Dickson Polynomials that Generate Involutions with More Than 3 Fixed Points

Natalia M. Pacheco-Tallaj
Computer Science Department
University of Puerto Rico, Rio Piedras Campus

May 30, 2016

1 Introduction

Let $\mathbb{F}_q$ be a finite field of prime order q. This research studies the Dickson Polynomials $D_i(x, a)$ that generate a permutation of $\mathbb{F}_q$ such that D_i decomposes into cycles of uniform length 2, i.e. D_i is an involution. Our goal is to provide a necessary and sufficient formula to construct i such that the Dickson Polynomial $D_i(x, a)$ has a particular amount d of fixed points. We wish to find a formula for i in terms of d and q, similarly to what we were able to achieve with Permutation Monomials in [1].

2 Preliminaries

The *Dickson Polynomial* of degree i es defined as:

$$D_i(x, a) := \sum_{j=0}^{\lfloor i/2 \rfloor} \frac{i}{i-j} \binom{i-j}{j} (-a)^j \; x^{i-2j}$$

Notice that the monomials x^i (studied as involutions in [1, 2, 3, 4]) are a Dickson Polynomial of the form $D_i(x, 0)$ and generate involutions of $\mathbb{F}_q$ if and only if $gcd(i, q-1) = 1$. The following is a more general result

Lemma 2.1. A Dickson Polynomial with $a \neq 0$ produces a permutation of $\mathbb{F}_q$ if and only if $gcd(i, q^2 - 1) = 1$.

Dickson Polynomials are closed under composition if and only if $a = 0, 1, -1$, therefore, to find Dickson Polynomial involutions, we need only study the cases where $a = 1, -1$, since $a = 0$ was studied in [1] and any other cases are not closed under composition. [5]

3 Work Developed

3.1 Simulations with $a = 1$

We began working with the case of $a = 1$, i.e. Dickson polynomials of the form $D_i(x, 1)$.

Different functions were implemented to calculate or construct Dickson polynomials of the form $D_i(x, 1)$. Each one was unit tested. Each function's running time was compared in order to choose the most efficient. Most importantly, the functions differed in one factor: some functions generated Dickson Polynomials as Symbolic Equation Objects which could then be evaluated for values of the variable (i.e. functions that create $D_i(x, 1$ for a generic x), while other functions generated the result of evaluating the Dickson Polyomial in a predetermined variable (i.e. functions that calculate $D_i(x, 1)$ for a specific x). The function that returned the desired Dickson Polynomial as a Symbolic Equation object was discarded for being comparatively inefficient, especially once calculating polynomials of very large degree. Instead, a function that evaluated the polynomial over a variable x as the polynomial got constructed, and reduced the polynomial modulo q in each step, was chosen.

The functions for constructing Dickson Polynomials that are being used are displayed in Code 1.

```
def D(i,x,q):
    sum = 0
    for j in range(i//2 + 1):
        sum += i/(i-j) * binomial(i-j,j) * (-1)^j * x^(i-2*j) % q
    return sum % q

def DD(i,x,q):
    var = D(i,x,q)
    sum = 0
    for j in range(i//2 + 1):
        sum += i/(i-j) * binomial(i-j,j) * (-1)^j * var^(i-2*j) % q
    return sum % q
```

Code 1: Construction of Dickson Polynomials

Here, `D(i,x,q)` takes integral inputs `i`, `x` and `q` and returns $D_i(x, 1) \pmod q$, and `DD(i,x,q)` takes integral inputs `i`, `x` and `q` and returns $(D_i \circ D_i)(x, 1) \pmod q = D_i(D_i(x, 1), 1) \pmod q$.

The initial approach used for searching involutions was very similar to that used in 2015 for searching monomial involutions:

```
for prime q < some_range:
    for i=0 to q-1:
        check if DD(i,x,q) = x for every x in Fp
        check if D(i,x,q) = x for the desired amount of fixed points
    return a list of all i that worked for this q
```

However, the simulations were extremely slow. Later it was realized that we needed to consider all i up to $q^2 - 1$, non inclusive. This made the simulations even slower, and they would frequently crashed.

