

A Linear Representation for Functions on Finite Sets

Roman Bacik
Vancouver, Canada

October 31, 2025

Abstract

We demonstrate that any function f from a finite set Y to itself can be represented linearly. Specifically, we prove the existence of an injective map j from Y into a modular ring $\mathbb{Z}/m\mathbb{Z}$ and a constant $a \in \mathbb{Z}/m\mathbb{Z}$ such that $j(f(y)) = a \cdot j(y)$ in $\mathbb{Z}/m\mathbb{Z}$ holds for all $y \in Y$. This result is established by analyzing the algebraic properties of the adjugate of the characteristic matrix associated with the function's digraph. The proof is constructive, providing a method for finding the embedding j , the modulus m , and the linear multiplier a .

Keywords: Functional graph, Linear representation, Adjugate matrix, Characteristic polynomial, Finite functions.

1 Introduction

Functions on finite sets are fundamental objects in discrete mathematics, combinatorics, and theoretical computer science. The structure of such a function $f : Y \rightarrow Y$ is completely described by its functional graph (or functional digraph), a directed graph where a unique edge emanates from each vertex y to its image $f(y)$. While these functions can exhibit complex and seemingly chaotic behavior, a central goal in mathematics is to find alternative representations that reveal underlying algebraic structure.

This article establishes that any such function becomes linear after a suitable embedding. We show that for any function f on a finite set, one can find an injective map j from the set into a ring of integers modulo m such that the action of f corresponds to multiplication by a constant a . That is for all $y \in Y$: $j(f(y)) = a \cdot j(y)$ in $\mathbb{Z}/m\mathbb{Z}$ and hence the following diagram commutes:

$$\begin{array}{ccc} Y & \xrightarrow{f} & Y \\ j \downarrow & & \downarrow j \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{a} & \mathbb{Z}/m\mathbb{Z} \end{array}$$

This result bridges the gap between arbitrary discrete maps and structured linear systems. Without loss of generality, we can identify elements of the finite set Y of size n with the set $\{0, 1, \dots, n-1\}$, which are elements of $\mathbb{Z}/n\mathbb{Z}$. The full formal proof of this result is in [5].

2 Main Results

Definition 2.1 (Adjacency Matrix of a Function). Let $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ be any function. The function f is represented by an $n \times n$ adjacency matrix $A = A_f$, where the entry $a_{ij} = \delta_{f(i),j}$ and

$\delta_{i,j}$ is the Kronecker delta. With this convention, each row of A contains exactly one non-zero entry.

Lemma 2.2. *Let $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ be any function and $A = A_f$ be the adjacency matrix of the function f . Then for all $i \in \{0, 1, \dots, n-1\}$ and $y \in \mathbb{Z}^n$*

$$(Ay)_i = y_{f(i)}.$$

Proof. The proof follows from the Definition 2.1.

$$(Ay)_i = \sum_{j=0}^{n-1} a_{ij}y_j = \sum_{j=0}^{n-1} \delta_{f(i),j}y_j = y_{f(i)}$$

□

Lemma 2.3. *Let $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ be any function and $A = A_f$ be the adjacency matrix of the function f . Let $v \in \mathbb{Z}^n$, $y = \text{adj}(xI - A)v$ and $m = \det(xI - A)$. Then for all $i \in \{0, 1, \dots, n-1\}$*

$$y_{f(i)} = xy_i - mv_i.$$

Proof. For adjugate matrix we have identity $(xI - A) \text{adj}(xI - A) = \det(xI - A)I$. Therefore,

$$mv = \det(xI - A)v = (xI - A) \text{adj}(xI - A)v = (xI - A)y = xy - Ay.$$

The final equality follows from the Lemma 2.2.

