Asia Pac. J. Math. 2026 **13**:137

# MATRIX ELEMENTARY ROW OPERATIONS FOR CONTINUED FRACTIONS OVER $\mathbb{F}_q[x]$: NON-ARCHIMEDEAN ERROR EQUALITIES AND THE REED–SOLOMON KEY EQUATION

EKKAWIT LAMPAI[1], WANNATIDA YONWILAD[2,*]

[1]Department of Mathematics, Faculty of Science and Technology, Rajabhat Maha Sarakham University, Maha Sarakham, Thailand

[2]Department of Learning Management Innovation, Faculty of Education and Educational Innovation, Kalasin University, Kalasin, Thailand

[*]Corresponding author: wantida.yo@ksu.ac.th

Received Jun. 16, 2026

Abstract. We extend the augmented-matrix elementary row operation (ERO) framework for continued fractions, recently introduced for the integers, to the polynomial ring $\mathbb{F}_q[x]$. Realising the Euclidean algorithm as EROs on $[\,I \mid v\,]$, we show that the determinant invariant $\det(A_k) = (-1)^k$ and the associated Bézout encoding carry over unchanged, in a closed form whose two columns display the convergent denominators and numerators. The two-sided sharp error bounds of the integer case then collapse, under the non-archimedean valuation at the infinite place, to the exact equality $|\alpha - p_k/q_k| = q^{-(\deg q_k + \deg q_{k+1})}$ for every convergent $p_k/q_k$ other than the last: an equality classical in the function-field setting but with no archimedean analogue, obtained here from the determinant invariant by a single application of ultrametric domination. Read at the finite ($x$-adic) place, dual via $x \mapsto 1/x$, the same construction solves the Reed–Solomon/BCH key equation: a degree-thresholded halt of the EROs recovers the error-locator and error-evaluator polynomials in a single row of the augmented matrix, the normalised halting coefficient being the connection polynomial returned by the Berlekamp–Massey algorithm. A single matrix construction thus yields, at two dual valuations, both best rational approximation and algebraic decoding.

2020 Mathematics Subject Classification. 11J61; 11J70; 11T55; 15A54; 94B35.

Key words and phrases. continued fractions; polynomial rings; finite fields; non-archimedean valuation; best rational approximation; Reed–Solomon codes; Berlekamp–Massey algorithm.

## 1. Introduction

For $k \geq 1$, the $k$-th convergent $p_k/q_k = [a_0; a_1, \ldots, a_k]$ of a continued fraction is the best rational approximation to its value among all fractions with denominator not exceeding $q_k$, a fact at the heart of classical Diophantine approximation; the excluded case $k = 0$ is genuinely exceptional over $\mathbb{Q}$, and one of the things the polynomial setting will repair (Remark 5.3). The convergent sequence is encoded by

DOI: 10.28924/APJM/13-137

the matrix product

$$\begin{pmatrix} q_{k-1} & q_k \\ p_{k-1} & p_k \end{pmatrix} = M_0 M_1 \cdots M_k, \qquad M_i = \begin{pmatrix} 0 & 1 \\ 1 & a_i \end{pmatrix},$$

yet this product exposes neither the underlying Euclidean remainder sequence nor sharp error bounds. The recent framework of Yonwilad et al. [14] addresses this for $a/b \in \mathbb{Q}$ by realising the Euclidean algorithm as a sequence of elementary row operations on the augmented matrix $[\, I \mid v \,]$, $v = (a, b)^{\mathsf{T}}$. There a determinant invariant encodes both the convergents and the Bézout coefficients.

The integers, however, are only one Euclidean domain among many, and the *width* of the classical error interval is an artefact of the archimedean absolute value on $\mathbb{Q}$. In this paper we transport the ERO framework to the polynomial ring $\mathbb{F}_q[x]$ over a finite field, where continued fractions have themselves been studied extensively [5, 6, 11]. Here the natural absolute value at the infinite place, $|f| = q^{\deg f}$, is *non-archimedean*, and the consequences are structural rather than cosmetic. While the determinant invariant carries over essentially unchanged (Theorem 3.1), the error analysis does not: the alternating telescoping series that produces an *interval* over $\mathbb{Q}$ is dominated by its first term in the ultrametric, collapsing the two-sided bound to the *exact equality* $|\alpha - p_k/q_k| = q^{-(\deg q_k + \deg q_{k+1})}$ (Theorem 4.1). That this equality holds in $\mathbb{F}_q((1/x))$ is classical [5, 11]; what the matrix formulation adds is that it is now a one-line consequence of the invariant of Theorem 3.1, and that the "sharpness" of the integer bound is thereby exhibited as the residue of an archimedean obstruction that simply vanishes over $\mathbb{F}_q[x]$.

The polynomial setting carries a second dividend. The same augmented-matrix algorithm, read not at the infinite place but at the finite $x$-adic place—the two being interchanged by $x \mapsto 1/x$—is precisely the extended Euclidean algorithm that underlies the decoding of Reed–Solomon and BCH codes [12, 13]. We make this explicit: halting the EROs at the first remainder of degree below the error-correction threshold recovers the error-locator and error-evaluator polynomials of the key equation in a single row of the augmented matrix (Theorem 6.3), and the accompanying Bézout coefficient at that halting index is, after normalisation, the connection polynomial computed by the Berlekamp–Massey algorithm [7], in accordance with the equivalence of that algorithm with the Euclidean one established by Cheng and Dornstetter [1, 2], building on the continued-fraction description of linear recurrences due to Mills [8] (see also [13]). A single matrix framework therefore unifies, across two dual valuations, the approximation-theoretic and the coding-theoretic faces of polynomial continued fractions.

