Nice description of Berlekamp BCH decoding algorithm as a partial fraction algorithm

Investigation of *T*-Numbers and *E*-Sequences

DAVID G. CANTOR*

University of California, Los Angeles

A *PV-number* θ is a real algebraic integer >1, whose algebraic conjugates have absolute value <1. A *T-number* is a real algebraic integer >1, whose algebraic conjugates have absolute value $\leqslant 1$, with at least one conjugate having absolute value $=1$. If x is a real number we shall denote by $N(x)$ the "nearest" integer to x, i.e., $N(x)$ is the unique integer* satisfying $x - \frac{1}{2} < N(x) \leqslant x + \frac{1}{2}$; and by $\|x\|$ we shall denote $|N(x) - x|$. It is known, Salem (1945), that the set of PV-number forms a closed, non-discrete subset of the real numbers and that the closure of the set of T-numbers includes the set of PV-numbers. However, nothing else is known concerning the closure of the set of T-numbers. The purpose of this investigation is to obtain numerical evidence concerning the distribution of T-numbers.

Let θ be a PV or T-number which is a zero of the monic polynomial $\sum_{i=0}^{n} c_i X^i$. It is known, Salem (1945), that there exist infinitely many λ in the field $\mathbf{Q}(\theta)$ such that if $a_n = N(\lambda\theta^n)$ then

$$|a_{n+1} - a_n{}^2/a_{n-1}| < \tfrac{1}{2} \tag{1}$$

for all large n. (If θ is PV any $\lambda \in \mathbf{Q}(\theta)$ such that $\lambda\theta^n$ is an algebraic integer for large n will do. In fact, a_n is the trace of $\lambda\theta^n$ and $\Sigma_i\, c_i\, a_{n-i} = 0$ for all large n.) Sequences $\{a_n\}$ satisfying (1) or, what is the same thing, $a_{n+1} = N(a_n{}^2/a_{n-1})$ are called *E-sequences*. Pisot (1938) and Flor (1960) have shown that if $a_1 \geqslant a_0 + 2\sqrt{a_0}$, then $\phi = \lim_{n\to\infty} a_{n+1}/a_n$ exists and is >1. Furthermore $|\phi - a_1/a_0| < \sqrt{3/32a_0}$. Such numbers $\phi > 1$ are called *E-numbers*. It follows that the set of *E-numbers* contains both the set of PV-numbers and the set of T-numbers. It is not known if the PV- and T-numbers comprise the E-numbers.

* The author wishes to thank the Sloan Foundation and NSF Grant GP 13164 for support during the preparation of this paper.

* Round up if a tie

We calculate E-sequences $\{a_n\}$ whose limiting ratios ϕ are close to 1, and check whether these E-sequences satisfy linear recurrence relationships with constant coefficients. (In actuality we can only check a finite initial segment of such an E-sequence.) If the E-sequence satisfies the recurrence $\sum_{i=0}^{r} c_i a_{n+i} = 0$, then ϕ is a root of $\sum_{i=0}^{r} c_i X^i = 0$ and is a PV- or T-number.

The sequence $\{a_n\}$ satisfies a linear recurrence relation if and only if the corresponding generating function $a = \sum_{n=0}^{\infty} a_n X^n$ is rational. To determine this, we work in the field of formal Laurent series of the shape $b = \sum_{n=n_0}^{\infty} b_n X^n$, where n_0 is an integer (possibly negative). We put $\lambda(b) = \sum_{n=n_0}^{0} b_n X^n$, more generally $\lambda_k(b) = \sum_{n=n_0}^{k} b_n X^n$. If $b_{n_0} \neq 0$, we put $\mathrm{ord}(b) = n_0$, and $\mathrm{ord}(0) = \infty$. We apply the analogue of the standard continued fraction algorithm for real numbers to a. The polynomials in $1/X$ play the role of the integers. This algorithm will terminate if and only if a is rational. (For a related algorithm see Berlekamp (1968)). Since this algorithm does not seem to be in the literature, we describe it here. (A special case for so-called J-fractions appears in Wall (1948).) Put $A_0 = a$ and $c_0 = \lambda(A_0)$. Inductively, for $n = 1, 2, 3, \ldots$ put $A_n = 1/(A_{n-1} - c_{n-1})$ and $c_n = \lambda(A_n)$. Then

$$a = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cdots}},$$

where the c_i's are polynomials in $1/X$. Put $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$ and inductively for $n = 0, 1, 2. \ldots$ let $p_n = c_n p_{n-1} + p_{n-2}$ and $q_n = c_n q_{n-1} + q_{n-2}$. Then p_n/q_n are approximants to a in the sense that $\mathrm{ord}(q_n a - p_n) = -\mathrm{ord}(q_{n+1})$ if a_{n+1} is defined, and otherwise $q_n a - p_n = 0$. If p, q are polynomials in $1/X$ satisfying $\mathrm{ord}(qa - p) > -\mathrm{ord}(q)$ then the fraction p/q is in fact among the fractions p_n/q_n. This means that any linear recurrence of degree d, which is satisfied by the sequence $\{a_n\}$ for d or more consecutive times, will give rise to one of the rational approximants p_n/q_n. The algorithm, as described, is unwieldy, for it involves working with the entire power series a, or at least with the entire initial segment of interest. The modification we describe now brings in coefficients of a when they are needed and no sooner.

