Analogue of the $3x + 1$ Problem in Polynomial Rings of Characteristic 2

Dan Nichols
nichols@math.umass.edu

University of Massachusetts

Oct. 3, 2015

The $3x + 1$ problem

- The $3x + 1$ map $T : \mathbb{Z} \to \mathbb{Z}$ is defined

$$T(x) = \begin{cases} (3x+1)/2, & x \text{ odd} \\ x/2, & x \text{ even} \end{cases}$$

  Iteration of this map defines a dynamical system on the positive integers
- More generally, replace 3 with some other odd integer m
- The trajectory of $x \in \mathbb{Z}$ is the sequence $x, T(x), T^2(x), \ldots$
  - For example, the trajectory of $x = 11$ is $11, 17, 26, 13, 20, 10, 5, 16, 8, 4, 2, 1, 2, 1, \ldots$
  - Eventually enters a cycle: $1, 2, 1, 2, \ldots$
- Problem: how can we tell if the trajectory of x diverges or enters a cycle?
- Collatz conjecture: for every x, the trajectory of x eventually reaches 1 (and then becomes cyclic).
  - Verified up to a huge range numerically, but still unproven

A reformulation of the conjecture:

- The stopping time $\sigma(x)$ is the minimum number of iterations before the trajectory of x reaches a number $< x$. That is,

$$\sigma(x) = \inf \left\{ k > 0 : T^k(x) < x \right\}.$$

  If the trajectory never goes below x, we say $\sigma(x) = \infty$.

- Example: the trajectory of $x = 11$ is $11, 17, 26, 13, 20, 10, 5, \ldots$. So $\sigma(11) = 5$.
- The Collatz conjecture is true if and only if every positive integer x has $\sigma(x) < \infty$.

Terras' theorem (1970s)

Theorem (Terras)

With probability 1, a randomly chosen positive integer has finite stopping time. Or,

$$\lim_{N\to\infty} P\left(\sigma(x) < \infty \,\middle|\, 0 < x \leq N\right) = 1$$

Proof sketch:

- parity sequence of x is $p_0, p_1, p_2, \ldots$ where $p_k \in \{0, 1\}$ is the parity of $T^k(x)$. Corresponds to ups and downs in trajectory
- Bijective map between positive integers $< 2^N$ and binary sequences of length N:

$$\Phi : \mathbb{Z}/2^N \longleftrightarrow \{0, 1\}^N$$

- Parity sequences are uniformly distributed in the set of sequences in $\{0, 1\}$
- Reduces problem to combinatorics on binary sequences. Most will be roughly half 1s, half 0s.

$3x + 1$ as random walk

- So $3x + 1$ can be modelled as a multiplicative random walk
  - Each iteration, multiply by either $3/2$ or by $1/2$ with equal probability
- Or (using logarithm) an additive random walk:

$$\log_2 T^k(x) \approx \log_2 x + \sum_{i=0}^{k-1} X_i$$

  where X_i are independent random variables which take values -1 or $-1 + \log_2 3$ each with $P = 1/2$.
- Expected value of each step: $-1 + \frac{1}{2}\log_2 3 \approx -0.208$
- (Actually bound between 2 random walks: $\frac{3}{2}x \leq \frac{3x+1}{2} \leq \frac{5}{3}x$)

$mx + 1$ problem in $\mathbb{F}_2[t]$

Idea: define similar systems in other rings, get random walks with slightly different parameters

- For an irreducible $m \in \mathbb{F}_2[t]$, we define the $mx + 1$ map $T : \mathbb{F}_2[t] \to \mathbb{F}_2[t]$ as follows:

$$T(f) = \begin{cases} (mf + 1)/t, & f \equiv 1 \mod t \\ f/t, & f \equiv 0 \mod t \end{cases}$$

