International Journal of Engineering, Science and Mathematics
Vol. 8,Issue 2, February 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

REDEI RATIONAL FUNCTIONS AS PERMUTATION FUNCTIONS AND AN ALGORITHM TO COMPUTE REDEI RATIONAL FUNCTIONS

Dr.D.CHAYA KUMARI*

Dr.S.ASHOK KUMAR**

Abstract

Permutation polynomials have received significantly wider attention because of their potential applications in cryptosystems and various combinatorial designs. A polynomial $f(x) \in F_q[x]$ of positive degree is called a permutation polynomial if and only if f (x) induces a bijection from F_q onto itself. The rational functions over $F_q[x]$ that yield permutations of F_q are called permutation functions. In the process of the study of necessary and sufficentt conditions for a polynomial to be permutation polynomial a special kind of polynomials $g_n(a; x)$ called Dickson polynomials are introduced by Dickson and the study of Dickson polynomials lead to the introduction of the special class of the special class of functions called Redei rational functions to be permutation functions are presented and an algorithm to compute the Redei rational functions is given which is useful in cryptosystems with Redei rational functions as trapdoor functions.

Keywords:

Permutation functions;
Redei rational functions;
Cryptosystem;

Author correspondence:

Dr.D.Chaya Kumari,
Associate Professor
AMC Engineering College,
Bannerughatta Road,Bangalore

Dr.S.Ashok Kumar
Assistant Professor
GVP College for Degree & P.G College(A)
M.V.P.Colony, Visakhapatnam

* Doctorate Program, Linguistics Program Studies, Udayana University Denpasar, Bali-Indonesia
** STIMIK STIKOM-Bali, Renon, Depasar, Bali-Indonesia

1. INTRODUCTION

A polynomial $f(x) \in F_q[x]$ of positive degree is called a permutation polynomial if and only if $f(x)$ induces a bijection from F_q onto itself. Permutation polynomials have received significantly wider attention because of their potential applications in cryptosystems and various combinatorial designs.

The rational functions over $F_q[x]$ that yield permutations of F_q are called permutation functions. Special kind of polynomials $g_n(a; x)$ called Dickson polynomials are introduced by Dickson in the process of the study of necessary and sufficient conditions for a polynomial to be permutation polynomial and the study of Dickson polynomials led to the introduction of the special class of functions called Redei rational functions that are quotients of some Dickson polynomials.

In this paper, the necessary and sufficient conditions for the Redei rational functions to be permutation functions are presented and an algorithm to compute Redei rational functions is given which is useful in the cryptosystem with Redei rational functions as trapdoor functions.

2. Permutation Polynomials:

Definition 1. Let F_q be a finite field. A Polynomial $p(x) \in F_q[x]$ in one variable is called a permutation polynomial over F_q if the mapping $\pi_p : F_p \to F_q$ as $\alpha \to p(\alpha)$ for $\alpha \in F_q$ is a permutation of F_q .

Example 1. (i) $p(x) = 4x^5 + 3 \in F_7$ is a permutation polynomial over F_7 .

X	0	1	2	3	4	5	6
P(x)	3	0	5	2	4	1	6

Hence, $p(x)$ is a permutation polynomial.

(ii) $p(x) = 2x^2 + 3 \in F_7$ is not a permutation polynomial over F_7 .

X	0	1	2	3	4	5	6
P(x)	3	5	4	0	0	4	5

Hence, $p(x)$ is not a permutation polynomial.

Theorem 1. If $p(x)$ is a permutation polynomial over F_q ,then $ap(x) + b$ is a permutation polynomial for any $a \neq 0, b \in F_q$.

Theorem 2. If $p(x)$ and $q(x)$ are permutation polynomials then the compo-sition $P(Q(x))$ is also a permutation polynomial.

Theorem 3. Carlitz's theorem: For odd q the polynomial $f(x) = x^{\frac{(q+1)}{2}} + ax \in \mathrm{F}_q[x]$ is a permutation polynomial if and only if $a^2 - 1$ is a non-zero square.