3.2 Optimizations

Given the unreasonably slow velocity of the code, different questions arose about ways to optimize it. The most important was: must the code check all $i < q^2 - 1$ such that $gcd(i, q^2 - 1) = 1$, or is it sufficient to check only for $i < q$? Code was written to reduce Dickson polynomials of degree i, $q < i < q^2 - 1$, over $\mathbb{F}_q$, and verify whether they reduced to other Dickson polynomials. If they reduced to other Dickson polynomials, then they would already be accounted for when checking the degrees $i < q$ and thus we could optimize the code by checking for i up to q instead of $q^2 - 1$. However, this was not the case, as verified by Code 2.

```
def D(i,x,q):
    sum = 0
    for j in range(i//2 + 1):
        sum += i/(i-j) * binomial(i-j,j) * (-1)^j * x^(i-2*j)
    print "\t",sum
    return sum

def reduceD(i,x,q):
    sum = 0
    for j in range(i//2 + 1):
        sum += ((i-j) * binomial(i-j,j) * (-1)^j % q) * x^((i-2*j)
   %(q-1))
    print "\t",sum
    return sum

def compareD(i,q):
    x = var('x')

    degs = [k%q for k in range(i+1) if (k-i)%2==0]
    deg_reduced = max(degs)
    del degs

    return reduceD(i,x,q) == D(deg_reduced,x,q)


_range = 100
for q in [p for p in range(3,_range) if is_prime(p)]:
    for i in range(q, q^2):
        print "q="+str(q)+" i="+str(i)
        print "\t" + str(compareD(i,q))
```

Code 2: Verifying the reduction of Dickson Polynomials

Dickson polynomials do not necessarily reduce to other dickson polynomials mod $\mathbb{F}_q$, so it is necessary to check i up to $q^2 - 1$. However, it is not necessary to check every $i < q^2 - 1$. As stated in Section 2, it is only necessary to check i coprime to

q^2-1. This optimization, along with many improvements, yielded the code currently in use to find Dickson involutions (See Code 3).

```
def findInvolutions(q):
    print "Involutions over F", q, ":",
    coprime = (q^2-1).coprime_integers(q^2-1)
    for i in coprime:
        works = True
        x = 0
        while works == True and x < q:
            if not DD(i,x,q) == x:
                works = False
            x += 1
        if works == True:
            print i,
    del coprime
    print

def dFixedpoints(d, q):
    print "Involutions over F", q, "with",d,"fixed points:",
    coprime = (q^2-1).coprime_integers(q^2-1)
    for i in coprime:
        fp = 0
        works = True
        x = 0
        while works == True and x < q and fp <= d:
            if not DD(i,x,q) == x:
                works = False
            elif D(i,x,q) == x:
                fp += 1
            x += 1
        if fp == d and works == True:
            print i,
    del coprime
    print
```

Code 3: Finding Involutions

Here, `findInvolutions(q)` takes a prime, integral input `q` and evaluates each $i < q^2-1$ to verify whether D_i produces an involution of $\mathbb{F}_q$. The function `dFixedPoints(d,q)` does the same thing as `findInvolutions(q)`, but takes an additional input `d` and only returns the involutions with d fixed points. These functions were then iterated over many values of q to produce the numerical results in Section 4. The code was excecuted in 3 Intel Core i7 Mac computers, continuously over the course of one month.

3.3 The case of $a = -1$

This case is yet to be studied, after having determined more concrete results for the case of $a = 1$.

4 Results

4.1 Determinations about the search range

Unlike the case with monomial permutations, in the case of Dickson Polynomials, evaluating polynomials with any possible degree $i < q$ is not enough. The possibility for distinct Dickson involutions with degree i such that $q < i < q^2 - 1$ exists. The question of whether this is true arose from Lemma 2.1. The necessity to update the simulation code to evaluate i in range$(q^2 - 1)$ was determined intuitively and later confirmed with the code in Section 3.2.

4.2 Exhaustive Search

The results of the final search algorithm described in Section 3.2 can be found in Appendix B.

One interesting fact is that, contrary to the results in [1], the tendency seems to be that there are less Dickson involutions with smaller amounts of fixed points. For example, in the case of $d = 5$, the only involutions found were over $\mathbb{F}_5$, $\mathbb{F}_7$ and $\mathbb{F}_{11}$. We evaluated up to $\mathbb{F}_{101}$ and no other Dickson involutions were found, which prompts the impression that there exist no more involutions.

