Bull. Aust. Math. Soc. **111** (2025), 260–271
doi:10.1017/S0004972724000601

ON THE BINARY SEQUENCE $(1, 1, 0, 1, 0^3, 1, 0^7, 1, 0^{15}, \ldots)$

GRAHAM H. NORTON

(Received 7 May 2024; accepted 30 May 2024; first published online 23 October 2024)

Dedicated to Gladys Jackson (1922–2012) in loving memory

Abstract

Let $\mathbb{F}$ be a field and $(s_0, \ldots, s_{n-1})$ be a finite sequence of elements of $\mathbb{F}$. In an earlier paper [G. H. Norton, 'On the annihilator ideal of an inverse form', *J. Appl. Algebra Engrg. Comm. Comput.* **28** (2017), 31–78], we used the $\mathbb{F}[x, z]$ submodule $\mathbb{F}[x^{-1}, z^{-1}]$ of Macaulay's inverse system $\mathbb{F}[[x^{-1}, z^{-1}]]$ (where z is our homogenising variable) to construct generating forms for the (homogeneous) annihilator ideal of $(s_0, \ldots, s_{n-1})$. We also gave an $O(n^2)$ algorithm to compute a special pair of generating forms of such an annihilator ideal. Here we apply this approach to the sequence r of the title. We obtain special forms generating the annihilator ideal for $(r_0, \ldots, r_{n-1})$ without polynomial multiplication or division, so that the algorithm becomes linear. In particular, we obtain its linear complexities. We also give additional applications of this approach.

2020 *Mathematics subject classification*: primary 13P10; secondary 11Y16, 94A55.

Keywords and phrases: annihilator ideal, finite sequence, form, homogeneous ideal, linear complexity, Macaulay's inverse system.

1. Introduction

The binary sequence $r = (1, 1, 0, 1, 0^3, 1, 0^7, 1, 0^{15}, 1, \ldots)$ has been studied by a number of authors. In [11], Rueppel conjectured that r has a perfect linear complexity profile (PLCP), that is, for any $n \geq 1$, the linear complexity of the first n terms is $\lfloor (n+1)/2 \rfloor$. According to Dai [1, page 441], this was verified by Massey for $n = 2^k - 1$ and $n = 2^k$ using his linear-feedback shift register (LFSR) algorithm [5]. The PLCP of this sequence was first proved in [1] by applying the Euclidean algorithm (EA) to shift-register synthesis; the essential proposition [1, Proposition 2] is proved in [2, Lemma 5]. The proof in [1] also uses an unmotivated element ρ in a quadratic extension of the rational function field GF(2)(x).

The continued fraction algorithm for the power series of r in GF(2)$[[x^{-1}]]$ was used in [6, Corollary 2], a quadratic algorithm requiring polynomial division. We note that the methods of [4, page 439] and [3, Example 4.8] do not apply since the first $2b$ terms of the sequence are required, where b is an upper bound for the linear complexity (LC)

of the sequence of length $2b$ (compare [3, Example 4.8] and [10, Example 3.7]). A derivation via the LFSR algorithm for $n = 2^k$ appeared in [12, pages 46–47]. However, the derivation in [12] *assumes* that the 'discrepancy' $\Delta_n = 1$ if and only if n is odd. As far as we know, the PLCP of r has not been established using the LFSR algorithm.

Let $\mathbb{F}$ be any field. Recall that the $\mathbb{F}[x, z]$ module $\mathbb{F}[[x^{-1}, z^{-1}]]$ of 'inverse series' in variables x^{-1}, z^{-1} is known as Macaulay's inverse system (in two variables, z will be our homogenising variable). Now, $\mathbb{F}[x^{-1}, z^{-1}]$ is an $\mathbb{F}[x, z]$ submodule of $\mathbb{F}[[x^{-1}, z^{-1}]]$. This elementary algebraic structure underlies our approach. The sequence $(s_0, \ldots, s_{n-1})$ has a 'generating form' $s_{n-1}x^{1-n} + \cdots + s_0 z^{1-n}$ and hence a (homogeneous) annihilator ideal. In [8], we gave an inductive construction for the generators of such an ideal, yielding an $O(n^2)$ algorithm which is easier to understand, analyse and remember than the LFSR algorithm.

Here, we specialise to $\mathbb{F} = \mathrm{GF}(2)$ and r, with $(r_0, \ldots, r_9)$ and its inverse form as a running example (see Examples 4.2, 4.3). Our main results are Theorem 4.4 and *linear* Algorithm 4.7. We conclude by relating Theorem 4.4 to [1] and LFSRs.

Our approach is simpler and more efficient than the previous $O(n^2)$ methods in the literature and: (i) it is inductive, adapting to the next term of the sequence, so we do not need all of $(r_0, \ldots, r_{n-1})$ as in [1]; (ii) it does not use multiplication in $\mathbb{F}[x, y]$; (iii) we do not use the roots ρ, ρ^{-1} of $Y^2 + xY + 1$ in an extension of $\mathrm{GF}(2)(x)$ as in [1]. In fact, ρ arises naturally in the solution of a polynomial recurrence (Theorem 4.9); (iv) we do not assume an upper bound b on LC and $2b$ terms of the sequence as in [3, 4]; (v) unlike [6], we use no polynomial multiplications or divisions, but work with forms in $\mathbb{F}[x^{-1}, z^{-1}]$, so there are no convergence or irrationality considerations and we work with denominators only.

2. Preliminaries

We let $\mathbb{F}$ be an arbitrary field. For $f \in \mathbb{F}[x]^\times$, we write f^* for the reciprocal of f. We put $\mathrm{R} = \mathbb{F}[x, z]$; multiplication in R is written as juxtaposition. For $\varphi, \varphi' \in \mathrm{R}$ and $k \in \mathbb{N}^\times$, $x^k\varphi + \varphi'$ means $x^k\varphi(x, z) + \varphi'(x, z)$ and similarly for $\varphi + z^k\varphi'$. The total degree of $\varphi \in \mathrm{R}^\times$ is $|\varphi|$, with $|x| = |z| = 1$. The ideal of R generated by $\varphi, \psi \in \mathrm{R}$ is written $\langle \varphi, \psi \rangle$.

