Journal of Integer Sequences, Vol. 4 (2001),
Article 01.1.1

The Number-Wall Algorithm: an LFSR Cookbook

W. F. Lunnon

Department of Computer Science
National University of Ireland
Maynooth, Co. Kildare, Ireland

Email address: fred@cs.may.ie

Abstract

This paper might fairly be said to fall between three stools: the presentation and justification of a number of related computational methods associated with LFSR sequences, including finding the order, recurrence and general term; the exploration of tutorial examples and survey of applications; and a rigorous treatment of one topic, the recursive construction of the number wall, which we believe has not previously appeared.

The *Number Wall* is the table of Toeplitz determinants associated with a sequence over an arbitrary integral domain, particularly $\mathbf{Z}$, $\mathbf{F}_p$, $\mathbf{R}$, and their polynomial and series extensions by many variables. The relation borne by number walls to LFSR (linear recurring shift register) sequences is analogous to that borne by difference tables to polynomial sequences: They can be employed to find the order and recurrence §3, or to compute further terms and express the general term explicitly §10 (although other more elaborate methods may be more efficient §12, §8).

Much of the paper collects and summarizes relevant classical theory in Formal Power Series §1, Linear Recurrences §2, Padé Blocks (essentially) §3, Vandermonde Interpolation §8, and Difference Tables §9. A 'frame' relation between the elements of the number wall containing zeros (a *non-normal C-table*, in Padé terminology) is stated and proved §4, with the resulting recursive generation algorithm and some special cases §5; the consequences of basing the wall on this algorithm instead are explored §6, and a cellular automaton is employed to optimize it in linear time §7.

The connections between number walls and classical Padé tables are discussed briefly §11, with other associated areas (Linear Complexity, QD Algorithm, Toda Flows, Berlekamp-Massey) reviewed even more briefly §12. Among topics covered incidentally are the explicit number wall for an LFSR, in particular for a diagonal binomial coefficient §8; dealing with high-degree 'polynomials' over finite fields, fast computation of LFSR order over $\mathbf{F}_p$, and the wall of a linear function of a given sequence §9. There are numerous examples throughout, culminating in a final gruelingly extensive one §13.

Keywords: Number Wall, Zero Window, Persymmetric, Toeplitz Matrix, Hankel Determinant, Linear Complexity, Finite Field, Cryptographic Security, LFSR, Extrapolation, Toda Flow, Linear Recurring Sequence, Difference Equation, Zero-Square Table, QD Method, Vandermonde, Formal Laurent Series, Padé Table.

AMS Subject Classification: 94A55, 65D05, 11C20, 65-04, 68Q15, 68Q68, 41A21.

0. Introduction and Acknowledgements

The initial aim of this rambling dissertation was to codify what J. H. Conway has christened the *Number Wall*, an efficient algorithm for computing the array of Toeplitz determinants associated with a sequence over an arbitrary integral domain: particularly interesting domains in this context are integers $\mathbf{Z}$, integers modulo a prime $\mathbf{F}_p$, reals $\mathbf{R}$, and their polynomials and power series extensions. §1 (Notation and Formal Laurent Series) sketches elementary the algebraic machinery of these domains and their pitfalls, and §2 (LFSR Sequences) summarizes the elementary theory of Linear Feedback Shift Registers.

Our original program is now carried out with an earnest aspiration to rigor that may well appear inappropriate (and may yet be incomplete): however, on numerous occasions, we discovered the hard way that to rely on intuition and hope for the best is an embarrassingly unrewarding strategy in this deceptively elementary corner of mathematical folklore. In §3 (Determinants and Zero-windows) we define the number wall, give simple algorithms for using it to determine the order and recurrence of an LFSR, establish the recursive construction rule in the absence of zeros (a.k.a. the Sylvester Identity) and the square window property of zeros (a.k.a. the Padé Block Theorem) which, despite of its great age and simplicity of statement, appears to have evaded a substantial number of previous attempts to furnish it with a coherent demonstration. In §4 (The Frame Theorems) we develop the central identities connecting elements around inner and outer frame of a window of zeros in a wall; equally contrary to expectation, these prove to be a notably delicate matter! §5 (The Algorithm, Special Cases) discusses the recursive algorithm implicit in the Frame Theorems, particularly the special cases of an isolated zero and of a binary domain, and digressing along the way to an instructive fallacy which felled a earlier attempted proof. §6 (General Symmetric Walls) explores the consequences of employing this oddly symmetric algorithm — rather than the original Toeplitz determinant — to build a generalized wall from an arbitrary pair of sequences of variables or numerals. We show the denominators are always monomial, and that there is arbitrarily large long-range dependence; and give some striking examples. §7 (Performance and the FSSP) explores how an apparently unrelated idea from Cellular Automaton Theory — Firing Squad Synchronization — plays a major part in tuning a fast computational algorithm, which has actually been implemented for the binary domain.

At this point in writing, the focus shifted rather towards a survey of existing methods, as it became apparent that — while much if not all of this material is known by somebody — there is no collected source reference for a whole batch of elementary computational problems associated with LFSRs. §8 (Interpolation and Vandermonde Matrices) summarizes classical material which is used to find explicitly the coefficients needed in §10, digressing to give explicitly the wall for binomial coefficient diagonals, and a formula for the general element of the wall in terms of the general element of the sequence in the LFSR case. §9 (Difference Tables) takes a look at a venerable ancestor, the difference table being to polynomials what the number wall (in a more general way) is to linear recurrences. Appropriate definition and effective evaluation of a polynomial are nontrivial for finite characteristic; the ensuing investigation leads *inter alia* to a fast algorithm for computing the order of an LFSR over $\mathbf{F}_p$, applicable to a recent study of deBruijn sequences. At least some of these strands are pulled together in §10 (Explicit Term of an LFSR Sequence) where we discuss efficient methods of computing the roots and coefficients of the 'exponential' formula for the general element of an LFSR sequence from a finite set of its elements.

In §11 (Padé Tables) we make the classical connection between number walls and rational approximation, and develop some pleasantly straightforward algorithms for series reciprocal and ('non-normal') Padé approximants. §12 (Applications and Related Algorithms) surveys applications including linear complexity profiles (LCPs) and numerical roots of polynomials (Rutishauser QD), with a brief description of the well-known Berlekamp-Massey algorithm for computing the recurrence of an LFSR sequence from its elements. Finally §13 (Hideous Numerical Example) features an intimidating computation, intended to illustrate some of the nastier aspects of the Outer Frame Theorem, and succeeding we fear only too well.

As a third strand, we have felt obliged to make this something of a tutorial, and to that end have sketched proofs for the sake of completeness wherever practicable: existing proofs of well-known results in this area seem often to be difficult of access, incomplete, over-complicated or just plain wrong. We have included frequent illustrative examples, some of which we hope are of interest in their own right; and a number of conjectures, for this is still an active research area (or would be if more people knew about it).

It would be surprising if much of the material presented here was genuinely new — we have been scrupulous in acknowledging earlier sources where known to us — but we felt it worth collating under a uniform approach. We originally unearthed the Frame Theorems over 25 years ago, and although the result might now quite reasonably be considered to lie in the public domain, to the best of our knowledge no complete proof has ever been published. We trust it is at last in a form fit for civilized consumption: if so, some of the credit should go to the numerous colleagues who have persistently encouraged, struggled with earlier drafts, and made suggestions gratefully incorporated — in particular Simon Blackburn, David Cantor, John Conway, Jim Propp, Jeff Shallit, Nelson Stephens.

1. Notation and Formal Laurent Series

For applications we are interested principally in sequences over the integers $\mathbf{Z}$ or a finite field $\mathbf{F}_p$, especially the binary field. However, to treat these cases simultaneously, as well as to facilitate the proofs, we shall need to formulate our results over an arbitrary ground *integral domain*, i.e. a commutative ring with unity and without divisors of zero. Such a domain may be extended to its field of fractions by **Her75** §3.6, permitting elementary linear algebra, matrices and determinants to be defined and linear equations to be solved in the usual way; and further extended to its ring of polynomials and field of (formal) Laurent power series in a transcendental variable, following a fairly routine procedure to be expounded below.

There is rarely any need for us to distinguish between variables over these different domains, so they are all simply denoted by italic capitals. Integer variables (required for subscripts etc, whose values may include $\pm\infty$ where this makes sense) are denoted by lower-case italic letters. Vectors, sequences and matrices are indicated by brackets — the sequence $[S_n]$ has elements $\ldots, S_0, S_1, S_2, \ldots$, and the matrix $[F_{ij}]$ has determinant $|F_{ij}|$. A sequence is implicitly infinite in both directions, where not explicitly finite; context should suggest if a truncated segment requires extrapolation by zero elements, periodic repetition, or the application of some LFSR.

In §4 the elements are actually polynomials over the ground domain; and all the quantities we deal with could be expressed as rational functions (quotients of polynomials) over it. While it is both feasible and conceptually simpler to couch our argument in terms of these, the mechanics of the order notation $\mathcal{O}(X^k)$ introduced below become unnecessarily awkward; therefore we prefer to utilize the slightly less familiar concept of *Formal Laurent Series* (FLS).

We define the field of FLS to be the set of two-sided sequences $[\ldots, S_k, \ldots]$ whose components lie in the given ground field, and which are *left-finite*, that is only finitely many components are nonzero for $k < 0$. Arithmetic is defined in the usual Taylor-Laurent power-series fashion: that is, addition and negation are term-by-term, multiplication by Cauchy (polynomial) product, reciprocal of nonzeros by the binomial expansion. The ground field is injected into the extension by $S_0 \to [\ldots, 0, S_0, 0, \ldots]$.

As usual we write an FLS as an infinite sum of integer powers of the transcendental X with finitely many negative exponents: its *generating function*. The notation is suggestive, but has to be interpreted with some care. For instance, we cannot in general map from FLSs to values in the ground field by substituting some value for X, since this would require the notion of convergence to be incorporated in the formalism. Fortunately we have no need to do so here, since we only ever *specialize* $X \to 0$, defined simply as extracting the component S_0 with zero subscript.

The following property is deceptively important in subsequent applications.

> **Theorem:** Specialization commutes with FLS arithmetic: that is, if $W(V(X), \ldots)$ denotes some (arithmetic) function of FLS elements $V(X), \ldots$, and $V(0)$ denotes $V(X)$ with $X \to 0$ etc, then $W(V(0), \ldots) \ = \ W(V(X), \ldots)(0)$. (1.0)

Proof: This is the case $k = 0$ of the nontrivial fact that two FLSs $U = [\ldots, S_k, \ldots]$ and $V = [\ldots, T_k, \ldots]$ are equal under the operations of field arithmetic (if and) only if they are equal component-wise, that is only if $S_k = T_k$ for all k. For suppose there existed distinct sequences $[S_k], [T_k]$ for which $U = V$ arithmetically. Then $U - V = 0$, where the sequence corresponding to $U - V$ has some nonzero component. Using the binomial expansion, we calculate its reciprocal; now $1 = (U - V)^{-1} \cdot (U - V) = (U - V)^{-1} \cdot 0 = 0$. So the field would be trivial, which it plainly is not, since it subsumes the ring of polynomials in X. ■

In this connection it is instructive to emphasize the significance of left-finiteness. If this restriction were abandoned, we could consider say (expanding by the binomial theorem)

$$\begin{aligned} U \ &= \ 1/(1 - X) \ = \ 1 + X^1 + X^2 + X^3 + \ldots, \\ -V \ &= \ X^{-1}/(1 - X^{-1}) \ = \ \ldots + X^{-3} + X^{-2} + X^{-1}; \end{aligned}$$

now by elementary algebra $U = V$ despite the two distinct expansions, and (1.0) would no longer hold. Related to this difficulty is the fact that we no longer have a field: $U - V$ for instance, the constant unity sequence, has no square.

One unwelcome consequence is that the generating function approach frequently employed as in **Nie89** to discuss Linear Complexity is applicable only to right- (or mut. mut. left-) infinite sequences, and is unable to penetrate the 'central diamond' region of a number-wall (§3) or shifted LCP (§12), being restricted to a region bounded to the South by some diagonal line. [It is noteworthy that, elementary as they might be, these matters have on occasion been completely overlooked elsewhere in the literature.]

Definition: For FLS U, the statement

$$U = \mathcal{O}(X^k) \tag{1.1}$$

shall mean that $U_l = 0$ for $l < k$.

It is immediate from the definition that

$$\begin{aligned}
0 &= \mathcal{O}(X^\infty); \\
U + \mathcal{O}(X^k) &= U + \mathcal{O}(X^l) \\
&\ \text{for } l \le k \text{ (asymmetry of equality);} \\
(U + \mathcal{O}(X^k)) \pm (V + \mathcal{O}(X^l)) &= (U \pm V) + \mathcal{O}(X^{\min(k,l)}); \\
(U + \mathcal{O}(X^k)) \cdot (V + \mathcal{O}(X^l)) &= (U \cdot V) + \mathcal{O}(X^{\min(k+n,l+m)}) \\
&\ \text{if } U = \mathcal{O}(X^m) \text{ and } V = \mathcal{O}(X^n); \\
(U + \mathcal{O}(X^k))/(V + \mathcal{O}(X^l)) &= (U/V) + \mathcal{O}(X^{\min(k-n,l+m)}) \\
&\ \text{if in addition } V_n \ne 0, \text{ so } n \text{ is maximal.}
\end{aligned}$$

Notice that we can only let $X \to 0$ in $U + \mathcal{O}(X^k)$ if $k > 0$, otherwise the component at the origin is undefined; and in practice, we only ever do so when also $U = \mathcal{O}(1)$. In §4 – §5 we shall implicitly make extensive use of these rules.

For completeness, we should perhaps mention the more usual classical strategy for ensuring that a set of FLSs forms a field: to define convergence and enforce it, say over some annular region of the domain of complex numbers. The connection with our counterexample above is of course that any S, T corresponding to the same meromorphic function in distinct regions will give $U - V = 0$. The elementary definitions and algorithms of FLS arithmetic are fully discussed in standard texts such as **Hen74** §1.2, or **Knu81** §1.2.9 and §4.7. With the exception of the thorough tutorial **Niv69**, these authors consider only the ring of formal Taylor series with exponents $k \ge 0$; however, it is a fairly routine matter to extend the ring to a field, and there seems little reason to constrain oneself in this manner.

2. LFSR Sequences

A sequence S_n is a *linear recurring* or *linear feedback shift register* (LFSR) sequence when there exists a nonzero vector $[J_i]$ (the *relation*) of length $r+1$ such that

$$\sum_{i=0}^{r} J_i S_{n+i} \;=\; 0 \quad \text{for all integers } n.$$

The integer r is the *order* of the relation. If the relation has been established only for $a \leq n \leq b-r$ we say that the relation *spans* (at least) $S_a, \ldots, S_b$, with $a = -\infty$ and $b = +\infty$ permitted. LFSR sequences over finite fields are discussed comprehensively in **Lid86** §6.1–6.4.

It is usual to write a relation as an *auxiliary* polynomial $J(\mathbf{E})$ of degree r in the *shift* operator $\mathbf{E}: \; S_n \to S_{n+1}$:

Definition: The LFSR sequence $[S_n]$ satisfies the relation $J(\mathbf{E})$ just when for all n

$$J(\mathbf{E})[S_n] \;\equiv\; \sum_i J_i \mathbf{E}^i [S_n] \;\equiv\; \sum_i J_i [S_{n+i}] \;=\; [O_n], \tag{2.1}$$

the zero sequence (with order 0 and relation $J(\mathbf{E}) \;=\; 1$).

Notice that the number of nonzero components or *dimension* of a relation as a vector is in general $r+1$, two relations being regarded as equal (as for projective homogeneous coordinates) if they differ only by some nonzero constant multiple; also in the case of sequences whose values are given by a polynomial in n §9, the *degree* of the polynomial is in general $r-1$.

The *order* of a sequence (infinite in both directions) is normally understood to mean the minimum order of any relation it satisfies; this *minimal* relation is simply the polynomial highest common factor of all relations satisfied by the sequence, and is therefore unique. [The existence of such an HCF is guaranteed by the Euclidean property of the ring of polynomials in a *single* variable $\mathbf{E}$ over the ground domain, see **Her75** §3.9.] The leading and trailing coefficients J_r, J_0 of the minimal relation J of a (two-way-infinite) sequence are nonzero: such relations we shall call *proper*. These definitions must be interpreted with care when applied to segments with finite end-points, principally because even minimal relations may fail to be proper: both leading and trailing zero coefficients will then need to be retained during polynomial arithmetic on relations. Furthermore, if the minimum order is r and the span has length $< 2r$, a minimal relation is no longer unique, since there are too few equations to specify its coefficients.

By the elementary theory (**Lid86** §6.2) we have an explicit formula for an LFSR sequence:

Theorem: $[S_n]$ satisfies $J(\mathbf{E})[S_n] \;=\; [O_n]$ just when

$$S_n \;=\; \sum_i K_i {X_i}^n \quad \text{for all } n, \tag{2.2}$$

where the X_i are the roots of $J(X)$ and the K_i are coefficients, both lying in the algebraic closure of the ground domain when $J(X)$ has distinct roots; when the root X_i occurs with multiplicity e_i, K_i is a polynomial in n of degree $e_i - 1$.

Proof: Since we make frequent reference to this well-known result, we sketch a demonstration for the sake of completeness. [Over ground domains of finite characteristic, it is important that the 'polynomials' $K_i(n)$ are defined in terms of binomial coefficients; we return to this point in §9.]

