Quasigroups and Related Systems **18** (2010), 59 – 82

Polynomial functions on the units of $\mathbb{Z}_{2^n}$

Smile Markovski, Zoran Šunić and Danilo Gligoroski

Devoted to the memory of Valentin D. Belousov (1925-1988)

Abstract. Polynomial functions on the group of units Q_n of the ring $\mathbb{Z}_{2^n}$ are considered. A finite set of reduced polynomials $\mathcal{RP}_n$ in $\mathbb{Z}[x]$ that induces the polynomial functions on Q_n is determined. Each polynomial function on Q_n is induced by a unique reduced polynomial - the reduction being made using a suitable ideal in $\mathbb{Z}[x]$. The set of reduced polynomials forms a multiplicative 2-group. The obtained results are used to efficiently construct families of exponential cardinality of, so called, huge k-ary quasigroups, which are useful in the design of various types of cryptographic primitives. Along the way we provide a new (and simpler) proof of a result of Rivest characterizing the permutational polynomials on $\mathbb{Z}_{2^n}$.

1. Introduction

The need for new kinds of computational methods and devices is growing as a result of the possibility of their application in the new developing fields in mathematics and computer science, in particular cryptography and coding theory. Finite fields and integer quotient rings are traditionally used for such computational needs. The integer quotient rings are somewhat disadvantaged due to the fact that their nonzero multiplicative structure does not form a group (except when they happen to be fields). The structure of the ring of polynomials over rings, and especially over integer quotient rings, has been under investigation for almost a century. Let us mention here chronologically some of the authors: Kempner (1921) [9], Nöbauer (1965) [13], Keller and Olson (1968) [7], Mullen and Stevens (1984) [12],

2000 Mathematics Subject Classification: 13F20, 20N05, 20D99
Keywords: group, ring, polynomial, polynomial function, quasigroup.
The visit of the first and the third author to the "Special semester on Gröbner bases – Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics", April 30 - May 06, 2006 in Linz, Austria, organized by RISC and RICAM, was very helpful and stimulated some of the ideas that are presented in this paper.
The second author was partially supported by NSF grant DMS-0805932.

Rivest (2001) [15], Bandini (2002) [1], Zhang (2004) [18]. We emphasize that the paper of Rivest [15] is closest to our work and his results can be inferred from ours (see Section 5).

We consider its group of units Q_n in $\mathbb{Z}_{2^n}$ and define a finite set $\mathcal{RP}_n$ of reduced polynomials over $\mathbb{Z}$ that induce the set $\mathcal{PF}_n$ of all polynomial functions that keep Q_n invariant. The set $\mathcal{RP}_n$ is a finite 2-group under polynomial multiplication modulo functional equivalence. Exactly half of the reduced polynomials induce permutations on Q_n.

The reduced polynomials are obtained by using an ideal I_n in $\mathbb{Z}[x]$ such that every polynomial in I_n induces the 0 constant function on Q_n and two polynomials are functionally equivalent over Q_n if and only if they are equivalent with respect to the ideal I_n.

By using our reduction algorithms we are able to give efficient answers to several problems. We show that there are efficient algorithms (polynomial complexity with respect to the input parameters) for the following problems:

(i) given a polynomial inducing a polynomial function on Q_n, determine the reduced polynomial inducing the same polynomial function,

(ii) given a polynomial inducing a permutation on Q_n, determine the reduced polynomial inducing the inverse permutation.

(iii) given a polynomial inducing a polynomial function on Q_n, determine the reduced polynomial for the multiplicative inverse.

In the last part of the paper we use the obtained results to construct families of quasigroups of large cardinality. We define the concept of huge quasigroups as quasigroups of large order that can be handled effectively, in the sense that the multiplication in the quasigroup, as well as in its adjoint operations, can be effectively realized (polynomial complexity with respect of $\log n$, where n is the order of the quasigroup). The need for permutations and quasigroups of large (huge) orders such as 2^{16}, 2^{32}, 2^{64}, 2^{128}, that can be easily handled is associated with the development of the modern massively produced 32-bit and 64-bit processors. Strong links between modern cryptography and quasigroups (equivalently, Latin squares) have been observed by Shannon [17] more than 50 years ago. Subsequently, the cryptographic potential of quasigroups in the design of different types of cryptographic primitives has been addressed in numerous works. Authentication schemas have been proposed by Dènes and Keedwell (1992) [5], secret sharing schemes by Cooper, Donovan and Seberry (1994) [4], a version of popular DES block cipher by using Latin squares by Carter, Dawson, and Nielsen (1995) [3], different proposals for use in the design of cryptographic hash functions by several authors [16], a hardware stream cipher by Gligoroski, Markovski, Kocarev and Gusev (2005) [6]. One application of the quasigroups as defined here can be found in the paper [11], where a new public key cryptsystem is defined.

We want to emphasize that the results in this work concerning effective constructions of large quasigroups, besides in cryptography, can also be of interest in other areas (such as coding theory, design theory, ...).

1.1. Organization of the content

Well known background on the structure of the group Q_n and on Hensel lifting (useful to extract inverses in Q_n) is presented in Section 2. Full description of the polynomials in $\mathbb{Z}[x]$ that induce transformations on Q_n (and the finite set of reduced polynmials that represent them) is provided in Section 3, while the polynomials in $\mathbb{Z}[x]$ that induce permutations on Q_n are characterized in Section 4. Section 5 is a brief interlude in which we use our results to present a new proof or a result of Rivest [15] providing a characterization of polynomials in $\mathbb{Z}[x]$ that induce permutations on $\mathbb{Z}_{2^n}$. The group of reduced polynomials under multiplication is briefly considered in Section 6. Section 7 provides polynomial algorithms that handle construction of reduced polynomials related to interpolation, functional inversion, and multiplicative inversion. Finally, applications to effective constructions of large k-ary quasigroups are provided in Section 8.

2. The group $(Q_n, \cdot)$

The integer quotient ring $(\mathbb{Z}_k, +, \cdot)$, where k is a positive integer, is a well known mathematical structure, where the addition and multiplication are interpreted modulo k. This ring is associative and commutative ring with a unit element 1. Here we are concerned solely with the case $k = 2^n$. The set $Q_n = \{1, 3, \ldots, 2^n - 1\}$ is a subgroup of the multiplicative semigroup $(\mathbb{Z}_{2^n}, \cdot)$. Indeed, Q_n is precisely the group of units of $\mathbb{Z}_{2^n}$. Note that if $n = 1$, then Q_n is trivial, and if $n = 2$, $Q_2 = \mathbb{Z}_2 = \langle -1 \rangle$. The structure of the abelian group Q_n, for $n \geqslant 3$, is given by the following result.

Proposition 1. *Let $n \geqslant 3$. Then $(Q_n, \cdot) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$. Moreover, Q_n is generated by -1 and 5, the order of -1 is 2, and the order of 5 is 2^{n-2}.*

Proof. The subset $F_n \subseteq Q_n$ of numbers of the form $4k+1$ forms a subgroup of index 2 in Q_n. Since $5 \in F_n$, we have $5^{2^{n-2}} = 1$ in Q_n. On the other hand,

$$5^{2^{n-3}} = (4+1)^{2^{n-3}} = \sum_{i=0}^{2^{n-3}} \binom{2^{n-3}}{i} 2^{2i}.$$

The highest power of 2 dividing $i!$ is $\lfloor i/2 \rfloor + \lfloor i/4 \rfloor + \cdots < i/2 + i/4 + \cdots = i$. Thus each of the terms $\binom{2^{n-3}}{i} 2^{2i}$ is divisible by $2^{n-3+2i-(i-1)} = 2^{n-2+i}$ and we have

$$5^{2^{n-3}} \equiv 1 + 2^{n-3} \cdot 2^2 \equiv 2^{n-1} + 1 \pmod{2^n}. \tag{1}$$

Therefore $5^{2^{n-3}} \neq 1$ in Q_n, the order of 5 is 2^{n-2}, and F_n is a cyclic group generated by 5.