However, for $d = 47$ fixed points, involutions were found over $\mathbb{F}_{47}$, $\mathbb{F}_{61}$, $\mathbb{F}_{67}$, $\mathbb{F}_{71}$, $\mathbb{F}_{73}$ and $\mathbb{F}_{79}$. The last q evaluated was $\mathbb{F}_{89}$, which prompts the impression that there could be more results for higher values of q.

Additionally, it was noticed that 8 or 16 involutions were found fixing a particular d and q, but in the majority of the cases all of these 8 polynomials reduce to the same polynomial modulo q. The results for the reduced polynomials can be found in Appendix A.

The cases in which all the Dickson involutions with same d and q (same amount of fixed points and same finite field) did not reduce to the same Polynomial were the following:

1. $d = 17$, $\mathbb{F}_{23}$
2. $d = 29$, $\mathbb{F}_{37}$
3. $d = 29$, $\mathbb{F}_{41}$
4. $d = 29$, $\mathbb{F}_{47}$ [1]
5. $d = 47$, $\mathbb{F}_{71}$
6. $d = 67$, $\mathbb{F}_{89}$
7. $d = 67$, $\mathbb{F}_{97}$ [2]

The cases (1), (3) and (5) are among those that found 16 polynomials instead of 8. It is likely that these reduce to two different polynomials, one of the form $P(x) = c_i x^{2i+1} + c_{i-1} x^{2i-1} + \ldots + c_0 x$ and another of the form $H(x) = (q - c_i)x^{2i+1} + (q -$

[1] These are all the cases with 29 that were found, except for the identity over $\mathbb{F}_{29}$.

[2] These are all the cases with 29 that were found, except for the identity over $\mathbb{F}_{67}$.

$c_{i-1})x^{2i-1} + \ldots + (q - c_0)x$. This was only verified for a few terms and is yet to be confirmed to be true in all of the polynomials in question. Cases (2), (4), (6), (7) only have 8 polynomials.

4.3 Non-Exhaustive Search

Before the findings of Section 4.1, the algorithm to find Dickson Polynomials over $\mathbb{F}_q$ only evaluated any possible degree $i < q$ and did not consider the possibility of degrees $q < i < q^2 - 1$. While the simulations likely did not find every possible Dickson polynomial involution for the specified parameter, the lesser search range on the degree of the polynomial allowed the simulations to run over a wider search range for the size q of the finite field. Similarly to the case of $d = 5$ detailed in Section 4.2, this non-exhaustive simulations found no polynomials over finite fields with $q \geq 13$ in the case of $d = 5$. This simulation checked every finite field with $q < 500$, while the exhaustive search in Section 4.2 checked $q < 60$. If we base ourselves off of extrapolation, we can imagine there are no Dickson Polynomials with 5 fixed points in the range of finite fields $13 \leq q \leq 499$. However, this extrapolation is not necessarily safe, since the case of $d = 11$ showed results for some finite fields that yield no Dickson involutions with $i < q$ but do yield several Dickson involutions with $q < i < q^2 - 1$.

5 Work in Progress

We are currently working on using the results detailed in Section 4 and the Appendices to create a Conjecture for the formulas to construct $D_i(x, 1)$.

6 Future Work

Once the work in Section 5 has been completed, we intend to repeat the research procress for Dickson Polynomials of the form $D_i(x, -1)$.

7 Presentations

References

[1] Francis Castro, Carlos Corrada-Bravo, Natalia Pacheco, and Ivelisse Rubio. Explicit formulas for monomial involutions over finite fields. 2016.

[2] Italo J. Dejter and Ivelisse Rubio. Monomial permutations with uniform cycle decomposition. *Congressus Numerantium*, 69:245–252, 1988.

[3] Oscar Moreno and Ivelisse Rubio. Cyclic decomposition of monomial permutations. *Congressus Numerantium*, 73:147–158, 1990.

[4] Ivelisse Rubio and Carlos J. Corrada-Bravo. Cyclic decomposition of permutations of finite fields obtained using monomials.

[5] Ivelisse M Rubio, Gary R. Mullen, Carlos Corrada, and Francis N. Castro. Dickson permutation polynomials that decompose in cycles of same length. *Contemporary Mathematics*, 491, 2008.

