Indian J Pure Appl Math (2026) 57:1685–1690
https://doi.org/10.1007/s13226-024-00668-3

ORIGINAL RESEARCH

Construction of permutation polynomials with specific cycle structure over finite fields

Anitha G · P. Vanchinathan

Received: 7 November 2023 / Accepted: 11 June 2024 / Published online: 22 July 2024
© The Indian National Science Academy 2024

Abstract For a finite field of odd order q, and a divisor n of $q-1$, we construct families of permutation polynomials of n terms with one fixed-point (namely zero) and remaining elements being permuted as disjoint cycles of same length. Our polynomials will all be of same format: that is the degree, the terms are identical. For our polynomials their compositional inverses are also polynomials in the same format and are easy to write down. The special cases of $n = 2, 3$ give very simple families of permutation binomials and trinomials. For example, in the field of 121 elements our methods provide 4080 permutation trinomials all decomposing into three disjoint cycles of length 40 along with a unique fixed point.

Keywords Permutation polynomials · Binomial · Trinomial · Cycle type

1 Introduction

Polynomials defined over finite fields which are bijective functions on that field have been an object of study by Hermite[8] and Dickson [5] in late nineteenth century. Called permutation polynomials they have found applications in cryptography, algebraic coding theory and in combinatorics [1,19,25,27].

Any automorphism of the multiplicative group extended to the whole field by sending 0 to 0, is given by monomials $f(x) = x^k$, with k coprime to the order of the multiplicative group.

These monomials along with the linear polynomials $ax + b,\ a \neq 0$ are readily the easiest permutation polynomials one can think of.

More and more families of permutation polynomials have been found by various mathematicians. Chapter 8 of the monograph by Mullen and Panerio [22] and Chapter 7 of Lidl and Niedereiter [20] and the survey article [9] by Hou provide a wealth of information on varieties of permutation polynomials. Due to ease of applying to electronic hardware, permutation polynomials for fields of characteristic 2 have received lot of attention. (See, for example, [24,28,29].)

Permutation binomials with terms involving just $X^{(q+1)/2}$ and X over a finite field $\mathbf{F}_q$ have been completely determined. (See page 352, Theorem 7.11 in [20], for a list of normalised binomials). A result of Carlitz and Wells [3] assures existence of permutation binomials of the form $x^{d+1} + ax$ for all $d|q-1$. More results on binomial permutations are in Lappano [16], Hou and Lappano [13], Hou and Lavorante [15] and [23]. Another survey article by Hou [12] is exclusively devoted to permutation binomials and trinomials.

Communicated by V Arvind.

Anitha G. · P. Vanchinathan (✉)
School of Advanced Sciences Vellore Institute of Technology, Chennai 600 127, India
E-mail: vanchinathan.p@vit.ac.in

Anitha G.
E-mail: anitha.g2019@vitstudent.ac.in

Newer construction of permutation trinomials can be found in the works of Bartoli and Timponella [2], Gupta and Sharma [6] (in characteristic 2), Hou, [10,11], Lavorante [14], and Li, Qu and Chen [18].

However, the determination of the cycle type as a permutation for known permutation polynomials is a difficult task. Knowing the cycle type for a permutation polynomial $f(x)$ does not make it easy to determine the same for $cf(x)$ for a constant c. (Because the cycle type of composition of two permutations is tricky even when we know it for them individually). There does not seem to be any easily discernible relationship between polynomials on the one hand, and the cycle types of the permutations they provide on the other. Even the problem of giving a family of polynomials all giving rise to permutations of some specific cycle type is stated to be difficult (see [4]) as recently as in the year 2022. Recent work [21] discusses a weaker notion of cycle structure, their main aim being construction of complete permutation polynomials. Their result, for example, will not distinguish between two permutations of 7 elements having cycle type $3+1+1+1+1$ and $3+3+1$ respectively. Otherwise literature on this question is very limited. *In this paper we report our findings on constructing families of permutation polynomials which are simultaneously simple as polynomials (binomial, trinomial etc) and have uncomplicated cycle type.*

For all the polynomials that we constructed the inverse polynomials also turn out to be in the same format, i.e., having the same degree, same terms and natural choice of coefficients.

At the outset we would like to mention that all the permutation polynomials constructed in this paper fall under the category of cyclotomic mappings. (See [26]). However, our proofs make no use of results from cyclotomic mappings.

