Exact Orbit Enumeration for the Prefix-XOR Operator

A Closed-Form Solution for OEIS Sequence A007886

Laurent Neau

January 8, 2026

Abstract

We provide a complete algebraic proof for the closed-form formula enumerating the cycles induced by the Prefix-XOR operator on $\mathbb{F}_2^n$. This resolves the orbit counting problem for OEIS sequence A007886. The proof relies on the isomorphism between $\mathbb{F}_2^n$ and the polynomial quotient ring $\mathbb{F}_2[t]/(t^n)$, the properties of the Frobenius endomorphism in characteristic 2, and Möbius inversion on the poset of powers of 2.

1 Main Result

Let $a(n)$ denote the number of cycles of the Prefix-XOR operator (equivalent to the Gray code permutation) on the vector space $\mathbb{F}_2^n$.

Theorem 1. *Define $F_j := 2^{\min(n,2^j)}$ for $j \geq 0$ and set $F_{-1} := 0$. Then*

$$a(n) = \sum_{j=0}^{\lceil \log_2 n \rceil} \frac{F_j - F_{j-1}}{2^j}.$$

Equivalently,

$$a(n) = \sum_{j=0}^{\lceil \log_2 n \rceil} \frac{2^{\min(n,2^j)} - 2^{\min(n,2^{j-1})}}{2^j},$$

with the convention $F_{-1} = 0$.

2 Definitions and Algebraic Setup

Definition 1 (Prefix-XOR Operator)**.** Let $V = \mathbb{F}_2^n$. The Prefix-XOR operator $I : V \to V$ maps a vector $x = (x_0, \ldots, x_{n-1})$ to $y = (y_0, \ldots, y_{n-1})$ where:

$$y_k = \sum_{i=0}^{k} x_i \pmod 2.$$

In matrix form, I is the $n \times n$ lower triangular matrix of all ones.

Lemma 1 (Ring Isomorphism)**.** *The vector space V is isomorphic to the quotient ring $R = \mathbb{F}_2[t]/(t^n)$ via the map*

$$\phi : (x_0, \ldots, x_{n-1}) \longmapsto \sum_{i=0}^{n-1} x_i t^i.$$

Under this isomorphism, the operator I corresponds to multiplication by $\alpha = (1+t)^{-1}$ in R.

Proof. Let $P(t) = \sum x_i t^i$. Multiplication by $(1+t)$ yields

$$(1+t)P(t) = \sum_{i=0}^{n-1} (x_i + x_{i-1}) t^i$$

(with $x_{-1} = 0$), which is the adjacent-difference operator and hence the inverse of the prefix-sum operation. Therefore the prefix-sum operation is given by multiplication by $(1+t)^{-1}$ in R. Note that $(1+t)$ is invertible in R because its constant term is 1 (a unit in $\mathbb{F}_2$) and t is nilpotent. Explicitly one has the finite geometric expansion

$$(1+t)^{-1} = \sum_{m=0}^{n-1} t^m \qquad \text{in } R,$$

since $t^n = 0$. □

3 Fixed Point Enumeration

We determine the number of fixed points of the iterated operator I^{2^k}.

Proposition 1. *Let $F_k = |\operatorname{Fix}(I^{2^k})|$. Then:*

$$F_k = 2^{\min(n, 2^k)}.$$

Proof. The operator I^{2^k} corresponds to multiplication by $\alpha^{2^k} = ((1+t)^{-1})^{2^k}$ in R. Recall that over $\mathbb{F}_2$ the Frobenius endomorphism satisfies $(a+b)^{2^k} = a^{2^k} + b^{2^k}$ for all a, b, hence

$$(1+t)^{2^k} = 1 + t^{2^k}.$$

Therefore $\alpha^{2^k} = (1+t^{2^k})^{-1}$. Since $t^n = 0$ in R, the inverse can be written as the finite geometric series

$$(1+t^{2^k})^{-1} = \sum_{m=0}^{\lfloor (n-1)/2^k \rfloor} (t^{2^k})^m.$$

A polynomial $x(t) \in R$ is fixed by I^{2^k} iff

$$\alpha^{2^k} x(t) = x(t) \iff (1+t^{2^k})^{-1} x(t) = x(t).$$

Multiplying by $(1+t^{2^k})$ yields $t^{2^k} x(t) = 0$. Thus the fixed points are exactly the kernel of the multiplication-by-t^{2^k} map in R.