The order of -1 is clearly 2. Since -1 is not in F_n (it has the form $4k+3$) we have that $Q_n = \langle -1 \rangle \times \langle 5 \rangle = \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$. □

Corollary 1. *Let $n \geqslant 3$. The multiplicative order of every $a \in Q_n$ divides 2^{n-2}.* □

Given a large value of n and $a \in Q_n$, can we effectively find the inverse a^{-1}? Note that if we express a as $a = (-1)^i \cdot 5^j$, for some $i \in \{0,1\}$, $j \in \{0, 1, \ldots, 2^{n-2}-1\}$, then its inverse in Q_n is given by

$$a^{-1} = (-1)^i \cdot 5^{2^{n-2}-j}.$$

However, this requires representing a in the form $a = (-1)^i \cdot 5^j$, for some $i \in \{0,1\}$. It is fairly easy to decide if $i = 0$ or $i = 1$. Indeed, $i = 0$ when a is of the form $4k+1$ and $i = 1$ otherwise. However, to determine j we need to solve a discrete logarithm problem of the type $5^x = a \pmod{2^n}$. This apparent difficulty can be sidestepped by calculating the inverse by applying Hensel lifting [14] (also known as Newton-Hensel lifting [8]).

The basic idea is to use binary representation of the integers modulo 2^n. Given $r \in \mathbb{Z}_{2^n}$, its binary representation is $r_{n-1} r_{n-2} \ldots r_1 r_0$, where $r_j \in \{0,1\}$ is the $(j+1)-$th bit of r. In the same way, the binary representation of a variable x is given by $x_{n-1} x_{n-2} \ldots x_1 x_0$, where x_j are bit variables. Now, let r be a root of the polynomial $P(x)$. Then $P(x) = (x-r)S(x)$ for some polynomial $S(x)$. The equality $P(x) = (x-r)S(x)$ in the ring $\mathbb{Z}_{2^k}$, where $k < n$, is given by

$$P(x_{k-1} \ldots x_1 x_0) = (x_{k-1} \ldots x_1 x_0 - r_{k-1} \ldots r_1 r_0) S(x_{k-1} \ldots x_1 x_0).$$

The last equality shows that if we want to find the k least significant bits of a root r of $P(x)$, we need to consider the equation $P(x) = 0$ in the ring $\mathbb{Z}_{2^k}$.

One variant of the Hensel lifting algorithm for finding a root of $P(x)$ is the following:

STEP 1: *Determine a bit r_0 such that $P(r_0) = 0$ in $\mathbb{Z}_2$.*

This can be accomplished simply by checking if $P(0) = 0$ or $P(1) = 0$ (or both!) in $\mathbb{Z}_2$.

Let the bits $r_0, \dots, r_{k-1}$ be already chosen in STEP 1 – STEP k.

STEP $k+1$: *Determine a bit r_k such that $P(r_k r_{k-1} \dots r_0) = 0$ in $\mathbb{Z}_{2^{k+1}}$.*

Since the bits $r_0, \dots, r_{k-1}$ are known, this can be accomplished by checking if $P(0r_{k-1} \dots r_0) = 0$ or $P(1r_{k-1} \dots r_0) = 0$ (or both) in $\mathbb{Z}_{2^{k+1}}$.

The algorithm stops after STEP n.

In order to find all roots of a polynomial one has to follow all the branching points of the algorithm (whenever both 0 and 1 are good choices one has to follow both choices, and whenever neither 0 nor 1 are good choices one discards that particular branch of the search).

Given $a \in Q$, the root of the polynomial $ax - 1$ is the inverse of a. In this case, the above algorithm has polynomial complexity in n, since there is only one root and the above algorithm will produce the unique correct bit of a^{-1} at each step (there is no branching).

3. Polynomial functions on Q_n

Every polynomial $P(x)$ from the polynomial ring $\mathbb{Z}[x]$ induces a polynomial function $p : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ by the evaluation map (taken modulo 2^n). We are interested here in polynomial functions on Q_n, i.e., polynomial functions $p : Q_n \to Q_n$ induced by polynomials $P(x)$ in $\mathbb{Z}[x]$ such that $p(Q_n) \subseteq Q_n$. Denote by $\mathcal{P}_n$ the set of polynomials in $\mathbb{Z}[x]$ that induce polynomial function on Q_n and denote by $\mathcal{PF}_n$ the set of corresponding polynomial functions on Q_n. We implicitly assume that $n \geqslant 2$ (as was already mentioned, Q_1 is trivial).

We first determine precisely the polynomials over $\mathbb{Z}$ that induce polynomial functions on Q_n, i.e., we determine $\mathcal{P}_n$.

Proposition 2. *Let $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a polynomial in $\mathbb{Z}[x]$. Then $P(x)$ is in $\mathcal{P}_n$ (i.e., $P(x)$ induces a polynomial function on Q_n) if and only if the sum of the coefficients $a_0 + a_1 + \cdots + a_d$ is odd, which, in turn, is equivalent to the condition that $p(1)$ is odd.*

Proof. For every odd number a, all the powers a^i, $i = 0, \dots, d$ are also odd. Thus the parity of $p(a) = a_0 + a_1 a + \dots + a_d a^d$ is equal to the parity of $a_0 + \dots + a_d$. $\square$

The finite set $\mathcal{PF}_n$ of polynomial functions on Q_n is induced by the infinite set of polynomials in $\mathcal{P}_n$. We will determine a finite set of polynomials, that induce all polynomial functions in $\mathcal{PF}_n$. In order to define this set, we need some preliminary definitions.

For an integer i, define $t_i = \lfloor i/2 \rfloor + \lfloor i/4 \rfloor + \lfloor i/8 \rfloor + \dots$, i.e., t_i is the largest integer ℓ such that 2^ℓ divides $i!$. Let d_n be the largest integer i such that $n - i - t_i$ is positive.

Definition 1. A polynomial $P(x) = a_0 + a_1 x + \dots + a_d x^d$ in $\mathcal{P}_n$ is called *reduced* if

(i) the degree of $P(x)$ is no higher than d_n,

(ii) $0 \leqslant a_i \leqslant 2^{n-i-t_i} - 1$, for $i = 0, \dots, d_n$.

Denote the set of reduced polynomials in $\mathcal{P}_n$ by $\mathcal{RP}_n$.

Proposition 3. *The number of reduced polynomials in $\mathcal{RP}_n$ is*

$$|\mathcal{RP}_n| = 2^{(2n-d_n)(d_n+1)/2-1-\sum_{i=0}^{d_n} t_i}.$$

Proof. The number of polynomial of degree at most d_n with restrictions on the coefficients given by (ii) is

$$2^{\sum_{i=0}^{d_n} n-i-t_i} = 2^{n(d_n+1)-d_n(d_n+1)/2-\sum_{i=0}^{d_n} t_i}.$$

Exactly half of such polynomials also satisfies the condition required by Proposition 2 on the parity of the sum of the coefficients. Indeed, we can match up any polynomial $P(x) = a_0 + a_1 x + \dots + a_d x^d$ in that satisfies the conditions (i) and (ii) with the polynomial $P(x) + 1$ if a_0 is even and with $P(x) - 1$ if a_0 is odd. In both cases, the obtained polynomial also satisfies the conditions (i) and (ii). In such a matching exactly one polynomial in each pair has odd sum of coefficients. $\square$

Two polynomials $P(x)$ and $T(x)$ in $\mathcal{P}_n$ are said to be *functionally equivalent* over Q_n if they induce the same polynomial function on Q_n. In that case we write $P(x) \approx T(x)$. Clearly, $\approx$ is an equivalence relation on $\mathcal{P}_n$.

The polynomials $P(x)$ and $T(x)$ are functionally equivalent over Q_n if and only if the difference $P(x) - T(x)$ induces the constant 0 function on Q_n. With this in mind, we define now a finite set of polynomials over $\mathbb{Z}$ that induce the 0 constant function on Q_n.

Definition 2. For $i = 0, \dots, d_n$, define the polynomial

$$P_{n,i}(x) = 2^{n-i-t_i}(x+1)(x+3)\dots(x+2i-1)$$

of degree i. When $i = 0$ the understanding is that $P_{n,0} = 2^n$. Define also the polynomial

$$P_{n,d_n+1}(x) = (x+1)(x+3)\dots(x+2d_n+1)$$

of degree $d_n + 1$.