From the Pascal triangle recursion, by induction on e

$$\begin{aligned} (\mathbf{E}-1)\binom{n}{e-1} \;&=\; \binom{n}{e-2}, \\ (\mathbf{E}-1)^e\binom{n}{e-1} \;&=\; 0; \end{aligned} \tag{2.3}$$

and so by expressing the arbitrary polynomial $K(n)$ of degree $e-1$ in n as a linear combination of binomial coefficients, we see that its e-th difference $(\mathbf{E}-1)^e K(n)$ is zero. Similary $(\mathbf{E}-X)X^n \;=\; 0$ and $(\mathbf{E}-X)^e K(n) X^n \;=\; 0$ for arbitrary X. Suppose S_n has the explicit form above (2.2), where $J(X)$ has just m distinct roots; let $X \;\equiv\; X_m$ etc., and let primes denote the analogous expressions involving only the other $m-1$ roots; then

$$\begin{aligned} J(\mathbf{E})S_n \;&=\; \prod_i (\mathbf{E}-X_i)_i^e S_n \\ &=\; J'(\mathbf{E})\big((\mathbf{E}-X)^e K(n) X^n\big) \;+\; (\mathbf{E}-X)^e\big(J'(\mathbf{E}){S'}_n\big) \\ &=\; J'(\mathbf{E})(0) + (\mathbf{E}-X)^e(0) \;=\; 0 \end{aligned}$$

for all n, using induction on m.

The converse can be approached constructively as in **Lid86** (who prove the distinct case only) by setting up linear equations for the K_i and showing that they possess a unique solution, as we shall do in (8.6) (for distinct X_i) and (9.2) (for coincident X_i effectively). In the general case of multiple roots, it is simpler to observe that the set of sequences satisfying a given relation J (assumed to possess nonzero leading and trailing coefficients) comprise a vector space **Her75** §4 whose dimension must be r, since each is completely determined by its initial r terms. The set constructed earlier is also a subspace of dimension r, so the two sets are identical by **Her75** Lemma 4.1.2. ■

If J is minimal then all the K_i are nonzero: for the Galois group of an irreducible factor of J is transitive on those X_i and their corresponding K_i while leaving S_n invariant, so those K_i must all be nonzero or all zero. In the latter case, J may be divided by the factor and so is not minimal. When all the roots coincide at unity, S_n equals an arbitrary polynomial of degree $r-1$ in n; so the latter are seen to be a special case of LFSR sequences.

3. Determinants and Zero-windows

Given some sequence $[S_n]$, we define its *Number Wall* (also *Zero Square Table* or — misleadingly — *QD Table*) $[S_{m,n}]$ to be the two dimensional array of determinants given by

Definition:

$$S_{m,n} \;=\; \begin{vmatrix} S_n & S_{n+1} & \dots & S_{n+m} \\ S_{n-1} & S_n & \dots & S_{n+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n-m} & S_{n-m+1} & \dots & S_n \end{vmatrix}. \tag{3.1}$$

The value of $S_{m,n}$ is defined to be unity for $m=-1$, and zero for $m<-1$. [These are known as *Toeplitz* determinants; or, with a reflection making them symmetric, and a corresponding sign change of $(-1)^{\binom{m+1}{2}}$, as *persymmetric* or *Hankel* determinants.] The rows and columns are indexed by m, n resp. in the usual orientation, with the m axis increasing to the South (bottom of page) and n to the East (right). [For examples see the end of §5 and elsewhere.]

Lemma: For any sequence $[S_n]$ and integers n and $m \geq 0$, we have $S_{m-1,n} \neq 0$ and $S_{m,n}=0$ just when there is a proper linear relation of minimum order m spanning at least $S_{n-m}, \dots, S_{n+m}$. Its coefficients J_i are unique up to a common factor. Further, when

$$S_{m,n} = S_{m,n+1} = \dots = S_{m,n+g-1} = 0 \quad \text{and} \quad S_{m,n-1} \neq 0,\; S_{m,n+g} \neq 0 \tag{3.2}$$

the relation maximally spans $S_{n-m}, \dots, S_{n+m+g-1}$. [Notice that we may have $n=-\infty$ or $g=+\infty$.]

Proof: by elementary linear algebra. For $g = 1$, set up $m+1$ homogeneous linear equations for the J_i, with a unique solution when they have rank m:

$$\begin{aligned} S_{n-m}J_0 \;+\; S_{n-m+1}J_1 \;+\; \ldots \;+\; S_nJ_m \;&=\; 0, \\ &\vdots \\ S_nJ_0 \;+\; S_{n+1}J_1 \;+\; \ldots \;+\; S_{n+m}J_m \;&=\; 0, \\ &\vdots \\ S_{n+g-1}J_0 \;+\; S_{n+g}J_1 \;+\; \ldots \;+\; S_{n+m+g-1}J_m \;&=\; 0. \end{aligned}$$

Using $S_{n-m+1}, \ldots, S_{n+m+1}$ on the right-hand side instead of $S_{n-m}, \ldots, S_{n+m}$ leaves m of these equations unaltered, so by induction on g the solution is constant over the whole segment of $[S_n]$ of length $2m+g$, and no further. This solution is proper: for if $J_m = 0$ there would be a nontrivial solution to the equations with m replaced by $m-1$, and so we should have $S_{m-1,n} = 0$ contrary to hypothesis; similarly if $J_0 = 0$. Similarly, it is minimal. Conversely, if a there is a relation, then $S_{m,n} = 0$; if it is minimal, then it is unique, and if it is also proper then m cannot be reduced, so $S_{m-1,n} \neq 0$. ■

> **Corollary:** $[S_n]$ is an LFSR sequence of order r if and only if row r (and all subsequent rows) of its number-wall degenerate to the zero sequence, but row $r-1$ does not. (3.3)

Given as many terms as we require of an LFSR sequence $[S_n]$, we can use (3.3) to compute its order r from its number-wall. Now suppose in addition we require to find the linear relation $J(\mathbf{E})$ which generates it. We introduce a new sequence of polynomials in a transcendental X over the domain, defined by

$$U_n(X) \;=\; (\mathbf{E} - X)S_n \;=\; S_{n+1} - X.S_n,$$

and form its number wall $U_{m,n}(X)$. If we set $X \to \mathbf{E}$, both sequence and wall (for $m \neq -1$) perforce degenerate to all zeros; therefore each $U_{m,n}(\mathbf{E})$ is a relation spanning those $2m+2$ elements of $[S_n]$ from which it was computed. Now for degree r there is only one such polynomial (modulo a constant factor), and that is the required minimal relation $J(\mathbf{E})$: for all n therefore, $U_{r-1,n}$ equals $J(X)$ multiplied by some domain element (nonzero since setting $X \to 0$ gives the wall for $[S_n]$ itself); and similarly $U_{r-1,n} = 0$ on all subsequent rows $m \geq r$.

> **Corollary:** $[S_n]$ is an LFSR sequence of order r if and only if row r (and all subsequent rows) of the number-wall of $S_{n+1} - X.S_n$ degenerate to the zero sequence, but row r does not; then row $r-1$ equals the minimal relation $J(X)$ of $[S_n]$ times a geometric sequence over the ground domain. (3.4)

This algorithm is slower than the more sophisticated Berlekamp-Massey method (12.1), taking time of order r^4 arithmetic operations over the ground domain (using straightforward polynomial multiplication) rather than r^2; but it is noticeably easier to justify, and it also gives the relations of intermediate (odd) spans.

A simple recursive rule for constructing the number-wall of a given sequence in the absence of zeros is classical, and follows immediately from the pivotal condensation rule styled by **Ioh82** §1.2 the *Sylvester Identity* [described by **Ait62** §45 as an *extensional* identity due to Jacobi, and elsewhere credited to Desnanot, Dodgson or Frobenius]:

> **Lemma:** Given an $m \times m$ matrix $[F_{ij}]$ and an arbitrary $(m-k) \times (m-k)$ minor $[G_{ij}]$ where $0 \leq k \leq m$, define H_{ij} to be the cofactor in $|F|$ selecting all the rows and columns of $|G|$, together with the i-th row and j-th column not in $|G|$. Then (3.5)
>
> $$|F_{ij}| \;\times\; |G_{ij}|^{k-1} \;=\; |H_{ij}|.$$

Proof: We may suppose the elements of $[F_{ij}]$ to be distinct variables transcendental over the ground domain, thus avoiding any problem with singular matrices. We may also suppose the rows and columns of $[F_{ij}]$ permuted so that $[G_{ij}]$ occupies the SE corner, $i, j > k$: this leaves the determinant unaltered except for a possible change of sign. Consider the matrix $[E_{ij}]$ with E_{ij} being F_{ij} when $i > k$, or $|G|$ bordered by row i and column j of F when $i \leq k$. Expanding this determinant by its first row, we see (with some difficulty — the reader is advised to work through a small example) that

$$E_{ij} \ = \ |G|F_{ij} \ + \ \sum_q A_{iq}F_{iq},$$

where the A_{iq} are cofactors from the last $m-k$ rows which do not depend on j. So $[E_{ij}]$ is effectively $[F_{ij}]$ with each of its first k rows multiplied by $|G|$, then subjected to a sequence of elementary column operations which leave the determinant unaltered. On the one hand then, $|E| = |F| \times |G|^k$.

Again,

$$E_{ij} \ = \ \begin{cases} H_{ij} & \text{for } 1 \leq i \leq k \text{ and } 1 \leq j \leq k \text{ by definition,} \\ G_{ij} & \text{for } k < i \leq m \text{ and } k < j \leq m \text{ by definition,} \\ 0 & \text{for } 1 \leq i \leq k \text{ and } k < j \leq m \text{ (determinant with equal columns).} \end{cases}$$

So on the other hand $|E| = |H| \times |G|$. Canceling the nonzero $|G|$ from $|E|$ gives the result. ■

Theorem: A symmetrical relation between the elements of the number-wall is

$$S_{m,n}^2 \ = \ S_{m+1,n}S_{m-1,n} \ + \ S_{m,n+1}S_{m,n-1}. \tag{3.6}$$

Proof: In (3.5) choose $k = 2$, $|F_{ij}| = S_{m+1,n}$, and $|G_{ij}| = S_{m-1,n}$ where this last is the cofactor occupying the interior of $[F_{ij}]$. Then the H_{ij} also turn out to be entries in the wall, and we find

$$S_{m+1,n} \times S_{m-1,n} \ = \ \begin{vmatrix} S_{m,n} & S_{m,n+1} \\ S_{m,n-1} & S_{m,n} \end{vmatrix}. \ ■$$

Corollary: A partial recursive construction for the number-wall is

$$\begin{aligned} S_{-2,n} \ &= \ 0, \quad S_{-1,n} \ = \ 1, \quad S_{0,n} = S_n, \\ S_{m,n} \ &= \ \big(S_{m-1,n}{}^2 \ - \ S_{m-1,n+1}S_{m-1,n-1})\big)/S_{m-2,n} \quad \text{for } m > 0, \\ &\qquad\qquad \text{provided } S_{m-2,n} \neq 0. \end{aligned} \tag{3.7}$$

[The initial row of zeros is not a great deal of use at this point, but comes in useful later as an *outer frame* for zeros occurring in the sequence.]

The possibility of zero elements in the wall is a stumbling block to the use of (3.7) for its computation, particularly if the ground domain happens to be a small finite field, when they are almost certain to occur. The next result sharpens a classical one in the study of Padé Tables §11, the first half of the 'Padé Block Theorem'. All proofs of it (including this author's) should be regarded with suspicion, having a disconcerting tendency to resort to hand-waving at some crucial point in the proceedings: for this reason we feel regretfully unable to recommend a prior version.

A *region* of a number wall is defined to be a simply-connected subset of elements, where two elements are *connected* when they have one subscript (m or n) equal, the other (n or m) differing by unity. The regions which we consider are $g \times g'$ *rectangles*, having at most four boundary segments along each of which some subscript is constant; their *lengths* g, g' (measured in numbers of elements along each segment) may range from zero to infinity. The *inner frame* of a rectangle is the smallest connected set which disconnects the region from its complement: it normally comprises four edges and four corners. The *outer frame* similarly disconnects the union of the rectangle with its inner frame from the complement. [In the example at the end of §5 will be found a 4×4 (square) rectangle of zeros, with an inner frame of ones.]

> **Theorem:** Square Window Theorem: Zero elements $S_{m,n} = 0$ of a number-wall occur only within *zero-windows*, that is square $g \times g$ regions with nonzero inner frames. The nullity of (the matrix corresponding to) a zero element equals its distance h from the inner frame. (3.8)

Proof: To start with, by (3.6) if $S_{m-1,n} = S_{m,n-1} = 0$ then $S_{m,n} = 0$, and by (3.6) shifting $m \leftarrow m-1, n \leftarrow n-1$, similarly $S_{m-1,n-1} = 0$; the mirror-image argument yields the converse. Now by an easy induction, any connected region of zeros must be a (possibly infinite) rectangle.

Now let there be such a rectangle with g rows, g' columns, and NW corner (n increasing to the East and m to the South) located at $S_{m,n}$: in detail,

$$\begin{aligned} S_{m,n} = 0,\ \ldots,\ S_{m,n+g'-1} = 0;\\ S_{m,n} = 0,\ \ldots,\ S_{m+g-1,n} = 0,\\ S_{m,n+g'-1} = 0,\ \ldots,\ S_{m+g-1,n+g'-1} = 0,\\ S_{m+g-1,n} = 0,\ \ldots,\ S_{m+g-1,n+g'-1} = 0,\\ S_{m-1,n} \neq 0,\ \ldots,\ S_{m-1,n+g'} \neq 0;\\ S_{m,n} \neq 0,\ \ldots,\ S_{m+g,n} \neq 0;\\ S_{m,n+g'} \neq 0,\ \ldots,\ S_{m+g,n+g'} \neq 0;\\ S_{m+g,n} \neq 0,\ \ldots,\ S_{m+g,n+g'} \neq 0. \end{aligned}$$

Then by (3.2) a unique minimal relation $J(\mathbf{E})$ of order m spans $S_{n-m}, \ldots, S_{n+m+g-1}$. Suppose $g' > g$: then the relation $\mathbf{E}^g J$ of order $m+g$ spans $S_{n-m-g}, \ldots, S_{n+m+g}$, so by (3.2) $S_{m+g,n} = 0$, contrary to hypothesis. Suppose $g' < g$: then since $S_{m+g',n} = 0$, there is a relation spanning $S_{n-m-g'}, \ldots, S_{n+m+g'}$; also since $S_{m+g'-1,n-1} \neq 0$ is a nonzero minor of $S_{m+g',n}$, the latter has nullity 1 and the relation must therefore be unique. One such relation is simply $\mathbf{E}^{g'} J$: so J spans $S_{n-m+g'}, \ldots, S_{n+m+g'}$ and by (3.2) $S_{m,n+g'} = 0$, contrary to hypothesis. The only possibility remaining is that $g' = g$, and the rectangle must be a square.

Consider this square divided by its diagonals $i - j = m - n$ and $i + j = m + n + g - 1$ into North, East, South, West quarters; let h denote the distance of the element $S_{i,j}$ from the frame in the same quarter. All the elements in the North quarter have rank m, since the only relations spanning subintervals of $S_{n-m}, \ldots, S_{n+m+g-1}$ are (polynomial) multiples of J itself: in particular, if g is odd, the central element has rank m and nullity $h = [(g+1)/2]$. If g is even, there are four elements at the centre, the North pair having rank m and nullity h as before; the South pair have rank $m+1$, since (for example) any relation corresponding to $S_{m+g/2,n+g/2-1}$ spans $S_{m-n-1}, \ldots, S_{n+m+g/2}$, but S_{m-n-1} lies outside the span of J (the relations are multiples of $\mathbf{E}J$). So for any g the central elements have nullity equal to their distance h from the frame. Now observe that the nullity of any element $S_{i,j}$ can only differ from that of its neighbors $S_{i-1,j}, S_{i,j-1}, S_{i,j+1}, S_{i+1,j}$ by at most unity, since the matrices differ essentially by a single row or column. Therefore it must decrease with h in all directions, in order to reach zero with h at the inner frame where all elements are nonzero. ■

A simple consequence of (3.8) is the occurrence of 'prime windows' in a wall over some larger ground domain:

> **Corollary:** Elements divisible by some prime ideal P clump together in square regions, elements at distance h from the frame being divisible by (at least) P^h. (3.9)

In particular, these windows are noticeable for ordinary primes p in integer walls.

A less obvious but more useful and rather elegant consequence, credited to Massey in **Cha82**, quantifies the notion that, if two different sequences have a large common portion, then at least one of them has high linear order. It could be proved directly by linear dependence arguments.

> **Corollary:** Massey's Lemma: The sum of the orders of proper relations spanning two intervals of a sequence exceeds the length of the intersection, unless each relation spans their union. (3.10)

Proof: Let the intervals (a_i, b_i) of the sequence be spanned maximally by minimal proper relations of orders r_i, for $i = 1, 2$. By (3.2), (3.8) there are corresponding windows in the number-wall at (m_i, n_i) of size g_i where $a_i = n_i - m_i$, $b_i = n_i + m_i + g_i - 1$, so

$$m_i = r_i, \quad n_i = a_i + r_i, \quad g_i = b_i - a_i - 2r_i + 1.$$

Suppose the windows to be distinct (failing which their parameters coincide in pairs); since they are square and cannot overlap, one of the following is true:

$$m_1 + g_1 < m_2, \quad n_1 + g_1 < n_2, \quad m_2 + g_2 < m_1, \quad n_2 + g_2 < n_1.$$

Substituting, either

$$\begin{cases} b_1 - a_1 - r_1 + 1 < r_2 & \text{or} \\ b_1 - r_1 + 1 < a_2 + r_2 & \text{or} \\ b_2 - a_2 - r_2 + 1 < r_1 & \text{or} \\ b_2 - r_2 + 1 < a_1 + r_1 \end{cases}$$

whence

$$r_1 + r_2 \ > \ 1 + \min(b_1 - a_1, b_1 - a_2, b_2 - a_2, b_2 - a_1).$$

as claimed.