□

Lemma 2.4. *Let M be an $n \times n$ matrix with polynomial entries $m_{ij} \in \mathbb{Z}[x]$. Then*

$$\deg(\det(M)) \leq \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \deg(m_{ij}).$$

Proof. The determinant is a sum over permutations σ of products $\prod_{i=0}^{n-1} m_{\sigma(i),i}$. Each product has degree at most $\sum_{i=0}^{n-1} \deg(m_{\sigma(i),i})$. Since a single element of a sum is at most the whole sum (when all terms are non-negative), this is bounded by $\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \deg(m_{ij})$. The degree of a sum is at most the maximum degree of its summands.

□

Lemma 2.5. *Let A be an $n \times n$ matrix with integer entries. The characteristic matrix $\chi_A(x) = xI - A$ has determinant equal to the characteristic polynomial:*

$$\det(\chi_A(x)) = \det(xI - A)$$

For all $n \in \mathbb{N}$, this polynomial is monic of degree n .

Proof. This follows from the standard properties of the characteristic polynomial.

□

Lemma 2.6. *Let A be an $n \times n$ matrix with integer entries and $\chi_A(x) = xI - A$ be its characteristic matrix. For $i \neq j$, the (i, j) entry of $\text{adj}(\chi_A(x))$ has degree at most $n - 2$.*

Proof. The adjugate entry $\text{adj}(\chi_A(x))_{ij}$ equals the determinant of the characteristic matrix with row j and column i removed from $\chi_A(x)$.

This submatrix has diagonal entries from $\chi_A(x)$ except at diagonal positions i and j (which are deleted). Since $\chi_A(x)$ has diagonal entries of degree 1 (from xI) and off-diagonal entries of degree 0 (from $-A$), the submatrix has exactly $n - 2$ diagonal entries of degree 1 and all other entries of degree 0.

By Lemma 2.4, the determinant has degree at most $n - 2$.

□

Lemma 2.7. Let $M = M(x) = \text{adj}(xI - A)$ be the adjugate of the characteristic matrix $xI - A$. Then the matrix entries $m_{ij} = p_{ij}(x)$ are polynomials in x for all $i, j \in \{0, 1, \dots, n-1\}$ such that

- $p_{ii}(x)$ is monic of degree $n-1$ for all $i \in \{0, 1, \dots, n-1\}$ and
- $p_{ij}(x)$ has degree at most $n-2$ for all $i \neq j \in \{0, 1, \dots, n-1\}$.

Proof. The diagonal entries of $\text{adj}(xI - A)$ are characteristic polynomials of $(n-1) \times (n-1)$ submatrices, hence monic of degree $n-1$ by Lemma 2.5.

The off-diagonal case follows directly from Lemma 2.6. $\square$

Definition 2.8. For a polynomial $p(x) = \sum_{i=0}^d p_i x^i \in \mathbb{Z}[x]$, we define the coefficients bound:

$$|p| = \sum_{i=0}^d |p_i|$$

Lemma 2.9. If $p \in \mathbb{Z}[x]$ has positive leading coefficient, then for all integers $n \geq |p|$, we have $n > 0$ and $p(n) > 0$.

Proof. Lemma is trivially true for $d = 0$ so we can assume $d \geq 1$. Write $p(n) = an^d + r(n)$ where $a \geq 1$ is the leading coefficient of p , $d = \deg(p)$, and $\deg(r) < d$. For $n \geq |p|$:

$$n \geq |p| \geq a \geq 1 > 0.$$

Since $n \geq 1$, we have $|r(n)| \leq Bn^{d-1}$ where $B = |p| - a$. Therefore,

$$p(n) = an^d + r(n) \geq an^d - Bn^{d-1} = n^{d-1}(an - B) \geq (a|p| - B) \geq |p| - B = a \geq 1 > 0.$$

$\square$

Lemma 2.10. Let $M = (m_{ij}) = M(x) = \text{adj}(xI - A)$ be the adjugate of the characteristic matrix $xI - A$. Let $v = (1, 2, \dots, n)^T$ and $m = m(x) = \det(xI - A)$. Then for sufficiently large integer x :

$$0 < y_0 < y_1 < \dots < y_{n-1} < m$$

Proof. The proof follows from Lemma 2.7 and Lemma 2.9. Let $y = Mv$. Then $y_i = \sum_{k=0}^{n-1} m_{ik}(k+1)$.

