathrm{nl}, \deg, \mathrm{bal}) - N$ constitutes that N functions with nonlinearity nl, algebraic degree deg, and balance bal ($\mathrm{bal} = 0$ — not balanced, $\mathrm{bal} = 1$ — balanced) were found.

Computational experiments for $d = 3$

d	n	$G(x)$	$(\mathrm{nl}, \deg, \mathrm{bal}) - N$
3	2	$x^8 + 3x^7 + 2x^6 + 3x^5 +$	$(120, 2, 0) - 1$, $(112, 5, 0) - 3$
		$2x^3 + 3x + 1$	$(108, 5, 1) - 333$, $(108, 5, 0) - 1400$
		Random sample	$(108, 4, 0) - 12$, $(104, 5, 1) - 839$
			$(104, 5, 0) - 3455$, $(104, 4, 1) - 6$
	3	$x^8 + 3x^7 + 2x^6 +$	$(110, 7, 1) - 8$, $(110, 7, 0) - 18$
		$3x^5 + 4x^4 + 6x^3 +$	$(109, 8, 0) - 154$, $(108, 7, 1) - 53$
		$4x^2 + 7x + 1$	$(108, 7, 0) - 506$
		Random sample	$(107, 8, 0) - 1202$
			$(106, 7, 1) - 179$
	4	$x^8 + 11x^7 + 10x^6 +$	$(111, 8, 0) - 5$, $(110, 7, 1) - 8$
		$11x^5 + 4x^4 + 6x^3 +$	$(110, 7, 0) - 38$, $(109, 8, 0) - 333$
		$4x^2 + 7x + 1$	$(108, 7, 1) - 117$, $(108, 7, 0) - 971$
		Random sample	$(108, 6, 1) - 2$, $(108, 6, 0) - 1$
			$(107, 8, 0) - 2387$, $(106, 7, 1) - 349$

Computational experiments for $d = 5$

d	n	$G(x)$	$(\mathrm{nl}, \deg, \mathrm{bal}) - N$
5	2	$x^8 + 2x^6 + 3x^4 +$	$(112, 5, 0) - 1$, $(108, 5, 1) - 58$
		$3x^3 + 3x + 1$	$(108, 5, 0) - 204$, $(104, 5, 1) - 125$
		Random sample	$(104, 5, 0) - 526$
	3	$x^8 + 4x^7 + 2x^6 +$	$(110, 7, 1) - 3$, $(110, 7, 0) - 4$
		$4x^5 + 3x^4 + 3x^3 +$	$(108, 7, 1) - 15$, $(108, 7, 0) - 181$
		$4x^2 + 7x + 1$	$(106, 7, 1) - 65$, $(106, 7, 0) - 523$
		Random sample	$(104, 7, 1) - 76$, $(104, 7, 0) - 595$
	4	$x^8 + 4x^7 + 10x^6 +$	$(111, 8, 0) - 1$, $(110, 7, 1) - 2$
		$12x^5 + 11x^4 + 11x^3 +$	$(110, 7, 0) - 6$, $(109, 8, 0) - 57$
		$12x^2 + 7x + 1$	$(108, 7, 1) - 19$, $(108, 7, 0) - 176$
		Random sample	$(107, 8, 0) - 391$, $(106, 7, 1) - 42$

Thank you for your attention!