We write $\succ$ for the graded-lexicographic order (grlex) on monomials of $\mathrm{R}^\times$, with $|x| = |z| = 1$ and $x \succ z \succ 1$. The leading term of a form $\varphi \in \mathrm{R}$ is written $\mathrm{LT}(\varphi)$. We define $\mathcal{L}$ to be the set of *'leading forms'*:

$$\mathcal{L} = \{\varphi \in \mathrm{R}^\times : \varphi \text{ is a form and } z \nmid \mathrm{LT}(\varphi)\}.$$

We also use $|\ |$ for the degree function on $\mathbb{F}[x]$, with $|0| = -\infty$. Recall that the *homogenisation* of $c \in \mathbb{F}[x]^\times$ is the form $c^\wedge \in \mathrm{R}$ given by $c(x, z) = z^{|c|}c(x/z)$ and the *dehomogenisation* of $f \in \mathrm{R}[x, z]^\times \cap \mathcal{L}$ is $f^\vee(x) = f(x, 1) \in \mathbb{F}[x]$.

Throughout the paper, $F \in \mathrm{M}^\times = \mathbb{F}[x^{-1}, z^{-1}]^\times$ denotes a typical nonzero inverse form of total degree $m = |F| \leq 0$. We also order the monomials of $\mathrm{M}^\times$ using grlex, now written $\prec$, but with $|x^{-1}| = |z^{-1}| = -1$ and $x^{-1} \prec z^{-1} \prec 1$.

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

If F is also a form, that is, an *inverse form*, we write $F = \sum_{j=m}^{0} F_{j,m-j}x^j z^{m-j}$; *when m is understood, we write F_j for $F_{j,m-j}$*. We will use a restriction of the exponential valuation v for inverse forms: the *order* of F is

$$\mathrm{v} = \mathrm{v}(F) = \max\{j : |F| \le j \le 0, F_j \neq 0\}.$$

The *augmentation of F by $a \in \mathbb{F}$* is $ax^{m-1} + Fz^{-1}$, an inverse form of total degree $m-1$. For example, the augmentation of z^m by a is $ax^{m-1} + z^{m-1}$. A form F defines (nonzero) *inverse subforms* $\{F^{(j)} : m \le j \le \mathrm{v}\}$ by $F^{(\mathrm{v})} = x^{\mathrm{v}}$ and

$$F^{(j)} = F_j x^j + F^{(j+1)}z^{-1} = F_j x^j + \cdots + x^{\mathrm{v}} z^{j-\mathrm{v}} \quad \text{for } m \le j \le \mathrm{v}-1.$$

Throughout, $n \ge 1$, $(s_0, \ldots, s_{n-1})$ *is a nonzero sequence (of elements of* $\mathbb{F}$) and $F = F_{(s_0,\ldots,s_{n-1})} = s_{n-1}x^{1-n} + \cdots + s_0 z^{1-n}$ is the *inverse form* of $(s_0, \ldots, s_{n-1})$; $s_{-\mathrm{v}(F)}$ corresponds to the first nonzero term of the sequence, $ax^{m-1} + Fz^{-1}$ corresponds to the augmented sequence $(s_0, \ldots, s_{n-1}, a)$ and the inverse subforms of F correspond to (nonzero) initial subsequences of $(0, \ldots, 0, s_{-\mathrm{v}(F)}, \ldots, s_{n-1})$.

We recall the R submodule $\mathrm{M} = \mathbb{F}[x^{-1}, z^{-1}]$ of inverse polynomials.

DEFINITION 2.1. For nonnegative integers p, q, u, v,

$$x^p z^q \circ x^{-u} z^{-v} = \begin{cases} x^{p-u} z^{q-v} & \text{if } p-u \le 0, q-v \le 0, \\ 0 & \text{otherwise.} \end{cases} \tag{2.1}$$

The R module structure of M is obtained by linearly extending (2.1) to all of R and M.

By linearity and without loss of generality, we can *assume that an inverse form F satisfies $F_{\mathrm{v}} = 1$*, that is, $F = F_m x^m + \cdots + F_{\mathrm{v}-1}x^{\mathrm{v}-1}z^{m-\mathrm{v}+1} + x^{\mathrm{v}}z^{m-\mathrm{v}}$.

The *annihilator ideal* of an inverse form F is $\mathcal{I}_F = \{\varphi \in \mathrm{R} : \varphi \circ F = 0\}$.

PROPOSITION 2.2 [8, Proposition 3.7]. *The ideal $\mathcal{I}_F$ is homogeneous.*

PROPOSITION 2.3 [8, Lemma 3.1]. *For forms $\varphi \in \mathrm{R}$ and $F \in \mathrm{M}$ with $d = |\varphi| + |F|$ either (i) $d > 0$ and $\varphi \circ F = 0$ or (ii)*

$$\varphi \circ F = \sum_{j=d}^{0} [\varphi \cdot F]_j \, x^j z^{d-j}.$$

Thus, we trivially have $x^n \in \mathcal{I}_F$ if $n > -|F|$.

2.1. A bijection. Next, we detail the bijection between characteristic polynomials of a sequence and the leading annihilating forms of its inverse form.

We use polynomial coefficients in their natural order, not the reversed order of 'feedback coefficients' and without using 'shift registers' as in the engineering literature. This definition enables us to exhibit a bijection between the set of 'characteristic polynomials' of a sequence and the leading forms of the homogeneous ideal $\mathcal{I}_F$ of R.

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

We say that $c \in \mathbb{F}[x]^\times$ is a *characteristic polynomial* of $(s_0, \ldots, s_{n-1})$ if c is monic, $l = |c|$ and either: (i) $l \geq n$ or (ii)

$$c_l s_{k+l} + \cdots + c_0 s_k = 0 \quad \text{for } 0 \leq k \leq n - l - 1 \tag{2.2}$$

and $\chi(s_0, \ldots, s_{n-1}) = \{c \in \mathbb{F}[x]^\times : c \text{ is a characteristic polynomial of } (s_0, \ldots, s_{n-1})\}$.