Appendices

A Reductions

All the Dickson involutions with d fixed points, d a prime number, over $\mathbb{F}_d$, reduce to the indentity: x

All the Dickson involutions with $d = 11$ fixed points over $\mathbb{F}_{59}$ reduce to: $58x^{47} + 46x^{45} + 13x^{43} + 29x^{41} + 37x^{39} + 39x^{37} + 3x^{35} + 56x^{33} + 54x^{31} + 20x^{29} + 27x^{27} + 17x^{25} + 45x^{23} + 54x^{21} + 31x^{19} + 48x^{17} + 14x^{15} + 55x^{13} + 13x^{11} + 53x^9 + 11x^7 + 42x^5 + 13x^3 + 49x^1$

All the Dickson involutions with $d = 11$ fixed points over $\mathbb{F}_{73}$ reduce to: $1x^{53} + 21x^{51} + 34x^{49} + 37x^{47} + 30x^{45} + 57x^{43} + 2x^{41} + 55x^{39} + 25x^{37} + 54x^{35} + 23x^{33} + 15x^{31} + 18x^{29} + 12x^{27} + 58x^{25} + 31x^{23} + 54x^{21} + 30x^{19} + 48x^{17} + 57x^{15} + 46x^{13} + 51x^{11} + 42x^9 + 68x^7 + 16x^5 + 11x^3 + 54x^1$

All the Dickson involutions with $d = 17$ fixed points over $\mathbb{F}_{41}$ reduce to: $1x^{31} + 11x^{29} + 36x^{27} + 30x^{25} + 30x^{23} + 40x^{21} + 22x^{19} + 30x^{17} + 15x^{15} + 22x^{13} + 14x^{11} + 22x^9 + 23x^7 + 18x^5 + 6x^3 + 9x^1$

All the Dickson involutions with $d = 17$ fixed points over $\mathbb{F}_{59}$ reduce to: $1x^{41} + 19x^{39} + 33x^{37} + 1x^{35} + 24x^{33} + 18x^{31} + 10x^{29} + 31x^{27} + 10x^{25} + 35x^{23} + 30x^{21} + 52x^{19} + 30x^{17} + 41x^{15} + 52x^{13} + 41x^{11} + 9x^9 + 10x^7 + 18x^5 + 38x^3 + 29x^1$

All the Dickson involutions with $d = 17$ fixed points over $\mathbb{F}_{83}$ reduce to: $1x^{73} + 11x^{71} + 78x^{69} + 40x^{67} + 56x^{65} + 8x^{63} + 65x^{61} + 58x^{59} + 2x^{57} + 64x^{55} + 34x^{53} + 9x^{49} + 46x^{47} + 26x^{45} + 72x^{43} + 76x^{41} + 51x^{39} + 42x^{37} + 15x^{35} + 56x^{33} + 50x^{31} + 26x^{29} + 4x^{27} + 29x^{25} + 78x^{23} + 54x^{21} + 24x^{19} + 76x^{17} + 6x^{15} + 75x^{13} + 46x^{11} + 11x^9 + 8x^7 + 77x^5 + 9x^3 + 29x^1$

All the Dickson involutions with $d = 19$ fixed points over $\mathbb{F}_{41}$ reduce to: $40x^{27} + 26x^{25} + 28x^{23} + 16x^{21} + 23x^{19} + 1x^{17} + 37x^{15} + 5x^{13} + 11x^{11} + 14x^9 + 38x^7 + 40x^5 + 29x^3 + 21x^1$

All the Dickson involutions with $d = 19$ fixed points over $\mathbb{F}_{73}$ reduce to: $72x^{41} + 40x^{39} + 63x^{37} + 6x^{35} + 70x^{33} + 39x^{31} + 38x^{29} + 15x^{27} + 13x^{25} + 15x^{23} + 43x^{21} + 25x^{19} + 32x^{17} + 18x^{15} + 34x^{13} + 36x^{11} + 55x^7 + 48x^5 + 31x^3 + 38x^1$

All the Dickson involutions with $d = 23$ fixed points over $\mathbb{F}_{29}$ reduce to: $28x^{27} + 26x^{25} + 19x^{23} + 23x^{21} + 19x^{19} + 2x^{17} + 25x^{15} + 19x^{13} + 25x^9 + 18x^7 + 8x^5 + 8x^3 + 13x^1$

All the Dickson involutions with $d = 23$ fixed points over $\mathbb{F}_{71}$ reduce to: $70x^{53} + 52x^{51} + 3x^{49} + 4x^{47} + 59x^{45} + 68x^{43} + 42x^{41} + 12x^{39} + 67x^{37} + 65x^{35} + 68x^{33} + 7x^{31} + 41x^{29} + 54x^{27} + 3x^{25} + 26x^{23} + 38x^{21} + 12x^{19} + 66x^{17} + 14x^{15} + 54x^{13} + 22x^{11} + 55x^9 + 47x^7 + 2x^5 + 27x^3 + 17x^1$

