REFERENCES

A Polynomial Analogue of the $3n + 1$ Problem

Kenneth Hicks, Gary L. Mullen, Joseph L. Yucas, and Ryan Zavislak

1. INTRODUCTION. The $3n + 1$ problem (also known as the Collatz, Syracuse, Kakutani's, or Ulam's problem and Hasse's algorithm, see Lagarias [**3**] and Wirsching [**5**]) starts with a positive integer n, and iterates the Collatz function

$$C(n) = \begin{cases} 3n+1 & \text{if } n \equiv 1 \pmod 2 \\ \frac{n}{2} & \text{if } n \equiv 0 \pmod 2 \end{cases}$$

viewed as mapping the integers to itself. The famous $3n + 1$ conjecture postulates that after a finite number of iterations one always arrives at the value 1. This has been shown to be true for all $n < 2^{40}$. Whether it converges to 1 for every positive integer n is an open problem, see Lagarias [**3**].

The intricate relationship between the ring Z of integers and the polynomial ring $F_q[x]$ of polynomials in a single variable x over the finite field F_q has been studied extensively. This discussion has included many topics such as comparisons between prime integers and irreducible polynomials, Goldbach type problems in both the integer and polynomial settings (Effinger and Hayes [**1**]), and the study of twin primes and twin irreducibles and their densities, see [**2**]. In [**2**], the authors allude to the fact that in many (but not all) cases an analogous problem in the polynomial setting may be easier to resolve than the original problem. The result presented here indeed provides an example of that phenomenon.

We start with the binary field F_2 since this is the case most analogous to the integer version, see [**2**]. In the integer case, the first two primes are of course 2 and 3. In the $F_2[x]$ setting, the first two irreducible polynomials are x and $x + 1$. The analogue to the $3n + 1$ problem for polynomials is the map

$$C_1(f(x)) = \begin{cases} (x+1)f(x)+1 & \text{if } f(0) \neq 0 \\ \dfrac{f(x)}{x} & \text{if } f(0) = 0 \end{cases}$$

acting on the polynomial ring $F_2[x]$. Repeated application m times is denoted by $C_1^{(m)}(f(x))$. The main result of this paper is given in section 2. We prove that for any polynomial $f(x)$ of degree $n \geq 1$ over the binary field F_2, $C_1^{(I)}(f(x)) = 1$ for some $I \leq n^2 + 2n$. In section 5, a generalization of this result is shown to hold in any field.

In section 3, we find a lower bound on the maximum number of iterations for a polynomial of degree n over F_2 to converge to 1, and in section 4 we develop some necessary conditions on polynomials of degree n over the binary field which require the maximum number of iterations.

Matthews and Leigh [**4**] also discuss a finite field polynomial version of the original $3n + 1$ problem. In particular, in their Example 2, they discuss the problem where one uses the function

$$C_2(f(x)) = \begin{cases} (x+1)^2 f(x)+1 & \text{if } f(0) \neq 0 \\ \dfrac{f(x)}{x} & \text{if } f(0) = 0. \end{cases}$$

In this case, Matthews and Leigh provide an example which has a divergent trajectory, namely a starting polynomial $f(x)$ whose iterates have degrees which increase without bound. In addition, in their Example 1, they provide another case of an initial polynomial with a divergent trajectory when the term $(x+1)^2$ above is replaced by $(x+1)^3$. See [**4**] for further details.

2. MAIN RESULT.

Theorem 2.1. *For any polynomial $f(x)$ of degree $n \geq 1$ over the binary field F_2, $C_1^{(I)}(f(x)) = 1$ for some $I \leq n^2 + 2n$.*

Proof. We use induction on the degree n. For $n = 1$, $f(x) = x + a_0$. If $a_0 = 0$, we divide by x and we are done. If $a_0 = 1$, then after one iteration we obtain the polynomial x^2, which after two iterations ends at 1.

Assume now that the result holds for any polynomial over F_2 of degree $n-1$, i.e., after a finite number of iterations, any polynomial over F_2 of degree $n-1$ converges to 1 in at most $(n-1)^2 + 2(n-1)$ iterations.

