THE COMPOSITIONAL INVERSE OF A CLASS OF PERMUTATION POLYNOMIALS OVER A FINITE FIELD*

ROBERT S. COULTER AND MARIE HENDERSON

Abstract. A new class of bilinear permutation polynomials was recently identified. In this note we determine the class of permutation polynomials which represents the functional inverse of the bilinear class.

1. Introduction and Main Result

Throughout $\mathbb{F}_q$ denotes the finite field of $q = p^e$ elements for some prime p and positive integer e with $\mathbb{F}_q[X]$ representing the ring of polynomials in the indeterminate X over $\mathbb{F}_q$. For polynomials $f, g \in \mathbb{F}_q[X]$, we write $f \circ g = f(g(X))$ for the functional composition of f with g. A *permutation polynomial* over $\mathbb{F}_q$ is a polynomial which, under evaluation, induces a permutation of the elements of $\mathbb{F}_q$. Clearly, permutation polynomials are the only polynomials which have a (functional) inverse with respect to composition, *id est* for a permutation polynomial $f \in \mathbb{F}_q[X]$ there exists (a unique) $f^{-1} \in \mathbb{F}_q[X]$ of degree less than q such that $f(f^{-1}(X)) \equiv f^{-1}(f(X)) \equiv X \bmod (X^q - X)$. We call f^{-1} the compositional inverse of f (or vice versa).

The problem of discovering new classes of permutation polynomials is non-trivial and has generated much interest, see the surveys and open problems given in [3, 4, 6]. Discovering classes where the inverse polynomials can also be described seems to be even more difficult: there are very few known classes of permutation polynomials for which their compositional inverses are also known. To the authors knowledge, the classes with explicit formulae for inverses are:

(1) The linear polynomials: $X + a$ where $a \in \mathbb{F}_q$ is trivially a permutation polynomial of $\mathbb{F}_q$ with the inverse polynomial being $X - a$.

1991 *Mathematics Subject Classification.* 11T06.

*THIS RESEARCH WAS PARTIALLY SUPPORTED BY THE AUSTRALIAN RESEARCH COUNCIL

(2) The monomials: X^n is a permutation polynomial over $\mathbb{F}_q$ if and only if $(n, q-1) = 1$. In such cases, the compositional inverse of X^n is obviously the monomial X^m where $nm \equiv 1 \bmod (q-1)$.
(3) The Dickson polynomials of the 1st kind: $D_n(X, a)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $(n, q^2-1) = 1$, see [5, Chapter 3]. In such cases, for $a \in \{0, \pm 1\}$, the compositional inverse of $D_n(X, a)$ is $D_m(X, a)$ where $nm \equiv 1 \bmod (q^2-1)$, see [5, Chapter 3].

We note that there are classes for which inverses can be determined (for example linearised and sub-linearised polynomials) but that no explicit formulas for the inverses are known.

Recently, a new class of permutation polynomials was introduced in [1]. Here we give a description for the compositional inverse of this class of permutation polynomials.

Theorem 1. *Let $q = 2^k$ for some integer k. Let n be an odd positive integer and set $Q = q^n$. Denote the trace mapping from $\mathbb{F}_Q$ to $\mathbb{F}_q$ by*

$$Tr(X) = X + X^q + \ldots + X^{q^{n-1}}.$$

For any $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$, the polynomial

$$f_\alpha(X) = X\,Tr(X) + (\alpha + 1)X^2$$

is a permutation polynomial over $\mathbb{F}_Q$. For α as above and for any integer i satisfying $1 \le i \le k-1$, define

$$C_i = \frac{\alpha^{2^{k-1}+2^{k-1-i}-1} + 1}{\alpha + 1}.$$

Set

$$A_\alpha(X) = C_{k-1}\left(X^{2^{nk-1}} + \alpha^{2^{k-1}-1}\,Tr(X)^{2^{k-1}}\right)$$

and

$$B_\alpha(X) = \sum_{i=1}^{k-1} C_i\,Tr(X)^{2^{k-1}-2^{k-1-i}} \left(\sum_{j=1}^{(n-1)/2} (X\,Tr(X) + X^2)^{2^{2jk-2-i}} \right).$$

The polynomial $g_\alpha = A_\alpha + B_\alpha$ is the compositional inverse of f_α over $\mathbb{F}_Q$.

