Permutation Polynomials Modulo 2^w

Ronald L. Rivest
Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139
rivest@mit.edu

October 25, 1999

Abstract

We give an exact characterization of permutation polynomials modulo $n = 2^w$, $w \geq 2$: a polynomial $P(x) = a_0 + a_1x + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo n if and only if a_1 is odd, $(a_2 + a_4 + a_6 + \cdots)$ is even, and $(a_3 + a_5 + a_7 + \cdots)$ is even. We also characterize polynomials defining latin squares modulo $n = 2^w$, but prove that polynomial multipermutations (that is, a pair of polynomials defining a pair of orthogonal latin squares) modulo $n = 2^w$ do not exist.

Keywords: permutation polynomial, latin square, multipermutation.

1 Introduction

A polynomial $P(x) = a_0 + a_1x + \cdots + a_dx^d$ is said to be a *permutation polynomial* over a finite ring R if P permutes the elements of R.

Permutation polynomials have been extensively studied; see Lidl and Niederreiter[4, Chapter 7] for a survey. Permutation polynomials have numerous applications, including cryptography[7]. Indeed, the RSA cryptosystem[13] is one such application.

Most studies have assumed that R is a finite field. See, for example, the survey of Lidl and Mullen[5, 6].

In this paper we consider the case that R is the ring $(\mathbf{Z}_n, +, \cdot)$ where n is a power of two: $n = 2^w$. Modern computers perform computations modulo 2^w efficiently (where $w = 8, 16, 32,$ or 64 is the word size of the machine), and so it is of interest to study permutation polynomials modulo a power of two.

We note that the RC6 block cipher[12] makes essential use of the fact that the polynomial $x(2x+1)$ is a permutation polynomial modulo $n = 2^w$, where w is the word size of the machine.

2 Characterizing Permutation Polynomials

In this section we give a simple characterization of permutation polynomials modulo $n = 2^w$.

Our result stands in surprising contrast to the situation for finite fields, where the problem of determining whether a given input polyomial is a permutation polynomial is quite challenging, and has not yet been shown to be in $\mathcal{P}$. There are, however, efficient probabilistic algorithms for this problem[17, 8].

We assume for convenience that P is an integral polynomial; that is, its coefficients are integers, rather than elements of $\mathbf{Z}_n$. This assumption allows us to talk about the same polynomial with different values of n. In particular, our proof will work by induction on w, where $n = 2^w$.

2.1 The case $n = 2$

The case $n = 2$ $(w = 1)$ is trivial:

Lemma 1 *A polynomial $P(x) = a_0 + a_1x + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 2 if and only if $(a_1 + a_2 + \cdots + a_d)$ is odd.*

Proof: Trivial, since $0^i = 0$ and $1^i = 1$ modulo 2 for $i \geq 1$. ∎

2.2 The case $n = 2^w$, $w > 1$

Lemma 2 *Let $P(x) = a_0 + a_1x + \cdots + a_dx^d$ be a polynomial with integral coefficients and let $n = 2m$, where m is an even positive integer. If $P(x)$ is a permutation polynomial modulo n, then a_1 is odd.*

Proof: If a_1 were even, then then $a_i \cdot 0^i = a_i \cdot m^i = 0 \pmod{n}$ for $i \geq 1$, implying that $P(0) = P(m)$, a contradiction with the assumption that P is a permutation polynomial modulo n. ∎

Lemma 3 *Let $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a polynomial with integral coefficients, let $n = 2^w$, where $w > 0$, and let $m = 2^{w-1} = n/2$. If $P(x)$ is a permutation polynomial modulo n then $P(x)$ is a permutation polynomial modulo m.*

Proof: Clearly, $P(x+m) = P(x) \pmod{m}$, for any x.

Assume that $P(x)$ is a permutation polynomial modulo n. If P is not a permutation polynomial modulo m, then there are two distinct values x, x' modulo m such that $P(x) = P(x') = y \pmod{m}$, for some y. This collision means there are *four* values $\{x, x+m, x', x'+m\}$ modulo n that P maps to a value congruent to y modulo m. But there can only be two such values if P is a permutation polynomial, since there are only two values in $\mathbf{Z}_n$ congruent to y modulo m. ∎

Lemma 4 *Let $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a polynomial with integral coefficients, and let $n = 2m$, If $P(x)$ is a permutation polynomial modulo n, then $P(x+m) = P(x) + m \pmod{n}$ for all $x \in \mathbf{Z}_n$.*

Proof: This follows directly from Lemma 3, since the only two values modulo n that are congruent modulo m to $P(x)$ are x and $P(x) + m$. ∎

Lemma 5 *Let $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a polynomial with integral coefficients, and let $n = 2m$, where m is even, If $P(x)$ is a permutation polynomial modulo m, then $P(x)$ is a permutation polynomial modulo n if and only if $(a_3 + a_5 + a_7 + \cdots)$ is even.*

Proof: By Lemma 2, a_1 is odd. Since $P(x+m) = P(x) \pmod{m}$ for any x, and since P is a permutation polynomial modulo m, the only way P could fail to be a permutation polynomial modulo n would be if $P(x+m) = P(m) \pmod{n}$ for some x.

