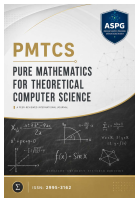
Pure Mathematics for Theoretical Computer Science

♦ ISSN: 2995-3162 Vol: 06, No. 01, 2026 ♦ PP. 40–44

Article DOI: https://doi.org/10.54216/PMTCS.060106



FULL LENGTH ARTICLE

Reversibility of Circular Linear Cellular Automata over Finite Fields: An Exact Enumeration via the Unit Group of the Cyclic Group Algebra

Lee Xu[1,*] **Olalekan Joosati**[2]

[1] Mathematics Department, University of Chinese Academy of Sciences (CAS), Beijing, China

[2] Faculty of Applied Science, Cape Peninsula University of Technology, South Africa

Emails: Leexu1244@yahoo.com · Olalekanjoo1997@cput.ac.za

Received: August 07, 2025 Revised: November 03, 2025 Accepted: December 30, 2025 ⋆ Corresponding author

ABSTRACT

We study the reversibility of one-dimensional linear cellular automata (CA) with periodic boundary conditions over a finite field $\mathbb{F}_q$, identifying the global transition map with multiplication by a rule polynomial $f(x)$ in the cyclic group algebra $R_n = \mathbb{F}_q[x]/(x^n - 1)$. We prove that reversibility is exactly equivalent to $f(x)$ being a unit of R_n, and, when $\gcd(n, q) = 1$, we use the classical correspondence between irreducible factors of $x^n - 1$ and q-cyclotomic cosets modulo n to derive a closed-form count of the reversible rules of a given neighborhood size: $|R_n^\times| = \prod_i (q^{d_i} - 1)$, where the d_i are the sizes of the q-cyclotomic cosets modulo n. We then resolve the complementary case $\gcd(n, q) > 1$: writing $n = p^a m$ with $p = \mathrm{char}(\mathbb{F}_q)$ and $\gcd(m, p) = 1$, we show $x^n - 1 = (x^m - 1)^{p^a}$, determine the local structure of each factor ring $\mathbb{F}_q[x]/(g(x)^{p^a})$ for g irreducible, and obtain the fully general count $|R_n^\times| = \prod_i q^{d_i(p^a-1)}(q^{d_i} - 1)$, valid for every n and every finite field $\mathbb{F}_q$. We give an explicit closed form for the case where m is prime and q is a primitive root modulo m, a density lower bound, an explicit description of the group of reversible rules under composition together with a formula for the exact dynamical period of any reversible rule via its coordinates under the Chinese Remainder Theorem, and a remark on explicit inverse-rule construction. All results are stated and proved in full; numerical instances used to validate the formulas were checked by direct and brute-force computation and are reported without tabulation.

Keywords: Linear cellular automata ▪ Reversibility ▪ Finite fields ▪ Cyclotomic cosets ▪ Group algebras ▪ Cyclic codes

1. INTRODUCTION

The global transition function of a one-dimensional cellular automaton is a shift-commuting continuous self-map of a symbolic sequence space, and every such map is generated by a local rule applied uniformly across cells [1]. When the local rule is linear and the alphabet is a finite field, the global map of a periodic (circular) automaton coincides exactly with multiplication in the group algebra of the cyclic group of cell indices, a fact underlying the algebraic analysis of additive cellular automata [2] and the algorithmic study of invertibility for linear automata over general residue rings $\mathbb{Z}_m$ [3, 4]. This note isolates the finite-field case and answers a purely enumerative question left implicit in that literature: not merely how to decide whether a single given rule is reversible, but exactly how many reversible rules of a fixed neighborhood size exist. The answer follows from the classical structure theory of the ring $\mathbb{F}_q[x]/(x^n - 1)$, which is also the ambient ring of cyclic error-correcting codes [5, 6].