- Stopping time $\sigma(f)$ is the number of steps before trajectory reaches a polynomial of lower degree than f
- For many m, there are nontrivial cycles (do not include 1)
- Matthews & Leigh (1987) showed provably divergent trajectory when $m = t^2 + 1$
- Hicks, Mullen, Yucas, Zadislav (2008) proved that all trajectories reach 1 for $m = t + 1$

Theorem (Terras for polynomials)

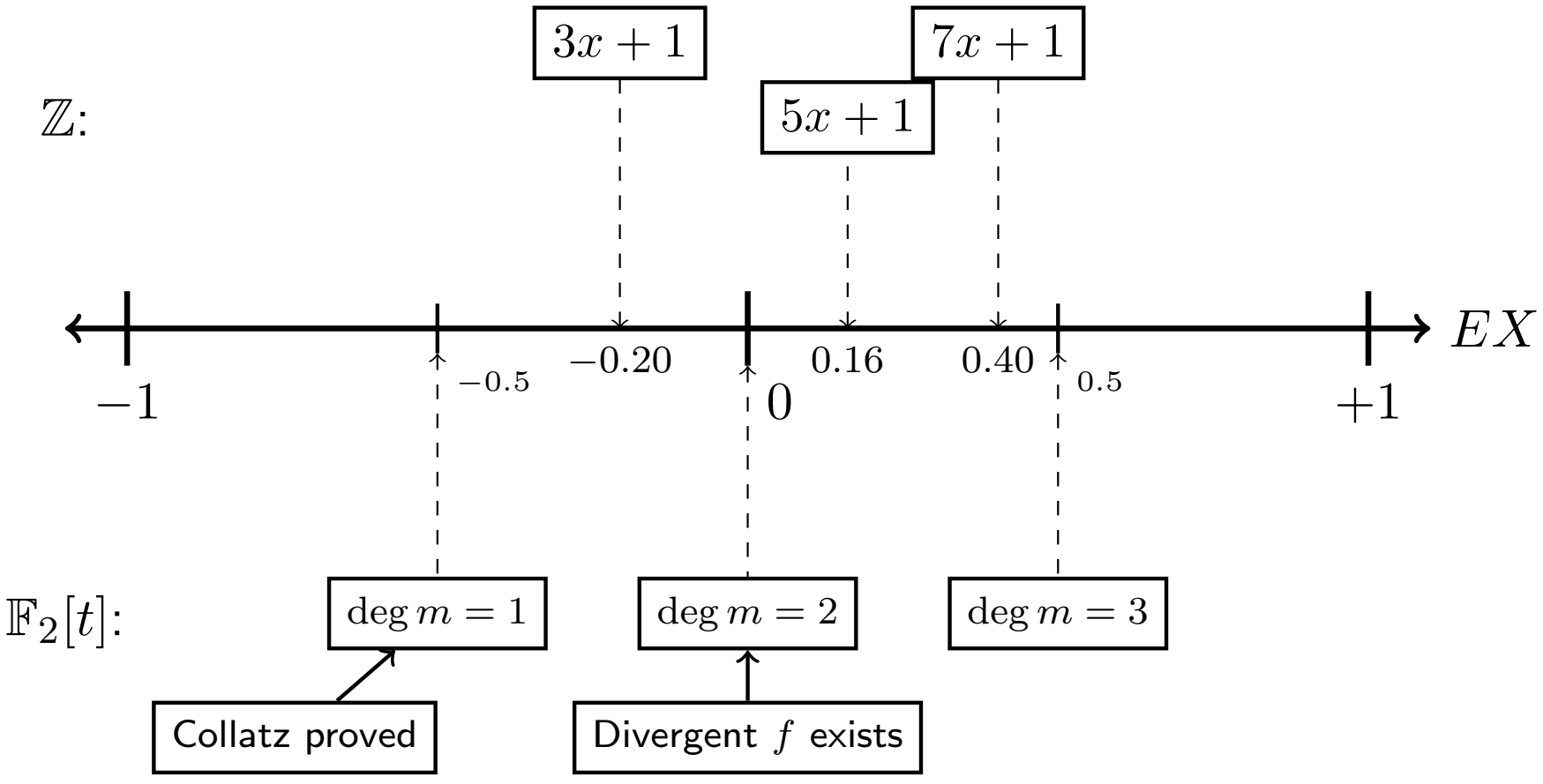
If $\deg m \leq 2$*, the probability that a randomly-chosen polynomial* $f \in \mathbb{F}_2[t]$ *has* $\sigma(f) < \infty$ *is 1. If* $\deg m = d > 2$*, the probability is equal to the smallest root of the polynomial* $g_d(z) = z^d - 2z + 1$*.*