Assume that $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ has degree n over F_2. If $a_0 = 0$, we divide by x to obtain a monic polynomial of degree $n-1$ over F_2, which by the induction hypothesis converges to 1 in at most $(n-1)^2 + 2(n-1)$ iterations. Hence we assume that $a_0 = 1$ and define j with $1 \leq j \leq n$ to be the smallest value so that $a_j = 1$. Hence $f(x)$ has the form $x^n + \cdots + x^j + 1$. The next iteration gives a polynomial of the form $x^{n+1} + \cdots + x^j + x$, so we divide by x to obtain the polynomial $x^n + \cdots + x^{j-1} + 1$.

Continuing, we see that with each pair of iterations, the smallest exponent on the first nonzero term decreases by 1. Hence after $2(j-1)$ iterations, we reach a polynomial of the form

$$h(x) = x^n + \cdots + x + 1.$$

Another iteration yields a polynomial of degree $n+1$ which is divisible by x^2. After dividing by x^2, we are left with a polynomial $h(x)$ of degree $n-1$. Notice that we have used $2(j-1)+3$ iterations so far. By the induction hypothesis, $h(x)$ converges to 1 in at most $(n-1)^2 + 2(n-1)$ iterations. Consequently, $f(x)$ converges to 1 in at most $2(j-1) + 3 + (n-1)^2 + 2(n-1)$ iterations. Since $j \leq n$, the result follows. ∎

3. NUMBER OF ITERATIONS OVER $F_2[x]$.

For a binary polynomial $f(x)$ denote by $I_{f(x)}$ the number of iterations of the algorithm needed in order for the polynomial $f(x)$ to converge to 1. Let M_n be the maximum number of iterations required for any binary polynomial of degree n to converge to 1. In this section we study the following problem:

Problem 3.1. For a given degree n, what is M_n and which polynomials $f(x)$ of degree n satisfy $I_{f(x)} = M_n$?

In the appendix of this paper we give M_n for $n \leq 30$. We also provide all of the polynomials requiring this maximum number of steps.

The proof of the main result in the previous section suggests that over F_2, the polynomial $f(x) = x^n + 1$ may have a large value of $I_{f(x)}$. We use this observation to provide a lower bound for M_n.

Theorem 3.2. *For $2^k < n \leq 2^{k+1}$, the polynomial $f(x) = x^n + 1$ requires exactly $n + 2^{k+2}$ iterations to converge to 1. In particular,*

$$M_n \geq n + 2^{k+2}$$

Before proving this theorem, we prove a series of needed results.

Lemma 3.3. *Suppose $f(0) = 1$. Then after two iterations on $f(x)$ one obtains*

$$(x+1)\frac{f(x)+1}{x} + 1.$$

Proof. Since the constant term of $f(x)$ is 1, after two iterations we obtain

$$\frac{(x+1)f(x)+1}{x} = \frac{(x+1)f(x)+x+1}{x} + 1 = (x+1)\frac{f(x)+1}{x} + 1. \qquad \blacksquare$$

Notice that by the previous lemma after two iterations on $x^n + 1$ we obtain the polynomial

$$(x+1)x^{n-1} + 1.$$

Applying two more iterations yields

$$(x+1)^2x^{n-2} + 1.$$

Thus, by induction we have:

Lemma 3.4. *After 2n iterations on $x^n + 1$ one obtains the polynomial $(x+1)^n + 1$.*

Consequently, we are now led to examine the polynomial $(x+1)^n + 1$.

Lemma 3.5. *Suppose n is odd. Then $I_{(x+1)^{n+1}+1} = I_{(x+1)^n+1} - 1$.*

Proof. Since $n+1$ is even, x^2 divides $(x+1)^{n+1} + 1$, so after two iterations one obtains

$$\frac{(x+1)^{n+1}+1}{x^2}.$$

Now, $(x+1)^n + 1$ is divisible by x but not by x^2, so after one iteration we get

$$\frac{(x+1)^n+1}{x},$$

and after two more iterations we obtain

$$(x+1)\frac{(x+1)^n+x+1}{x^2} + 1 = \frac{(x+1)^{n+1}+1}{x^2}. \qquad \blacksquare$$

The previous result now yields information on $x^n + 1$, the polynomial of interest.

Lemma 3.6. *Suppose n is odd. Then $I_{x^{n+1}+1} = I_{x^n+1} + 1$.*

Proof. By Lemma 3.4, after $2n+2$ iterations on $x^{n+1}+1$ we obtain $(x+1)^{n+1}+1$ and after $2n$ iterations on x^n+1 we obtain $(x+1)^n+1$. The result now follows from the previous lemma. ∎

One final lemma is needed for the proof of Theorem 3.2.