**Contributions.** Our aim is a single matrix construction from which both faces of polynomial continued fractions are read off. (i) We establish the determinant invariant and the Bézout encoding over $\mathbb{F}_q[x]$ in an explicit closed form for the $2 \times 2$ block, which identifies its two columns with the convergent denominators and numerators (Theorem 3.1). (ii) From that invariant we derive in one ultrametric step the exact non-archimedean error equality at the infinite place—classical in the power-series setting [5, 11]—and contrast it explicitly with the archimedean interval (Theorem 4.1). (iii) We deduce

the corresponding best-polynomial-approximation property with respect to the degree valuation, within the non-archimedean continued-fraction framework of Welch and Scholtz [13], directly from the same block (Theorem 5.2). (iv) We give a dual-place reading of the identical construction that solves the Reed–Solomon key equation in the sense of Sugiyama et al. [12] and returns at its halting index, after normalisation, the connection polynomial of the Berlekamp–Massey algorithm [1,2,7,8] (Theorem 6.3).

## 2. Notation and Preliminaries

Throughout, $p$ is a prime, $\mathbb{F}_q$ is the finite field with $q = p^m$ elements, $\mathbb{F}_q[x]$ the polynomial ring, and $\mathbb{F}_q(x)$ its field of fractions. We equip $\mathbb{F}_q(x)$ with the absolute value at the *infinite place*,

$$|f| = q^{\deg f}, \qquad \deg(g/h) = \deg g - \deg h, \qquad \deg 0 := -\infty, \quad |0| = 0,$$

which is *non-archimedean*: $|f+g| \le \max(|f|,|g|)$, with the isosceles strengthening $|f| \neq |g| \Rightarrow |f+g| = \max(|f|,|g|)$. The completion at this place is the Laurent-series field $\mathbb{F}_q((1/x))$. A second, dual valuation—the finite $x$-adic place $\operatorname{ord}_x$, related to the infinite place by $x \mapsto 1/x$—is used only in Section 6.

Let $\alpha = a/b$ with $a, b \in \mathbb{F}_q[x]$ and $\gcd(a,b) = 1$, and let $\alpha = [a_0; a_1, \dots, a_n]$ be its continued fraction obtained from the Euclidean algorithm. Since each partial quotient arises as a quotient of polynomials of strictly decreasing degree, $\deg a_i \ge 1$ for all $i \ge 1$. The convergents $p_k/q_k$ satisfy, for $k \ge 0$,

$$p_k = a_k p_{k-1} + p_{k-2},\ p_{-1} = 1,\ p_{-2} = 0, \qquad q_k = a_k q_{k-1} + q_{k-2},\ q_{-1} = 0,\ q_{-2} = 1, \tag{1}$$

so that $p_0 = a_0$ and $q_0 = 1$.

The framework operates on the augmented matrix $M_0 = [\,I \mid v\,] = \left(\begin{smallmatrix} 1 & 0 & a \\ 0 & 1 & b \end{smallmatrix}\right)$, $v = (a,b)^{\mathsf{T}}$. With $r_0 = a$, $r_1 = b$, one sets

$$a_k = \lfloor r_k / r_{k+1} \rfloor \qquad (k \ge 0),$$

where $\lfloor g/h \rfloor$ denotes the polynomial quotient of $g$ by $h$ furnished by the division algorithm (equivalently, the polynomial part of the Laurent expansion of $g/h$ at the infinite place); one then applies the type-III operation $R_1 \to R_1 - a_k R_2$, followed by the type-I swap $R_1 \leftrightarrow R_2$, iterating until the $(2,3)$-entry vanishes. Since $\alpha = [a_0; a_1, \dots, a_n]$, the iteration performs exactly $n+1$ steps, producing the quotients $a_0, \dots, a_n$ and terminating with $r_{n+2} = 0$; this count uses only the length of the expansion. Under the standing hypothesis $\gcd(a,b) = 1$ the last nonzero remainder $r_{n+1}$, being a greatest common divisor of $a$ and $b$, lies in $\mathbb{F}_q^*$. Writing $A_k$ for the left $2 \times 2$ block after the $k$-th such step, the augmented column carries the remainder pair $(r_k, r_{k+1})^{\mathsf{T}}$, so that $A_0 = I$ and

$$A_{k+1} = E_k A_k, \qquad E_k = \begin{pmatrix} 0 & 1 \\ 1 & -a_k \end{pmatrix}, \qquad A_k v = (r_k, r_{k+1})^{\mathsf{T}}. \tag{2}$$

**Lemma 2.1** (Cassini–Euler). *For every $k \geq -2$ for which $p_{k+1}, q_{k+1}$ are defined, $p_{k+1}q_k - p_k q_{k+1} = (-1)^k \in \mathbb{F}_q$; in particular $|p_{k+1}q_k - p_k q_{k+1}| = 1$.*

*Proof.* For $k = -2$ and $k = -1$ the identity reads $p_{-1}q_{-2} - p_{-2}q_{-1} = 1$ and $p_0 q_{-1} - p_{-1}q_0 = -1$, both immediate from (1). For $k \geq 0$, induction on (1) gives $p_{k+1}q_k - p_k q_{k+1} = (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1}) = -(p_k q_{k-1} - p_{k-1}q_k) = (-1)^k$. □

**Lemma 2.2** (Degree growth). $\deg q_0 = 0$ *and* $\deg q_k = \sum_{i=1}^{k} \deg a_i$ *for* $k \geq 1$; *hence* $(\deg q_k)_{k\geq 0}$ *is strictly increasing.*

*Proof.* By induction $\deg q_{k-1} > \deg q_{k-2}$, so $\deg(a_k q_{k-1}) = \deg a_k + \deg q_{k-1} \geq 1 + \deg q_{k-1} > \deg q_{k-2}$. No leading-term cancellation occurs in $q_k = a_k q_{k-1} + q_{k-2}$, whence $\deg q_k = \deg a_k + \deg q_{k-1} > \deg q_{k-1}$. □