Theorem 4. Let q = 3m + 1 be sufficiently large. Then the polynomial $f(x) = x^{m+1} + ax$ is a permutation polynomial in F_q for some possible choice of $a \in \mathrm{F}_q$.

Theorem 5. Generalized theorem of Carlitz:

Let e > 1 be any integer. Then there exists some constant m_e such that, in any finite field of order q; $q \equiv 1 \bmod e$, $q > m_e$, there is an element $a \neq 0$ with the property : Every polynomial $f = x^c\left(x^{\frac{(q-1)}{e}} + a\right)^k$, $\gcd(c, q-1) = 1,\ k \geq 1$ is a permutation polynomial.

Theorem 6. Hermites-Dickson Criterion

A polynomial f over the finite field K of order q and characteristic p is a permutation polynomial if and only if

a) f has exactly one root in K.

b) The reduction of f^t; $0 < t < q - 1$; $t \equiv 0 \bmod p$ has a degree less than or equal to q − 2.

Theorem 7. A polynomial $f \in \mathrm{F}_q[x]$ is a permutation polynomial of all finite extensions of F_q if and only if it is of the form $f(x) = ax^{p^h} + b$ where $a \neq 0$, p is the characteristic of F_q and h is a non-negative integer.

3. Permutation Function:

Definition 2. Let n be a positive integer and g(x) be a polynomial over integers. Then, g(x) is said to be a permutation polynomial modulo n if the mapping π_g given as $\pi_g(i) \equiv g(i) \bmod n$ is a permutation on the set $\mathbf{Z}_n$ of all residue classes modulo n.

Definition 3. Let n be a positive integer and $q(x) = \frac{g(x)}{h(x)}$, a quotient of polynomials g(x); h(x) over integers, such that $g(x)$ and $h(x)$ are relatively prime. $q(x)$ is said to be a permutation function modulo n, if $h(i)$ is a prime residue class modulo n for each integer i and the mapping $\pi_q : \mathbf{Z}_n \to \mathbf{Z}_n$ given as $\pi_q(i) = h(i)^{-1} g(i)$ is a permutation on $\mathbf{Z}_n$.

Theorem 8. Let n=ab with a and b are co-prime. Then $q(x)=\frac{g(x)}{h(x)}$ is a permutation function modulo n if and only if $q(x)$ isa permutation function modulo a and modulo b.

Theorem 9. Let p be a prime and $q(x)$ is a permutation function modulo p if $h(r)g'(r)-g(r)h'(r)\not\equiv 0 \bmod p$ for all r then the function $q(x)=\frac{g(x)}{h(x)}$ is a permutation function modulo p^e for all e, the prime powers of p.

In the study of permutation polynomials over F_p Schur in 1923 conjectured that, If f(x) is a polynomial with integer coeficients is a permutation polynomial of F_p for infinitely many primes p, then f(x) is a composition of $(ax^n + b)$ and Dickson polynomials are introduced and now we define Dickson polynomials, describe some of its properties and study the necessary and suficient conditions for Dickson polynomials to be permutation polynomials are stated.

Definition 4. Let K be a commutative ring. The polynomial $g_k(a,x)=\sum_{i=0}^{\frac{k}{2}}\frac{k}{k-i}\binom{k-i}{i}(-a)^i x^{k-2i}$ for a $\in$ K is called a Dickson polynomial of degree k.

Theorem 10. If K is a finite field of order q and characteristic p and $a\neq 0\in K$ then a Dickson polynomial $g_k(a; x) \in K[x]$ if and only if $\gcd(k; q^2 - 1) = 1$ and $g_k(a; x)$ is a regular permutation polynomial

Dickson polynomials as permutation polynomials over Z_n

For $a = 1$, to extend the Dickson polynomials $g_k(a;x)$ as permutation poly-nomials on Z_n for $n = p_1^{e_1} p_2^{e_2} .....p_r^{e_r}$ the Dickson polynomial must be regular polynomial modulo Z_{p_i} for each $i = 1; 2; \cdots r$.

