**Polynomial Functions in Fields of Countable Size**

*Abstract*

This paper is a simple proof that shows for any field of countable size, all possible functions can be represented as polynomials with the highest possible degree being one less than the size of the field.

*Proof*

Firstly, given a field **F** of size *w*, there are exactly *ww* possible functions *f*: **F** 🡪 **F**. This is easily calculable. For every possible input x (of which there a *w*), there are exactly *w* possible outputs, thus *ww*.

Second of all, the amount of polynomials in the field of which the highest degree is *w-1* is exactly *ww*. Again, this is easy enough to show. The polynomial *p(x)* can be represented in the following way:

Where all *ai* ∈ **F**.

Since there are exactly *w* terms, and each of which has exactly *w* possible coefficients, then there are exactly *ww* polynomials.

Now to show that all the possible functions *f*: **F** 🡪 **F** can be mapped to a polynomial, one must simply show that all polynomials give a different output from all the others, such that each one has its own outputs, unique to that polynomial. This will show that the polynomials will cover all the possible functions since they will map one to one (injective) (all are unique solutions to a given set of outputs of the function) and since they are the same size, bijective (and thus also surjective).

Assume not, assume two different polynomials are equivalent. This can be represented in the following manner:

As per the Fundamental Theorem of Algebra (IDK IF IT HOLDS for countable fields), any polynomial of degree *w-1* will have at most *w-1* roots. However since *x* ∈ **F**, there are exactly *w* values *x* can take, the function above has *w* roots, which is a contradiction, and thus they cannot be equal unless and the terms *(ai - bi) = 0*, which would imply they are the same polynomial.

Thus there are *ww* different polynomials, and there are exactly *ww* different functions. Therefore every function must be assigned a unique polynomial, and vice versa, every polynomial must be assigned a unique function.

This means that all functions can be represented by polynomials (in fields of countable size), which implies that anything proven to be true to all polynomials of degree *w-1* in a field of size *w* must hold true for all functions possible in that field.

For example, in a Galois Field of 5, the function *2x* can be represented as a polynomial of form ax4+bx3+cx2+dx+e

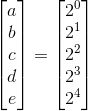
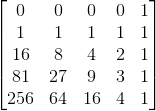
|  |  |
| --- | --- |
| X | 2x |
| 0 | 1 |
| 1 | 2 |
| 2 | 4 |
| 3 | 3 |
| 4 | 1 |

Knowing the maximal degree of the polynomial is 4, we get:

If x=0: a0+b0+c0+d0+e = 1; e=1

If x=1: a1+b1+c1+d1+e = 2

So on and so forth, resulting in the following matrix equation:



Thus the resulting coefficients are 1/4, -13/6, 21/4,-7/3, 1, respectively. However, these are not properly in the field. The 1/4 for example signifies the number that multiplied by 4 gives 1, which in this field is 4. For -13/6, we first perform the modulus operation on the numerator, giving us 2/6, we then perform modulus on the denominator, giving us 2/1, which means the number that multiplied by 1 gives 2, which is 2. The same follows for the others, giving 4, 1, 1 respectively. Thus the polynomial is:

|  |  |
| --- | --- |
| X | 4x4+2x3+4x2+x+1 |
| 0 | 1 |
| 1 | 2 |
| 2 | 4 |
| 3 | 3 |
| 4 | 1 |

Thus all the properties of polynomials apply likewise to the function *2x*.

The methodology of finding the polynomial can further be generalized to:

Where for any field, the matrix is the same, thus its inverse is also the same regardless of the desired outputs. This shows that if an inverse is computed, it can be used to quickly find any polynomial given the desired outputs.

Another way to prove what this paper proves is by showing that the above matrix is always invertible, meaning it is singular, and thus no two sets of coefficients can give the same function outputs.

<https://en.wikipedia.org/wiki/Vandermonde_matrix>