Relaxing the maximality constraint on the intervals and the minimality on the order does not affect the result. ■

As an illustration, suppose we are to find the order and relation spanning

$$S \ = \ [0, 0, 0, 1, 16, 170, 1520, 12411, 96096, 719860, \ldots].$$

The following pair of number-walls can be computed via (3.6): The final row of zeros of the first suggests (3.3) that the order might be $r = 4$. The final row of the second gives (3.4) the auxiliary polynomial $J \ = \ \mathbf{E}^4 - 16\mathbf{E}^3 + 86\mathbf{E}^2 - 176\mathbf{E} + 105 \ = \ 0$, that is S satisfies the relation

$$S_{n+4} - 16S_{n+3} + 86S_{n+2} - 176S_{n+1} + 105S_n \ = \ 0.$$

$m \backslash n$	0	1	2	3	4	5	6	7	8	9
−2	0	0	0	0	0	0	0	0	0	0
−1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	1	16	170	1520	12411	96096	719860
1	0	0	0	1	86	4580	200530	7967001	300258756	
2	0	0	0	1	176	21946	2449616	262848811		
3				1	105	11025	115762			
4					0	0				

0	0	0	0	0	0	0
1	1	1	1	1	1	1
0	0	1	$16-X$	$170-16X$	$1520-170X$	$12411-1520X$
0	0	1	$86-16X+X^2$	$4580-1200X+86X^2$	$200530-59824X+4580X^2$	
		1	$176-86X+16X^2-X^3$	$21946-13456X+2711X^2-176X^3$		
			$105-176X+86X^2-16X^3+X^4$			

4. The Frame Formulae

We are now ready to tackle the central undertaking of this investigation: the elucidation of conditions on the number-wall elements of the inner and outer frames surrounding a zero-window, permitting the recursive rule (3.7) to be completed. The results to be proved are as follows, the adjacent diagram illustrating the notation employed, to be explained in more detail as we proceed.

Diagram Window Notation

$$\begin{array}{cccccccccc}
 & E_0 & E_1 & E_2 & \dots & E_k & \dots & E_g & E_{g+1} & \\
F_0 & B, A_0 & A_1 & A_2 & \dots & A_k & \dots & A_g & A, C_{g+1} & G_{g+1} \\
F_1 & B_1 & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \dots & \mathbf{0} & C_g & G_g \\
F_2 & B_2 & \mathbf{0} & \ddots & (P) & \rightarrow & & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & (Q) & \ddots & & \uparrow & \mathbf{0} & C_k & G_k \\
F_k & B_k & \mathbf{0} & \downarrow & & \ddots & (R) & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & & \leftarrow & (T) & \ddots & \mathbf{0} & C_2 & G_2 \\
F_g & B_g & \mathbf{0} & \dots & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} & C_1 & G_1 \\
F_{g+1} & B, D_{g+1} & D_g & \dots & D_k & \dots & D_2 & D_1 & D, C_0 & G_0 \\
 & H_{g+1} & H_g & \dots & H_k & \dots & H_2 & H_1 & H_0 &
\end{array}$$

Theorem: Frame Ratio Theorem: The inner frame of a $g \times g$ zero-window comprises four geometric sequences, along the North, West, East, South edges, with ratios P, Q, R, T resp., and origins at the NW and SE corners. They satisfy

$$PT/QR \;=\; (-)^g; \tag{4.1}$$

Corollary: Inner Frame Theorem: The inner frame sequences A_k, B_k, C_k, D_k satisfy

$$A_k D_k / B_k C_k \;=\; (-)^{gk} \quad \text{for } 0 \le k \le g+1; \tag{4.2}$$

Theorem: Outer Frame Theorem: The outer frame sequences E_k, F_k, G_k, H_k lie immediately outside A_k, B_k, C_k, D_k resp., and are aligned with them. They satisfy the relation: For $g \ge 0$, $0 \le k \le g+1$,

$$QE_k/A_k \;+\; (-)^k PF_k/B_k \;=\; RH_k/D_k \;+\; (-)^k TG_k/C_k. \tag{4.3}$$

The method of proof is straightforward in principle: unfortunately, the details are somewhat involved. Suppose we are given an *original* sequence $[S_n]$ with elements in some given ground domain, such that the number wall displays a $g \times g$ zero-window with NW corner $S_{m,n}$. We proceed to modify one element by adding a transcendental

$$S_{n+m+g-1} \;\leftarrow\; S_{n+m+g-1} + (-)^m X,$$

yielding a *perturbed* sequence over the domain extended to formal power series, whose (perturbed) wall has only a $(g-1) \times (g-1)$ zero-square at the same location.

Now assuming the exact result for the smaller zero-window over the extension, we proceed to prove it by induction for the perturbed wall, then finally let $X \to 0$ [i.e. specialize to FLS coefficient of X^0]. To avoid unnecessarily complicating an already quite sufficiently involved notation, we do not explicitly distinguish between the original and perturbed quantities; but claims referring to the latter are styled *Lemma* rather than *Theorem*, and explicitly involve X. We make heavy implicit use of our $\mathcal{O}(X^k)$ notation and rules (1.1).

Here we digress to emphasize that, for this induction to take effect, the perturbed configuration must itself constitute the number wall of some actual sequence; the importance of this will subsequently be underlined by a counterexample (5.4). Failure to respect this principle fatally compromised at least one earlier attempted proof of an essentially equivalent result — credited to Gilewicz and Froissart in **Gil78** — where the postulated configuration of four perturbed inner edges, each linear in the perturbing variable, can be seen by (4.5) to be impossible. [It is intriguing to speculate how such a strategy might have come to be preferred over that adopted here. A partial explanation may lie in the various other pitfalls awaiting us below, which shall duly be paraded for the reader's edification.]

Diagram Perturbed Window Notation

$$
\begin{array}{ccccccccccc}
 & E_0 & E_1 & E_2 & \dots & E_k & \dots & \dots & E_g & E_{g+1} & \\
F_0 & B, A_0 & A_1 & A_2 & \dots & A_k & \dots & \dots & A_g & A, C_{g+1} & G_{g+1} \\
F_1 & B_1 & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \dots & \mathbf{0} & M_g & C_g & G_g \\
F_2 & B_2 & \mathbf{0} & \ddots & (P) & \rightarrow & & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & (Q) & \ddots & & \uparrow & \mathbf{0} & M_k & C_k & G_k \\
F_k & B_k & \mathbf{0} & \downarrow & & \ddots & (R) & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & & \leftarrow & (T) & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \mathbf{0} & \dots & \mathbf{0} & \dots & \dots & \mathbf{0} & M_2 & C_2 & G_2 \\
F_g & B_g & N_g & \dots & N_k & \dots & \dots & N_2 & N, M_1 & C_1 & G_1 \\
F_{g+1} & B, D_{g+1} & D_g & \dots & D_k & \dots & \dots & D_2 & D_1 & D, C_0 & G_0 \\
 & H_{g+1} & H_g & \dots & H_k & \dots & \dots & H_2 & H_1 & H_0 &
\end{array}
$$

The perturbed window is illustrated in the accompanying Diagram, representing a region within the perturbed wall, for some sequence which is not shown. Below and on the counter diagonal, all perturbed elements are polynomial (finite FLS); above it, they remain as original. The original zero-window had inner frame comprising A, B, C, D and outer frame E, F, G, H on its North, West, East, South sides; the perturbed window has inner frame M, N (where originally there were zeros) and outer frame C, D on its East, South. The frame vectors are of length $g + 2$ (original) or $g + 1$ (perturbed), indexed from 0: the origin of North frame vectors is on column $n - 1$, of West on row $m - 1$ (A_0 and B_0 are identical), of East on row $m + g$, and of South on column $n + g$ (C_0 and D_0 are identical). It will emerge that A, B, C, D, M, N are approximately geometric sequences (4.5) – (4.7), their ratios denoted by $A_1/A_0 = P, Q, R, T, U, V$ respectively.

Lemma: There are elements U, V such that for $1 \le k \le g+1$,

$$\begin{aligned} M_k \;&=\; A_g U^{k-g-1}, \quad N_k \;=\; B_g V^{k-g-1}; \\ \text{in fact,}\quad U \;&=\; P/X, \quad V \;=\; (-)^{g-1}Q/X. \end{aligned} \tag{4.5}$$

Proof: By definition (3.1)

$$M_g \;=\; \begin{vmatrix} S_{n+g-1} & \ldots & S_{n+g+m-1} + (-)^m X \\ \vdots & \ddots & \vdots \\ S_{n+g-m-1} & \ldots & S_{n+g-1} \end{vmatrix}$$

$$= \begin{vmatrix} S_{n+g-2} & \ldots & S_{n+g+m-3} \\ \vdots & \ddots & \vdots \\ S_{n+g-m-1} & \ldots & S_{n+g-2} \end{vmatrix} X \;+\; \begin{vmatrix} S_{n+g-1} & \ldots & S_{n+g+m-1} \\ \vdots & \ddots & \vdots \\ S_{n+g-m-1} & \ldots & S_{n+g-1} \end{vmatrix},$$

expanding the determinant;

$$= \; A_{g-1}X \;+\; 0$$

in terms of the original wall. Also $M_{g+1} \equiv A_g$, so we can define

$$U \;=\; M_{g+1}/M_g \;=\; A_g/A_{g-1}X, \quad \text{or} \quad U \;=\; P/X.$$

For N, V, Q the only difference is that the determinant is order $m+g-1$; notice that we can use the same X in both contexts, by (3.8). Finally, for $1 \le k \le g-1$, by (3.6), ${M_{k+1}}^2 = M_{k+2}M_k$, showing that $[M_k]$ is geometric with ratio U; similarly for N. ■

Lemma: There are elements P, Q such that for $0 \le k \le g+1$,

$$A_k \;=\; A_0 P^k \;+\; \mathcal{O}(X), \quad B_k \;=\; B_0 Q^k \;+\; \mathcal{O}(X). \tag{4.6}$$

Proof: For $0 \le k \le g$, see the end of the proof of (4.5) with $P = A_1/A_0$, $Q = B_1/B_0$. For $k = g+1$, using (3.6) and (4.6) [A is exactly geometric for $k < g+1$], we have

$$A_{g+1} \;=\; ({A_g}^2 - E_g M_g)/A_{g-1} \;=\; A_0 P^{g+1} - E_g X.$$

B behaves similarly. ■

It is important to bear in mind that we may always divide by elements of the inner frame or by ratios, since we know these to be nonzero; indeed the same is true of C and D, even in the perturbed case (4.7). And when multiplying or dividing FLSs (1.1), we need to ascertain that the factors have order sufficiently large to justify the order claimed for the error in their product: E, F, G, H are always $\mathcal{O}(1)$ at worst; A, B, C, D and P, Q, R, T are $\mathcal{O}(1)$ exactly; but U, V are $\mathcal{O}(1/X)$.

Notice here too that the 'ratios' R, T of the approximately geometric outer frames are defined explicitly by $C_1/C_0, D_1/D_0$, rather than retaining their original values, an apparently insignificant detail which is central to the proof: it allows us to get an unexpectedly small and explicit first perturbation term in the expansions (4.7) of C, D, without which the crucial information carried by the perturbation term in the proof of the central result (4.9) would be swamped by noise of order $\mathcal{O}(X)$.

Lemma: There are elements R, T such that for $2 \le k \le g+1$,

$$\begin{aligned} C_k \;&=\; C_0 R^k \;-\; (R/P)^{g-k+3} G_{k-1} X^{g-k+2} \;+\; \mathcal{O}(X^{g-k+3}), \\ D_k \;&=\; D_0 T^k \;-\; (-)^{(g-1)k} (T/Q)^{g-k+3} H_{k-1} X^{g-k+2} \;+\; \mathcal{O}(X^{g-k+3}). \end{aligned} \tag{4.7}$$

Proof: By induction on k. For $k = 1$ we have $C_1 = C_0 R$ exactly by definition; the Lemma fails here, but still $C_1 = C_0 R + \mathcal{O}(X^{g+1})$ as required to commence the induction. For $2 \le k \le g+1$,

$$\begin{aligned} C_k &= {C_{k-2}}^{-1}({C_{k-1}}^2 - M_{k-1}G_{k-1}) \quad \text{by (3.6)}, \\ &= {C_0}^{-1}R^{2-k}({C_0}^2 R^{2k-2} \ - \ A_g(X/P)^{g-k+2}G_{k-1}) \ + \ \mathcal{O}(X^{g-k+3}), \end{aligned}$$

by (4.5) and hypothesis or definition; now we get the result since by (4.6) and the previous line

$$ {C_0}^{-1}A_g \ = \ \big({C_{g+1}}^{-1}R^{g+1} + \mathcal{O}(X)\big)\big(A_{g+1}P^{-1} + \mathcal{O}(X)\big) \ = \ R^{g+1}/P + \mathcal{O}(X). $$

D_k is treated similarly. ■

We proceed to the perturbed forms of the Frame Ratio and Outer Frame Theorems. The form of Lemma (4.9) demands some explanation. As explained earlier, the sequence and its wall have been perturbed so that the window of size g has shrunk to size $g-1$, and the natural approach would seem to be simply to apply the original Outer Frame Theorem (4.3) to compute the perturbed row D inductively, then find H immediately by (3.6) as $H_k = ({D_k}^2 - D_{k-1}D_{k+1})/N_k$: the idea is illustrated towards the end of §13.

There are several reasons why this program fails in a formal context. To begin with, finding one H_k would require three elements from D, which in turn involve three from E and F, rather than the single one demanded by the Theorem (4.3) to be proved. Then we should need to divide by $N_k = \mathcal{O}(X^{g-1-k})$ by (4.5): this implies that all terms of smaller order in the numerator must cancel, so requires pre-evaluation of this many terms of the polynomials D_k. Finally similar reasons demands the polynomials C_k, which would have to be calculated in some unrelated fashion, since we have only one equation connecting E, F, C, D: to wit (4.3) with C, D playing the part of G, H etc. [It is a fairly safe bet that (4.3) is the only condition possible on the outer frame elements, since by manipulating the original sequence, we can arrange for E,F,G to take arbitrary values. Consequential alterations to the inner frame, being fixed by just four elements A_0, P, Q, R, have little influence on this situation.]

Lemma:

$$ PT/QR \ = \ (-)^g \ + \ \mathcal{O}(X^{g+1}). \tag{4.8} $$

Proof: By (4.5), $QU/PV = (-)^{g-1}$ (avoiding induction on g); and using (4.5) with $k = 2$ and (4.7) with $k = g$ (both of which in fact need no error term)

$$\begin{aligned} N_2/M_2 &= B_g V^{1-g}/A_g U^{1-g} \\ &= A_0 P^g (X/P)^{g-1}/B_0 Q^g (X/Q)^{g-1}(-)^{(g-1)^2} \ = \ V/U, \end{aligned}$$

noting that $A_0 = B_0$ and $(g-1)^2$, $(g-1)$ have the same parity; also by (4.7)

$$ C_1/D_1 \ = \ C_0 R/D_0 T \ = \ R/T. $$

Collecting,

$$\begin{aligned} QR/PT &= (QU/PV)(V/U)(R/T) \ = \ (-)^g N_2 C_1/M_2 D_1 \\ &= (-)^g(-M_2 D_1 + M_1^2)/M_2 D_1 \quad \text{by (3.6)} \\ &= -(-)^g + \mathcal{O}(X^{g+1}) \quad \text{by (4.5).} \ ■ \end{aligned}$$

Lemma: For $g \ge 0$, $0 \le k \le g+1$,

$$ QE_k/A_k \ + \ (-)^k PF_k/B_k \ = \ RH_k/D_k \ + \ (-)^k TG_k/C_k + \mathcal{O}(X) \tag{4.9} $$

Proof in cases $k = 0, g+1$: By (3.6) and definition of P, Q, R, T,

$$ {A_0}^2 \ = \ B_1 E_0 + A_1 F_0 \ = \ A_0 Q E_0 + A_0 P F_0, $$

whence $A_0{}^{-1}(QE_0 \;+\; PF_0) \;=\; 1$; similarly $C_0{}^{-1}(RH_0 \;+\; TG_0) \;=\; 1$. Also $A_0 = B_0$ and $C_0 = D_0$, which proves case $k = 0$; case $k = g + 1$ is similar.