**Lemma 2.3** (Ultrametric strict domination). *Let $x_0, \ldots, x_m$ lie in a non-archimedean valued field. If $|x_0| > |x_j|$ for $1 \leq j \leq m$, then $\left|\sum_{j=0}^{m} x_j\right| = |x_0|$.*

*Proof.* Put $S = \sum_{j=1}^{m} x_j$. The ultrametric inequality gives $|S| \leq \max_{1\leq j\leq m} |x_j| < |x_0|$. Since $|x_0| \neq |S|$, the isosceles property yields $|x_0 + S| = |x_0|$. □

## 3. Determinant Invariant and Convergent Encoding

**Theorem 3.1** (Determinant invariant over $\mathbb{F}_q[x]$). *Let $A_k$ be the left $2 \times 2$ block of the augmented matrix after the $k$-th step. Then, for every $0 \leq k \leq n+1$,*

$$A_k = \begin{pmatrix} (-1)^k q_{k-2} & (-1)^{k+1} p_{k-2} \\ (-1)^{k+1} q_{k-1} & (-1)^{k+2} p_{k-1} \end{pmatrix}. \tag{3}$$

*Consequently $\det(A_k) = (-1)^k$; the first column of $A_k$ consists of the convergent denominators $q_{k-2}, q_{k-1}$ and the second of the convergent numerators $p_{k-2}, p_{k-1}$, each up to an alternating sign; and the first row $(u_k, v_k)$ of $A_k$ satisfies the Bézout identity*

$$u_k a + v_k b = r_k, \qquad \textit{explicitly} \qquad (-1)^k\big(q_{k-2}\, a - p_{k-2}\, b\big) = r_k. \tag{4}$$

*Proof.* We induct on $k$ using (2). For $k = 0$ the right-hand side of (3) is $\left(\begin{smallmatrix} q_{-2} & -p_{-2} \\ -q_{-1} & p_{-1} \end{smallmatrix}\right) = I = A_0$ by the initial data in (1). Assume (3) at $k$. Then $A_{k+1} = E_k A_k$ has first row equal to the second row of $A_k$, namely $\big((-1)^{k+1} q_{k-1},\ (-1)^{k+2} p_{k-1}\big)$, which is the first row of (3) with $k$ replaced by $k+1$; and second row

$$\big((-1)^k q_{k-2} - a_k(-1)^{k+1} q_{k-1},\ (-1)^{k+1} p_{k-2} - a_k(-1)^{k+2} p_{k-1}\big) = \big((-1)^k q_k,\ (-1)^{k+1} p_k\big)$$

by (1), which is the second row of (3) at $k+1$. This proves (3).

Expanding (3), $\det A_k = q_{k-2}p_{k-1} - p_{k-2}q_{k-1} = (-1)^{k-2} = (-1)^k$ by Lemma 2.1 applied at index $k-2 \geq -2$. (Equivalently: $\det A_0 = 1$, a type-III operation leaves the determinant unchanged, the type-I swap negates it, and each full step performs exactly one swap.) Finally, EROs preserve $A_k v = (r_k, r_{k+1})^{\mathsf{T}}$ as recorded in (2); its first coordinate is precisely (4). □

*Remark* 3.2. The signs in (3) alternate *entrywise*, so that no scalar can be factored out of a column of $A_k$: the first column is $\big((-1)^k q_{k-2}, (-1)^{k+1} q_{k-1}\big)^{\mathsf{T}}$, not a multiple of $(q_{k-2}, q_{k-1})^{\mathsf{T}}$. For instance, over $\mathbb{F}_3[x]$ with $a = 1 + 2x + 2x^2 + x^4$ and $b = x + x^3$ one finds $A_2 = \left(\begin{smallmatrix} q_0 & -p_0 \\ -q_1 & p_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -x \\ -(1+x) & 1+x+x^2 \end{smallmatrix}\right)$.

**Corollary 3.3** (Lowest terms)**.** *There is $c \in \mathbb{F}_q^*$ with $q_n = cb$ and $p_n = ca$; in particular $\alpha = p_n/q_n$, and this representation is in lowest terms.*

*Proof.* Take $k = n+1$ in (3): the second row of $A_{n+1}$ is $\big((-1)^{n+2} q_n,\ (-1)^{n+3} p_n\big)$, and by (2) it satisfies $A_{n+1} v = (r_{n+1}, r_{n+2})^{\mathsf{T}}$ with $r_{n+2} = 0$; reading the second coordinate gives $q_n a - p_n b = 0$. By Lemma 2.1 we have $\gcd(p_n, q_n) = 1$, so $q_n \mid b$; and $\gcd(a, b) = 1$ gives $b \mid q_n$. Hence $q_n = cb$ with $c \in \mathbb{F}_q^*$, and then $p_n = ca$. □

*Remark* 3.4. The proof of Theorem 3.1 uses only multiplicativity of the determinant and the ring structure of $\mathbb{F}_q[x]$, not the metric; the argument therefore applies verbatim over any Euclidean domain, the integer case included. The substantive consequences of the polynomial setting appear in Sections 4 and 6, which consume this invariant under two different valuations.

