Canonical Number Systems on Polynomial Quotients: A Finite-Generators Pipeline

Haoyuan Wang *

Posted Date: 24 November 2025

doi: 10.20944/preprints202511.1800.v1

Keywords: canonical number system (CNS); n-dimensional numeration; polynomial quotient ring; Gröbner elimination; graph ideal; digit folding; finite generators; countable rings

Article

Canonical Number Systems on Polynomial Quotients: A Finite-Generators Pipeline

Haoyuan Wang

University of California, Irvine CA 92617, USA; jeremw7@uci.edu

Abstract

I introduce an n-dimensional canonical number system (CNS) on modules: a finite base frame $\mathbf{b}$, an E-linear shift T, and a finite digit set D yield unique finite expansions along places $\{T^k(b_i)\}$. For a finitely generated ring $R = \mathbb{Z}[a_1, \ldots, a_n]$, I use the presentation $R \cong \mathbb{Z}[x_1, \ldots, x_n]/\ker(\phi)$ and compute $\ker(\phi)$ via a graph-ideal elimination scheme. When the quotient has finitely many standard monomials, choosing a non–zero-divisor prime p equips R with a base-p CNS (pre-folding) that uses those monomials as places. A digit-folding lemma then compresses coordinates whenever some place has only finitely many powers, preserving uniqueness. This provides a constructive pipeline from presentations of finitely generated, countable rings to explicit multi-dimensional CNS representations, supporting the conjecture that every such ring is isomorphic to an n-dimensional CNS.

Keywords: canonical number system (CNS); n-dimensional numeration; polynomial quotient ring; Gröbner elimination; graph ideal; digit folding; finite generators; countable rings

MSC: Primary 11A63; Secondary 11R04, 13P10, 13F20

---

1. Introduction

Conjecture 1. *Let R be a ring with $|R| \leq \aleph_0$ that is finitely generated. Then R is isomorphic to an n-dimensional-base canonical number system (CNS).*

The main results of this paper are the following theorems.

Definition 1 (Canonical number system; following laus Scheicher and Jörg M. Thuswaldner [1], and Christiaan E. van de Woestijne [2])**.** *Let R be a commutative ring and $\varphi : R \to R$ a homomorphism with finite cokernel (i.e. $[R : \varphi(R)] < \infty$). A finite set $D \subset R$ is a* digit set *if it is a complete set of representatives of $R/\varphi(R)$ (contains exactly one element from each coset). We call (R, φ, D) a* canonical number system (CNS) *if every $r \in R$ admits a* finite expansion

$$r = \sum_{k=0}^{\ell} \varphi^k(d_k) \quad \text{with } d_k \in D,$$

and the expansion is unique *whenever D is irredundant (a true transversal).*

Polynomial/base specialization. Let $P(x) \in \mathbb{Z}[x]$ be monic with $|P(0)| \geq 2$, put $R = \mathbb{Z}[x]/(P)$, and let $\bar{x}$ be the class of x in R. With the digit set $\mathcal{N} = \{0, 1, \ldots, |P(0)| - 1\}$ (a transversal of $R/\bar{x}R$), we say $(P, \mathcal{N})$ (or equivalently $(R, \bar{x}, \mathcal{N})$) is a CNS if every $\gamma \in R$ has a unique finite expansion

$$\gamma = \sum_{k=0}^{\ell} n_k \bar{x}^k, \qquad n_k \in \mathcal{N}.$$

If P is irreducible and α is a root, this is the same as unique finite α-expansions in $R \cong \mathbb{Z}[\alpha]$; in this case α is called a CNS base.

 doi:10.20944/preprints202511.1800.v1

Definition 2 (n–dimensional CNS). *Let E be a commutative ring and let L be an E–module.*

Digits. *Fix finite digit alphabets*

$$D_1,\ D_2,\ \ldots,\ D_n\ \subset E, \qquad |D_i| < \infty \text{ for each } i,$$

and set the product digit set

$$D := D_1 \times D_2 \times \cdots \times D_n.$$

Base. *Fix a finite base frame*

$$\mathbf{b} = (b_1, \ldots, b_n) \in L^n \quad \big(|\mathbf{b}| = n < \infty\big).$$