Proof in cases $1 \leq k \leq g$: For $g = 0$ there are no (further) cases to consider. For $g \geq 1$, we assume (4.9), replacing g by $g - 1$ for the induction; C_k, D_k, G_k, H_k by M_{k+1}, N_{k+1}, C_{k+1}, D_{k+1}, noticing the shift in origin caused by the new SE corner; R, T by U, V; and letting $X \to 0$. Then by inductive hypothesis

$$\begin{aligned}
&Q.E_k/A_k \;+\; (-)^k P.F_k/B_k \\
&\quad = \; U.D_{k+1}/N_{k+1} \;+\; (-)^k V.C_{k+1}/M_{k+1} \\
&\quad = \; (P/X)(-)^{(g+1)k} B_g{}^{-1} (X/Q)^{k-g} D_{k+1} \\
&\qquad + \; (-)^{k+g+1} (Q/X) A_g{}^{-1} (X/P)^{k-g} C_{k+1} \;+\; \mathcal{O}(X) \quad \text{by (4.5)} \\
&\quad = \; Y + Z + \mathcal{O}(X^{g-k+2}) \;+\; \mathcal{O}(X), \quad \text{say.}
\end{aligned}$$

At this point we expand C, D by (4.7) and separate them into main Y, first perturbation Z and residual error terms. The main terms cancel to order X, as expected:

$$\begin{aligned}
Y &= X^{k-g-1}(-)^{g+k+1}\big((-)^{gk+g+1} D_0 B_g{}^{-1} Q^{-g} (T/Q)^k PT \;+\; C_0 A_g{}^{-1} P^{-g} (R/P)^k QR\big) \\
&= \; X^{k-g-1}(-)^{g+k+1} A_0 C_0 \big((-)^{gk+g+1}(T/Q)^k PT + (R/P)^k QR\big) \\
&\quad \text{since } B_g Q^{-g} = B_0 = A_0 = A_g P^{-g},\ D_0 = C_0; \\
&= \; X^{k-g-1}(-)^{g+k+1} A_0 C_0 (R/P)^k QR(-1+1) \;+\; \mathcal{O}(X^{g+1}) \\
&\quad \text{since } T/Q = (-)^g R/P + O(X^{g+1}),\ PT = (-)^g QR \;+\; \mathcal{O}(X^{g+1}) \text{ by (4.8);} \\
&= \; \mathcal{O}(X^k).
\end{aligned}$$

The first perturbation terms incorporate the desired right-hand side:

$$\begin{aligned}
Z &= (-)^{g+k}\big((-)^k B_g{}^{-1} PQ^{-2} T^{g-k+2} H_k \;+\; A_g{}^{-1} P^{-2} QR^{g-k+2} G_k\big) \\
&\quad \text{simplifying — the exponents of X cancel exactly;} \\
&= \; (-)^{g+k}\big((-)^k (PT/QR) RH_k/D_k + (QR/PT) TG_k/C_k\big) \;+\; \mathcal{O}(X) \\
&\quad \text{since } A_g PR^{g-k+1} = C_k \;+\; \mathcal{O}(X) \text{ etc by (4.6) then (4.7) with } k = g+1; \\
&= \; RH_k/D_k \;+\; (-)^k TG_k/C_k \;+\; \mathcal{O}(X) \quad \text{by (4.8).}
\end{aligned}$$

Collecting Y, Z, etc and checking that the error terms are all $\mathcal{O}(X)$ now gives the result. ■

Finally, setting $X \to 0$ in (4.8) and (4.9), we are home and dry in the original wall: (4.1) and (4.3) are immediate, and (4.2) is a simple consequence of (4.8), (4.6), (4.7). However, notice that this last step is only possible because specialization commutes with arithmetic (1.0).

5. The Algorithm, Special Cases

By isolating T, D_k and H_k on the left-hand side of the Frame Theorems, we immediately get a comprehensive and efficient recursion for computing the number-wall by induction on rows m:

Corollary: If $m \leq 0$ or $S_{m-2,n} \neq 0$ use (3.7); otherwise, determine whether $S_{m,n}$, with respect to the zero-window immediately to the North, lies within:
(i) the interior, when by (4.1)

$$S_{m,n} = 0 \quad \text{and} \quad T \ = \ (-)^g QR/P;$$

(ii) the inner frame, when by (4.2) (5.1)

$$S_{m,n} \ \equiv \ D_k \ = \ (-)^{gk} B_k C_k / A_k;$$

(iii) the outer frame, when by (4.3)

$$S_{m,n} \ \equiv \ H_k \ = \ (D_k/R)(QE_k/A_k + (-1)^k(PF_k/B_k - TC_k/M_k)).$$

Illustrative examples are given later in this section.

In principle the original Sylvester recursion (3.6) might be dispensed with, since the Frame Theorems hold even for $g = k = 0$; but in practice it is impossible to avoid programming the latter as a special case anyway, so the saving is only conceptual. [To quote Alf van der Poorten **Poo96**: In theory, there is no difference between theory and practice. In practice, it doesn't quite work that way.]

The special case $g = k = 1$ can be recast in the simplified form:

Corollary: In the notation of the attached figure depicting a portion of the number-wall, for an isolated zero at W we have $ED^2 + HA^2 = FC^2 + GB^2$; (5.2)

this follows directly by setting $W = 0$ in the (polynomial) identity:

Lemma: In the notation of the attached figure

$$ED^2 + HA^2 - W(EH + AD) \ = \ FC^2 + GB^2 - W(FG + BC). \tag{5.3}$$

$$\begin{array}{ccccc} & & E & & \\ & L & A & K & \\ F & B & W & C & G \\ & N & D & M & \\ & & H & & \end{array}$$

Proof: Suppose W transcendental over the ground domain of $[S_n]$ [strictly, W is some not-identically-vanishing function of transcendental X, such as $W = LX$ where $L \neq 0$ and X is the perturbation of $[S_n]$ in the proof of (4.5)]. Expanding $LK \cdot NM = LN \cdot KM$ via (3.6) then rearranging,

$$(A^2 - EW)(D^2 - HW) \ = \ (B^2 - FW)(C^2 - GW),$$

$$(BC + AD)(AD - BC) \ + \ W(FC^2 + GB^2 - ED^2 - HA^2) \ + \ W^2(EH - FG) \ = \ 0.$$

Again using (3.6), substituting for $BC + AD \ = \ W^2$, canceling W and rearranging gives the desired equation. We can now argue, as in the proof of (3.5), that for fixed m this is a polynomial identity in elements of a sequence $[S_n]$ of distinct transcendentals, so it remains true even when some of the constituent elements such as W take zero values. Alternatively, in the spirit of §7, we can examine each possible pattern of zeros individually, and resolve it by applying (3.8), (4.2) for various $g \leq 3$. ■

[The above approach is noteworthy by reason of its beguiling unreliability: not only does equation (5.2) possess more symmetry than the general Outer Frame Theorem — obstructing attempts to guess the latter — but we have so far been unable to construct an analogous identity for the the $g = 2$ case, even though already in possession of (4.3). The analytically motivated proof technique conceals a pitfall, on which we now dilate.] We have been careful throughout to ensure that every table considered is actually the valid number wall of some sequence. To emphasize that this is not merely some pedantic logical conceit, we give a simple example to illustrate the consequences of abandoning this restriction during a proof, irrelevant though it might be to the initial formulation of a conjecture.

Consider the portion of a number wall shown (diagram left), where the NW zero is S_{mn}, say, and the three zeros are all isolated.

$$\begin{array}{ccccc} . & . & E & . & . \\ . & . & . & A & . \\ F & . & \mathbf{0} & Y & \mathbf{0} \\ . & B & Z & X & . \\ . & . & \mathbf{0} & . & . \end{array} \qquad\qquad \begin{array}{ccccc} . & . & E & . & . \\ . & . & . & A & . \\ F & . & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ . & B & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ . & . & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{array} \qquad\qquad \begin{array}{ccccc} . & . & E & . & . \\ . & . & . & A & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{array}$$

By (5.2) and (3.6) we have $FY^2 = EZ^2$ and $Y^2 = AX$, $Z^2 = BX$; substituting the latter into the former gives $EBX = FAX$, from which we cancel X to get $EB = FA$. Letting $X \to 0$, by (3.8) $Y, Z \to 0$ also, leaving a 3×3 window (diagram centre) for which we have established the engagingly succinct

Canard: Fool's Frame Theorem: In the notation of the diagram, there is reason to believe that

$$EB = FA. \tag{5.4}$$

Sadly, the attached period 6 wall over **Z**, where $A = E = 1$, $F = 2$, $B = 4$, offers little comfort to anyone disposed to give this credence.

0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
−1	−1	1	1	1	1	1	−1	−1
2	2	2	0	0	0	2	2	2
4	0	4	0	0	0	4	0	4
8	−8	8	0	0	0	8	−8	8
16	−16	16	−16	16	−16	16	−16	16
0	0	0	0	0	0	0	0	0

What went wrong? We could just shrug and say 'where's the sequence?'; but for the sake of explaining the phenomenon a little more convincingly, let us temporarily abandon the formal algebraic context and restrict the wall to some continuous ground domain such as **R**, in particular interpreting $X \to 0$ as the familiar limit operator.

By (3.2), if $Z \neq 0$ then there is a proper relation of order $m + 2$ spanning $S_{n-m-2}, ..., S_{n+m+2}$; and if $A \neq 0$, $Y = 0$, there is a proper relation of order m spanning $S_{n-m}, ..., S_{n+m+2}$. Then as $X \to 0$, by continuity both claims become true. The sum of the orders is $2m + 2$ and the length of the intersection is $2m + 3$, so by a minor abuse of (3.10) the two relations must be identical. Hence the limiting configuration is actually a window of size 5×5 with NW corner at $S_{m,n-2}$ (diagram right): in particular, $F = B = 0$, and (5.4) is actually true for the subset of number walls to which we have inadvertently restricted ourselves — it's just not very interesting.

A second interesting special case of the Frame Theorems occurs when the ground domain is the binary field $\mathbf{F}_2$: The frame ratios P, Q, R, S and inner frames A, B, C, D are nonzero, so they must all be unity, and the algorithm reduces to

Corollary: Over the binary field, $S_{m,n} = 0$ in the interior of a window, $S_{m,n} = 1$ along its inner frame, and $S_{m,n} \equiv H_k = E_k + F_k + G_k \pmod 2$ along its outer frame. (5.5)

We illustrate (5.5) with a rather more extensive example of a number-wall. $[S_n]$ is the minimal order binary deBruijn sequence (see §9) with period [1111000011010010], and binary wall as in the Diagram (periodic horizontally, zero above and below vertically):

Diagram Binary Wall

m\n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
-1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	1	1	1	0	0	0	0	1	1	0	1	0	0	1	0
1	1	0	0	1	0	0	0	0	1	1	1	1	0	0	1	1
2	1	0	0	1	0	0	0	0	1	0	1	1	1	1	1	1
3	1	1	1	1	0	0	0	0	1	1	1	0	1	1	0	0
4	1	0	0	1	1	1	1	1	1	0	1	1	1	1	0	0
5	1	0	0	1	0	1	0	0	1	1	1	1	0	1	1	1
6	1	1	1	1	1	1	0	0	1	0	0	1	1	1	1	0
7	1	0	0	0	0	1	1	1	1	0	0	1	1	0	1	1
8	1	0	0	0	0	1	0	0	1	1	1	1	1	1	1	0
9	1	0	0	0	0	1	0	0	1	1	1	0	0	1	1	1
10	1	0	0	0	0	1	1	1	1	0	1	0	0	1	0	1
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

For example, assuming rows $m < 7$ already to hand, we can immediately complete the 4×4 window of zeros with NW corner at $(m, n) = (7, 1)$, together with its inner frame of ones. Once rows $m < 12$ are to hand, we can find element $(12, 0)$ by (3.7), then element $(12, 1)$ by (5.5) with $k = 4$, $E = S_{5,4} = 0$, $F = S_{10,15} = 1$, $G = S_{7,6} = 1$, $H = S_{12,1} = 0 + 1 + 1 = 0$ (mod 2). The final row of zeros shows that the order over the binary domain is $r = 12$.

If instead we regard $[S_n]$ as defined over the integers, the following wall results. To find element $(10, 7)$ from previous rows we can employ (5.2) with $A, B, C, D \;=\; 3, 6, 3, -6$ and $E, F, G = -2, 1, 1$, getting

$$H \;=\; (FC^2 + GB^2 - ED^2)/A^2 \;=\; (1.9 + 1.36 + 2.36)/9 \;=\; 13.$$

To find find our way around the window at $(0, 4)$ with $g = 4$ demands the full works: happily $P = Q = R = 1$ so $T = 1$ by (4.1), $A = B = C = 1$ so $D = 1$ by (4.2), and we find say element $(5, 7)$ by (4.3) with $k = 1$ and $E, F, G = 0, 1, 3$, $H = (QE/A - PF/B + TG/C)D/R = 2$. The order over the integer domain is $r = 13$.

Diagram Integer Wall

$m\backslash n$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
−2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
−1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	1	1	1	0	0	0	0	1	1	0	1	0	0	1	0
1	1	0	0	1	0	0	0	0	1	1	−1	1	0	0	1	−1
2	1	0	0	1	0	0	0	0	1	2	1	1	1	1	1	1
3	1	1	1	1	0	0	0	0	1	3	1	0	−1	−1	0	0
4	1	2	2	1	1	1	1	1	1	4	1	1	1	1	0	0
5	1	2	2	−1	0	1	−2	2	−3	5	−3	1	0	−1	1	−1
6	3	1	3	1	1	1	2	−2	−1	4	4	1	1	1	3	4
7	5	−4	4	2	0	−1	−3	3	−3	4	−4	−3	−1	2	5	−7
8	−1	−4	8	4	2	1	6	0	3	1	7	5	7	9	13	6
9	5	−6	20	0	−8	11	−12	−6	−3	−5	−11	8	−4	−5	23	−7
10	17	16	50	40	32	25	35	13	−7	−8	23	4	8	13	38	−11
11	93	99	93	51	−3	−45	−75	−69	−51	−45	−51	−21	−3	27	69	75
12	72	72	72	72	72	72	72	72	72	72	72	72	72	72	72	72
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Finally, it is natural to ask is whether a simple recursive algorithm exists for number walls over more general ground rings, in particular over $\mathbf{Z}/q\mathbf{Z}$ for q an arbitrary natural number. [The obvious approach, to compute the wall over $\mathbf{Z}$ and then reduce (mod q), is less than ideal since the intermediate integers may be very large.] If $q = \prod_k {p_k}^{e_k}$ is expressed as a product of prime powers, the residue (mod q) can be computed easily from residues (mod p^e) via the Chinese Remainder Theorem **Dav88** §A.5.1, reducing the problem to the case $q = p^e$. By (3.8), the power of p (or in general, any prime ideal) dividing an element at distance h from the frame within a zero-window (mod p) must be at least p^h, and one might naïvely hope that perhaps it might be exactly p^h (it needn't); or failing that, the frames might behave in a fashion which generalizes the situation modulo p, involving the excess over p^h near a particular point on the frame. However, it is easy to construct a wall modulo $q = 4$ with a large window (mod 2) which is also perfectly square (mod 4), but for which the outer frame sum $E + F + G + H$ varies irregularly between 0 and 2 (mod 4) — strongly suggesting that the hope is unjustified. [However some progress in this area has been made — see **Ree85**.]

6. General Symmetric Walls

We now need no longer rely on the determinant approach (3.1) to define the number-wall, but may generate it instead by placing an arbitrary pair of sequences $[T_n], [S_n]$ on rows $m = -1, 0$ — subject to zero-windows (3.8), and supplemented where necessary by consistent frame data around such windows — then employing frame recursion (5.1) for $m > 0$, and by reflection for $m < -1$. The unexpected square-tiling symmetry of the new definition is noteworthy: Since neither m nor n appears explicitly, we have invariance under 2-D translations; furthermore, despite an apparent asymmetry of (3.1) between m and n, (4.1) – (4.3) are invariant under reflection in diagonals of the window, and under half-turn about its centre. [This last is rather less mysterious when viewed in the context of Padé tables §11, where it arises directly from the fact that the reciprocal transpose of the Padé table for $F(X)$ is the table for $1/F(X)$.] To distinguish the new wall from the *special number wall* (SNW) of (3.1) etc, we refer to it as a *general symmetric wall* (GSW). [It must be admitted that at the moment this construction, as was memorably observed of an entirely different subject, fills a much-needed gap.]

The elements of a GSW are plainly rational functions in the elements from which they are generated; and it seems reasonable to suppose that they should possess some explicit characterization, analogous to (3.1) defining the SNW. Such an expression would undoubtedly be immediately useful (see below), but at present we have in lieu only the following partial result, initially communicated to us by Jim Propp as a corollary of a more general combinatorial expression in **Rob86**.

> **Theorem:** For $m \geq 1$, the general element $S_{m,n}$ of a GSW constructed (via (3.7)) from sequences of variables $S_{-1,n} = U_n$ and $S_{0,n} = V_n$ is of the form $S_{m,n} \ = \ W_{m,n}/Z_{m,n}$, where $W_{m,n}$ is an irreducible polynomial of total degree (at most) $2(m^2 - m + 1)$ in the assorted variables, and $Z_{m,n}$ is (a factor of) the degree $m^2 + (m-1)^2$ monomial
>
> $$Z_{m,n} \ = \ \prod_{k=1-m}^{k=m-1} U_{n+k}{}^{m-|k|} V_{n+k}{}^{m-1-|k|}. \tag{6.1}$$

For $m < 0$, immediately by symmetry

$$S_{m,n}(\ldots, U_k, \ldots, V_k, \ldots) \ = \ S_{-1-m,n}(\ldots, V_k, \ldots, U_k, \ldots).$$

Proof: Notice that in the setting of a GSW, both m and n subscripts may be arbitrarily translated; so without loss of generality, we may represent an arbitrary element $S_{m,n}$ by $S_{4,4}$. By (3.6),

$$S_{44} \ = \ (S_{34}^2 - S_{33}S_{35})/S_{24}. \tag{6.2}$$

Also, substituting for the $S_{3,j}$,

$$S_{44} \ = \ \big((S_{24}^2 - S_{23}S_{25})^2/S_{14}^2 - (S_{23}^2 - S_{22}S_{24})(S_{25}^2 - S_{24}S_{26})/S_{13}S_{15}\big)/S_{24}.$$

Most of the terms in the numerator of the right-hand side above have a factor S_{24}, the exceptions simplifying to

$$-S_{23}S_{25}^2(S_{14}^2 - S_{13}S_{15})/S_{13}S_{14}^2S_{15}S_{24} \ = \ -S_{04}S_{23}S_{25}^2S_{24}/S_{13}S_{14}^2S_{15}S_{24}$$

using (3.6); so S_{24} cancels completely from the denominator, giving

$$S_{44} \ = \ \frac{S_{13}S_{15}S_{24}^3 - 2S_{13}S_{15}S_{23}S_{24}S_{25} - S_{14}^2S_{22}S_{24}S_{26} + S_{14}^2S_{23}^2S_{26} + S_{14}^2S_{22}S_{25}^2 - S_{04}S_{23}^2S_{25}^2}{S_{13}S_{14}^2S_{15}}. \tag{6.3}$$

We proceed by induction on m: elementary computation as above establishes (6.1) for $m = 1, 2$. For $m > 2$, translating (6.2) and (6.3) from $S_{4,4}$ to $S_{m,n}$, we see $S_{m,n}$ must be of the form (6.1), possibly divided by some factor of the HCF of $W_{m-2,n}$ and $W_{m-3,n}^2 W_{m-3,n-1} W_{m-3,n+1}$. However, we show below that $W_{i,j}$

is an irreducible polynomial in the U_k and V_k, so this HCF is unity, and $S_{m,n}$ is also of the form (6.1) as required.

