Counting Polynomial Functions over Rings

Arya Eskandarian

May 2, 2015

Abstract

A proof that every function from a finite field $\mathbb{F}$ to itself can be represented as a polynomial over $\mathbb{F}$ is presented. A method for counting the number of functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ that can be represented as polynomials over $\mathbb{Z}_n$ is devised for small values of n.

1 Introduction

There are many functions from the $\mathbb{R}$ to $\mathbb{R}$, and they are incredibly difficult to characterize. However, if we consider continuous functions from $\mathbb{R}$ to $\mathbb{R}$ we have a nice result: any continuous function on closed interval can be uniformly approximated by a polynomial as close as desired[1]. So a certain important class of functions over the reals can be represented by polynomials.

A natural inquiry is to consider functions not over the field of the reals, but over a finite field. Given a function from a finite field $\mathbb{F}$ to $\mathbb{F}$, is it possible to represent that function as polynomial over $\mathbb{F}$? That is, for every function f from $\mathbb{F}$ to $\mathbb{F}$, does there exist a polynomial $p(x)$ such that $f(a) = p(a)$ for every a in $\mathbb{F}$? We will show that every function from a field $\mathbb{F}$ to itself can be represented as a polynomial over $\mathbb{F}$. In addition, we will study functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ and state a few result concerning the number of functions that can be represented as a polynomial over $\mathbb{Z}_n$.

2 Results for Fields

Given any finite non-collinear collection of points in the real plane, it is possible to interpolate a polynomial between those points. We will try to apply a similar procedure over finite fields.

Proposition 1. *Any function from a finite field $\mathbb{F}$ to $\mathbb{F}$ can be represented as a polynomial over $\mathbb{F}$.*

Proof. Take any function g from $\mathbb{F}$ to $\mathbb{F}$, where $\mathbb{F}$ is a finite field. Then we have a finite list of all the elements of $\mathbb{F}$, label them $f_1, f_2, \ldots, f_n$, where $f_i \neq f_j$ for any distinct i and j. We want to find an n degree polynomial that has the value $g(f_i)$ at f_i for every i. This is equivalent to solving the following system of equations for $a_1, \ldots, a_n$:

$$\begin{aligned} a_0 + a_1(f_1) + a_2(f_1)^2 + \ldots + a_n(f_1)^n &= g(f_1) \\ a_0 + a_1(f_2) + a_2(f_2)^2 + \ldots + a_n(f_2)^n &= g(f_2) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 + a_1(f_n) + a_2(f_n)^2 + \ldots + a_n(f_n)^n &= g(f_n) \end{aligned}$$

This linear system can be represented with the help of the Vandermonde matrix, V.

$$V = \begin{bmatrix} 1 & f_1 & f_1^2 & \dots & f_1^{n-1} \\ 1 & f_2 & f_2^2 & \dots & f_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & f_n & f_n^2 & \dots & f_n^{n-1} \end{bmatrix}$$

Now if we let $a = [a_0, a_1, \dots, a_n]^T$ and let $g = [g(f_1), g(f_2), \dots, g(f_n)]^T$, then we can find our coefficients by solving the system $Va = g$ for a. The question of whether the polynomial exists reduces to the question of whether the determinant of V is non-zero. The determinant of the Vandermonde matrix is $\prod_{i<j}(f_i - f_j)$ [2]. Since every one of our f_i are distinct, the determinant is non-zero and therefore a unique solution exists. So for every function from $\mathbb{F}$ to $\mathbb{F}$, we can find a polynomial over $\mathbb{F}$ that agrees with that function at every point. □

3 Results for Rings

The next natural generalization is to consider functions from R to R, where R is any finite ring, and see if it is possible to represent that function as a polynomial over R. Unfortunately, as R is not necessarily a field, it is impossible to use the same approach we used above. We do know that there is only a finite number of polynomials we need to consider.

