Advances in Mathematics of Communications
Volume 11, No. 2, 2017, 301–306
doi:10.3934/amc.2017022

EXPLICIT FORMULAS FOR MONOMIAL INVOLUTIONS OVER FINITE FIELDS

Francis N. Castro

Department of Mathematics
University of Puerto Rico, Río Piedras
Box 70377, S.J., PR 00936-8377

Carlos Corrada-Bravo, Natalia Pacheco-Tallaj and Ivelisse Rubio*

Department of Computer Science
University of Puerto Rico, Río Piedras
Box 70377, S.J., PR 00936-8377

(Communicated by Min Sha)

Abstract. Permutations of finite fields have important applications in cryptography and coding theory. Involutions are permutations that are its own inverse and are of particular interest because the implementation used for coding can also be used for decoding. We present explicit formulas for all the involutions of $\mathbb{F}_q$ that are given by monomials and for their fixed points.

1. Introduction

Permutations play an important role in communications as they are used in applications ranging from speech encryption to coding theory and cryptography. In most applications the permutation and its inverse are stored in memory, a burden for environments with limited resources like mobile computing, smart cards and RFID tags. Hence, it is important to find permutations that are easily implemented and with a fairly small memory footprint. For the first issue, permutations generated by polynomials over rings [6] and finite fields [2] have been presented, for the second issue a simple solution is to use permutations that are its own inverse (involutions). One solution that solves both problems is to use involutions generated by monomials over finite fields [3, 4, 5].

The number of fixed points is important in cryptography, specifically for applications using block ciphers. One way to create block ciphers is with substitution-permutation networks (SPN) where S–boxes are created using permutations and it has been shown that the nonlinearity of a permutation is inversely proportional to the number of fixed points. Knowing the exact position of the fixed points allows the use of various techniques to minimize or completely eliminate the fixed points [3].

Let $\mathbb{F}_q$ be the finite field with q elements. Involutions of $\mathbb{F}_q$ obtained from monomials x^i were characterized in [2] but an explicit formula for i was not given. Recently, an algorithmic method to construct involutions of $\mathbb{F}_q$ using cyclotomic mappings was presented in [7]. In this work we prove that, given $\mathbb{F}_q$ and a number of fixed points

2010 *Mathematics Subject Classification:* Primary: 11T06; Secondary: 11T71.
Key words and phrases: Permutations, monomials, involutions, cryptography, Rèdei functions.
* Corresponding author.

$d+1$, there are at most two involutions x^i with exactly $d+1$ fixed points, and this happens if and only if $d \mid (q-1)$ and $\gcd\left(d, \frac{q-1}{d}\right) \in \{1,2\}$. We provide explicit formulas for all the involutions of $\mathbb{F}_q$ that are given by monomials and for their fixed points. Our results can be easily modified to get monomial involutions over cyclic groups. From [5] we see that our results can also be applied to Rèdei functions.

2. Explicit formulas for all monomial involutions

It is known that x^i induces a permutation of $\mathbb{F}_q$ if and only if $\gcd(i, q-1) = 1$, and easy to show that x^i is an involution of $\mathbb{F}_q$ if and only if $i^2 \equiv 1 \pmod{q-1}$. We call an involution induced by a monomial a *monomial involution*. The number of monomial involutions of $\mathbb{F}_q$ is the number of solutions of $x^2 \equiv 1 \pmod{q-1}$. This can also be thought as the number of monomial permutations of $\mathbb{F}_q$ with cycles of length 1 or 2 [2].

Lemma 2.1. *Let $q-1 = 2^e p_1^{e_1} \cdots p_r^{e_r}$. The number of monomial involutions is*

$$\begin{cases} 2^r & \text{if } e = 0, \text{ or } e = 1, \\ 2^{r+1} & \text{if } e = 2, \\ 2^{r+2} & \text{if } e \geq 3. \end{cases}$$

We want to find explicit formulas for all the monomial involutions of $\mathbb{F}_q$ and determine their set of fixed points. We start by studying the set of fixed points.