The polynomials f_α were shown to be permutation polynomials in [1]. From Theorem 1 we have the following obvious corollary.

Corollary 2. *For $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$, the polynomials g_α, as defined in Theorem 1, are permutation polynomials over $\mathbb{F}_Q$.*

Bull. Austral. Math. Soc. 65 (2002), 521-526

2. The Proof of Theorem 1

Our attention from this point is directed to establishing the remaining statements of Theorem 1, which is to show that g_α is the compositional inverse of f_α. Our proof involves establishing a set of sequential propositions, basically involving closer examination of $f_\alpha \circ g_\alpha$, primarily in terms of the two polynomials A_α and B_α. For n odd, we have $\mathrm{Tr}(\mathrm{Tr}(x)) = \mathrm{Tr}(x)$. This identity is used many times in the following propositions. We begin by collecting some useful identities.

Proposition 3. *For $A_\alpha, B_\alpha \in \mathbb{F}_Q[X]$ and C_i as defined in Theorem 1 we have*

(i) $C_i^2 = (\alpha^{(2^{k-i}-1)} + 1)/(\alpha^2 + 1)$,
(ii) $A_\alpha^2(X) \equiv C_{k-1}^2(X + \alpha^{-1}\,Tr(X)) \bmod (X^Q + X)$,
(iii) $Tr(A_\alpha) \equiv \alpha^{2^{k-1}-1}\,Tr(X)^{2^{k-1}} \bmod (X^Q + X)$, *and*
(iv) $Tr(B_\alpha) \equiv 0 \bmod (X^Q + X)$.

Proof. (i) Squaring C_i we obtain the identity:

$$C_i^2 = \frac{\alpha^{2^k+2^{k-i}-2} + 1}{\alpha^2 + 1} = \frac{\alpha^{2^{k-i}-1} + 1}{\alpha^2 + 1}.$$

(ii) Squaring $A_\alpha(X)$ gives $C_{k-1}^2(X^{2^{nk}} + \alpha^{2^k-2}\mathrm{Tr}^{2^k}(X))$ which reduced modulo $(X^Q + X)$ is $C_{k-1}^2(X + \alpha^{-1})$
(iv) Using the definition of $A_\alpha(X)$ given in Theorem 1,

$$\begin{aligned}\mathrm{Tr}(A_\alpha(X)) &= C_{k-1}(\mathrm{Tr}(X)^{2^{nk-1}} + \alpha^{(2^{k-1}-1)}\mathrm{Tr}(X)^{2^{k-1}}) \\ &\equiv \mathrm{Tr}(X)^{2^{k-1}} C_{k-1}(1 + \alpha^{(2^{k-1}-1)}) \bmod (X^Q + X) \\ &\equiv \alpha^{(2^{k-1}-1)}\mathrm{Tr}(X)^{2^{k-1}} \bmod (X^Q + X).\end{aligned}$$

(v) This is immediate as $\mathrm{Tr}(X\,\mathrm{Tr}(X) + X^2) = 0$. □

The proof of the following result is tedious but seemingly necessary.

Proposition 4. *Using the same notation as above then*

$f_\alpha(g_\alpha(X)) \bmod (X^Q + X)$

$$= X + c_\alpha\Big(X^{2^{nk-1}}\,Tr(X)^{2^{k-1}} + Tr(X) + \sum_{i=1}^{k} Tr(X)^{2^k-2^{k-i}} S_i(X)\Big)$$

where $c_\alpha = (\alpha^{(2^{k-1}-1)} + 1)/(\alpha + 1)$ and

$$S_i(X) = \sum_{j=1}^{(n-1)/2} (X\,Tr(X) + X^2)^{2^{2jk-i-1}} \qquad (1)$$

Proof. By expanding $f_\alpha(X) \circ g_\alpha(X)$ (with $g_\alpha(X) = A_\alpha(X) + B_\alpha(X)$) and using Proposition 3 (iv),

$$\begin{aligned} &f_\alpha(g_\alpha(X)) \bmod (X^Q + X) \\ &\qquad = (A_\alpha(X) + B_\alpha(X))\mathrm{Tr}(A_\alpha(X)) + (\alpha+1)(A_\alpha^2(X) + B_\alpha^2(X)). \end{aligned}$$