All the Dickson involutions with $d = 23$ fixed points over $\mathbb{F}_{79}$ reduce to: $78x^{69} +$

$68x^{67} + 1x^{65} + 19x^{63} + 69x^{61} + 64x^{59} + 9x^{57} + 59x^{55} + 15x^{53} + 35x^{51} + 56x^{49} + 35x^{47} + 39x^{45} + 1x^{43} + 35x^{41} + 3x^{39} + 4x^{37} + 76x^{35} + 45x^{33} + 63x^{31} + 26x^{29} + 63x^{27} + 55x^{25} + 66x^{23} + 59x^{19} + 64x^{17} + 7x^{15} + 45x^{13} + 21x^{11} + 41x^9 + 50x^7 + 50x^5 + 14x^3 + 9x^1$

All the Dickson involutions with $d = 31$ fixed points over $\mathbb{F}_{41}$ reduce to: $40x^{39} + 38x^{37} + 31x^{35} + 6x^{33} + 38x^{31} + 30x^{29} + 6x^{27} + 2x^{25} + 3x^{23} + 37x^{21} + 29x^{19} + 9x^{17} + 34x^{15} + 23x^{13} + 28x^{11} + 24x^9 + 29x^7 + 15x^5 + 9x^3 + 21x^1$

All the Dickson involutions with $d = 31$ fixed points over $\mathbb{F}_{43}$ reduce to: $42x^{41} + 40x^{39} + 33x^{37} + 8x^{35} + 3x^{33} + 11x^{31} + 5x^{29} + 30x^{27} + 35x^{25} + 9x^{23} + 21x^{21} + 37x^{19} + 17x^{17} + 33x^{15} + 11x^{13} + 35x^{11} + 24x^9 + 2x^7 + 13x^5 + 21x^3 + 1x^1$

All the Dickson involutions with $d = 31$ fixed points over $\mathbb{F}_{59}$ reduce to: $58x^{57} + 56x^{55} + 49x^{53} + 24x^{51} + 51x^{49} + 10x^{47} + 54x^{45} + 55x^{43} + 58x^{41} + 35x^{39} + 19x^{37} + 26x^{35} + 43x^{33} + 7x^{31} + 55x^{29} + 27x^{27} + 46x^{25} + 20x^{23} + 42x^{21} + 21x^{19} + 37x^{17} + 40x^{15} + 23x^{13} + 32x^{11} + 9x^9 + 48x^7 + 18x^5 + 40x^3 + 1x^1$

All the Dickson involutions with $d = 31$ fixed points over $\mathbb{F}_{67}$ reduce to: $1x^{43} + 25x^{41} + 16x^{39} + 36x^{37} + 42x^{35} + 21x^{33} + 49x^{31} + 18x^{29} + 29x^{27} + 56x^{25} + 60x^{21} + 17x^{19} + 24x^{17} + 10x^{15} + 32x^{13} + 39x^{11} + 2x^9 + 42x^7 + 4x^5 + 49x^3 + 32x^1$

All the Dickson involutions with $d = 37$ fixed points over $\mathbb{F}_{73}$ reduce to: $1x^{71} + 3x^{69} + 10x^{67} + 35x^{65} + 53x^{63} + 24x^{61} + 37x^{59} + 11x^{57} + 1x^{55} + 33x^{53} + 53x^{51} + 45x^{49} + 72x^{47} + 17x^{45} + 56x^{43} + 70x^{41} + 58x^{39} + 59x^{37} + 37x^{35} + 19x^{33} + 30x^{31} + 53x^{29} + 51x^{27} + 53x^{25} + 15x^{23} + 20x^{21} + 32x^{19} + 26x^{17} + 20x^{15} + 63x^{13} + 41x^{11} + 37x^9 + 63x^7 + 27x^5 + 15x^3 + 2x^1$