To establish the irreducibility of $W_{m,n}$, we consider first the special number wall of a transcendental sequence $[V_k]$, i.e. $U_k = 1$ for all k. Notice that any factor of a homogeneous polynomial must also be homogeneous, since the product of two polynomials with minimum total degree a, c and maximum b, d resp. necessarily contains terms of degrees $a + c$ and $b + d$. Fixing say $n = m$, by (3.1)

$$S_{m,m} = \begin{vmatrix} V_m & \dots & V_{2m} \\ \vdots & \ddots & \vdots \\ V_0 & \dots & V_m \end{vmatrix}.$$

V_{2m} has cofactor $S_{m-1,m-1}$, which by assumption is irreducible. So if $S_{m,m}$ factorizes properly, it has a linear factor containing V_{2m}; and the other factor must equal $S_{m-1,m-1}$, which does not contain ${V_m}^m$. So their product does not contain ${V_m}^{m+1}$, and cannot be $S_{m,m}$: thus in the special number wall of a sequence of distinct transcendentals, $S_{m,m}$ and by translation $S_{m,n}$ is an irreducible polynomial.

Now consider the GSW. If $W_{m,n}$ factorizes properly, it has a factor containing no V_k elements (otherwise we could specialize to a factorization for the special wall above). By an easy induction using (3.6), $W_{m,n}$ contains just one term which is a multiple of ${V_n}^{m+1}$: specifically, $Z_{m,n}{V_n}^{m+1}/U_n^m$. So any factor can only be a monomial which (partially) cancels with the denominator as given above, and what remains of the numerator is irreducible. ■

A more refined induction ought to show that not even monomial cancellation can occur above; hence that the polynomial degrees and the form of $Z_{m,n}$ given in (6.1) are exact, and indeed that the total degree of $W_{m,n}$ in the U_k, V_k separately is uniformly $m(m-1)$, $m(m-1)+2$ resp. Moreover we conjecture that the sum of the absolute values of the coefficients of $W_{m,n}$ is $2^{m(m+1)/2}$. This last quantity — essentially the number of terms in the m-th row of a polynomial GSW — is uncomfortably large: for example, $W_{4,n}$ is a polynomial of about $30,000$ terms, each of degree 26.

A referee has made the point that we have inadvertently introduced not one but two generalizations here. Given sequences $[T_n], [S_n]$ over the ground domain, firstly we generate the 'numerical' GSW $S_{m,n}$ via recursion (5.1); secondly we substitute them for $[U_n], [V_n]$ in the formal GSW (6.1). [It is assumed both $[T_n], [S_n]$ everywhere nonzero, ensuring both that (3.8) holds initially — without which no (5.1)) — and that the denominators $Z_{m,n}$ are nonzero in (6.1).] Now, are the two walls equal? If we had an explicit expression for the GSW element, we might consider adapting the Frame Theorem proof to incorporate it. Failing that, we can at least observe that they are surely equal if either wall is everywhere nonzero, since algorithms (3.7) and (5.1) are then equivalent; and again, they are equal if $[T_n], [S_n]$ happen to be a pair of adjacent rows (or indeed columns) from some pukka SNW, by the existing Frame Theorem.

Now any given GSW element depends on only a finite subset of $[T_n], [S_n]$. We might therefore seek to show that every finite region of the GSW may be embedded in some SNW, generated by some sequence $[R_n]$ say (dependent on the region). [The region may be taken to be a (square) diamond, with base on the row $[T_n]$ and apices at some target element and its reflection in the base]. In specific instances, this embedding is straightforward to verify: the equations for $[R_n]$ turn out to be linear in $[T_n], [S_n]$, and it appears sufficient to consider $[R_n]$ of period at most thrice the diameter. However, a general proof is complicated by the fact that any fixed scheme of equations may be rendered singular by some zero within the region, in spite of the fact that in practice such zero-windows make a specific problem easier to solve.

We turn to another question posed by Propp, the statement and solution of which exemplify the geometric nature of the number wall. It concerns the extent to which the frame rules might be in some covert fashion *local*, in the sense that the value of an element is independent on those outside some bounded neighborhood. Specifically he asks: given arbitrarily large k, do there exist two distinct walls with k (or more, but only finitely many) consecutive rows in common? Such questions as what ground domain is specified, whether horizontal and/or vertical translations are to be regarded as differences in this context, and whether the wall is special, can be postponed; we shall see that the answer turns out to satisfy the most stringent of such conditions.

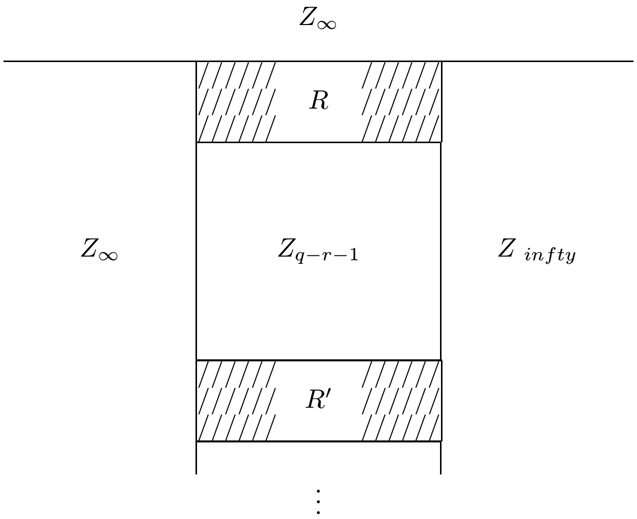
Consider an arbitrary relation J of order r with leading and trailing coefficients equal to unity, with $[S_n]$ satisfying $S_1 = \ldots = S_{r-1} = 0$ and $S_r = 1$ (the so-called *impulse response sequence* or IRS), and having period q; then define

$$T_n \;=\; \begin{cases} S_n & \text{if } r \leq n \leq q; \\ 0 & \text{otherwise.} \end{cases}$$

Then the wall for T is easily seen to be of form diagrammed, where Z_g denotes a $g \times g$ window (with inner frame unity), R denotes the $(r+1) \times (q-r+1)$ rectangular region comprising one period of the wall for $[S_n]$ but excluding its initial Z_{r-1}, and R' denotes the reflection of R about a horizontal line. Now replace the original relation J by any other relation satisfying the same restrictions: all rows meeting the interior of R or R' will in general be altered, whereas those meeting the finite windows must remain the same. So the wall generated satisfies Propp's conditions with $k = q - r + 1$.

Incidentally, there is a sense in which the 'real' wall here is actually just the finite rectangle R; we make this manifest by repositioning the inner frames of the infinite windows, so that there are instead four half-infinite frames spiraling away in the same sense (as in the next example) from the corners of R, which is now isolated at the centre. The result is easily verified to be a GSW.

Diagram Generalized Wall



[For the remainder of this section we assume the ground domain is binary.] The simplest examples of these GSW's occur when R is itself a single $g \times g$ window, surrounded by four infinite windows. This is the special case $h = \infty$ of what one might call a 'bathroom wall': an offset tiling of windows of sizes $g+1$ and $h+1$ (note the increase in size resulting from the frame), where $0 \leq g < h \leq \infty$. Another important example, the case $g = 0, h = 1$ is the unique binary wall with minimum density (1/5) of zeros; it consists of the pattern below, replicated on a tiling of squares.

```
0 1 1 1 1
1 1 0 1 1
1 1 1 1 0
1 0 1 1 1
1 1 1 0 1
```

Finally, an entertaining problem is suggested by the observation that there are binary GSW's with isolated rectangular regions, and also with isolated square windows: are there any with nontrivial isolated squares, i.e. possessing some interior structure? The answer is a little surprising: there is essentially just one, as follows. The relation

$$J \;=\; (\mathbf{E}+1)(\mathbf{E}^3+\mathbf{E}+1)^2 \;=\; \mathbf{E}^7+\mathbf{E}^6+\mathbf{E}^3+\mathbf{E}^2+\mathbf{E}+1,$$

has IRS period comprising a block of $r-1$ zeros followed by the coefficients of J itself (because $J(X)J(1/X) = X^r + X^{-r}$):

$$S_n \;=\; [\ldots,0,0,0,0,0,0,1,1,1,1,0,0,1,1,\ldots],$$

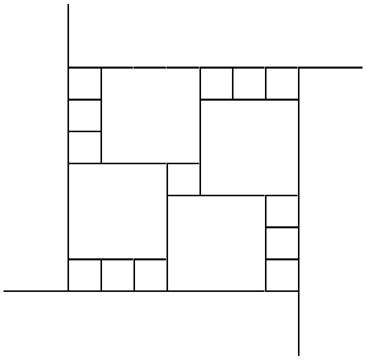
and $r = 7, q = 14$ in the earlier notation. The wall (illustrated below) of the modified sequence

$$T_n \;=\; [...,0,0,0,0,0,0,1,1,1,1,0,0,1,1,0,0,0,0,0,0,...],$$

manipulated as above, is essentially an isolated 8x8 square R which is not a 6×6 window; it has four symmetries generated by quarter-turns, and the only other solution is its reflection R'.

Diagram Isolated Square Wall

```
0 0 1 0 0 0 0 0 0 0 0 0
0 0 1 0 0 0 0 0 0 0 0 0
0 0 1 1 1 1 1 1 1 1 1 1
0 0 1 1 0 0 1 1 1 1 0 0
0 0 1 1 0 0 1 0 0 1 0 0
0 0 1 1 1 1 1 0 0 1 0 0
0 0 1 0 0 1 1 1 1 1 0 0
0 0 1 0 0 1 0 0 1 1 0 0
0 0 1 1 1 1 0 0 1 1 0 0
1 1 1 1 1 1 1 1 1 1 0 0
0 0 0 0 0 0 0 0 0 1 0 0
0 0 0 0 0 0 0 0 0 1 0 0
```



The uniqueness is a matter of constructing all binary polynomials with period twice their order, a straightforward exercise in finite field theory. As the diagram suggests, it can be regarded geometrically as a question of packing a square with smaller squares, with side-conditions equivalent to (5.5), which does not look too easy combinatorially!

7. Performance and the FSSP

For a number-wall of length and depth N, the complexity of a straightforward implementation of the number-wall algorithm as described above is easily seen to be of order N^2 space and N^3 time (assuming arithmetic operations to be of constant complexity); an extra factor of N arises in both requirements from the necessity to locate the frame of the current zero-window, which may itself be of size N. [The time could be improved simply by storing the origin and size of the window above for each element of the current row, at the cost of storing three rows of integers.]

It is possible to reduce the complexity to order N space and N^2 time, at least in the binary case, by 'hard-wiring' the algorithm as a *Cellular Finite-State Automaton* (C-A; see **Min67**). Briefly, the C-A stores the current row m of the wall, each cell n holding the value of a single binary determinant $S_{m,n}$ (in practice, two copies of the array are required, for old and new values of the state). The state is a 44-valued product comprising 2 bits for left and right-shifting buffers for the outer frames of the current zero-window, and 11 states for a slightly modified Firing-Squad Synchronization Problem machine (FSSP; see **Maz86**) to locate the South edge of the inner frame.

[It would take us too far afield to go into detail about the FSSP. Briefly, imagine a squad of identical soldiers, each equipped with his own gun and with a (synchronized) clock marking instants of time; between instants a soldier assumes any one of an initially determined set of states. At each instant the state of a soldier changes to a new value, completely determined by his own previous state and those of his two nearest neighbors. There are g soldiers in the line, but none of them knows the value of g. Initially, the whole squad is *Quiescent*; but at some random instant the leftmost soldier assumes the *Command* state. The problem is to train the squad identically so that at some instant ($2g-1$ after the command is in general the minimum achievable) they will all for the first time simultaneously assume the *Firing* state.]

In the notation of the Frame Theorems (§4 figure), each cell picks up E from the North of the window, then shifts it rightward until it hits the East frame, where G is added in, after which $E+G$ is sent leftward. In the meantime F from the West is shifted rightward until the two collide on the South frame, where they are added to give H. The FSSP is started by commands in both North corners of the window simultaneously, so that it fires after g steps rather than $2g$; sadly, this means we cannot employ Mazoyer's beautiful asymmetric 6-state solution **Maz87**, although we could use Balzer's symmetric 8-state solution to reduce the state total to 40. The transition table for the binary C-A is only 85 Kbyte, and it is quite stunningly fast: a single 3-D array lookup for each determinant computed. Because of the localization of the data, on a massively parallel machine the complexity improves to order N time and space.

The C-A method can in principle be generalized to ground field $\mathbf{Z}_p$, but implementation seems to demand on the order of p^5 states, so is unlikely to be feasible for $p > 3$. A more practical approach is to retain the FSSP synchronization and the technique of shifting frame values right or left till they bounce off the frame of the window, but abandon any attempt to do arithmetic in the control structure: the values of the frame elements are simply shifted separately, each inner or outer edge having its own row of shifting buffers (A, E need two each, but their rightward buffers can be shared with B, F). The arithmetic for the South frame is all performed explicitly when the FSSP fires. This requires around ten one-dimensional arrays to implement, and retains the order N space and N^2 time complexity of the C-A, as well as its potential for parallelization.

The Frame algorithm (5.1), including the binary C-A variant, has been implemented in C-language as part of a sophisticated application program running on a Sun SPARC workstation, incorporating a graphical front-end allowing large segments (up to one million elements) of a number-wall to be viewed in color-coding. At a more modest level, there is available a pedagogic Maple implementation of most of the algorithms described here, designed for the examples shown here.

8. Interpolation and Vandermonde Matrices

In the next three sections we turn to a distinct but closely related problem, which receives surprisingly little attention in standard texts: the efficient computation of the explicit form of S_n for an LFSR sequence $[S_n]$ from its relation and/or from (a sufficiency of) its terms. The first two sections summarize and dilate upon standard material required for the third.

We denote by $\sigma_i(X_1, \dots, X_r)$ the elementary symmetric function of degree i on r variables X_i, and recall the well-known

Lemma: The polynomial equation with roots $X = X_1, \dots, X_r$

$$J(X) \;=\; \prod_k (X - X_k) \;=\; \sum_i J_i X^i \tag{8.1}$$

has coefficients given by $J_i = (-)^{r-i}\sigma_{r-i}((X_1, \dots, X_r))$.