Proposition 1. $g_k(a; x)$ is a permutation polynomial over Z_n if and only if $\gcd\left(k,\left[p_i^{e_i-1}(p_i)^2-1\right]\right)=1$ for $i = 1; 2 \cdots r$. where $\left[p_i^{e_i-1}(p_i)^2-1\right]_{i=1}^{r}$ is the lcm of $\left[p_1^{e_1-1}(p_1)^2-1, p_2^{e_2-1}(p_2)^2-1, ...p_r^{e_r-1}(p_r)^2-1\right]$

The study of Dickson polynomials as permutation polynomials led to the introduction of the special class of functions called Redei rational functions. These functions are quotients of some Dickson polynomials. The construction of Redei rational functions, and the necessary and suficient conditions for the Redei rational functions to be permutation functions are described.

Lemma 1. The polynomials $N_n(x)$ and $D_n(x)$ satisfy the recurrence relations

$$N_n(x) = xN_{n-1}(x) + bD_{n-1}(x)$$

$$D_n(x) = N_{n-1}(x) + (x + a)D_{n-1}(x)$$

for all $n > 1$ with initial values $N_1(x) = x$ and $D_1(x) = 1$

Corollary 1. $Q_n(x)$ satisfy the recurrence relations

$$Q_n(x) = \frac{xQ_{n-1}(x)+b}{Q_{n-1}(x)+(x+a)}$$

forall $n > 1$ with initial value $Q_1(x) = x$.

R.Nobauer[8] and W.Nobauer[8] made slight modification in the above definition for**4. Redei Rational Function**

Definition 5. Let $d \neq 0$ be a non-square positive integer. The Redei rational functions devolped from $\left(z+\sqrt{d}\right)^n$ by the expression

$$\left(z+\sqrt{d}\right)^n = N_n(d,z)+D_n(d,z)\sqrt{d}$$

When $N_n(d,z)=\sum_{k=0}^{\left[\frac{n}{2}\right]}\binom{n}{2k}d^k z^{n-2k}$ and $D_n(d,z)=\sum_{k=0}^{\left[\frac{n-1}{2}\right]}\binom{n}{2k+1}d^k z^{n-2k-1}$

Are denoted by $Q_n(d,z)$ and are defined as

$$Q_n(d,z)=\frac{N_n(d,z)}{D_n(d,z)}\forall n\geq 1,\quad n\in \mathbf{Z}$$

Theorem 11. Let $p\neq 2$ and n represents a natural number with $\gcd(n,q+1)=1$. Choose a non-square element d in $\mathbf{F}_q$ then $Q_n(d,z)$ is a permutation function whenever $\gcd(n,q+1)=1$ for $\sqrt{d}\notin \mathrm{F}_q$ and $\gcd(n,q-1)=1$ for $\sqrt{d}\in \mathrm{F}_q$.

Proof: $\left(z+\sqrt{d}\right)^n = N_n(d,z)+D_n(d,z)\sqrt{d}$, $D_n(d,z)\neq 0$ if $\gcd(n,q+1)=1$

For,

$$D_n(d,z)=0$$

$$\Rightarrow \left(z+\sqrt{d}\right)^n = N_n(d,z)+0\sqrt{d}$$

$$\Rightarrow \left(\sqrt{d}\right)^n \in \mathrm{F}_q$$

But $\gcd(n,q+1)=1$

$$nr+(q+1)s=1$$

$$\Rightarrow \sqrt{d}=\left(\sqrt{d}\right)^{nr+(q+1)s}$$

$$= \left(\sqrt{d}\right)^{nr} \left(\sqrt{d}\right)^{(q+1)s}$$

$$= \left(\sqrt{d}\right)^{nr} (a)^{s}$$

$$\Rightarrow \left(\sqrt{d}\right) \in \mathrm{F}_q \text{ which is contradiction}$$