Places. *Fix a countable index set $I = \mathbb{N}_0$ and an E–linear "shift" endomorphism $T : L \to L$. The place set is*

$$\mathcal{B}_\infty\ :=\ \{\, T^k(b_i)\ :\ i = 1, \ldots, n,\ k \in I \,\}\ \subset L.$$

Expansion. *For $\mathbf{d} = (d_1, \ldots, d_n) \in D$ write $\langle \mathbf{d}, \mathbf{b} \rangle := \sum_{i=1}^{n} d_i\, b_i \in L$. We say $(L, T, \mathbf{b}, D)$ is an* n–dimensional canonical number system *if every $r \in L$ admits a* unique finite *expansion*

$$\boxed{\ r\ =\ \sum_{k \in I}^{\text{finite}} \big\langle \mathbf{d}_k,\ T^k \mathbf{b} \big\rangle, \qquad \mathbf{d}_k \in D.\ }$$

Equivalently (by E–linearity of T),

$$r\ =\ \sum_{k \in I}^{\text{finite}} T^k\big(\, \langle \mathbf{d}_k, \mathbf{b} \rangle \,\big).$$

Lemma 1 (Finite–generators presentation). *Let R be a commutative ring with 1 and suppose $R = \mathbb{Z}[a_1, \ldots, a_n]$ for some $a_1, \ldots, a_n \in R$. Then there exists a surjective ring homomorphism*

$$\phi :\ \mathbb{Z}[x_1, \ldots, x_n]\ \twoheadrightarrow\ R, \qquad \phi(x_i) = a_i\ (1 \le i \le n),$$

and hence an isomorphism of rings

$$R\ \cong\ \mathbb{Z}[x_1, \ldots, x_n] \big/ \ker(\phi).$$

Proof. By the universal property of the polynomial algebra on a finite set of indeterminates (Stacks Project, Tag 00S0 [3]), there exists a unique ring morphism

$$\phi :\ \mathbb{Z}[x_1, \ldots, x_n] \longrightarrow R \quad \text{with} \quad \phi|_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}},\ \ \phi(x_i) = a_i.$$

Then

$$\mathrm{Im}(\phi)\ \supseteq\ \mathbb{Z}[\phi(x_1), \ldots, \phi(x_n)]\ =\ \mathbb{Z}[a_1, \ldots, a_n]\ =\ R,$$

hence $\mathrm{Im}(\phi) = R$ and ϕ is surjective. The first isomorphism theorem yields

$$R\ \cong\ \mathbb{Z}[x_1, \ldots, x_n] \big/ \ker(\phi).$$

□

 doi:10.20944/preprints202511.1800.v1

$$\text{Fix } j \in \{1,\dots,n\}, \qquad \boxed{\begin{aligned} E &:= \mathbb{Z}[x_1,\dots,\widehat{x_j},\dots,x_n] \\ &= \{\, f \in \mathbb{Z}[x_1,\dots,x_n] : \deg_{x_j} f = 0 \,\} \\ &= \mathbb{Z}[x_1,\dots,x_{j-1},x_{j+1},\dots,x_n] \end{aligned}}$$

$$L := \mathbb{Z}[x_1,\dots,x_n], \quad T : L \to L,\ T(h) = x_j h, \quad \mathbf{b} = (1) \in L, \quad \langle g, \mathbf{b}\rangle = g \in E.$$

$$\boxed{\forall f \in L\ \exists!\, g_0,\dots,g_d \in E : \quad f = \sum_{k=0}^{d} T^k\big(\langle g_k, \mathbf{b}\rangle\big) = \sum_{k=0}^{d} g_k\, x_j^k.}$$

Lemma 2 (Digit folding for an n–dimensional CNS)**.** *Let E be a commutative ring, L an E–module, and let $T, U \in \mathrm{End}_E(L)$ commute ($TU = UT$). Fix a finite base frame $\mathbf{b}^\circ = (b_1,\dots,b_m) \in L^m$ and an integer $M \geq 1$. Form the expanded base*

$$\widetilde{\mathbf{b}} \;:=\; (\,U^0 b_1,\dots,U^{M-1}b_1;\ \dots\ ;\ U^0 b_m,\dots,U^{M-1}b_m\,) \in L^{mM}.$$

Let the digit alphabets be finite $D_1,\dots,D_m \subset E$ and set $D := D_1 \times \cdots \times D_m$, $\widetilde{D} := D^M$ (blockwise Cartesian product).