All the Dickson involutions with $d = 41$ fixed points over $\mathbb{F}_{53}$ reduce to: $52x^{51} + 50x^{49} + 43x^{47} + 18x^{45} + 33x^{43} + 15x^{41} + 33x^{39} + 31x^{37} + 17x^{35} + 1x^{33} + 52x^{31} + 5x^{29} + 8x^{27} + 2x^{25} + 20x^{23} + 46x^{21} + 5x^{17} + 22x^{15} + 8x^{13} + 41x^{11} + 29x^9 + 22x^7 + 31x^5 + 28x^3 + 25x^1$

All the Dickson involutions with $d = 41$ fixed points over $\mathbb{F}_{59}$ reduce to: $1x^{57} + 3x^{55} + 10x^{53} + 35x^{51} + 8x^{49} + 49x^{47} + 5x^{45} + 4x^{43} + 2x^{41} + 42x^{39} + 52x^{37} + 17x^{35} + 41x^{33} + 43x^{31} + 27x^{29} + 16x^{27} + 18x^{25} + 4x^{23} + 57x^{21} + 30x^{19} + 38x^{17} + 44x^{15} + 9x^{13} + 26x^{11} + 37x^9 + 48x^7 + 21x^5 + 40x^3 + 41x^1$

All the Dickson involutions with $d = 41$ fixed points over $\mathbb{F}_{61}$ reduce to: $60x^{59} + 58x^{57} + 51x^{55} + 26x^{53} + 57x^{51} + 27x^{49} + 5x^{47} + 14x^{45} + 38x^{43} + 9x^{41} + 22x^{39} + 40x^{37} + 31x^{35} + 5x^{33} + 20x^{31} + 14x^{29} + 17x^{27} + 48x^{25} + 14x^{23} + 50x^{21} + 28x^{19} + 28x^{17} + 35x^{15} + 41x^{13} + 40x^{11} + 55x^9 + 32x^7 + 47x^5 + 16x^3 + 49x^1$

All the Dickson involutions with $d = 43$ fixed points over $\mathbb{F}_{61}$ reduce to: $60x^{59} + 58x^{57} + 51x^{55} + 26x^{53} + 57x^{51} + 26x^{49} + 53x^{47} + 31x^{45} + 29x^{43} + 38x^{41} + 7x^{39} + 57x^{37} + 54x^{35} + 7x^{33} + 44x^{31} + 45x^{29} + 45x^{27} + 12x^{25} + 34x^{23} + 11x^{21} + 1x^{19} + 22x^{17} + 52x^{15} + 8x^{13} + 10x^{11} + 14x^9 + 44x^7 + 54x^5 + 47x^3 + 41x^1$

All the Dickson involutions with $d = 43$ fixed points over $\mathbb{F}_{83}$ reduce to: $82x^{81} + 80x^{79} + 73x^{77} + 48x^{75} + 41x^{73} + 47x^{71} + 22x^{69} + 79x^{67} + 65x^{65} + 9x^{63} + 16x^{61} + 50x^{59} + 67x^{57} + 42x^{55} + 44x^{53} + 14x^{51} + 56x^{49} + 54x^{47} + 11x^{45} + 56x^{43} + 30x^{41} + 65x^{39} + 17x^{37} + 74x^{33} + 77x^{31} + 7x^{29} + 68x^{27} + 45x^{25} + 80x^{23} + 49x^{21} + 5x^{19} + 81x^{17} + 22x^{15} + 16x^{13} + 3x^{11} + 45x^9 + 24x^7 + 43x^5 + 36x^3 + 1x^1$

All the Dickson involutions with $d = 47$ fixed points over $\mathbb{F}_{61}$ reduce to: $60x^{59} + 58x^{57} + 51x^{55} + 26x^{53} + 57x^{51} + 26x^{49} + 53x^{47} + 31x^{45} + 29x^{43} + 37x^{41} + 47x^{39} + 48x^{37} + 11x^{35} + 25x^{33} + 57x^{31} + 5x^{29} + 22x^{27} + 8x^{25} + 2x^{23} + 32x^{21} + 40x^{17} + 40x^{15} + 12x^{13} + 57x^{11} + 37x^9 + 46x^7 + 14x^5 + 17x^3 + 29x^1$