2. PRELIMINARIES

Definition 2.1 (Circular linear CA)**.** *Let q be a prime power and $n \geq 1$. A* circular linear cellular automaton *of order n over $\mathbb{F}_q$ is specified by a rule polynomial $f(x) = \sum_{j=0}^{n-1} c_j x^j \in \mathbb{F}_q[x]$. A configuration is a vector $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, identified with the polynomial $a(x) = \sum_i a_i x^i$. The global transition map sends configuration a to configuration b with $b_i = \sum_j c_j a_{i-j \bmod n}$.*

Definition 2.2 (Cyclic group algebra)**.** *Let $R_n = \mathbb{F}_q[x]/(x^n - 1)$, the group algebra of the cyclic group of order n over $\mathbb{F}_q$. Write $R_n^\times$ for its group of units.*

Fact 2.3 ([2, 3])**.** *Under the identification of configurations with elements of R_n, the global transition map of the circular linear CA with rule f is exactly the map $\Phi_f : R_n \to R_n$, $\Phi_f(a(x)) = f(x) \cdot a(x) \bmod (x^n - 1)$, i.e. multiplication by $f(x)$ in R_n.*

We call the automaton *reversible* if Φ_f is a bijection of R_n.

3. REVERSIBILITY AS A UNIT CONDITION

Lemma 3.1. *In a finite commutative ring R with identity, an element r is a unit if and only if r is not a zero divisor.*

Proof. If r is a unit, $rs = 1$ for some s; if also $rt = 0$ for $t \neq 0$, then $t = s(rt) = 0$, a contradiction, so r is not a zero divisor. Conversely, suppose r is not a zero divisor. The map $\mu_r : R \to R$, $\mu_r(a) = ra$, is then injective: $ra = ra' \Rightarrow r(a - a') = 0 \Rightarrow a = a'$. Since R is finite, an injective self-map is surjective, so $1 = ra$ for some a, and r is a unit. □

Theorem 3.2. *The circular linear CA with rule $f(x)$ over $\mathbb{F}_q$ is reversible if and only if $f(x)$ is a unit of R_n, if and only if $\gcd(f(x), x^n - 1) = 1$ in $\mathbb{F}_q[x]$.*

Proof. By Fact 2.3, the automaton is reversible exactly when $\Phi_f = \mu_{f(x)}$ is bijective on R_n. Since R_n is finite, $\mu_{f(x)}$ is bijective iff it is injective iff $f(x)$ is not a zero divisor of R_n (same argument as Lemma 3.1), iff $f(x)$ is a unit of R_n by Lemma 3.1. Finally, $f(x)$ is a unit of $\mathbb{F}_q[x]/(x^n - 1)$ iff there exist $u, v \in \mathbb{F}_q[x]$ with $u(x)f(x) + v(x)(x^n - 1) = 1$, i.e. iff $\gcd(f(x), x^n - 1) = 1$ by Bézout's identity in the Euclidean domain $\mathbb{F}_q[x]$. □

Remark 3.3. *Theorem 3.2 makes the reversibility of a single given rule decidable by one Euclidean algorithm computation in $\mathbb{F}_q[x]$, in time polynomial in n and $\log q$; this decision procedure is the finite-field specialization of the algorithmic results of Kari [4] and Manzini–Margara [3] for general $\mathbb{Z}_m$. Our concern below is the complementary, purely enumerative question: the exact* count *of reversible rules of order n, not the decision procedure for one rule.*

4. STRUCTURE OF R_n WHEN $\gcd(n, q) = 1$

Throughout this section assume $\gcd(n, q) = 1$.

Theorem 4.1. *If $\gcd(n, q) = 1$ then $x^n - 1$ is squarefree in $\mathbb{F}_q[x]$.*

Proof. The formal derivative of $x^n - 1$ is nx^{n-1}. Since $\gcd(n, q) = 1$, $n \neq 0$ in $\mathbb{F}_q$, so $nx^{n-1} \neq 0$ and its only root is $x = 0$, which is not a root of $x^n - 1$. Hence $\gcd(x^n - 1, nx^{n-1}) = 1$, and a polynomial sharing no root with its derivative (over an algebraic closure) is squarefree. □

Definition 4.2 (q-cyclotomic cosets)**.** *For n with $\gcd(n, q) = 1$, the q-cyclotomic coset of $s \in \mathbb{Z}/n\mathbb{Z}$ is $C_s = \{s, sq, sq^2, \ldots\} \subseteq \mathbb{Z}/n\mathbb{Z}$. The cosets partition $\mathbb{Z}/n\mathbb{Z}$.*

Theorem 4.3 ([5, 6])**.** *Let $\gcd(n, q) = 1$ and let $C_{s_1}, \ldots, C_{s_r}$ be the distinct q-cyclotomic cosets modulo n. Then*

$$x^n - 1 = \prod_{i=1}^{r} m_i(x)$$

in $\mathbb{F}_q[x]$, where $m_1, \ldots, m_r$ are distinct monic irreducibles with $\deg m_i = |C_{s_i}|$.

