Moduli Selection in Robust Chinese Remainder Theorem: Closed-Form Solutions and Layered Design

Wenyi Yan, *Student Member, IEEE,* Lu Gan, *Senior Member, IEEE*, Hongqing Liu, *Senior Member, IEEE,* Shaoqing Hu, *Member, IEEE*

Abstract

We study the fundamental problem of *moduli selection* in the Robust Chinese Remainder Theorem (RCRT), where each residue may be perturbed by a bounded error. Consider L moduli of the form $m_i = \Gamma_i m$ $(1 \leq i \leq L)$, where Γ_i are pairwise coprime integers and $m \in \mathbb{R}^+$ is a common scaling factor. For small L $(L = 2, 3, 4)$, we obtain exact solutions that maximize the robustness margin under dynamic-range and modulus-bound constraints. We also introduce a Fibonacci-inspired *layered* construction (for $L = 2$) that produces exactly K robust decoding layers, enabling predictable trade-offs between error tolerance and dynamic range. We further analyze how robustness and range evolve across layers and provide a closed-form expression to estimate the success probability under common data and noise models. The results are promising for various applications, such as sub-Nyquist sampling, phase unwrapping, range estimation, modulo analog-to-digital converters (ADCs), and robust residue-number-system (RNS)-based accelerators for deep learning. Our framework thus establishes a general theory of moduli design for RCRT, complementing prior algorithmic work and underscoring the broad relevance of robust moduli design across diverse information-processing domains.

Index Terms

Chinese Remainder Theorem (CRT), moduli construction, multi-level error tolerance, dynamic range, robustness.

I. Introduction

The classical Chinese Remainder Theorem (CRT) states that an integer can be uniquely reconstructed from its residues modulo L pairwise coprime integers $\{m_1, m_2, \ldots, m_L\}$, with the reconstruction guaranteed within the least common multiple (lcm) of the moduli. Owing to its algebraic structure, CRT underpins applications in digital arithmetic [2], cryptography [3], coding theory [3]–[8], sequence design for collision channels [9], [10] and secure communication [11].

Despite its versatility, the classical CRT is inherently noise-sensitive. Within information theory, *CRT codes* have been studied as error-correcting codes under an erasure error model, where some residues are received correctly

Wenyi Yan, Lu Gan, and Shaoqing Hu are with the College of Engineering, Design and Physical Sciences, Brunel University of London, UK. Hongqing Liu is with the School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, China. Part of this work was presented at ICASSP 2024 [1].

while others may be erroneous [7]. In practice, however, all residues may be corrupted, and robustness against such perturbations becomes essential. To address this challenge, Wang and Xia introduced Robust CRT (RCRT), which extends the classical model by allowing every residue to be perturbed by a bounded error [12]. Their framework guarantees a unique and stable reconstruction provided that the noise amplitude remains below a modulus-dependent threshold. Notably, RCRT can be formulated for both integer-valued and real-valued moduli and inputs, broadening its scope beyond discrete arithmetic and making it applicable to a wide range of problems, including sub-Nyquist sampling [13]–[15], phase unwrapping [16], range estimation [17]–[19], motion estimation [20], modulo analog-to-digital converters (ADCs) [1], [21]–[23], and fault-tolerant analog neural network training [24], [25].

Building on this foundation, numerous RCRT variants have been developed, including multi-stage grouping-based methods [26], lattice-based approaches [18], [19], [27], [28], and search-based strategies [29]. Extensions to multiple integer inputs [30], [30], multidimensional [31]–[33] and complex-valued systems [22], [34] have also been explored. Among these, the layered RCRT model of Xiao *et al.* [35] is particularly notable, as it introduces K robust layers atop the classical CRT, enabling multi-level reconstruction that trades dynamic range for improved error tolerance. Together, these advances highlight the central importance of robustness in modern CRT-based systems.

Although substantial progress has been made on reconstruction algorithms, systematic moduli design remains an open challenge, with most existing approaches relying on heuristic parameter choices. Note that classical digital residue number systems (RNS) adopt structured modulus sets such as $\{2^n-1, 2^n, 2^n+1\}$ to facilitate hardware efficiency [36]–[38]. Although effective for error-free digital systems, such RNS constructions do not address robustness requirements in scenarios where *all* residues are corrupted by noise. This limitation is particularly pronounced in emerging applications such as multi-channel modulo ADCs [21], [22] and *optical DNN accelerators* [24], [25], which exploit CRT for parallelism and precision but remain vulnerable to rounding errors and hardware imperfections. These considerations motivate the development of moduli design strategies explicitly tailored for robustness.

This paper addresses the above-mentioned issues by developing explicit, closed-form moduli construction strategies tailored for RCRT systems in information processing. Our key contributions are:

- **Closed-form Moduli Design for the full CRT Layer:** We derive optimal constructions to select $L \in \{2, 3, 4\}$ moduli that maximize error tolerance at the full CRT layer. The solutions satisfy design constraints on modulus size and dynamic range with computational complexity $\mathcal{O}(1)$, enabling efficient hardware implementation in applications such as range estimation, modulo ADCs and analog neural network training.
- **Layered Moduli Construction via Fibonacci-like Sequences:** We propose an explicit construction method for two-moduli systems supporting exactly K robust layers. By leveraging Fibonacci-like integer sequences, the design guarantees controlled remainder chain length and facilitates predictable trade-offs between dynamic range and robustness.
- **Analysis of Range–Robustness Trade-offs and Success Probability:** We analyze how the number of robust layers K influences both dynamic range and error tolerance across layers. Moreover, we derive closed-form estimates for overall success probability under representative signal and noise models, providing valuable guidelines for system-level design.

The rest of this paper is organized as follows. Section II reviews the principles of RCRT and multi-level

TABLE I: List of Notations

Notation	Explanation
x / $\tilde{x}$	Real-valued input signal / Reconstructed signal
L	Number of moduli
Γ_i	Coprime base moduli, for $1 < i \leq L$
m	Common scaling factor
m_i	Moduli: $m_i = m\Gamma_i$
r_i / $\tilde{r}_i$	Noiseless / noisy remainders modulo m_i
e_i	Additive error on r_i
n_i	True folding integers: $n_i = \lfloor x/m_i \rfloor$
$\tilde{n}_i$	Estimated folding integers: $\tilde{n}_i = \lfloor \tilde{x}/m_i \rfloor$
N_{th}	Target dynamic range threshold
$m_{\max}$	Maximum allowed modulus
ρ	Design ratio: $\rho = N_{\mathrm{th}}/m_{\max}$
ζ_d	Multiplier in Fibonacci-based construction
$F_{d,k}$	Fibonacci-like sequence with seed $(d, 1)$
K	Number of robust decoding layers
σ_j	Remainder at layer j, for $1 \leq j \leq K+1$
P_j	Dynamic range at layer j
P_{K+1}	Final-layer dynamic range
τ_j	Tolerable error at layer j: $\tau_j = \frac{m\sigma_j}{4}$
$T(x)$	Piecewise error bound function
η_{succ}	Success probability of reconstruction
ϵ, ς	Noise bound / standard deviation
φ	Golden ratio: $\varphi = \frac{1+\sqrt{5}}{2}$

reconstruction. Existing research on moduli selection is also discussed. Section III presents closed-form moduli designs for the full CRT layer with $L = 2, 3$, and 4 moduli. Section IV introduces the proposed Fibonacci-inspired construction for layered systems with two moduli. Section V presents range–robustness trade-offs and derives probabilistic performance estimates. Section VI validates the proposed methods through simulation and concludes in Section VII.

Notations: The greatest common divisor and least common multiple of integers a and b are denoted by $\gcd(a, b)$ and $\mathrm{lcm}(a, b) = |ab|/\gcd(a, b)$, respectively. Modulo operation is written as $x \bmod m$, and the congruence relation as $a \equiv b \pmod{m}$. The floor, ceiling are denoted by $\lfloor \cdot \rfloor$ and $\lceil \cdot \rceil$. $\mathbb{Z}_{>a}$ denotes the integers greater than a; $\mathbb{N}$, the positive integers. $\mathcal{O}(\cdot)$ indicates computational complexity. The main variables and parameters used in this paper are summarized in Table I.

II. Literature Review

This section reviews the literature on RCRT systems, with particular emphasis on reconstruction methods that admit simple closed-form solutions, analogous to the classical CRT for integer inputs. Such methods are promising for real-time and low-latency applications.

Let $x \geq 0$ be a real-valued signal observed via L moduli $\{m_i\}_{i=1}^{L}$. For each modulus m_i, x can be decomposed as $x = n_i m_i + r_i$, where $n_i = \lfloor x/m_i \rfloor$ is the folding integer and $r_i = x \bmod m_i = x - n_i m_i$ is the remainder. In practical settings, however, the observed remainders are often corrupted by noise, yielding:

$$\tilde{r}_i = r_i + e_i = (x \bmod m_i) + e_i, \tag{1}$$

where e_i is the residue (or remainder) error. Let $\tilde{x}$ denote the reconstructed signal from the noisy remainders $\{\tilde{r}_i\}$. In this context, we adopt the following definition of robust reconstruction [12].

Definition 1 (Robust Reconstruction)**.** *Let $\tilde{n}_i = \lfloor \tilde{x}/m_i \rfloor$ and $n_i = \lfloor x/m_i \rfloor$ denote the estimated and true folding integers, respectively. Reconstruction is said to be robust if $\tilde{n}_i = n_i$ for all $i = 1, \ldots, L$.*

A. Single-layer Standard RCRT systems

Wang *et al*. introduced a common factor m among the moduli [12]. Each modulus is written as $m_i = m\Gamma_i$, where Γ_i are pairwise coprime integers. A simple, closed-form reconstruction was also developed in [12]. The following Proposition provides the theoretical guarantee for accurate reconstruction under bounded noise.

Proposition 1 (Real-Valued RCRT [12])**.** *Let the moduli be $m_i = m\Gamma_i$ for $1 \leq i \leq L$, where $m > 0$ and $\Gamma_1, \ldots, \Gamma_L$ are pairwise coprime integers. Then for any $x \in [0, P)$ with*

$$P = m \cdot \prod_{i=1}^{L} \Gamma_i,$$

the folding integers $n_i = \lfloor x/m_i \rfloor$ can be determined from noisy remainders $\tilde{r}_i = x \bmod m_i + e_i$, provided the remainder errors satisfy

$$|e_1 - e_i| < \frac{m}{2}, \quad \textit{for } 2 \leq i \leq L. \tag{2}$$

A sufficient condition for (2) *is the uniform bound*

$$|e_i| < \frac{m}{4}, \quad \textit{for all } i, \tag{3}$$

commonly referred to as the ***error bound****.*

To further improve robustness, Xiao *et al.* developed a multi-stage RCRT framework [26] that relaxes the restrictive pairwise coprimality of Γ_i. By grouping moduli into stages and applying RCRT hierarchically, this framework achieves larger error bounds and offers greater flexibility in system design.

Lattice-based CRT optimisation [18], [19], [27], [28] reformulates the reconstruction as the closest vector search in a lattice defined by the moduli. These methods are applicable even when moduli are not co-prime and offer strong robustness under noise, but they incur significantly higher computational complexity compared to closed-form RCRT methods.

Similarly, Xiao *et al.* proposed maximum likelihood estimation (MLE) based RCRT algorithms [29], [39], which formulate reconstruction as a modular least-squares problem. These methods are highly flexible and robust to non-uniform and unbounded errors, but their exhaustive search nature leads to computational costs that scale poorly with dynamic range and the number of moduli, limiting practical deployment in real-time applications.

B. Layered Robustness in RCRT Systems

To address the trade-off between robustness and dynamic range, a *layered robustness* framework was developed for two-moduli systems [35], [40]. The key idea is to partition the full dynamic range into multiple layers, each associated with a distinct error bound and dynamic range, as described below.

Proposition 2 (Layered Dynamic Range for Two-Moduli RCRT [35])**.** *Let the moduli be* $m_1 = m\Gamma_1$ *and* $m_2 = m\Gamma_2$*, where* Γ_1 *and* Γ_2 *are coprime positive integers and* $m > 0$ *is the common scaling factor. Define* $\{\sigma_j\}$ *recursively by*

$$\sigma_{-1} = \Gamma_2,\ \sigma_0 = \Gamma_1,\ \sigma_j = \sigma_{j-2} \bmod \sigma_{j-1}\ (j \geq 1), \tag{4}$$

where the layer depth K *is uniquely determined by the termination condition* $\sigma_{K+1} = 1$ *of the Euclidean algorithm on* (Γ_1, Γ_2)*.*

Then, for any layer $j \in \{1, \ldots, K+1\}$*, the folding integers* n_1, n_2 *can be uniquely recovered from noisy remainders* $\tilde{r}_i = x \bmod m_i + e_i$ *if*

$$|e_1 - e_2| < \frac{m\sigma_j}{2}. \tag{5}$$

The corresponding dynamic range at layer j *is*

$$P_j = m \cdot \min\left(\Gamma_2(1 + \ddot{n}_{2,j}),\ \Gamma_1(1 + \ddot{n}_{1,j})\right), \tag{6}$$

where $\ddot{n}_{i,j}$ *are the maximum correctly decodable folding integers at layer* j*, given in [35, Eqs. (51), (52)].*

Condition (5) holds whenever $|e_i| < \frac{m}{4}\sigma_j$ for $i = 1, 2$, which is known as the *layer-j* error bound. An alternative expression for $P_j = mN_j$ was provided in [29], where

$$\begin{cases} N_{-1} = \Gamma_1, \quad N_0 = \Gamma_2, \\ N_j = N_{j-2} + \left\lfloor \dfrac{\sigma_{j-1}}{\sigma_j} \right\rfloor (N_{j-1} - \sigma_j), \quad j \geq 1. \end{cases} \tag{7}$$

This layered RCRT architecture enables a controlled trade-off between error tolerance and dynamic range. In addition to the full CRT range $P = m\Gamma_1\Gamma_2$, it provides K intermediate robust layers, each capable of tolerating larger errors at the cost of a reduced dynamic range. Such a multi-resolution representation is particularly beneficial in noisy environments such as ADCs and range estimation.