Denote the ideal generated by $P_{n,i}(x)$, $i = 0, \dots, d_n+1$, in $\mathbb{Z}[x]$ by I_n. Thus

$$I_n = \left\{ \sum_{i=0}^{d_n+1} S_i(x)P_{n,i}(x) \mid S_i(x) \in \mathbb{Z}[x],\ i = 0, \dots, d_n+1 \right\}.$$

Proposition 4. *Every polynomial in I_n induces the 0 constant function on Q_n.*

Proof. What we need to prove is that, for every $x \in Q_n$

$$p_{n,i}(x) \equiv 0 \pmod{2^n}.$$

This is clear since, for any $x \in Q_n$ the product $(x+1)(x+3)\dots(x+2i-1)$ is a product of i consecutive even numbers and it is therefore divisible by $2^i i!$, implying that it is divisible by 2^{i+t_i}. For $i = 0, \dots, d_n$ we then have that $p_{n,i}(x)$ is divisible by $2^{n-i-t_i} \cdot 2^{i+t_i} = 2^n$. For $i = d_n+1$, we have that $n \leqslant i + t_i$, and therefore 2^n divides $p_{n,i}(x)$ in this case as well. $\square$

We state now the two main results of this section.

Theorem 1. *Two polynomials $P(x)$ and $T(x)$ in $\mathcal{P}_n$ are functionally equivalent over Q_n if and only if $P(x) - T(x)$ is a member of I_n.*

Theorem 2. *Every polynomial function in $\mathcal{PF}_n$ is induced by a unique reduced polynomial in $\mathcal{RP}_n$.*

We will prove the Theorem 1 and Theorem 2 through a series of lemmas and propositions. Along the way we provide some additional information (for instance Proposition 6 establishes a linear upper bound on the degree of a reduced polynomial). While some other approaches are certainly possible, we chose to follow a simple constructive route, since we are interested in algorithmic/complexity issues (see Section 7).

Proof of Theorem 1, *sufficiency.* If $P(x) - T(x)$ is in I_n then, by Proposition 4, $P(x) - T(x)$ induces the constant 0 function on Q_n, implying that $P(x)$ and $Q(x)$ are functionally equivalent over Q_n. □

Proposition 5. *Every polynomial function in $\mathcal{PF}_n$ is induced by a reduced polynomial in $\mathcal{RP}_n$. Moreover, for every polynomial $P(x)$ in $\mathbb{Z}[x]$ there exists a polynomial $S_P(x)$ in I_n such that $P(x) - S_P(x)$ is reduced and functionally equivalent to $P(x)$ over Q_n.*

Proof. Let $p(x)$ be a polynomial function in $\mathcal{PF}_n$ induced by the polynomial $P(x)$.

If the degree d of $P(x)$ is higher than d_n we may replace $P(x)$ by $P(x) - a_d x^{d-d_n-1} P_{n,d_n+1}$, where a_d is the coefficient of x^d in $P(x)$. The polynomial $P(x) - a_d x^{d-d_n-1} P_{n,d_n+1}$ has degree smaller than d and is functionally equivalent to $P(x)$. We may continue this until we obtain a polynomial that is functionally equivalent to $P(x)$ and has degree no higher than d_n.

We assume now that $P(x)$ has degree no higher than d_n. If $P(x)$ is reduced we are done. Otherwise, let i be the highest degree of a coefficient a_i of x^i that does not satisfy the requirement $0 \leqslant a_i \leqslant 2^{n-i-t_i} - 1$. If q is the quotient obtained by dividing a_i by 2^{n-i-t_i} then $P(x) \approx P(x) - qP_{n,i}$, and the coefficient at degree i in $P(x) - qP_{n,i}$ is in the correct range $0, \ldots, 2^{n-i-t_i} - 1$.

We repeat this procedure with the next highest degree that has a coefficient out of range until we reach a reduced polynomial that is functionally equivalent to $P(x)$. □

Example 1. Let $n = 5$. We have $0 + t_0 = 0$, $1 + t_1 = 1$, $2 + t_2 = 3$, $3 + t_3 = 4$ and $4 + t_4 = 7$. Therefore $d_5 = 3$, and every reduced polynomial has the form

$$R(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3,$$

where $0 \leqslant a_0 \leqslant 31$, $0 \leqslant a_1 \leqslant 15$, $0 \leqslant a_2 \leqslant 3$ and $0 \leqslant a_3 \leqslant 1$. The polynomials $P_{5,i}(x)$, $i = 0, 1, 2, 3, 4$ are given by

$$\begin{aligned}
P_{5,0}(x) &= 2^5 = 32,\\
P_{5,1}(x) &= 2^4(x+1) = 16 + 16x,\\
P_{5,2}(x) &= 2^2(x+1)(x+3) = 12 + 16x + 4x^2,\\
P_{5,3}(x) &= 2(x+1)(x+3)(x+5) = 30 + 14x + 18x^2 + 2x^3,\\
P_{5,4}(x) &= (x+1)(x+3)(x+5)(x+7) = 9 + 16x + 22x^2 + 16x^3 + x^4.
\end{aligned}$$

Then, for the polynomial $P(x) = 3x^5 + 1$, we have

$$\begin{aligned} P(x) &= 1 + 3x^5 \approx (1 + 3x^5) - 3xP_{5,4}(x) \approx 1 + 5x + 16x^2 + 30x^3 + 16x^4 \\ &\approx (1 + 5x + 16x^2 + 30x^3 + 16x^4) - 16P_{5,4}(x) \\ &\approx 17 + 5x + 16x^2 + 30x^3 \approx (17 + 5x + 16x^2 + 30x^3) - 15P_{5,3}(x) \\ &\approx 15 + 19x + 2x^2 \approx (15 + 19x + 2x^2) - P_{5,1}(x) \\ &\approx 31 + 3x + 2x^2. \end{aligned}$$

The calculations are done modulo 32 all the time. This is equivalent to using $P_{5,0} = 32$ to make reductions. □

Proposition 6. *Every polynomial function in $\mathcal{PF}_n$ is induced by a polynomial of degree smaller than $(n + 1 + \lfloor \log_2 n \rfloor)/2$.*

Proof. We need to prove that $d_n < (n + 1 + \lfloor \log_2 n \rfloor)/2$.

First note that $i - 1 - \lfloor \log_2 i \rfloor \leqslant t_i$. Indeed $t_i = \lfloor i/2 \rfloor + \lfloor i/4 \rfloor + \dots$. Only the first $\lfloor \log_2 i \rfloor$ terms of the series are possibly positive. Thus $t_i = \sum_{k=1}^{\lfloor \log_2 i \rfloor} \lfloor i/2^k \rfloor > \sum_{k=1}^{\lfloor \log_2 i \rfloor} (i/2^k - 1) = i\left(1 - \frac{1}{2^{\lfloor \log_2 i \rfloor}}\right) - \lfloor \log_2 i \rfloor > i\left(1 - \frac{1}{2^{\log_2 i - 1}}\right) - \lfloor \log_2 i \rfloor = i - 2 - \lfloor \log_2 i \rfloor$.

Assume that $n \geqslant i \geqslant \frac{n+1+\lfloor \log_2 n \rfloor}{2}$. Then

$$i + t_i \geqslant 2i - 1 - \lfloor \log_2 i \rfloor \geq 2\frac{n + 1 + \lfloor \log_2 n \rfloor}{2} - 1 - \lfloor \log_2 n \rfloor = n.$$

Since d_n is the largest integer i such that $n - i - t_i$ is positive, we must have $d_n < \frac{n+1+\lfloor \log_2 n \rfloor}{2}$. □

Lemma 1. *Let M_m be the $(m + 1) \times (m + 1)$ Vandermonde matrix*

$$M_m = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 3 & 3^2 & \dots & 3^m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (2m+1) & (2m+1)^2 & \dots & (2m+1)^m \end{bmatrix},$$

in which the rows and columns are indexed by $0, \dots, m$. The matrix M_m is row equivalent over $\mathbb{Z}$ to a matrix of the form

$$R_m = \begin{bmatrix} 1 & * & \dots & * \\ 0 & 2 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 2^m m! \end{bmatrix},$$

where the $*$'s represent integers (whose values are irrelevant for our purposes), and the only type of row reduction used is the one in which an integer multiple of a row is added to another row.