For development and analysis of algorithmic efficiency, we need to make the point that all the 'defective' symmetric functions $\sigma_i(\dots, X_{\neq k}, \dots)$ — that is, on $r-1$ variables excluding X_k — can be computed efficiently in order r^2 time by first employing and then reversing the usual inductive algorithm:

Algorithm: Initially for $i = 0$, $k = 0, 1, \dots, r$ set $\sigma_0(X_1, \dots, X_k) = 1$;
for $k = 0$, $i = 1, \dots, r$ set $\sigma_i() = 0$;
for $k = 1, 2, \dots, r$ set

$$\begin{aligned} \sigma_0(X_1, \dots, X_k) &= 1, \\ \sigma_{i+1}(X_1, \dots, X_k) &= \sigma_{i+1}(X_1, \dots, X_{k-1}) + X_k \sigma_i(X_1, \dots, X_{k-1}); \end{aligned} \tag{8.2}$$

then for $k = 1, 2, \dots, r$ set

$$\begin{aligned} \sigma_0(\dots, X_{\neq k}, \dots) &= 1, \\ \sigma_{i+1}(\dots, X_{\neq k}, \dots) &= \sigma_{i+1}(X_1, \dots, X_r) - X_k \sigma_i(\dots, X_{\neq k}, \dots). \end{aligned}$$

From now on we shall assume that the $[X_i]$ are *distinct*, that is either they are transcendental or $X_i \neq X_j$ for $1 \leq (i,j) \leq r$. We require some properties of the (fairly) well-known *Vandermonde* matrix M, defined by

Definition:

$$M_{ij} \;=\; (X_j)^i. \tag{8.3}$$

Its determinant is given by

Theorem:

$$|M_{ij}| \;=\; \prod_k \prod_{l<k} (X_k - X_l), \tag{8.4}$$

and its matrix inverse by $N \cdot M = I$ where

Theorem:

$$N_{ji} \;=\; \frac{(-)^{i-1}\sigma_{r-i}(\ldots, X_{\neq j}, \ldots)}{\prod_{k\neq j}(X_k - X_j)}. \tag{8.5}$$

Proof: As any undergraduate used to know, by subtracting column l from k, the determinant divides by $(X_k - X_l)$; and by inspecting the diagonal term, the remaining constant factor is unity. The inverse (hinted at darkly in **Knu81** §1.2.3 Ex. 40 and in **Ait62** §49) is more or less immediate by (8.1) with X_j replacing X and omitted from the roots:

$$\begin{aligned}
(N \cdot M)_{ij} &= \sum_k N_{ik} M_{kj} \\
&= \frac{\sum_k (-)^{i-1}\sigma_{r-k}(\ldots, X_{\neq i}, \ldots)(X_j)^k}{\prod_{k\neq j}(X_k - X_j)} \\
&= \prod_{k\neq i}(X_k - X_j) / \prod_{k\neq j}(X_k - X_j) \;=\; I_{ij}
\end{aligned}$$

where I_{ij} denotes the Kronecker delta. [The commutation $M \cdot N = I$ is considerably less obvious!] ■

By (8.5) we can explicitly solve the simultaneous linear equations $K \cdot M = S$ arising in fitting a linear combination of given exponentials, since $K = S \cdot N$:

Corollary:

$$S_i \;=\; \sum_j K_j {X_j}^i$$

if and only if

$$K_j \;=\; \frac{\sum_i S_i (-)^i \sigma_{r-i-1}(\ldots, X_{\neq j}, \ldots)}{\prod_{k\neq j}(X_k - X_j)}. \tag{8.6}$$

Returning to our illustration, suppose we have established as in §2 or §3 that $S \;=\; [0,0,0,1,\ldots]$ is an LFSR sequence with relation which turns out to factor as $J(\mathbf{E}) \;=\; (\mathbf{E}-7)(\mathbf{E}-5)(\mathbf{E}-3)(\mathbf{E}-1)$; so its roots are $[X_1, X_2, X_3, X_4] \;=\; [7,5,3,1]$ and the difference products $[(X_2 - X_1)(X_3 - X_1)(X_4 - X_1), \ldots] \;=\; [-48, +16, -16, +48]$. Computing the elementary and defective symmetric functions via (8.2) gives

$i \backslash k$	0	1	2	3	4
0	1	1	1	1	1
1	0	7	12	15	16
2	0	0	35	71	86
3	0	0	0	105	176
4	0	0	0	0	105

$i \backslash k$	1	2	3	4
0	1	1	1	1
1	9	11	13	15 .
2	23	31	47	71
3	15	21	35	105

Substituting all these into (8.6) gives $[K_1, K_2, K_3, K_4] \;=\; [+1, -3, +3, -1]/48$, whence the explicit form is

$$S_n \;=\; (1 \cdot 7^n - 3 \cdot 5^n + 3 \cdot 3^n - 1 \cdot 1^n)/48.$$

Finally, a surprising application of the Vandermonde determinant gives a formula for the number-wall of an LFSR sequence:

> **Theorem:** If $S_n = \sum_i K_i {X_i}^n$, then in its number-wall $S_{m,n} = \sum_j B_j {Y_j}^{n-m}$, where $Y_j = \prod_k X_k$ is the product of any $m+1$ of the X_i, and
>
> $$B_j \;=\; \prod_k K_k \cdot \prod_k \prod_{l \neq k} (X_k - X_l). \tag{8.7}$$
>
> Here j indexes subsets of size $m+1$ from $\{1, \ldots, r\}$, the indices k, l being restricted to this j-th subset.

Proof: Express the $m = r-1$ case as product of two Vandermonde determinants:

$$S_{m,n} \;=\; |S_{n+i-j}| \;=\; \big|\sum_k K_k {X_k}^{n+i-j}\big| = |K_j {X_j}^i| \;\cdot\; |{X_i}^{n-j}|.$$

For $0 \le m \le r-1$ every term of the expanded determinant defines a unique subset of $m+1$ from r; collecting together all the terms with the same subset, we see that we must sum the VDM product over all such subsets. [This is best worked through on a small example: the sign of the result requires care.] ■

We shall later require an explicit formula for the number-wall for the binomial coefficients along the diagonals of the Pascal triangle, discussed in greater depth in the next section (9.4):

> **Theorem:** The number-wall for $S_n = \binom{n}{r-1}$ is given by

$$S_{m,n} \;=\; \begin{cases} \displaystyle\prod_{k=0}^{k=m} \binom{n-k}{r-1-m} \Big/ \binom{r-1-m+k}{r-1-m} & \text{if } -1 \le m \le r-1, \\ 0 & \text{otherwise.} \end{cases} \tag{8.8}$$

Proof: Assume for the moment that $S_{m,n}$ is *defined* by the above expression. Evidently $S_{-1,n} = 1$ and $S_{0,n} = \binom{n}{r-1}$ as required. If we ignore the sole $r-2 \;\times\; r-2$ zero-window at the origin (which turns out to give no trouble), we need only show that (3.6) is satisfied to clinch the result.

For $-1 \le m \le r-1$ the expression may be recast, more explicitly if less elegantly, as

$$S_{m,n} \;=\; \prod_{k=0}^{k=r-1} \left(\frac{n-k}{k+1}\right)^{\min(k+1,\; r-1-k,\; m+1,\; r-1-m)}.$$

By somewhat tedious comparison of the k-th exponents in pairs of elements of this form, it can be shown that, for $0 \le m < r/2 - 1$ at least,

$$\begin{aligned} S_{m-1,n}/S_{m,n} \;&=\; (r-1-m) \ldots (m+1)/(n-m)...(n-r+m+2), \\ S_{m+1,n}/S_{m,n} \;&=\; (n-m-1) \ldots (n-r+m+3)/(r-2-m)...(m+2), \\ S_{m,n-1}/S_{m,n} \;&=\; (n-r+m+1) \ldots (n-r+1)/(n)...(n-r), \\ S_{m,n+1}/S_{m,n} \;&=\; (n+1) \ldots (n-r+1)/(n-r+m+2)...(n-r+2); \end{aligned}$$

whence easily

$$\begin{aligned} S_{m-1,n} S_{m+1,n}/S^2_{m,n} \;&=\; (m+1)(r-m-1)/(n-m)(n-r+m+2), \\ S_{m,n-1} S_{m,n+1}/S^2_{m,n} \;&=\; (n-r+1)(n+1)/(n-m)(n-r+m+2); \end{aligned}$$

so

$$(S_{m-1,n}S_{m+1,n} \ + \ S_{m,n-1}S_{m,n+1})/S_{m,n}^2 \ = \ 1,$$

and (3.6) is satisfied.

For $r/2 - 1 \leq m < r$, notice that the recast expression is symmetric under $m \to r-2-m$; therefore the entire wall is symmetric about its horizontal midline, and (3.6), also symmetric, is satisfied here too. ■

We are (almost) in a position to characterize the rows of an LFSR wall:

Corollary: If $[S_n]$ is an LFSR sequence of order r, then for each m $[S_{m,n}]$ is an LFSR sequence of order at least $\max(0, 1+(m+1)(r-1-m))$ and at most $\binom{r}{m+1}$. (8.9)

Proof: the upper bound results from assuming all the Y_j distinct in (8.7), and applying (2.2) conversely; the lower bound from assuming that the Y_j coincide (say with unity), then observing that (3.10) in the nonzero region is the product of $m+1$ polynomials of degree $r-1-m$ in n; by expanding the Toeplitz determinant, the addition of lower-degree terms to $K(n)$ and the geometric factor $Y^n = X^{mn}$ make no difference to the order.

Any coincidence between two Y_j corresponding to distinct choices of X_i in (8.7) serves merely to reduce the order of the row by the smaller of their contributions. The general case of multiple roots X_i in the relation itself is more involved: it would divert us too far to attempt to analyse it here, and we content ourselves with a plausible assertion: the order of any row of the wall of an LFSR sequence, satisfying a given relation with possibly multiple roots, cannot increase if the relation is massaged so as to cause coincidences additional to those already present. ■

The computation of the actual relation satisfied by a given row of the wall generated by a given relation is an interesting exercise in symmetric functions, which again shall not detain us here.

9. Difference Tables

Extrapolation of a sequence is a common requirement, arising in numerical computation, recreational problems, critical-point estimation and cryptographic contexts. The familiar *Difference Table*, see for example **Fro85** §14, is defined by the recursion

Definition:

$$\begin{aligned} T_{0,n} \ &= \ S_n; \\ T_{m,n} \ &= \ (\mathbf{E}-1)^m S_n \ = \ \boldsymbol{\Delta}^m S_n \ = \ T_{m-1,n+1} \ - \ T_{m-1,n} \quad \text{for } m > 0; \end{aligned} \tag{9.1}$$

it has the property that $T_{m,n}$ vanishes for all $m > r$ just when S_n equals a polynomial in n of degree r. By extending the region of zeros with n then reversing the direction of the recursion with m, we can efficiently extrapolate such a sequence to greater n. Further, the explicit form of the polynomial may be recovered via Newton's forward difference formula, subject to the caveat below:

Theorem: If the polynomial sequence $[S_n]$ has difference table $[T_{i,j}]$ then

$$S_n \ = \ \sum_i T_{i,0}\binom{n}{i}. \tag{9.2}$$

Similarly if $[S_n]$ is LFSR of order r, then by (3.3) its wall vanishes for $m > r$. Since by (2.2) a polynomial sequence of degree r is a (special case of a) LFSR sequence of degree $r+1$, the same use may be made of the number-wall to give a generalized extrapolation algorithm, albeit requiring an extra term and a rather more complicated computation of the explicit form. This application is described in an elementary fashion in **Slo95** §1 and **Con96** §3, employing an ingenious notation unhappily compromised by a clutch of demoralizing misprints.

A difficulty with interpreting (2.2) for finite ground characteristic p is that the Little Fermat Theorem $n^p = n \pmod p$ effectively prevents the degree of 'naïve' polynomials based on powers n^j from exceeding $p-1$. A straightforward solution to the difficulty is suggested by (9.2): to base our polynomials on binomial coefficients $\binom{n}{j}$ instead. This falls over in a similar fashion if we attempt the usual

Definition:

$$\binom{n}{j} \;=\; \prod_{0\le i<j} (n-i)/(i+1). \tag{9.3}$$

But as it happens, the computation of binomial coefficients for characteristic p is the stuff of numerous recreational articles and student projects. Write $l = p^k$. Decomposing the difference table for $\binom{n}{l-1}$ (which is just the IRS of $\mathbf{E}^l - 1$) into p^2 blocks of edge l/p, observing that each block is a multiple of the table for $\binom{n}{p^{l/p}-1}$, and that the blocks themselves satisfy the Pascal triangle recursion (2.3), by induction on k we get the pretty result (ascribed to Lucas in the survey article **Gra96**):

Theorem:

$$\binom{n}{m} \;\equiv\; \begin{cases} \prod_i \binom{n_i}{m_i} \pmod p & \text{if } n \ge 0,\ m \ge 0, \\ (-)^{-n+m-1}\binom{-n+m-1}{m} & \text{if } n < 0,\ m \ge 0, \\ 0 & \text{if } m < 0, \end{cases} \tag{9.4}$$

where n_i and m_i denote the digits of n and m written to base p; the later parts of the right-hand side are elementary.

This costs order $\log n$ time; the terms on the right-hand side can be computed easily via (2.3) as a table of p^2 entries. It also demonstrates that the binomial coefficient is mathematically defined within the domain, allowing us to apply all the usual machinery of difference calculus within the domain as well. A simple illustration of the situation is $[S_n] = [0,0,0,1,0,0,0,1,\ldots]$ for $n = 0,1,2,\ldots$, with relation $S_{n+4} - S_n = 0$ whose quadruple root over the binary domain is $X = 1$. By LFT, no naïve binary polynomial can have period > 2; but as required

$$[\binom{n}{3}] \;=\; [0,0,0,1,4,10,20,35,...] \;\equiv\; [S_n] \pmod 2$$

Sequences with period a power of the characteristic have a useful property:

Lemma: If $[S_n]$ has period $l = p^k$ then

$$(\mathbf{E}^l - 1)[S_n] \;=\; (\mathbf{E} - 1)^l [S_n] \;=\; [O_n], \tag{9.6}$$

since $\binom{l}{j} = 0$ except when $j = 0, l$, using (9.4). So by (2.2), S_n is a polynomial (in the binomial sense) of degree r, where $l/p < r \le l$ (unless the period is l/p or smaller). By (9.1), we can employ a difference table rather than a number wall to compute its order. Moreover, by (9.6) in reverse, we can difference p^i times in the same time as differencing once: so initially setting $i = k$ and progressively reducing i as the period of the current row m decreases, we can compute the order in kp rows instead of l, giving about order lp time.

We illustrate the method with a Maple program:

Algorithm:

```
orderSpk := proc (S, p, k)
local T, dT, m, j, l;
l := p^k; m := 0; T := S;
while l > 1 do
dT := [seq((T[j+l/p mod l +1] - T[j+1]) mod p, j = 0..l-1)];
if sum(dT[j+1], j = 0..l-1) = 0
then l := l/p else m := m + l/p; T := dT fi od;
m + min(1, T[1]) end;
```

(9.7)

An application of the preceding theory occurs in the study of deBruijn sequences, which are defined traditionally over a finite set of size q as k-distributed (every k-tuple occurring with the same frequency), and having minimum period q^k. In the case where the set is actually a finite field, the extra structure allows us to define and compute the order of the sequence *qua* LFSR sequence over that domain; now the method outline above can be employed to substantially reduce the time (by the traditional factor of $l/\log l$). In an investigation such as **Bla96**, **Cha82** where the computation of the order is the inner loop of a lengthy combinatorial search, such a reduction is crucial. [In fact **Bla96** employed a more involved formulation of polynomials, basing the computation of the order on a modified Fast Fourier Transform.]

As a numerical example, we compute the order of the deBruijn sequence with $q = p = 2$, $k = 5$ and order $r = 21$ over $\mathbf{F}_2$ (but 25 over $\mathbf{Z}$). [It is essentially unique, modulo reflection and (independent) complementation of the first or last half.] T denotes the current m-th difference of S, l the currently detected period; when the l/p-th difference of T would be zero, the period is reduced instead.

l	m	$dT = 0?$	T
32	0	N	11111001000001010011101011000110
32	16	Y	11000011110000111100001111000011
16	16	Y	1100001111000011
8	16	N	1100001111000011
8	20	Y	11111111
4	20	Y	1111
2	20	Y	11
1	20	N	1
0	21		

For the deBruijn sequence with $q = p = 2$, $k = 4$ at the end of §6, we find from the full difference table (not shown) that $T_{i,0} = 1$ only for $i = 0, 4, 10, 11$; therefore an explicit ‘binomial’ expression for the n-th term is

$$S_n \;=\; 1 + \binom{n}{4} + \binom{n}{10} + \binom{n}{11}.$$

Finally, we touch on a rather curious interaction between difference tables and number walls, which comes to light when we try to establish exactly what effect a simple transformation of the sequence has on its wall. For instance, a little thought suggests that term-by-term addition of a low-order LFSR sequence to $[S_n]$ will only have a (literally) marginal effect on any large windows, causing their frames to shift by at most the order added. However, our only explicit progress in this direction is the

Theorem: The wall for $1 + S_n$ is just the wall for S_n itself added to the wall for $-\boldsymbol{\Delta}^2 S_{n-1}$ shifted down by one row. That is,

$$\text{Let } R_n \;=\; 1 + S_n, \quad T_n \;=\; -S_{n+1} + 2.S_n - S_{n-1}; \quad \text{then } R_{m,n} = S_{m,n} + T_{m-1,n} \tag{9.8}$$

Proof: Rather than attempt a formal but notationally impenetrable proof for the general case, we illustrate it by the case $m = n = 3$. Starting from the determinant definition (3.1), $R_{33} \;=$

$$\begin{vmatrix} 1+S_3 & 1+S_4 & 1+S_5 & 1+S_6 \\ 1+S_2 & 1+S_3 & 1+S_4 & 1+S_5 \\ 1+S_1 & 1+S_2 & 1+S_3 & 1+S_4 \\ 1+S_0 & 1+S_1 & 1+S_2 & 1+S_3 \end{vmatrix};$$

expanding each by column in turn, and noticing that any determinant with two or more equal columns of ones must be zero, this becomes

$$S_{33} + \begin{vmatrix} 1 & 1+S_4 & 1+S_5 & 1+S_6 \\ 1 & 1+S_3 & 1+S_4 & 1+S_5 \\ 1 & 1+S_2 & 1+S_3 & 1+S_4 \\ 1 & 1+S_1 & 1+S_2 & 1+S_3 \end{vmatrix} + \begin{vmatrix} 1+S_3 & 1 & 1+S_5 & 1+S_6 \\ 1+S_2 & 1 & 1+S_4 & 1+S_5 \\ 1+S_1 & 1 & 1+S_3 & 1+S_4 \\ 1+S_0 & 1 & 1+S_2 & 1+S_3 \end{vmatrix} + \ldots + \begin{vmatrix} 1+S_3 & 1+S_4 & 1+S_5 & 1 \\ 1+S_2 & 1+S_3 & 1+S_4 & 1 \\ 1+S_1 & 1+S_2 & 1+S_3 & 1 \\ 1+S_0 & 1+S_1 & 1+S_2 & 1 \end{vmatrix};$$

then subtracting row $i+1$ from row i for $i = 1, \ldots, m$ and pivoting on the bottom one for each determinant,

$$S_{33} \;-\; \begin{vmatrix} \mathbf{\Delta}S_3 & \mathbf{\Delta}S_4 & \mathbf{\Delta}S_5 \\ \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}S_1 & \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 \end{vmatrix} + \begin{vmatrix} \mathbf{\Delta}S_2 & \mathbf{\Delta}S_4 & \mathbf{\Delta}S_5 \\ \mathbf{\Delta}S_1 & \mathbf{\Delta}S_3 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}S_0 & \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 \end{vmatrix} - \begin{vmatrix} \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 & \mathbf{\Delta}S_5 \\ \mathbf{\Delta}S_1 & \mathbf{\Delta}S_2 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}S_0 & \mathbf{\Delta}S_1 & \mathbf{\Delta}S_3 \end{vmatrix} + \begin{vmatrix} \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}S_1 & \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 \\ \mathbf{\Delta}S_0 & \mathbf{\Delta}S_1 & \mathbf{\Delta}S_2 \end{vmatrix}.$$