Since $m = n/2$ is even,

$$(x+m)^i = x^i + imx^{i-1} \pmod{n}$$

for $i \geq 1$. Therefore

$$a_i(x+m)^i = a_i x^i \pmod{n}$$

unless a_i is odd and either

- $i = 1$ or
- $i > 1$ and both x and i are odd,

in which cases

$$a_i(x+m)^i = a_i x^i + m \pmod{n} .$$

Since a_1 is odd, $a_1(x+m) = a_1 x + m \pmod{n}$ for all x. Thus $P(x+m) = P(x) + m \pmod{n}$ for all even $x \in \mathbf{Z}_n$ and $P(x+m) = P(x) + (a_1 + a_3 + a_5 + a_7 + \cdots)m \pmod{n}$ for all odd $x \in \mathbf{Z}_n$. The lemma follows directly. ∎

The previous lemmas can now be combined to give our main theorem.

Theorem 1 *Let $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a polynomial with integral coefficients. Then $P(x)$ is a permutation polynomial modulo $n = 2^w$, $w \geq 2$, if and only if a_1 is odd, $(a_2 + a_4 + a_6 + \cdots)$ is even, and $(a_3 + a_5 + a_7 + \cdots)$ is even.*

Proof: If $P(x)$ is a permutation polynomial modulo n, then a_1 is odd by Lemma 2. Furthermore, $P(x)$ is also a permutation polynomial modulo $m = n/2$, by application of Lemma 3, and so $(a_3 + a_5 + a_7 + \cdots)$ is even, by Lemma 5. Finally, by repeated application of Lemma 3 as necessary, $P(x)$ is a permutation polynomial modulo 2, and so $(a_1 + a_2 + a_3 + \cdots)$ is odd by Lemma 1. The "if" direction of the proof is then complete.

Conversely, if a_1 is odd, $(a_2+a_4+a_6+\cdots)$ is even, and $(a_3+a_5+a_7+\cdots)$ is even, then $P(x)$ is a permutation polynomial modulo $n = 2^w$, by induction on w, using Lemma 1 for the base case ($w = 1$) and Lemma 5 for the inductive step. ∎

Examples. The following are permutation polynomials modulo $n = 2^w$, $w \geq 1$:

- $x(a + bx)$ where a is odd and b is even.
- $x + x^2 + x^4$.
- $1 + x + x^2 + \cdots + x^d$, where $d = 1 \pmod{4}$. (If we work over $GF(p^k)$, where p is odd, instead of modulo 2^w, Matthews[9] shows that this polynomial is a permutation polynomial if and only if $d = 1 \pmod{p(p^k - 1)}$.)

After the first draft of this paper was written, we became aware of the paper by Mullen and Stevens[10], in which it is stated that "It is a direct consequence of Theorem 123 of [3] that $f(x)$ in (2.2) permutes the elements of $\mathbf{Z}/p^n\mathbf{Z}$ if and only if it permutes the elements of $\mathbf{Z}/p\mathbf{Z}$ and $f'(a) \not\equiv 0 \pmod{p}$ for every integer a." [Here the reference number has been changed to match our bibliography, and (2.2) refers to the polynomial representation of f in terms of factorial powers.] An alternate (and slightly simpler) derivation of our main theorem can be obtained using this characterization; details are omitted here. Mullen and Stevens also give a (somewhat complicated) formula for counting the number of polynomials that represent permutations modulo $m = p^n$.

3 Latin Squares and Multipermutations

A function $f : S^2 \rightarrow S$ on a finite set S of size $n > 0$ is said to be a *latin square* (*of order* n) if for any value $a \in S$ both functions $f(a, \cdot)$ and $f(\cdot, a)$ are permutations of S. Latin squares exist for all orders n—e.g. consider addition modulo n.

A pair of functions $f_1(\cdot,\cdot), f_2(\cdot,\cdot)$ is said to be *orthogonal* if the pairs $(f_1(x,y), f_2(x,y))$ are all distinct, as x and y vary. Orthogonal latin squares were first studied by Euler[1] in 1782, who called them *graeco-latin squares*. For an overview of orthogonal latin squares see Lidl and Niederreiter[4, section 9.4] or Hall[2, Chapter 13]. Orthogonal latin squares exist for all orders except $n = 2$ or $n = 6$.

Shannon[15] observed that latin squares are useful in cryptography; more recently Schnorr and Vaudenay[14, 16] applied pairs of orthogonal latin squares (which they called *multipermutations*) to cryptography.