Therefor $D_n(d,z) \neq 0 \ \forall z \in \mathrm{F}_q$ if $\gcd(n, q+1) = 1$

Now for $D_n(d,z) \neq 0 \ \forall z \in \mathrm{F}_q$, we have the mapping $f : \mathrm{F}_q \to \mathrm{F}_q$ gives as $f(z) = Q_n(d,z)$ is a bijection. For any $u, v \in \mathrm{F}_q$, $f(u) = f(v), \Rightarrow Q_n(d,u) = Q_n(d,v)$

Now as

Now for $D_n(d,z) \neq 0 \ \forall z \in \mathrm{F}_q$, we have the mapping $f : \mathrm{F}_q \to \mathrm{F}_q$ gives as $f(z) = Q_n(d,z)$ is a bijection. For any $u, v \in \mathrm{F}_q$, $f(u) = f(v), \Rightarrow Q_n(d,u) = Q_n(d,v)$

Now as

$$Q_n(d,u) = Q_n(d,v)$$

$$\Rightarrow \frac{Q_n(d,u) + \sqrt{d}}{Q_n(d,u) - \sqrt{d}} = \frac{Q_n(d,v) + \sqrt{d}}{Q_n(d,v) - \sqrt{d}}$$

$$\Rightarrow \left(\frac{u+\sqrt{d}}{u-\sqrt{d}}\right)^n = \left(\frac{v+\sqrt{d}}{v-\sqrt{d}}\right)^n$$

Since $\dfrac{Q_n(d,z) + \sqrt{d}}{Q_n(d,z) - \sqrt{d}} = \left(\dfrac{z+\sqrt{d}}{z-\sqrt{d}}\right)^n$

$$\Rightarrow \left[\frac{\left(u+\sqrt{d}\right)\left(v-\sqrt{d}\right)}{\left(u-\sqrt{d}\right)\left(v+\sqrt{d}\right)}\right]^n = 1$$

$$\Rightarrow \left[\frac{(uv-d)+(v-u)\sqrt{d}}{(uv-d)-(v-u)\sqrt{d}}\right]^n = 1$$

$$\Rightarrow (u-v) = (v-u)$$

$$\Rightarrow u = v$$

Therfore $Q_n(d,z)$ is a permutatuion function when ever $\gcd(n, q+1) = 1$ for all $\sqrt{d} \notin \mathrm{F}_q$

Now, for $\sqrt{d} \in \mathrm{F}_q$ we have $\left(z+\sqrt{d}\right)^n = N_n(d,z) + D_n(d,z)\sqrt{d}$. For $\sqrt{d} = a \in \mathrm{F}_q$

$\left(z+\sqrt{d}\right)^n = (z+a)^n = (fog)(z)$ for $g(z) = (z+a)$ and $f(z) = z^n$. Then, we have $g(z)$ is a permuation polynomial and $f(z)$ is apermutation whenever $\gcd(n, q-1) = 1$ by Carlitz[6], their comoposition $(fog)(z)$ is a permutation polynomial whenever gcd $(n, q-1) = 1$.

Therefore, $Q_n(d,z)$ is a permutation function whenever $\gcd(n,q+1)=1$ for all $\sqrt{d}\notin \mathrm{F}_q$ and $\gcd(n,q-1)=1$ for $\sqrt{d}\in \mathrm{F}_q$.

Theorem 12. The redei rational function $Q_k(d,z)$ for $z\in \mathbf{Z}_n$ for $n=p_1^{e_1}p_2^{e_2}.....p_r^{e_r}$ and d is a non-square positive integer is a permutation polynomial if gcd $\left(k,\left[p_i^{e_i-1}(p_i+1)\right]_{i=1}^{r}\right)=1$

Theorem 14. For $Q_m(d,z)\circ Q_n(d,z)=Q_m\left(d,Q_n(d,z)\right)$, we have $Q_m(d,z)\circ Q_n(d,z)=Q_{mn}(d,z)$.