We split the terms of this sum so that $f_\alpha(X) \circ g_\alpha(X) = a(X) + b(X) \bmod (X^Q + X)$ where $a(X) = A_\alpha(X)\mathrm{Tr}(A_\alpha(X)) + (\alpha+1)A_\alpha^2(X)$ and $b(X) = B_\alpha(X)\mathrm{Tr}(A_\alpha(X)) + (\alpha+1)B_\alpha^2(X)$. Using Proposition 3 (ii) and (iii),

$$\begin{aligned} a(X) =& C_{k-1}^2(\alpha^{(2^{k-1}-1)} + 1)(X^{2^{nk-1}}\mathrm{Tr}(X)^{2^{k-1}} + \alpha^{(2^{k-1}-1)}\mathrm{Tr}(X)) \\ &+ C_{k-1}^2(\alpha+1)(X + \alpha^{-1}\mathrm{Tr}(X)) \bmod (X^Q + X). \end{aligned}$$

From Proposition 3 (i), $C_{k-1}^2 = (\alpha+1)^{-1}$ and as $c_\alpha = c_\alpha\alpha^{(2^{k-1}-1)} + \alpha^{-1}$ then

$$a(X) = X + c_\alpha(X^{2^{nk-1}}\mathrm{Tr}(X)^{2^{k-1}} + \mathrm{Tr}(X)) \bmod (X^Q + X).$$

Next put $b_1(X) = \mathrm{Tr}(A_\alpha(X))B_\alpha(X)$. Identically

$$b_1(X) = \alpha^{(2^{k-1}-1)}\mathrm{Tr}(X)^{2^{k-1}} \sum_{i=1}^{k-1} C_i \mathrm{Tr}(X)^{(2^k - 2^{k-1-i})} S_{i+1}(X).$$

Using $\alpha^{(2^{k-1}-1)}C_i = (\alpha^{(2^{k-1}-1)} + \alpha^{(2^{k-i}-1)})/(\alpha+1)$ and re-writing the sum in $b_1(X)$ then we arrive at

$$b_1(X) = \sum_{i=2}^{k} \Big(\frac{\alpha^{(2^{k-1}-1)} + \alpha^{(2^{k-i}-1)}}{\alpha+1}\Big)\mathrm{Tr}(X)^{(2^k - 2^{k-i})} S_i(X). \tag{2}$$

Finally, put $b_2(X) = (\alpha+1)B_\alpha^2(X)$. Then

$$b_2(X) = (\alpha+1)\sum_{i=1}^{k-1} C_i^2 \mathrm{Tr}(X)^{(2^k - 2^{k-1-i})} S_{i+1}^2(X).$$

As $S_{i+1}^2(X) = S_i(X)$, from Proposition 3 (i) we have

$$b_2(X) = \sum_{i=1}^{k-1} \Big(\frac{\alpha^{(2^{k-i}-1)} + 1}{\alpha+1}\Big)\mathrm{Tr}(X)^{(2^k - 2^{k-i})} S_i(X). \tag{3}$$

So from Equations 2 and 3 we have

$$\begin{aligned} b(X) &= b_1(X) + b_2(X) \\ &= \sum_{i=2}^{k-1} c_\alpha \mathrm{Tr}(X)^{(2^k-2^{k-i})} S_i(X) + c_\alpha \mathrm{Tr}(X)^{(2^k-2^{k-1})} S_1(X) + c_\alpha S_k(X) \\ &= c_\alpha \sum_{i=1}^{k} \mathrm{Tr}(X)^{(2^k-2^{k-i})} S_i(X). \end{aligned}$$

The result now follows from calculating the sum $a(X) + b(X)$. □

Proposition 5. *For $\beta \in \mathbb{F}_q$ then $f_\alpha(g_\alpha(\beta X)) = \beta f_\alpha(g_\alpha(X))$.*

Proof. As $\mathrm{Tr}(\beta X) = \beta \mathrm{Tr}(X)$, it is simple to see

$$(\beta X)^{2^{nk-1}} + \mathrm{Tr}(\beta X)^{2^{k-1}} + \mathrm{Tr}(\beta X) = \beta(X^{2^{nk-1}} + \mathrm{Tr}(X)^{2^{k-1}}).$$