Lemma 3.7. *Let* $g(x) = f(x^2)$. *Then* $I_{g(x)} = 2I_{f(x)}$.

Proof. Proceed by induction on $I_{f(x)}$. If $I_{f(x)} = 1$ then $f(x) = x$ and $I_{g(x)} = 2$. Suppose $I_{f(x)} > 1$. We consider two cases:

Case 1: Suppose $f(0) = 1$. By Lemma 3.3, after two iterations on $f(x)$ we obtain

$$f_2(x) = (x+1)\frac{f(x)+1}{x} + 1.$$

Notice also that $g(0) = 1$ so after two iterations on $g(x)$ we obtain

$$g_2(x) = (x+1)\frac{f(x^2)+1}{x} + 1.$$

Since x^2 divides $f(x^2)+1$, we see that $g_2(0) = 1$, so after two more iterations we obtain

$$g_4(x) = (x+1)^2\frac{f(x^2)+1}{x^2} + 1 = f_2(x^2).$$

By induction $I_{g_4(x)} = 2I_{f_2(x)}$ and thus

$$I_{g(x)} = I_{g_4(x)} + 4 = 2I_{f_2(x)} + 4 = 2(I_{f_2(x)} + 2) = 2I_{f(x)}.$$

Case 2: Suppose $f(0) = 0$. After one iteration on $f(x)$ we obtain

$$f_1(x) = \frac{f(x)}{x}.$$

In this case x^2 divides $g(x)$, so after two iterations on $g(x)$ we obtain

$$g_2(x) = \frac{g(x)}{x^2} = \frac{f(x^2)}{x^2} = f_1(x^2).$$

Consequently, again by induction we have

$$I_{g(x)} = I_{g_2(x)} + 2 = 2I_{f_1(x)} + 2 = 2(I_{f_1(x)} + 1) = 2I_{f(x)}.$$ ∎

We are now able to prove Theorem 3.2.

Proof of Theorem 3.2. We induct on n. The result is trivial for $n = 1$. Suppose $n > 1$. If n is even then $2^{k-1} < n/2 \le 2^k$, so by induction $I_{x^{n/2}+1} = 2^{k+1} + n/2$. By Lemma 3.7, $I_{x^n+1} = 2(2^{k+1} + n/2) = 2^{k+2} + n$. If n is odd then $2^{k-1} < (n+1)/2 \le 2^k$, so by induction $I_{x^{(n+1)/2}+1} = 2^{k+1} + (n+1)/2$. By Lemma 3.7, $I_{x^{n+1}+1} = 2(2^{k+1} + (n+1)/2) = 2^{k+2} + n + 1$. The result now follows from Lemma 3.6. ∎

Combining Theorem 2.1 and Theorem 3.2 we have:

Corollary 3.8. *For any degree n, the number M_n of iterations required in order for all polynomials of degree n to converge to 1 is bounded by*

$$n + 2^{k+2} \leq M_n \leq n^2 + 2n,$$

where the nonnegative integer k is determined by $2^k < n \leq 2^{k+1}$.

4. CONDITIONS ON $f(x)$ WITH $I_{f(x)} = M_n$. In this section, some necessary conditions are developed on polynomials $f(x)$ of degree n over the binary field F_2 with $I_{f(x)} = M_n$.

Proposition 4.1. *Suppose $f(x)$ is a polynomial of degree n over F_2 with $I_{f(x)} = M_n$. Then $f(x)$ is a multiple of $x + 1$. In particular, $f(x)$ must have even weight.*

Proof. If $f(1) = 1$ then

$$\frac{x(f(x) + 1)}{x + 1} + 1$$

has degree n and reduces to $f(x)$ after two iterations, so $f(1) = 0$. ∎

Proposition 4.2. *Suppose $f(x) = g(x) + x + 1$ is a polynomial over F_2 of degree $n \geq 2$ where x^2 divides $g(x)$. Then $f(x)$ cannot require the maximum number of iterations for polynomials of degree n, i.e., $I_{f(x)} < M_n$.*