- In $\mathbb{Z}$, best known result (Terras) is upper & lower bounds on this probability.
  - For $m = 3$, lower bound is 1
  - Hard to get a good result for $m = 5, 7, \ldots$
- But in $\mathbb{F}_2[t]$, exact probability can be found (numerically)
- Also defined similar dynamical system in ring $\mathbb{F}_2[x,t]/(x^2 + tx + q(t))$ for some irreducible $q \in \mathbb{F}_2[t]$.
  - Proved Terras analogue here too

$\deg m$	$P(\sigma(f) < \infty)$
1	1
2	1
3	0.6180340
4	0.5436890
5	0.5187901
6	0.5086604
7	0.5041383
8	0.5020171
9	0.5009942
10	0.5004931
11	0.5002455

Random walk comparison of $mx + 1$ problems

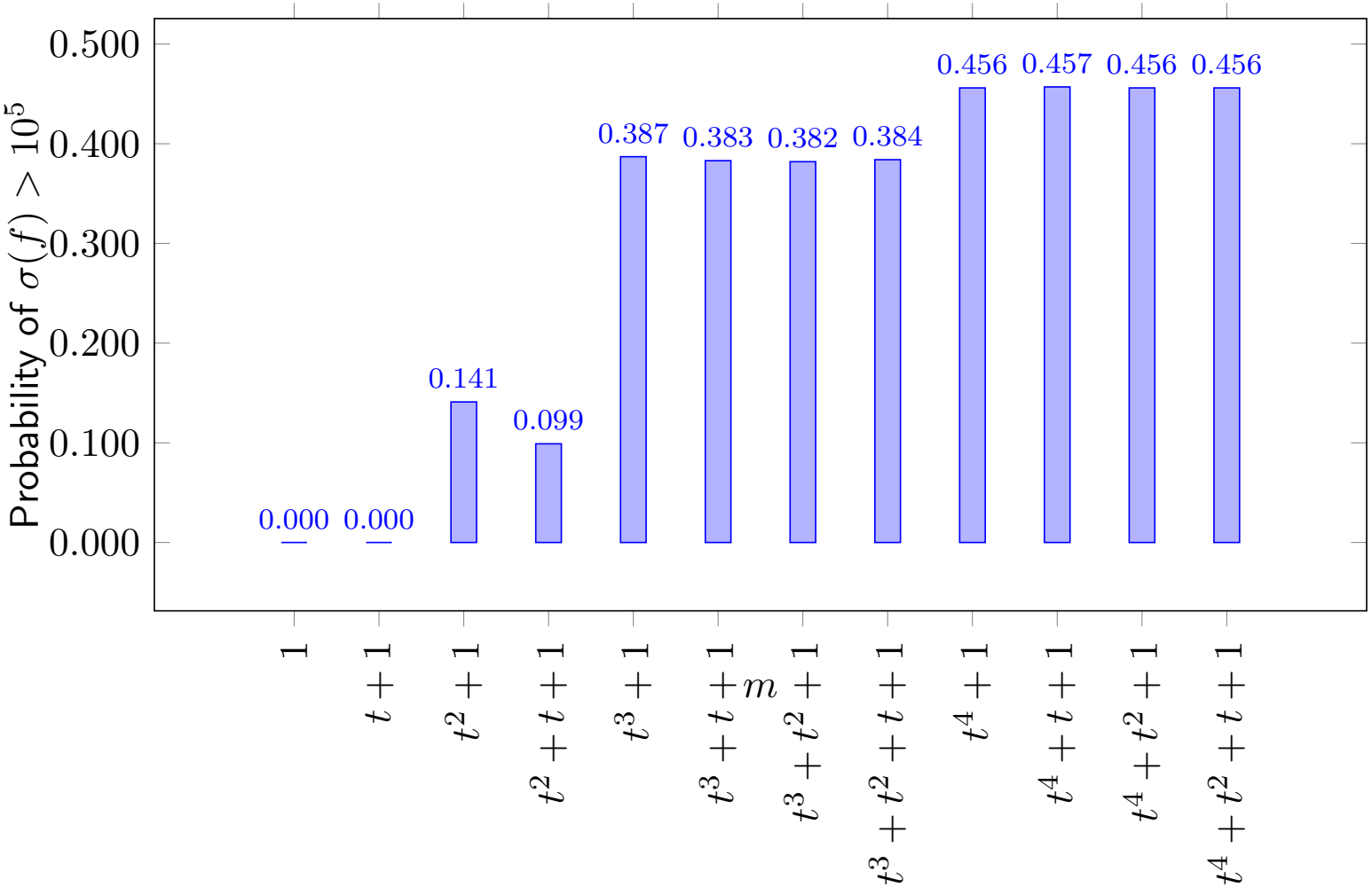
Expected value of one iteration of $mx + 1$ map:



Experimental results

- Wrote C++ code to efficiently calculate $mx + 1$ trajectories for $\mathbb{F}_2$-polynomials.
  - Store polynomials as array of bits representing coefficients.
  - All fast operations, heavily optimized
- For each irreducible $m \in \mathbb{F}_2[t]$ of interesting degree...
  - For each $f \in \mathbb{F}_2[t]$ of degree ≤ 19,
    - Compute $T^k(f)$ up to $k = 10^5$
    - Find $\sigma(f)$ if $\sigma(f) < 10^5$
    - Look for cycle in trajectory using Brent's algorithm (similar to Pollard rho algorithm)
    - If no cycle or stopping time detected after 100,000 iterations, give up. f (probably) diverges and (probably) has $\sigma(f) = \infty$.

Figure: Frequency of long stopping times ($\sigma(f) > 10^5$) for various $m \in \mathbb{F}_2[t]$



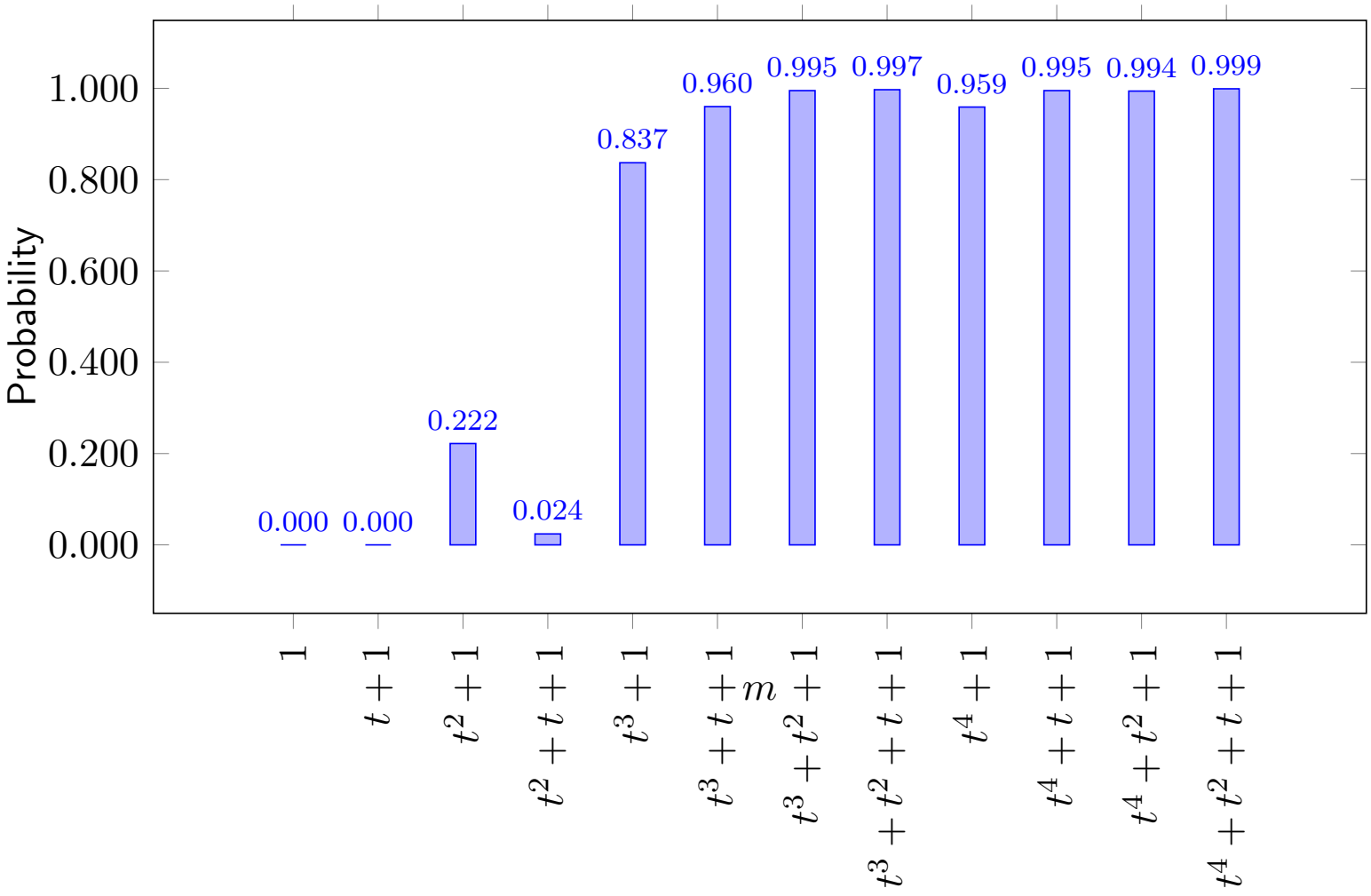
Stopping time distribution for quadratic $m \in \mathbb{F}_2[t]$

Figure: Frequency count of $\sigma(f)$ among polynomials of degree < 20. Bin size 50.