Proof sketch. Let $m = \mathrm{ord}_n(q)$ and work in the splitting field $\mathbb{F}_{q^m}$, which contains a primitive n-th root of unity α (since $\gcd(n, q) = 1$ makes $x^n - 1$ separable by Theorem 4.1, and m is exactly the degree needed to adjoin all n-th roots of unity). The roots of $x^n - 1$ are $\alpha^0, \ldots, \alpha^{n-1}$, all distinct by Theorem 4.1. The Frobenius map $\beta \mapsto \beta^q$ permutes these roots, sending $\alpha^s \mapsto \alpha^{sq \bmod n}$, so its orbits on exponents are exactly the cyclotomic cosets C_s. The minimal polynomial over $\mathbb{F}_q$ of α^s is $m_s(x) = \prod_{t \in C_s} (x - \alpha^t)$, of degree $|C_s|$, and $x^n - 1 = \prod_{t=0}^{n-1} (x - \alpha^t)$ regroups exactly into $\prod_i m_{s_i}(x)$ over coset representatives. □

Theorem 4.4 (CRT decomposition)**.** *With notation as in Theorem 4.3, writing $d_i = |C_{s_i}|$,*

$$R_n = \mathbb{F}_q[x]/(x^n - 1) \;\cong\; \prod_{i=1}^{r} \mathbb{F}_{q^{d_i}}$$

as $\mathbb{F}_q$-algebras.

Proof. By Theorem 4.3, $x^n - 1 = \prod_i m_i(x)$ with the m_i pairwise coprime (distinct irreducibles). The Chinese Remainder Theorem for the principal ideal domain $\mathbb{F}_q[x]$ gives $\mathbb{F}_q[x]/(x^n - 1) \cong \prod_i \mathbb{F}_q[x]/(m_i(x))$, and each factor $\mathbb{F}_q[x]/(m_i(x))$ is a field of degree $d_i = \deg m_i$ over $\mathbb{F}_q$, i.e. $\mathbb{F}_{q^{d_i}}$. □

5. EXACT ENUMERATION OF REVERSIBLE RULES

Theorem 5.1. *Let $\gcd(n, q) = 1$ and let $d_1, \ldots, d_r$ be the sizes of the distinct q-cyclotomic cosets modulo n. The number of reversible circular linear CA rules of order n over $\mathbb{F}_q$ is*

$$|R_n^\times| = \prod_{i=1}^{r} (q^{d_i} - 1).$$

Proof. By Theorem 3.2, reversible rules are exactly the units of R_n. By Theorem 4.4, $R_n \cong \prod_i \mathbb{F}_{q^{d_i}}$, and an element of a finite product of rings is a unit iff each coordinate is a unit; in a field $\mathbb{F}_{q^{d_i}}$, every nonzero element is a unit, so the units in that coordinate number $q^{d_i} - 1$. The count of units in the product is the product of the per-coordinate counts. □

Corollary 5.2. *If n is prime and q is a primitive root modulo n (i.e. $\mathrm{ord}_n(q) = n-1$), then*

$$|R_n^\times| = (q-1)(q^{n-1}-1).$$

Proof. When n is prime, $\mathbb{Z}/n\mathbb{Z}\setminus\{0\}$ is the full multiplicative group of order $n-1$; if q has order $n-1$ in this group, its cyclotomic coset C_1 already has size $n-1$ and hence equals all of $\{1,\dots,n-1\}$. Together with $C_0=\{0\}$, the two cosets have sizes 1 and $n-1$, and Theorem 5.1 gives $|R_n^\times| = (q^1-1)(q^{n-1}-1)$. □