Proof. By Proposition 4.1, we may assume that $f(1) = 0$. Write $f(x) = (x + 1)h(x)$ for some polynomial $h(x)$ of degree $n - 1$. Notice that after one iteration on $f(x)$ we obtain $(x + 1)f(x) + 1 = (x + 1)g(x) + x^2$. Since x^2 divides $g(x)$ we obtain after two more iterations

$$(x + 1)\frac{g(x)}{x^2} + 1 = (x + 1)\frac{f(x) + x + 1}{x^2} + 1 = \frac{f(x)(x + 1) + 1}{x^2}.$$

Thus after three iterations on $f(x)$ we obtain

$$\frac{f(x)(x + 1) + 1}{x^2}.$$

Now consider the polynomial $f'(x) = xh(x) + 1$ of degree n. We will show that it takes five iterations for $f'(x)$ to reduce to

$$\frac{f(x)(x + 1) + 1}{x^2},$$

thus showing that $f'(x)$ requires more iterations than $f(x)$. After one iteration on $f'(x)$ we obtain $x^2h(x) + x + xh(x)$. In the next step we divide by x and get $xh(x) + 1 + h(x)$. Since $f(0) = 1$, $h(0) = 1$ so $h(x) + 1$ is divisible by x. Once again we divide by x and get

$$h(x) + \frac{h(x) + 1}{x}.$$

Now since $g(x) + x + 1 = (x + 1)h(x)$ we have $h(x) + 1 = g(x) + x(h(x) + 1)$. Since x^2 divides $g(x)$ and x divides $h(x) + 1$ we see that x^2 divides $h(x) + 1$. In particular the constant term of

$$h(x) + \frac{h(x) + 1}{x}$$

is $h(0) = 1$. So the next iteration is

$$(x + 1)\left(h(x) + \frac{h(x) + 1}{x}\right) + 1 = xh(x) + \frac{h(x) + 1}{x}.$$

Dividing by x yields

$$h(x) + \frac{h(x) + 1}{x^2} = \frac{h(x)(x^2 + 1) + 1}{x^2} = \frac{f(x)(x + 1) + 1}{x^2},$$

as desired. ∎

Proposition 4.3. *Suppose $f(x)$ is a polynomial of degree n over F_2. Then $I_{f(x)} \equiv n \pmod 2$. In particular, $M_n \equiv n \pmod 2$.*

Proof. C_1 either increases or decreases the degree of a polynomial by one. Thus the parity of the degree of $C_1^{(n)}(f(x))$ is the same as the parity of the degree of $f(x)$ if n is even, and the parities are different if n is odd. ∎

5. A POLYNOMIAL VERSION OVER ANY FIELD. Unfortunately, Theorem 2.1 does not hold for other finite fields. For example, consider $f(x) = x^2 + 1$ over F_3. After six iterations we arrive at $f(x)$ and enter a cycle.

In this final section we give a general version of Theorem 2.1 which does hold over any field. However, we do lose the aesthetics. The proof is a straightforward generalization of the proof of Theorem 2.1, so it is omitted.

Let F be a field and let $F[x]$ denote the unique factorization domain of all polynomials in a single indeterminate x over the field F. For $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ define $C_F(f(x))$ by

$$C_F(f(x)) = \begin{cases} \left(x - \dfrac{a_0}{a_j}\right) f(x) + \dfrac{a_0^2}{a_j} & \text{if } f(0) \neq 0 \\ \dfrac{f(x)}{x} & \text{if } f(0) = 0, \end{cases}$$

where j is the smallest value so that $1 \leq j \leq n$ and $a_j \neq 0$.

Notice that when $F = F_2$, C_F reduces to our C_1 studied in the previous sections.

Theorem 5.1. *For any monic polynomial $f(x)$ of degree $n \geq 1$ over F, $C_F^{(I)}(f(x)) = 1$ for some $I \leq n^2 + 2n$.*

APPENDIX. For $n \leq 30$, in the following table we give the maximum number M_n of steps required to reach 1 for any polynomial of degree n, and for each n we give all of the polynomials requiring this maximum number of steps, i.e., all polynomials $f(x)$ with the property that $I_{f(x)} = M_n$. We list a binary polynomial $f(x)$ by listing the