For $\beta \in \mathbb{F}_q$, from Equation 1

$$S_i(\beta X) = \sum_{j=1}^{(n-1)/2} \beta^{2^{2jk-i}} (X\mathrm{Tr}(X) + X^2)^{2^{2jk-i-1}} = \beta^{2^{k-i}} S_i(X).$$

and it follows

$$\begin{aligned} \sum_{i=1}^{k} \mathrm{Tr}(\beta X)^{(2^k-2^{k-i})} \beta^{2^{k-i}} S_i(X) &= \sum_{i=1}^{k} \beta^{2^k} \mathrm{Tr}(X)^{(2^k-2^{k-i})} S_i(X) \\ &= \beta \sum_{i=1}^{k} \mathrm{Tr}(X)^{(2^k-2^{k-i})} S_i(X). \end{aligned}$$

We then have, using Proposition 4 and these identities, that for $\beta \in \mathbb{F}_q$, $f_\alpha(g_\alpha(\beta X)) = \beta f_\alpha(g_\alpha(X))$ as required. □

Proof of Theorem 1: For $x \in \mathbb{F}_Q$, if $\mathrm{Tr}(x) = 0$ then from Proposition 4 it follows directly that $f_\alpha(g_\alpha(x)) = x$. Suppose $\mathrm{Tr}(x) = 1$ for $x \in \mathbb{F}_Q$.

Using Proposition 4

$$\begin{aligned} f_\alpha(g_\alpha(x)) &= x + c_\alpha\Big(x^{2^{nk-1}} + 1 + \sum_{i=1}^{k}\sum_{j=1}^{(n-1)/2}(x+x^2)^{2^{2jk-1-i}}\Big) \\ &= x + c_\alpha\Big(x^{2^{nk-1}} + 1 + \sum_{j=1}^{(n-1)/2}\sum_{i=0}^{k}(x+x^2)^{2^{2jk-1-i}}\Big) \\ &= x + c_\alpha\Big(x^{2^{nk-1}} + 1 + \sum_{j=1}^{(n-1)/2} x^{2^{2jk}} + x^{2^{(2j-1)k}}\Big) \\ &= x + c_\alpha(1+\mathrm{Tr}(x)). \end{aligned}$$

As we have assumed that $\mathrm{Tr}(x) = 1$ then again $f_\alpha(g_\alpha(x)) = x$. Every element $y \in \mathbb{F}_Q$ satisfying $\mathrm{Tr}(y) \neq 0$ can be written in the form $y = \beta x$ where $\beta \in \mathbb{F}_q$, and $\mathrm{Tr}(x) = 1$ for some $x \in \mathbb{F}_Q$. By Proposition 5, $f_\alpha(g_\alpha(y)) = \beta f_\alpha(g_\alpha(x)) = \beta x = y$. Thus $f_\alpha(g_\alpha(X)) \equiv X \bmod (X^q + X)$. □

The determination of the inverse class given in this article relied on using the MAGMA algebra package [2] to generate examples for small fields. This result underlines that, in general, inverses for known permutation polynomial classes are not simple to describe.

References

[1] A. Blokhuis, R.S. Coulter, M. Henderson, and C.M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Finite Fields and Applications: proceedings of the Fifth International Conference on Finite Fields and Applications (D. Jungnickel and H. Niederreiter, eds.), 2001, pp. 37–42.

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[3] R. Lidl and G.L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly **95** (1988), 243–246.

[4] ———, *When does a polynomial over a finite field permute the elements of the field?, II*, Amer. Math. Monthly **100** (1993), 71–74.

[5] R. Lidl, G.L. Mullen, and G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Appl. Math., vol. 65, Longman Scientific and Technical, Essex, England, 1993.

[6] G.L. Mullen, *Permutation polynomials: a matrix analogue of schur's conjecture and a survey of recent results*, Finite Fields Appl. **1** (1995), 242–258.

Bull. Austral. Math. Soc. 65 (2002), 521-526

Information Security Research Centre, Queensland University of Technology, GPO Box 2434, Brisbane, Queensland, 4001, Australia
E-mail address: shrub@isrc.qut.edu.au

Centre for Discrete Mathematics and Computing, Department of Computer Science and Electrical Engineering, The University of Queensland, St. Lucia, Queensland, 4072, Australia
E-mail address: marie@itee.uq.edu.au

Bull. Austral. Math. Soc. 65 (2002), 521-526