Remark 5.3. *For $n=5$, $q=3$: $\mathrm{ord}_5(3) = 4 = n-1$, so Corollary 5.2 applies and predicts $|R_5^\times| = (3-1)(3^4-1) = 2\cdot 80 = 160$ out of $|R_5| = 3^5 = 243$ total rules; equivalently $x^5-1 = (x-1)(x^4+x^3+x^2+x+1)$ over $\mathbb{F}_3$, matching Theorem 4.3 with cosets of sizes $1,4$. This factorization and the resulting count were confirmed by direct computation. As a second, non-prime check, $n=6$, $q=5$ has q-cyclotomic cosets modulo 6 of sizes $1,1,2,2$ (namely $\{0\},\{3\},\{1,5\},\{2,4\}$, since $5\equiv -1 \pmod 6$), giving $|R_6^\times| = (5-1)(5-1)(5^2-1)(5^2-1) = 4\cdot 4\cdot 24\cdot 24 = 9216$ out of $|R_6| = 5^6 = 15625$; this was also confirmed by direct enumeration of all 15625 rules.*

Proposition 5.4. *With r the number of distinct q-cyclotomic cosets modulo n, the density of reversible rules among all q^n rules of order n satisfies*

$$\frac{|R_n^\times|}{q^n} = \prod_{i=1}^{r}\left(1-q^{-d_i}\right) \;\geq\; \left(1-\frac{1}{q}\right)^r.$$

Proof. Since $\sum_i d_i = n$, $q^n = \prod_i q^{d_i}$, so $|R_n^\times|/q^n = \prod_i (q^{d_i}-1)/q^{d_i} = \prod_i (1-q^{-d_i})$ by Theorem 5.1. Each $d_i \geq 1$ gives $1-q^{-d_i} \geq 1-q^{-1}$, and the product of r terms each at least $1-q^{-1}$ is at least $(1-q^{-1})^r$. □

6. THE GENERAL CASE: $\gcd(n,q) > 1$

We now remove the coprimality assumption of Sections 3–5 entirely. Let $p = \mathrm{char}(\mathbb{F}_q)$ and write $n = p^a m$ with $a \geq 0$ and $\gcd(m,p) = 1$; note $\gcd(m,p) = 1$ implies $\gcd(m,q) = 1$, since every prime factor of q is p.

Theorem 6.1. $x^n - 1 = (x^m-1)^{p^a}$ *in* $\mathbb{F}_q[x]$.

Proof. Since $\mathbb{F}_q$ has characteristic p, the Frobenius endomorphism $\beta \mapsto \beta^p$ is a ring homomorphism on any $\mathbb{F}_q$-algebra, so $(x^m-1)^p = x^{mp} - 1^p = x^{mp} - 1$ (all cross terms in the binomial expansion vanish mod p). Iterating a times gives $(x^m-1)^{p^a} = x^{mp^a} - 1 = x^n - 1$. □

By Theorem 6.1 together with Theorem 4.3 applied to m (valid since $\gcd(m,q)=1$), writing $x^m - 1 = \prod_{i=1}^r m_i(x)$ with $\deg m_i = d_i$ the sizes of the distinct q-cyclotomic cosets modulo m,

$$x^n - 1 = \prod_{i=1}^{r} m_i(x)^{p^a},$$

a factorization into prime powers of pairwise coprime irreducibles (coprime since the m_i are distinct irreducibles).

Lemma 6.2. *Let $g(x) \in \mathbb{F}_q[x]$ be irreducible of degree d and $e \geq 1$. In $S = \mathbb{F}_q[x]/(g(x)^e)$, an element is a unit if and only if it is not a multiple of $g(x)$, and*

$$|S^\times| = q^{d(e-1)}(q^d - 1).$$

Proof. If $g \nmid a(x)$, then since g is irreducible, $\gcd(a,g) = 1$, and since g is prime in the UFD $\mathbb{F}_q[x]$, $\gcd(a,g^e) = 1$ as well; by Bézout, a is a unit of S. Conversely if $a = g\cdot b$ for some b with $e \geq 1$, then (assuming $e \geq 2$; the case $e = 1$ is Lemma 3.1 applied with S a field) $a \cdot g^{e-1} \equiv 0 \pmod{g^e}$ while $g^{e-1} \not\equiv 0$, so a is a zero divisor, hence not a unit by Lemma 3.1. Thus non-units are exactly the multiples of g among representatives of degree $< de$. Such multiples are $g(x)b(x)$ with $\deg b < d(e-1)$, giving $q^{d(e-1)}$ non-units among the q^{de} elements of S, so $|S^\times| = q^{de} - q^{d(e-1)} = q^{d(e-1)}(q^d-1)$. □