As x^n is (vacuously) a characteristic polynomial of $(s_0, \ldots, s_{n-1})$, $\chi(s_0, \ldots, s_{n-1})$ is nonempty and

$$\lambda = \lambda(s_0, \ldots, s_{n-1}) = \min\{|c| : \ c \in \chi(s_0, \ldots, s_{n-1})\}$$

is well defined. Thus, *minimal polynomials* of $(s_0, \ldots, s_{n-1})$, that is, characteristic polynomials of *minimal degree* $\lambda = \lambda(s_0, \ldots, s_{n-1}) \in \mathbb{N}$ are well defined; λ is the *LC* of $(s_0, \ldots, s_{n-1})$. We note that in [1], a characteristic polynomial of $(s_0, \ldots, s_{n-1})$ is written c_n, that is, it is indexed by the *length* of the sequence, not its last term.

Recall that $\mathcal{L}$ is the set of monic, leading forms in R, that is, φ such that $z \nmid \mathrm{LT}(\varphi)$. If F is an inverse form, then $x^{1-|F|} \in \mathcal{I}_F^\times \cap \mathcal{L}$. Thus, $\mathcal{I}_F^\times \cap \mathcal{L} \neq \emptyset$ and we can consider forms in $\mathcal{I}_F^\times \cap \mathcal{L}$ of minimal total degree. So we define

$$\lambda(F) = \min\{|f| : \ f \in \mathcal{I}_F^\times \cap \mathcal{L}\}$$

and call $\lambda(F)$ the *LC of* F.

THEOREM 2.4. *Let* $(s_0, \ldots, s_{n-1})$ *be a sequence with inverse form* $F \in \mathrm{M}^\times$. *Then,*

$$\wedge : \chi(s_0, \ldots, s_{n-1}) \leftrightarrows \mathcal{I}_F^\times \cap \mathcal{L} : \vee$$

given by $\wedge(c) = c^\wedge$ *and* $\vee(f) = f^\vee$ *are mutual, degree-preserving bijections so that for* $c \in \chi(s_0, \ldots, s_{n-1})$, $|\wedge(c)| = |c|$ *and for* $f \in \mathcal{I}_F^\times \cap \mathcal{L}$, $|\vee(f)| = |f|$. *Therefore,* $\lambda(s_0, \ldots, s_{n-1}) = \lambda(F)$.

PROOF. We have $|F| = 1 - n$ and $|c^\wedge| = |c| = l$. From Proposition 2.3, $c^\wedge \circ F = 0$ if and only if $[c^\wedge \cdot F]_j = 0$ for $l + |F| \leq j \leq 0$. Now, $c \in \chi(s_0, \ldots, s_{n-1})$ if and only if c satisfies (2.2), and substituting k for $-j$, one sees that (2.2) is equivalent to $[c^\wedge \cdot F]_j = 0$ for $l + |F| \leq j \leq 0$, that is, equivalent to $c^\wedge \in \mathcal{I}_F \cap \mathcal{L}$. So $c \in \chi(s_0, \ldots, s_{n-1})$ if and only if $c^\wedge \in \mathcal{I}_F^\times \cap \mathcal{L}$, we have the required bijections and hence, $\lambda(s_0, \ldots, s_{n-1}) = \lambda(F)$. □

REMARK 2.5. Instead of (2.2), the LFSR algorithm uses the equivalent l and 'connection' polynomial $\gamma \in \mathbb{F}[x]^\times$ satisfying

$$\gamma_0 s_j + \cdots + \gamma_l s_{j-l} = 0 \quad \text{for } l \leq j \leq n - 1,$$

where $\gamma_0 = 1$ and γ_l may be zero (put $j = k + l$ and $\gamma(x) = c^*(x) = x^l \cdot c(x^{-1})$, the reciprocal of c, made monic). Then the LFSR synthesis algorithm returns l and γ. Unfortunately, the formulation using reciprocal polynomials vitiates our algebraic approach.

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

3. Viable ordered pairs (VOPs)

3.1. The inductive construction and algorithm. We recall from [8] how to construct a *'leading generator'* f of $\mathcal{I}_F$ in $\mathcal{L}$ which gives a minimal annihilator of F and, hence, a minimal polynomial $f^\vee$ of $(s_0, \dots, s_{n-1})$. Then we give some additional properties and discuss LC profiles.

This construction is iterative, with a simple inductive basis (Proposition 3.1) and an undemanding inductive step (Theorem 3.3).

Let F be an inverse form. We say that an ordered pair of forms $(f, g) \in \mathrm{R}^2$ is a *viable ordered pair (VOP) for* $\mathcal{I}_F$ if:

(i) f, g are nonzero monic forms, $f \in \mathcal{L}$ and $z \mid g$;
(ii) $\mathcal{I}_F = \langle f, g\rangle$ (we call f *a leading generator* and g a *cogenerator* of $\mathcal{I}_F$);
(iii) $|f| + |g| = 2 - |F|$.

PROPOSITION 3.1 [8, Proposition 3.8]. *If $F = x^m$, then $\mathcal{I}_F = \langle x^{1-m}, z\rangle$.*

The reader may check that $(f, g) = (x^{1-m}, z)$ is a VOP for $\mathcal{I}_{x^m}$. If $f \in \mathcal{I}_F \cap \mathcal{L}$, we call f a *leading form* for $\mathcal{I}_F$. Given a VOP (f, g) for $\mathcal{I}_F$ and $G = ax^{m-1} + Fz^{-1}$ for some $a \in \mathbb{F}$, we need to know how to construct a VOP (φ, ψ) for $\mathcal{I}_G$. This requires a notion of *'discrepancy'* that shows how a and $\mathcal{I}_F$ affect $\mathcal{I}_G$. It is our analogue of 'discrepancy' introduced in [5]; it is the obstruction to extending f to a leading form of $\mathcal{I}_G$.

DEFINITION 3.2. If $f \in \mathcal{I}_F^\times$ is a form and $G = ax^{m-1} + z^{-1}F$, then the *discrepancy* $\Delta(f; G)$ of f and G is 0 if $|f| + |G| > 0$ and $[f \cdot G]_{(|f|+|G|,0)} \in \mathbb{F}$ otherwise.

The inductive step is given by the following result.