Proposition 2. *For a finite ring R of order n, any function that can be represented as a polynomial over R can be represented as a polynomial over R of degree less than n.*

Proof. Let $r_1, r_2, \dots, r_n$ be a list of all the elements of R. Take any polynomial $f(x)$. $f(x)$ can be expressed as $f(x) = (x-r_1)(x-r_2)\dots(x-r_n)q(x)+g(x)$, where $q(x)$ is a polynomial over R and the degree of $g(x)$ is less than n. Now if we evaluate f at any $r_i \in R$, we will find $f(r_i) = (r_i-r_1)\dots(r_i-r_i)\dots(r_i-r_n)+g(r_i) = g(r_i)$. Therefore $f(x)$ and $g(x)$ are the same as functions over R. We have established that any function $f(x)$ that can be represented as a polynomial over R can be represented as a polynomial $g(x)$ of degree less than n. □

The above proposition implies that if a particular function is not given by a polynomial of degree less that n, that particular function is not given by any polynomial from R to R. We will use this proposition to prove the proposition below, which lets us count the number of functions that can be represented as polynomials over a few rings of the form $\mathbb{Z}_n$.

Proposition 3. *Let V be the the following matrix over the ring $\mathbb{Z}_n$:*

$$V = \begin{bmatrix} 1 & 1 & 1^2 & \dots & 1^{n-1} \\ 1 & 2 & 2^2 & \dots & 2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & n & n^2 & \dots & n^{n-1} \end{bmatrix}$$

The number of different polynomial functions is equal to the order of the column space of V, $Col(V) = \{Vx : x \in \mathbb{Z}_n^n\}$. If $Nul(V) = \{x : Ax = 0, x \in \mathbb{Z}_n\}$, then both $Col(V)$ and $Nul(V)$ are subgroups of $\mathbb{Z}_n^n$. Moreover, $|Nul(V)||Col(V)| = n^n$.

Proof. The column space $Col(V)$ of V will consist of all the different polynomial functions of degree less than n over $\mathbb{Z}_n$. It is easy to see that $Col(V)$ is a subgroup of $\mathbb{Z}_n^n$:

1. $0 \in Col(V)$, so $Col(V)$ is nonempty.
2. If $x_1, x_2 \in Col(V)$, then $x_1 = a_0c_0 + \dots + a_{n-1}c_{n-1}$ and $x_2 = b_0c_0 + \dots + b_{n-1}c_{n-1}$ for some $a_i, b_i \in \mathbb{Z}_n$, where c_i are the column vectors. Then $x_1 + x_2 = (a_0 + b_0)c_0 + \dots + (a_{n-1} + b_{n-1})c_{n-1}$, which implies that $x_1 + x_2 \in Col(V)$.

3. If $x \in Col(V)$ then $x = a_0c_0 + \ldots + a_{n-1}c_{n-1}$. Then $-x = (-a_0)c_0 + \ldots + (-a_{n-1})c_{n-1}$, which implies that $-x \in Col(V)$. In other words, $x^{-1} \in Col(V)$.

We have shown that $Col(V)$ is a subgroup of $\mathbb{Z}_n^n$ and that it consists of all the different polynomial functions of degree less than n over $\mathbb{Z}_n$. From Proposition 2 we know that all polynomial functions are expressible as polynomial functions of degree less than n, so the order of $Col(V)$ is equal to the number of different polynomial functions over $\mathbb{Z}_n$. The null space of V is $Nul(V) = \{x \in \mathbb{Z}_n^n : Vx = 0\}$. Like $Col(V)$, $Nul(V)$ is a subgroup of $\mathbb{Z}_n^n$:

1. $0 \in Nul(V)$, so $Nul(V)$ is nonempty.
2. If $x_1, x_2 \in Nul(V)$, then $V(x_1 + x_2) = Vx_1 + Vx_2 = 0 + 0 = 0$ so $x_1 + x_2 \in Nul(V)$.
3. If $x \in Nul(V)$, then $V(-x) = -Vx = -0 = 0$. Therefore $x^{-1} \in Nul(V)$.

So $Nul(V)$ is a subgroup of $\mathbb{Z}_n^n$. Because $\mathbb{Z}_n^n$ is Abelian, both $Col(V)$ and $Nul(V)$ are normal subgroups. Our matrix V also acts as a homomorphism from $\mathbb{Z}_n^n$ to $Col(V)$, with $Nul(V)$ is its kernel. From the First Isomorphism Theorem for groups, we have that $Col(V)$ is isomorphic to $\mathbb{Z}_n^n/Nul(V)$. This implies that $|Col(V)| = |\mathbb{Z}_n^n|/|Nul(V)|$. In other words, $|Nul(V)||Col(V)| = |\mathbb{Z}_n^n| = n^n$. □

Proposition 3 implies that in order to calculate the number of functions that are represented as polynomials over $\mathbb{Z}_n$, all we need to do is find the order of $Nul(V)$. We use this result to count the the number of functions that are represented as polynomials over $\mathbb{Z}_4$ and $\mathbb{Z}_6$. For $\mathbb{Z}_4$, we have the matrix