Geometric intuition (pairwise–difference view). Eq. (5) admits a minimum–separation interpretation in the two–moduli residue plane. Fig. 1 illustrates (r_1, r_2) for $m = 1.5$, $\Gamma_1 = 12$, $\Gamma_2 = 17$. The Euclidean remainders are $\sigma_1 = 5$, $\sigma_2 = 2$, and $\sigma_3 = 1$, i.e., $K = 2$ robust layers followed by a full-CRT layer. Each valid pair of folding integers (n_1, n_2) generates a family of slanted lines $r_2 = r_1 + mc, \quad c \in \mathbb{Z}$, with *non-uniform* gaps whose

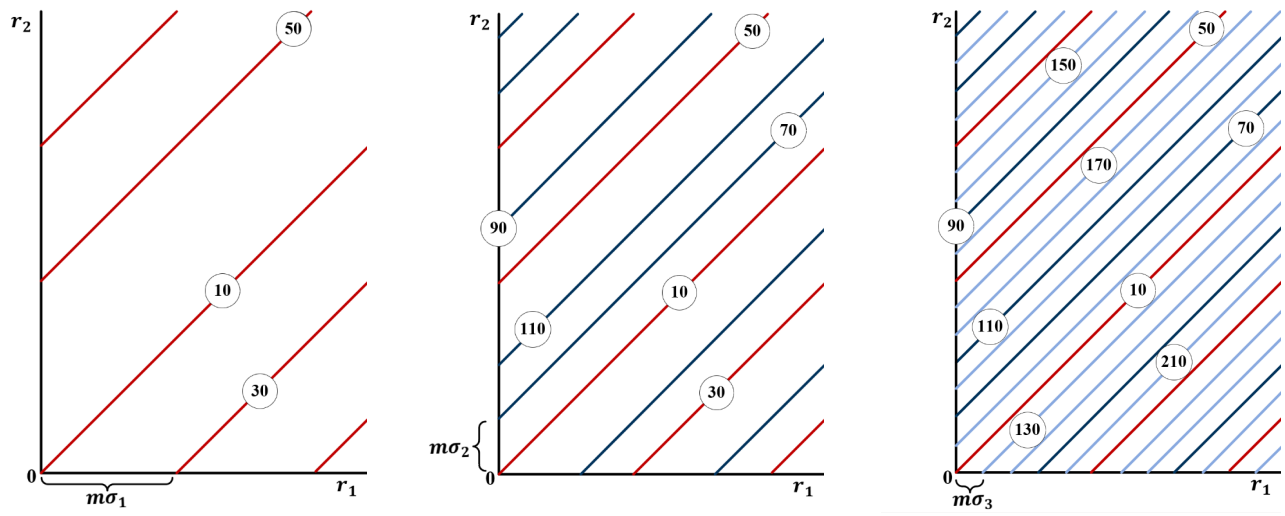


Fig. 1: Layered RCRT residue maps in the (r_2, r_1) plane for $\Gamma_1 = 12$, $\Gamma_2 = 17$, $m = 1.5$, and $K = 2$. Each plotted point is (r_2, r_1) generated by a value x, with $r_\ell = x \bmod m_\ell$ and $m_\ell = \Gamma_\ell m$ $(\ell = 1, 2)$. Small circled labels indicate the corresponding x. Slanted families depict the pairwise-difference structure; at layer j the inter-family spacing equals $m\sigma_j$ and the admissible dynamic range is $[0, P_j)$. (a) Robust layer 1: $x \in [0, 54]$, $m\sigma_1 = 7.5$. (b) Robust layer 2: $x \in [0, 127.5]$, $m\sigma_2 = 3$. (c) Full CRT layer: $x \in [0, 306]$, $m\sigma_3 = 1.5$.

local minimum separation at layer j is lower-bounded by $m\,\sigma_j$. Consequently, the decoder succeeds whenever the pairwise residue perturbation satisfies (5). Fig. 1 (a)–(c) visualize how the admissible dynamic range expands from $[0, 54)$ to $[0, 127.5)$ and finally to $[0, 306)$, while the guaranteed local separation (and thus the error tolerance) tightens from $m\,\sigma_1 = 7.5$ to $m\,\sigma_2 = 3$ and then to $m\,\sigma_3 = 1.5$.

C. Moduli Selection in RCRT Systems

Moduli selection plays a critical role in both performance and hardware efficiency for RCRT-based systems. Classical integer CRT and RNS often adopt structured modulus sets near powers of two to enable fast arithmetic and binary-friendly implementations [38]. While effective for digital computation, these designs do not account for robustness against noise or perturbations, and their coarse granularity limits applicability in analog domains such as modulo ADCs [1].

For RCRT with a single full CRT layer, prior work has explored moduli selection for various applications. Xiao *et al.* [29] studied random prime-based selection to achieve statistical robustness in residue coding. Akhlaq *et al.* [18], [27] proposed search-based wavelength selection schemes for least square-based range estimation by optimizing the underlying lattice geometry. However, these methods rely on solving the Closest Vector Problem (CVP) in high-dimensional lattices, which is computationally expensive and lacks deterministic error bounds. Moreover, optimized moduli often require high-precision parameters (e.g., Examples D in [18]), which pose challenges for hardware

implementation. Even for single-layer systems, none of these approaches yields explicit, closed-form strategies for moduli design within the RCRT framework.

To our knowledge, no existing work addresses moduli selection for *layered RCRT systems*, where additional robust layers are introduced to improve error tolerance at the cost of reduced dynamic range. This gap highlights the need for closed-form, analytically grounded moduli design techniques applicable to both single-layer and layered RCRT. Developing such methods is essential for enabling efficient reconstruction and hardware implementation, which is the core motivation of this work.

III. Moduli selection for Multi-modular Systems

In applications of RCRT systems (e.g., modulo ADCs, sub-Nyquist sampling, phase unwrapping, analog neural network training), moduli selection must satisfy: (*i*) a hardware-imposed maximum modulus $m_i \leq m_{\max}$ and (*ii*) an application-driven dynamic range threshold $P \geq N_{\text{th}}$.

To enable efficient and closed-form reconstruction algorithms (e.g., based on RCRT [12]), we also require Γ_i ($1 \leq i \leq L$) to be *pairwise coprime*. Although some prior studies (e.g., [18], [26], [35]) have explored non-coprime Γ_i with more advanced decoding, such approaches typically involve complicated residue grouping or solving CVP problems in lattice search, making them less attractive for real-time applications.

Given a maximum modulus $m_{\max}$ and a dynamic range threshold N_{th}, the goal is to select L strictly increasing integers $\Gamma_1 < \Gamma_2 < \cdots < \Gamma_L$, and define the moduli as

$$m_i = m \cdot \Gamma_i, \quad i = 1, \ldots, L, \tag{8}$$

subject to the following constraints:

$$\textbf{Pairwise coprimality:} \quad \gcd(\Gamma_i, \Gamma_j) = 1 \quad \forall\, i \neq j, \tag{9}$$

$$\textbf{Modulus threshold:} \quad m \cdot \Gamma_L \leq m_{\max}, \tag{10}$$

$$\textbf{Dynamic range:} \quad m \cdot \prod_{i=1}^{L} \Gamma_i \geq N_{\text{th}}. \tag{11}$$

By Proposition 1, the error bound is proportional to the common scaling factor m, motivating its maximisation for noise robustness. From (10), we set

$$m = \frac{m_{\max}}{\Gamma_L}. \tag{12}$$

Substituting into (11) yields

$$\prod_{i=1}^{L-1} \Gamma_i \geq \rho, \quad \text{where} \quad \rho = \frac{N_{\text{th}}}{m_{\max}}. \tag{13}$$

Since $m \propto 1/\Gamma_L$, the design reduces to

$$\min_{2 \leq \Gamma_1 < \cdots < \Gamma_L} \quad \Gamma_L, \tag{14}$$

subject to the *pairwise coprimality* condition (9) and the *product* constraint (13).

Finding an optimal solution to the above problem for an arbitrary L is computationally intractable due to the combinatorial nature of the pairwise coprimality and product constraints. However, in many practical RCRT

applications, the number of moduli L is typically small due to hardware limitations. For instance, in multi-channel modulo ADCs [21], each channel samples at the Nyquist rate f_{NYQ}, yielding a total sampling rate of Lf_{NYQ}. The analog modulo operation [41], [42] on each channel requires digital counters and comparators, with complexity growing quickly as L increases. On platforms constrained by size, weight, or power, such as implantable devices or portable radio frequency sensors, the number of parallel channels is therefore limited to small L. Similar restrictions arise in RCRT-based frequency and phase estimation [17], [20], where each modulus requires an additional sensing or measurement channel, making large L impractical in radar, sonar, or communication systems. An analogous limitation is present in emerging analog neural network training accelerators based on residue number systems [24], [25], where implementing many parallel modular channels is infeasible due to optical hardware overhead and noise sensitivity. In all these cases, closed-form optimal constructions for small L are highly desirable.

To address this need, we derive closed-form optimal solutions for $L = 2, 3,$ and 4, which maximize the scaling factor m under the design constraints (9)–(11). These constructions rely on the following elementary lemma on the pairwise coprimality of integers.

Lemma 1 (Basic Coprimality Properties)**.** *Let $\alpha \in \mathbb{N}$. Then the following hold:*

(i) Two consecutive integers α and $\alpha + 1$ are coprime, i.e., $\gcd(\alpha, \alpha + 1) = 1$.

(ii) Two consecutive odd integers $2\alpha - 1$ and $2\alpha + 1$ are coprime.

(iii) Any three consecutive odd integers $\{2\alpha - 1,\ 2\alpha + 1,\ 2\alpha + 3\}$ are pairwise coprime.

(iv) Any three consecutive integers $\{\alpha,\ \alpha + 1,\ \alpha + 2\}$ with α odd are pairwise coprime.

The proof follows directly from elementary properties of gcd *and is omitted.*

Based on Lemma 1, we now present optimal constructions for $L = 2, 3,$ and 4, maximizing the feasible value of $m = m_{\max}/\Gamma_L$.

Theorem 1 (Optimal Moduli Selection for $L = 2, 3, 4$)**.** *Let $\rho > 1$ be given by* (13)*. Under the design constraints* (9)–(11)*, the following constructions maximize $m = m_{\max}/\Gamma_L$.*

- ***Case** $L = 2$: The optimal coprime pair is*

$$\{\Gamma_1, \Gamma_2\} = \{\lceil \rho \rceil,\ \lceil \rho \rceil + 1\}. \tag{15}$$

- ***Case** $L = 3$: When $1 < \rho \leq 6$, the unique optimal triple is*

$$(\Gamma_1, \Gamma_2, \Gamma_3) = (2, 3, 5).$$

When $\rho > 6$, define

$$b = \min\{n \in \mathbb{Z},\ n \geq 3 : n(n-1) \geq \rho\} \tag{16}$$

Then the optimal triple is chosen as follows:

$$\{\Gamma_1, \Gamma_2, \Gamma_3\} = \{b - 1,\ b,\ b + 1\}, \qquad \text{if } b \text{ is even}, \tag{17}$$

$$\{\Gamma_1, \Gamma_2, \Gamma_3\} = \{b - 2,\ b,\ b + 1\}, \qquad \text{if } b \text{ is odd, } b \geq 5,\ (b-2)b \geq \rho, \text{ and } (b+1) \bmod 3 \neq 0, \tag{18}$$

TABLE II: Optimal quartet $\{\Gamma_i\}_{i=1}^4$ for $\rho > 6$ with b defined in (20). The symbols "$\wedge$" and "$\vee$" denote logical "and" / "or".

Case label & product gap	**Optimal quartet** $\{\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4\}$
A – Odd b	
A1 : $b \bmod 3 \neq 1$	$\{b-2,\ b-1,\ b,\ b+2\}$
A2 : $b \bmod 3 = 1$	$\{b-2,\ b,\ b+1,\ b+2\}$
B – Even b **with** $(b-3)(b-1)b \geq \rho$	
B1 : $b \bmod 6 \in \{2,4\}$	$\{b-3,\ b-1,\ b,\ b+1\}$
B2 : $b \bmod 6 = 0 \wedge b \bmod 5 \neq 3$	$\{b-3,\ b-1,\ b+1,\ b+2\}$
B3 : $b \bmod 6 = 0 \wedge b \bmod 5 = 3$	
B3.1: if $(b-5)(b-1)(b+1) \geq \rho \wedge b \bmod 7 \neq 5$	$\{b-5,\ b-1,\ b+1,\ b+2\}$
B3.2: otherwise	$\{b-1,\ b+1,\ b+2,\ b+3\}$
C – Even b **with** $(b-3)(b-1)b < \rho \leq (b-3)(b-1)(b+1)$	
C1 : $b \bmod 3 \neq 1 \wedge b \bmod 5 \neq 3$	$\{b-3,\ b-1,\ b+1,\ b+2\}$
C2 : $b \bmod 3 = 1 \wedge b \bmod 5 \neq 3$	$\{b-1,\ b,\ b+1,\ b+3\}$
C3 : $b \bmod 5 = 3$	
C3.1: $b \bmod 3 \neq 1$	$\{b-1,\ b+1,\ b+2,\ b+3\}$
C3.2: $b \bmod 3 = 1$	$\{b-1,\ b,\ b+1,\ b+3\}$
D – Even b **with** $(b-3)(b-1)(b+1) < \rho$	
D1 : $b \bmod 3 \neq 0 \wedge b \bmod 5 \neq 3$	$\{b-1,\ b,\ b+1,\ b+3\}$
D2 : $b \bmod 3 = 0 \vee b \bmod 5 = 3$	$\{b-1,\ b+1,\ b+2,\ b+3\}$

$$\{\Gamma_1, \Gamma_2, \Gamma_3\} = \{b,\, b+1,\, b+2\}, \qquad \textit{otherwise}. \tag{19}$$

- ***Case*** $L = 4$***:*** *When* $1 < \rho \leq 30$*, the unique optimal (sorted, pairwise–coprime) quadruple is*

$$(\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4) = (2, 3, 5, 7).$$

When $\rho > 30$*, define*

$$b = \min\{n \in \mathbb{Z},\, n \geq 5 : n(n-1)(n-2) \geq \rho\,\}. \tag{20}$$

The corresponding optimal quartets $\{\Gamma_i\}$ *are enumerated in Table II.*

The proof will be provided in Appendix A. The constructions in Theorem 1 are explicit and involve only a few arithmetic operations and comparisons. Hence, for $L = 2, 3$ and 4, the optimal moduli can be computed easily, making them suitable for hardware front-ends.

Example 1. Suppose that $m_{\max} = 100$ and $N_{\text{th}} = 10^6$, yielding $\rho = N_{\text{th}}/m_{max} = 10^4$.

For $L = 3$, we compute $b = 101$ from (16). As b is odd and the fallback condition fails because $(b-2) \cdot b < \rho$ and $(b+1) \bmod 3 = 0$. We therefore adopt the configuration $\{101, 102, 103\}$, which is pairwise coprime and yields a common factor $m = 100/103 \approx 0.97$.

For $L = 4$, we compute $b = 22$. The selected set $\{21, 22, 23, 25\}$ corresponds to **Case C2** in Table II, where $b \bmod 3 = 1$ and $b \bmod 5 \neq 3$. This yields $\Gamma_4 = 25$, giving a common factor $m = 100/25 = 4$.

Example 2. Consider a 3-moduli setting ($L = 3$) with dynamic range threshold $N_{\text{th}} = 2 \times 10^4$ and modulus bound $m_{\max} = 55$, yielding $\lceil \rho \rceil = 364$. We compare the proposed modulus selection strategy against two common alternatives: (*i*) restricting all Γ_i to prime numbers [29], and (*ii*) using the hardware-friendly form $\{2^n-1, 2^n, 2^n+1\}$, commonly used in residue-based data storage [43]. Using Theorem 1, our method yields $(\Gamma_1, \Gamma_2, \Gamma_3) = (19, 20, 21)$ with scaling factor $m = 2.6190$. Among prime-only configurations, the best is $(17, 23, 29)$ with $m = 1.8966$, while the best structured triple is $(31, 32, 33)$, yielding $m = 1.6667$. This implies our design has a 38% improvement over prime-only methods and a 57% improvement over structured digital alternatives.