For each entry y_i , we express it as evaluation of a polynomial $p_i(x) = \sum_{k=0}^{n-1} m_{ik}(x)(k+1) \in \mathbb{Z}[x]$. By Lemma 2.7, the diagonal entry m_{ii} is monic of degree $n-1$, while off-diagonal entries m_{ik} (for $k \neq i$) have degree at most $n-2$. Therefore, the coefficient of x^{n-1} in p_i is $i+1 > 0$ (dominated by the $m_{ii}(i+1)$ term).

For the difference $p_j - p_i$ with $j > i$, the leading term comes from $(m_{jj}(j+1) - m_{ii}(i+1))$. Since both m_{jj} and m_{ii} are monic of degree $n-1$, the leading coefficient of $p_j - p_i$ is $(j+1) - (i+1) = j - i > 0$.

Similarly, for $p_m(x) = \det(xI - A) - p_i(x)$, since $\det(xI - A)$ is monic of degree n (by Lemma 2.5) and p_i has degree at most $n-1$, the leading coefficient is 1.

Since $p_0(x)$ has leading coefficient $0+1 = 1 > 0$, we have $y_0 > 0$ for sufficiently large x .

Applying Lemma 2.9 to these polynomials with positive leading coefficients gives the existence of x_0 such that all required inequalities hold for $x > x_0$. $\square$

Definition 2.11 (Linear Representation). Let $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ be any function. A linear representation of f is an injective function $j : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ such that for all $i \in \{0, 1, \dots, n-1\}$,

$$j(f(i)) = a \cdot j(i)$$

in $\mathbb{Z}/m\mathbb{Z}$, where m is a positive integer and a is a constant from $\mathbb{Z}/m\mathbb{Z}$ depending on f .

Theorem 2.12 (Main Theorem). *Any finite function $f : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ has a linear representation.*

Proof. Let us define $m = \det(xI - A)$, $a = x$ and $j(i) = y_i$ for $i \in \{0, 1, \dots, n-1\}$, where $y = Mv$ with $v = (1, 2, \dots, n)^T$. By Lemma 2.10, we can choose x large enough such that:

$$0 < y_0 < y_1 < \dots < y_{n-1} < m$$

Since m is monic of degree n , we can choose x such that $x < m(x)$. This shows that j is injective and $a \in \{0, 1, \dots, m-1\}$.

Lemma 2.3 shows that $y_{f(i)} = xy_i - mv_i$ and hence $y_{f(i)} \equiv xy_i \pmod{m}$.

Therefore, j is a linear representation of f with modulus m and constant a . $\square$

Examples

Example 2.13 (Quadratic Function in $\mathbb{Z}/3\mathbb{Z}$). Consider the function $f : \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$ defined by $f(x) = x^2$. This function maps:

$$\begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ 2 &\mapsto 4 \equiv 1 \pmod{3} \end{aligned}$$

Despite being a non-linear function, Theorem 2.12 guarantees that f has a linear representation.

The adjacency matrix is:

$$A_f = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

The characteristic matrix is:

$$xI - A_f = \begin{pmatrix} x-1 & 0 & 0 \\ 0 & x-1 & 0 \\ 0 & -1 & x \end{pmatrix}$$

The characteristic polynomial is:

$$m = \det(xI - A_f) = (x-1)^2 \cdot x = x^3 - 2x^2 + x$$

The adjugate matrix is:

$$\text{adj}(xI - A_f) = \begin{pmatrix} x(x-1) & 0 & 0 \\ 0 & x(x-1) & 0 \\ 0 & (x-1) & (x-1)^2 \end{pmatrix}$$