THEOREM 3.3 [8, Proposition 4.6, Theorem 4.12]. *Let (f, g) be a VOP for $\mathcal{I}_F$, $a \in \mathbb{F}$ and $G = ax^{|F|-1} + Fz^{-1}$. Suppose that $g \notin \mathcal{I}_G$ and put $\Delta' = \Delta(g; G) \in \mathbb{F}^\times$, $d = |g| - |f|$, $\Delta = \Delta(f; G) \in \mathbb{F}$. If $\Delta = 0$, set $(\varphi, \psi) = (f, zg)$ and $d = d + 1$. However, if $\Delta \neq 0$, put $q = \Delta/\Delta'$ and*

$$(\varphi, \psi) = \begin{cases} (f - q\,x^{-d} g, z\,g) & \text{if } d \le 0, \\ (x^{+d} f - q\,g, zf) & \text{otherwise.} \end{cases}$$

Then, (φ, ψ) is a VOP for G and manifestly $|\varphi| = |f|$ if $d \le 0$ and $|\varphi| = |g|$ otherwise. In particular, $|\varphi| = \max\{|g|, |f|\}$.

For the next iteration:

(i) *$e = |\psi| - |\varphi| = 1$ if $\Delta = 0$ and $e = 1 - |d|$ if $\Delta \neq 0$;*
(ii) *if $d > 0$, $b \in \mathbb{F}$ and $\Delta(\varphi; b\,x^{|G|-1} + Gz^{-1}) \neq 0$, we put $\Delta' = \Delta$, otherwise Δ' is unchanged.*

PROPOSITION 3.4 [8, Proposition 3.5]. *If (f, g) is a VOP for F, then $\lambda(F) = |f|$.*

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

We will often write $d_k = |g^{(k)}| - |f^{(k)}|$ and $\Delta_k = \Delta(f^{(k)}; F^{(-k-1)})$. We will refer to x^{d_k} (if $\Delta_k \neq 0$ and $d_k > 0$) and x^{-d_k} (if $\Delta_k \neq 0$ and $d_k \leq 0$) as the *intermediate shifts* in the construction. The following $O(m^2)$ algorithm is based on Theorem 3.3.

ALGORITHM 3.5 (VOP)

`Input`: *Inverse form* $F \in \mathrm{M}^{\times}$.
`Output`: *VOP* (f, g) *for* $\mathcal{I}_F$.

(Inductive basis: find* $F^{(\mathrm{v})}$ *and a VOP for* $\mathcal{I}_F$ **)*
$\lceil j \leftarrow 1$; `repeat` $j \leftarrow j - 1$ `until` $(F_j \neq 0)$; $\mathrm{v} \leftarrow j$;
$(f, g) \leftarrow (x^{1-\mathrm{v}}, z)$;

(Inductive Step *)*
$\Delta' \leftarrow 1$; $G \leftarrow x^{\mathrm{v}}$; $d \leftarrow \mathrm{v}$;
`for` $j \leftarrow \mathrm{v} - 1$ `downto` $|F|$ `do`
  $\lceil G \leftarrow F_j x^j + G z^{-1}$; $\Delta \leftarrow \Delta(f; G)$; $q \leftarrow \Delta/\Delta'$;
  `if` $(\Delta \neq 0)$ `then if` $(d \leq 0)$ `then` $f \leftarrow f - q\, x^{-d}\, g$;
    `else` $\lceil t \leftarrow f$; $f \leftarrow x^{+d} f - q\, g$; $g \leftarrow t$;
      $\Delta' \leftarrow \Delta$; $d \leftarrow -d$; $\rfloor$
  $g \leftarrow zg$; $d \leftarrow 1 + d$; $\rfloor$

`return` (f, g).$\rfloor$

We note that homogenising $(\mu, \nu) \in \mathbb{F}[x]^2$ of [7] also yields a VOP (see [8, Theorem 6.15]).

3.2. Some additional properties. If $F = x^m$, then $\mathcal{I}_F = \langle x^{1-m}, z \rangle$ by Proposition 3.1 and $\gcd(x^{1-m}, z) = 1$. The next result shows that a VOP (f, g) always satisfies $\gcd(f, g) = 1$.

PROPOSITION 3.6. *If* (f, g) *is a VOP for* $\mathcal{I}_F$, $\gcd(f, g) = 1$ *and* φ, ψ *are as constructed, then* $\gcd(\varphi, \psi) = 1$.

PROOF. If $\Delta = 0$ and $h \mid \gcd(f, zg)$, then $h = z$ or $h \mid g$. However, if $z \mid f$, then $z \mid \mathrm{LT}(f)$ which is impossible, so $h \mid \gcd(f, g)$. Suppose that $\Delta \neq 0$ and $d \leq 0$. Then, $\gcd(\varphi, \psi) = \gcd(f, zg) = \gcd(f, g) = 1$ as before. However, suppose that $d > 0$. If $h \mid zf$ and $h \mid g$, then either: (i) $h = z$ and $h \mid \varphi$ or (ii) $h \mid f$ and $h \mid (x^d f - q\, g)$. However, item (i) is impossible since $z \nmid \mathrm{LT}(\varphi)$ so item (ii) is obtained and $h \mid \gcd(f, g) = 1$. □

We know that (x^{1-m}, z) is a VOP for $\mathcal{I}_F$ and x^{1-m} is a leading form of minimal degree. However, so is $x^{1-m} + \varphi\, z$ for any form with $|\varphi| = -m$. More generally, we have the following result.

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

COROLLARY 3.7 (Compare [6, Theorem 1]). *Let* $\Theta = \Theta_F = \{\theta \in \mathcal{I}_F \cap \mathcal{L} : |\theta| \text{ is minimal}\}$. *If* (f, g) *is a VOP for* $\mathcal{I}_F$, *then*

$$\Theta = \begin{cases} \{f\} & \text{if } |g| > |f|, \\ \{f\} \cup \{f + \psi \cdot g : \psi \text{ is a form and } |\psi| = |f| - |g|\} & \text{otherwise.} \end{cases}$$

PROOF. If $|g| > |f|$ and then f is the only monic leading annihilating form of minimal degree $|f|$ since $\mathcal{I}_F = \langle f, g\rangle$. However, if $|g| \le |f|$ and $\psi \in \mathrm{R}^\times$ is a form with $|\psi| = |f| - |g|$, then $h = f + \psi \cdot g \in \mathcal{I}_F$ is a monic leading form since $\mathrm{LT}(h) = \mathrm{LT}(f)$ and $|h| = |f|$ is minimal. □

In [8, Example 4.24], we obtained $(f, g) = (x^4 + x^3z + x^2z^2, x^3z + x^2z^2 + xz^3 + z^4)$ for the inverse form $F = x^{-6} + x^{-4}z^{-2} + x^{-3}z^{-3} + z^{-6}$. Here, $f(0, 1) = 0$. However, $h = f + g \in \mathcal{I}_F$ satisfies $h(0, 1) = 1$. (In fact, $h \in \mathcal{I}_{z^{-1}F}$.)