Hardware-friendly design. A key advantage of the proposed closed-form construction is its compatibility with finite-precision hardware implementations. In practical systems, the moduli m_i are typically realized through analog circuits or digitally controlled elements with limited resolution. Our design permits simple precision management: the scalar m can be truncated (denoted $\hat{m}$) to match hardware precision (e.g., ℓ decimal places), while keeping the Γ_i unchanged. This allows the RCRT formula to remain valid, with only slight degradation in dynamic range due to scaling by $\hat{m}/m$.

Note that some existing works [18] select rational moduli that are not pairwise coprime, leading to modulus values like $\frac{101039}{66}$, $\frac{1076285}{682}$, etc. (see Example D in [18]). These require precise handling of both numerators and denominators, potentially necessitating more complex re-optimization of moduli to meet hardware precision limits.

Remark. For $L = 4$ and even b, the expressions for the optimal solution $\{\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4\}$ in Table II can become lengthy due to the need to account for different ranges of ρ. To simplify the design while maintaining near-optimality, one may instead consider $b' = b+1$ and select the candidate set $\{b'-2,\ b'-1,\ b',\ b'+2\}$ when $b' \bmod 3 \neq 1$, or $\{b'-2,\ b'-1,\ b',\ b'+3\}$ when $b' \bmod 3 = 1$ as in **Case A** of Table II. This heuristic yields simplified selection with performance close to optimal.

For systems that can tolerate one or two additional channels ($L = 5$ or 6), an exact optimization quickly becomes prohibitive, yet a simple heuristic suffices in practice. Starting from the closed-form quartet in Table II, one can append each extra modulus by (*i*) estimating the size that would keep the overall product on the order of $\rho^{1/(L-1)}$, (*ii*) scanning outward for the nearest prime moduli, and (*iii*) updating the cumulative product to calculate the remaining moduli.

IV. Fibonacci-Inspired Two-Moduli Design for Layered RCRT Reconstruction

A. Basics of Fibonacci-like Sequences

As a step beyond the full CRT layer moduli selection in Sec. III, we now consider the design of two-moduli RCRT systems that support *layered reconstruction*. Note that the sequence σ_j in (4) corresponds to the remainder chain of the Euclidean algorithm computing $\gcd(\Gamma_1, \Gamma_2)$. As Γ_1 and Γ_2 are coprime, there exists a finite index K such that $\sigma_{K+1} = 1$. Notably, consecutive Fibonacci numbers (F_{K+3}, F_{K+4}) represent the smallest inputs requiring

exactly $K+1$ Euclidean steps. Leveraging this connection, we introduce Fibonacci-like integer sequences whose algebraic structure guarantees the desired remainder chain.

Definition 2 (Fibonacci-like sequence $\{F_{d,k}\}$)**.** *Let $d \geq 0$ be an integer. The Fibonacci-like sequence $\{F_{d,k}\}$ is defined recursively by*

$$F_{d,0} = d,\ F_{d,1} = 1,\ F_{d,k} = F_{d,k-1} + F_{d,k-2} \quad (k \geq 2) \tag{21}$$

This extends the classical Fibonacci sequence by initializing with seed d at $k = 0$; seed-parameterized variants of this kind have been investigated in the Fibonacci literature [?], [44].

Remark. When $d = 0$, the sequence $\{F_{d,k}\}$ reduces to the standard Fibonacci sequence $(0, 1, 1, 2, 3, \cdots)$, i.e., $F_{0,k} = F_k$. For $d = 1$, it becomes a one-step right shift of the standard sequence: $F_{1,k} = F_{0,k+1}$. When $d = 2$, the sequence coincides with the Lucas numbers [45]. The generalized sequence $\{F_{d,k}\}$ preserves key number-theoretic properties of the Fibonacci sequence, such as the coprimality of consecutive terms: $\gcd(F_{d,k}, F_{d,k+1}) = 1$. Since the recurrence relation remains unchanged, i.e., $F_{d,k} = F_{d,k-1} + F_{d,k-2}$, its asymptotic growth is exponential and governed by the golden ratio φ:

$$\lim_{k\to\infty} \frac{F_{d,k+l}}{F_{d,k}} = \varphi^l. \tag{22}$$

We next prove two key algebraic properties of $\{F_{d,k}\}$ instrumental for our recursive construction.

Lemma 2 (Properties of the Fibonacci-like Sequence $\{F_{d,k}\}$)**.** *Let $d \in \mathbb{Z}_{\geq 0}$, and let $\{F_{d,k}\}$ denote the Fibonacci-like sequence in Definition 2. Then the following hold:*

(i) ***Linear in seed property****: For all $k \geq 2$,*

$$F_{d,k} = F_{1,k-1} + d\, F_{1,k-2}. \tag{23}$$

(ii) ***Mixed d'Ocagne identity****: For $s, t \in \mathbb{Z}$ and $s \geq t \geq 1$,*

$$F_{d,s}F_{1,t} - F_{d,s+1}F_{1,t-1} = (-1)^t F_{d,s-t}. \tag{24}$$

Proof: (i) We prove by induction on $k \geq 2$. Base case $k = 2$: $F_{d,2} = F_{d,1} + F_{d,0} = 1 + d = F_{1,1} + dF_{1,0}$. Assume the identity holds for k and $k-1$. Then:

$$\begin{aligned} F_{d,k+1} &= F_{d,k} + F_{d,k-1} \\ &= \big(F_{1,k-1} + d\, F_{1,k-2}\big) + \big(F_{1,k-2} + d\, F_{1,k-3}\big) \\ &= F_{1,k-1} + F_{1,k-2} + d\,\big(F_{1,k-2} + F_{1,k-3}\big) \\ &= F_{1,k} + dF_{1,k-1}. \end{aligned}$$

Hence, by the recurrence of the Fibonacci sequence, the identity holds for all $k \geq 2$.

(ii) By the classical d'Ocagne's identity [44], [46], for $a, b \in \mathbb{Z}_{>0}$ and $(a \geq b)$, the Fibonacci sequence $F_{0,k}$ satisfies

$$F_{0,a+1}F_{0,b+1} - F_{0,a+2}F_{0,b} = (-1)^b F_{0,a-b+1}, \tag{25}$$

Since $F_{1,k} = F_{0,k+1}$, this implies

$$F_{1,a}F_{1,b} - F_{1,a+1}F_{1,b-1} = (-1)^b F_{1,a-b}. \tag{26}$$

That is, (24) holds for $d = 1$. When $d > 1$, applying (23) for $F_{d,s}$ and $F_{d,s+1}$, the left-hand side (LHS) of (24) can be written as

$$\begin{aligned}
&F_{d,s}F_{1,t} - F_{d,s+1}F_{1,t-1} \\
=&(F_{1,s-1} + d\,F_{1,s-2})F_{1,t} - (F_{1,s} + d\,F_{1,s-1})F_{1,t-1} \\
=&[F_{1,s-1}F_{1,t} - F_{1,s}F_{1,t-1}] + d[F_{1,s-2}F_{1,t} - F_{1,s-1}F_{1,t-1}].
\end{aligned}$$

Using (26), the above can be simplified to

$$(-1)^t F_{1,s-t-1} + d(-1)^t F_{1,s-t-2} = (-1)^t F_{d,s-t},$$

which completes the proof. ■

B. Construction of Moduli for Layered-Design

We now formalize the two–moduli design for *layered RCRT*. Select two moduli

$$\{m_1, m_2\} = \{m\,\Gamma_1,\ m\,\Gamma_2\}, \qquad \Gamma_1 < \Gamma_2,$$

to support one full CRT layer and K additional robust layers while satisfying Eqs. (9)–(11). Our goal is to *maximize* the guaranteed full CRT layer error tolerance, which is achieved by maximizing m. Since the modulus bound implies $m = m_{\max}/\Gamma_2$, this is equivalent to minimizing Γ_2. Accordingly, the design problem is

$$\min_{\Gamma_1,\Gamma_2\in\mathbb{Z}} \ \Gamma_2 \tag{27}$$

subject to

$$\Gamma_2 \ > \ \Gamma_1 \ \geq \ \rho \ > \ 1, \quad \Gamma_\ell \in \mathbb{Z}\ (\ell = 1, 2), \tag{28}$$

$$\gcd(\Gamma_1, \Gamma_2) = 1, \tag{29}$$

$$\sigma_{K+1} = 1, \tag{30}$$

where ρ and the remainder chain $\{\sigma_k\}$ are defined in (13) and (4), respectively. Minimizing Γ_2 under (28)–(30) therefore maximizes m and hence the decoder's full CRT layer error tolerance, while ensuring exactly K robust layers.

A key fact from the analysis of the Euclidean algorithm [44], [47] is that the consecutive Fibonacci pair $(F_{1,K+2}, F_{1,K+3})$ is the smallest positive integer pair whose Euclidean algorithm takes exactly $K+1$ divisions. Hence, among all pairs that realize the required depth $\sigma_{K+1} = 1$, a consecutive Fibonacci choice minimizes Γ_2, provided that the range constraint $\Gamma_1 \geq \rho$ is already met. This leads to an immediate solution when $\rho \leq F_{1,K+2}$, as stated in the following proposition.

Proposition 3. *Fix $K \geq 1$. If $\rho \leq F_{1,K+2}$, then an optimal solution of* (27) *subject to* (28)–(30) *is*

$$\Gamma_1 = F_{1,K+2}, \qquad \Gamma_2 = F_{1,K+3}.$$

A convenient estimate for the smallest layer index K^* with $\rho \leq F_{1,K^*+2}$ is

$$K^* \;=\; \max\left\{1,\; \left\lceil \frac{\ln(\rho\sqrt{5})}{\ln\varphi} - 3 \right\rceil \right\}, \qquad \varphi = \tfrac{1+\sqrt{5}}{2}. \tag{31}$$

Proof: A classical fact on Euclidean algorithm (see, e.g., [47]) is that the smallest positive integers yielding exactly $K+1$ divisions and terminating at 1 are consecutive Fibonacci numbers $(F_{0,K+3}, F_{0,K+4})$. Using $F_{1,k} = F_{0,k+1}$ gives $(\Gamma_1, \Gamma_2) = (F_{1,K+2}, F_{1,K+3})$, which minimizes Γ_2 among all pairs meeting the depth constraint $\sigma_{K+1} = 1$ and $\Gamma_1 \geq \rho$. For (31), apply Binet's approximation $F_{1,k} \approx \varphi^{k+1}/\sqrt{5}$ and solve $F_{1,K^*+2} \geq \rho$ for K^*. ■

Theorem 2 provides a constructive solution when $\rho > F_{1,K+2}$.

Theorem 2 (Fibonacci-Inspired Moduli Construction)**.** *Let $\{F_{d,k}\}$ be the d-seed Fibonacci sequence given in Definition 2. Fix $K \geq 1$ and let $\rho = N_{th}/m_{\max}$ be given with $\rho > F_{1,K+2}$. For each integer seed $d \geq 1$, set*

$$\zeta_d = \lceil (\rho - F_{d,K})/F_{d,K+1} \rceil, \tag{32}$$

$$\Gamma_1(d) = \zeta_d F_{d,K+1} + F_{d,K},\ \Gamma_2(d) = \Gamma_1(d) + F_{d,K+1}. \tag{33}$$

(i) Remainder Chain and Dynamic Range: *The pair $(\Gamma_1(d), \Gamma_2(d))$ is coprime with $\Gamma_1(d) \geq \rho$, having Euclidean remainders:*

$$\sigma_j = F_{d,K+2-j}, \quad 1 \leq j \leq K+1. \tag{34}$$

The dynamic-range breakpoints P_j ($1 \leq j \leq K$) are:

$$P_j = \begin{cases} m\Gamma_1(d) F_{\zeta_d, 2j_0}, & j = 2j_0 - 1, \\ m\Gamma_2(d) F_{\zeta_d - 1, 2j_0+1}, & j = 2j_0, \end{cases} \tag{35}$$

with $P_{K+1} = \Gamma_1(d)\Gamma_2(d)m$. Robust recovery holds for $x \in [0, P_j)$ when $|e_1 - e_2| < m\sigma_j/2$.

(ii) Optimal Seed Selection: *For $\Gamma_1(d)$ and $\Gamma_1(d)$ defined in* (33)*, the minimal Γ_2 is obtained via:*

$$(\Gamma_1^\star, \Gamma_2^\star) = \arg\min_{1 \leq d \leq 3} \Gamma_2(d),$$

where testing $d = 1, 2, 3$ suffices, i.e., no larger seed yields smaller Γ_2 in (33)*, thus maximizing $m = m_{\max}/\Gamma_2^\star$.*

The proof is in Appendix B.

Remark. When $\rho \leq F_{1,K+2}$, $(F_{1,K+2}, F_{1,K+3})$ is optimal (no search is needed). For $\rho > F_{1,K+2}$, each seed d defines ζ_d via (32) to ensure $\Gamma_1(d) \geq \rho$, yielding candidate pairs $(\Gamma_1(d), \Gamma_2(d))$. Theorem 2 guarantees that the family-optimal pair is found by evaluating only $d = 1, 2, 3$ via (32) and (33), requiring just three comparisons.

Corollary 1 next shows that when $K \leq 2$, this construction actually yields *globally optimal* solutions with deterministic seed selection of d.

TABLE III: Examples of (Γ_1, Γ_2) under different ρ and K

ρ	K	d	Γ_1	Γ_2	σ_j: $\sigma_1, \sigma_2, \ldots, \sigma_{K+1}$	ζ_d
150	1	1	151	153	(2, 1)	75
	2	1	152	155	(3, 2, 1)	50
	3	1	153	158	(5, 3, 2, 1)	30
	4	1	157	165	(8, 5, 3, 2, 1)	19
		3	150	161	(11, 7, 4, 3, 1)	13
250	6	1	265	286	(21, 13, 8, 5, 3, 2, 1)	12
		2	250	279	(29, 18, 11, 7, 4, 3, 1)	8

Corollary 1 (Closed-Form Global Optima for $K \leq 2$)**.** *For $\rho > F_{1,K+2}$ and $K \in \{1, 2\}$, Theorem 2's construction achieves global optimality with:*

(i) $K = 1$: Always use $d = 1$ with

$$\zeta_1 = \lceil (\rho - 1)/2 \rceil, \quad \Gamma_1 = 2\zeta_1 + 1, \quad \Gamma_2 = 2\zeta_1 + 3$$

(ii) $K = 2$: For $\lceil \rho \rceil = 12\ell + 3$ ($\ell \geq 1$), take $d = 2$:

$$\zeta_2 = 3\ell, \quad \Gamma_1 = 4\zeta_2 + 3, \quad \Gamma_2 = 4\zeta_2 + 7$$

Otherwise, use $d = 1$:

$$\zeta_1 = \lceil (\rho - 2)/3 \rceil, \quad \Gamma_1 = 3\zeta_1 + 2, \quad \Gamma_2 = 3\zeta_1 + 5$$

In all cases, Γ_2 is globally minimized (maximizing m).