Lemma 2.2. *Let x^i be an involution of $\mathbb{F}_q$. There are exactly $\gcd(i-1, q-1)+1$ elements fixed by x^i, each of the form $0, \alpha^j$ where α is a primitive root of $\mathbb{F}_q$, $j = \frac{q-1}{d} l$, $l = 1, \ldots, d$, and $d = \gcd(i-1, q-1)$.*

Proof. Let α be a primitive root in $\mathbb{F}_q$. The element α^j is a fixed point of x^i if and only if $j(i-1) \equiv 0 \pmod{q-1}$. Hence j gives a fixed point if and only if $j = \frac{q-1}{d} l$, $l \in \{1, \ldots, d\}$, where $d \mid (i-1)$ and $d \mid (q-1)$. If $d = \gcd(i-1, q-1)$, all the fixed points have this form. Note that $j_s = \frac{q-1}{d} l_s \not\equiv j_t = \frac{q-1}{d} l_t \pmod{q-1}$ for $l_s \neq l_t$, $l_s, l_t \in \{1, \ldots, d\}$. Since 0 is a fixed point of x^i, we have that the number of fixed points is exactly $d+1$. □

We need the next lemma to characterize all the i that produce monomial involutions with exactly $d+1$ fixed points.

Lemma 2.3. *Let d be such that $d \mid (q-1)$, $i \equiv \frac{q-1}{d} k - 1 \pmod{q-1}$ for some integer k, and suppose that $d \mid (i-1)$. If $a = \gcd(i-1, q-1)$ and $2 \mid (q-1)$, then $a = d$ or $a = 2d$. If $a = \gcd(i-1, q-1)$ and $2 \nmid (q-1)$, then $a = d$.*

Proof. Suppose that $a = \gcd(i-1, q-1)$. Then, $d \mid a$ and $a \mid (i-1)$ imply that $a = dk_1$ and $dk_1 \mid \left(\frac{dk_1 h}{d} k - 2\right)$. Therefore $k_1 \mid 2$. If $2 \mid (q-1)$, then $a = d$ or $a = 2d$. If $2 \nmid (q-1)$, then $a = d$. □

We now prove that certain i's always produce monomial involutions.

Lemma 2.4. *Let $d \mid (q-1)$. If $i \equiv \frac{q-1}{d} k - 1 \pmod{q-1}$ for some integer k, and $i \equiv 1 \pmod{d}$, then x^i is an involution of $\mathbb{F}_q$. Moreover, if $d = \gcd(i-1, q-1)$, then x^i has exactly $d+1$ fixed points of the form $0, \alpha^j$, where α is a primitive root of $\mathbb{F}_q$ and $j = \frac{q-1}{d} l$, $l = 1, \ldots, d$.*

Proof. Let $i \equiv \frac{q-1}{d} k - 1 \pmod{q-1}$ and $i \equiv 1 \pmod{d}$. Then $(i+1)(i-1) = \frac{q-1}{d} k(i-1) \equiv 0 \pmod{q-1}$. This implies that x^i is an involution of $\mathbb{F}_q$. The rest follows from Lemma 2.2. □

Propositions 1, 2 and 3 below give formulas for k so that, for $i \equiv \frac{q-1}{d}k - 1 \pmod{q-1}$, x^i is a monomial involution of $\mathbb{F}_q$ with exactly $d+1$ fixed points. In Theorem 2.5 we will see that the k's given in these propositions produce all the monomial involutions of $\mathbb{F}_q$. The function ϕ in the formulas is Euler's function.

Proposition 1. *Let* $q-1 = 2^e p_1^{e_1} \cdots p_r^{e_r}$, $e \geq 0$, $d = 2^e p_1^{k_1} \cdots p_r^{k_r}$, $k_i \in \{0, e_i\}$. *If*

$$i \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}, \text{ where } k = 2\left(\frac{q-1}{d}\right)^{\phi(d)-1}$$

is reduced $\pmod d$, *then* x^i *is an involution of* $\mathbb{F}_q$ *with* $d+1$ *fixed points.*

Proof. By Lemma 2.4, we have to prove that $i \equiv 1 \pmod d$ and $d = \gcd(i-1, q-1)$.

We have $\gcd\left(d, \frac{q-1}{d}\right) = 1$, and can easily check that $y = 2\left(\frac{q-1}{d}\right)^{\phi(d)-1} \pmod d$ is a solution to $\left(\frac{q-1}{d}\right) y \equiv 2 \pmod d$, where ϕ is Euler's function. Therefore $i \equiv \left(\frac{q-1}{d}\right)\left(2\left(\frac{q-1}{d}\right)^{\phi(d)-1}\right) - 1 \equiv 1 \pmod d$, x^i is an involution, and d is a common divisor of $q-1$ and $i-1$.