Proof. We will prove, by induction on m, that

(i) every vector $r_{i,m} = (1, 2i+1, \dots, (2i+1)^m)$, $i \geqslant m+1$, is a linear combination of the rows $0, \dots, m$ in M_m,

(ii) the matrix R_m can be obtained by row reduction of the indicated type from M_m.

(iii) assuming $r_{i,m} = \alpha_0 r_{0,m} + \dots + \alpha_m r_{m,m}$ in (i),

$$r_{i,m+1} - (\alpha_0 r_{0,m+1} + \dots + \alpha_m r_{m,m+1}) = (0, 0, \dots, 0, s_i),$$

where $s_{m+1} = 2^{m+1}(m+1)!$ and s_i is divisible by $2^{m+1}(m+1)!$ if $i \geqslant m+2$.

The claims (i),(ii),(iii) are clear for $m = 0$ and assume they are valid for some $m \geqslant 0$. We proceed to the inductive step.

(i) Consider the vector $r_{i,m+1} = (1, 2i+1, \dots, (2i+1)^{m+1})$, $i \geqslant m+2$. From the inductive assumption (iii),

$$r_{i,m+1} - (\alpha_0 r_{0,m+1} + \dots + \alpha_m r_{m,m+1}) = (0, 0, \dots, 0, s_i)$$

and

$$r_{m+1,m+1} - (\alpha'_0 r_{0,m+1} + \dots + \alpha'_m r_{m,m+1}) = (0, 0, \dots, 0, 2^{m+1}(m+1)!).$$

Since $2^{m+1}(m+1)!$ divides s_i we see that $r_{i,m+1}$ can be indeed written as a linear combination of the rows $0, \dots, m+1$ in M_{m+1}.

(ii) Since, from inductive assumption (iii),

$$r_{m+1,m+1} - (\alpha'_0 r_{0,m+1} + \dots + \alpha'_{m,m} r_{m,m+1}) = (0, 0, \dots, 0, 2^{m+1}(m+1)!).$$

we see that M_{m+1} is row equivalent to a matrix R'_{m+1} in which the bottom row is $(0, 0, \dots, 0, 2^{m+1}(m+1)!)$ and the upper left block of size $(m+1) \times (m+1)$ is M_m. The inductive assumption (ii) shows that R'_{m+1} is row equivalent to R_{m+1}.

(iii) Consider the matrix $M_{m+2}(i)$ obtained from M_{m+1} by extending it by the column vector $(1, 3^{m+2}, \dots, (2m+3)^{m+2})$ on the right and then by the row vector $r_{i,m+2}$, $i \geqslant m+2$, at the bottom. The new matrix is the $(m+3) \times (m+3)$ Vandermonde matrix corresponding to the values $1, 3, 5, \dots, 2m+3$ and $2i+1$. From parts (i) and (ii) of the inductive step that we just proved, we know that $M_{m+2}(i)$ is row equivalent to a matrix $R_{m+2}(i)$ in which the bottom row is $(0, 0, \dots, s_i)$, for some integer s_i, and the upper left block of size $(m+2)\times(m+2)$ is R_{m+1}. The determinant of the Vandermonde matrix $M_{m+2}(i)$ is equal to

$$\begin{aligned}\det(M_{m+2}(i)) =&(3-1)\cdot(5-3)(5-1)\cdot\ldots\cdot((2m+3)-(2m+1))\ldots\\ &\ldots((2m+3)-1)\cdot((2i+1)-(2m+3))\ldots((2i+1)-1)\\ =&\det(M_{m+1})\cdot((2i+1)-(2m+3))\ldots((2i+1)-1).\end{aligned}$$

On the other hand, the row equivalence of $M_{m+2}(i)$ and $R_{m+2}(i)$ shows that

$$\det(M_{m+2}(i))=\det(R_{m+2}(i))=\det(R_{m+1})\cdot s_i=\det(M_{m+1})\cdot s_i.$$

Since $\det(M_{m+1})\neq 0$ we obtain that

$$s_i=((2i+1)-(2m+3))\ldots((2i+1)-1).$$

In case $i=m+2$, $s_{m+2}=2\cdot 4\cdot\cdots\cdot(2(m+2))=2^{m+2}(m+2)!$.

If $i\geqslant m+3$, then s_i is a product of $m+2$ consecutive even numbers and is therefore divisible by $2^{m+2}(m+2)!$. The inductive claim (iii) now easily follows. □

Proof of Theorem 2, uniqueness. Let p be a polynomial function in $\mathcal{PF}_n$. All reduced polynomials inducing p are given by

$$P(x)=a_0+a_1x+\cdots+a_dx^d,$$

where $d=d_n$, and the coefficients $a_0,\ldots,a_d$ satisfy the linear system

$$M_d(a_0,a_1,\ldots,a_d)^T=(p(1),p(3),\ldots,p(2d+1))^T,$$

where $(.)^T$ stands for transposition. By Lemma 1, this system is equivalent in $\mathbb{Z}_{2^n}$ to the upper triangular system

$$R_d(a_0,a_1,\ldots,a_d)^T=(b_0,b_1,\ldots,b_d)^T,$$

where b_i are some elements in $\mathbb{Z}_{2^n}$. Since odd numbers are units in $\mathbb{Z}_{2^n}$ this system is equivalent to a triangular system

$$R'_d(a_0,a_1,\ldots,a_d)^T=(b'_0,b'_1,\ldots,b'_d),$$

where

$$R'_d=\begin{bmatrix}2^{0+t_0} & * & \ldots & * \\ 0 & 2^{1+t_1} & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 2^{d+t_d}\end{bmatrix}. \tag{2}$$

The last equation of this system now reads $2^{d+t_d}a_d = b'_d$. Since $0 \leqslant a_d \leqslant 2^{n-d-t_d} - 1$ this equation can only have one solution in $\mathbb{Z}_{2^n}$. We can substitute this solution in the second to last equation to obtain an equation $2^{d-1+t_{d-1}}a_{d-1} = b''_{d-1}$, which will also have a unique solution in $\mathbb{Z}_{2^n}$ since $0 \leqslant a_{d-1} \leqslant 2^{n-d-1-t_{d-1}} - 1$.

Continuing with the backward substitution in the triangular system with matrix R'_d we obtain a unique solution for all the coefficients $a_d, a_{d-1}, \dots, a_0$ of $P(x)$. $\square$

Proposition 7. *The number of polynomial functions in $\mathcal{PF}_n$ is equal to the number of reduced polynomials in $\mathcal{RP}_n$.*

Example 2. Let $n = 4$. In this case $d = d_4 = 2$. Let p be a polynomial function in $\mathcal{PF}_4$ for which $p(1) = 9$, $p(3) = 5$ and $p(5) = 9$. We are trying to determine the unique reduced polynomial $P(x) = a_0 + a_1x + a_2x^2$ in $\mathcal{RP}_4$ that induces p. Note that the coefficients must satisfy the range conditions $0 \leqslant a_0 \leqslant 15$, $0 \leqslant a_1 \leqslant 7$, and $0 \leqslant a_2 \leqslant 1$. The known values of p give the system

$$\begin{bmatrix} 1 & 1 & 1 & | & 9 \\ 1 & 3 & 9 & | & 5 \\ 1 & 5 & 9 & | & 9 \end{bmatrix},$$

which is row equivalent to

$$\begin{bmatrix} 1 & 1 & 1 & | & 9 \\ 0 & 2 & 8 & | & 12 \\ 0 & 0 & 8 & | & 8 \end{bmatrix}.$$

The last equation $8a_2 = 8$, together with the condition $0 \leqslant a_2 \leqslant 1$, gives $a_2 = 1$. The second equation $2a_1 + 8a_2 = 12$, together with the conditions $a_2 = 1$ and $0 \leqslant a_1 \leqslant 7$, gives $a_1 = 2$. Finally, the first equation $a_0 + a_1 + a_2 = 9$, together with the conditions $a_2 = 1$, $a_1 = 2$ and $0 \leqslant a_0 \leqslant 15$, gives $a_0 = 6$. Thus the unique reduced polynomial inducing p is $P(x) = 6 + 2x + x^2$. $\square$

Example 3. It is clear that one can uniquely determine the reduced polynomial $R(x)$ that is functionally equivalent to $P(x)$ from the value of p at any $d_n + 1$ consecutive values of x.