The proof is given in Appendix C.

Example 3. Table III illustrates the construction for various values of ρ and K. Although Theorem 2 requires checking $d = 1, 2, 3$ for optimality, the case $d = 1$ alone yields near-optimal results across all tested scenarios, achieving an excellent trade-off between performance and simplicity.

Remark. Corollary 1 guarantees global optimality for $K \leq 2$, but *not* for $K \geq 3$. For instance, when $K = 3$ and $\rho = 19$, Theorem 2 with $d = 1$ yields the near-optimal pair $(23, 28)$, while $(19, 26)$ has a smaller Γ_2 with the same $K+1 = 4$ steps. Remarkably, even in this case, the $d = 1$ construction stays within 8% of the optimal Γ_2. Although global optimality for $K \geq 3$ remains open, the method's efficiency and consistently near-optimal performance make it practically attractive.

V. Layer-Wise Performance Analysis: Scaling Laws and Statistical Behavior

A. Layer-Wise Scaling of Dynamic Range and Error Bounds

To understand how the number of robust layers K influences the system's performance, we theoretically analyze the dynamic range and error tolerance provided by our layered construction. This cross-layer analysis characterizes how both dynamic range and error tolerance scale with depth, covering the full CRT layer as well as intermediate robust layers, and reveals the trade-offs inherent in choosing K.

Full CRT Layer: From Sec. III, we recall the moduli definitions: $m_1 = m\,\Gamma_1, \quad m_2 = m\,\Gamma_2 = m_{\max}$, where $m_{\max}$ is the hardware-constrained largest modulus. The scaling factor is therefore $m = m_{\max}/\Gamma_2$, and for the final reconstruction layer ($j = K{+}1$), we have:

$$\tau_{K+1} = \frac{m}{4} = \frac{m_{\max}}{4\,\Gamma_2}, \quad P_{K+1} = m\,\Gamma_1\Gamma_2 = \Gamma_1\,m_{\max}. \tag{36}$$

1) Exponential Scaling Regime: From proposition 3, we know that when $K > K^*$, the optimal pair $(\Gamma_1, \Gamma_2) = (F_{1,K+2}, F_{1,K+3})$. By (36), $P_{K+1} \propto \Gamma_1$ and $\tau_{K+1} \propto \Gamma_2^{-1}$, which implies that

$$P_{K+1} \propto \varphi^K, \quad \tau_{K+1} \propto \varphi^{-K},$$

illustrating a controlled trade-off between dynamic range and robustness depth.

2) Small-Depth Regime ($K < 3$): When $K = 0$, we recover the classical CRT with adjacent coprime moduli: $\Gamma_1 = \lceil \rho \rceil$, $\Gamma_2 = \Gamma_1 + 1$. For $K = 1, 2$, Corollary 1 provides closed-form constructions with Γ_i differing from the $K = 0$ baseline by small offsets, yielding similar dynamic range and noise tolerance at full CRT layer.

Intermediate Layers: Theorem 2 indicates that the error tolerance bound $T(x)$ as a function of signal amplitude x follows a staircase profile

$$T(x) = \tau_j \quad \text{if} \quad P_{j-1} \le x < P_j, \qquad P_0 := 0. \tag{37}$$

in which P_j takes the form of (35) and the per-residue error bound τ_j is given by

$$\tau_j = \frac{m}{4}\sigma_j = \frac{m}{4}F_{d,K+2-j}. \tag{38}$$

The next Corollary describes how P_j and τ_j $(1 \le j \le K)$ evolve across K robustness layers.

Corollary 2 (Scaling Laws for Intermediate Layers)**.** *For the layered construction in Theorem 2 with $K \ge 1$:*

- *Error bounds converge as:*

$$\frac{\tau_j}{\tau_{j+1}} = \frac{F_{d,K+2-j}}{F_{d,K+1-j}} \to \varphi \quad (j \textit{ fixed}, K \to \infty) \tag{39}$$

- *Plateaux ratios satisfy:*

$$P_2/P_1 = \Gamma_2/\Gamma_1, \quad K \ge 2 \tag{40}$$

$$P_1/P_{K+1} \approx 1/F_{d,K+1}, \quad \zeta_d \gg 1 \tag{41}$$

$$P_K/P_{K+1} < 1/(d+1) \tag{42}$$

$$2 < P_{j+2}/P_j < 3 \quad (1 \le j \le K-2,\ K \ge 3) \tag{43}$$

$$P_{j+2}/P_j \to \varphi^2 \approx 2.618 \quad (j \to \infty) \tag{44}$$

Proof:

(*i*) Eq. (39) is straightforward from (38) and (22).

(*ii*) When $K \geq 2$, for the first two robust layers, (35) implies

$$P_1 = m\Gamma_1 F_{\zeta_d - 1,3}, \quad P_2 = m\Gamma_2 F_{\zeta_d,2}. \tag{45}$$

By definition of Fibonacci-like sequence in (21), one can calculate that $F_{\zeta_d-1,3} = F_{\zeta_d,2} = \zeta_d + 1$, indicating (40) holds for all $K \geq 2$.

(*iii*) Combining the closed form of P_1 in (45) with $F_{\zeta_d-1,3} = \zeta_d + 1$ and $P_{K+1} = m\Gamma_1\Gamma_2$ produces

$$\frac{P_1}{P_{K+1}} = \frac{\zeta_d + 1}{(\zeta_d + 1)F_{d,K+1} + F_{d,K}} \approx \frac{1}{F_{d,K+1}}, \tag{46}$$

where the approximation $\approx$ assumes $(\zeta_d + 1)\, F_{d,K+1} \gg F_{d,K}$ for typical $\zeta_d \gg 1$ or large K.

(iv) Substituting $j = K{+}1$ into (7) gives

$$N_{K+1} = N_{K-1} + \left\lfloor \frac{\sigma_K}{\sigma_{K+1}} \right\rfloor (N_K - \sigma_K).$$

Using $\sigma_j = F_{d,K+2-j}$, we have $\sigma_K = F_{d,2} = d{+}1$ and $\sigma_{K+1} = 1$, hence

$$N_{K+1} = N_{K-1} + (d{+}1)(N_K - 1).$$

Since $\{N_k\}$ is monotonically increasing in k, we have $N_{K-1} \geq N_0 = \Gamma_2$ for $K \geq 1$. From (33), $\Gamma_2 > F_{d,K+1} \geq F_{d,2} = d{+}1$, so $N_{K-1} > d{+}1$ and therefore

$$N_{K+1} = N_{K-1} + (d{+}1)(N_K - 1) > (d{+}1) + (d{+}1)(N_K - 1) = (d{+}1)N_K.$$

Recalling $P_{K+1} = mN_{K+1}$ and $P_K = mN_K$, it follows that $P_{K+1} > (d{+}1)P_K$, which proves (42).

(v) From (35) and the recurrence $F_{d,k+2} = F_{d,k+1} + F_{d,k} = 2F_{d,k} + F_{d,k-1}$, we obtain

$$\frac{P_{j+2}}{P_j} = \begin{cases} \dfrac{F_{\zeta_d,\, 2j_0+2}}{F_{\zeta_d,\, 2j_0}} = 2 + \dfrac{F_{\zeta_d,\, 2j_0-1}}{F_{\zeta_d,\, 2j_0}}, & j = 2j_0 - 1, \\ \dfrac{F_{\zeta_d-1,\, 2j_0+3}}{F_{\zeta_d-1,\, 2j_0+1}} = 2 + \dfrac{F_{\zeta_d-1,\, 2j_0}}{F_{\zeta_d-1,\, 2j_0+1}}, & j = 2j_0. \end{cases}$$

For $d \geq 1$ and $k \geq 1$, the Fibonacci-like sequence is strictly increasing in k, i.e, $0 < F_{d,k}/F_{d,k+1} < 1$. Hence $2 < P_{j+2}/P_J < 3$, which proves (43). Finally, using the above expression for P_{j+2}/P_j together with the growth law (22) (for which $F_{d,k+2}/F_{d,k} \to \varphi^2$ as $k \to \infty$), we obtain (44). ■

Example 4. Table IV evaluates Corollary 2 for a layered RCRT system with $\Gamma_1 = 34$, $\Gamma_2 = 47$ (obtained with $d = 1$), and recursion depth $K = 5$. The ratios $\sigma_1/\sigma_2 = 1.625$ and $\sigma_2/\sigma_3 = 1.6$ closely approach φ, verifying (39). The dynamic range ratio $P_1/P_{K+1} = 0.0638$ agrees with $1/F_{1,6} = 1/13 \approx 0.0769$ in (41), while $P_K/P_{K+1} = 0.383 < 1/(d+1) = 0.5$, confirming (42).

Example 5. Given $N_{\text{th}} = 3000$ and $m_{\max} = 200$ (i.e., $\rho = 150$), we use Theorem 2 to construct (Γ_1, Γ_2) for $0 \leq K \leq 15$.

TABLE IV: Verification of Scaling Laws in Layered RCRT for $\Gamma_1 = 34$ and $\Gamma_2 = 47$.

j	σ_j	σ_j/σ_{j+1}	P_j	P_{j+2}/P_j
1	13	$\sigma_1/\sigma_2 = 1.625$	102	$P_3/P_1 = 2.356$
2	8	$\sigma_2/\sigma_3 = 1.6$	141	$P_4/P_2 = 2.667$
3	5	$\sigma_3/\sigma_4 = 1.667$	238	$P_5/P_3 = 2.57$
4	3	$\sigma_4/\sigma_5 = 1.5$	376	-
5	2	$\sigma_5/\sigma_6 = 2$	612	-
6	1	-	1598	-

Fig. 2a plots P_{K+1} and τ_{K+1} vs. K. The critical depth from (31) is $K^* = 10$. For $K \geq K^*$ the curves follow the predicted $P_{K+1} \propto \varphi^K$ and $\tau_{K+1} \propto \varphi^{-K}$. On the other hand, for $K \leq 3$ they remain similar to the $K = 0$ baseline, showing that one or two robust layers incur nearly no full-range loss.

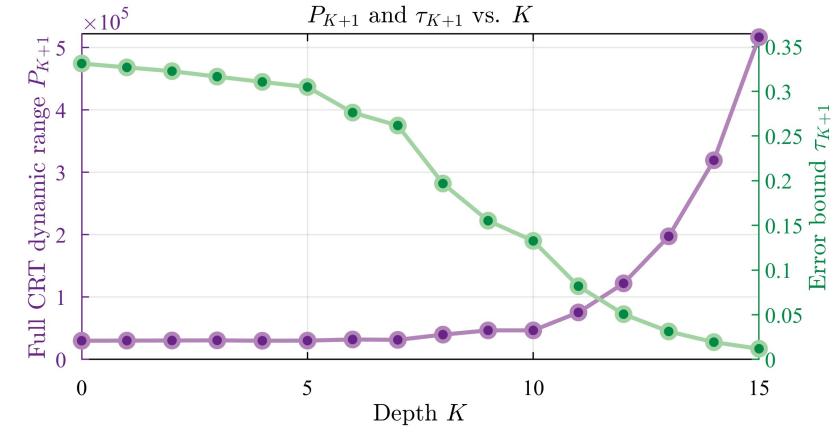
Fig. 2b ($K \leq 3$) and Fig. 2c ($K > 3$) depict the staircase error bound $T(x)$ of (37). Each step spans $[P_{j-1}, P_j)$ and has height $\tau_j = \frac{m}{4}\sigma_j$. Successive ratios satisfy $\tau_j/\tau_{j+1} \approx \varphi$ and $2 < P_{j+2}/P_j < 3$. As can be observed, small K yields wide plateaux, whereas large K produces a comb-like staircase whose ever-narrower steps cluster near the origin, visually confirming the range–robustness trade-off in Corollary 2.

B. Statistical Effects on Reconstruction

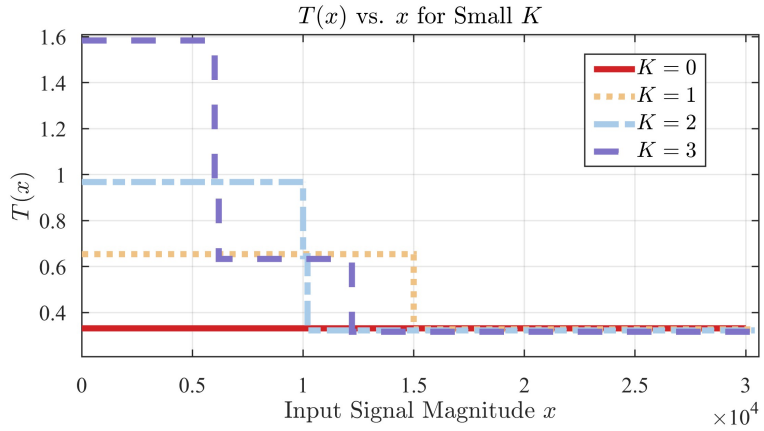
In this subsection, we present a statistical analysis of the layered reconstruction performance under noisy residue observations. The goal is to evaluate the probability of successful reconstruction when the input signal x is drawn from a continuous distribution and the observed remainders are corrupted by independent additive noise. We assume that x is a non-negative real-valued signal with distribution supported on $[0, P_{K+1})$ with very high probability (e.g., probability $\geq 1 - 10^{-5}$).

To quantify decoding performance under noise, we follow the layered reconstruction strategy of [29], [35], where the estimate $\tilde{r}_1 - \tilde{r}_2$ is matched to the nearest slanted line associated with valid folding integers. Decoding succeeds in layer j if *(i)* the signal x lies in the dynamic range interval $[P_{j-1}, P_j)$, and *(ii)* the remainder difference satisfies $|e_1 - e_2| < m\sigma_j/2$. This yields a lower bound on the success rate as given below.