Assume $(L, T, \widetilde{\mathbf{b}}, \widetilde{D})$ is an mM–dimensional CNS, i.e. every $r \in L$ has a unique finite expansion

$$r = \sum_{k\geq 0}^{\text{finite}} \langle \widetilde{\mathbf{d}}_k,\ T^k \widetilde{\mathbf{b}}\rangle, \qquad \widetilde{\mathbf{d}}_k = (d_{k,i,j})_{1\leq i\leq m,\ 0\leq j<M} \in \widetilde{D}.$$

Define the folded digit set

$$D_i^\circ \;:=\; \left\{ \sum_{j=0}^{M-1} d_j\, u^j \;\middle|\; d_j \in D_i \right\} \subset E[u]/(u^M) \quad (1 \leq i \leq m), \qquad D^\circ := D_1^\circ \times \cdots \times D_m^\circ,$$

and let $E[u]$ act on L via $u \cdot v := U(v)$.

Then every $r \in L$ admits a finite folded *CNS expansion with base $\mathbf{b}^\circ$:*

$$\boxed{r = \sum_{k\geq 0}^{\text{finite}} \langle \mathbf{e}_k,\ T^k \mathbf{b}^\circ\rangle, \qquad \mathbf{e}_k = (e_{k,1},\dots,e_{k,m}) \in D^\circ, \quad e_{k,i} = \sum_{j=0}^{M-1} d_{k,i,j}\, u^j.}$$

If the original expansion with $(\widetilde{\mathbf{b}}, \widetilde{D})$ is unique and T is injective, then the folded expansion with $(\mathbf{b}^\circ, D^\circ)$ is also unique.

2. Proofs of Main Results

In this section, we will prove the Conjecture 1
From the Lemma 1 and Conjecture 1 we need to know the $\ker(\phi)$

Setup 1 (Finite–generators presentation)**.** *Let R be a commutative ring with 1, generated (as a ring) by $a_1,\dots,a_n \in R$. Choose a presentation*

$$R \;\cong\; \mathbb{Z}[y_1,\dots,y_m]/J$$

for some ideal $J \subset \mathbb{Z}[y_1,\dots,y_m]$, and polynomials $p_i(y) \in \mathbb{Z}[y_1,\dots,y_m]$ such that the image of $p_i(y)$ in R equals a_i. Define

$$\phi :\ \mathbb{Z}[x_1,\dots,x_n] \longrightarrow R, \qquad \phi(x_i) = a_i.$$

 doi:10.20944/preprints202511.1800.v1

Setup 2 (Big ring and graph ideal)**.** *Set the* big ring

$$S \;:=\; \mathbb{Z}[x_1,\ldots,x_n,\; y_1,\ldots,y_m].$$

Define the graph ideal *in S by*

$$I \;:=\; J \;+\; \big(x_1 - p_1(y),\; \ldots,\; x_n - p_n(y)\big) \;\subset\; S.$$

Proposition 1 (Kernel as an elimination ideal)**.** *With I as above,*

$$\ker(\phi) \;=\; I \cap \mathbb{Z}[x_1,\ldots,x_n].$$

Because

Proposition 2. *Let $\phi : \mathbb{Z}[x_1,\ldots,x_n] \to R$ be a ring homomorphism and put $K := \ker(\phi) \triangleleft \mathbb{Z}[x_1,\ldots,x_n]$. If $K = (f_1,\ldots,f_r)$ for some $f_i \in \mathbb{Z}[x_1,\ldots,x_n]$, then*

$$\mathbb{Z}[x_1,\ldots,x_n]/K \;\cong\; \mathbb{Z}[x_1,\ldots,x_n]/(f_1,\ldots,f_r).$$

Proof. Set $J := (f_1,\ldots,f_r)$. Since $J = K$, define

$$\Psi :\; \mathbb{Z}[x_1,\ldots,x_n]/J \longrightarrow \mathbb{Z}[x_1,\ldots,x_n]/K, \qquad \Psi(a+J) := a+K.$$