For an integer $m \geq 0$, $t^m P(t) = 0$ in R iff $t^m P(t)$ is divisible by t^n in $\mathbb{F}_2[t]$, i.e. iff $P(t)$ is divisible by t^{n-m} when $m < n$. Consequently the kernel is the ideal $\langle t^{n-m} \rangle$ with basis

$$\{t^{n-m}, t^{n-m+1}, \ldots, t^{n-1}\},$$

of dimension m. If $m \geq n$ then $t^m = 0$ in R and the kernel is the whole space of dimension n. Applying this to $m = 2^k$ gives

$$\dim \ker(\times t^{2^k}) = \min(n, 2^k),$$

so

$$F_k = 2^{\min(n, 2^k)}.$$

□

4 Counting Cycles via Möbius Inversion

Lemma 2. *The operator I on $\mathbb{F}_2^n$ is a linear permutation. The length of every cycle is a power of 2.*

Proof. Let 2^k be the smallest power of two such that $2^k \geq n$. Since $t^n = 0$ in R it follows that $t^{2^k} = 0$, hence $1 + t^{2^k} = 1$ and $I^{2^k} = \mathrm{Id}$. The order of I is therefore a power of 2, and by Lagrange's theorem every orbit size divides this order; thus every cycle length is a power of 2. □

Proof of Theorem 1. Let C_j be the number of cycles of length exactly 2^j. For $k \geq 0$ the set of fixed points of I^{2^k} is the disjoint union of all cycles whose lengths divide 2^k, hence

$$F_k = \sum_{j=0}^{k} 2^j C_j.$$

On the chain of powers of two, Möbius inversion reduces to successive differences. For $k \geq 1$ we have

$$F_k - F_{k-1} = 2^k C_k,$$

so

$$C_k = \frac{F_k - F_{k-1}}{2^k} \quad (k \geq 1),$$

and with the convention $F_{-1} = 0$ we also obtain $C_0 = F_0$. Summing all C_j up to the smallest j with $2^j \geq n$ (i.e. $j = \lceil \log_2 n \rceil$) yields the formula of Theorem 1, since $F_j = 2^{\min(n, 2^j)}$. □

5 Connection to Gray Codes

Remark 1. The standard Gray code permutation G on $\mathbb{F}_2^n$ is defined by $G(x) = x \oplus (x \gg 1)$. The bit-reversal permutation R conjugates G to the Prefix-XOR operator I:

$$G = R^{-1} \circ I^{-1} \circ R.$$

Cycle structure is invariant under conjugation and inversion, so $a(n)$ also enumerates the cycles of the Gray code, matching OEIS sequence A007886. This equivalence is discussed, for example, in Culberson [2] and Oteo–Ros [3].

References

[1] OEIS Foundation Inc. (2025), The On-Line Encyclopedia of Integer Sequences, Sequence A007886, https://oeis.org/A007886

[2] J. Culberson, "Mutation-Crossover Isomorphisms and the Construction of Discriminating Functions", *Evolutionary Computation* 2(3): 279–311, 1994

[3] J. A. Oteo and J. Ros, "A Fractal Set from the Binary Reflected Gray Code", *J. Phys. A: Math. Gen.* 38 (2005) 8935–8949

[4] G. Langlet, "L'intégrale de parité", *Bulletin de l'APL*, 1992. , https://integrale2parite.blogspot.com/