The first two determinants have identical columns except the leftmost, say $[F_i]$ in the first and $[G_i]$ in the second; we contract them into a single determinant, with first column $[F_i - G_i]$. Each remaining determinant contains both columns; we subtract $[F_i]$ from $[G_i]$ and change the sign, giving

$$S_{33} \;-\; \begin{vmatrix} \mathbf{\Delta}^2S_2 & \mathbf{\Delta}S_4 & \mathbf{\Delta}S_5 \\ \mathbf{\Delta}^2S_1 & \mathbf{\Delta}S_3 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}^2S_0 & \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 \end{vmatrix} + \begin{vmatrix} \mathbf{\Delta}^2S_2 & \mathbf{\Delta}S_3 & \mathbf{\Delta}S_5 \\ \mathbf{\Delta}^2S_1 & \mathbf{\Delta}S_2 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}^2S_0 & \mathbf{\Delta}S_1 & \mathbf{\Delta}S_3 \end{vmatrix} - \begin{vmatrix} \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}^2S_1 & \mathbf{\Delta}S_2 & \mathbf{\Delta}S_3 \\ \mathbf{\Delta}^2S_0 & \mathbf{\Delta}S_1 & \mathbf{\Delta}S_2 \end{vmatrix}.$$

We are now in a similar situation, except that $[F_i]$ and $[G_i]$ are now the column two of the first two determinants. Repeating the previous operation,

$$S_{33} \;-\; \begin{vmatrix} \mathbf{\Delta}^2S_2 & \mathbf{\Delta}^2S_3 & \mathbf{\Delta}S_5 \\ \mathbf{\Delta}^2S_1 & \mathbf{\Delta}^2S_2 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}^2S_0 & \mathbf{\Delta}^2S_1 & \mathbf{\Delta}S_3 \end{vmatrix} + \begin{vmatrix} \mathbf{\Delta}^2S_2 & \mathbf{\Delta}^2S_3 & \mathbf{\Delta}S_4 \\ \mathbf{\Delta}^2S_1 & \mathbf{\Delta}^2S_2 & \mathbf{\Delta}S_3 \\ \mathbf{\Delta}^2S_0 & \mathbf{\Delta}^2S_1 & \mathbf{\Delta}S_2 \end{vmatrix}.$$

Finally after $m-2$ iterations, we are left with the required expression

$$S_{33} \;-\; \begin{vmatrix} \mathbf{\Delta}^2S_2 & \mathbf{\Delta}^2S_3 & \mathbf{\Delta}^2S_4 \\ \mathbf{\Delta}^2S_1 & \mathbf{\Delta}^2S_2 & \mathbf{\Delta}^2S_3 \\ \mathbf{\Delta}^2S_0 & \mathbf{\Delta}^2S_1 & \mathbf{\Delta}^2S_2 \end{vmatrix} = S_{33} \; + T_{23}. \blacksquare$$

Hence by (3.1) we easily get the wall for $R_n = A + B.S_n$: with S_n and T_n as in (9.8), $R_{m,n} = B^{m+1}S_{m,n} + A^{m+1}T_{m-1,n}$. Notice also that the wall for $R_n = C^nS_n$ is $R_{m,n} = C^{(m+1)n}S_{m,n}$.

10. Explicit Form of an LFSR Sequence

We shall briefly discuss efficient methods for computing the roots X_i and coefficients K_i in the explicit form (2.2) for S_n. From now on we mostly restrict ourselves to the integer domain $\mathbf{Z}$ embedded within the complex numbers $\mathbf{C}$; still, much of what we say is interpretable in a more general context of a continuous algebraic completion of the ground domain. ‘Combinatorial explosion’ (exponential numerical growth) is a constant hazard in integer algebraic computation, and it may sometimes be worth remembering a spectacular trick: where there is good reason to suppose that, for instance, the coefficients of the relation of a given sequence are going to be small, then the Berlekamp-Massey algorithm can perfectly well be applied modulo a smallish prime instead; or even modulo several very small primes and, the result being reconstructed by the Chinese Remainder Theorem as in **Dav88** §4.

In order to calculate the relation for a given sequence, or the explicit coefficients for given roots, it is possible to set up simultaneous linear equations and solve them in order r^3 time. This approach becomes cumbersome by hand for $r > 4$, whereas (by contrast) the coefficient equations are rapidly solvable explicitly. A more practical approach is to compute the relation polynomial $J(X)$ using Berlekamp-Massey (12.1), which costs order r^2 time; then extract its roots X_i formally, or more likely approximate them numerically using one of the various available methods surveyed for instance in **Hen74** §6.9. With the X_i to hand, assuming them to be distinct we can immediately apply (8.6) to find the K_i, again in order r^2 time.

We have avoided the general case of multiple roots in the present treatment; in this direction we currently have only partial results. In the first place, multiple roots of polynomials are numerically ill-conditioned, so that it’s quite likely that we never get to the point of trying to find the coefficients at all. If we do, and it happens that all the roots coincide, then S_n is a known exponential times a polynomial, and the latter is found by (9.2). For the general confluent case, the analogue of the Vandermonde determinant $|M|$ and the explicit form of $S_{m,n}$ can be evaluated; but the formal inversion of the matrix M looks rather gruesome, and will be postponed for the present.

An alternative approach bypasses the relation and Vandermonde inverse altogether, approximating roots and coefficients directly via quotients of number wall elements. The point here is that if $|X_1| > |X_2| > \ldots$, then for large n, $Y_1^n = (X_1 X_2 \ldots X_{m+1})^n$ dominates in (8.7). So it becomes possible to divide out unwanted factors from this term in the explicit representation, leaving only the desired quantities together with error terms which decrease exponentially with n — in fact, as $|X_m/X_{m+1}|^{-n}$. Of course, n can be made arbitrarily large simply by extrapolating from the bottom (zero) row of the number-wall upwards. In this way, we approximate first the $[X_i]$, then the $[K_i]$:

Corollary: If the roots X_i of the relation $J(\mathbf{E}) = 0$ for $[S_n]$ have distinct magnitudes (so are real), then

$$(S_{m,n+1}/S_{m-1,n+1})/(S_{m,n}/S_{m-1,n}) \to X_m \tag{10.1}$$

in order of magnitude descending as m increases.

Corollary: With X_i as above,

$$S_{m,n}/S_{m-1,n} \to L_m K_m {X_m}^n$$

where

$$L_m \;=\; \prod_{k<m} (1 - X_m/X_k)(1 - X_k/X_m) \tag{10.2}$$

depends only on m and the X_i.

Notice that the relative error in K_m is n times larger than that in X_m, because of the factor ${X_m}^n$; as a result, the direct method (8.6) gives more accurate results.

In the case of equal magnitudes, the ratios on the relevant rows fail to converge, but it is still possible to approximate the polynomial isolating the set of troublesome roots:

Corollary: With X_i as above, save for a pair of roots X_m, X_{m+1} of equal magnitude, these satisfy the approximate quadratic

$$(S_{m,n}/S_{m-1,n})X^2 \;-\; (S_{m,n+1}/S_{m-1,n+1})X \;+\; (S_{m,n+2}/S_{m-1,n+2}) \;=\; 0; \tag{10.3}$$

the extension to many roots should be obvious.

Finally, from the X_i the relation components J_i can be approximately recovered as elementary symmetric functions of the roots, via (8.1), (8.2).

Returning to our illustration, we extrapolate the sequence and its wall out to $n = 49$ by reversing algorithm (3.7) (assuming that any zeros have been left behind) using floating-point fixed-precision arithmetic, and apply (10.1), (10.2), (8.1), to get the following approximations:

m	0	1	2	3	4	
$S_{m-1,n-1}$	1	$.7646532757^{39}$	$.1940424956^{71}$	$.1965470321^{92}$	$.8985007667^{91}$	
$S_{m-1,n-2}$	1	$.5352573381^{40}$	$.6791487340^{72}$	$.2063743832^{94}$	$.9434258044^{93}$	
X_m		7.000000590	4.999999574	2.999999995	1.000000002	.
L_m		1.000000000	$-.1142858304$	.2031745788	-21.94285652	
K_m		.02083324281	$-.06250021019$	.06250000887	$-.02083333304$	
J_m	1	16.00000016	86.00000058	176.0000002	104.9999999	

Here superscript k denotes multiplication by 10^k. Comparison with the exact answers found earlier shows that we have solved all three problems quite successfully and, as it were, under one roof. The worst relative error is $\frac{1}{2}10^{-5}$ in K_1; this could be reduced by a factor of ten, by employing (8.6) instead.

Finally, we should mention fast techniques for computing a distant element S_n of an LFSR which avoid solving explicitly for the general term or computing every intermediate element. In the case that the recurrence $J(\mathbf{E})$ is available, we can use J.C.P.Miller's method: evaluate $\mathbf{E}^n \bmod J(\mathbf{E})$ as a polynomial of degree r in $\mathbf{E}$, using the standard 'divide-and-conquer' algorithm for exponentiation in time of order $\log n$, then $S_n = \mathbf{E}^n S_0$ gives S_n in terms of $S_0, \ldots S_{r-1}$. If $S_0, \ldots S_{2r-1}$ is available but not $J(\mathbf{E})$, we can progress by extending S_j to $j = 4r$ (reversing the wall as above), starting a new wall based on $2r$ alternate terms S_{2j} or S_{2j+1} (depending on whether n is even or odd), then iterating and shifting according to the binary digits of n as for exponentiation. When working to fixed precision, numerical instability is a potential complication.

11. Padé Tables

The *Padé Table* of a function $F(Y)$ of one variable Y is essentially the array $R_{i,j} \;=\; P_{i,j}/Q_{i,j}$ of rational functions, with numerator and denominator polynomials of degree j and i resp., whose FLS agree with that of F in their first $i+j+1$ coefficients. [As earlier, there is no need to involve notions of convergence at this point.] We shall assume for simplicity that F is defined by a series with no negative powers of Y, and with constant coefficient unity.

There is a strong connection between linear recurrence relations and Padé approximation, resulting from the fact that (by simple algebra) the generating function for any right-infinite LFSR sequence $[S_n]$ is a rational function $P(Y)/Q(Y)$, where $Q(1/\mathbf{E})$ is a linear relation satisfied by $[S_n]$; we shall use the variable $Y \to 1/\mathbf{E}$ rather than $X \to \mathbf{E}$ to emphasize that the polynomial must be reversed. Older algorithms for computing (entries of) the Padé Table, as mentioned in the readable but casual compendium **Bak75** or detailed in the extensive survey **Wyn60**, break down when the table fails to be 'normal', that is when the function mimics a rational function over the initial portion of its series: the difficulty is essentially that of circumnavigating zero windows in the number wall, and can be overcome by the straightforward though leisurely method subsequently described here.

If $P(Y) = 1$, the sequence generated is the *Impulse Response Sequence* $[S_n]$ of $Q(1/\mathbf{E})$ commencing $[0, 0, ..., 0, 1, ...]$; the initial $r-1$ zeros will be consigned to the region $n < 0$ for now, the unity occupying $n = 0$. In practice, the entire left-hand halves of the number walls we consider here are zero (for $m \neq -1$ and $n < 0$), with $S_{-1,n} = S_{m,0} = 1$; the situation suggests that there might be an interesting connection between the two sequences $[S_n] = [S_{0,n}]$ and $[T_m] = [S_{m,1}]$, and so it transpires:

> **Algorithm:** Let $F(Y) \;=\; \sum_n S_n Y^n$ and $1/F(Y) \;=\; \sum_n T_n Y^n$. Then $T_n \;=\; (-)^{n+1} S_{n,1}$ where $[S_{m,n}]$ is the number wall for $[S_n]$, and vice-versa. (11.1)

Proof: Elementary theory of determinants, applied to the definition (3.1) of $S_{m,n}$ (here nearly triangular) and convolution product of the series for F and $1/F$. ■

At order (N^2) time this algorithm for $1/F$ is more efficient than simple-minded approaches to series division, but no more so than standard methods such as **Knu81** §4.7.

Now let $F(Y) \;=\; \sum_n S_n Y^n$, where $S_n = 0$ for $n < 0$, and $S_0 = 1$. By inspecting the reasoning behind (3.4) a little more closely, it can be seen that $Q_{i,j} \;=\; C \times U_{i-1,j-1}$; where essentially as earlier $U_n(Y) = S_n - S_{n+1}Y$, and C lies in the ground domain and depends on i, j. Also, since the Padé table for $1/F(Y) \;=\; \sum_n T_n Y^n$ is simply $Q_{j,i}/P_{j,i}$, we have similarly $P_{i,j} = D \times V_{j-1,i-1}$, where $V_n(Y) = T_{n+1}Y - T_n$. The ratio D/C turns out to be a sign change $(-)^{ij}$; so finally

> **Algorithm:** The Padé table entries for $F(Y) \;=\; \sum_n S_n Y^n$ are given by
>
> $$R_{i,j} \;=\; (-)^{ij} V_{j-1,i-1}/U_{i-1,j-1}$$
>
> where $U_{m,n}$ and $V_{m,n}$ are the number walls for
>
> $$U_n(Y) \;=\; S_{n+1}Y - S_n \qquad \text{and} \qquad V_n(Y) \;=\; T_{n+1}Y - T_n, \tag{11.2}$$
>
> and
>
> $$T_n \;=\; (-)^{n+1} S_{n,1}$$
>
> where $S_{m,n}$ is the number wall for S_n.

Note the transposition of subscripts and of offsets. [In the Padé Table literature, such polynomial number walls — with variant sign and origin — go by the name of *C-tables* or some similar term.]

An alternative approach to computing the numerators utilizes the observation that the $P_{0,j}$ are just the partial sums $W_n(Y)$ of the series, so it's reasonable to guess that the $P_{i,j}$ might be related to its wall $W_{m,n}$. As before there is an adjustment required [effectively because we would prefer to initialize $W_{-1,n} = Y^n$], and we find

Algorithm: The Padé table entries for $F(Y) = \sum_n S_n Y^n$ are given by

$$R_{i,j} = (-)^i Y^{-ij} W_{i,j}/U_{i-1,j-1}$$

where $U_{m,n}$ and $W_{m,n}$ are the number walls for (11.3)

$$U_n(Y) = S_{n+1}Y - S_n \qquad \text{and} \qquad W_n(Y) = \sum S_n Y^k.$$

Though less elegant, this variation avoids the reciprocal function altogether, and is (somewhat) quicker when only a few rows of the table are required.

The expressions for $P_{i,j}$ and $Q_{i,j}$ essentially as Toeplitz determinants in U_n and W_n are ascribed to Jacobi **Bak75** (3.44); the resulting Sylvester identity (3.6) between five adjacent numerators or denominators is credited to Frobenius **Bak75** (3.30).

Both these algorithms, like (3.4) on which they are based, take order n^4 time (if elementary polynomial multiplication is employed), which for an individual approximant is slow compared to established methods; their performance improves when used to compute numerical values of Pade approximants directly, without first finding the polynomials. Even so, they are somewhat faster than the algorithm based on an elegant identity due to Wynn

$$1/(R_{i+1,j} - R_{i,j}) + 1/(R_{i-1,j} - R_{i,j}) = 1/(R_{i,j+1} - R_{i,j}) + 1/(R_{i,j-1} - R_{i,j})$$

(proved in **Wyn66** or **Gra72**), recommended by several authors, which can only cope with normal tables. Where the table fails to be normal, a 'Padé Block' (corresponding to a zero window in the wall for $[S_n]$), as generated by our algorithms, has identical approximants along its North and West edges with 0/0 elsewhere; strictly, that same approximant is valid throughout the NW half and on the diagonal, though none is customarily defined in the SE half.

Another topic closely interwoven with both Padé tables and LFSR sequences is that of continued fractions; see **Gil78** or **Bak75** §4 for a leisurely introduction.

12. Applications and Related Algorithms

The *Linear Complexity Profile* (LCP) is the traditional device for exploring the extent to which a sequence is piecewise definable by linear relations. It is defined as the sequence of orders of minimal linear recurrences satisfied by the finite segments $[S_0, \ldots, S_n]$ for $n = 0, 1, 2, \ldots$, a *recurrence* being a semi-proper (as it were) relation, having leading coefficient unity. [This restriction is partly justified by the consideration that the recurrence might be required for computing the sequence; more importantly, it avoids the unpleasant prospect of auxiliary polynomials with leading zeros. The distinction explains the confusing phenomenon of minimal recurrences whose order substantially exceeds half of their span.]

The connection between LCP notation and the number wall is discussed in the explanatory paper **Ste92**: broadly, the LCP (as it were) 'tracks' a zig-zag path along an adjacent pair of diagonals across the number wall, normally increasing by unity every two steps, but suffering a 'pause' as it traverses a window, punctuated by a 'jump' as the it crosses the counter-diagonal. (12.1) and (3.4) are not in practice very suitable for computing shifted LCPs, and the discussion in **Ste92** concluded that the most efficient method is in fact to compute the number wall first, then deduce the LCP from it (slightly tricky on account of the asymmetry mentioned above).