More generally, if we have an inverse form F and begin iterating with $(x^{1-|F|}, z)$, then the construction provides a VOP (f, g) with $\gcd(f, g) = 1$. Hence, if $f(a, b) = 0$ for some $a, b \in \mathbb{F}$, then $g(a, b) \neq 0$ and if $|g| \le |f|$, then $h = f + x^{|f|-|g|}g$ is a leading form in $\mathcal{I}_F$ such that $h(a, b) \neq 0$. However, if $|g| > |f|$, then $h = x^{|g|-|f|}f + g \in \mathcal{I}_F$ is a leading form such that $h(a, b) \neq 0$, but of increased degree $|g|$.

3.3. LC profiles. An inverse form F has subforms $F^{(j)}$ for $m = |F| \le j \le \mathrm{v} = \mathrm{v}(F)$, with $F^{(\mathrm{v})} = x^{\mathrm{v}}$ and $F^{(m)} = F$. We write $\lambda(F^{(j)})$ for the LC of the subform $F^{(j)}$.

We call the sequence $(\lambda(F^{(\mathrm{v})}), \ldots, \lambda(F^{(m)}))$ of integers the *LC profile* of F and say that F has a *PLCP* if $\mathrm{v} = 0$ and $\lambda(F^{(-k)}) = \lfloor (k + 1)/2 \rfloor$ for $0 \le k \le -m$. From Theorem 2.3, this agrees with the usual notion of the LC profile of a sequence. Next we relate the notion of PLCP to the intermediate shifts occurring in Theorem 3.3.

PROPOSITION 3.8. *Let* F *be an inverse form with* $F_0 = 1$. *For* $1 \le k < -m$, *let* $(f^{(k)}, g^{(k)})$ *be a VOP for* $\mathcal{I}_{F^{(-k)}}$ *and* $F^{(-1-k)}$ *be the* $(-1-k)$*th subform of* F. *Put* $\Delta_k = \Delta(f^{(k)}; F^{(-1-k)})$. *The following are equivalent:*

(i) *F has a PLCP;*
(ii) *the intermediate shift is x if and only if k is odd.*

PROOF. The quantity $\lfloor (k + 1)/2 \rfloor$ is 1 for $k = 1$, and increases by 1 if and only if k is odd. Since $F_0 = 1$, $(f^{(0)}, g^{(0)}) = (x, z)$, that is, $|f^{(0)}| = 1$ and $d_0 = 0$. Thus, either $(f^{(1)}, g^{(1)}) = (x, z^2)$ or $(f^{(1)}, g^{(1)}) = (x - z, z^2)$. Next, the degree $|f^{(k)}|$ increases by 1 if and only if k is odd, and is equivalent to $f^{(k+1)} = xf^{(k)} - q_k g^{(k)}$ if k is odd and $f^{(k+1)} = f^{(k)} - q_k g^{(k)}$ if k is even. □

Proposition 3.8 is an analogue of [6, Theorem 2] without an irrationality hypothesis and our intermediate shifts are analogous to the partial quotients of [6].

Moreover, Δ_k is arbitrary when k is even. The average LC of a random binary $(s_0, \ldots, s_{n-1})$ is $n/2 + a_n$, where $0 \le a_n \le 5/18$ [12, Ch. 4]. Thus, a binary sequence with $s_0 = 1$ and s_i chosen so that $\Delta_k = 1$ when k is odd and randomly when k is even will: (i) have a PLCP and (ii) be a good approximation to a *random* binary sequence.

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

4. The sequence r and its inverse forms

From now on, $\mathbb{F} = \mathrm{GF}(2)$ and $r = (1, 1, 0, 1, 0^3, 1, 0^7, 1, 0^{15}, 1, \ldots)$, where $r_i = 1 \in \mathbb{F}$ if $i = 2^k - 1$ for some $k \geq 0$ and $r_i = 0$ otherwise.

DEFINITION 4.1. For $n \geq 1$, the inverse form of $(r_0, \ldots, r_{n-1})$ is

$$R^{(1-n)} = R^{(1-n)}(x^{-1}, z^{-1}) = \sum_{j=1-n}^{0} r_{-j} x^j z^{1-n-j} \in \mathbb{F}[x^{-1}, z^{-1}].$$

We write $\mathcal{I}_{n-1}$ for $\mathcal{I}_{R^{(1-n)}}$. Note that $R^{(1-n)}$ and $\mathcal{I}_{n-1}$ are indexed using the last index of $(r_0, \ldots, r_{n-1})$ rather than the length of the sequence. We have $|R^{(1-n)}| = 1 - n$, $R^{(1-2^k)} = \sum_{j=k}^{0} x^{1-2^j} z^{2^j-2^k}$ for $k \geq 0$, and if $k \geq 1$, then $R^{(1-2^k)} = x^{1-2^k} + R^{(1-2^{k-1})} z^{-2^{k-1}}$. In addition, if $2^k - 1 < n < 2^{k+1} - 1$, then $R^{(-n)} = R^{(1-2^k)} z^{2^k-1-n} \in z^{-1}\mathrm{M}$.

EXAMPLE 4.2. The inverse forms $R^{(j)}$ for $-9 \leq j \leq 0$ are given in Table 1.

Recall that $\Delta_{k-1} = \Delta(f^{(k-1)}; R^{(-k)}) = [f^{(k-1)} \cdot R^{(-k)}]_{(|f^{(k-1)}|-k,0)}$ and $q_{k-1} = \Delta_{k-1}$ for $0 \leq k - 1 \leq n - 1$.