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 0 & 0 \\ 1 & -1 & 1 & -1 \end{bmatrix}$$

Which we can reduce to the matrix below, using typical Gaussian elimination methods:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

From here we can count the number of elements in $Nul(V)$. Consider any element $x = [a_0, a_1, a_2, a_3]^T$ of $\mathbb{Z}_4^4$. Now Vx will be:

$$Vx = \begin{bmatrix} a_0 \\ a_1 + a_2 + a_3 \\ 2a_2 + 2a_3 \\ 2a_3 \end{bmatrix}$$

If Vx is in the null space, then every row must equal 0. We know that there is only 1 choice, 0, for a_0. There are only 2 elements in $\mathbb{Z}_4$ that satisfy $2y = 0$, so we have 2 choices for a_3. Looking at the third row, we notice that $2a_3 = 0$, and so there are likewise 2 choices for a_2. Finally, our choices of a_2 and a_3 completely determine a_1, so we have 1 choices for a_1. Therefore there are 4 elements $x \in \mathbb{Z}_4^4$ such that $Vx = 0$. In other words, the order of $Nul(V)$ is 4. Now by Proposition 3 we know that $|Col(V)| = |\mathbb{Z}_4^4|/|Nul(V)| = 4^4/4 = 4^3$. Therefore there are 4^3 functions that can be represented as polynomials over $\mathbb{Z}_4$.

For $\mathbb{Z}_6$, we have

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 2 & 4 & 2 \\ 1 & 3 & 3 & 3 & 3 & 3 \\ 1 & 4 & 4 & 4 & 4 & 4 \\ 1 & -1 & 1 & -1 & 1 & -1 \end{bmatrix}$$

Which we can reduce to

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

We count the order of $Nul(V)$ similarly to how we counted it for $\mathbb{Z}_4$. Consider any element $x = [a_0, a_1, a_2, a_3, a_4, a_5]^T$ of $\mathbb{Z}_6^6$. Now Vx will be:

$$Vx = \begin{bmatrix} a_0 \\ a_1 + a_2 + a_3 + a_4 + a_5 \\ 2a_2 + 2a_4 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

If Vx is in the null space, then every row must equal 0. We know that there is only 1 choice, 0, for a_0. There are no restrictions on a_3, a_4 or a_5, so there are 6 choices for each. Now consider $2a_2 + 2a_4 = 0$. We can rewrite it as $2(a_2 + a_4) = 0$. Which implies that $a_2 + a_4 = 0$ or $a_2 + a_4 = 3$. Since a_4 is already determined, we have 2 choices for a_2. a_1 is completely determined by our choices for a_2, a_3, a_4 and a_5. In total, $Nul(V)$ has $6^3 2$ elements. So $|Col(V)| = |\mathbb{Z}_6^6|/|Nul(V)| = 6^6/(6^3 2) = 2^2 3^3$. Therefore there are $2^2 3^3$ functions that can be represented as polynomials over $\mathbb{Z}_6$.

4 Conclusion

Given any continuous function over the reals, we can approximate it using a polynomial function as closely as desired. If we consider functions over finite fields, using the Vandermonde matrix we proved that any function over a finite field can be represented as a polynomial over that finite field.

We can not use the same approach to prove that every function over a finite ring can be represented as a polynomial over that finite ring. We developed a method to count the number of functions over small rings of the form $\mathbb{Z}_n$ that can be represented as a polynomial over $\mathbb{Z}_n$. In fact, for rings $\mathbb{Z}_4$ and $\mathbb{Z}_6$ we found that there are many functions that can not be represented as a polynomial over $\mathbb{Z}_4$ or $\mathbb{Z}_6$. This raises some further questions. If not every function can be represented as a polynomial over that ring, how many functions can be for any given ring? In which rings is it possible to represent every function over the ring as a polynomial over that ring? Is there a systematic way to count the number of functions that can be represented as a polynomial over generic rings? The answers to these questions might have relevance to certain problems in symbolic dynamics which depend on the solvability of matrices over rings[3].

References

[1] W. Rudin, *Principles of Mathematical Analysis*, McGraw-Hill, 1976. 159-160.

[2] R. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 2013. 37.

[3] W. Ching, Linear Equations over Commutative Rings, *Linear Algebra and Its Applications* 18 (1977), 257-266.