All the Dickson involutions with $d = 47$ fixed points over $\mathbb{F}_{67}$ reduce to: $66x^{65} + 64x^{63} + 57x^{61} + 32x^{59} + 8x^{57} + 7x^{55} + 26x^{53} + 64x^{51} + 11x^{49} + 15x^{47} + 39x^{45} + 50x^{43} + 64x^{41} + 42x^{39} + 7x^{37} + 5x^{35} + 36x^{33} + 65x^{31} + 26x^{29} + 63x^{27} + 12x^{25} + 36x^{23} + 42x^{21} + 35x^{19} + 30x^{17} + 47x^{15} + 27x^{13} + 21x^{11} + 49x^9 + 61x^7 + 32x^5 + 1x^3$

All the Dickson involutions with $d = 47$ fixed points over $\mathbb{F}_{73}$ reduce to: $72x^{71} + 70x^{69} + 63x^{67} + 38x^{65} + 20x^{63} + 49x^{61} + 36x^{59} + 62x^{57} + 72x^{55} + 41x^{53} + 41x^{51} + 62x^{49} + 38x^{47} + 13x^{45} + 1x^{43} + 5x^{41} + 70x^{39} + 39x^{37} + 17x^{35} + 4x^{33} + 58x^{31} + 38x^{29} + 34x^{27} + 5x^{25} + 16x^{23} + 34x^{21} + 71x^{19} + 22x^{17} + 37x^{15} + 56x^{13} + 10x^{11} + 5x^9 + 5x^7 + 62x^5 + 69x^3 + 53x^1$

All the Dickson involutions with $d = 47$ fixed points over $\mathbb{F}_{79}$ reduce to: $1x^{77} + 3x^{75} + 10x^{73} + 35x^{71} + 46x^{69} + 56x^{67} + 58x^{65} + 55x^{63} + 47x^{61} + 12x^{59} + 69x^{57} + 52x^{55} + 60x^{53} + 50x^{51} + 2x^{49} + 64x^{47} + 11x^{45} + 74x^{43} + 5x^{41} + 45x^{39} + 35x^{37} + 57x^{35} + 62x^{33} + 78x^{31} + 41x^{29} + 29x^{27} + 53x^{25} + 49x^{23} + 50x^{21} + 28x^{19} + 42x^{17} + 33x^{15} + 12x^{13} + 15x^{11} + 6x^9 + 19x^7 + 35x^5 + 15x^3 + 9x^1$

B Results

. The results are written in the format

$$d : [q_1, i_1], [q_2, i_2], \ldots [q_r, i_r]//q_{max}$$

where $[q, i]$ is a pair such that $D_i(x, 1)$ is an involution of $\mathbb{F}_q$ with d fixed points, and q_{max} is the range of the simulation, i.e. the largest q such that involutions over $\mathbb{F}_q$ were searched for.
4: [] //101
5: [5,1], [5,5], [5,7], [5,11], [5,13], [5,17], [5,19], [5,23], [7,5], [7,11], [7,13], [7,19], [7,29], [7,35], [7,37], [7,43], [11,7], [11,17], [11,43], [11,53], [11,67], [11,77], [11,103], [11,113] //101
7: [7,1], [7,7], [7,17], [7,23], [7,25], [7,31], [7,41], [7,47], [11,13], [11,23], [11,37], [11,47], [11,73], [11,83], [11,97], [11,107] //109
11: [11,1], [11,11], [11,49], [11,59], [11,61], [11,71], [11,109], [11,119], [13,29], [13,41], [13,43], [13,55], [13,113], [13,125], [13,127], [13,139], [59,191], [59,829], [59,911], [59,1549],