n	M_n	$f(x)$
2	6	2 0
3	11	3 0
4	14	4 3 2 0
5	21	5 0
6	24	6 5 4 0
	24	6 5 4 3 2 0
7	29	7 6 3 0
8	34	8 7 6 5 3 0
9	41	9 0
10	48	10 9 7 0
11	55	11 9 8 5 4 0
12	58	12 11 9 8 7 5 4 3 2 0
13	65	13 11 10 9 5 0
14	72	14 13 12 10 8 5 4 0
15	81	15 14 13 10 5 0
16	86	16 15 12 10 8 5 4 0
17	93	17 15 12 10 9 5 4 0
18	100	18 17 16 13 10 9 5 0
	100	18 17 16 15 14 10 9 5 4 0
19	117	19 18 17 14 9 0
20	122	20 19 16 14 12 9 8 0
21	129	21 19 16 14 13 9 8 5 4 0
	129	21 19 18 15 14 9 8 7 6 0
22	132	22 21 17 16 14 13 12 11 9 8 7 5 4 3 2 0
	132	22 21 19 18 17 15 14 13 12 11 9 7 6 5 4 3 2 0
23	139	23 21 19 18 17 16 14 13 12 11 9 8 6 5 4 0
	139	23 21 20 19 15 10 9 8 6 5 4 0
24	152	24 19 14 9 8 0
25	159	25 24 21 19 17 14 13 9 8 0
	159	25 24 21 19 17 14 13 9 8 5 4 0
26	166	26 24 21 19 18 14 13 9 8 5 4 0
27	169	27 26 22 21 19 18 17 16 14 13 12 11 9 8 6 5 4 0
	169	27 26 22 21 19 18 17 16 14 13 12 11 9 8 7 5 4 3 2 0
	169	27 26 24 23 22 20 19 18 17 16 14 12 9 0
28	180	28 24 23 19 18 14 13 9 7 0
29	191	29 28 27 26 25 19 18 17 16 15 9 0
30	198	30 27 26 18 17 9 8 0
	198	30 27 26 25 24 18 16 9 8 0

exponents of the terms with nonzero coefficients. Thus for example, the polynomial $x^4 + x^3 + x^2 + 1$ is listed as 4 3 2 0. In cases where there is more than one polynomial $f(x)$ with $I_{f(x)} = M_n$, we have listed those polynomials in separate rows.

ACKNOWLEDGMENT. We would like to thank the referees for a number of helpful comments which improved an earlier version of our paper.

REFERENCES

1. G. W. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials Over a Finite Field*, Oxford University Press, Oxford, United Kingdom, 1991.
2. G. Effinger, K. Hicks, and G. L. Mullen, Integers and polynomials: comparing the close cousins Z and $F_q[x]$, *Math. Intelligencer* **27** (2005) 26–34.
3. J. C. Lagarias, The $3X + 1$ problem and its generalizations, this MONTHLY **85** (1985) 1–21; also available at `http://www.cecm.sfu.ca/organics/papers/lagarias/`.
4. K. R. Matthews and G. M. Leigh, A generalization of the Syracuse algorithm in $F_q[x]$, *J. Number Thy.* **25** (1987) 274–278.
5. G. J. Wirsching, *The Dynamical System Generated by the* $3n + 1$ *Function*, Lecture Notes in Mathematics, vol. 1681, Springer-Verlag, Berlin, 1998.

KENNETH HICKS received his Ph.D. in Physics from the University of Colorado in 1984. He joined the faculty at Ohio University in 1988 and now serves as Director for O.U.'s "Structure of the Universe" Project. He is supported by the National Science Foundation, publishes regularly in physics journals, and enjoys doing computational mathematics in his spare time.
Department of Physics and Astronomy, Ohio University, Athens, OH 45701
hicks@ohio.edu

GARY L. MULLEN serves as Professor of Mathematics at the Pennsylvania State University. He also serves as Editor-in-Chief of Finite Fields and Their Applications, published by Elsevier. In his spare time he enjoys the outdoors and likes to contemplate the serene beauty of mathematics.
Department of Mathematics, The Pennsylvania State University, University Park, PA 16802
mullen@math.psu.edu

JOSEPH L. YUCAS serves as Professor of Mathematics at Southern Illinois University. His hobbies include music and billiards.
Department of Mathematics, Southern Illinois University, Carbondale, IL 62901
jyucas@math.siu.edu

RYAN ZAVISLAK received a B.S. degree in Mathematics from Ohio University in 2005. In his senior year, he did a special topics course with Dr. Hicks on the connections between physics and number theory. He has passionately pursued the $3n + 1$ problem over the years and plans to publish his findings in the near future. He is currently working with the U.S. government.
Department of Physics and Astronomy, Ohio University, Athens, OH 45701
ryanzavislak@hotmail.com