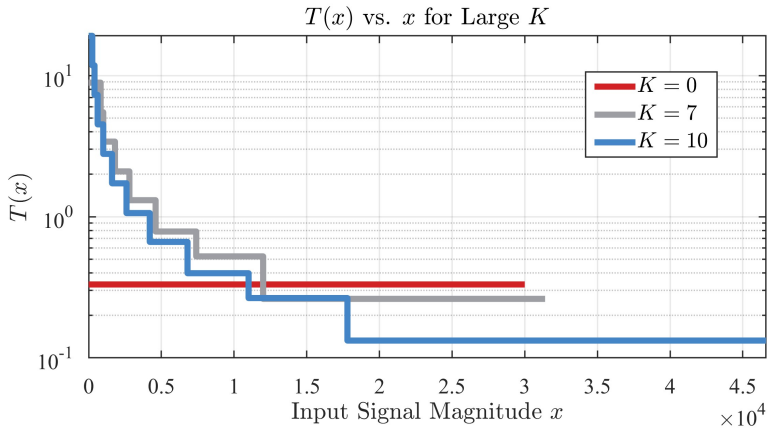
Proposition 4 (Lower bound on success probability (pairwise-difference decoder))**.** *Consider two-moduli RCRT with $m_\ell = m\,\Gamma_\ell$ ($\ell = 1, 2$), where $\Gamma_1 < \Gamma_2$ are coprime, yielding K robust layers followed by one full CRT layer. Let x be a real-valued random signal drawn from a continuous distribution and assume x is independent of the noise terms e_1, e_2, which are independent of each other. Let $\{P_j\}_{j=0}^{K+1}$ be the dynamic-range breakpoints with $P_0 = 0$ (as in* (7)*), let $\{\sigma_j\}_{j=1}^{K+1}$ be the Euclidean-remainder sequence from* (4)*, and define the layerwise tolerance*



(a)



(b)



(c)

Fig. 2: Error bound vs. dynamic range for the proposed K-layer robust system. **(a)** Full CRT layer: P_{K+1} and τ_{K+1} vs K. **(b)** $T(x)$ vs. x for $K = 0, 1, 2, 3$. **(c)** $T(x)$ vs. x for $K = 0, 7, 10$.

$\tau_j = \frac{m\,\sigma_j}{4}$ $(1 \le j \le K+1)$. *Then the reconstruction success probability satisfies*

$$\eta_{\text{succ}} \;\ge\; \sum_{j=1}^{K+1} \mathbb{P}(\,|e_1 - e_2| < 2\,\tau_j\,)\;\mathbb{P}(\,x \in [P_{j-1}, P_j)\,)\,, \tag{47}$$

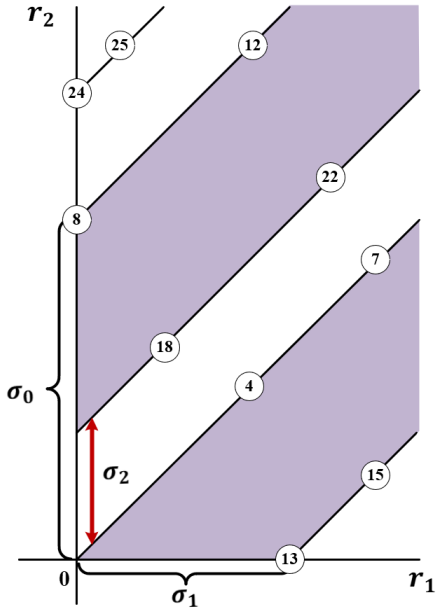


Fig. 3: Residue space (r_1, r_2) for moduli pair $(m_1, m_2) = (8, 13)$ with $K = 3$ robust layers. The diagram shows the second layer ($j = 2$), where the theoretical minimum line spacing is $\sigma_2 = 3$, and the dynamic range is $x \in [0, 26)$. Each slanted line represents a unique folding pair (n_1, n_2), forming a valid decoding region. The shaded area exhibits a gap of $\sigma_0 - \sigma_2 = \sigma_1 = 5 > \sigma_2$, revealing non-uniform spacing caused by the residue space geometry.

where $\mathbb{P}(\cdot)$ denotes probability; the first factor is taken with respect to the noise variables (e_1, e_2) and the second with respect to x.

Proof: On the event $\{x \in [P_{j-1}, P_j)\}$, the closed-form pairwise-difference decoder succeeds whenever $|e_1 - e_2| < \frac{m\sigma_j}{2} = 2\tau_j$ (cf. Eq. (5)). Taking the union over disjoint layer intervals and using independence of x and (e_1, e_2) yields (47) by the law of total probability. ■

Typical Signal Priors: In many RCRT applications, the input x follows a known prior distribution, depending on the sensing or communication context. For example, phase retrieval or frequency estimation problems often assume uniform distribution, while communication or radar signals processed by modulo ADCs may follow Rayleigh, exponential, or folded-Gaussian distributions. The interval probability $\mathbb{P}(x \in (P_{j-1}, P_j])$ admits a closed-form expression:

- **Uniform** ($x \sim \mathcal{U}(0, P_{K+1})$): $\dfrac{P_j - P_{j-1}}{P_{K+1}}$.
- **Rayleigh** ($x \sim \text{Rayleigh}(\beta)$, typical for envelope of complex Gaussian signals): $\exp\left(-\frac{P_{j-1}^2}{2\beta^2}\right) - \exp\left(-\frac{P_j^2}{2\beta^2}\right)$.
- **Exponential** ($x \sim \text{Exp}(\lambda)$): $\exp\left(-\frac{P_{j-1}}{\lambda}\right) - \exp\left(-\frac{P_j}{\lambda}\right)$.
- **Folded–Gaussian** (magnitude of real Gaussian signals, $x \sim |\mathcal{N}(0, \vartheta^2)|$): $\text{erf}\left(\frac{P_j}{\sqrt{2}\vartheta}\right) - \text{erf}\left(\frac{P_{j-1}}{\sqrt{2}\vartheta}\right)$.

Typical Noise Models: Here, we consider two typical noise models.

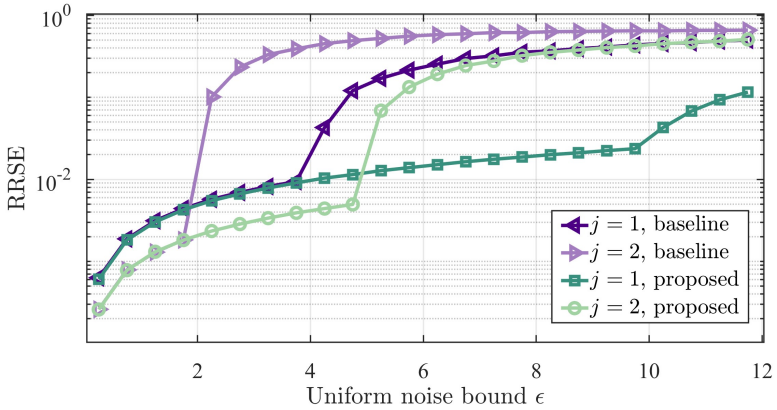


Fig. 4: RRSE vs ϵ for two-moduli system with $K = 1$, $N_{\text{th}} = 680$, and $m_{\max} = 136$, where remainder errors $e \sim \mathcal{U}(-\epsilon, \epsilon)$, $\epsilon \in [0, 12]$. **(a)** Baseline design from [35]: $(\Gamma_1, \Gamma_2, m) = (5, 17, 8)$, yielding $(P_1, \tau_1) = (285, 4)$, $(P_2, \tau_2) = (680, 2)$. **(b)** Proposed design: $(\Gamma_1, \Gamma_2, m) = (5, 7, 19\frac{3}{7})$, yielding $(P_1, \tau_1) = (291\frac{3}{7}, 9\frac{5}{7})$ and $(P_2, \tau_2) = (680, 4\frac{6}{7})$.

Gaussian Noise: $e_i \sim \mathcal{N}(0, \varsigma^2)$ independently. In this case,

$$\mathbb{P}(|e_1 - e_2| < 2\tau_j) = \text{erf}\left(\frac{\tau_j}{\sqrt{2}\varsigma}\right), \tag{48}$$

where erf$(\cdot)$ denotes the error function.

Uniform Noise: $e_i \sim \mathcal{U}(-\varepsilon, \varepsilon)$ independently. Then, $e_1 - e_2 \sim$ Triangular$(-2\varepsilon, 2\varepsilon)$, i.e.,

$$\mathbb{P}(|e_1 - e_2| < 2\tau_j) = \begin{cases} 1, & \tau_j > \varepsilon, \\ \frac{2\tau_j}{\varepsilon} - \frac{\tau_j^2}{\varepsilon^2} & \tau_j \leq \varepsilon. \end{cases} \tag{49}$$

System Level Design: The analytical expressions for various signal/noise distributions can be directly substituted into (47) to compute theoretical success probabilities, enabling system designers to estimate performance without exhaustive simulations. These closed-form approximations guide parameter selection, including the number of robustness layers K, moduli pair (Γ_1, Γ_2), and error threshold $m\sigma_j/2$ per layer. For instance, Rayleigh-distributed signal magnitudes concentrate probability mass near the origin, making lower robustness layers (small j) most critical for reconstruction.

However, the lower bound in Proposition 4 will *become loose* for large K due to non-uniform spacing of valid decoding regions. As shown in Fig. 3, slanted line gaps are non-uniform for small j when $K \geq 3$, and larger gaps between adjacent lines reduce captured probability mass despite the minimum separation being lower bounded by $m\sigma_j$. This will be verified through simulations in Sec. VI.

VI. Simulations

In this section, we present simulation results to evaluate the effectiveness of the proposed moduli selection methods and to analyze the robustness performance of layered RCRT systems under different signal and noise models.

TABLE V: Comparison of Random and Optimal Moduli Selection under Different L and ρ

L	ρ	Selection Strategy	β_{succ}	$[\tau_{\min}, \tau_{\max}]$	τ_{avg}
3	100	Random	30.07%	$[5, 19.23]$	6.51
		Optimal	1	19.23	19.23
	200	Random	28.1%	$[2.5, 7.35]$	3.17
		Optimal	1	7.35	7.35
4	1000	Random	35.24%	$[2.5, 17.86]$	3.27
		Optimal	1	19.23	19.23
	2000	Random	34.26%	$[1.25, 7.35]$	1.62
		Optimal	1	8.33	8.33

Simulation 1. We evaluate the optimal moduli construction in Theorem 1 against randomly chosen moduli. We fix $N_{\text{th}} = 10^5$ and test two scenarios: $L = 3$ with $\rho \in \{100, 200\}$, and $L = 4$ with $\rho \in \{1000, 2000\}$. For each case, we perform 10^5 Monte Carlo trials to estimate the success rate β_{succ} of random modulus selection in satisfying both the pairwise coprimality constraint (9) and the dynamic range requirement (11). For $L = 3$, three integers are drawn uniformly at random from $[2, 100]$. For $L = 4$, three odd integers and one even integer are sampled from the same range to ensure parity diversity.

Table V summarizes the results. Random selection exhibits low success rates and poor average robustness. While optimal bounds are occasionally achieved for $L = 3$, the average τ remains low. For $L = 4$, the success rate is slightly higher due to the imposed parity diversity, but achieving the optimal bound becomes even more difficult, and the average τ further decreases.

Simulation 2. We revisit Example 1 from [35], which uses moduli $(\Gamma_1, \Gamma_2) = (5, 17)$ and a common factor $m = 8$, yielding a two-layer system with $(P_1, \tau_1) = (285, 4)$ and $(P_2, \tau_2) = (680, 2)$. Under the same dynamic range $N_{\text{th}} = \Gamma_1\Gamma_2 m = 680$ and modulus bound $m_{\max} = \Gamma_2 m = 136$, our proposed design in Theorem 2 produces $(\Gamma_1, \Gamma_2) = (5, 7)$ and $m = \frac{136}{7} = 19\frac{3}{7}$, resulting in $(P_1, \tau_1) = (291\frac{3}{7}, 9\frac{5}{7}))$ and $(P_2, \tau_2) = (680, 4\frac{6}{7})$. Relative to the baseline from [35], the optimized moduli nearly double the tolerance at both layers, with negligible change in P_1 and no loss in P_2.

To empirically verify the improvement, we carry out Monte Carlo simulations under both configurations. Both settings adopt the same two-level decoding: Algorithm 1 from [35] is used at the first layer, and the closed-form RCRT in [12] at the second. In each trial, the ground-truth x is uniformly drawn from $[1, P_j)$, with remainder noise sampled from $[-\epsilon, \epsilon]$, $\epsilon \in (0, 12]$. The Root Relative Squared Error (RRSE) over $R = 10^4$ Monte Carlo trials is

given by

$$\text{RRSE} = \sqrt{\frac{\sum_{i=1}^{R}(x_i - \tilde{x}_i)^2}{\sum_{i=1}^{R} x_i^2}}, \tag{50}$$

where x_i and $\tilde{x}_i$ denote the true and reconstructed values in the ith trial. As shown in Fig. 4, the proposed moduli improve robustness at both levels, doubling the error tolerance with similar P_ℓ ($\ell = 1, 2$). This confirms the practical advantage of our design under fixed constraints.

Simulation 3. We study how K affects reconstruction under Rayleigh-distributed inputs: $x \sim \text{Rayleigh}(360)$, with dynamic range $N_{\text{th}} = 1800$ (outlier probability approximately 3.73×10^{-6}). The modulus bound is $m_{\max} = 120$, yielding $\rho = N_{\text{th}}/m_{\max} = 15$, and $K^* = 5$ via (31). Moduli pairs (Γ_2, Γ_1) are selected using Theorem 1 for $K = 0$ and Theorem 2 for $K \in \{1, 2, 3, 4, 10\}$.

The remainder noise e_i ($i = 1, 2$) is drawn either from a zero-mean Gaussian distribution $e_i \sim \mathcal{N}(0, \varsigma^2)$ or a uniform distribution $e_i \sim \mathcal{U}(-\epsilon, \epsilon)$, where $\varsigma, \epsilon \in [0, 6]$ with a step size of 0.5. For reconstruction, the RCRT from [12] is used at the final layer ($j = K + 1$). For $K \geq 1$, layers $j = 1$ and $2 \leq j \leq K$ are decoded via Algorithms 1 and 2 of [35], respectively. Each success rate η_{succ} is estimated from 10^5 Monte Carlo trials.

Fig. 5 presents both theoretical predictions (solid lines) and empirical results (markers) for overall success probability as noise intensity increases. The left plot corresponds to Gaussian noise (parameterized by standard deviation ς), while the right shows uniform noise (with amplitude bound ϵ). The insets zoom in on the high-success region. From this figure, one can observe:

- For small noise (e.g., $\varsigma \lesssim 1$, $\epsilon \lesssim 1.5$), all configurations achieve near-perfect success.
- As noise increases, adding robust layers ($K \geq 1$) exhibit slower degradation and outperform the baseline $K = 0$ by a wide margin.
- For $K \leq 2$, theoretical bounds closely match the simulation results. For larger K, the empirical performance increasingly exceeds the bound, highlighting its looseness as K increases, a behavior predicted by our earlier analysis.
- The most substantial gains occur for $K = 1$ or 2. Beyond $K = 3$, improvements are not obvious due to the geometric narrowing of admissible plateaux ($P_{j+2}/P_j \to \varphi^2$).