## 4. From Sharp Bounds to an Exact Equality

**Theorem 4.1** (Exact error equality)**.** *For every $0 \leq k \leq n-1$,*

$$\left| \alpha - \tfrac{p_k}{q_k} \right| = q^{-(\deg q_k + \deg q_{k+1})} = \frac{1}{|q_k|\,|q_{k+1}|},$$

*an exact equality.*

*Proof.* By Corollary 3.3, $\alpha = p_n/q_n$ in lowest terms. For $k \leq j \leq n-1$, Lemma 2.1 gives $\frac{p_{j+1}}{q_{j+1}} - \frac{p_j}{q_j} = \frac{(-1)^j}{q_j q_{j+1}}$, so telescoping the finite sum,

$$\alpha - \frac{p_k}{q_k} = \sum_{j=k}^{n-1} \frac{(-1)^j}{q_j q_{j+1}}.$$

The $j$-th term has absolute value $q^{-(\deg q_j + \deg q_{j+1})}$, which is strictly decreasing in $j$ by Lemma 2.2; the term $j = k$ strictly dominates. Lemma 2.3 then gives $|\alpha - p_k/q_k| = q^{-(\deg q_k + \deg q_{k+1})}$. □

*Remark* 4.2. The equality of Theorem 4.1 is classical in the power-series setting, where it is the standard replacement for the archimedean two-sided estimate; see [11] and the survey [5]. The point of the derivation above is that in the ERO framework it is not an independent input but a one-line consequence of the invariant of Theorem 3.1 together with Lemma 2.3.

*Remark* 4.3. If $q$ is even then $-1 = 1$; the signs vanish but $|\pm 1| = 1$, so the theorem holds in every characteristic.

*Remark* 4.4. Nothing in the proof uses finiteness of the expansion beyond the identification $\alpha = p_n/q_n$. If $\alpha \in \mathbb{F}_q((1/x)) \setminus \mathbb{F}_q(x)$ has infinite continued fraction $[a_0; a_1, a_2, \dots]$, then—granting the standard fact that its convergents tend to $\alpha$ in $\mathbb{F}_q((1/x))$—the telescoping series $\alpha - p_k/q_k = \sum_{j\geq k}(-1)^j/(q_j q_{j+1})$ converges in the completion and its terms have strictly decreasing absolute values by Lemma 2.2. Since $\mathbb{F}_q((1/x))$ is complete and $|\cdot|$ is continuous, the ultrametric inequality passes from the partial sums to their limit; and since the value group of $\mathbb{F}_q((1/x))$ is $q^{\mathbb{Z}}$, the tail $\sum_{j>k}$ then has absolute value at most $q^{-1}$ times that of the term $j = k$, so the argument of Lemma 2.3 applies with the finite sum replaced by the series. Hence the equality of Theorem 4.1, and with it Theorem 5.2 below, holds for every $k \geq 0$ in that case as well.

*Remark* 4.5. Over $\mathbb{Q}$ the identical telescoping is an alternating *archimedean* series; strict domination fails and one recovers only the classical two-sided interval $\frac{1}{q_k(q_k+q_{k+1})} \leq |\alpha - p_k/q_k| \leq \frac{1}{q_k q_{k+1}}$ (see e.g. [3,4,10]; with the normalisation produced by the Euclidean algorithm, for which $a_n \geq 2$, the left inequality is in fact strict). The equality above is therefore a genuinely non-archimedean phenomenon, not a notational restatement.

## 5. Best Polynomial Approximation

Write $\varepsilon_j := \alpha q_j - p_j = q_j(\alpha - p_j/q_j)$. By Theorem 4.1,

$$|\varepsilon_j| = |q_j| \cdot q^{-(\deg q_j + \deg q_{j+1})} = q^{-\deg q_{j+1}}, \tag{5}$$

for $0 \leq j \leq n-1$; at $j = n$ one has $\varepsilon_n = \alpha q_n - p_n = 0$ since $\alpha = p_n/q_n$. Over this range $|\varepsilon_j|$ is strictly decreasing in $j$. For $0 \leq k \leq n-1$, setting $c_k = (p_k, q_k)^{\mathsf{T}}$ and $c_{k+1} = (p_{k+1}, q_{k+1})^{\mathsf{T}}$, Lemma 2.1 gives $\det(c_k\ c_{k+1}) = p_k q_{k+1} - p_{k+1} q_k = (-1)^{k+1} \in \mathbb{F}_q^*$, a unit; hence $c_k, c_{k+1}$ form an $\mathbb{F}_q[x]$-basis of $\mathbb{F}_q[x]^2$.

**Lemma 5.1** (Minimal residue)**.** *Fix $0 \leq k \leq n-1$ and let $r, s \in \mathbb{F}_q[x]$ with $(r, s) \neq (0, 0)$ and $\deg s < \deg q_{k+1}$. Then $|\alpha s - r| \geq |\alpha q_k - p_k| = q^{-\deg q_{k+1}}$, with equality iff $(r, s) = c(p_k, q_k)$ for some $c \in \mathbb{F}_q^*$.*

*Proof.* Write $(r, s)^{\mathsf{T}} = A\, c_k + B\, c_{k+1}$ with $A, B \in \mathbb{F}_q[x]$, so $s = Aq_k + Bq_{k+1}$ and $\alpha s - r = A\varepsilon_k + B\varepsilon_{k+1}$; since $c_k, c_{k+1}$ is a basis and $(r, s) \neq (0, 0)$, we have $(A, B) \neq (0, 0)$.

If $B \neq 0$, then $\deg(Bq_{k+1}) \geq \deg q_{k+1} > \deg s$; in particular $A \neq 0$, since $A = 0$ would give $s = Bq_{k+1}$ of degree at least $\deg q_{k+1}$. Hence $Bq_{k+1}$ must be cancelled in $s$ by $Aq_k$, forcing $\deg A = \deg B + (\deg q_{k+1} - \deg q_k) = \deg B + \deg a_{k+1} \geq 1$. Then, by (5), $|A\varepsilon_k| = |A| q^{-\deg q_{k+1}} \geq q^{\deg a_{k+1}} q^{-\deg q_{k+1}} = q^{-\deg q_k} > q^{-\deg q_{k+1}}$. If $k+1 = n$ then $\varepsilon_{k+1} = \varepsilon_n = 0$ and $\alpha s - r = A\varepsilon_k$ directly; otherwise $|A\varepsilon_k|/|B\varepsilon_{k+1}| = q^{(\deg A - \deg B) + (\deg q_{k+2} - \deg q_{k+1})} > 1$. In either case $|\alpha s - r| = |A\varepsilon_k| > q^{-\deg q_{k+1}}$ by domination.