Put $h_n = q_n a - p_n$ and $h_n^{(m)} = q_n \lambda_m(a) - p_n$. The identity $A_n = -h_{n-2}/h_{n-1}$ is easy to verify. It follows that $c_n = -\lambda(h_{n-2}/h_{n-1})$ and in fact $c_n = -\lambda(h_{n-2}^{(m)}/h_{n-1}^{(m)})$ for all sufficiently large m. The algorithm follows:

I. (Initialize).
Put $h_{-2} = a_0, h_{-1} = -1, q_{-2} = 1, q_{-1} = 0, n = 0, m = 0.$

II. (Increase m if necessary). Bring in new coefficients if you need them
If $h_{n-1} = 0$ or if $\mathrm{ord}(q_{n-2}) - \mathrm{ord}(h_{n-1}) + m < 0$ or if $\mathrm{ord}(q_{n-1}) + \mathrm{ord}(h_{n-2}) - 2\,\mathrm{ord}(h_{n-1}) + m < 0$ then

A. Put $h'_{n-2} = h_{n-2} + q_{n-2}\, a_{m+1} X^{m+1}$
$h'_{n-1} = h_{n-1} + q_{n-1}\, a_{m+1} X^{m+1}$
$m' = m + 1.$

B. Replace m, h_{n-1}, h_{n-2} by m', h'_{n-1}, h'_{n-2}, respectively.

C. Repeat Step II.

III. (Calculate c_n and h_n).
When the conditions of step II are no longer met, put $c_n = -\lambda(h_{n-2}/h_{n-1})$, $q_n = c_n q_{n-1} + q_{n-2}$, and $h_n = c_n h_{n-1} + h_{n-2}$. Increase n by 1 and go to step II.

The algorithm terminates when m (or n) is large enough. Note that the quantity called h_n in the algorithm is in fact what was denoted by $h_n^{(m)}$ earlier. When using this algorithm one finds that the coefficients of the power series (which must be kept exactly) are rational numbers whose numerators and denominators are enormous integers with varying, unpredictable numbers of digits. For this reason a multiple-precision arithmetic package with automatic storage allocation was written.† Doesnt apply for finite fields

The results of these calculations are still preliminary in nature and will be described later. However, it is noteworthy that the E-sequences we have calculated (mostly with $a_0 \leqslant 20$) seem to satisfy recurrences of low degree if they satisfy any recurrence we can find. Furthermore the coefficients of these recurrences are always small integers. Paul Galyean has made use of this empirical fact by performing the continued fraction algorithm (mod p) where p is a large prime, in our case $2^{31} - 1$, thus speeding calculations considerably. These results are then checked using multiple precision arithmetic. In no case has a false recurrence been found.

Pisot (1938) showed that all E-sequences with $a_0 = 2$ and $a_0 = 3$ satisfy linear recurrence relations of low degrees and actually obtained their coefficients. It is not surprising that he did not continue for $a_0 = 4$, for our calculations show that the E-sequence with $a_0 = 4$, $a_1 = 13$ satisfies no recurrence relation of degree $\leqslant 100$. A10900 A somewhat surprising result was that certain initial segments of E-sequences satisfied recurrences, not of the PV or T type, for many terms. For example the sequence with $a_0 = 8$, $a_1 = 10$ satisfied the recurrence $a_n = a_{n-1} + a_{n-6}$ for $6 \leqslant n \leqslant 37$. Since the roots of $x^6 = x^5 + 1$ are not PV or T numbers the above recurrence cannot hold for all n. A10916

† This package, written in 360 assembly language for use with PL/I, is suitable for large 360's and is available from the author.

Berlekamp, E. (1968). "Algebraic Coding Theory". 178–192. McGraw Hill, New York.

Flor, P. (1960). Über eine Klasse von Folgen natürlicher Zahlen. *Math. Ann.* **140,** 299–307.

Pisot, C. (1938). La Répartition Modulo un et les nombres algébriques, *Annali dr. r. Scuola Normal Sup. Pisa*, Ser. 2 **7,** 205–248.

Salem, R. (1945). Power Series with Integral Coefficients, *Duke Math. J.* **12,** 153–172.

Wall, H. W. (1948). "Analytic Theory of Continued Fractions". Van Nostrand, New York (reprinted (1967) by Chelsea, New York.).