The following elementary fact which is easy to prove will be repeatedly used:

Lemma 1.1 *Let R be a commutative ring with unity. Assume the group of units of R has a finite subgroup U, say, of order M. Let $u \in U$, be an element of order m, and let $d = M/m$. Then, (i) the function $f : U \to U$ defined as $f(x) = ux$ is a permutation of U, (ii) $f(x)$ takes each coset of the cyclic subgroup generated by u in U to itself and (iii) the cycle type of the permutation given by $f(x)$ on U is*

$$\underbrace{m + m + \cdots + m}_{d \text{ terms}}$$

Note: In future we will use the simpler notation m^d, to indicate the occurrence of d disjoint cycles of length m.

Before giving a description of our work we need to set up our notations.

Notations and Conventions:

q:	Power of an odd prime
$\mathbf{F}_q$:	Finite field of order q
g:	A generator of $\mathbf{F}_q^*$
m, d:	Pair of integers factorizing $q-1$ as $q-1 = md$
φ:	Euler totient function
H_0:	The subgroup of $\mathbf{F}_q^*$ of order m (and hence index d)
H_i:	Coset of H_0 by g^i, $i = 0, 1, \ldots, d-1$

By the order of a (non-zero) element, we always mean the order as an element of the *multiplicative group* of the field.

Note that our definition of m, d allows us to express any element of $\mathbf{F}_q^*$ uniquely as g^{i+dj} for $i = 0, 1, \ldots, d-1$ and $j = 0, 1, \ldots, m-1$.

2 Main results

With all the notations set up we are now ready to state our results. The first result constructs permutation polynomials of n terms, for $n|(q-1)$.

Theorem 2.1 *Let $n > 1$ be a positive integer. Consider any finite field $\mathbf{F}_q$ with $q \equiv 1 \pmod{n}$ and let $\zeta = g^{(q-1)/n}$, an element of order n. We assume d to be a multiple of n and $\varphi(m) \geq n$. For any n elements*

$u_0, u_1, \ldots, u_{n-1}$ from $\mathbf{F}_q^*$ all of the same order m, we define a new set of n elements $a_t \in \mathbf{F}_q$, $t = 0, 1, 2, \ldots, n-1$, by the follwoing Vandermonde linear transformation:

$$\begin{pmatrix} a_{n-1} \\ a_{n-2} \\ a_{n-3} \\ \vdots \\ a_1 \\ a_0 \end{pmatrix} = \frac{1}{n} \begin{pmatrix} 1 & \zeta & \zeta^2 \cdots & \zeta^{n-2} & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 \cdots & \zeta^{2(n-2)} & \zeta^{2(n-1)} \\ 1 & \zeta^3 & \zeta^6 \cdots & \zeta^{3(n-2)} & \zeta^{3(n-1)} \\ \vdots & \vdots & \vdots \cdots & \vdots & \vdots \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} \cdots & \zeta^{(n-1)(n-2)} & \zeta^{(n-1)(n-1)} \\ 1 & 1 & 1 \cdots & 1 & 1 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-2} \\ u_{n-1} \end{pmatrix} \tag{1}$$

Then the polynomial,

$$f(x) = x \sum_{t=0}^{n-1} a_t x^{t(q-1)/n}$$

(i) is a permutation polynomial on $\mathbf{F}_q$.
(ii) the permutation has cycle type $1 + m^d$.
(iii) the permutation inverse to this is also given by a polynomial of again n terms involving the same powers of x as $f(x)$. Its coefficients are determined by another Vandermonde transformation (1) obtained from the above by replacing u_i, $0 \le i \le n-1$ with its inverse in $\mathbf{F}_q^*$.

Proof Before going to the proof we first note, for future use, that the a_t's are defined in terms of u_t's with Vandermonde matrix. The inverse for this matrix is well-known, allowing us to express u's in terms of a's as below:

$$u_r = \sum_{t=0}^{n-1} a_t \zeta^{rt} \tag{2}$$

Now we get on to the proof. As $f(x)$ maps zero to zero we only need to analyze what it does to nonzero elements. The nonzero elements are given as g^{i+dj} with $i = 0, 1, \ldots, d-1$, $j = 0, 1, \ldots, m-1$. Our hypothesis has n as a divisor of d. To evaluate $f(x)$ at g^{i+dj} we express i as $i = nk + r$, $0 \le r < n$, for some k.