Analogy to μ-law and A-law companding. Classical μ-law and A-law quantizers apply a logarithmic companding curve so that small amplitudes receive finer resolution and large amplitudes coarser resolution. The layered RCRT architecture exhibits a similar non-uniform treatment in the remainder domain. Its staircase error-tolerance curve $T(x)$ takes higher values for small $|x|$ and progressively smaller values as it $|x|$ increases, while the dynamic-range intervals $[P_{j-1}, P_j)$ behave conversely: narrow near the origin and wider at large magnitude. Hence, low-amplitude samples enjoy large error margins but occupy short ranges, whereas high-amplitude samples see tighter margins over longer ranges. This built-in "unequal error protection" is well matched to sources such as speech, audio, or communication signals, whose probability density of signal magnitude is high near zero. Choosing one or two robust layers ($K = 1$ or 2) therefore protects the portion of the signal that occurs most frequently, much as the knee of a companding curve preserves small-signal fidelity.

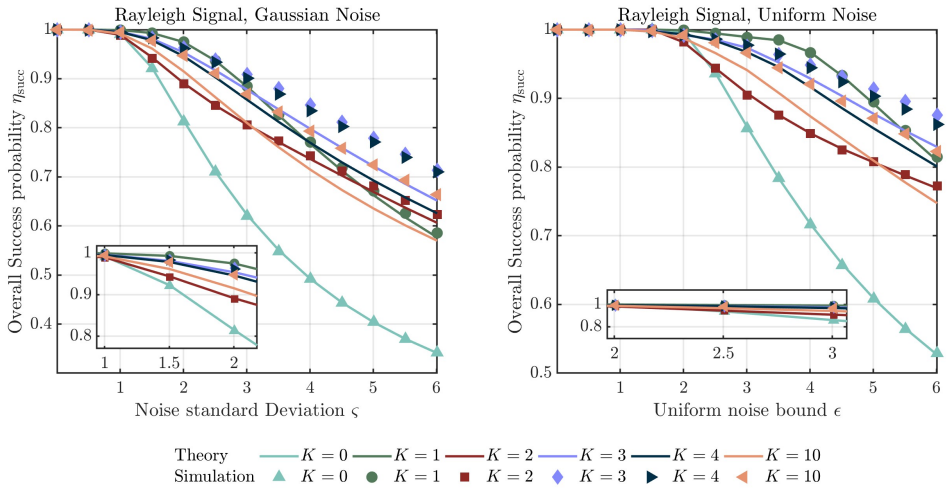


Fig. 5: Overall success probability η_{succ} vs noise intensity under Rayleigh-distributed signals with scale $\beta = 360$. Left: Gaussian noise $e_i \sim \mathcal{N}(0, \varsigma^2)$, $\varsigma \in [0, 6]$, step size 0.5. Right: Uniform noise $e_i \sim \mathcal{U}(-\epsilon, \epsilon)$, $\epsilon \in [0, 6]$, step size 0.5. Solid lines show theoretical predictions; markers indicate simulated results for recursion depths $K \in \{0, 1, 2, 3, 4, 10\}$.

Design Implications: The proposed layered RCRT framework supports flexible trade-offs between range and robustness, offering the following practical insights:

- **Signal statistics:** For signals concentrated near the origin, e.g., Rayleigh or folded Gaussian distributions, adding one or two robust layers ($K = 1$ or 2) significantly improves decoding success rates, since a high proportion of signal magnitudes fall within the inner plateaux.
- **Resource-constrained systems:** In resource-constrained applications, e.g., with limited buffer size or processing power, small K ($K \leq 2$) offers improved robustness without significant complexity overhead.
- **Multi-resolution applications:** Layered RCRT can support multi-user or multi-resolution reconstruction, where each user operates at a layer tuned to their dynamic range requirement. Moderate values of K (e.g., $K = 3, 4$) are especially useful in such scenarios.
- **Limited returns for large K:** Adding many layers ($K > K^*$) provides only marginal improvement in success probability at low signal-to-noise ratio (SNR), as the robust range contracts and the dominant failure events are not further mitigated. As shown in Fig. 5, performance curves flatten beyond $K = 3$, indicating that deep layering may not be cost-effective for most use cases.

VII. Conclusion and Future Work

This paper presents a unified design framework for moduli selection in RCRT decoding algorithms [12], [35]. For the basic RCRT system with a single layer, we derive closed-form optimal moduli for $L = 2, 3$, and 4 that maximize error tolerance. For multi-layer systems, we propose a Fibonacci-inspired construction that ensures exactly K robust decoding layers in addition to the full CRT layer. We further analyze how the number of robust layers K affects

both the dynamic range and the error tolerance, and derive closed-form success probabilities under typical signal and noise models, offering system-level insights for practical design. All theoretical developments are supported by examples and simulations, confirming the validity and practical potential of the proposed methods. Simulation results demonstrate that adding one or two robust layers (i.e., $K = 1, 2$) offers substantial robustness gains with minimal compromise in full CRT range, which makes the method especially well-suited to practical applications.

Future work may include tighter probabilistic analysis of success rates for $K \geq 3$, generalization to multi-moduli layered systems ($L > 2$), and alternative optimization objectives beyond error tolerance at the full CRT layer. To further enhance robustness, one may also incorporate distributional uncertainty, adaptive modeling, or Bayesian priors in reconstruction, depending on the target applications.

APPENDIX A
PROOF OF THEOREM 1

Proof:

Case $L = 2$**:** By (13), we must have $\Gamma_1 \geq \lceil \rho \rceil$. To minimize Γ_2, we select $\Gamma_2 = \Gamma_1 + 1$. From Lemma 1, they are coprime, which means this selection is optimal.

Case $L = 3$: *Trivial regime* $1 < \rho \leq 6$*):* The smallest sorted coprime pair is $(\Gamma_1, \Gamma_2) = (2, 3)$, which meets the range constraint since $\Gamma_1\Gamma_2 = 6 \geq \rho$. The minimal admissible $\Gamma_3 > \Gamma_2$ coprime to both 2 and 3 is 5 (4 is excluded as it shares a factor with 2). Hence $(\Gamma_1, \Gamma_2, \Gamma_3) = (2, 3, 5)$ is feasible and minimizes Γ_3.

General regime $\rho > 6$*:* Since $\Gamma_1 \leq \Gamma_2 - 1$ and ρ is defined in (13), we have $\Gamma_2(\Gamma_2 - 1) \geq \Gamma_2\Gamma_1 \geq \rho$. Let b be the smallest integer (with $b \geq 3$) such that $b(b-1) \geq \rho$ (cf. (16)). Then necessarily

$$\Gamma_2 \ \geq \ b, \qquad \Gamma_3 \ \geq \ b+1.$$

Even b. The triple $\{\Gamma_1, \Gamma_2, \Gamma_3\} = \{b-1, b, b+1\}$ achieves the lower bound $\Gamma_3 = b+1$, satisfies $\Gamma_1\Gamma_2 = (b-1)b \geq \rho$, and is pairwise coprime by Lemma 1. Hence it is feasible and has minimal Γ_3.

Odd b. First try $(\Gamma_2, \Gamma_3) = (b, b+1)$ and ask whether there exists $\Gamma_1 < b$ with $\Gamma_1\Gamma_2 \geq \rho$ and pairwise coprimality.

$\underline{(b+1) \not\equiv 0 \pmod 3}$. Then $\gcd(b-2, b+1) = \gcd(3, b+1) = 1$, and by Lemma 1 also $\gcd(b-2, b) = \gcd(b, b+1) = 1$. If $b(b-2) \geq \rho$, choosing

$$(\Gamma_1, \Gamma_2, \Gamma_3) = (b-2, b, b+1)$$

meets the range constraint with pairwise coprimality and achieves $\Gamma_3 = b+1$, which is minimal.

$\underline{(b+1) \equiv 0 \pmod 3}$. Now $\gcd(b-1, b+1) = 2$ and $\gcd(b-2, b+1) = 3$, so neither $\Gamma_1 = b-1$ nor $\Gamma_1 = b-2$ is coprime to $\Gamma_3 = b+1$. Moreover, for any $\beta \geq 3$,

$$b(b-\beta) \ \leq \ b(b-3) \ < \ (b-1)(b-2) \ < \ \rho,$$

so any $\Gamma_1 \leq b-3$ violates the range constraint. Thus no $\Gamma_1 < b$ works when $\Gamma_3 = b+1$, and therefore $\Gamma_3 \geq b+2$ is necessary. One checks that

$$(\Gamma_1, \Gamma_2, \Gamma_3) = (b, b+1, b+2)$$

is pairwise coprime and satisfies $\Gamma_1\Gamma_2 = b(b+1) \geq \rho$, so it is feasible and has the smallest admissible Γ_3 in this subcase.

Finally, if $b(b-2) < \rho$ (still with b odd), the choice $(\Gamma_1, \Gamma_2) = (b-2, b)$ cannot meet the range constraint, and the above argument again forces $\Gamma_3 \geq b+2$; the triple $(b, b+1, b+2)$ is feasible and minimal.

Case $L = 4$**:** *Trivial regime* $1 < \rho \leq 30$. The smallest pairwise–coprime triple is $(2, 3, 5)$; thus we set $(\Gamma_1, \Gamma_2, \Gamma_3) = (2, 3, 5)$, which satisfies the range constraint since $\Gamma_1\Gamma_2\Gamma_3 = 30 \geq \rho$. To minimize Γ_4 subject to ordering and coprimality with $(2, 3, 5)$, the smallest admissible value > 5 is 7 (as 6 shares factors with $2, 3$). Therefore $(\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4) = (2, 3, 5, 7)$ is feasible and minimizes Γ_4 for all $1 < \rho \leq 30$.

General regime $\rho > 30$*:* We verify, for each row of Table II, that (*i*) the product constraint holds, (*ii*) pairwise coprimality holds (via Lemma 1 and the stated congruence classes), and (iii) Γ_4 is minimal by excluding any smaller admissible value. Let b be defined by (20); then necessarily $\Gamma_3 \geq b$ and $\Gamma_4 \geq b+1$. When $\Gamma_4 = b+1$ is feasible, optimality is immediate; when $\Gamma_4 \in \{b+2, b+3\}$, we show any smaller choice violates (*i*) or (*ii*).

Case A: odd b

Rows A1–A2. From (20),

$$(b-1)(b-2)(b-3) \;\leq\; \rho \;<\; b(b-1)(b-2). \tag{51}$$

Both quartets $\{b-2, b-1, b, b+2\}$ (A1) and $\{b-2, b, b+1, b+2\}$ (A2) satisfy the product bound. For coprimality: $\{b-2, b-1, b\}$ and $\{b-2, b, b+2\}$ are pairwise coprime (Lemma 1). Moreover, $\gcd(b-1, b+2) = 1$ when $b \not\equiv 1 \pmod 3$ (A1), and the analogous checks hold for A2. For optimality, suppose a quartet with $\Gamma_4 = b+1$ exists. Since $b+1$ is even, the remaining three moduli must be odd. Note that the three largest $< b+1$ are b, $b-2$, $b-4$. But then

$$(b-4)(b-2)b \;<\; (b-1)(b-2)(b-3) \;\leq\; \rho,$$

contradicting the product constraint. Hence $\Gamma_4 \geq b+2$ and the listed quartets are optimal.

Case B: Even b*,* $(b-3)(b-1)b > \rho$

Row B1. ($b \bmod 6 \in \{2, 4\}$)

The product requirement is satisfied by assumption. Pairwise coprimality holds for $\{b-3, b-1, b+1\}$ and $\{b-1, b, b+1\}$, and $\gcd(b, b-3) = 1$ since $b \bmod 3 \neq 0$. Optimality follows from $\Gamma_4 \geq b+1$.

Row B2. ($b \bmod 6 = 0$, $b \bmod 5 \neq 3$)

The product constraint holds for $\{b-3, b-1, b+1\}$ by assumption. The sets $\{b-3, b-1, b+1\}$ and $\{b+1, b+2\}$ are pairwise coprime. In addition, $\gcd(b-1, b+2) = 1$ (since $b \bmod 3 \neq 1$) and $\gcd(b+2, b-3) = 1$ (since $b \bmod 5 \neq 3$). Hence, coprimality holds.

Assume that $\Gamma_3 = b$ and $\Gamma_4 = b+1$. Since b is even, the remaining two moduli must be odd. However, $\gcd(b, b-3) = 3$ excludes $b-3$. Thus, the largest available odd numbers are $b-1$ and $b-5$. Then:

$$b(b-1)(b-5) < (b-1)(b-2)(b-3) < \rho,$$

violating the product requirement. Hence, $\Gamma_3 \geq b+1$ and $\Gamma_4 \geq b+2$, proving optimality.

Row B3. ($b \bmod 6 = 0$, $b \bmod 5 = 3$)

From the proof of Row B2, when $b \bmod 6 = 0$: (*i*) $\Gamma_3 \geq b+1$, $\Gamma_4 \geq b+2$, and (*ii*) $\gcd(b, b-3) = 3$, so b and $b-3$ cannot coexist. Additionally, $\gcd(b+2, b-3) = 5$, so $b-3$ and $b+2$ cannot coexist.

Row B3.1.: ($b \bmod 6 = 0$, $b \bmod 5 = 3$, $(b-5)(b-1)(b+1) > \rho$ and $b+2 \bmod 7 \neq 0$)

The quartet $\{b-5, b-1, b+1, b+2\}$ satisfies the product constraint. By Lemma 1, $\{b-1, b+1, b+2\}$ are pairwise coprime. We also have $\gcd(b-5, b-1) = \gcd(4, b-1) = 1$, $\gcd(b-5, b+1) = 1$ (since $b \bmod 6 = 0$), and $\gcd(b-5, b+2) = 1$ (since $b+2 \bmod 7 \neq 0$). Optimality follows from the result of B2.

Row B3.2.: The quartet $\{b-1, b+1, b+2, b+3\}$ satisfies $(b-1)(b+1)(b+2) > \rho$. Pairwise coprimality is satisfied for $\{b-1, b+1, b+3\}$ and $\{b+1, b+2, b+3\}$ from Lemma 1. Also, $\gcd(b+2, b-1) = 1$ since $b \bmod 6 = 0$. Thus, all pairs are coprime.

To prove optimality, assume $\Gamma_4 = b+2$. Then all other moduli must be odd. We cannot select $b-3$ since $\gcd(b+2, b-3) = 5$). In addition, either $(b-5)(b-1)(b+1) \leq \rho$ or $\gcd(b+2, b-5) = 7$ excludes $b-5$. The remaining choice is $\{b+1, b-1, b-7\}$, but:

$$(b-7)(b-1)(b+1) < (b-5)(b-1)(b+1) \leq \rho,$$

which violates the product constraint. Hence, $\Gamma_4 \geq b+3$, and the construction is optimal.

Case C – Even b with $(b-3)(b-1)b < \rho \leq (b-3)(b-1)(b+1)$

Row C1 ($b \bmod 3 \neq 1$, $b \bmod 5 \neq 3$).

The quartet $\{b-3, b-1, b+1, b+2\}$ satisfies the product bound because $(b-3)(b-1)(b+1) > \rho$. Pairwise coprimality follows from Lemma 1: $\gcd(b-3, b+2) = 1$ since $b \bmod 5 \neq 3$, and $\gcd(b-1, b+2) = 1$ since $b \bmod 3 \neq 1$. To prove optimality, assume $\Gamma_4 = b+1$. Then $\Gamma_3 = b$ (even) and the two remaining moduli must be odd. The largest such pair is $\{b-1, b-3\}$. As $(b-3)(b-1)b \leq \rho$, the product condition is violated. Any smaller odd choice further reduces the product, so $\Gamma_4 = b+1$ is impossible; hence $\Gamma_4 \geq b+2$, and the selected quartet is optimal.