Since the focus of this paper is on polynomials, we now restrict attention to latin squares and multipermutations defined by bivariate polynomials modulo $n = 2^w$.

Since the conditions in Theorem 1 depend only on the parity of the coefficients, it is easy to state necessary and sufficient conditions for a bivariate polynomial to represent a latin square of order $n = 2^w$. For convenience, these conditions are stated in terms of conditions on derived univariate polynomials. The proof is omitted.

Theorem 2 *A bivariate polynomial* $P(x, y) = \sum_{i,j} a_{ij}x^iy^j$ *represents a latin square modulo* $n = 2^w$*, where* $w \geq 2$*, if and only if the four univariate polynomials* $P(x, 0), P(x, 1), P(0, y)$*, and* $P(1, y)$ *are all permutation polynomials modulo* n*.*

Mullen[11] has derived necessary and sufficient conditions for a bivariate polynomial to be a latin square modulo a prime p; these conditions turn out to be rather more complicated than the conditions given here for $n = 2^w$.

For example, here is a second-degree polynomial representing a latin square modulo $n = 2^w$:

$$\begin{aligned} 2xy + x + y &= x \cdot (2y+1) + y \\ &= y \cdot (2x+1) + x \ . \end{aligned}$$

Sadly, however, the situation is different for orthogonal latin squares modulo 2^w, as shown by the following theorem.

Theorem 3 *There are no two polynomials $P_1(x,y)$, $P_2(x,y)$ modulo 2^w for $w \geq 1$ that form a pair of orthogonal latin squares.*

Proof: Lemma 4 implies that $P(x+m) = P(x) + m \pmod{m}$ for any permutation polynomial modulo $n = 2m$. Thus

$$\begin{aligned} P_i(x+m, y+m) &= P_i(x+m, y) + m \pmod{n} \\ &= P_i(x,y) + 2m \pmod{n} \\ &= P_i(x,y) \pmod{n} \end{aligned}$$

Therefore $(P_1(x,y), P_2(x,y)) = (P_1(x+m, y+m), P_2(x+m, y+m))$, and the pair (P_1, P_2) fails (rather badly) at being a pair of orthogonal latin squares. ∎

Acknowledgments

I would like to thank Gary Mullen for bringing a number of relevant references to my attention.

References

[1] L. Euler. Recherches sur une nouvelle espece des quarrés magiques. *Verh. Zeeuwsch Gennot. Weten Vliss*, 9:85–239, 1782.

[2] Marshall Hall, Jr. *Combinatorial Theory.* Blaisdell Publishing Company, 1967.

[3] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford Clarendon Press, fourth edition, 1975.

[4] R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley, 1983.

[5] Rudolf Lidl and Gary L. Mullen. When does a polynomial over a finite field permute the elements of the field? *The American Math. Monthly*, 95(3):243–246, Mar 1988.

[6] Rudolf Lidl and Gary L. Mullen. When does a polynomial over a finite field permute the elements of the field?, II. *The American Math. Monthly*, 100(1):71–74, Jan 1993.

[7] Rudolf Lidl and Winfried B. Müller. Permutation polynomials in RSA-cryptosystems. In D. Chaum, editor, *Proc. CRYPTO 83*, pages 293–301, New York, 1984. Plenum Press.

[8] Keju Ma and Joachim von zur Gathen. The computational complexity of recognizing permutation functions. In *Proc. 26th ACM Symp. on Theory of Computing*, pages 392–401, Montreal, 1994. ACM.

[9] Rex Matthews. Permutation properties of the polynomials $1+x+\cdots+x^k$ over a finite field. *Proc. Amer. Math. Soc.*, 120(1):47–51, Jan 1994.

[10] G. Mullen and H. Stevens. Polynomial functions (mod m). *Acta Mathematica Hungarica*, 44(3–4):237–241, 1984.

[11] Gary L. Mullen. Local polynomials over Z_p. *The Fibonacci Quarterly*, 18(2):104–107, 1980.

[12] Ronald L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin. The RC6 block cipher. Submitted to NIST as a candidate for the AES; See `http://theory.lcs.mit.edu/~rivest/rc6.pdf` or `http://csrc.nist.gov/encryption/aes/`.

[13] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[14] C. P. Schnorr and S. Vaudenay. Black box cryptanalysis of hash networks based on multipermutations. In De Santis, editor, *Proc. EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 47–57, 1994.

[15] C. E. Shannon. Communication theory of secrecy systems. *Bell Sys. Tech. J.*, 28:657–715, 1949.

[16] Serge Vaudenay. On the need for multipermutations: cryptanalysis of MD4 and SAFER. In Bart Preneel, editor, *Fast Software Encryption*,

volume 1008 of *Lecture Notes in Computer Science*, pages 286–297. Springer-Verlag, 1994.

[17] Joachim von zur Gathen. Tests for permutation polynomials. *SIAM J. Computing*, 20(3):591–602, June 1991.