If $B = 0$, then $A \neq 0$, $(r, s) = A(p_k, q_k)$ and $|\alpha s - r| = |A| q^{-\deg q_{k+1}} \geq q^{-\deg q_{k+1}}$, with equality iff $|A| = 1$, i.e. $A \in \mathbb{F}_q^*$. □

**Theorem 5.2** (Best approximation; cf. Welch–Scholtz [13]). *Fix $0 \leq k \leq n-1$. For every $r, s \in \mathbb{F}_q[x]$ with $s \neq 0$, $\deg s \leq \deg q_k$ and $r/s \neq p_k/q_k$,*

$$\left|\alpha - \tfrac{p_k}{q_k}\right| < \left|\alpha - \tfrac{r}{s}\right|.$$

*Proof.* Since $s \neq 0$ we have $(r, s) \neq (0, 0)$, and $\deg s \leq \deg q_k < \deg q_{k+1}$, so Lemma 5.1 applies. If $\deg s < \deg q_k$,

$$\left|\alpha - \tfrac{r}{s}\right| = \frac{|\alpha s - r|}{|s|} \geq \frac{q^{-\deg q_{k+1}}}{|s|} > \frac{q^{-\deg q_{k+1}}}{q^{\deg q_k}} = q^{-(\deg q_k + \deg q_{k+1})} = \left|\alpha - \tfrac{p_k}{q_k}\right|.$$

If $\deg s = \deg q_k$ but $r/s \neq p_k/q_k$, then $(r, s)$ is not of the form $c(p_k, q_k)$ with $c \in \mathbb{F}_q^*$, so Lemma 5.1 gives the strict inequality $|\alpha s - r| > q^{-\deg q_{k+1}}$, whence $|\alpha - r/s| > q^{-(\deg q_k + \deg q_{k+1})} = |\alpha - p_k/q_k|$. □

*Remark* 5.3. Theorem 5.2 includes the case $k = 0$, in contrast with its archimedean counterpart: over $\mathbb{Q}$ the convergent $p_0/q_0 = a_0$ need not be a best approximation among fractions with denominator at most $q_0 = 1$. For instance, for $5/3 = [1; 1, 2]$ one has $|5/3 - p_0/q_0| = |5/3 - 1| = 2/3$, while $2/1$ has the same denominator and $|5/3 - 2| = 1/3$. The obstruction is the possibility of rounding $a_0$ upwards, and the ultrametric removes it: if $\deg s \leq \deg q_0 = 0$ then $s \in \mathbb{F}_q^*$, so $r/s$ is a polynomial, and $r/s \neq p_0/q_0 = a_0$ makes $a_0 - r/s$ a nonzero polynomial, whence $|a_0 - r/s| \geq 1$. Since $|\alpha - a_0| = q^{-\deg q_1} < 1$ by Theorem 4.1, the isosceles property gives $|\alpha - r/s| = |a_0 - r/s| \geq 1 > |\alpha - p_0/q_0|$. The exception that the archimedean theory must carry therefore disappears over $\mathbb{F}_q[x]$.

## 6. The Dual Place: Reed–Solomon Key Equation and Berlekamp–Massey

Read now at the finite $x$-adic place. Given a syndrome polynomial $S \in \mathbb{F}_q[x]$ with $\deg S < 2t$ from the decoding of a Reed–Solomon or BCH code correcting up to $t$ errors, the key equation asks for an error locator $\sigma$ and error evaluator $\omega$ with

$$\sigma(x) S(x) \equiv \omega(x) \pmod{x^{2t}}, \qquad \deg \omega < \deg \sigma \leq t,\ \sigma(0) \neq 0,\ \gcd(\sigma, \omega) = 1.$$

In terms of that valuation the congruence reads $\operatorname{ord}_x(\sigma S - \omega) \geq 2t$, and since $\sigma(0) \neq 0$ it is equivalent to $\operatorname{ord}_x\big(S - \omega/\sigma\big) \geq 2t$: the key equation asks for a rational function of controlled degree approximating $S$ to order $2t$ at the finite place. This is the counterpart there of the approximation problem solved at the infinite place in Sections 4 and 5. Throughout this section the framework of Section 2 is run on $v = (x^{2t}, S)^{\mathsf{T}}$, i.e. with $a = x^{2t}$, $b = S$, $r_0 = x^{2t}$, $r_1 = S$, so that $\alpha = x^{2t}/S$ and (4) reads $u_k x^{2t} + v_k S = r_k$. The coprimality convention of Section 2 is *not* in force here: $\gcd(x^{2t}, S)$ is a power of $x$, and a nontrivial one whenever the first syndrome vanishes. This is harmless: nothing in this section uses coprimality,

since Theorem 3.1 and Lemma 6.1 rest only on (1) and (2), and everything below rests on those two results. The hypothesis enters only through Corollary 3.3, hence only in Sections 4 and 5.

**Lemma 6.1** (Degree identity)**.** *For every $k \geq 1$ for which $A_{k-1}$ is defined, one has* $\deg v_k = 2t - \deg r_{k-1}$.

*Proof.* By (2), the second rows of consecutive blocks give $v_{k+2} = v_k - a_k v_{k+1}$, with $v_0 = 0$ and $v_1 = 1$. Here $\deg a_0 \geq 1$, because $\deg r_0 = 2t > \deg S$; and $\deg a_k \geq 1$ for $k \geq 1$, as in Section 2. Hence no leading-term cancellation occurs, so that $(\deg v_k)_{k\geq 1}$ is strictly increasing while $(\deg r_k)_{k\geq 0}$ is strictly decreasing.