[59,1931], [59,2569], [59,2651], [59,3289], [73,413], [73,845], [73,1819], [73,2251], [73,3077], [73,3509], [73,4483], [73,4915] //107
12: [] //97
17: [17,1], [17,17], [17,127], [17,143], [17,145], [17,161], [17,271], [17,287], [23,65], [23,89], [23,109], [23,131], [23,133], [23,155], [23,175], [23,199], [23,329], [23,353], [23,373], [23,395], [23,397], [23,419], [23,439], [23,463], [41,71], [41,391], [41,449], [41,769], [41,911], [41,1231], [41,1289], [41,1609], [59,331], [59,389], [59,1351], [59,1409], [59,2071], [59,2129], [59,3091], [59,3149], [83,811], [83,1567], [83,1877], [83,2633], [83,4255], [83,5011], [83,5321], [83,6077] //97
19: [19,1], [19,19], [19,161], [19,179], [19,181], [19,199], [19,341], [19,359], [41,139], [41,181], [41,659], [41,701], [41,979], [41,1021], [41,1499], [41,1541], [73,179], [73,253], [73,2411], [73,2485], [73,2843], [73,2917], [73,5075], [73,5149]
23: [23,1], [23,23], [23,241], [23,263], [23,265], [23,287], [23,505], [23,527], [29,181], [29,209], [29,211], [29,239], [29,601], [29,629], [29,631], [29,659], [31,161], [31,191], [31,209], [31,239], [31,241], [31,271], [31,289], [31,319], [31,641], [31,671], [31,689], [31,719], [31,721], [31,751], [31,769], [31,799], [71,449], [71,881], [71,1639], [71,2071], [71,2969], [71,3401], [71,4159], [71,4591], [79,649], [79,1351], [79,1769], [79,2471], [79,3769], [79,4471], [79,4889], [79,5591] //79
29: [29,1], [29,29], [29,391], [29,419], [29,421], [29,449], [29,811], [29,839], [37,305], [37,341], [37,343], [37,379], [37,989], [37,1025], [37,27], [37,1063], [41,169], [41,209], [41,239], [41,281], [41,559], [41,601], [41,631], [41,71], [41,1009], [41,1049], [41,1079], [41,1121], [41,1399], [41,1441], [41,1471], [41,1511], [47,137], [47,185], [47,919], [47,967], [47,1241], [47,1289], [47,23],[47,2071], [71,181], [71,251], [71,2269], [71,2339], [71,2701], [71,2771], [71,789], [71,4859] //101
31: [31,1], [31,31], [31,449], [31,479], [31,481], [31,511], [31,929], [31,959],[41,379], [41,419], [41,421], [41,461], [41,1219], [41,1259], [41,1261], [41,1301], [43,265], [43,307], [43,617], [43,659], [43,1189], [43,1231], [43,1541], [43,1583], [59,481], [59,539], [59,1201], [59,1259], [59,2221], [59,2279], [59,2941], [59,2999], [67,307], [67,373], [67,1871], [67,1937], [67,2551], [67,2617], [67,4115], [67,4181] //107
37: [37,1], [37,37], [37,647], [37,683], [37,685], [37,721], [37,1331], [37,1367], [73,1079], [73,1153], [73,1511], [73,1585], [73,3743], [73,3817], [73,4175], [73,4249] //97
41: [41,1], [41,41], [41,799], [41,839], [41,841], [41,881], [41,1639], [41,1679], [53,649], [53,701], [53,703], [53,755], [53,2053], [53,2105], [53,2107], [53,2159], [59,521], [59,581], [59,1159], [59,1219], [59,2261], [59,2321], [59,2899], [59,2959], [61,311], [61,371], [61,1489], [61,1549], [61,2171], [61,2231], [61,3349], [61,3409] //67
43: [43,1], [43,43], [43,881], [43,923], [43,925], [43,967], [43,1805], [43,1847], [61,559], [61,619], [61,1241], [61,1301], [61,2419], [61,2479], [61,3101], [61,3161], [83,337], [83,419], [83,3025], [83,3107], [83,3781], [83,3863], [83,6469], [83,6551] //103
47: [47,1], [47,47], [47,1057], [47,1103], [47,1105], [47,1151], [47,2161], [47,2207], [61,869], [61,929], [61,931], [61,991], [61,2729], [61,2789], [61,2791],[61,2851], [67,749], [67,815], [67,1429], [67,1495], [67,2993], [67,3059], [67,3673], [67,3739], [71,559], [71,631], [71,1009, [71,1079], [71,1441], [71,1511], [71,1889], [71,1961], [71,3079], [71,3151], [71,3529], [71,3599], [71,3961], [71,4031], [71,4409], [71,4481], [73,667], [73,739], [73,1925], [73,1997], [73,3331], [73,3403], [73,4589], [73,4661], [79,311], [79,391], [79,2729], [79,2809], [79,3431], [79,3511], [79,5849], [79,5929] //89

67: [67,1], [67,67], [67,2177], [67,2243], [67,2245], [67,2311], [67,421], [67,4487], [89,1891], [89,1979], [89,1981], [89,2069], [89,5851], [89,939], [89,5941], [89,6029], [97,1471], [97,1567], [97,3137], [97,3233], [97,6175], [97,271], [97,7841], [97,7937] //101
83: [83,1], [83,83], [83,3361], [83,3443], [83,3445], [83,3527], [83,805], [83,6887] //103