Chebyshev mappings of finite fields

Julian Rosen, Zachary Scherr, Benjamin Weiss and Michael E. Zieve

Abstract

For a fixed prime p, we consider the set of maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ of the form $a \mapsto T_n(a)$, where $T_n(x)$ is the degree-n Chebyshev polynomial of the first kind. We observe that these maps form a semigroup, and we determine its size and structure.

1 Introduction

Some of the "world's most interesting" polynomials [2] are the *Chebyshev polynomials* [4], which are defined for any positive integer n to be

$$T_n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} 2^{n-2k-1} x^{n-2k}.$$

The first few Chebyshev polynomials are

n	$T_n(x)$
1	x
2	$2x^2 - 1$
3	$4x^3 - 3x$
4	$8x^4 - 8x^2 + 1$
5	$16x^5 - 20x^3 + 5x$
6	$32x^6 - 48x^4 + 18x^2 - 1$
7	$64x^7 - 112x^5 + 56x^3 - 7x$

Chebyshev polynomials have integer coefficients and satisfy $T_n(\cos\theta) = \cos n\theta$ for any $\theta \in \mathbb{R}$. Of particular interest are the mappings $a \mapsto T_n(a)$, since (in view of the functional equation) any two such mappings commute, and more generally, $T_n \circ T_m = T_{nm}$. The Chebyshev polynomials induce especially remarkable mappings on the rings $\mathbb{Z}/p\mathbb{Z}$ for prime p: for instance, if $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ has degree at most $p^{1/4}$, and the map $a \mapsto f(a)$ describes a bijection $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, then f is a composition of Chebyshev polynomials, cyclic polynomials x^d, and linear polynomials[1] [1, 5]. The purpose of this note is to analyze the collection

[1] The coefficients of these linear polynomials are only required to lie in the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$.

of maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ which are induced by Chebyshev polynomials. Since there are only finitely many maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ of any sort, there must be infinitely many pairs (n, m) of distinct positive integers such that T_n and T_m induce the same map $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. This leads to the following questions:

(1) When do T_n and T_m induce the same map $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$?

(2) For fixed p, how many distinct maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ are induced by Chebyshev polynomials?

We can say more about the structure of the collection of maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induced by Chebyshev polynomials, which we will call *Chebyshev maps*. For, the identity $T_n \circ T_m = T_{nm}$ implies that (for a fixed prime p) the set of Chebyshev maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is closed under composition, and hence forms a semigroup. This fact already distinguishes Chebyshev polynomials from most other classes of polynomials, and raises the question

(3) What is the structure of the semigroup of Chebyshev maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$?

As often happens, the prime $p = 2$ behaves differently from other primes. The answers to our questions for $p = 2$ are as follows.

Theorem 1. *The polynomials T_n and T_m induce the same map $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ if and only if $n \equiv m \pmod 2$. There are a total of two Chebyshev maps $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, namely the identity and the constant map 1. These form a semigroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$ under the operation of multiplication.*

For odd primes p, the answers to our questions are as follows.

Theorem 2. *Let p be an odd prime. The polynomials T_n and T_m induce the same map $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ if and only if n is congruent to either $\pm m$ or $\pm pm$ modulo $(p^2 - 1)/2$. The number of distinct Chebyshev maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is $(p+1)(p+3)/8$. The semigroup of Chebyshev maps $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is isomorphic to the quotient of the multiplicative semigroup $\mathbb{Z}/((p^2 - 1)/2)\mathbb{Z}$ by the subgroup $\{1, -1, p, -p\}$.*

Before proving these results, we illustrate Theorem 2 by writing it out in the two smallest cases.

- When $p = 3$, there are three Chebyshev maps on $\mathbb{Z}/p\mathbb{Z}$, induced by T_1, T_2, and T_4. Here T_1 is the identity, T_4 is the constant map 1, and $T_2 \circ T_2 = T_4$. These three maps comprise the quotient of the semigroup $\mathbb{Z}/4\mathbb{Z}$ (under multiplication) by the subgroup $\{1, -1\}$; the cosets of this subgroup are $\{1, -1\}$, $\{0\}$, and $\{2\}$.
- When $p = 5$, there are six Chebyshev maps on $\mathbb{Z}/p\mathbb{Z}$. These maps correspond to the cosets of the subgroup $\{1, -1, 5, -5\}$ of the semigroup $\mathbb{Z}/12\mathbb{Z}$ (under multiplication), namely,

$$\{0\}, \{1, 5, 7, 11\}, \{2, 10\}, \{3, 9\}, \{4, 8\}, \{6\}.$$

Here a prescribed coset corresponds to the map $a \mapsto T_n(a)$, where n is any positive integer whose image in $\mathbb{Z}/12\mathbb{Z}$ lies in the prescribed coset. The coset containing 1 is the identity element, and in this case it is the only invertible element in the quotient semigroup. Note that the cosets have sizes 1, 2, and 4. This also holds for larger primes, and will be made explicit in the proof of Theorem 2.