EXAMPLE 4.3 (Example 4.2 continued). Since $R^{(0)} = 1$, $\mathcal{I}_0 = \langle f^{(0)}, g^{(0)} \rangle = \langle x, z \rangle$ from Proposition 3.1. However, we can and will take $(f^{(0)}, g^{(0)}) = (x + z, z)$ so that $f^{(0)}(0, 1) = 1$. The key ingredients for the construction are the degree increment $d_k = |g^{(k)}| - |f^{(k)}|$ and the discrepancy Δ_k, so that we know how to update $(f^{(k)}, g^{(k)})$. We obtain the results shown in Table 2. For $0 \leq k \leq 9$, $f^{(k)} = \lfloor (k + 2)/2 \rfloor = \lambda_{k+1}$ (recall that $f^{(k)} \circ (r_0, \ldots, r_k) = 0$ where there are $k + 1$ terms of r). From Corollary 3.7, $f^{(k)}$ is the unique leading annihilating form of minimal total degree if k is odd and $f^{(k)} + g^{(k)}$ is the only other leading annihilating form of minimal total degree when k is even.

The significance of the underlined terms will become clear in the proof of Theorem 4.4.

We now come to our main result.

THEOREM 4.4. *Let* $(f^{(0)}, g^{(0)}) = (x + z, z)$ *and for* $k \geq 0$, *let* $(f^{(k+1)}, g^{(k+1)})$ *be as constructed in Theorem 3.3.*

(A) *If k is even, then $\Delta_k = 0$; otherwise, $\Delta_k = 1$ and $d_k = 1$.*
(B) *We have*

$$(f^{(k+1)}, g^{(k+1)}) = \begin{cases} (f^{(k)}, zg^{(k)}) & \text{if } k \text{ is even,} \\ (xf^{(k)} + g^{(k)}, zf^{(k)}) & \text{otherwise.} \end{cases}$$

(C) $|f^{(k+1)}| = \lfloor (k + 3)/2 \rfloor$.
(D) $f^{(k+1)}(0, 1) = g^{(k+1)}(0, 1) = 1$.

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

TABLE 1. Inverse forms $R^{(j)}$ for Example 4.2.

j	$R^{(j)}$
0	$1 = R^{(0)}$
−1	$x^{-1} + z^{-1} = R^{(-1)}$
−2	$x^{-1}z^{-1} + z^{-2} = R^{(-1)}z^{-1}$
−3	$x^{-3} + x^{-1}z^{-2} + z^{-3} = R^{(-3)}$
−4	$x^{-3}z^{-1} + x^{-1}z^{-3} + z^{-4} = R^{(-3)}z^{-1}$
−5	$x^{-3}z^{-2} + x^{-1}z^{-4} + z^{-5} = R^{(-3)}z^{-2}$
−6	$x^{-3}z^{-3} + x^{-1}z^{-5} + z^{-6} = R^{(-3)}z^{-3}$
−7	$x^{-7} + x^{-3}z^{-4} + x^{-1}z^{-6} + z^{-7} = R^{(-7)}$
−8	$x^{-7}z^{-1} + x^{-3}z^{-5} + x^{-1}z^{-7} + z^{-8} = R^{(-7)}z^{-1}$
−9	$x^{-7}z^{-2} + x^{-3}z^{-6} + x^{-1}z^{-8} + z^{-9} = R^{(-7)}z^{-2}$

TABLE 2. Calculations for the VOP algorithm for Example 4.2.

k	d_{k-1}	Δ_{k-1}	$f^{(k)}$	$g^{(k)}$
0	–	–	$f^{(0)} = x + \underline{z}$	z
1	0	0	$f^{(0)}$	z^2
2	1	1	$xf^{(1)} + g^{(1)} = x^2 + \underline{xz} + z^2$	$f^{(0)}z$
3	0	0	$f^{(2)}$	$f^{(0)}z^2$
4	1	1	$xf^{(3)} + g^{(3)} = x^3 + x^2z + \underline{z^3}$	$f^{(2)}z$
5	0	0	$f^{(4)}$	$f^{(2)}z^2$
6	1	1	$xf^{(5)} + g^{(5)} = x^4 + \underline{x^3z} + x^2z^2 + z^4$	$f^{(4)}z$
7	0	0	$f^{(6)}$	$f^{(4)}z^2$
8	1	1	$xf^{(7)} + g^{(7)} = x^5 + x^4z + \underline{x^2z^3} + xz^4 + z^5$	$f^{(6)}z$
9	0	0	$f^{(8)}$	$f^{(6)}z^2$

PROOF. We have $(f^{(0)}, g^{(0)}) = (x + z, z)$, where $\Delta_0 = 0$, $|f^{(0)}| = 1 = \lfloor 2/2 \rfloor$ and $f^{(0)}(0, 1) = 1 = g^{(0)}(0, 1)$. Suppose inductively that the result is true for k.

(A) For $f^{(k+1)}$, we have to determine $\Delta_k = [f^{(k)} \cdot R^{(-1-k)}]_{(|f^{(k)}|-1-k,0)}$. Let $P = 2^p - 1 \le k + 1 < 2^{p+1} - 1$ for some $p \ge 1$. Put $e = |f^{(k)}|$ and $l = e - 1 - k$. Then,

$$S = R^{(-1-k)} = \Big(\sum_{j=p}^{0} x^{1-2^j} z^{2^j-2^p} \Big) z^{P-1-k} \quad \text{and} \quad \Delta_k = [f^{(k)} \cdot S]_{(l,0)}.$$

We consider three cases.

Case (i): k even, $P = k + 1$. We have to show that $\Delta_k = 0$. Since $k - 1$ is odd, the inductive hypothesis gives $\Delta_{k-1} = 1$, $d_{k-1} = 1$ and $(f^{(k)}, g^{(k)}) = (xf^{(k-1)} + g^{(k-1)}, zf^{(k-1)})$.

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

Also, $|f^{(k)}| = |f^{(k-1)}| + 1 = k/2 + 1 = 2^{p-1}$, so $l = |f^{(k)}| - k - 1 = 2^{p-1} + 1 - 2^p = 1 - 2^{p-1}$. By part (A), $f^{(k)}(0, 1) = 1$, so we can write $f^{(k)} \cdot S$ as

$$(x^e + \alpha + z^e) \cdot (x^{1-2^p} + x^{1-2^{p-1}} z^{-2^{p-1}} + \beta).$$

Then $x^e \cdot x^{1-2^p} = x^l$, and one checks that $(\alpha + z^e) \cdot (x^{1-2^{p-1}} z^{-2^{p-1}} + \beta) = x^l$ plus terms in $z^{-1}\mathrm{M}$, so $\Delta_k = [f^{(k)} \cdot S]_{(l,0)} = 0$ and $f^{(k+1)} = f^{(k)}$.