$$\begin{aligned} f(g^{nk+r+dj}) &= g^{nk+r+dj} \sum_{t=0}^{n-1} a_t \left(g^{nk+r+dj}\right)^{t(q-1)/n} \\ &= g^{nk+r+dj} \sum_{t=0}^{n-1} a_t \left(\zeta^{(nk+r+dj)t}\right) \\ &= g^{nk+r+dj} \sum_{t=0}^{n-1} a_t \zeta^{rt} \\ &= u_r g^{nk+r+dj} \quad \text{by using Eq. (2)} \end{aligned}$$

So the polynomial $f(x)$ represents the function admitting the description below:

$$f(g^{i+dj}) = u_r g^{i+dj}.$$

(Note that as per our notation the subscript r above is the least non-negative integer obtained from i by going modulo n.) Now it is clear that $f(x)$ is a permutation polynomials and its cycle type can be deduced from Lemma 1.1 to be $1 + m^d$. □

Now we state a variation, with the same notation, of the above theorem with u's of different multiplicative orders.

Theorem 2.2 *For any n elements $u_0, u_1, \ldots u_{n-1}$ from $\mathbf{F}_q^*$, not all the same, with u_i of order m_i dividing m, write $n_i = \frac{m}{m_i}$, $0 \le i \le n-1$. The polynomial $f(x)$ given in Theorem (2.1)*

(i) *is a permutation polynomial on $\mathbf{F}_q$.*

(ii) *the permutation has cycle type*

$$1 + m_0^{dn_0/n} + m_1^{dn_1/n} + m_2^{dn_2/n} + \cdots$$

(iii) *its inverse permutation is also a polynomial of n terms involving the same powers of x as $f(x)$. Its coefficients are determined from the system (1) modified by replacing u_i's with their inverses.*

The proof for Theorem 2.1 given above works for this case too without any change, except for the statement about cycle type. The mildly more complicated cycle type is a consequence of u_i's being of different orders now and not difficult to see, and so the details of the proof are omitted.

Now we want to state two important special cases of Theorem 2.2 where we get permutation binomials and trinomials respectively. There the structure of polynomial is very simple and more transparent.

Theorem 2.3 (Special case $n = 2$) *Under the notation of the Introduction, with the restriction of d being even, choose two distinct elements u, v from the subgroup H_0. Let their orders be m_0 and m_1 respectively, write $n_i = m/m_i,\ i = 0, 1$. The binomial*

$$f(x) = ax^{(q+1)/2} + bx$$

where $a = (v - u)/2$ and $b = (u + v)/2$

(i) *is a permution binomial on $\mathbf{F}_q$.*
(ii) *the permutation has cycle type $1 + m_0^{dn_0/2} + m_1^{dn_1/2}$*
(iii) *the inverse of this permutation is also a binomial given by*

$$f^{-1}(x) = a'x^{(q+1)/2} + b'x$$

where $a' = (v^{-1} - u^{-1})/2$ and $b' = (u^{-1} + v^{-1})/2$.

Theorem 2.4 (Special case $n = 3$) *Let $q \equiv 1 \pmod 3$ and ζ be an element of order 3 in the multiplicative group of the field of q elements. Consider the positive integers m, d such that $d \equiv 0 \pmod 3$, $q - 1 = md$. For any three elements $u, v, w \in \mathbf{F}_q^*$ whose orders are m_0,m_1 and m_2 respectively, write $n_i = \frac{m}{m_i},\ i = 0, 1, 2$.*

The trinomial

$$f(x) = ax^{(2q+1)/3} + bx^{(q+2)/3} + cx$$

where $a = (u + v\zeta + w\zeta^2)/3$, $b = (u + v\zeta^2 + w\zeta)/3$ and $c = (u + v + w)/3$

(i) *is a permution trinomial on $\mathbf{F}_q$*
(ii) *the permutation has cycle type*

$$1 + m_0^{dn_0/3} + m^{dn_1/3} + m_2^{dn_2/3}$$

(iii) *its inverse permutation also trinomial given by*

$$f^{-1}(x) = a'x^{(2q+1)/3} + b'x^{(q+2)/3} + c'x$$

where $a' = (u^{-1} + v^{-1}\zeta + w^{-1}\zeta^2)/3$, $b' = (u^{-1} + v^{-1}\zeta^2 + w^{-1}\zeta)/3$ and $c' = (u^{-1} + v^{-1} + w^{-1})/3$.