On the other hand, not any $d_n + 1$ values are sufficient. Indeed, let $n = 4$ and p be a polynomial function in $\mathcal{PF}_4$ for which $p(1) = 9$, $p(5) = 9$ and $p(9) = 9$. We are trying to determine a reduced polynomial $R(x) =$

$a_0 + a_1x + a_2x^2$ in $\mathcal{RP}_4$ that induces p. The known values of p give the system

$$\begin{bmatrix} 1 & 1 & 1 & | & 9 \\ 1 & 5 & 9 & | & 9 \\ 1 & 9 & 1 & | & 9 \end{bmatrix},$$

which, together with the range conditions $0 \leqslant a_0 \leqslant 15$, $0 \leqslant a_1 \leqslant 7$, and $0 \leqslant a_2 \leqslant 1$, gives the following 4 solutions: $R(x) = 9$, $R(x) = 6 + 2x + x^2$, $R(x) = 5 + 4x$, $R(x) = 2 + 6x + x^2$. Note than one of these is the solution obtained in Example 2. $\square$

Proof of Theorem 1, necessity. Let $P(x)$ and $T(x)$ be two functionally equivalent polynomials. By Proposition 5, there exists polynomials $S_P(x)$ and $S_T(x)$ in I_n such that $P(x) - S_P(x)$ and $T(x) - S_T(x)$ are reduced polynomials which are functionally equivalent to $P(x)$ and $T(x)$. Theorem 2 then shows that $P(x) - S_P(x) = T(x) - S_T(x)$, implying that $P(x) - T(x) = S_P(x) - S_T(x) \in I_n$. $\square$

Proposition 8. *The set of polynomials in $\mathbb{Z}_{2^n}[x]$ that induce the 0 constant function on Q_n is precisely the ideal I_n.*

Proof. We already know from Proposition 4 that the polynomials in I_n induce the constant 0 function on Q_n. Conversely, let $P(x)$ induce the constant 0 function on Q_n. By Proposition 5 there exists a polynomial $S_P(x)$ in I_n such that $P(x) - S_P(x)$ is reduced and functionally equivalent to $P(x)$. Since the zero polynomial is reduced, we must have $P(x) - S_P(x) = 0$, by Theorem 2. Therefore $P(x) = S_P(x) \in I_n$. $\square$

4. Permutational polynomial functions on Q_n

Some polynomial function on Q_n are permutations on Q_n. Denote the set of such (permutational) polynomial functions by $\mathcal{PPF}_n$ and the set of polynomials over $\mathbb{Z}$ inducing such functions by $\mathcal{PP}_n$.

Proposition 9. *Let $P(x) = a_0 + a_1x + \cdots + a_dx^d$ be a polynomial in $\mathcal{P}_n$. Then $P(x)$ is in $\mathcal{PP}_n$ (i.e. $P(x)$ induces a permutational polynomial function on Q_n) if and only if the sum of the odd indexed coefficients $a_1 + a_3 + a_5 + \cdots$ is an odd number.*

Proof. Let $a, b \in Q_n$. We have

$p(a) - p(b) = a_1(a - b) + a_2(a^2 - b^2) + \cdots + a_d(a^d - b^d) =$

$= (a-b)(a_1A_1 + a_2A_2 + \cdots + a_dA_d),$

where $A_1 = 1$ and $A_i = a^{i-1} + a^{i-2}b + \cdots + ab^{i-2} + b^{i-1}$, for $i \geqslant 2$. The number A_i is even if and only if i is even. Consequently, $a_1A_1 + a_2A_2 + \cdots + a_dA_d$ is odd if and only if $a_1 + a_3 + a_5 + \cdots$ is odd number.

If $a_1 + a_3 + a_5 + \cdots$ is even then $(a-b)(a_1A_1 + a_2A_2 + \cdots + a_dA_d) \equiv 0 \pmod{2^n}$, for $a = 2^{n-1}+1$, $b = 1$. Thus, for this choice of a and b, we have $p(a) = p(b)$ and, therefore, p is not a permutation on Q_n.

If $a_1 + a_3 + a_5 + \cdots$ is odd then $(a-b)(a_1A_1 + a_2A_2 + \cdots + a_dA_d) \equiv 0 \pmod{2^n}$ if and only if $a - b \equiv 0 \pmod{2^n}$, i.e., $a = b$ in Q_n. Thus p is a permutation in this case. □

Since we have a bijective correspondence between reduced polynomials and polynomial functions, it is clear that we also have a bijective correspondence between the reduced polynomials in $\mathcal{RP}_n$ with odd sum of odd indexed coefficients and the permutational polynomial functions in $\mathcal{PPF}_n$.

Proposition 10. *The number of permutational polynomial functions in $\mathcal{PPF}_n$ is equal to*

$$|\mathcal{PPF}_n| = 2^{(2n-d_n)(d_n+1)/2-2-\sum_{i=0}^{d_n} t_i}$$

Example 4. Reduced polynomials in $\mathcal{RP}_n$ of degree at most 3 that induce permutational polynomial functions in $\mathcal{PPF}_n$ have the form $a_0 + a_1x + a_2x^2 + a_3x^3$, where $a_1 + a_3$ is odd, $a_0 + a_2$ is even, $0 \leqslant a_0 \leqslant 2^n - 1$, $0 \leqslant a_1 \leqslant 2^{n-1} - 1$, $0 \leqslant a_2 \leqslant 2^{n-3} - 1$, and $0 \leqslant a_3 \leqslant 2^{n-4} - 1$. □

Proposition 11. *The inverse of a permutational polynomial function $p \in \mathcal{PPF}_n$ is also a polynomial function.*

Proof. If $p \in \mathcal{PF}_n$ is a permutation on Q_n, then $p \in \sigma(Q_n)$, where $\sigma(Q_n)$ denotes the full permutation group of Q_n. Let r be the order of p in $\sigma(Q_n)$. Then $p^{-1} = p^{r-1}$ and therefore, if p is induced by the polynomial $P(x)$, then p^{-1} is induced by the polynomial $\underbrace{P(P(\dots P(}_{r-1}x)))$. □

Example 5. A linear permutational polynomial function p has a linear permutational polynomial function as its inverse. Indeed, if p is induced by $b + ax$, then a must be odd, a^{-1} exists in $\mathbb{Z}_{2^n}$ and p^{-1} is induced by the polynomial $-a^{-1}b + a^{-1}x$. □

We can use the permutational polynomial functions on Q_n to define permutations on $\mathbb{Z}_{2^n}$ (this will be useful in our last section). Denote by Q'_n the set $\mathbb{Z}_{2^n} \setminus Q_n$ (consisting of 0 and all zero divisors in $\mathbb{Z}_{2^n}$). We can easily conjugate the action of a polynomial function on Q_n to an action on Q'_n. Namely, given a polynomial function $h : Q_n \to Q_n$, define $h' : Q'_n \to Q'_n$ by $h'(x) = h(x+1) - 1$.

Given a permutation $p \in \mathcal{PF}_n$, we can define a permutation $\hat{p}$ on $\mathbb{Z}_{2^n}$ by

$$\hat{p}(x) = \begin{cases} p(x), & x \in Q_n \\ p'(x), & x \in Q'_n \end{cases}. \tag{3}$$

More generally, given permutations $p, h \in \mathcal{PF}_n$, a permutation $f_{p,h}$ on $\mathbb{Z}_{2^n}$ can be defined by

$$f_{p,h} = \begin{cases} p(x), & x \in Q_n \\ h'(x), & x \in Q'_n \end{cases}. \tag{4}$$

5. On a result of Rivest

The main result of Rivest in [15] provides a criterion for a polynomial over $\mathbb{Z}$ to induce a permutation on $\mathbb{Z}_{2^n}$. We infer now this result from our results. Note that our proof only relies on Proposition 2 and Proposition 9, both of which have short and rather elementary proofs.