Case (ii): k even, $P < k + 1 < 2^{p+1} - 1$. Here, $P - k - 1 < 0$ and $S \in z^{-1}\mathrm{M}$. As in case (i), $(f^{(k)}, g^{(k)}) = (xf^{(k-1)} + g^{(k-1)}, zf^{(k-1)})$ and $e = |f^{(k)}| = |f^{(k-1)}| = 2^{p-1}$. Then,

$$f^{(k)} \cdot S = (x^e + (f^{(k)} + x^e)) \cdot R^{(-P)} z^{P-k-1}.$$

However, $x^e \cdot R^{(-P)} z^{P-k-1}$, $(f^{(k)} + x^e) \cdot x^{-P}$, $(f^{(k)} + x^e) \cdot (R^{(-P)} + x^{-P}) z^{P-k-1} \in z^{-1}\mathrm{M}$, so $\Delta_k = 0$ and again $f^{(k+1)} = f^{(k)}$.

Case (iii): k odd and $P \le k < 2^{p+1} - 1$. For $k = 1$, $\Delta_1 = [(x + \underline{z}) \cdot (x^{-1}z^{-1} + z^{-2})]_{(1-2,0)} = 1$; the term $\underline{z}$ of $f^{(1)}$ has triggered $\Delta_1 = 1$. The reader may easily verify that $\underline{xz} = \alpha z$ triggers $\Delta_3 = 1$ and that $\underline{z}^3 = \beta z$ triggers $\Delta_5 = 1$. Now let k be odd and $p \ge 3$, $P = 2^p - 1 \le k < 2^{p+1} - 1$. Define maps $\alpha, \beta : \mathrm{R} \to \mathrm{R}$ by $(\alpha\ f)(x, z) = x \cdot f(x, z)$ and $(\beta\ f)(x, z) = z^2 \cdot f(x, z)$. Since $k - 1$ is even, the inductive hypothesis gives

$$f^{(k)} = f^{(k-1)} = xf^{(k-2)} + g^{(k-2)} = \alpha\ f^{(k-2)} + \beta\ f^{(k-4)},$$

$e = |f^{(k)}| = |f^{(k-1)}| = (k + 1)/2$ and $l = e + |S| = (k + 1)/2 - 1 - k = -(k + 1)/2$.

Put $t_k = x^{u_k} z^{v_k}$, where $u_k = P - (k + 1)/2$, $v_k = k + 1 - P$. Then, $|t_k| = (k + 1)/2 = |f^{(k)}|$ and $t_k = \alpha^{u_k} \beta^{(v_k-1)/2} z$. Since z is a term of $f^{(1)}$, t_k is a term of $f^{(2u_k+2v_k-1)} = f^{(k)}$.

Let $L = \mathrm{LT}(S)$, where $S = R^{(-P)} z^{P-k-1} \in z^{-1}\mathrm{M}$. Then,

$$f^{(k)} \cdot S = f^{(k)} \cdot (L + S) + f^{(k)} \cdot L = f^{(k)} \cdot (L + S) + t_k \cdot L + (f^{(k)} + t_k) \cdot L$$

and $t_k \cdot L = x^{(k-1)/2} z \cdot x^{-k} z^{-1} = x^l$. It is straightforward that $f^{(k)} \cdot (L + S) \in z^{-1}\mathrm{M}$ and $(f^{(k)} + t_k) \cdot L \in z^{-1}\mathrm{M}$. Thus, $\Delta_k = [f^{(k)} \cdot S]_{(l,0)} = [t_k \cdot L]_{(l,0)} = 1$, the term t_k of $f^{(k)}$ triggers $\Delta_k = 1$ and $(f^{(k+1)}, g^{(k+1)}) = (xf^{(k)} + g^{(k)}, zf^{(k)})$.

(B) This is a simple consequence of part (A).

(C) Suppose that $|f^{(k)}| = \lfloor (k + 2)/2 \rfloor$. From part (B), if k is even, then $|f^{(k+1)}| = |f^{(k)}| = (k + 2)/2 = \lfloor (k + 3)/2 \rfloor$ and if k is odd, then $|f^{(k+1)}| = |f^{(k)}| + 1 = \lfloor (k + 2)/2 \rfloor + 1 = (k + 1)/2 + 1 = (k + 3)/2 = \lfloor (k + 3)/2 \rfloor$.

(D) We know that $f^{(k)}(0, 1) = g^{(k)}(0, 1) = 1$ for $k = 0, 1$, so suppose that the result is true for k. If k is even, $f^{(k+1)}(0, 1) = f^{(k)}(0, 1) = 1$ and $g^{(k+1)}(0, 1) = 1$, whereas if k is odd, $f^{(k+1)}(0, 1) = g^{(k)}(0, 1) = 1$ and $g^{(k+1)}(0, 1) = f^{(k)}(0, 1) = 1$. □

REMARK 4.5. In Example 4.3, the underlined terms trigger a discrepancy of 1: for odd k and $2^p - 1 \le k < 2^{p+1} - 1$, $u_{k+1} = u_k - 1$, $v_{k+2} = v_k + 2$, so that the t_k in the proof of Theorem 4.4 take the values $x^p z^1, x^{p-1} z^3, x^{p-2} z^5, \ldots, x^0 z^{2^p-1}$.

The next result is immediate from Proposition 3.8, Theorem 4.4 and Corollary 3.7.

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

COROLLARY 4.6.

(i) *The sequence* $(r_0, r_1, \ldots)$ *has a PLCP.*
(ii) *If* n *is odd,* $(r_0, \ldots, r_{n-1})$ *has a unique leading form of minimal degree, namely* $f^{(n-2)}$*, or the leading forms of minimal degree are precisely the two forms* $f^{(n-2)}$ *and* $f^{(n-2)} + g^{(n-2)}$.

From Theorem 4.4, no multiplications in R are required to compute a VOP, giving the following linear algorithm.

ALGORITHM 4.7 (VOP algorithm specialised to $R^{(1-n)}$).