Proof: We have $Q_{mn}(d,z)=\dfrac{N_{mn}(d,z)}{D_{mn}(d,z)}$ *for* $\left(z+\sqrt{d}\right)^{mn}=N_{mn}(d,z)+\sqrt{d}D_{mn}(d,z)$

and $$\left(z+\sqrt{d}\right)^{mn}=\left(\left(z+\sqrt{d}\right)^{n}\right)^{m}$$

$$=\left(N_n(d,z)+\sqrt{d}D_n(d,z)\right)^{m}$$
$$=\left(D_n(d,z)\right)^{m}.\left(Q_n(d,z)+\sqrt{d}\right)$$
$$=\left(D_n(d,z)\right)^{m}.\left(N_m\left(d,Q_n(d,z)\right)+\sqrt{d}D_m\left(d,Q_n(d,z)\right)\right)$$

Therefore we have

$$\frac{N_{mn}(d,z)}{D_{mn}(d,z)}=\frac{N_m\left(d,Q_n(d,z)\right)}{D_m\left(d,Q_n(d,z)\right)}$$
$$\Rightarrow Q_{mn}(d,z)=Q_m\left(d,Q_n(d,z)\right)=Q_m(d,z)\circ Q_n(d,z)$$

We can extend this definition of Redei rational functions to negative indices n through this metrical approach.

Definition 6: $Q_m(d,z)\square_d Q_n(d,z)=\dfrac{d+Q_m(d,z)Q_n(d,z)}{Q_m(d,z)+Q_n(d,z)}$

Proposition 2. The product $\square_d$ on Redei rational functions satisfies

$Q_m(d,z)\square_d Q_n(d,z)=Q_{m+n}(d,z)\ \forall m,n\geq 1; m,n\in \mathbf{Z}.$

Theorem 16. $Q_n(d,a)\square_d Q_n(d,b)=Q_n\left(d,\dfrac{d+ab}{a+b}\right)$.

Theorem 17. For any z and a non-square positive integer $d, N_n(d,z)$ and $D_n(d,z)$ satisfy the recurrence relations

$$N_{n+1}=2zN_n-\left(z^2-d\right)N_{n-1}$$
$$D_{n+1}=2zD_n-\left(z^2-d\right)D_{n-1}$$