Row C2 ($b \bmod 3 = 1$, $b \bmod 5 \neq 3$).

The proof of the product and pairwise property is straightforward.

To show optimality, the proof of C1 already indicates that $\Gamma_4 \geq b+2$. Assume for contradiction that $\Gamma_4 = b+2$ and $\Gamma_3 = b+1$. The remaining two moduli must be odd and less than $b+1$. However, $b-1$ is excluded because $\gcd(b+2, b-1) = \gcd(3, b-3) = 3$ (as $b \bmod 3 = 1$). Thus, the largest valid odd pair is $\{b-5, b-3\}$. Again, as

$$(b-5)(b-3)(b+1) < (b-3)(b-1)b < \rho,$$

the product constraint is not met. Hence, $\Gamma_4 = b+2$ is infeasible and the chosen quartet with $\Gamma_4 = b+3$ is optimal.

Row C3 ($b \bmod 5 = 3$).

Product: By definition of b, the product constraint is satisfied as $(b-1)(b+1)(b+2) > (b+1)b(b-1) > \rho$.

Coprimality: The set depends on $b \bmod 3$. If $b \bmod 3 = 1$, then $\gcd(b+2, b-1) = \gcd(3, b-3) = 3$, so $b-1$ and $b+2$ cannot be used together. We instead select $\{b-1, b, b+1, b+3\}$, which is pairwise coprime by Lemma 1. Otherwise, use $\{b-1, b+1, b+2, b+3\}$, which is also pairwise coprime (proof as in B3.2).

Optimality: As mentioned before, the proof of C1 already establishes that $\Gamma_4 \geq b+2$. Suppose, for contradiction, that $\Gamma_4 = b+2$. As $b \bmod 5 = 3$, we must exclude $b-3$ since $\gcd(b+2, b-3) = \gcd(b+2, 5) = 5$. Thus, the largest three odd integers below $b+2$ are $b+1$, $b-1$, and $b-5$, whose product is

$$(b-5)(b-1)(b+1) < (b-3)(b-1)b < \rho,$$

contradicting the product constraint. Hence, $\Gamma_4 \geq b+3$, which confirms optimality of the selected quartet.

Case D — even b with $(b+1)(b-1)(b-3) < \rho$

Product: As $b(b-1)(b-2) \geq \rho$, it is trivial to prove that both selected quartet $\{b-1, b, b+1, b+3\}$ and $\{b-1, b+1, b+2, b+3\}$ satisfy the product requirement.

Coprimality: For Row D1, the subsets $\{b-1, b+1, b+3\}$ and $\{b-1, b, b+1\}$ are pairwise coprime by Lemma 1. Since $b \bmod 3 \neq 0$, we have $\gcd(b, b+3) = 1$, guaranteeing the full quartet's pairwise coprimality.

For Row D2, the proof is analogous. The subsets $\{b-1, b+1, b+3\}$ and $\{b+1, b+2, b+3\}$ are pairwise coprime by Lemma 1. Moreover, with b even and $b \bmod 3 = 0$, we obtain $\gcd(b+2, b-1) = \gcd(b-1, 3) = 1$, thus ensuring the full quartet's pairwise coprimality.

Optimality: We demonstrate that the minimal pair $(\Gamma_4, \Gamma_3) = (b+1, b)$ cannot be selected. Under this choice, the remaining moduli must be odd since b is even, yielding the largest available odd values $(\Gamma_2, \Gamma_1) = (b-1, b-3)$. However, the assumption $(b-3)(b-1)b < (b-3)(b+1) < \rho$ violates the product constraints.

We proceed to establish that $\Gamma_4 = b+2$ is also infeasible. This selection leaves $b+1$, $b-1$, and $b-3$ as the three largest available odd integers. The corresponding assumption $(b-3)(b-1)(b+1) < \rho$ again violates the product constraint. Therefore, $\Gamma_4 \geq b+3$, and since the proposed quartet achieves this lower bound, optimality is established.

■

APPENDIX B: PROOF OF THEOREM 2

Part (i): Remainder Chain and Layered Dynamic Range

1) Coprimality. Clearly $\Gamma_1(d) \geq \rho$ by construction. Let $g = \gcd(\Gamma_1(d), \Gamma_2(d))$. Since g divides both numbers, it divides their difference:

$$\Gamma_2(d) - \Gamma_1(d) = F_{d,K+1} \quad \Rightarrow \quad g \mid F_{d,K+1}.$$

Also $g \mid \Gamma_1(d)$ implies

$$g \mid \big(\Gamma_1(d) - \zeta_d F_{d,K+1}\big) = F_{d,K}.$$

Hence g divides both $F_{d,K}$ and $F_{d,K+1}$. By the Euclidean algorithm, $\gcd(F_{d,K}, F_{d,K+1}) = \gcd(F_{d,0}, F_{d,1}) = \gcd(d, 1) = 1$, so $g = 1$.

2) Exact remainder chain.: $\sigma_{-1} = \Gamma_2(d)$ and $\sigma_0 = \Gamma_1(d)$. A simple calculation gives $\sigma_1 = \Gamma_2(d) - \Gamma_1(d) = F_{d,K+1}$. Assume inductively $\sigma_j = F_{d,K+2-j},\ \sigma_{j-1} = F_{d,K+3-j}$ for some $j \geq 1$. Using $F_{d,k+2} = F_{d,k+1} + F_{d,k}$,

$$\sigma_{j+1} = \sigma_{j-1} \bmod \sigma_j = \sigma_{j-1} - \sigma_j = F_{d,K+1-j},$$

so by induction $\sigma_j = F_{d,K+2-j}$ $(1 \leq j \leq K+1)$ and the algorithm terminates after $K+1$ steps at $\sigma_{K+1} = F_{d,1} = 1$.

3) Layered dynamic range. Let $P_j = m\, N_j$. Proving (35) is equivalent to showing that, for $1 \leq j \leq K$,

$$N_j = \begin{cases} \Gamma_1(d)\, F_{\zeta_d,\, 2j_0}, & j = 2j_0 - 1, \\ \Gamma_2(d)\, F_{\zeta_d - 1,\, 2j_0+1}, & j = 2j_0, \end{cases} \tag{52}$$

where $j_0 \in \mathbb{Z}_{\geq 1}$. We proceed in three steps.

(a) Two auxiliary identities. We first prove that

$$\Gamma_2(d)\, F_{\zeta_d - 1,\, j} - \Gamma_1(d)\, F_{\zeta_d,\, j} = \sigma_j, \quad j \text{ odd}, \tag{53}$$

$$\Gamma_1(d)\, F_{\zeta_d,\, j} - \Gamma_2(d)\, F_{\zeta_d - 1,\, j} = \sigma_j, \quad j \text{ even}. \tag{54}$$

Let us consider the case of odd $j = 2j_0 - 1$. For $j = 1$ (i.e., $j_0 = 1$), $F_{\zeta_d - 1,1} = F_{\zeta_d,1} = 1$, hence

$$\Gamma_2(d) - \Gamma_1(d) = F_{d,K+1} = \sigma_1,$$

proving (53). For $j = 2j_0 - 1 > 1$, write $F_{\zeta_d - 1,j} = F_{1,j-1} + (\zeta_d - 1)F_{1,j-2} = F_{\zeta_d,j} - F_{1,j-2}$, and use the equality of $\Gamma_2(d) - \Gamma_1(d) = F_{d,K+1}$ from (33) to obtain

$$\Gamma_2(d)F_{\zeta_d - 1,j} - \Gamma_1(d)F_{\zeta_d,j} = F_{d,K+1}F_{\zeta_d,j} - \Gamma_2(d)F_{1,j-2}.$$

With $F_{\zeta_d,k} = F_{1,k-1} + \zeta_d F_{1,k-2}$ and $\Gamma_2(d) = (\zeta_d + 1)F_{d,K+1} + F_{d,K}$, a short cancellation yields

$$\Gamma_2(d)F_{\zeta_d - 1,j} - \Gamma_1(d)F_{\zeta_d,j} = -(F_{d,K}F_{1,j-2} - F_{d,K+1}F_{1,j-3}).$$

Applying the mixed d'Ocagne identity (Lemma 2) with $s = K$ and $t = j - 2$ gives

$$-(F_{d,K}F_{1,j-2} - F_{d,K+1}F_{1,j-3}) = (-1)^{j-1}F_{d,K+2-j} = \sigma_j$$

for $j = 2j_0 - 1$, proving (53). The even case (54) follows by the same argument with roles interchanged.

(b) Base layers $j = 1, 2$. From (4) and (33), $\sigma_0 = \Gamma_1(d)$ and $\sigma_1 = \Gamma_2(d) \bmod \Gamma_1(d) = F_{d,K+1}$, hence $\lfloor \sigma_0/\sigma_1 \rfloor = \zeta_d$. Using (7) with $N_{-1} = \Gamma_1(d)$ and $N_0 = \Gamma_2(d)$,

$$\begin{aligned} N_1 &= N_{-1} + \left\lfloor \frac{\sigma_0}{\sigma_1} \right\rfloor (N_0 - \sigma_1) \\ &= \Gamma_1(d) + \zeta_d\big(\Gamma_2(d) - F_{d,K+1}\big) \\ &= \Gamma_1(d) + \zeta_d\Gamma_1(d) = \Gamma_1(d)F_{\zeta_d,2}, \end{aligned}$$

so (52) holds for $j = 1$. For $j = 2$, since $\lfloor \sigma_1/\sigma_2 \rfloor = \lfloor F_{d,K+1}/F_{d,K} \rfloor = 1$ and (54) with $j = 2$ gives $\sigma_2 = \Gamma_1(d)F_{\zeta_d,2} - \Gamma_2(d)F_{\zeta_d - 1,2}$, we obtain

$$\begin{aligned} N_2 &= N_0 + \left\lfloor \tfrac{\sigma_1}{\sigma_2} \right\rfloor (N_1 - \sigma_2) = \Gamma_2(d) + \Gamma_1(d)F_{\zeta_d,2} - \sigma_2 \\ &= \Gamma_2(d) + \Gamma_2(d)F_{\zeta_d - 1,2} = \Gamma_2(d)F_{\zeta_d - 1,3}, \end{aligned}$$

verifying (52) for $j = 2$.

(c) Induction. Assume that (52) holds for $(2j_0 - 1, 2j_0)$ with $1 \le j_0 < \lceil K/2 \rceil$, i.e., $N_{2j_0-1} = \Gamma_1(d)F_{\zeta_d,\,2j_0}$ and $N_{2j_0} = \Gamma_2(d)F_{\zeta_d-1,\,2j_0+1}$. For $2 \le j \le K$, the Euclidean remainders satisfy $\lfloor \sigma_{j-1}/\sigma_j \rfloor = \lfloor F_{d,K+3-j}/F_{d,K+2-j} \rfloor = 1$. Then

$$\begin{aligned} N_{2j_0+1} &= N_{2j_0-1} + \Big(N_{2j_0} - \sigma_{2j_0+1}\Big) \\ &= \Gamma_1(d)F_{\zeta_d,\,2j_0} + \Big(\Gamma_2(d)F_{\zeta_d-1,\,2j_0+1} - \sigma_{2j_0+1}\Big) \\ &= \Gamma_1(d)F_{\zeta_d,\,2j_0} + \Gamma_1(d)F_{\zeta_d,\,2j_0+1} = \Gamma_1(d)F_{\zeta_d,\,2j_0+2}, \end{aligned}$$

where we used (53) with $j = 2j_0+1$ in the third line. Thus (52) holds for $j = 2j_0+1$. The even step is analogous: using (54) with $j = 2j_0 + 2$ gives

$$\begin{aligned} N_{2j_0+2} &= N_{2j_0} + \Big(N_{2j_0+1} - \sigma_{2j_0+2}\Big) \\ &= \Gamma_2(d)F_{\zeta_d-1,\,2j_0+1} + \Big(\Gamma_1(d)F_{\zeta_d,\,2j_0+2} - \sigma_{2j_0+2}\Big) \\ &= \Gamma_2(d)F_{\zeta_d-1,\,2j_0+1} + \Gamma_2(d)F_{\zeta_d-1,\,2j_0+2} = \Gamma_2(d)F_{\zeta_d-1,\,2j_0+3}. \end{aligned}$$

By induction, (52) holds for all $1 \le j \le K$, and hence $P_j = m\,N_j$ equals (35).

Part (ii): Bounded Search for Optimal d

For $d = 1$, $\Gamma_2(1) = \big(\zeta_1 + 1\big)F_{1,K+1} + F_{1,K}$. Recall that for each $d > 1$, the construction yields $\Gamma_2(d) = \Gamma_1(d) + F_{d,K+1}$. To ensure feasibility, we require $\Gamma_1(d) \ge \rho$, which implies that $\Gamma_2(d) \ge \rho + F_{d,K+1}$. By definition of ζ_1, we have

$$\rho > (\zeta_1 - 1)F_{1,K+1} + F_{1,K},$$

which implies that

$$\Gamma_2(d) > (\zeta_1 - 1)F_{1,K+1} + F_{1,K} + F_{d,K+1}$$

To guarantee improvement over $\Gamma_2(1)$, i.e., $\Gamma_2(d) < \Gamma_2(1)$, we further require

$$\Gamma_2(d) < (\zeta_1 + 1)F_{1,K+1} + F_{1,K},$$

which produces

$$(\zeta_1 - 1)F_{1,K+1} + F_{1,K} + F_{d,K+1} < (\zeta_1 + 1)F_{1,K+1} + F_{1,K},$$

and can be simplified to $F_{d,K+1} < 2F_{1,K+1}$. Substituting $F_{d,K+1} = F_{1,K} + dF_{1,K-1}$ from Lemma 2 along with the recursion $F_{1,K+1} = F_{1,K} + F_{1,K-1}$, we know that d needs to satisfy the following constraint

$$(d-2)F_{1,K-1} < F_{1,K}. \tag{55}$$

When $K = 1$, as $F_{1,0} = 1$ and $F_{1,1} = 1$, we have $d < 3$. When $K = 2$, as $F_{1,2} = 2$, we get $d < 4$, which indicates $d \le 3$. When $K \ge 3$, as $F_{1,K} < 2F_{1,K-1}$, we arrive at $(d-2)F_{1,K-1} < 2F_{1,K-1}$, implying $d < 4$, i.e., $d \le 3$. Summarising, we only need to check $1 \le d \le 3$.

APPENDIX C: PROOF OF COROLLARY 1

Proof: By Theorem 2, the construction guarantees $\Gamma_1 \geq \lceil \rho \rceil$ and $\gcd(\Gamma_1, \Gamma_2) = 1$. It therefore suffices to show that Γ_2 is minimal under these constraints.