By Theorem 3.1 we have $A_{k-1} v = (r_{k-1}, r_k)^{\mathsf{T}}$ and $\det A_{k-1} = (-1)^{k-1}$, so that

$$v = (-1)^{k-1} \operatorname{adj}(A_{k-1}) \, (r_{k-1}, r_k)^{\mathsf{T}}.$$

Reading the first coordinate gives

$$x^{2t} = (-1)^{k-1} \big( v_k r_{k-1} - v_{k-1} r_k \big).$$

Since $\deg v_k > \deg v_{k-1}$ and $\deg r_{k-1} > \deg r_k$, we have $\deg(v_k r_{k-1}) > \deg(v_{k-1} r_k)$, so by Lemma 2.3 the left-hand term dominates and $\deg v_k + \deg r_{k-1} = 2t$. □

For the rest of this section we fix the following data, used in Lemma 6.2 and Theorem 6.3: an integer $e$ with $1 \leq e \leq t$, a polynomial $S$ with $\deg S < 2t$, and a pair $\sigma_0, \omega_0 \in \mathbb{F}_q[x]$ with

$$\sigma_0 S \equiv \omega_0 \pmod{x^{2t}}, \qquad \deg \sigma_0 = e, \quad \deg \omega_0 < e, \quad \sigma_0(0) = 1, \quad \gcd(\sigma_0, \omega_0) = 1.$$

The motivating instance is the decoding one: if $S$ is the syndrome of an error pattern of weight $e$, with error locators $X_1, \ldots, X_e \in \mathbb{F}_q^*$ and values $Y_1, \ldots, Y_e$, then $\sigma_0 = \prod_i (1 - X_i x)$ and $\omega_0 = \sum_i Y_i X_i \prod_{j \neq i} (1 - X_j x)$ satisfy all of the above. Only the displayed conditions are used below, however; in particular $\sigma_0$ need not split over $\mathbb{F}_q$, and in Example 7.3 it does not.

**Lemma 6.2** (Minimality)**.** *Let $k \geq 1$ be an index for which $A_k$ is defined, and suppose*

$$\deg v_k \leq e \qquad \textit{and} \qquad \deg r_k < 2t - e.$$

*Then $v_k = c\,\sigma_0$ and $r_k = c\,\omega_0$ for some $c \in \mathbb{F}_q^*$.*

*Proof.* By Theorem 3.1, $v_k S \equiv r_k \pmod{x^{2t}}$, while $\sigma_0 S \equiv \omega_0 \pmod{x^{2t}}$ by hypothesis. Multiplying the first congruence by $\sigma_0$, the second by $v_k$, and subtracting gives $\sigma_0 r_k \equiv \omega_0 v_k \pmod{x^{2t}}$. Both sides have degree less than $2t$: indeed $\deg(\sigma_0 r_k) < e + (2t - e) = 2t$, and $\deg(\omega_0 v_k) \leq (e-1) + e \leq 2t - 1$ because $e \leq t$. Hence

$$\sigma_0 \, r_k = \omega_0 \, v_k.$$

Since $\gcd(\sigma_0, \omega_0) = 1$, we get $\sigma_0 \mid v_k$; moreover $v_k \neq 0$, because $\deg r_{k-1} \leq 2t$ and so Lemma 6.1 gives $\deg v_k = 2t - \deg r_{k-1} \geq 0$. Therefore $\deg v_k \geq \deg \sigma_0 = e$. Together with $\deg v_k \leq e$ this forces $v_k = c\sigma_0$ with $c \in \mathbb{F}_q^*$, and then $r_k = c\omega_0$. □

**Theorem 6.3** (ERO solution of the key equation)**.** *With $S$, $e$, $\sigma_0$, $\omega_0$ as above, run the ERO framework on $M_0 = [\, I_2 \mid v \,]$, $v = (x^{2t}, S)^{\mathsf{T}}$, halting at the first index $k^\star$ with $\deg r_{k^\star} < t$. Then:*

(i) *$v_{k^\star}(0) \neq 0$, and $\sigma := v_{k^\star}/v_{k^\star}(0)$, $\omega := r_{k^\star}/v_{k^\star}(0)$ satisfy $\sigma = \sigma_0$ and $\omega = \omega_0$; in particular the pair $(\sigma, \omega)$ solves the key equation;*

(ii) *$\deg \sigma = e \leq t$, $\deg \omega < \deg \sigma$ and $\gcd(\sigma, \omega) = 1$; moreover $\sigma$ is of least degree among all solutions of the key equation, in the sense that every pair $(\lambda, \mu)$ with $\lambda S \equiv \mu \pmod{x^{2t}}$, $\deg \mu < \deg \lambda \leq t$ and $\gcd(\lambda, \mu) = 1$ satisfies $\deg \lambda \geq \deg \sigma$;*

(iii) *the Bézout coefficients $v_1, \ldots, v_{k^\star}$ appearing in the second column of the blocks $A_1, \ldots, A_{k^\star}$ are, by (3), the convergent numerators $p_{-1}, \ldots, p_{k^\star-2}$ of $\alpha = x^{2t}/S$, up to sign; equivalently, they are the denominators of the convergents of the reciprocal expansion $S/x^{2t}$. In particular $\sigma = v_{k^\star}/v_{k^\star}(0)$ is the connection polynomial returned by the Berlekamp–Massey algorithm [7] applied to the coefficient sequence of $S$, as the classical equivalence of the two algorithms predicts [1, 2, 8, 9, 13]. Away from the halting index the correspondence is looser than a step-by-step identification: it is stated only up to reciprocation and a normalising scalar [2], and a single Euclidean step may absorb several Berlekamp–Massey iterations [1]. Accordingly the coefficients $v_k$ with $k < k^\star$ need not themselves be connection polynomials of that sequence, and may even vanish at 0. Finally, the first row $(u_{k^\star}, v_{k^\star} \mid r_{k^\star})$ of the augmented matrix at step $k^\star$ exhibits $\sigma$ and $\omega$ simultaneously, with $\det A_{k^\star} = \pm 1$.*