Theorem 3 (Rivest [15]). *A polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ of degree $d \geqslant 1$ over $\mathbb{Z}$ induces a permutation on $\mathbb{Z}_{2^n}$ if and only if the following conditions are satisfied:*

(a) *the sum $a_2 + a_4 + a_6 + \ldots$ is even,*

(b) *the sum $a_3 + a_5 + a_7 + \ldots$ is even,*

(c) *a_1 is odd.*

Proof. If $P(x)$ is a polynomial that permutes $\mathbb{Z}_{2^n}$ then all elements in $Q'_n = \mathbb{Z}_{2^n} \setminus Q_n$ are mapped to elements of Q'_n or all of them are mapped to elements in Q_n depending on the parity of a_0. Let us first characterize those polynomials over $\mathbb{Z}$ that permute both Q_n and Q'_n. They are precisely the polynomials for which

(i) a_0 is even,

(ii) the sum of all coefficients $a_0 + a_1 + \cdots + a_d$ is odd,

(iii) the sum of the odd index coefficients $a_1 + a_3 + \ldots$ is odd,

(iv) the sum of the odd index coefficients in $P(x+1)-1$ is odd.

The first condition ensures that Q'_n is invariant, the second that Q_n is invariant (Proposition 2), the third that $P(x)$ induces a permutation on Q_n (Proposition 9) and the last that $P(x)$ induces a permutation on Q'_n (by conjugating the action from Q'_n to Q_n we can again use Proposition 9). Let $S(x) = P(x+1)-1$. The sum of odd index coefficients of $S(x)$ is odd exactly when $(S(1)-S(-1))/2$ is odd. But $(S(1)-S(-1))/2 = (P(2)-P(0))/2 = a_1 + 2a_2 + 2^2a_3 + \cdots + 2^{d-1}a_d$, and therefore this condition is equivalent to a_1 being odd. Therefore the conditions (i)-(iv) are equivalent to

(i') a_0 is even,
(ii') the sum $a_2 + a_4 + a_6 + \ldots$ is even,
(iii') the sum $a_3 + a_5 + a_7 + \ldots$ is even,
(iv') a_1 is odd.

Thus, in order to characterize all polynomials that induce a permutation on $\mathbb{Z}_{2^n}$ we just need to drop the condition that a_0 is even (which allows Q_n and Q'_n to be mapped to each other, when a_0 is odd). $\square$

In fact, we may establish a precise connection between the (permutational) polynomial functions on Q_n and those on $\mathbb{Z}_{2^n}$.

Proposition 12. *Let $n \geqslant 2$. For every pair of polynomials functions $p, h \in \mathcal{PF}_n$, there exists a polynomial function g on $\mathbb{Z}_{2^n}$, such that*

$$g(x) = f_{p,h}(x),$$

for x in $\mathbb{Z}_{2^n}$.

Proof. Consider the polynomial

$$V_0(x) = \begin{cases} x^{2^{n-2}}, & n \geqslant 4 \\ x^4, & n = 3, \\ x^2, & n = 2. \end{cases}$$

We claim that, for the associated polynomial function $v_0(x)$ on $\mathbb{Z}_{2^n}$,

$$v_0(x) = \begin{cases} 1, & x \in Q_n, \\ 0, & x \in Q'_n. \end{cases}$$

The claim can be easily verified directly for $n = 2, 3$. Assume $n \geqslant 4$. From Proposition 1, it follows that $v_0(x) = 1$, for $x \in Q_n$. On the other hand, $2^{n-2} \geqslant n$, for $n \geqslant 4$, which then implies that $v_0(x) = x^{2^{n-2}} = 0$, for $x \in Q'_n$.

Let $V_1(x) = 1 - V_0(x)$. For the associated polynomial function $v_1(x)$ we clearly have

$$v_1(x) = \begin{cases} 0, & x \in Q_n, \\ 1, & x \in Q'_n. \end{cases}$$

Therefore, if $P(x)$ and $H(x)$ are polynomial representing the polynomial functions $p(x)$ and $h(x)$ then the polynomial

$$G(x) = P(x)V_1(x) + H'(x)V_0(x),$$

where $H'(x) = H(x+1) - 1$, induces the function $f_{p,h}$, showing that this function is a polynomial function on $\mathbb{Z}_{2^n}$. $\square$

Corollary 2. *Let $n \geqslant 2$. The number of permutational polynomial functions on $\mathbb{Z}_{2^n}$ is*

$$2^{(2n-d_n)(d_n+1)-3-2\sum_{i=0}^{d_n} t_i}, \tag{5}$$

where t_i is the largest integer ℓ such that 2^ℓ divides $i!$, and d_n is the largest integer i such that $n - i - t_i$ is positive.

Proof. Note that the correspondence that associates to each pair of permutational polynomial functions (p,h) on Q_n the element $f_{p,h}$ in the set of permutational polynomial functions on $\mathbb{Z}_{2^n}$ that keep both Q_n and Q'_n invariant is a bijection. Thus, the number of such permutational polynomial functions on $\mathbb{Z}_{2^n}$ is $|\mathcal{PPF}_n|^2$. The number of permutational polynomial functions on $\mathbb{Z}_{2^n}$ is twice larger than this number since we need to take into account the polynomial functions that permute Q_n and Q'_n. Thus, the total number is

$$2|\mathcal{PPF}_n|^2 = 2^{(2n-d_n)(d_n+1)-3-2\sum_{i=0}^{d_n} t_i}. \qquad \square$$

It is interesting to compare the last corollary to earlier results counting permutational polynomial functions on $\mathbb{Z}_{2^n}$. For instance, the following formula is proved in [7]. For $n \geqslant 2$, the number of permutational polynomial functions on $\mathbb{Z}_{2^n}$ is equal to

$$2^{3+\sum_{j=3}^{n} \beta_j}, \tag{6}$$

where β_j is the smallest integer s such that 2^j divides $s!$. Combining this with our result yields the identity

$$2\sum_{i=0}^{d_n} t_i + \sum_{j=3}^{n} \beta_j = (2n - d_n)(d_n + 1) - 6,$$

for $n \geqslant 2$. We note that the number of permutational polynomials given by our formula (5) in Corollary 2 seems easier to evaluate than by using (6), since the summation goes to a smaller bound (d_n rather than n) and the summands are easier to compute.

6. Multiplication operation on reduced polynomials

Here we consider the multiplication operation on the set $\mathcal{RP}_n$ of reduced polynomials.

We recall that $\mathcal{RP}_n$ is the set of representatives of the congruences classes of $\mathcal{P}_n$ modulo the functional equivalence relation $\approx$. In that sense, given $P(x), S(x) \in \mathcal{RP}_n$, we denote by $P(x) \cdot S(x)$ the corresponding reduced polynomial inducing the same polynomial function as the product $P(x)S(x)$ of the polynomials $P(x)$ and $S(x)$. The set $\mathcal{P}_n$ forms a monoid under polynomial multiplication. Indeed, if the sum of the coefficient of both $P(x)$ and $S(x)$ is odd, then $p(1)$ and $s(1)$ are odd and therefore so is p(1)s(1), implying that the sum of the coefficients of $P(x)S(x)$ is also odd.

Theorem 4. *The equivalence $\approx$ is a congruence on $\mathcal{P}_n$. The factor $(\mathcal{RP}_n, \cdot) = \mathcal{P}_n/\approx$ is a finite 2-group.*

Proof. Let $P_i(x) \approx S_i(x)$, for $i = 1, 2$, $T_P(x) = P_1(x)P_2(x)$, and $T_S(x) = S_1(x)S_2(x)$. Then $t_P(x) = p_1(x)p_2(x) = s_1(x)s_2(x) = t_S(x)$. Thus we have $P_1(x)P_2(x) \approx S_1(x)S_2(x)$ and $\approx$ is a congruence on $\mathcal{P}$.

For every $a \in Q_n$, we have $a^{2^{n-2}} = 1$ in Q_n. Therefore, for any polynomial $P(x)$ in $\mathcal{P}_n$, the polynomial $P(x)^{2^{n-2}}$ is functionally equivalent to 1. Thus each reduced polynomial has a multiplicative inverse. □

In order to avoid confusion we denote inverses of polynomial functions under composition by $(.)^{-1}$, and the inverse of a reduced polynomial $P(x)$ under multiplication by $\frac{1}{P(x)}$.