This is a well-defined ring homomorphism because $a+J = b+J \iff a-b \in J = K \iff a+K = b+K$. Define $\Theta : \mathbb{Z}[x_1,\ldots,x_n]/K \to \mathbb{Z}[x_1,\ldots,x_n]/J$ by $\Theta(a+K) := a+J$. Then

$$(\Theta\circ\Psi)(a+J) = a+J, \qquad (\Psi\circ\Theta)(a+K) = a+K,$$

so Ψ is an isomorphism with inverse Θ. □

Thus we have

Lemma 3 (Third isomorphism for quotients)**.** *Let A be a ring and let $J \subseteq K$ be ideals. The canonical map*

$$\pi :\; A/J \longrightarrow A/K, \qquad \overline{a} \longmapsto \overline{a}$$

is surjective with kernel K/J. Hence

$$(A/J)/(K/J) \;\cong\; A/K.$$

In particular, if $K = (f_1,\ldots,f_r)$ then $A/K \cong A/(f_1,\ldots,f_r)$.

Proof. By the correspondence theorem for ideals, the ideals of A/J are exactly the quotients L/J with L an ideal of A containing J; in particular K/J is an ideal of A/J. The map π is clearly surjective, and $\ker\pi = \{\overline{a} \in A/J :\; a \in K\} = K/J$. Apply the first isomorphism theorem. See, e.g., ([4], Prop. 1.1 and Cor. 1.3) or ([3], Isomorphism theorems for rings). □

Lemma 4 (Finite standard monomials)**.** *Assume there exist integers $M_1,\ldots,M_n \geq 1$ such that in R every monomial $x^\alpha = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ is congruent to a $\mathbb{Z}$–linear combination of monomials with $\alpha_i < M_i$ for each i. Equivalently, the set*

$$\mathcal{B} \;:=\; \big\{\, \overline{x^\alpha} \in R \;:\; 0 \leq \alpha_i < M_i \;(1 \leq i \leq n) \,\big\}$$

is a finite $\mathbb{Z}$–basis of R. Let $m := |\mathcal{B}|$ and list $\mathbf{b} = (b_1,\ldots,b_m)$ the elements of $\mathcal{B}$.

 doi:10.20944/preprints202511.1800.v1

Lemma 5 (Digits and place map). *Fix a prime p which is not a zero divisor in R and define*

$$T : R \to R, \quad T(r) := p\, r, \qquad D := \Big\{ \sum_{j=1}^{m} d_j\, b_j \;\Big|\; d_j \in \{0, 1, \ldots, p-1\} \Big\} \subset R.$$

Theorem 1 (Folded CNS). *Assume the pre–folding CNS of Theorem 2 is realized in the module form by commuting endomorphisms $T, U \in \mathrm{End}_E(L)$ and data*

$$\widetilde{\mathbf{b}} = \big(U^0 b_1, \ldots, U^{M-1} b_1;\ \ldots\ ;\ U^0 b_m, \ldots, U^{M-1} b_m\big), \qquad \widetilde{D} = D^M,$$

for some finite frame $\mathbf{b}^\circ = (b_1, \ldots, b_m)$ and $M \geq 1$. Then there exists a folded *digit set $D^\circ \subset E[u]/(u^M)$ and the same base frame $\mathbf{b}^\circ$ such that every $r \in L$ has a finite folded expansion*

$$r = \sum_{k \geq 0}^{\text{finite}} \big\langle \mathbf{e}_k,\ T^k \mathbf{b}^\circ \big\rangle, \qquad \mathbf{e}_k \in D^\circ.$$

If the pre–folding expansion is unique and T is injective, then the folded expansion is also unique. Consequently, $(L, T, \mathbf{b}^\circ, D^\circ)$ is an m–dimensional CNS.