We now see that $d = \gcd(i-1, q-1)$. Suppose that $a = \gcd(i-1, q-1)$. Then, by Lemma 2.3, $a = d$ or $a = 2d$. But $a = 2d$ is impossible because $2d \nmid (q-1)$. Therefore, $a = d$ and the involution has exactly $d+1$ fixed points. □

Proposition 2. *Let* $q-1 = 2^e p_1^{e_1} \cdots p_r^{e_r}$, $e \geq 2$, $d = 2^{e-1} p_1^{k_1} \cdots p_r^{k_r}$, $k_i \in \{0, e_i\}$. *If*

$$i \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}, \text{ where } k = \left(\frac{q-1}{2d}\right)^{\phi(d)-1} + \frac{d}{2}$$

is reduced $\pmod d$, *then* x^i *is an involution of* $\mathbb{F}_q$ *with* $d+1$ *fixed points.*

Proof. By Lemma 2.4, we have to prove that $i \equiv 1 \pmod d$ and $d = \gcd(i-1, q-1)$.

We have $\gcd\left(d, \frac{q-1}{2d}\right) = 1$, and can check that $y = \left(\frac{q-1}{2d}\right)^{\phi(d)-1} + \frac{d}{2}$ is a solution to $\left(\frac{q-1}{d}\right) y \equiv 2 \pmod d$. Therefore $i \equiv \left(\frac{q-1}{d}\right)\left(\left(\frac{q-1}{2d}\right)^{\phi(d)-1} + \frac{d}{2}\right) - 1 \equiv 1 \pmod d$, x^i is an involution, and d is a common divisor of $q-1$ and $i-1$.

Suppose that $a = \gcd(i-1, q-1)$. Then, by Lemma 2.3, $a = d$ or $a = 2d$. If $a = d$ the involution has exactly $d+1$ fixed points and we are done. We now see that $a \neq 2d$. Suppose the contrary. Then, since $2d \mid (i-1)$,

$$\begin{aligned} i - 1 \equiv \left(\frac{q-1}{d}\right)\left(\left(\frac{q-1}{2d}\right)^{\phi(d)-1} + \frac{d}{2}\right) - 2 \equiv 0 \pmod{2d}, \\ \left(\frac{q-1}{2d}\right)^{\phi(d)} + \left(\frac{q-1}{4}\right) - 1 \equiv 0 \pmod d. \end{aligned} \tag{1}$$

This implies that $\frac{q-1}{4} \equiv 0 \pmod d$, and $d \mid \frac{q-1}{4}$ which is a contradiction. Hence, $d = \gcd(i-1, q-1)$ and this completes the proof. □

Remark 1. Note that $y = \left(\frac{q-1}{2d}\right)^{\phi(d)-1}$ is another solution to $\left(\frac{q-1}{d}\right) y \equiv 2 \pmod d$. However, the involution x^i, where $i \equiv \left(\frac{q-1}{d}\right)\left(\left(\frac{q-1}{2d}\right)^{\phi(d)-1}\right) - 1 \pmod{q-1}$, produces $2d+1$ fixed points.

The next proposition completes all the possible cases for which $\gcd\left(d, \frac{q-1}{d}\right) \in \{1, 2\}$.

Proposition 3. *Let* $q-1=2^e p_1^{e_1}\cdots p_r^{e_r}$, $e\geq 3$, $d=2p_1^{k_1}\cdots p_r^{k_r}$, $k_i\in\{0,e_i\}$. *If*

$$i\equiv\left(\frac{q-1}{d}\right)k-1 \pmod{q-1},\ \text{where } k=\left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1}+\ t,\ t\in\left\{0,\frac{d}{2}\right\},$$

is reduced $\pmod d$, *then* x^i *is an involution of* $\mathbb{F}_q$ *with* $d+1$ *fixed points.*

Proof. By Lemma 2.4, we have to prove that $i\equiv 1 \pmod d$ and $d=\gcd(i-1,q-1)$.