2 Even characteristic

In this section we prove the following result, which implies Theorem 1.

Proposition 3. *If n is even then $T_n(x) \equiv 1 \pmod{2}$; if n is odd then $T_n(x) \equiv x \pmod{2}$.*

We begin with an alternate development of Chebyshev polynomials. For any positive integer n, the Fundamental Theorem of Symmetric Polynomials [6, p. 99] implies that there is a unique $f \in \mathbb{Z}[x, y]$ such that $f(u + v, uv) = u^n + v^n$. Moreover, $f(tx, t^2y)$ is homogeneous in t of degree n, so $f(x, y) = \sum_{i=0}^{\lfloor n/2\rfloor} f_i x^{n-2i} y^i$ for some integers f_i. Now put $g(x) := f(x, 1) = \sum_{i=0}^{\lfloor n/2\rfloor} f_i x^{n-2i}$, so that $g(u+u^{-1}) = u^n + u^{-n}$. Then $h(x) := g(2x)/2$ satisfies $h((z+z^{-1})/2) = (z^n + z^{-n})/2$, which for $z = e^{i\theta}$ implies that $h(\cos\theta) = \cos n\theta$. Hence $h - T_n$ vanishes at $\cos\theta$, and since θ is arbitrary it follows that $h = T_n$.

We now determine the lowest-degree term of h, and use it to compute the reduction of h mod 2. If n is even then substituting $u = -v$ yields

$$2v^n = (-v)^n + v^n = f(0, -v^2) = f_{n/2} \cdot (-v^2)^{n/2},$$

so that $f_{n/2} = 2 \cdot (-1)^{n/2}$. Since $h = \sum_{i=0}^{\lfloor n/2\rfloor} f_i x^{n-2i} 2^{n-2i-1}$ and each f_i is an integer, it follows for even n that $h \equiv 1 \pmod{2}$. If n is odd then

$$\frac{u^n + v^n}{u + v} = \sum_{i=0}^{(n-1)/2} f_i (u + v)^{n-1-2i} (uv)^i;$$

substituting $u = -v$ on the right yields $f_{(n-1)/2}(-v^2)^{(n-1)/2}$, and evaluating the left side at $u = -v$ (for instance, via l'Hôpital's rule) yields nv^{n-1}. Thus we find that $f_{(n-1)/2} = n \cdot (-1)^{(n-1)/2}$ is odd, so that $h \equiv x \pmod{2}$. This proves the Proposition (and more).

3 Odd characteristic

In this section we prove Theorem 2. Let p be an odd prime, and write $\mathbb{F}_p$ and $\overline{\mathbb{F}}_p$ for the field $\mathbb{Z}/p\mathbb{Z}$ and its algebraic closure. As noted in the previous section, $T_n((z + z^{-1})/2) = (z^n + z^{-n})/2$.

Lemma 4. *For any $\alpha \in \mathbb{F}_p$, the number of elements $\beta \in \overline{\mathbb{F}}_p^*$ such that $\beta + \beta^{-1} = \alpha$ is either one or two, and if it is two then the elements are reciprocals of one another.*

Proof. For $\beta \in \overline{\mathbb{F}}_p^*$, the equality $\beta + \beta^{-1} = \alpha$ holds precisely when β is a root of $x^2 - \alpha x + 1$. But this polynomial has either one or two roots in $\overline{\mathbb{F}}_p^*$, and if it has two then they are reciprocals. □

For any $\alpha \in \mathbb{F}_p$, write $\alpha = \beta + \beta^{-1}$ with β as in the lemma; then, since pth powering is an automorphism of $\overline{\mathbb{F}}_p$ which fixes $\mathbb{F}_p$, we have

$$\beta^p + \beta^{-p} = \alpha^p = \alpha = \beta + \beta^{-1},$$

so the lemma implies that $\beta^p \in \{\beta, \beta^{-1}\}$, whence $\beta^{p\pm1} = 1$. Conversely, if $\beta \in \overline{\mathbb{F}}_p$ satisfies $\beta^{p\pm1} = 1$, then $\beta + \beta^{-1}$ is fixed by pth powering, and hence lies in $\mathbb{F}_p$. Thus the elements of $\mathbb{F}_p$ are precisely the elements $(\beta + \beta^{-1})/2$ where $\beta \in \overline{\mathbb{F}}_p$ and $\beta^{p\pm1} = 1$.

Now, if $\beta^{p\pm1} = 1$ then

$$\begin{aligned} T_n\left(\frac{\beta+\beta^{-1}}{2}\right) = T_m\left(\frac{\beta+\beta^{-1}}{2}\right) \quad &\Leftrightarrow \quad \beta^n + \beta^{-n} = \beta^m + \beta^{-m} \\ &\Leftrightarrow \quad \text{either} \quad \beta^n = \beta^m \quad \text{or} \quad \beta^n = \beta^{-m} \\ &\Leftrightarrow \quad \text{either} \quad \beta^{n-m} = 1 \quad \text{or} \quad \beta^{n+m} = 1. \end{aligned}$$

Thus, T_n and T_m define the same maps σ_n and σ_m on $\mathbb{F}_p$ if and only if every $(p \pm 1)$th root of unity in $\overline{\mathbb{F}}_p$ is either an $(n-m)$th root of unity or an $(n+m)$th root of unity. Since $\overline{\mathbb{F}}_p$ contains both primitive $(p+1)$th roots of unity and primitive $(p-1)$th roots of unity, it follows that $\sigma_n = \sigma_m$ if and only if $n \equiv \pm m \pmod{p+1}$ and $n \equiv \pm m \pmod{p-1}$, or equivalently, $n \equiv \pm m$ or $\pm\, pm \pmod{(p^2-1)/2}$.