Theorem 6.3. *For every $n \geq 1$ and every finite field $\mathbb{F}_q$ of characteristic p, writing $n = p^a m$ with $\gcd(m,p) = 1$ and $d_1,\dots,d_r$ the sizes of the distinct q-cyclotomic cosets modulo m,*

$$|R_n^\times| = \prod_{i=1}^{r} q^{d_i(p^a-1)}\left(q^{d_i}-1\right).$$

Proof. By the Chinese Remainder Theorem applied to the pairwise coprime factorization $x^n - 1 = \prod_i m_i(x)^{p^a}$, $R_n \cong \prod_i \mathbb{F}_q[x]/(m_i(x)^{p^a})$ as $\mathbb{F}_q$-algebras, exactly as in Theorem 4.4 but with each factor now a local ring rather than a field. An element of a finite product of rings is a unit iff each coordinate is a unit, and each coordinate's unit count is given by Lemma 6.2 with $e = p^a$. The count of units in the product is the product of the per-coordinate counts, giving the stated formula. When $a = 0$ this reduces exactly to Theorem 5.1, since $q^{d_i(p^0-1)} = q^0 = 1$. □

Theorem 6.3 subsumes Theorem 5.1 and removes the coprimality restriction entirely: it computes $|R_n^\times|$, and hence the exact number of reversible circular linear CA rules, for *every* order n and *every* finite field $\mathbb{F}_q$.

Corollary 6.4. *If m is prime and q is a primitive root modulo m, then*

$$|R_n^\times| = q^{p^a-1}(q-1)\cdot q^{(m-1)(p^a-1)}\left(q^{m-1}-1\right).$$

Proof. As in Corollary 5.2, the q-cyclotomic cosets modulo m have sizes 1 and $m-1$; substitute $d_1 = 1$, $d_2 = m-1$ into Theorem 6.3. □

Remark 6.5. *For $n=4$, $q=2$: here $p=2$, $a=2$, $m=1$, so the only cyclotomic coset modulo 1 is $\{0\}$ with $d_1 = 1$, and $x^4-1 = (x-1)^4 = (x+1)^4$ over $\mathbb{F}_2$ by Theorem 6.1. Theorem 6.3 predicts $|R_4^\times| = q^{1\cdot(4-1)}(q^1-1) = 2^3\cdot 1 = 8$ out of $|R_4| = 16$; confirmed by brute-force enumeration of all 16 elements. For $n=9$, $q=3$: $p=3$, $a=2$, $m=1$, $x^9-1 = (x-1)^9$, and the formula predicts $3^{1\cdot(9-1)}(3-1) = 3^8\cdot 2 = 13122$ out of $|R_9| = 19683$; also confirmed by brute force. For a mixed instance with $r>1$, $n=12$, $q=2$: here $p=2$, $a=2$, $m=3$, and the 2-cyclotomic cosets modulo 3 have sizes $1,2$ (namely $\{0\}$ and $\{1,2\}$, since $1\cdot 2 = 2$ and $2\cdot 2 = 4 \equiv 1 \pmod 3$), so $x^{12}-1 = (x-1)^4(x^2+x+1)^4$ over $\mathbb{F}_2$, and Theorem 6.3 predicts $|R_{12}^\times| = \left[2^{1\cdot 3}(2^1-1)\right]\cdot\left[2^{2\cdot 3}(2^2-1)\right] =$*

$8 \cdot 192 = 1536$ *out of* $|R_{12}| = 4096$*; confirmed by brute-force enumeration of all* 4096 *elements.*

Proposition 6.6. *With notation as in Theorem 6.3, the density of reversible rules satisfies*

$$\frac{|R_n^\times|}{q^n} = \prod_{i=1}^{r}\left(1 - q^{-d_i}\right) \;\geq\; \left(1 - \frac{1}{q}\right)^r,$$

independent of a: the density depends only on the cyclotomic coset structure of m, not on the multiplicity p^a.