Since $\gcd\left(\frac{d}{2},\frac{q-1}{2d}\right)=1$, the congruence $\left(\frac{q-1}{2d}\right)y\equiv 1 \pmod{\frac{d}{2}}$ has a unique solution $y=\left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1} \pmod{\frac{d}{2}}$. Note that

$$\left(\frac{q-1}{d}\right)\left(\left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1}\right)\equiv\left(\frac{q-1}{2d}\right)(2y)\equiv 2 \pmod d.$$

So, $y_1'=\left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1}$, $y_2'=\left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1}+\frac{d}{2}$ are solutions to $\left(\frac{q-1}{d}\right)y'\equiv 2 \pmod d$. Therefore, $i\equiv\left(\frac{q-1}{d}\right)\left(\left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1}+t\right)-1\equiv 1 \pmod d$, where $t\in\left\{0,\frac{d}{2}\right\}$. This implies that x^i is an involution for $t\in\left\{0,\frac{d}{2}\right\}$, and d is a common divisor of $q-1$ and $i-1$.

Suppose that $a=\gcd(i-1,q-1)$. Then, by Lemma 2.3, $a=d$ or $a=2d$. If $a=d$ the involution has exactly $d+1$ fixed points and we are done. We need to prove that $a\neq 2d$. Suppose the contrary. Then, since $2d\mid(i-1)$,

$$\begin{aligned} i-1&\equiv\left(\frac{q-1}{d}\right)\left(\left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1}+t\right)-2\equiv 0 \pmod{2d},\ \text{for } t\in\left\{0,\frac{d}{2}\right\},\\ &\left(\frac{q-1}{2d}\right)\left(\left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1}+t\right)-1\equiv 0 \pmod d,\ \text{for } t\in\left\{0,\frac{d}{2}\right\}. \end{aligned} \tag{2}$$

Since d and $\frac{q-1}{2d}$ are even, this is a contradiction. Hence, $d=\gcd(i-1,q-1)$ and this completes the proof. □

Now, if we count all the divisors that satisfy the conditions in Propositions 1, 2 and 3, and compare this number with the total number of involutions of $\mathbb{F}_q$, we see that we have obtained all the monomial involutions of $\mathbb{F}_q$ and hence found explicit formulas for all of them.

Theorem 2.5. *Let* $q-1=2^e p_1^{e_1}\cdots p_r^{e_r}$, $d=2^f p_1^{k_1}\cdots p_r^{k_r}$, $f\leq e$, $k_j\in\{0,e_j\}$. *The monomial* x^i *is an involution of* $\mathbb{F}_q$ *with exactly* $d+1$ *fixed points if and only if* $i\equiv\frac{q-1}{d}k-1 \pmod{q-1}$ *where*

$$k=\begin{cases} 2\left(\frac{q-1}{d}\right)^{\phi(d)-1}, & \text{if } f=e\geq 0,\\ \left(\frac{q-1}{2d}\right)^{\phi(d)-1}+\ \frac{d}{2}, & \text{if } f=e-1\geq 1,\\ \left(\frac{q-1}{2d}\right)^{\phi(\frac{d}{2})-1}+\ t,\ t\in\left\{0,\frac{d}{2}\right\}, & \text{if } f=1,e\geq 3, \end{cases}$$

and k *is reduced* $\pmod d$. *Moreover, these are all the involutions of* $\mathbb{F}_q$ *given by monomials and the fixed points have the form* $0,\alpha^j$, $j=\frac{q-1}{d}l$, $l=1,\ldots,d$.

Proof. Let $q-1=2^e p_1^{e_1}\ldots p_r^{e_r}$ and $d+1$ be the number of fixed points of x^i. First note that, if $e\geq 1$, i must be odd and then d is even. We divide the proof into cases.

If $e = 0$, then $d = p_1^{k_1} \dots p_r^{k_r}$, for $k_j \in \{0, e_j\}$. Proposition 1 gives one monomial involution for each d. Hence there are 2^r monomial involutions. From Lemma 2.1 we know that these are all the involutions for this case.

If $e = 1$, then d is even and $d = 2p_1^{k_1} \dots p_r^{k_r}$, for $k_j \in \{0, e_j\}$. Again, Proposition 1 gives one monomial involution for each d. Hence there are 2^r monomial involutions. From Lemma 2.1 we know that these are all the involutions for this case.