With intial conditions $N_0(d,z)=1; N_1(d,z)=z$ *and* $D_0(d,z)=0; D_1(d,z)=1$

4.Algorithm to compute Redei rational functions:

```
#include <stdio.h>
#include <math.
```

```
double getPower(double value, double index)
{
        int i;
   double dPower = 1;
   for (i = 0; i < index; i++)
   {
      dPower = dPower * value;
   }
   return dPower;
}
double getFact(double dval)
{
        int i;
   double dFact = 1;
   for ( i = 1; i <= dval; i++)
        {
      dFact = dFact * i;
        }

   return dFact;
}
double getModuvalue(double dvalue,int mod)
{
        long lvalue = (long)(dvalue/mod);
        return (dvalue - lvalue*mod);
}

double getNCR(double n, double r)
{
   return getFact(n) / (getFact(n - r) * getFact(r));
}
//////////////////////////////////////////////////////////
double DicksonPolynomial(int a, int k, int x)
{
```

```
        int i;
        double dicksonPolynomial = 0;
   int k1 = (int)floor ( k / 2 + 0.5);

   for ( i = 0; i <= k1; i++)
   {
      dicksonPolynomial += (k/(k - i)) * getNCR(k - i,i) * pow(-a,i)* pow(x,k - 2*i);
   }
   return dicksonPolynomial;
}
double getInverseModuloValue(int dVal,int mod)
{
        double dReturn = 0;
        int bFlag = 1;
        int multi = 1;
        if(dVal == 0)
                return -1;
        while(bFlag == 1)
        {
                int n = dVal*multi%mod;
                if(n == 1)
                {
                        bFlag = -1;
                        return multi;
                }
                else
                        multi++;
        }

        return dReturn;
}

//////////////////////////////////////////////////////////////////////
//////////////////////RedeiRational/////////////////////////////////
```

```
double getRedeiRational(double d, int z, int n,int mod)
{
        int k;
        double nDenom,inver,final;
   double dRedeiRational = 0.0;
   double dNume = 0.0;
   double dDenom = 0.0;
        double nDenom1;

   int n1 = (int)floor(n / 2 + 0.5);

   for (k = 0; k <= n1; k++)
   {
      dNume += getNCR(n, 2 * k) * getPower(d, k) * getPower(z, (n - 2 * k));

       dDenom += getNCR(n, 2 * k + 1) * getPower(d, k) * getPower(z, n - 2 * k - 1);
   }
        nDenom1 = floor(dDenom);

         nDenom1 = getModuvalue(nDenom1,mod);
        inver = getInverseModuloValue(nDenom1,mod);

        if(inver == -1)
        {
                printf("Inverse not Exist .....");
//              return;
        }
        else
        {
        final = getModuvalue(dNume*inver,mod);
        return final;
        }

}
```

```
//////////////////////////////////////////////////////////////////

void main()
{


        //////////////DicksonPolynomial function calling////////////////////////
        int a,k,x;
        double result;

        ////////////////////////RedeiRational declaration//////////////////
        double d;
        int z,n,mod;
        double result1;
        double sqrno;

        ////////////////////////////////////////

        printf(" ----------------------------DicksonPolynomial---------------------- \n");

        printf("enter a,k,x values\n");
        scanf("%d",&a);
        scanf("%d",&k);
        scanf("%d",&x);

        if( x>k )
        {
                printf("x value must be less than or equal to k value\n");

        }
        else
        {
                result = DicksonPolynomial(a,k,x);
```

```
            printf("%lf\n",result);

        }
        ////////////////////////////////////

        printf("**********************************RedeiRational**********
*****************\n");
        //////////////RedeiRational function calling/////
        printf("enter d,z,n,mod values and d must be non-square number\n");
        scanf("%lf",&d);
        sqrno = sqrt(d);

        if ((sqrno * sqrno)== d)
        {
            printf("d value must be non-square number\n");
        }
        else
        {
            scanf("%d",&z);
            scanf("%d",&n);
            scanf("%d",&mod);

            result1 = getRedeiRational(d,z,n,mod);


            printf("%lf\n",result1);
        }
        ////////////////////////////////////////////////

        printf("************************************Program
end**********************************\n");
}
```

5. Conclusion

To compu e Redei rational functions an algorithm is given to verify the properties of Redei rational functions easily which will be helpful in constructing cryptosystems.

REFERENCES

[1] Tom M. Apostol ,Introduction to Analytic Number Theory" Springer-Verlag, NewYork Inc.

[2] Stefano barbero; Umberto Cerruti and Nadir Murru,Solving the pell equation via Redei rational Functions Fibonacci quarterly, 2010.

[3] J. Buchmann \Introduction to cryptography" , Springer-Verlag 2001

[4] D.Burton, \ Elementary Number Theory Sixth ed, Mc Graw Hill, New York, 2007.

[5] Carlitz.L, A note on permutation functions over a nite eld, Duke Math.J.29, 325-332(1962).

[6] Carlitz.L,Sometheorems on permutation polynomials , Bull.Amer.Math.Soc.68(1962) 120-122.

[7] Nobauer.R, Cryptanalysis of the Redei Scheme, Contributions to general algebra,3,255-264,1984.

[8] Nobauer.W, Redei-Funktionen fur Zweierpotenzen, Periodica mathematica Hungaria, 17(1)(1986)pp 37-44.

[9] P.Anuradha Kameswari,R.Chaya Kumari,Cryptosystems with Redei rational Functions via Pell conics, IJCA, vol 54-number 15 pages 1-6.

[10] Redei.L, Uber eindeutig umkehrbare polynome in endlichen korpern, Actasci.Math. (szeged) 11, 85- 92(1946).

[11] Redei.L, Algebra I,Leipzig(1959).

[12] Weil.A, Number Theory: An approach through history, Birkhauser,Boston,1984