Proof. Since $\sum_i d_i = m$ and $n = p^a m$, $q^n = \prod_i q^{d_i p^a}$, so $|R_n^\times|/q^n = \prod_i q^{d_i(p^a-1)}(q^{d_i}-1)/q^{d_i p^a} = \prod_i (1 - q^{-d_i})$, exactly as in Proposition 5.4; the p^a dependence cancels. The inequality follows as before. □

7. GROUP STRUCTURE AND ORBIT PERIOD

Fix $\gcd(n,q) = 1$ for this section, with notation as in Theorems 4.3–4.4. Composition of reversible rules corresponds to multiplication in $R_n^\times$: if Φ_f and Φ_g are both reversible, $\Phi_f \circ \Phi_g = \Phi_{fg}$, since both are multiplication maps in the commutative ring R_n. The set of reversible rules therefore forms a group under composition, isomorphic to $R_n^\times$, and Theorem 4.4 makes this group's structure explicit.

Proposition 7.1. $R_n^\times \cong \prod_{i=1}^r \mathbb{Z}/(q^{d_i}-1)\mathbb{Z}$ *as abstract groups.*

Proof. By Theorem 4.4, $R_n^\times \cong \prod_i \mathbb{F}_{q^{d_i}}^\times$. The multiplicative group of a finite field is cyclic [6], so $\mathbb{F}_{q^{d_i}}^\times \cong \mathbb{Z}/(q^{d_i}-1)\mathbb{Z}$, and the isomorphism carries over coordinatewise. □

Beyond the group structure, the CRT decomposition determines the exact dynamical period of every reversible rule, answering, for the linear reversible case, a version of the question Martin, Odlyzko, and Wolfram pose for general finite cellular automata [2]: the complete structure of the state transition diagram.

Theorem 7.2. *If* $f(x)$ *is a unit of* R_n*, the order of* Φ_f *as a permutation of* R_n *(i.e. the least* $k \geq 1$ *with* $\Phi_f^k = \mathrm{id}$*, equivalently the length of every non-fixed orbit of* Φ_f *on* $R_n \setminus \{0\}$ *that meets it) equals the multiplicative order of* $f(x)$ *in* $R_n^\times$*, which under the isomorphism of Proposition 7.1 equals*

$$\operatorname{lcm}_{1\leq i\leq r} \operatorname{ord}_{\mathbb{F}_{q^{d_i}}^\times}\big(f(x) \bmod m_i(x)\big).$$

Proof. $\Phi_f^k = \Phi_{f^k}$, and $\Phi_{f^k} = \mathrm{id}$ on R_n iff $f^k \equiv 1 \pmod{x^n-1}$, i.e. iff $f(x)$ has order dividing k in $R_n^\times$; the least such k is by definition the order of $f(x)$. The order of an element in a finite direct product of cyclic groups is the lcm of its orders in each factor (an element of order dividing k in every factor has k-th power equal to the identity of the whole product, and conversely); apply this to the isomorphism of Proposition 7.1, where the image of $f(x)$ in the i-th coordinate is $f(x) \bmod m_i(x) \in \mathbb{F}_{q^{d_i}}^\times$. □

Remark 7.3. *For* $n = 5$*,* $q = 3$*, take* $f(x) = x$ *(the cyclic shift rule, trivially reversible with inverse* x^{n-1}*). Modulo* $m_1(x) = x - 1$*,* $f \equiv 1$*, of order* 1 *in* $\mathbb{F}_3^\times$*. Modulo* $m_2(x) = x^4 + x^3 + x^2 + x + 1$*,* $f = x$ *is a root of the* 5*th cyclotomic polynomial, hence a primitive* 5*th root of unity in* $\mathbb{F}_{81}^\times$*, of order* 5*; this was confirmed by direct computation of successive powers of* x *modulo* $m_2(x)$ *in* $\mathbb{F}_3[x]$*. By Theorem 7.2,* Φ_x *has order* $\operatorname{lcm}(1,5) = 5$*, correctly recovering the elementary fact that the pure cyclic shift on* $n = 5$ *cells has period exactly* $n = 5$.