The subset $\mathcal{PRP}_n$ of $\mathcal{RP}_n$ consisting of reduced polynomials that induce permutations on Q_n is not closed under multiplication. Indeed, $P(x) = 2+x$ induces a permutation on Q_n, while $P(x)^2 = 4 + 4x + x^2$ does not.

Proposition 13. *The set of reduced permutational polynomials $\mathcal{PRP}_n$ is closed under multiplicative inversion, i.e., $P(x) \in \mathcal{PRP}_n$ implies $\frac{1}{P(x)} \in \mathcal{PRP}_n$.*

Proof. This directly follows from the fact that different elements in Q_n have different multiplicative inverses. □

Example 6. We have $\frac{1}{2+x} = 2 + x$ in $\mathcal{RP}_3$, $\frac{1}{4+3x} = 3 + 3x + x^2$ in $\mathcal{RP}_4$, and $\frac{1}{31+2x+2x^2+x^3+x^4} = 4 + 7x + 2x^2$ in $\mathcal{RP}_5$. $\square$

We note that finding the inverse polynomial by using the equality $\frac{1}{P(x)} = P(x)^{2^{n-2}-1}$ is not effective. We provide an effective method in the next section.

7. Algorithmic aspects

We briefly address the complexity issues related to interpolation of polynomial functions, inversion of permutational polynomial functions and multiplicative inversion of polynomials.

Theorem 5. *There exists an algorithm of polynomial complexity in n that, given the values $p(1), p(3), \ldots, p(2d_n+1)$ of a polynomial function p in $\mathcal{PF}_n$, produces the unique reduced polynomial $R(x)$ that induces p.*

Proof. Note that d_n has a linear upper bound in n by Proposition 6. Running the row reduction on the $(d_n+1) \times (d_n+1)$ linear system as suggested in the uniqueness part of the proof of Theorem 2 takes polynomially many steps in terms of n. $\square$

Theorem 6. *There exists an algorithm of polynomial complexity in $n+m$ that, given a polynomial $P(x) \in \mathcal{P}_n$ of degree m (with coefficients reduced modulo 2^n, i.e., coefficients in the range between 0 and $2^n - 1$ inclusive), produces the unique reduced polynomial $R(x)$ that is functionally equivalent to $P(x)$.*

Proof. By Theorem 5 it is sufficient to calculate $p(1), p(3), \ldots, p(2d_n + 1)$ in polynomially many steps in terms of $n + m$. This is possible since the degree of $P(x)$ is m and the calculations are done modulo 2^n.

Another approach would be to use the reduction algorithm suggested in the proof of Proposition 5 and implemented in Example 1. $\square$

Theorem 7. *There exists an algorithm of polynomial complexity in $n+m$ that, given a polynomial $P(x)$ in $\mathcal{PP}_n$ of degree m (with coefficients reduced modulo 2^n), produces the unique reduced polynomial inducing the inverse polynomial function p^{-1}.*

Proof. First calculate $p(1), p(3), \ldots, p(2d_n+1)$. Set up a system of linear equations to determine the coefficients of the reduced polynomial $R(x) = a_0 + a_1x + \cdots + a_dx^d$ that is functionally equivalent to p^{-1}, where $d = d_n$. The system has the form

$$\begin{bmatrix} 1 & p(1) & p(1)^2 & \ldots & p(1)^d \\ 1 & p(3) & p(3)^2 & \ldots & p(3)^d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & p(2d+1) & p(2d+1)^2 & \ldots & p(2d+1)^d \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ \vdots \\ 2d+1 \end{bmatrix}.$$

We apply row reduction to this system. The crucial observation is that since, for every $a, b \in Q_n$,

$$P(a) - P(b) = (a-b)k_{a,b},$$

where $k_{a,b}$ is an odd number (see the proof of Proposition 9) and odd numbers are units in $\mathbb{Z}_{2^n}$ the row reduction will eventually lead to a system in which the matrix of the system has the form (2). This system has unique solution that can be found by back substitution. □

Example 7. Let $n = 4$ and $P(x) = 5 + x + x^2$. The polynomial $P(x)$ induces a permutation p on Q_4. We will find the unique reduced polynomial $R(x) = a_0 + a_1x + a_2x^2$, with $0 \leqslant a_0 \leqslant 15$, $0 \leqslant a_1 \leqslant 7$, and $0 \leqslant a_2 \leqslant 1$, that induces the inverse permutation p^{-1} on Q_n.

We calculate $p(1) = 7$, $p(3) = 1$ and $p(5) = 3$. We then perform row reduction (over $\mathbb{Z}_{16}$) on the system

$$\left[\begin{array}{ccc|c} 1 & 7 & 1 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 3 & 9 & 5 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 7 & 1 & 1 \\ 0 & 10 & 0 & 2 \\ 0 & 12 & 8 & 4 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 7 & 1 & 1 \\ 0 & 2 & 0 & 10 \\ 0 & 4 & 8 & 12 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 7 & 1 & 1 \\ 0 & 2 & 0 & 10 \\ 0 & 0 & 8 & 8 \end{array}\right],$$

where the third matrix is obtained from the second by re-scaling the second row by $13 = 5^{-1}$ and the third row by $11 = 3^{-1}$. The last system is triangular and has unique solution $a_2 = 1$ $a_1 = 5$ and $a_0 = 13$. Thus $R(x) = 13 + 5x + x^2$ induces the inverse polynomial function p^{-1}. □

Theorem 8. *There exists an algorithm of polynomial complexity in $n+m$ that, given a polynomial $P(x) \in \mathcal{P}_n$ of degree m (with coefficients reduced modulo 2^n), produces the multiplicative inverse $\frac{1}{P(x)}$ in reduced form.*

Proof. To calculate the reduced polynomial $S(x) = \frac{1}{P(x)}$ it suffices to calculate $p(x)$ for $x = 1, 3, \ldots, 2d_n+1$, then calculate the multiplicative inverses $s(x) = \frac{1}{p(x)}$, for $x = 1, 3, \ldots, 2d_n+1$, and finally use Theorem 5 to find the coefficients of $S(x)$. □

8. Huge quasigroups defined by polynomial functions

A k-groupoid ($k \geqslant 2$) is an algebra (Q, f) on a nonempty set Q as its universe and with one k-ary operation $f : Q^k \to Q$.

Definition 3. A k-groupoid (Q, f) is said to be a *k-quasigroup* if any k out of any $k+1$ elements $a_1, a_2, \dots, a_{k+1} \in Q$ satisfying the equality

$$f(a_1, a_2, \dots, a_k) = a_{k+1}$$

uniquely determine the remaining one.

A k-groupoid is said to be a *cancellative* k-groupoid if it satisfies the cancellation law

$$f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_k) = f(a_1, \dots, a_{i-1}, y, a_{i+1}, \dots, a_k) \Rightarrow x = y,$$

for each $i = 1, \dots, k$ and all $x, y, a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_k$ in Q.

For $k = 2$ we obtain the standard notion of a quasigroup.

The definition of a k-quasigroup immediately implies the following. Let (Q, f) be a finite k-quasigroup and let the map $\varphi : Q \to Q$ be defined by $\varphi(x) = f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_k)$, for some fixed $a_1, \dots, a_{i-1}, a_{i+1}, \dots$ $\dots, a_k$ in Q. Then φ is a permutation on Q.

Here we consider only finite k-quasigroups (Q, f), i.e., Q is a finite set, and in this case we have the following property ([10]).

Proposition 14. *The following statements are equivalent for a finite k-groupoid (Q, f):*

(a) (Q, f) is a k-quasigroup,

(b) (Q, f) is a cancellative k-groupoid. □

Given a k-quasigroup (Q, f) we can define k new k-ary operations f_i, $i = 1, 2, \dots, k$, by

$$f_i(a_1, \dots, a_k) = b \iff f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_k) = a_i.$$

These operations are called adjoint operations of f. Then (Q, f_i) are k-quasigroups as well ([2]).

Definition 4. A *huge* k-quasigroup is said to be a k-quasigroup (Q, f) such that all of the operations $f, f_1, f_2, \dots, f_k$ can be computed with complexity $\mathcal{O}((\log |Q|)^\alpha)$ for some constant α.