*Proof.* Let $j$ be the least index with $\deg r_j < 2t - e$. Such a $j$ exists, with $A_j$ defined, because the remainder degrees strictly decrease while $\deg r_{n+1} = \operatorname{ord}_x S = \operatorname{ord}_x \omega_0 \leq e - 1 < 2t - e$, forcing $j \leq n + 1$; and $j \geq 1$ because $\deg r_0 = 2t$. By minimality of $j$ we have $\deg r_{j-1} \geq 2t - e$, so Lemma 6.1 gives

$$\deg v_j = 2t - \deg r_{j-1} \leq e.$$

Thus Lemma 6.2 applies at $k = j$ and yields $v_j = c\sigma_0$, $r_j = c\omega_0$ with $c \in \mathbb{F}_q^*$. In particular $\deg r_j = \deg \omega_0 \leq e - 1 < t$, so the halting index satisfies $k^\star \leq j$; conversely $\deg r_{k^\star} < t \leq 2t - e$, so $j \leq k^\star$ by minimality of $j$. Hence $k^\star = j$ and

$$v_{k^\star} = c\,\sigma_0, \qquad r_{k^\star} = c\,\omega_0.$$

Consequently $v_{k^\star}(0) = c\,\sigma_0(0) = c \neq 0$, and $\sigma = v_{k^\star}/c = \sigma_0$, $\omega = r_{k^\star}/c = \omega_0$; this is (i), and the first three assertions of (ii) follow at once from the listed properties of $(\sigma_0, \omega_0)$. For the minimality assertion in (ii), let $(\lambda, \mu)$ be as stated. Multiplying $\lambda S \equiv \mu$ by $\sigma_0$ and $\sigma_0 S \equiv \omega_0$ by $\lambda$ and subtracting gives $\sigma_0\mu \equiv \omega_0\lambda \pmod{x^{2t}}$; both sides have degree at most $e + (t-1) \leq 2t - 1$ and $(e-1) + t \leq 2t - 1$

respectively, so $\sigma_0\mu = \omega_0\lambda$, and $\gcd(\sigma_0, \omega_0) = 1$ gives $\sigma_0 \mid \lambda$; since $\deg\mu < \deg\lambda$ forces $\lambda \neq 0$, this yields $\deg\lambda \geq e = \deg\sigma$.

Part (iii) is the identification (3) of the second column of $A_k$ with the convergent numerators of $\alpha = x^{2t}/S$; that $\sigma$ is the polynomial returned by the Berlekamp–Massey algorithm is the classical equivalence of the Euclidean and Berlekamp–Massey recursions [1,2,7–9,13]. For the caveat, (4) gives $v_k S \equiv r_k \pmod{x^{2t}}$, so the coefficient of $x^j$ in $v_k S$ vanishes for $\deg r_k < j \leq 2t-1$ and need not vanish for $j \leq \deg r_k$, whereas a connection polynomial of degree $L$ for the coefficient sequence of $S$ requires vanishing for every $j \geq L$. For $k < k^\star$ we have $\deg r_{k-1} > \deg r_k \geq t$, so Lemma 6.1 gives $\deg v_k = 2t - \deg r_{k-1} \leq t-1 < \deg r_k$ and the two ranges differ. Finally, the statement about the first row is (4) at $k = k^\star$, divided by $c$. □

*Remark* 6.4. Theorems 4.1 and 6.3 are the same matrix machine read at two dual places: at the infinite place it computes best rational approximation; at the finite $x$-adic place it performs algebraic decoding. The substitution $x \mapsto 1/x$ interchanges them.

## 7. Computational Examples

**Example 7.1** (Error equality over $\mathbb{F}_3[x]$)**.** Let $\alpha = a/b = (1+2x+2x^2+x^4)/(x+x^3) \in \mathbb{F}_3(x)$, with continued fraction $[\,x;\ 1{+}x,\ x,\ 2{+}x\,]$. Table 1 lists the convergents; the computed value of $\deg(\alpha - p_k/q_k)$ matches $-(\deg q_k + \deg q_{k+1})$ exactly for every $k \leq n-1$ (a table of equalities, in contrast to the interval table of the integer case).

Table 1. Convergents of $\alpha$ over $\mathbb{F}_3[x]$; $\deg(\alpha - p_k/q_k)$ equals $-(\deg q_k + \deg q_{k+1})$ exactly.

| $k$ | $a_k$ | $p_k/q_k$ | $\deg q_k$ | $\deg(\alpha - p_k/q_k) = -(\deg q_k + \deg q_{k+1})$ |
|---|---|---|---|---|
| 0 | $x$ | $x/1$ | 0 | $-1$ |
| 1 | $1+x$ | $(1+x+x^2)/(1+x)$ | 1 | $-3$ |
| 2 | $x$ | $(2x+x^2+x^3)/(1+x+x^2)$ | 2 | $-5$ |
| 3 | $2+x$ | $\alpha$ | 3 | — |

**Example 7.2** (Key equation over $\mathbb{F}_5[x]$)**.** Let $t = 2$, $\sigma = 1+3x+2x^2$, $\omega = 4+x$; then $S = \sigma^{-1}\omega \bmod x^4 = 4+4x+2x^3$. The EROs on $[\,I \mid (x^4, S)^{\mathsf{T}}]$ produce the remainder sequence

$$r_0 = x^4, \quad r_1 = 4+4x+2x^3, \quad r_2 = 3x+3x^2, \quad r_3 = 4+x,$$

and halt at $k^\star = 3$, the first index with $\deg r_{k^\star} = 1 < t$. The halting step returns $v_{k^\star} = 1+3x+2x^2 = \sigma$ and $r_{k^\star} = 4+x = \omega$ exactly, with $v_{k^\star}(0) = 1$, in accordance with $\deg\sigma = 2t - \deg r_{k^\star-1} = 4-2 = 2$.