8. EXPLICIT INVERSE CONSTRUCTION

Proposition 8.1. *If* $f(x)$ *is a unit of* R_n*, an explicit inverse rule* $u(x)$ *with* $u(x)f(x) \equiv 1 \pmod{x^n-1}$ *and* $\deg u < n$ *can be computed by the extended Euclidean algorithm applied to* $(f(x), x^n-1)$ *in* $\mathbb{F}_q[x]$*, using a number of field operations polynomial in n.*

Proof. By Theorem 3.2, $\gcd(f(x), x^n-1) = 1$, so the extended Euclidean algorithm on the pair $(f(x), x^n-1)$ terminates with polynomials $u(x), v(x)$ satisfying $u(x)f(x) + v(x)(x^n-1) = 1$; reducing mod x^n-1 gives $u(x)f(x) \equiv 1 \pmod{x^n-1}$ with $\deg u < n$. The Euclidean algorithm on two polynomials of degree at most n over a field performs a number of arithmetic operations polynomial in n. □

Remark 8.2. *Proposition 8.1 guarantees an inverse rule of support size at most n, but says nothing sharper: the naive bound does not bound the inverse's neighborhood radius independently of n. In the different setting of bi-infinite (non-circular) cellular automata, Czeizler and Kari [7] established a bound on the neighborhood radius of the inverse of a reversible CA purely in terms of the neighborhood radius of the forward rule, independent of the lattice size. Transporting a bound of that sharpness to the circular, finite-order setting of this paper is not immediate, since the group-algebra quotient* R_n *has no direct bi-infinite analogue, and we leave this as a direction for future work.*

9. COMPUTATIONAL REMARKS

Remark 9.1. *Unlike deciding reversibility of a single rule by Euclidean algorithm (Theorem 3.2), computing the exact count of Theorem 5.1 requires the coset sizes* d_i*, not a general polynomial factorization. These are obtained directly from the multiplicative orbit structure of* q *on* $\mathbb{Z}/n\mathbb{Z}$*: each coset is found by iterating* $s \mapsto sq \bmod n$ *from an unvisited residue until it repeats, an* $O(n)$*-time procedure overall (each residue is visited exactly once across all cosets), avoiding any appeal to general-purpose polynomial factorization algorithms over* $\mathbb{F}_q[x]$.

10. CONCLUSION

Reversibility of a circular linear cellular automaton over $\mathbb{F}_q$ is exactly unit membership in the cyclic group algebra R_n (Theorem 3.2). When $\gcd(n,q) = 1$, the semisimple decomposition of R_n along q-cyclotomic cosets (Theorems 4.3–4.4) yields a closed-form count of reversible rules (Theorem 5.1) and an explicit primitive-root case (Corollary 5.2). We then removed this restriction entirely: writing $n = p^a m$ with $\gcd(m,p) = 1$, Theorem 6.1 and Lemma 6.2 extend the count to every n and every finite field (Theorem 6.3), with a matching primitive-root corollary (Corollary 6.4) and a density bound that is, notably, independent of the multiplicity p^a

(Proposition 6.6). Restricting again to $\gcd(n,q) = 1$, the same CRT decomposition identifies the group of reversible rules under composition explicitly as a product of cyclic groups (Proposition 7.1) and gives a closed formula for the exact dynamical period of any reversible rule as an lcm of orders in finite fields (Theorem 7.2). Proposition 8.1 gives an explicit, polynomial-time inverse-rule construction, though sharpening its neighborhood-radius bound to match the bi-infinite results of Czeizler and Kari [7] in this circular, finite setting remains open.

REFERENCES

[1] G. A. Hedlund, "Endomorphisms and automorphisms of the shift dynamical system," *Mathematical Systems Theory*, vol. 3, no. 4, pp. 320–375, 1969.

[2] O. Martin, A. M. Odlyzko, and S. Wolfram, "Algebraic properties of cellular automata," *Communications in Mathematical Physics*, vol. 93, no. 2, pp. 219–258, 1984.

[3] G. Manzini and L. Margara, "Invertible linear cellular automata over $\mathbb{Z}_m$: Algorithmic and dynamical aspects," *Journal of Computer and System Sciences*, vol. 56, no. 1, pp. 60–67, 1998.

[4] J. Kari, "Reversibility and surjectivity problems of cellular automata," *Journal of Computer and System Sciences*, vol. 48, no. 1, pp. 149–182, 1994.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland, 1977.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 1997, vol. 20.

[7] E. Czeizler and J. Kari, "A tight linear bound on the neighborhood of inverse cellular automata," in *Automata, Languages and Programming (ICALP 2005)*, ser. Lecture Notes in Computer Science, vol. 3580. Springer, 2005, pp. 410–420.