We have shown that the number of maps $\mathbb{F}_p \to \mathbb{F}_p$ induced by Chebyshev polynomials equals the number of orbits of the action of multiplication by $\{1, -1, p, -p\}$ on residue classes mod $(p^2-1)/2$. There are precisely two orbits of size 1, namely $\{0\}$ and $\{(p^2-1)/4\}$. The orbits of size 2 are $\{\pm k(p-1)/2\}$ for $k = 1, 2, \ldots, (p-1)/2$ and $\{\pm \ell(p+1)/2\}$ for $\ell = 1, 2, \ldots, (p-3)/2$. The remaining $(p^2-4p+3)/2$ residue classes split into orbits of size 4. Hence the number of distinct orbits, which equals the number of distinct maps σ_n, is $(p^2+4p+3)/8$.

Finally, since $T_n \circ T_m = T_{nm}$, the map $n \mapsto \sigma_n$ is a semigroup homomorphism from the multiplicative semigroup of positive integers to the semigroup of maps $\mathbb{F}_p \to \mathbb{F}_p$ induced by Chebyshev polynomials. Since we showed above that $\sigma_n = \sigma_m$ precisely when $n \equiv \pm m$ or $\pm\, pm \pmod{(p^2-1)/2}$, it follows that the semigroup of Chebyshev maps $\mathbb{F}_p \to \mathbb{F}_p$ is isomorphic to the quotient of the multiplicative semigroup $\mathbb{Z}/((p^2-1)/2)\mathbb{Z}$ by the subgroup $\{\pm1, \pm p\}$.

4 Final remarks

It would be interesting to consider similar questions over more general fields or rings. Proposition 3 shows that if K is any commutative ring of characteristic 2 then the identity map and the constant map 1 are the only maps $K \to K$ induced by Chebyhsev polynomials. If K is a finite field whose order q is odd, then the proof of Theorem 2 shows that the number of Chebyshev maps $K \to K$ is $(q+1)(q+3)/8$, and the semigroup of Chebyshev maps is the quotient of the multiplicative semigroup $\mathbb{Z}/((q^2-1)/2)\mathbb{Z}$ by the subgroup $\{1, -1, q, -q\}$.

Theorem 2 implies that, for any odd prime p, the group of permutations of $\mathbb{Z}/p\mathbb{Z}$ induced by Chebyshev polynomials, or equivalently the group of invertible elements in our semigroup, is the quotient group $(\mathbb{Z}/((p^2-1)/2)\mathbb{Z})^*/\langle -1, p\rangle$. This recovers the main result of [3].

Finally, we note that when examining Chebyshev-like mappings of arbitrary fields K, it is often convenient to treat the related class of *Dickson polynomials*. These are defined for any positive integer n and any $\alpha \in K$ by

$$D_n(x, \alpha) = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k} \binom{n-k}{k} (-\alpha)^k x^{n-2k}$$

(it turns out that $\frac{n}{n-k}\binom{n-k}{k}$ is an integer). If $2\alpha \neq 0$ then the Dickson polynomial is related to the Chebyshev polynomial over $K(\sqrt{\alpha})$, via the change of variables

$$D_n(x, \alpha) = 2\sqrt{\alpha}^n \cdot T_n\left(\frac{x}{2\sqrt{\alpha}}\right).$$

Acknowledgements. We thank Florian Block, Kevin Carde, Jeff Lagarias, and the referees and editor-in-chief for valuable suggestions which improved the exposition in this paper.

References

[1] M. Fried, On a conjecture of Schur, *Michigan Math. J.* **17** (1970) 41–55.

[2] R. Lidl and G. L. Mullen, The world's most interesting class of integral polynomials, *J. Combin. Math. Combin. Comput.* **37** (2001) 87–100.

[3] W. Nöbauer, Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen, *J. Reine Angew. Math.* **231** (1968) 216–219.

[4] T. J. Rivlin, Chebyshev Polynomials: from Approximation Theory to Algebra and Number Theory, 2nd ed., John Wiley, New York, 1990.

[5] G. Turnwald, On Schur's conjecture, *J. Austral. Math. Soc. Ser. A* **58** (1995) 312–357.

[6] B. L. van der Waerden, *Algebra* (trans. F. Blum and J. R. Schulenberger), vol. I, Springer-Verlag, New York, 1991.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109
{rosenjh, zscherr, blweiss, zieve}@umich.edu