Proof. Apply Lemma 2 with the given $(L, T, U, \mathbf{b}^\circ, M)$. The lemma constructs D° and yields the folded expansion; its final clause gives uniqueness under the stated hypothesis on T. □

Thus from Lemma 1 and Lemma 2 we have

$$\text{Let } \phi :\ \mathbb{Z}[x_1, \ldots, x_n] \twoheadrightarrow R, \qquad K := \ker(\phi).$$

$$R \ \cong\ \mathbb{Z}[x_1, \ldots, x_n]/K \ \cong\ \mathbb{Z}[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$$

Thus from Lemma 1

$$\mathbb{Z}[x_1, \ldots, x_n]/(f_1, \ldots, f_r) \text{ is an } n\text{-dimensional CNS}$$

$$\Longrightarrow \quad R \ \cong\ \text{an } n\text{-dimensional CNS.}$$

3. Example

Example 1 (Pipeline on). $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$ ***Step 1: Presentation and kernel via graph ideal.*** *Let $R = \mathbb{Z}[t]/(t^2+1)$ and set $a_1 = \bar{t} \in R$. Define $\phi : \mathbb{Z}[x] \to R$, $\phi(x) = a_1$. Build the big ring $S = \mathbb{Z}[x, y]$ and the graph ideal*

$$I \ :=\ (\, y^2 + 1,\ x - y\,) \ \subset S.$$

Then $K := \ker(\phi) = I \cap \mathbb{Z}[x] = (x^2+1)$ (eliminating y gives x^2+1). Hence

$$R \ \cong\ \mathbb{Z}[x]/K \ \cong\ \mathbb{Z}[x]/(x^2+1).$$

(This mirrors the "big ring & graph ideal" step and kernel elimination in the paper.) *[3]*

Step 2: Finite standard monomials and pre–folding CNS. *In $\mathbb{Z}[x]/(x^2+1)$ every monomial reduces to a $\mathbb{Z}$–combination of $\{1, x\}$, so $\mathcal{B} = \{\bar{1}, \bar{x}\}$ is a finite $\mathbb{Z}$–basis. Fix a prime $p = 5$ (a non–zero–divisor in R), put*

$$T : R \to R,\ T(r) = 5r, \qquad D \ :=\ \{d_0 \cdot \bar{1} + d_1 \cdot \bar{x} \ :\ d_0, d_1 \in \{0, 1, 2, 3, 4\}\}.$$

Then every $r = a + b\bar{x} \in R$ has a (unique) pre–folding *base–5 expansion*

$$r = \sum_{k=0}^{\ell} 5^k \big(d_{k,0} \cdot \bar{1} + d_{k,1} \cdot \bar{x}\big), \quad a = \sum_k d_{k,0}\, 5^k,\ \ b = \sum_k d_{k,1}\, 5^k,\ d_{k,j} \in \{0, \ldots, 4\}.$$

 doi:10.20944/preprints202511.1800.v1

Concrete digits. *Take* $r = 37 + 11\,\bar{x}$. *Write* $37 = 2 + 2\cdot 5 + 1\cdot 5^2$ *and* $11 = 1 + 2\cdot 5$. *Thus*

$$r = \underbrace{(2+1\bar{x})}_{k=0} + 5\underbrace{(2+2\bar{x})}_{k=1} + 5^2\underbrace{(1+0\bar{x})}_{k=2}.$$

Step 3: Fold along a finite–power coordinate (digit folding). *Let* U *be multiplication by* $\bar{x}$; *since* $\bar{x}^2 = -1$, *only the two powers* $\bar{x}^0, \bar{x}^1$ *survive in normal form* ($M = 2$). *Apply the folding lemma with base frame* $b^\circ = (\bar{1})$, *so the expanded frame is* $(\bar{1}, \bar{x})$. *Pack each pair of coefficients at level* k *into a single folded digit* $e_k = d_{k,0} + d_{k,1}\,u \in \mathbb{Z}[u]/(u^2)$, *where* u *acts on* R *by* $u \cdot v := U(v) = \bar{x}v$. *For our* r:

$$e_0 = 2 + 1u, \qquad e_1 = 2 + 2u, \qquad e_2 = 1 + 0u.$$

The folded *CNS expansion is*

$$\boxed{r = \sum_{k=0}^{2} 5^k \,\langle e_k,\ T^k b^\circ\rangle = (2+1u) + 5(2+2u) + 5^2(1+0u),}$$

which is unique because the pre–folding expansion was unique and T *is injective.*

Conclusion. *We exhibited the full pipeline:*

$$\mathbb{Z}[i] \ \cong\ \mathbb{Z}[x]/(x^2+1) \implies \textit{pre–folding base–5 CNS on } \{\bar{1}, \bar{x}\} \implies \textit{folded 1–dim CNS on } (\bar{1}).$$

This exemplifies the definitions and the folding mechanism used in the paper.