Using vector $v = (1, 2, 3)^T$, we get:

$$y = \text{adj}(xI - A_f) \cdot v = \begin{pmatrix} x(x-1) \cdot 1 \\ x(x-1) \cdot 2 \\ (x-1) \cdot 2 + (x-1)^2 \cdot 3 \end{pmatrix} = \begin{pmatrix} x^2 - x \\ 2x^2 - 2x \\ (x-1)(3x-1) \end{pmatrix} = \begin{pmatrix} x^2 - x \\ 2x^2 - 2x \\ 3x^2 - 4x + 1 \end{pmatrix}$$

For $x = 4$, we compute:

$$\begin{aligned} y_0 &= 4^2 - 4 = 16 - 4 = 12 \\ y_1 &= 2(4^2) - 2(4) = 32 - 8 = 24 \\ y_2 &= 3(4^2) - 4(4) + 1 = 48 - 16 + 1 = 33 \\ m &= 4^3 - 2(4^2) + 4 = 64 - 32 + 4 = 36 \end{aligned}$$

The injection $j : \mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{Z}/36\mathbb{Z}$ is defined by $j(i) = y_i$:

$$j(0) = 12, \quad j(1) = 24, \quad j(2) = 33$$

These values are strictly increasing and bounded by $m = 36$, so j is injective.

We verify the linear representation property using Lemma 2.3.

The lemma states that $y_{f(i)} = xy_i - m \cdot v_i$, which we can rewrite as:

$$j(f(i)) \equiv xj(i) \pmod{m}.$$

Verification:

$$\begin{aligned} j(f(0)) &= j(0) = 12 \equiv 4 \cdot 12 - 36 \cdot 1 = 48 - 36 = 12 = 4 \cdot j(0) \pmod{36} \quad \checkmark \\ j(f(1)) &= j(1) = 24 \equiv 4 \cdot 24 - 36 \cdot 2 = 96 - 72 = 24 = 4 \cdot j(1) \pmod{36} \quad \checkmark \\ j(f(2)) &= j(1) = 24 \equiv 4 \cdot 33 - 36 \cdot 3 = 132 - 108 = 24 = 4 \cdot j(2) \pmod{36} \quad \checkmark \end{aligned}$$

Thus $j(f(i)) \equiv 4 \cdot j(i) \pmod{36}$ for all $i \in \mathbb{Z}/3\mathbb{Z}$, confirming the quadratic function $f(x) = x^2$ has a linear representation with modulus $m = 36$ and multiplier $a = 4$.

3 Discussion and Context

The representation of arbitrary functions in structured algebraic forms is a recurring theme. Our result provides one such representation, which can be compared to others.

- **Polynomial Interpolation:** Any function over a finite field or ring can be represented by a polynomial (e.g., via Lagrange interpolation). Our result is distinct in that it achieves a representation as a simple linear map, $z \mapsto az$, at the cost of requiring an embedding j into the ring rather than working on the original set's labels directly.
- **Linear Feedback Shift Registers (LFSRs):** In engineering and cryptography, functions on vector spaces over finite fields are often chosen to be linear for ease of implementation and analysis. Our result generalizes this principle, showing that *any* function on an arbitrary finite set can be viewed linearly in a suitable module.
- **Graph Theory:** In Graph Theory our results shows that any functional digraph is a subgraph of a functional graph of a linear map.

While the modulus m can be large, making this construction primarily of theoretical interest, it provides the powerful knowledge that every finite function possesses a hidden linear structure.

References

- [1] M. Drmota and B. Gittenberger. *The distribution of nodes of given degree in random trees*. Journal of Graph Theory, 31(3):227–253, 1997.
- [2] P. Flajolet and A. M. Odlyzko. *Random mapping statistics*. In Advances in Cryptology—EUROCRYPT '89, pages 329–354. Springer, 1990.
- [3] B. Harris. *Probability distributions related to random mappings*. The Annals of Mathematical Statistics, 31(4):1045–1062, 1960.
- [4] R. A. Horn and C. R. Johnson. *Matrix Analysis*, 2nd edition. Cambridge University Press, 2012.
- [5] R. Bacik. *FinLin*. <https://github.com/roman3017/FinLin>.