If $e = 2$, then d is even and $d = 2^f p_1^{k_1} \dots p_r^{k_r}$, for $f \in \{1, 2\}$, $k_j \in \{0, e_j\}$. Propositions 1 and 2 give one monomial involution for each d. Hence there are 2^{r+1} monomial involutions. From Lemma 2.1 we know that these are all the involutions for this case.

If $e \geq 3$, then d is even and $d = 2^f p_1^{k_1} \dots p_r^{k_r}$, for $1 \leq f \leq e$, $k_j \in \{0, e_j\}$. Propositions 1, 2 give one monomial involution for each d with $f = e, e-1$, and Proposition 3 gives two monomial involutions for each d with $f = 1$. Hence there are $2^{r+1} + 2\,(2^r) = 2^{r+2}$ monomial involutions. From Lemma 2.1 we know that these are all the involutions for this case.

Hence, Propositions 1, 2 and 3 give all the monomial involutions and also the amount and form of the fixed points. □

Remark 2. Note that the d's in the formulas for the monomial involutions x^i are all the d's such that $d \mid (q-1)$, $\gcd\left(d, \frac{q-1}{d}\right) \in \{1, 2\}$. This implies that the number of fixed points $d+1$ of a monomial involution is always such that $\gcd\left(d, \frac{q-1}{d}\right) \in \{1, 2\}$.

With the result in Theorem 2.5, given a finite field $\mathbb{F}_q$ and a number of fixed points, we can construct all the monomial involutions of $\mathbb{F}_q$ with that number of fixed points, if there is any. Also, given a number of "desired" fixed points $d+1$, we can construct all the finite fields and monomial involutions with that amount of fixed points.

Example 1. All the monomial involutions x^i of a finite field $\mathbb{F}_q$ that have $d+1 = 5$ fixed points are such that $q - 1 = 2^e p_1^{e_1} \dots p_r^{e_r}$ and

- $i \equiv \frac{q-1}{2} - 1 \pmod{q-1}$ and $e = 2$,
- $i \equiv \frac{q-1}{4} k - 1 \pmod{q-1}$, $k = \frac{q-1}{8} + 2$ reduced $\pmod 4$ and $e = 3$.

Example 2. Let $q - 1 = 255 = 3 \times 5 \times 17$. By Lemma 2.1 there are 2^3 monomial involutions of $\mathbb{F}_q$, and by Theorem 2.5, all the x^i with $d+1$ fixed points are such that $(i, d) \in \{(254, 1), (169, 3), (101, 5), (16, 15), (239, 17), (154, 51), (86, 85), (1, 255)\}$.

ACKNOWLEDGMENTS

The authors appreciate the careful review, and helpful suggestions to this paper made by the referees.

REFERENCES

[1] C. Corrada and I. Rubio, Deterministic interleavers for Turbo codes with random-like performance and simple implementation, in *Proc. 3rd Int. Symp. Turbo Codes Related Topics*, 2003, 555–558.

[2] C. Corrada and I. Rubio, Cyclic decomposition of permutations of finite fields obtained using monomials, in *Finite Fields and Applications*, 2004, 254–261.

[3] P. Charpin, S. Mesnager and S. Sarkar, On involutions of finite fields, in *Int. Symp. Inf. Theory-ISIT*, 2015, 186–190.

[4] P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inf. Theory*, **62** (2016), 2266–2276.

[5] A. Sakzad, D. Panario, M. Sadeghi and N. Eshghi, Self-inverse interleavers based on permutation functions for Turbo codes, in *2010 48th Ann. Allerton Conf. Commun. Control Comp.*, IEEE, 2010, 22–28.
[6] O. Takeshita, On maximum contention-free interleavers and permutation polynomials over integer rings, *IEEE Trans. Inf. Theory*, **52** (2006), 1249–1253.
[7] Q. Wang, A note on inverses of cyclotomic mapping permutation polynomials over finite fields, *Finite Fields Appl.*, **45** (2017), 422–427.

Received February 2016; revised March 2016.

E-mail address: franciscastr@gmail.com
E-mail address: carlos.corrada2@upr.edu
E-mail address: nataliamariapt@gmail.com
E-mail address: iverubio@gmail.com