Much work has been done on the theory of LCPs, often using generating functions: see for example the references to Niederreiter. However, the technique is hampered by the difficulty of incorporating one-dimensional LCPs based on fixed origins into a properly two-dimensional representation of all *shifted* LCPs. Furthermore, where the domain is of finite characteristic, linear complexity is represented more compactly by determinant than by LFSR order. We consider that the availability of an efficient algorithm for the number wall, together with the geometric viewpoint that it encourages, should cause it to supplant the LCP: geometric ideas play a particularly prominent role in linear complexity over $\mathbf{F}_p$ for $p = 2, 3$, see **Lun00**. The binary case is of practical importance since modified LFSR's are often employed as pseudo-random bit-stream generators for use in Monte-Carlo numerical methods, simulations and particularly stream ciphers: the frame recursion offers improved efficiency in testing such generators for *cryptographic insecurity*, expressed as exceptionally large zero-windows.

An attractive algorithm for extracting numerical approximations to the roots of a polynomial (as well as a number of related tasks such as eigenvalues of a matrix) is a modification of the number-wall known as the *QD method* of Rutishauser, described in detail in **Hen74** §7.6. Based on (8.1), this scheme computes the ratios directly on even rows, using odd rows for book-keeping: the elementary recursion (3.7) suffices for this purpose, the ground domain being the real numbers — where in numerical computation exact zeros are improbable — and in any case, he is able to choose the initial elements of his LFSR sequence so that no zeros can occur. [The convergence is only linear in n, but could in principle be accelerated, possibly using the techniques mentioned at the end of §10.]

Apparently Rutishauser himself had already considered the possibility of making the QD scheme continuous, that is interpolating between the rows and columns in the same way that discrete difference equations are interpolated into continuous differential equations. This topic seems to have only recently been much explored, under the heading of *Toda flows*: surveys are reported in **Fay94**, **Pap94**, for which I am indebted to Bill Dubuque.

We now summarize the *Berlekamp-Massey* algorithm for constructing the minimal relation generating a given LFSR sequence in order r^2 time:

> **Algorithm:** The minimal relation spanning $S_0, \ldots, S_{2r-1}, \ldots$ is $J(\mathbf{E}) \equiv \mathbf{E}^r U_{2r}(1/\mathbf{E})$, where: Initially construct the generating function $T = \sum_n S_n Y^n$ of $[S_n]$ where Y is transcendental, for $0 \leq n < 2r$ or further, and set
>
> $$U_0 = 1, \quad V_0 = Y, \quad k_0 = 0;$$
>
> then for $i = 1, 2, \ldots, 2r, \ldots$ iterate
>
> $$\begin{aligned} W_i &\leftarrow \text{coefficient of } Y^{i-1} \text{ in } U_{i-1}T; \\ U_i &\leftarrow U_{i-1} - V_{i-1}W_i; \\ V_i &\leftarrow \begin{cases} U_{i-1}Y/W_i & \text{if } W_i \neq 0 \text{ and } k_i \geq 0, \\ V_{i-1}Y & \text{otherwise;} \end{cases} \\ k_i &\leftarrow \begin{cases} -k_i & \text{if } W_i \neq 0 \text{ and } k_i \geq 0, \\ k_i + 1 & \text{otherwise.} \end{cases} \end{aligned} \tag{12.1}$$
>
> Used in 'exploratory' mode (where the order r is not known in advance), the algorithm generates $U_i = U_{2r}$ for $i \geq 2r$.

Proof: For this we refer the reader to **Lid86** §6.6, contenting ourselves with a few incidental observations. The variable Y corresponds to a backward shift $1/\mathbf{E}$ rather than forward, in order to avoid difficulties with leading zero coefficients in the polynomial arithmetic. At the i-th iteration, the result of evaluating the relation (corresponding to the reverse of) U_{i-1} for $\ldots, S_{i-1}$ is just W_i; there is no need to compute the entire polynomial product $U_{i-1}(Y)T(Y)$. Notice that intermediate U_i are not in general guaranteed to correspond to the minimal relations spanning $S_0, \ldots, S_{i-1}$. ■

The cost of computing a single relation is order r^2 time, a considerable improvement on (3.4). A generalization of this method to ground ring $\mathbf{Z}/q\mathbf{Z}$ is reported in **Ree85**.

As an illustration, suppose we are to find the minimal relation spanning

$$S = [0, 0, 0, 1, 16, 170, 1520, 12411, 96096, 719860, \ldots].$$

Following the scheme (12.1),

i	W_i	U_i	V_i	k_i
0		1	Y	0
1	0	1	Y^2	1
2	0	1	Y^3	2
3	0	1	Y^4	3
4	1	$1 - Y^4$	Y	-3
5	16	$1 - 16Y - Y^4$	Y^2	-2
6	-86	$1 - 16Y + 86Y^2 - Y^4$	Y^3	-1
7	176	$1 - 16Y + 86Y^2 - 176Y^3 - Y^4$	Y^4	0
8	-106	$1 - 16Y + 86Y^2 - 176Y^3 + 105Y^4$	$R(Y)$	0
9	0	$1 - 16Y + 86Y^2 - 176Y^3 + 105Y^4$	Y	$1 \cdot R(Y)$

where $R(Y)$ denotes $(-Y + 16Y^2 - 86Y^3 + 176Y^4 + Y^5)/106$. Further elements of this LFSR sequence would give $W_i = 0$, $U_i = U_8$, $V_i = Y^k R(Y)$, $k_i = i - 8$ for $i > 8$. Reversing U_8 gives the auxiliary polynomial $J = \mathbf{E}^4 - 16\mathbf{E}^3 + 86\mathbf{E}^2 - 176\mathbf{E} + 105 = 0$, that is S satisfies the relation

$$S_{n+4} - 16S_{n+3} + 86S_{n+2} - 176S_{n+1} + 105S_n = 0.$$

Algorithms reported by **Sen92** and **Ris74** compute the rank and inverse resp. of an individual numerical $n \times n$ Toeplitz matrix, at a cost of order n^2 time. The method involves decomposition into triangular matrices, and does not appear to compete with ours for number walls.

13. Hideous Numerical Example

In the number-wall diagrammed, all arithmetic (including division) is to be done modulo $p = 5$. The entire table wraps around cyclically with n. The LFSR order is $r = 21$ [hardly overwhelming news, since $r \leq n$ for any (periodic) sequence satisfying $\mathbf{E}^n - 1 \ = \ 0$].

Diagram Modulo 5 wall of test sequence S_n for $n = 1(1)21$ ($S_n = 3^{k(k+1)/2-n}$ with $k = [\sqrt{2n} + \frac{1}{2}]$.)

m\n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
-1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	3	1	4	3	1	2	4	3	1	1	2	4	3	1	3	1	2	4	3	1
1	3	3	4	3	0	0	0	0	0	3	4	0	0	0	2	3	0	0	0	0	3
2	0	4	2	1	0	0	0	0	0	4	1	0	0	0	4	3	0	0	0	0	4
3	3	2	0	2	0	0	0	0	0	2	4	0	0	0	3	3	0	0	0	0	2
4	2	1	3	4	0	0	0	0	0	1	1	4	1	4	1	3	0	0	0	0	1
5	1	0	4	3	0	0	0	0	0	3	3	4	2	1	3	3	3	3	3	3	3
6	3	1	2	1	2	4	3	1	2	4	2	0	0	0	1	0	0	3	0	0	1
7	3	4	2	4	2	0	3	4	1	4	3	0	0	0	2	0	0	3	0	0	2
8	2	0	4	2	2	1	3	3	0	2	2	0	0	0	4	2	1	3	1	2	4
9	3	3	3	4	1	2	2	1	4	1	3	3	3	3	3	0	2	1	2	3	1
10	3	3	3	4	4	2	4	1	3	2	3	3	1	1	1	2	4	4	1	1	3
11	0	0	4	1	3	4	2	4	3	0	1	2	1	0	3	4	4	2	1	1	1
12	0	0	2	1	0	0	2	0	3	1	2	1	1	2	4	2	2	0	4	0	2
13	1	4	1	1	0	0	2	1	3	4	3	2	4	0	4	4	1	1	1	2	4
14	3	1	1	1	3	4	2	3	0	2	3	2	1	2	4	1	1	2	1	1	2
15	2	2	0	3	3	2	1	4	3	1	0	3	3	4	1	3	4	3	4	2	4
16	2	4	4	4	1	4	4	1	2	3	4	2	2	4	1	0	2	4	0	3	1
17	0	4	4	4	0	1	2	2	2	1	3	2	2	1	1	1	1	2	2	2	0
18	0	4	0	4	1	4	3	0	1	0	3	4	1	1	0	1	2	3	0	3	0
19	3	4	1	4	3	3	2	1	3	2	3	4	1	1	4	1	1	2	3	2	1
20	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Perturbing S_{10} by subtracting X causes the following changes around the frames of the 5x5 window with NE corner at $S_{1,9}$. [The notation is as in §4 Diagram. Only terms significant to the inductive step of the proof of Lemma (4.9) are retained, along with the dominant term of the remainder; missing terms are indicated by a final '+'. Components not in range of the relevant lemma are omitted from vectors.]

$$\begin{aligned}
A &= [4,\ 3,\ 1,\ 2,\ 4,\ 3,\ 1+4X] \\
B &= [4,\ 3,\ 1,\ 2,\ 4,\ 3,\ 1+X] \\
C &= [\ ,\ 3+4X+4X^5+X^6,\ 1+4X^5,\ 2+4X+3X^2+X^3+X^4, \\
&\qquad 4+X+3X^2+4X^3,\ 3+3X+X^2,\ 1+4X] \\
D &= [\ ,\ 2+X+X^5+X^6,\ 1+X^5,\ 3+X+2X^2+4X^3+2X^4, \\
&\qquad 4+X+3X^2,\ 2+2X+3X^2,\ 1+X]
\end{aligned}$$

$$\begin{aligned}
E &= [1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1] \\
F &= [1,\ 4,\ 2,\ 0,\ 3,\ 4,\ 2] \\
G &= [2+X+,\ 3+,\ 1+2X+,\ 4+X+,\ 1+X+,\ 4+2X,\ 1] \\
H &= [4+4X+,\ 1+,\ 4+4X+,\ 3+4X+,\ 3X+,\ 2+3X+,\ 4+X]
\end{aligned}$$

$$\begin{aligned} M &= N = [\,,\ 4X^5,\ 3X^4,\ X^3,\ 2X^2,\ 4X,\ 3] \\ P &= Q = 2 \qquad U = V = 2/X \\ R &= 2+4X+3X^2+X^3+2X^4+2X^5+2X^6+ \\ T &= 3+X+2X^2+4X^3+3X^4+3X^5+X^6+ \end{aligned}$$

To illustrate the perturbed frame results of §4, we show the dominant term of the error in (4.7),(4.8),(4.9):

$$\begin{aligned} \mathrm{err}(C) &= [\,,\ ,\ 4X^5+,\ X^5+,\ 2X^3+,\ 2X^3+,\ 2X+] \\ \mathrm{err}(D) &= [\,,\ ,\ 3X^5+,\ 2X^5+,\ 4X^3+,\ 2X^3+,\ X+] \\ \mathrm{err}(PT/QR) &= 4X^6+ \\ \mathrm{err}(E+F+G+H) &= [0+,\ 3X+,\ 4X+,\ 3X+,\ 3X+,\ X+,\ 4X+] \end{aligned}$$

Now suppose that we knew the Frame Theorems for 4 × 4 only, and had computed the original table as far as the bottom of the 5 × 5 window. To compute the South frames of this square, we might proceed thus: First perturb the table as above, then find N by (4.2), D by (4.3), H by (3.6) since N is now nonzero, and finally let $X \to 0$. The inductive versions of these theorems for $g-1$ in the form required in the perturbed table for $1 \le k \le k+1$ are:

$$\begin{aligned} N_k &= (-)^{(g-1)(k-1)} M_k B_{k-1}/Ak-1 \\ D_k &= (N_k/U)(QE_{k-1}/A_{k-1} - (-1)^k (PF_{k-1}/B_{k-1} - VC_k/M_k)) \\ H_k &= ({D_k}^2 - D_{k-1}D_{k+1})/N_k \end{aligned}$$

Notice how we need to compute D to $\mathcal{O}(X^6)$ in order to be able to compute H_2 to $\mathcal{O}(X)$ — i.e. at all — because $N_2 = 4X^5$.

But all this is idle speculation, since we do know the Frame Theorems for all g, and can simply compute the original frames directly by (5.1).

References

Ait62 Aitken, A. *Determinants and Matrices,* Oliver & Boyd (1962).

Bak75 Baker, G. A. Jr. *Essentials of Padé Approximants,* Academic Press (1975).

Bla96 Blackburn, S. R. & Etzion, T. & Paterson, K. G. *Permutation Polynomials, deBruijn Sequences, and Linear Complexity,* J. Comb. Theory ser. A **76** (1996) 55–82.

Cha82 Chan, A. H. & Games, R. A. & Key, E. L. *On the Complexities of deBruijn Sequences,* J. Comb. Theory ser. A **33** (1982) 55–82.

Con96 Conway, J. H. & Guy, R. K. *The Book of Numbers,* Springer (1996).

Dav88 Davenport, J. H. & Siret, Y. & Tournier, E. *Computer Algebra,* Academic Press (1988).

Fay94 Faybusovich, Leonid *Rational functions, Toda flows, and LR-like algorithms,* Linear Algebra Appl. **203–204** (1994) 359–383.

Fro85 Froberg, C-E. *Numerical Mathematics,* Benjamin Cummings (1985).

Gil78 Gilewicz, Jacek *Approximants de Padé,* Springer Lecture Notes in Mathematics **667** (1978).

Gra72 Gragg, W. B. *The Padé Table and its Relation to Certain Algorithms of Numerical Analysis,* SIAM Review **14** (1972) 1–62.

Gra96 Granville, A. *The Arithmetic Properties of Binomial Coefficients,* in Proceedings of the Organic Mathematics Workshop (1996).

Hen74 Henrici, P. *Applied and Computational Complex Analysis,* Wiley (1974).

Her75 Herstein, N. *Topics in Algebra,* ed. 2, Wiley (1975).

Ioh82 Iohvidov, I. S. *Hankel and Toeplitz Matrices and Forms,* (trans. Thijsse, G. P. A.) Birkhäuser (1982).

Knu81 Knuth, D. *The Art of Computer Programming,* **1,2** ed 2, Addison-Wesley (1981).

Lan93 Lang, S. *Algebra,* Addison-Wesley (1993).

Lid86 Lidl, R. & Niederreiter, H. *Introduction to Finite Fields and their Applications,* Cambridge (1986).

Lun00 Lunnon, W. F. *Pagodas and Sackcloth: Ternary Sequences of Considerable Linear Complexity,* (to appear).

Maz86 Mazoyer, J. *An Overview of the FSSP,* in C. Choffrut (ed) *Automata Networks,* Springer (1986) 82–94.

Maz87 Mazoyer, J. *A Six-State Minimal-Time Solution to the FSSP,* Theoretical Computer Science **50** (1987) 183–238.

Min67 Minsky, M. *Computation: Finite and Infinite Machines,* Prentice-Hall (1967).

Nie89 Niederreiter, H. *Keystream Sequences with a Good Linear Complexity Profile for Every Starting Point,* in *Eurocrypt '89 Abstracts* Houthalen, Holland (1989).

Niv69 Niven, Ivan *Formal Power Series,* Amer. Math. Monthly **76** (1969) 871–889.

Pap94 Papageorgiou, V. & Grammaticos, B. & Ramani, A. *Integrable difference equations and numerical analysis algorithms,* pp. 269-280 in Levi, Decio (ed.) et al. *Symmetries and integrability of difference equations: Papers from the workshop, May 22–29, 1994, Esterel, Canada;* Amer. Math. Soc. Proc. Lect. Notes **9,** 1996.

Poo96 van der Poorten, Alf *Notes on Fermat's Last Theorem,* Wiley (1996)

Ree85 Reeds, J. A. & Sloane, N. J. A. *Shift-Register Synthesis (Modulo m),* SIAM J. Computing **14** (1985) 505–513.

Ris74 Rissanen, J. *Solution of Linear Equations with Hankel and Toeplitz Matrices,* Numer. Math. **22** (1974) 361–366.

Rob86 Robbins, D. P. & Rumsey Jr., H. *Determinants and Alternating Sign Matrices,* Adv. in Math. **62** (1986) 169–184.

Sen92 Sendra, J. R. & Llovat, J. *Rank of a Hankel Matrix over* $Z[x_1 \ldots x_r]$, Appl. Algebra in Eng. Comm. and Computing **3** (1992) 245–256.

Slo95 Sloane, N. J. A. & Plouffe, S. *The Encyclopedia of Integer Sequences,* Academic Press (1995).

Ste92 Stephens, N. M. *The Zero-square Algorithm for Computing Linear Complexity Profiles,* in Mitchell, Chris (ed.) *Cryptography and Coding II,* Clarendon press Oxford (1992) 259–272.

Wyn60 Wynn, P. *The Rational Approximation of Functions which are Formally Defined by a Power-Series Expansion,* Math. Comp.**14** (1960) 147–186.

Wyn66 Wynn, P. *Upon Systems of Recursions which Obtain among the Quotients of the Padé Table,* Numer. Math. **8** (1966) 264–269.