A necessary gap at the first step. Let $\sigma_1 = \Gamma_2 \bmod \Gamma_1 = \Gamma_2 - \Gamma_1$. The Euclidean chain length $K{+}1$ with terminal remainder 1 implies $\sigma_1 \geq F_{1,K+1}$. Otherwise, the chain would be shorter than that generated by the consecutive Fibonacci pair, contradicting the well-known minimality of Fibonacci numbers for Euclidean length. Hence,

$$\Gamma_2 \;\geq\; \Gamma_1 + F_{1,K+1} \;\geq\; \lceil \rho \rceil + F_{1,K+1}. \tag{56}$$

Case $K = 1$. Here $F_{1,2} = 2$, so (56) gives $\Gamma_2 \geq \Gamma_1 + 2$.

- If $\lceil \rho \rceil$ is odd, take $\Gamma_1 = \lceil \rho \rceil$ and $\Gamma_2 = \Gamma_1 + 2$; then $\gcd(\Gamma_1, \Gamma_2) = 1$ and the bound is tight.
- If $\lceil \rho \rceil$ is even, Γ_1 must be odd to ensure coprimality with $\Gamma_2 = \Gamma_1 + 2$; choose $\Gamma_1 = \lceil \rho \rceil + 1$ and $\Gamma_2 = \Gamma_1 + 2 = \lceil \rho \rceil + 3$. Reducing Γ_2 to $\lceil \rho \rceil + 2$ forces $\Gamma_1 = \lceil \rho \rceil$ (even) and breaks coprimality.

Thus the optimal pair is $\Gamma_1 = 2\zeta_1 + 1$ and $\Gamma_2 = \Gamma_1 + 2$, with $\zeta_1 = \lceil (\rho - 1)/2 \rceil$.

Case $K = 2$. Now $F_{1,3} = 3$, hence

$$\Gamma_2 \;\geq\; \Gamma_1 + 3 \;\geq\; \lceil \rho \rceil + 3. \tag{57}$$

We consider $\lceil \rho \rceil \equiv r \pmod 3$.

$\underline{r = 2}$: Take $\Gamma_1 = \lceil \rho \rceil$ and set $\Gamma_2 = \Gamma_1 + 3$; (57) is met with equality and the remainder chain is $(3, 2, 1)$.

$\underline{r = 1}$: If we tried $\Gamma_2 = \lceil \rho \rceil + 3$ with $\Gamma_1 = \lceil \rho \rceil$, then $\sigma_1 = 3$ and the remainder chain would be $(\sigma_1, \sigma_2) = (3, 1)$, i.e., only $K = 1$. Thus we must increase Γ_1 to keep $K = 2$ while respecting coprimality. Taking $\Gamma_1 = \lceil \rho \rceil + 1$ and $\Gamma_2 = \Gamma_1 + 3 = \lceil \rho \rceil + 4$ yields the chain $(3, 2, 1)$ and Γ_2 is minimal.

$\underline{r = 0}$: Write $\lceil \rho \rceil = 3k$. If $k \equiv 1 \pmod 4$, then $\lceil \rho \rceil \equiv 3 \pmod{12}$, i.e., $\lceil \rho \rceil = 12\ell + 3$ with $k = 4\ell + 1$. In this subcase, the choice $(\Gamma_1, \Gamma_2) = (12\ell{+}3,\ 12\ell{+}7)$ is optimal as reducing Γ_2 to $12\ell{+}6$ would give $\gcd(\Gamma_1, \Gamma_2) = 3$, breaking coprimality.

For the remaining classes $\lceil \rho \rceil \in \{12\ell,\ 12\ell + 6,\ 12\ell + 9\}$, take

$$\Gamma_1 = \lceil \rho \rceil + 2, \qquad \Gamma_2 = \Gamma_1 + 3 = \lceil \rho \rceil + 5,$$

which yields the remainder chain $(\sigma_1, \sigma_2, \sigma_3) = (3, 2, 1)$ (hence $K = 2$). Any smaller second modulus fails: (*i*) $\Gamma_2 = \lceil \rho \rceil + 3$ forces $\Gamma_1 = \lceil \rho \rceil$, so $\gcd(\Gamma_1, \Gamma_2) = 3$; (*ii*) $(\Gamma_1, \Gamma_2) = (\lceil \rho \rceil + 1, \lceil \rho \rceil + 4)$ collapses the chain to $(3, 1)$ (only $K = 1$); (*iii*) $(\Gamma_1, \Gamma_2) = (\lceil \rho \rceil, \lceil \rho \rceil + 4)$ gives $(4, 1)$ when $\lceil \rho \rceil = 12\ell + 9$ ($K = 1$), and violates coprimality when $\lceil \rho \rceil \in \{12\ell,\ 12\ell + 6\}$ since $\lceil \rho \rceil$ and $\lceil \rho \rceil + 4$ are both even (i.e., they have a common divisor of 2). Hence $\Gamma_2 = \lceil \rho \rceil + 5$ is minimal in these subcases. ■

REFERENCES

[1] W. Yan, L. Gan, S. Hu, and H. Liu, "Towards optimized multi-channel modulo-ADCs: Moduli selection strategies and bit depth analysis," in *ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2024, pp. 9496–9500.

[2] E. Di Claudio, F. Piazza, and G. Orlandi, "Fast combinatorial RNS processors for DSP applications," *IEEE Transactions on Computers*, vol. 44, no. 5, pp. 624–633, 1995.

[3] S.-M. Yen, S. Kim, S. Lim, and S.-J. Moon, "RSA speedup with Chinese remainder theorem immune against hardware fault cryptanalysis," *IEEE Transactions on Computers*, vol. 52, no. 4, pp. 461–472, 2003.

[4] D. M. Mandelbaum, "On a class of arithmetic codes and a decoding algorithm (corresp.)," *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 85–88, 1976.

[5] F. Barsi and P. Maestrini, "Improved decoding algorithms for arithmetic residue codes (corresp.)," *IEEE Transactions on Information Theory*, vol. 24, no. 5, pp. 640–643, 1978.

[6] A. Shiozaki, "Decoding of redundant residue polynomial codes using Euclid's algorithm," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1351–1354, 1988.

[7] O. Goldreich, D. Ron, and M. Sudan, "Chinese remaindering with errors," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1330–1338, 2000.

[8] J. G. F. Souza, S. I. R. Costa, and C. Ling, "Multilevel lattice codes from hurwitz quaternion integers," *IEEE Transactions on Information Theory*, pp. 1–1, 2025.

[9] K. W. Shum and W. S. Wong, "Construction and applications of CRT sequences," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5780–5795, 2010.

[10] Y. Chen, Y.-H. Lo, K. W. Shum, W. S. Wong, and Y. Zhang, "CRT sequences with applications to collision channels allowing successive interference cancellation," *IEEE Transactions on Information Theory*, vol. 64, no. 4, pp. 2910–2923, 2018.

[11] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular Ad-Hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[12] W. Wang and X.-G. Xia, "A closed-form robust Chinese remainder theorem and its performance analysis," *IEEE Transactions on Signal Processing*, vol. 58, no. 11, pp. 5655–5666, 2010.

[13] H. Xiao and G. Xiao, "Notes on CRT-based robust frequency estimation," *Signal processing*, vol. 133, pp. 13–17, 2017.

[14] X.-G. Xia and K. Liu, "A generalized Chinese remainder theorem for residue sets with errors and its application in frequency determination from multiple sensors with low sampling rates," *IEEE Signal Processing Letters*, vol. 12, no. 11, pp. 768–771, 2005.

[15] L. Yang and Y. Han, "A joint spatio-temporal sub-Nyquist sampling structure for wideband receivers," *IEEE Transactions on Instrumentation and Measurement*, vol. 73, pp. 1–15, 2024.

[16] W. Wang, X. Li, and X.-G. Xia, "An ML estimation based robust Chinese remainder theorem for reals," in *2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP)*, 2015, pp. 363–367.

[17] B. Yang, W. Wang, X. Xia, and Q. Yin, "Phase detection based range estimation with a dual-band robust Chinese remainder theorem," *Science China Information Sciences*, vol. 57, no. 2, pp. 1–9, Feb. 2014.

[18] A. Akhlaq, R. McKilliam, R. Subramanian, and A. Pollok, "Selecting wavelengths for least squares range estimation," *IEEE Transactions on Signal Processing*, vol. 64, no. 20, pp. 5205–5216, 2016.

[19] W. Li, X. Wang, and B. Moran, "Wireless signal travel distance estimation using non-coprime wavelengths," *IEEE Signal Processing Letters*, vol. 24, no. 1, pp. 27–31, 2016.

[20] C. Chi, S. Chen, R. Zhong, P. Zhang, P. Wang, Y. Li, J. Liu, and H. Huang, "Robust Chinese remainder theorem–based synthetic aperture sonar motion estimation," *IEEE Journal of Oceanic Engineering*, 2024.

[21] L. Gan and H. Liu, "High dynamic range sensing using multi-channel modulo samplers," in *2020 IEEE 11th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, Jun. 2020, pp. 1–5, iSSN: 2151-870X.

[22] Y. Gong, L. Gan, and H. Liu, "Multi-channel modulo samplers constructed from gaussian integers," *IEEE Signal Processing Letters*, vol. 28, pp. 1828–1832, 2021, conference Name: IEEE Signal Processing Letters.

[23] W. Yan, L. Gan, and Y. D. Zhang, "Threshold sensitivity in two-channel modulo ADCs: Analysis and robust reconstruction," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2025, pp. 1–5.

[24] C. Demirkiran, L. Nair, D. Bunandar, and A. Joshi, "A blueprint for precise and fault-tolerant analog neural networks," *Nature Communications*, vol. 15, no. 1, p. 5098, 2024.

[25] C. Demirkiran, G. Yang, D. Bunandar, and A. Joshi, "Mirage: An RNS-based photonic accelerator for DNN training," in *2024 ACM/IEEE 51st Annual International Symposium on Computer Architecture (ISCA)*. IEEE, 2024, pp. 73–87.

[26] L. Xiao, X.-G. Xia, and W. Wang, "Multi-stage robust Chinese remainder theorem," *IEEE Transactions on Signal Processing*, vol. 62, no. 18, pp. 4772–4785, 2014.

[27] A. Akhlaq, R. G. McKilliam, and R. Subramanian, "Basis construction for range estimation by phase unwrapping," *IEEE Signal Processing Letters*, vol. 22, pp. 2152–2156, 2015.

[28] W. Li, X. Wang, X. Wang, and B. Moran, "Distance estimation using wrapped phase measurements in noise," *IEEE Transactions on Signal Processing*, vol. 61, no. 7, pp. 1676–1688, 2013.

[29] H. Xiao, Y. Huang, Y. Ye, and G. Xiao, "Robustness in Chinese remainder theorem for multiple numbers and remainder coding," *IEEE Transactions on Signal Processing*, vol. 66, no. 16, pp. 4347–4361, 2018.

[30] H. Liao and X.-G. Xia, "A sharpened dynamic range of a generalized chinese remainder theorem for multiple integers," *IEEE Transactions on Information Theory*, vol. 53, no. 1, pp. 428–433, 2007.

[31] L. Xiao, X.-G. Xia, and Y.-P. Wang, "Exact and robust reconstructions of integer vectors based on multidimensional Chinese remainder theorem (MD-CRT)," *IEEE Transactions on Signal Processing*, vol. 68, pp. 5349–5364, 2020.

[32] L. Xiao, H. Huo, and X.-G. Xia, "Robust multidimensional Chinese remainder theorem for integer vector reconstruction," *IEEE Transactions on Signal Processing*, 2024.

[33] G. Guo and X.-G. Xia, "A construction of pairwise co-prime integer matrices of any dimension and their least common right multiple," *IEEE Transactions on Signal Processing*, 2025.

[34] X. Li, S. Sun, Q. Liao, and X.-G. Xia, "Maximum likelihood estimation based complex-valued robust Chinese remainder theorem and its fast algorithm," *arXiv preprint arXiv:2503.18625*, 2025.

[35] L. Xiao, X.-G. Xia, and H. Huo, "Towards Robustness in Residue Number Systems," *IEEE Transactions on Signal Processing*, vol. 65, no. 6, pp. 1497–1510, Mar. 2017.

[36] F. Pajuelo-Holguera, J. M. Granado-Criado, and J. A. Gómez-Pulido, "Fast Montgomery modular multiplier using FPGAs," *IEEE Embedded Systems Letters*, vol. 14, no. 1, pp. 19–22, 2022.

[37] P. Boyvalenkov, N. I. Chervyakov, P. Lyakhov, N. Semyonova, A. Nazarov, M. Valueva, G. Boyvalenkov, D. Bogaevskiy, and D. Kaplun, "Classification of moduli sets for residue number system with special diagonal functions," *IEEE Access*, vol. 8, pp. 156 104–156 116, 2020.

[38] C.-H. Chang, A. S. Molahosseini, A. A. E. Zarandi, and T. F. Tay, "Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications," *IEEE Circuits and Systems Magazine*, vol. 15, no. 4, pp. 26–44, 2015.

[39] H. Xiao and G. Xiao, "On solving ambiguity resolution with robust Chinese remainder theorem for multiple numbers," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 5179–5184, 2019.

[40] B. Parhami, "Digital arithmetic in nature: Continuous-digit RNS," *The Computer Journal*, vol. 58, no. 5, pp. 1214–1223, May 2015, conference Name: The Computer Journal.

[41] A. Bhandari, F. Krahmer, and T. Poskitt, "Unlimited sampling from theory to practice: Fourier-prony recovery and prototype ADC," *IEEE Transactions on Signal Processing*, vol. 70, pp. 1131–1141, 2021.

[42] S. Mulleti, E. Reznitskiy, S. Savariego, M. Namer, N. Glazer, and Y. C. Eldar, "A hardware prototype of wideband high-dynamic range analog-to-digital converter," *IET Circuits, Devices & Systems*, vol. 17, no. 4, pp. 181–192, 2023.

[43] M. Abdallah and A. Skavantzos, "On multimoduli residue number systems with moduli of forms r^a, $r^b - 1$, $r^c + 1$," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 52, no. 7, pp. 1253–1266, 2005.

[44] T. Koshy, *Fibonacci and Lucas Numbers with Applications, Volume 1*, 2nd ed. Hoboken, NJ: Wiley, 2018.

[45] S. Vajda, *Fibonacci and Lucas numbers, and the golden section: theory and applications*. Courier Corporation, 2008.

[46] R. Keskin, "Three identities concerning fibonacci and lucas numbers," *Notes on Number Theory and Discrete Mathematics*, vol. 20, no. 5, pp. 44–48, 2014. [Online]. Available: https://nntdm.net/papers/nntdm-20/NNTDM-20-5-44-48.pdf

[47] J. Shallit, "Origins of the analysis of the Euclidean algorithm," *Historia Mathematica*, vol. 21, no. 4, pp. 401–419, 1994.