The problem of effective constructions of quasigroups of any order can be solved, for example, by using P. Hall's algorithm for choosing different representatives for a family of sets. The algorithm is of complexity $\mathcal{O}(n^3)$, where n is the order of the quasigroup, and is not applicable for, let say, $n = 2^{16}$. We will show here how the permutational polynomial functions from $\mathcal{PF}_n$ can be used in order to construct families of huge quasigroups on the sets Q_n and $\mathbb{Z}_{2^n}$.

Theorem 9. *Let $p_1, p_2, \ldots, p_k$ be permutations in $\mathcal{PPF}_n$. Define a k-ary operation f on Q_n by*

$$f(a_1, a_2, \ldots, a_k) = p_1(a_1)p_2(a_2)\cdots p_k(a_k) \pmod{2^n}. \tag{7}$$

Then the k-groupoid (Q_n, f) is a huge quasigroup.

Proof. Let $r = 2^n$. The permutations in $\mathcal{PPF}_n$ are defined by polynomials $P(x)$ of degree smaller than $(\log_2 r{+}1{+}\lfloor \log_2(\log_2 r)\rfloor)/2$ (by Proposition 6). Then the evaluation of $P(x)$ modulo 2^n can be computed in polynomial complexity with respect to $\log_2 r$. Consequently, the function f defined by (7) can be computed in polynomial complexity with respect to $\log_2 r$.

Consider now the adjoint operations f_i of f. We have, for any $a_1, a_2, \ldots$ $\ldots, a_k, b \in Q_n$:

$$\begin{aligned}
&f_i(a_1, a_2, \ldots, a_k) = b \iff \\
&\quad\iff f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k) = a_i \\
&\quad\iff p_1(a_1)\cdots p_{i-1}(a_{i-1})p_i(b)p_{i+1}a_{i+1}\cdots p_k(a_k) = a_i \\
&\quad\iff p_i(b) = (p_{i-1}(a_{i-1}))^{-1}\cdots(p_1(a_1))^{-1}a_i(p_k a_k)^{-1}\cdots(p_{i+1}(a_{i+1}))^{-1} \\
&\quad\iff b = p_i^{-1}((p_{i-1}(a_{i-1}))^{-1}\cdots(p_1(a_1))^{-1}a_i(p_k a_k)^{-1}\cdots(p_{i+1}(a_{i+1}))^{-1})
\end{aligned}$$

By using the Hensel lifting technique the inverse elements $(p_j(a_j))^{-1}$ can be computed in polynomial complexity with respect to $\log_2 r$ (see Section 2), and the same is true for the inverse permutation p_i^{-1} by Theorem 7. $\square$

Theorem 10. *Let $p_1, p_2, \ldots, p_k$ be permutations in $\mathcal{PPF}_n$. Define a k-ary operation f on $\mathbb{Z}_{2^n}$ by*

$$f(a_1, a_2, \ldots, a_k) = \hat{p_1}(a_1) + \hat{p_2}(a_2) + \cdots + \hat{p_k}(a_k) \pmod{2^n}, \tag{8}$$

where $\hat{p_i}$ are defined by (3). Then the k-groupoid (Q_n, f) is a huge quasigroup.

Proof. The proof is similar to the proof of Theorem 9. We only need to note that the inverse permutation

$$\hat{p_i}^{-1} = \begin{cases} p_i^{-1}(a), & a \in Q_n \\ p_i^{-1}(a+1) - 1, & a \in Q'_n \end{cases}$$

can be computed in polynomially complexity with respect to $\log_2 r$. □

Theorem 11. *Let $p_1, \ldots, p_k$ and $h_1, \ldots, h_k$ be permutations in $\mathcal{PPF}_n$. Define a k-ary operation f on $\mathbb{Z}_{2^n}$ by*

$$f(a_1, a_2, \ldots, a_k) = f_{p_1,h_1}(a_1) + f_{p_2,h_2}(a_2) + \cdots + f_{p_k,h_k}(a_k) \pmod{2^n},$$

where f_{p_i,h_i} are defined by (4)*. Then the k-groupoid (Q_n, f) is a huge quasigroup.* □

We note that Rivest [15] gives a simple necessary and sufficient condition for a bivariate polynomial $P(x, y)$ modulo 2^n to represent a quasigroup on $\mathbb{Z}_{2^n}$, namely $P(x, 0)$, $P(x, 1)$, $P(0, y)$ and $P(1, y)$ should be univariate permutational polynomials on $\mathbb{Z}_{2^n}$. This result is based on his main result in [15] (see Theorem 3 in Section 5).

References

[1] **A. Bandini**, *Functions $f : \mathbb{Z}_{/p^n\mathbb{Z}} \to \mathbb{Z}_{/p^n\mathbb{Z}}$ induced by polynomials of $\mathbb{Z}[X]$*, Annali di Matem. **181** (2002), 95 – 104.

[2] **V. D. Belousov**, *n-ary quasigroups*, (Russian), Stiinca, Kishiniev, 1972.

[3] **G. Carter, E. Dawson and L. Nielsen**, *A latin square version of DES*, In Proc. Workshop of Selected Areas in Cryptography, Ottawa, Canada, 1995.

[4] **J. Cooper, D. Donovan and J. Seberry**, *Secret sharing schemes arising from Latin Squares*, Bull. Inst. Combin. Appl. **4** (1994), 33 – 43.

[5] **J. Dènes and A. D. Keedwell**, *A new authentication scheme based on latin squares*, Discrete Math., **106-107** (1992), 157 – 161.

[6] **D. Gligoroski, S. Markovski, L. Kocarev, and M. Gusev**, *Edon80 Hardware Synchronous stream cipher*, SKEW 2005 - Symmetric Key Encryption Workshop, Aarhus Denmark, 2005.

[7] **G. Keller and F. R. Olson**, *Counting polynomial functions* (*mod p^n*), Duke Math. J. **35** (1968), 835 – 838.

[8] **E. Kaltofen**, *Sparse Hensel Lifting*, EUROCAL'85, European Conf. Comput. Algebra Proc. **2** (1985), $4-17$.

[9] **A. J. Kempner**, *Polynomials and their residue systems*, Amer. Mat. Soc. Trans. **22** (1921), $240-288$.

[10] **S. Markovski, V. Dimitrova and A. Mileva**, *A new method for computing the number of n-quasigroups*, Bul. Acad. Sti. Republ. Moldova, Matematica **3(52)** (2006), $1-84$.

[11] **S. Markovski, S. Samardziska, D. Gligoroski, S. J. Knapskog**, *Multivariate trapdoor functions based on multivariate left quasigroups and left polynomial quasigroups*, Proc. 2nd Inter. Conf. Symbolic Computation and Cryptography SCC 2010, London (in print).

[12] **G. Mullen and H. Stevens**, *Polynomial functions* $\pmod m$, Acta Math. Hung. **44** (1984), $237-241$.

[13] **W. Nöbauer**, *Über permutations polynome und permutation function für primzahl potenzen*, Monatsh. Math. **69** (1965), $230-238$.

[14] **O. Perron**, *Obituary: Kurt Hensel*, Jber. Bayer. Akad. Wiss, München (1948), $234-236$.

[15] **R. L. Rivest**, *Permutation polynomials modulo* 2^w, Finite Fields and Their Appl. **7** (2001), $287-292$.

[16] **C. P. Schnorr and S. Vaudenay**, *Black Box Cryptanalysis of hash networks based on multipermutations*, In Advances of Cryptology - EUROCRYPT'94, Springer, Berlin 1995.

[17] **C. E. Shannon**, *Communication theory of secrecy systems*, Bell Sys. Tech. J. **28** (1949), $657-715$.

[18] **Q. Zhang**, *Polynomial functions and permutation polynomials over some finite commutative rings*, J. Numb. Theory **105** (2004), $192-202$.

Received December 09, 2009

S. Markovski

Ss Cyril and Methodius University, Faculty of Sciences, Institute of Informatics, P.O. Box 162, 1000 Skopje, Republic of Macedonia, E-mail: smile@ii.edu.mk

Z. Šunić

Department of Mathematics, Texas A&M University, College Station, TX 77843-3368, USA E-mail: sunic@math.tamu.edu

D. Gligoroski

Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology, O.S.Brag-stads plass 2B, N-7491 Trondheim, Norway, E-mail: danilog@item.ntnu.no