Remark 1 In [23] authors construct binomials where the coefficients are in similar format as $(v - u)/2$ and $(v + u)/2$. There the condition is simply that these u, v be both squares or both non-squares. Here we have additional constraints that both be of same order. But we reap the benefit of being able to say that these constructions provide permutations of specific cycle type.

Remark 2 This method shows, for any divisor m of $q - 1$, that there exist a family of (at least) $\varphi(m)(\varphi(m) - 1)$ binomials of degree $(q + 1)/2$ of cycle type $1 + m^d$ when $d = (q - 1)/m$ is even. To compute the number of trinomials for the case of $q = 11^2 = 121$, and the factorization $q - 1 = 40 \times 3$: we have $\varphi(40) = 16$ elements of order 40 from which we select 3 (at least 2 of them distinct) and permute them. This number is calculated to be $16!/(16 - 3)! + 16 * 15 * 3 = 4080$. These 4080 polynomials not only of the same cycle type they are in the format: $aX^{81} + bX^{41} + cX$. (More of this kind of data is computed and tabulated at the end of the paper).

While Theorem 2.1 constructs polynomials of n terms based on a choice of n elements we now present a new kind based on choice of just 2 elements. For this we take a factorization $q-1=md$, (q, as usual, is the order of our finite field assumed odd) with $d>2$, and construct a polynomial of $d+1$ terms where only two coefficients are distinct. More precisely:

Theorem 2.5 *For two distinct elements $u, v \in \mathbf{F}_q^*$, both of the same order m define and $a=\frac{u-v}{d}$. Then the polynomial*

$$f(x)=a\sum_{i=0}^{d-1}x^{im+1}+vx$$

is a permutation polynomial giving a permutation of cycle type $1+m^d$.

Proof Since given polynomial takes the value zero at zero, enough to show $f(x)$ permutes all non-zero elements which is shown by considering two cases: Let $b \in \mathbf{F}_q^*$.

Case: $b \in H_0$

$$\begin{aligned} f(b) &= a(b+b^{m+1}+b^{2m+1}+\cdots+b^{(d-1)m+1})+vb \\ &= ab(1+b^m+\cdots+b^{(d-1)m})+vb \\ &= abd+vb \quad (\text{since } b^m=1.) \\ &= ub \quad (\text{substituting value of } a.) \end{aligned}$$

Case: $b \notin H_0$

$$\begin{aligned} f(b) &= a(b+b^{m+1}+b^{2m+1}+\cdots+b^{(d-1)m+1})+vb \\ &= ab(1+b^m+\cdots+b^{(d-1)m})+vb \\ &= vb \quad (\text{since } 1+b^m+\cdots+b^{(d-1)m}=0) \end{aligned}$$

this completes the proof for the fact that $f(x)$ is a permutation polynomial; the cycle type is deduced by again appealing to Lemma 1.1. The statement about the compositonal inverse of this polynomial is also proved by arguments used earlier. □

Example We tabulate below, for the finite field of $121=11^2$ elements, the count of binomials and trinomials we were able to construct having specific cycle type. Each row of the table corresponds to a choice of factorization of 120= $m \times d$ leading to a specific conjugacy class of permutations.

Polynomial type	m	d	Cycle type	Count
$aX^{61}+bX$	3	40	$1+3^{40}$	2
	4	30	$1+4^{30}$	2
	5	24	$1+5^{24}$	12
	6	20	$1+6^{20}$	2
	10	12	$1+10^{12}$	12
	12	10	$1+12^{10}$	12
	15	8	$1+15^8$	56
	20	6	$1+20^6$	56
	30	4	$1+30^4$	56
	60	2	$1+60^2$	240
$aX^{81}+bX^{41}+cX$	5	24	$1+5^{24}$	60
	10	12	$1+10^{12}$	60
	8	15	$1+8^{15}$	60
	20	6	$1+20^6$	504
	40	3	$1+40^3$	4080

Acknowledgements The authors thank the reviewer for careful reading and suggestions that has resulted in the improvement of the paper.

Conflict of interest This Author(s) declare that they have no competing interests.