$\sigma(f)$	$t+1$	t^2+1	t^2+t+1	t^3+1
$0-50$	1048573	900255	930844	642494
$50-100$	0	413	12315	0
$100-150$	0	0	724	0
$150-200$	0	1	90	0
$200-250$	0	0	36	0
$250-300$	0	0	9	0
$300-350$	0	0	5	0
$350-400$	0	0	2	0
$400-450$	0	0	1	0
$> 10^5$	2	147906	104549	406081

Divergent trajectory data

Figure: Frequency of (probable) divergent trajectories for various $m \in \mathbb{F}_2[t]$



Further reading


The Ultimate Challenge: The $3x + 1$ Problem.
Edited by Jeffrey C. Lagarias.
American Mathematical Society, providence, RI, 2010.
xiv+344pp. ISNB: 978-0-8218-4940-8.


K.R. Matthews, G.M. Leigh.
A generalization of the Syracuse algorithm in $\mathbb{F}_q[x]$.
Journal of Number Theory 25 (1987), pp 274-278.


Kenneth Hicks, Gary L. Mullen, Joseph L. Yucas and Ryan Zavislak.
A polynomial analogue of the $3n + 1$ problem.
The American Mathematical Monthly Vol. 115 No. 7 (Aug. - Sep. 2008), pp 615-622.


Richard P. Brent. An improved Monte Carlo factorization algorithm. *BIT* 20 (1980) no. 2, pp 176-184.