Example 2. $\mathbb{F}_3$ *(and* $\mathbb{F}_3^n$*) as a CNS* ***Step 1 (Presentation via a kernel).*** *Let* $\phi : \mathbb{Z} \to \mathbb{F}_3$ *be the reduction mod* 3 *map,* $\phi(1) = \bar{1}$. *Then* $\ker(\phi) = 3\mathbb{Z}$ *and*

$$\mathbb{F}_3 \ \cong\ \mathbb{Z}/\ker(\phi) \ =\ \mathbb{Z}/(3).$$

Equivalently, for any $n \geq 1$ *one may take*

$$\Phi :\ \mathbb{Z}[x_1, \ldots, x_n] \longrightarrow \mathbb{F}_3, \qquad \Phi|_{\mathbb{Z}} = \textit{mod } 3,\ \ \Phi(x_i) = 0,$$

with $\ker(\Phi) = (3, x_1, \ldots, x_n)$, *so* $\mathbb{F}_3 \cong \mathbb{Z}[x_1, \ldots, x_n]/(3, x_1, \ldots, x_n)$.

Step 2 (CNS on $\mathbb{F}_3$***).*** *Work with the* 1*–dimensional module form of Definition 2:*

$$E = \mathbb{Z}, \quad L = \mathbb{Z}, \quad T : L \to L,\ T(m) = 3m, \quad \mathbf{b} = (1), \quad D = \{0,1,2\} \subset L.$$

Passing to the quotient $L/3L \cong \mathbb{F}_3$, *every* $\bar{a} \in \mathbb{F}_3$ *has the unique* finite *expansion (indeed, length* 0*)*

$$\boxed{\bar{a} = \langle d_0,\ T^0\mathbf{b}\rangle = d_0 \cdot \bar{1}, \qquad d_0 \in \{0,1,2\}.}$$

Here the "place" exponents are just 0 *(so the 'exponential vector' is trivially* 1^1*), and the digit set is exactly* $\{0,1,2\}$.

Step 3 (n***–dimensional version with identity frame).*** *Let* $L = \mathbb{Z}^n$ *with the standard basis* $\mathbf{b} = (e_1, \ldots, e_n)$ *(the* identity vector frame*), keep* $T = 3\,\mathrm{id}_L$, *and take the product digit set*

$$D = \{0,1,2\}^n = \{(d_1, \ldots, d_n) : d_i \in \{0,1,2\}\}.$$

Modulo 3, *we obtain* $L/3L \cong \mathbb{F}_3^n$, *and every* $\bar{v} \in \mathbb{F}_3^n$ *has a unique expansion of length* 0*:*

$$\boxed{\bar{v} = \langle \mathbf{d}_0,\ T^0\mathbf{b}\rangle = d_1\,\bar{e}_1 + \cdots + d_n\,\bar{e}_n, \qquad \mathbf{d}_0 = (d_1, \ldots, d_n) \in \{0,1,2\}^n.}$$

 doi:10.20944/preprints202511.1800.v1

Thus $\mathbb{F}_3$ (and, with the identity frame, $\mathbb{F}_3^n$) is a canonical n–dimensional number system whose digit vectors are drawn from $\{0,1,2\}^n$ and whose "place exponents" are the all–ones multiindex 1^n (i.e. only the $k=0$ place occurs after mod 3).

References

1. Klaus Scheicher and Jörg M. Thuswaldner, *On the characterization of canonical number systems*, Osaka Journal of Mathematics, vol. 41, no. 2, pp. 327–351, 2004.
2. Christiaan E. van de Woestijne, *Number systems and the Chinese Remainder Theorem*, arXiv:1106.4219 [math.NT], 2011.ms, Osaka Journal of Mathematics, vol. 41, no. 2, pp. 327–351, 2004.
3. The Stacks Project Authors, *The Stacks Project*. Tag 00S0 (Presentations of algebras; polynomial algebras on an arbitrary set of indeterminates).
4. M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison–Wesley, 1969.
5. The Stacks Project Authors, *The Stacks Project*, available online.