**Example 7.3** (Characteristic two, $\mathbb{F}_2[x]$)**.** Let $t = 2$, $\sigma = 1 + x + x^2$ (irreducible over $\mathbb{F}_2$), $\omega = 1 + x$; then $S = 1 + x^2 + x^3$. The remainder sequence is

$$r_0 = x^4, \quad r_1 = 1 + x^2 + x^3, \quad r_2 = 1 + x + x^2, \quad r_3 = 1 + x,$$

so the EROs halt at $k^\star = 3$ and recover $v_{k^\star} = \sigma$ and $r_{k^\star} = \omega$ exactly, again with $\deg \sigma = 2t - \deg r_{k^\star - 1} = 4 - 2 = 2$, confirming Theorem 6.3 in the characteristic relevant to practical Reed–Solomon parameters. Here $\sigma$ is irreducible, so the pair $(\sigma, \omega)$ does not arise from an error pattern with locators in $\mathbb{F}_2$; it satisfies the conditions fixed at the start of Section 6, which is all that Theorem 6.3 requires.

## 8. Conclusion

We have transported the augmented-matrix ERO framework for continued fractions to $\mathbb{F}_q[x]$, obtaining the block invariant (3) in closed form, and shown that the non-archimedean structure has genuine consequences within it: the integer error *interval* becomes an *exact equality* (Theorem 4.1), classical in the power-series setting but here a one-line corollary of the invariant, from which best polynomial approximation in the sense of Welch and Scholtz follows cleanly (Theorem 5.2), and without the exception at $k = 0$ that the archimedean theory must carry (Remark 5.3); and the same machine, read at the dual finite place, solves the Reed–Solomon key equation and returns the Berlekamp–Massey connection polynomial at its halting index (Theorem 6.3). Natural directions include continued fractions over $\mathbb{Z}[i]$ and other imaginary-quadratic Euclidean domains—where the absence of a total order makes the error analysis modulus-based and substantially harder—together with multisequence readings of the same framework.

**Authors' Contributions.** Both authors contributed equally to every stage of this work: the conception of the framework, the formulation and proofs of all results, the computational verification of the examples, and the writing of the manuscript. The authors have read and approved the final version.

**Conflicts of Interest.** The authors declare that there are no conflicts of interest regarding the publication of this paper.

## References

[1] U. Cheng, On the Continued Fraction and Berlekamp's Algorithm (Corresp.), IEEE Trans. Inf. Theory 30 (1984), 541–544. https://doi.org/10.1109/TIT.1984.1056906.

[2] J. Dornstetter, On the Equivalence between Berlekamp's and Euclid's Algorithms (Corresp.), IEEE Trans. Inf. Theory 33 (1987), 428–431. https://doi.org/10.1109/TIT.1987.1057299.

[3] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 2008.

[4] A.Ya. Khinchin, Continued Fractions, Dover Publications, 1997.

[5] A. Lasjaunias, A Survey of Diophantine Approximation in Fields of Power Series, Monatsh. Math. 130 (2000), 211–229. https://doi.org/10.1007/s006050070036.

[6] A. Lasjaunias, Continued Fractions for Hyperquadratic Power Series over a Finite Field, Finite Fields Appl. 14 (2008), 329–350. https://doi.org/10.1016/j.ffa.2007.01.001.

[7] J. Massey, Shift-Register Synthesis and BCH Decoding, IEEE Trans. Inf. Theory 15 (1969), 122–127. https://doi.org/10.1109/TIT.1969.1054260.

[8] W.H. Mills, Continued Fractions and Linear Recurrences, Math. Comput. 29 (1975), 173–180. https://doi.org/10.2307/2005473.

[9] H. Niederreiter, Sequences with Almost Perfect Linear Complexity Profile, in: D. Chaum, W.L. Price, (eds) Advances in Cryptology — EUROCRYPT '87, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, pp. 37–51, (1988). https://doi.org/10.1007/3-540-39118-5_5.

[10] A.M. Rockett, P. Szüsz, Continued Fractions, World Scientific, 1992. https://doi.org/10.1142/1725.

[11] W. Schmidt, On Continued Fractions and Diophantine Approximation in Power Series Fields, Acta Arith. 95 (2000), 139–166. https://doi.org/10.4064/aa-95-2-139-166.

[12] Y. Sugiyama, M. Kasahara, S. Hirasawa, T. Namekawa, A Method for Solving Key Equation for Decoding Goppa Codes, Inf. Control 27 (1975), 87–99. https://doi.org/10.1016/S0019-9958(75)90090-X.

[13] L. Welch, R. Scholtz, Continued Fractions and Berlekamp's Algorithm, IEEE Trans. Inf. Theory 25 (1979), 19–27. https://doi.org/10.1109/TIT.1979.1055987.

[14] W. Yonwilad, N. Thongmual, C. Sahatsathatsana, W. Pimpasalee, S. Hobanthad, A Matrix Elementary Operations Framework for Best Rational Approximation via Continued Fractions, Int. J. Math. Comput. Sci. 21 (2026), 535–539. https://doi.org/10.69793/ijmcs/02.2026/yonwilad.