`Input`: *Integer* $n \geq 1$.
`Output`: *Viable ordered pair* (f, g) *for* $\mathcal{I}_{n-1}$.
$\lceil (f, g) \leftarrow (x + z, z)$;
`for` $j \leftarrow 0$ `downto` $1 - n$ `do`
  $\lceil$ *if* j *is odd* `then` $\lceil t \leftarrow f$; $f \leftarrow xf + g$; $g \leftarrow t$; $\rfloor$
  $g \leftarrow zg$; $\rfloor$;
`return` (f, g).$\rfloor$

For additional properties of $\mathcal{I}_{n-1}$, for example, its codimension and how to compute its (unique) reduced grlex Groebner basis, see [8, Corollary 5.18, Algorithm 5.24] and [9, Section 4].

4.1. Relating Theorem 4.4 to [1] and LFSRs. We next give a closed-form expression for $f^{(2k-1)}$ dehomogenised; this also motivates the use of the roots $Y^2 + xY + 1$ in an extension of $\mathbb{F}(x)$, which were unmotivated in [1].

LEMMA 4.8. *Let* $h^{(k)} \in \mathbb{F}[x]$ *be given by* $h^{(0)} = x$, $h^{(1)} = x + 1$, $h^{(2)} = x^2 + x + 1$ *and* $h^{(k)} = x\,h^{(k-1)} + h^{(k-2)}$ *for* $k \geq 3$. *Then,*

$$x\,h^{(k)} = (1 + \rho)\rho^k + (1 + \rho^{-1})\rho^{-k},$$

where $\rho = \overline{Y} \in \mathbb{F}(x)[Y]/(Y^2 + xY + 1) = \mathbb{K}$.

PROOF. The given recurrence has characteristic polynomial $Y^2 + xY + 1 \in \mathbb{F}(x)[Y]$, which is irreducible. (One easily shows that if $Y^2 + xY + 1 = (Y + u)(Y + v)$ for some $u, v \in \mathbb{F}(x)$, then $x = 0$.) So let $\rho = \overline{Y} \in \mathbb{K}$. Solving $h^{(k)} = A\rho^k + B\rho^{-k}$ for $A, B \in \mathbb{F}(x)$ subject to $h^{(1)} = x + 1$, $h^{(2)} = x^2 + x + 1$ gives the required expression. □

We note that the 2×2 matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)$ much used in [1] has characteristic polynomial $Y^2 + xY + 1$.

We now set $\rho = \overline{Y} \in \mathbb{F}(x)[Y]/(Y^2 + xY + 1)$.

THEOREM 4.9. *For* $k \geq 1$, $x\,f^{(2k-2)}(x, 1) = x\,f^{(2k-1)}(x, 1) = (1 + \rho)\rho^k + (1 + \rho^{-1})\rho^{-k}$.

PROOF. Theorem 4.4 implies that we may take $h^{(k)} = f^{(2k-2)}(x, 1)$ in Lemma 4.8; $f^{(2k-2)} = f^{(2k-1)}$ and $|g^{(2k-1)}| = |f^{(2k-1)}| + 1$, so $f^{(2k-1)}$ is unique. □

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press

COROLLARY 4.10 (See [1, Lemma 5]). *Let* $\eta = (1+\rho)\rho^k + (1+\rho^{-1})\rho^{-k} \in \mathbb{K}$ *as in Lemma 4.8. Then,* $\eta \in \mathbb{F}[x]$, $x \mid \eta$ *and* $|\eta| = k+1$.

COROLLARY 4.11. *For* $k \geq 1$, *let* c_k *be the minimal polynomial for* $(r_0, \ldots, r_{2k-1})$ *as in* [1]. *Then,* $c_k(x) = f^{(2k-1)}(x, 1)$.

PROOF. Reference [1, Lemma 3] implies that c_k satisfies the recurrence of Lemma 4.8. □

COROLLARY 4.12. *The LFSR algorithm applied to* $(r_0, \ldots, r_{2k-1})$ *returns* k *and the reciprocal polynomial* $f^{(2k-1)}(x, 1)^*$.

PROOF. From Remark 2.5 and Theorem 4.4, $|f^{(2k-1)}(x,1)| = k$ and $f^{(2k-1)}(0,1) = 1$. □

References

[1] Z.-D. Dai, 'Proof of Rueppel's linear complexity conjecture', *IEEE Trans. Inform. Theory* **32** (1986), 440–443.

[2] Z.-D. Dai and Z. Wan, 'A relationship between the Berlekamp–Massey algorithm and the Euclidean algorithm for linear feedback shift register synthesis', *Acta Math. Sin. (N. S.)* **4** (1988), 55–63.

[3] P. Fitzpatrick, 'On the key equation', *IEEE Trans. Inform. Theory* **41** (1995), 1290–1302.

[4] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20 (Addison-Wesley, Reading, MA, 1983).

[5] J. L. Massey, 'Shift-register synthesis and BCH decoding', *IEEE Trans. Inform. Theory* **15** (1969), 122–127.

[6] H. Niederreiter, 'Sequences with almost perfect linear complexity profile', in: *Advances in Cryptology, EUROCRYPT'87*, Lecture Notes in Computer Science, 304 (eds. D. Chaum and W. L. Price) (Springer-Verlag, Berlin, 1988), 37–51.

[7] G. H. Norton, 'On the minimal realizations of a finite sequence', *J. Symbolic Comput.* **20** (1995), 93–115.

[8] G. H. Norton, 'On the annihilator ideal of an inverse form', *J. Appl. Algebra Engrg. Comm. Comput.* **28** (2017), 31–78.

[9] G. H. Norton, 'On the annihilator ideal of an inverse form. Addendum', *J. Appl. Algebra Engrg. Comm. Comput.* **28** (2019), 491–507.

[10] G. H. Norton, 'On Rueppel's linear complexity conjecture', Preprint (2023), arXiv:2305.00405.

[11] R. A. Rueppel, *New Approaches to Stream Ciphers*, PhD Dissertation (Institute of Telecommunications, Swiss Federal Institute of Technology, Zurich, 1984).

[12] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Communications and Control Engineering Series (Springer Verlag, Berlin–Heidelberg, 1986).

GRAHAM H. NORTON, School of Mathematics and Physics,
University of Queensland, Brisbane, Queensland 4072, Australia
e-mail: ghn@maths.uq.edu.au

https://doi.org/10.1017/S0004972724000601 Published online by Cambridge University Press