References

1. Muratović-Ribić, Amela, and Enes Pasalic. “A note on complete polynomials over finite fields and their applications in cryptography." *Finite Fields and Their Applications* 25 (2014): 306-315.
2. Bartoli, D and Timponella, M., “A family of permutation trinomials over F_{q^2}” *Finite Fields and Their Applications* 70 (2021).
3. Carlitz, L. and Wells, C., “The number of solutions of a special system of equations in a finite field”, Acta Arithmetica 12 (1966), pp. 77–84.
4. Capaverde, J., Masuda, A.M. and Rodrigues, V.M., “Rédei permutations with the same cycle structure”, *Finite Fields and Their Applications* Vol. 81 (2022).
5. Dickson, L.E., “The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group.” *The Annals of Mathematics 11.1/6* (1896), pp. 65–120.
6. Gupta, R., and Sharma, R.K. Some new classes of permutation trinomials over finite fields with even characteristic, *Finite Fields and Their Applications*, Vol. 41 (2016), pp. 89–96.
7. Gupta, R., More results about a class of quadrinomials over finite fields of odd characteristic, *Communications in Algebra*, Vol. 50:1, pp. 324–333,
8. Hermite, C., Sur les fonctions de sept lettres. *Académie des sciences*, Paris, 1863.
9. Hou, X. “Permutation polynomials over finite fields-a survey of recent advances”, *Finite Fields and Their Applications* Vol. 32 (2015), pp. 82–119.
10. Hou, X., “Determination of a type of permutation trinomials over finite fields” Acta Arith., Vol. 166 (2014), pp. 253–278.
11. Hou, X., “Determination of a type of permutation trinomials over finite fields II” *Finite Fields and Applications*, 35, (2015) pp. 16–35.
12. Hou, Xiang-dong. “A survey of permutation binomials and trinomials over finite fields." *Contemp. Math* 632 (2015): 177–191.
13. Hou, X., and Lappano, S.D., “Determination of a type of permutation binomials over finite fields”, *Journal of Number Theory*, Vol. 147 (2015), pp. 14–23.
14. Lavorante, V.P., arXiv:2105.12012v4, Jan (2022).
15. Hou, X., and Lavaronte, V.P., New results on permutation binomials of finite fields, *Finite Fields and Their Applications*, Volume 88 (2023).
16. Lappano, S.D., “A note regarding permutation binomials over F_{q^2}” *Finite Fields and Their Applications*, Volume 34 (2015), pp. 153–160
17. Lee, J.B., and Park, Y.H., “Determination of a class of permutation trinomials in characteristic three”, *Acta Mathematica Scientia* Vol. 17, (1997), pp 250–254.
18. Li, K., Qu, L., Chen X, “New classes of permutation binomials and permutation trinomials over finite fields”, *Finite Fields and Applications*, 43, 69–85 (2017).
19. R. Lidl, W.B. Mullen, Permutation polynomials in RSA-cryptosystems, in: *Advances in Cryptology*,Plenum, New York, 1984, pp. 293-301.
20. Lidl, R, and Niederreiter, H, *Finite fields*, No. 20. Cambridge University Press, 1997.
21. Lu, W., Wu, X., Wang, Y., and Cao, X. A general construction of regular complete permutation polynomials,*Designs, Codes and Cryptography*, (2023), pp. 1–21.
22. Mullen, G.L., and Panario, D., *Handbook of finite fields*, CRC Press, 2013.
23. Niederreiter, H., and Winterhof, A., “Cyclotomic R-orthomorphisms of finite fields”, *Discrete mathematics* 295.1-3 (2005): 161–171.
24. Tu, Z. et al. “Several classes of complete permutation polynomials over finite fields of even characteristic”, *Finite Fields and Their Applications* 68 (2020): 101737.
25. J. Schwenk, K. Huber, Public key encryption and digital signatures based on permutation polynomials, *Electron. Lett.* 34 (1998) 759-760.
26. Wang, Q. “Cyclotomy and permutation polynomials of large indices.” *Finite Fields and Their Applications* 22 (2013): 57–69.
27. Laigle-Chapuy, Yann. “Permutation polynomials and applications to coding theory.” *Finite Fields and Their Applications* 13.1 (2007): 58-70.
28. Wu, B., and Lin, B., “On constructing complete permutation polynomials over finite fields of even characteristic ”, *Discrete Applied Mathematics* 184 (2015): 213–222.
29. Zha, Z., Hu,L., and Fan, S. “Further results on permutation trinomials over finite fields with even characteristic”, *Finite Fields and Their Applications* 45 (2017): 43–52.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.