can select a large number of survivor paths. Fig. 2 shows an example of how our algorithm operates in the Rayleigh fading condition, where the proposed algorithm is denoted by the α-algorithm.

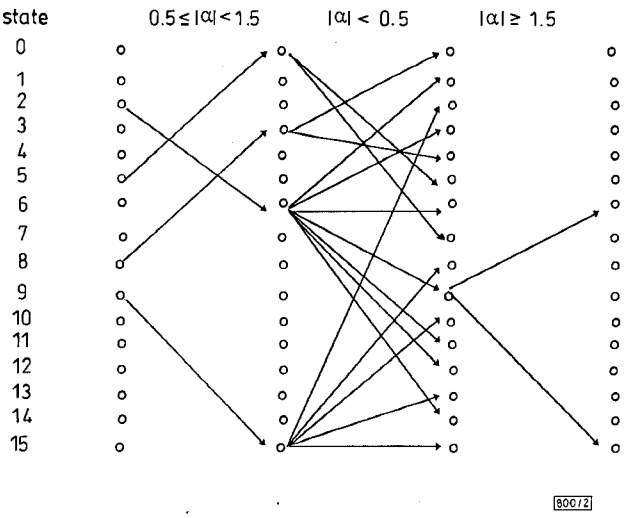

Fig. 2 *Example of operation of α-algorithm*

We use the following criterion to determine the number of survivor paths: (i) when $|\alpha| \leq 1.5$, we select only two survivor paths; (ii) when $0.5 \leq |\alpha| < 1.5$, four survivor paths exist; (iii) when $|\alpha| < 0.5$, all 16 paths are chosen. Finally, we search the path having the minimum metric from the survivor paths.

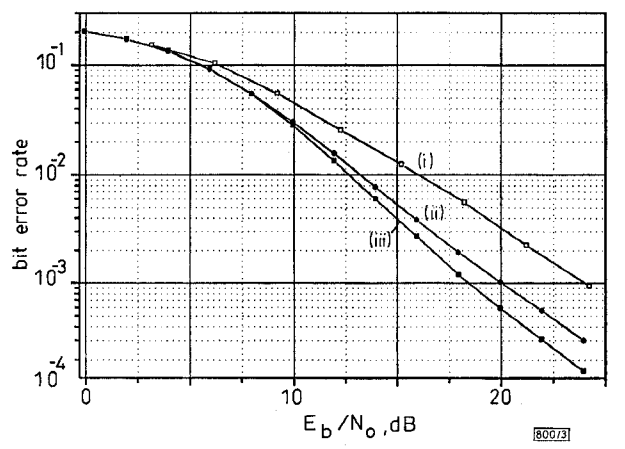

Fig. 3 *Bit error rate of three algorithms*

(i) M-algorithm ($M = 5$)
(ii) T-algorithm ($T = 10.0$)
(iii) α-algorithm

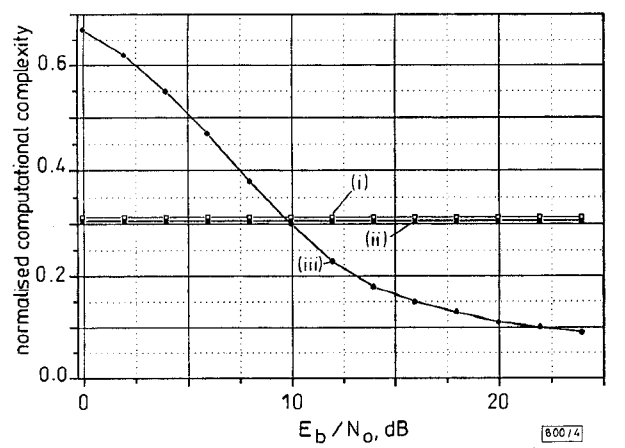

Fig. 4 *Normalised computational complexity for three Viterbi algorithms (16 state)*

(i) M-algorithm ($M = 5$)
(ii) α-algorithm
(iii) T-algorithm ($T = 10.0$)

Results and Discussion: Figs. 3 and 4 show the bit error rate (BER) and computational complexity of the three algorithms, respectively. In comparison, we choose $M = 5$ because the computational complexity of the M-algorithm with $M = 5$ is similar to that of the α-algorithm. For the T-algorithm, we choose $T = 10$ because the BER of the T-algorithm with $T = 10$ is similar to that of the α-algorithm. We can see that the detection performance of the M-algorithm is not satisfactory compared with both the T-algorithm and the α-algorithm as shown in Fig. 3. Here, all the computational complexities are normalised to the computational complexity of the original Viterbi algorithm. From Fig. 4, we can see that the computational complexity of the T-algorithm depends on the bit energy-to-noise ratio (E_b/N_0). When E_b/N_0 is < 10dB, the complexity of the α-algorithm is lower than the T-algorithm and when E_b/N_0 is > 10dB, its complexity is higher than the T-algorithm. We can see that the proposed algorithm has merits when $E_b/N_0 < 10$dB.

If the decision criterion to determine the number of the survivor paths according to the estimated channel conditions is chosen correctly, a good compromise between the computational complexity and the detection performance can be found.

1 April 1997
Electronics Letters Online No: 19970621

Goo-Young Jeong, Chang-Joo Kim and Hyuck-Jae Lee (*Radio Signal Processing Section, Electronics Telecommunications Research Institute, PO Box 106, Yusong, Taejon, 305-600 Korea*)

References

1 SAMPEI, S., and SUNAGA, T.: 'Rayleigh fading compensation for QAM in land mobile radio communications', *IEEE Trans.*, 1993, **VT-42**, pp. 137–147
2 KAMIO, Y., and SAMPEI, S.: 'Performance of a trellis-coded 16QAM/TDMA system for land mobile communications', *IEEE Trans.*, 1994, **VT-43**, pp. 528–536
3 KIM, C.J., KIM, Y.S., JEONG, G.Y., MUN, J.K., and LEE, H.J.: 'Symbol error rates of QAM with space diversity in Rayleigh fading channels', *ETRI J.*, 1996, **17**, (4), pp. 25–35
4 SIMMONS, S.J.: 'Breadth-first trellis decoding with adaptive effort', *IEEE Trans.*, 1990, **COM-38**, pp. 3–12
5 ANDERSON, J.B., and MOHAN, S.: 'Sequential coding algorithms: A survey and cost analysis', *IEEE Trans.*, 1984, **COM-32**, pp. 169–176

Variation on Euclid's algorithm for polynomials

L.C. Calvez, S. Azou and P. Vilbé

Indexing terms: Mathematical analysis, Algorithm theory

It is shown that the sequence of polynomials produced during a run of the extended Euclid's algorithm can be readily obtained via the non-extended algorithm, when properly initialised.

Introduction and notation: Since a paper by Sugiyama *et al.* [1], in 1975, showing that the key equation for decoding Goppa codes can be solved by Euclid's algorithm, there has been renewed interest in the use of the celebrated algorithm. The Padé approximation [2], signal processing [3 – 6], system theory and control engineering [7, 8] are all relevant.

Let $A(x)$ and $B(x)$ be fixed polynomials over a field with $a \triangleq \deg(A) \geq b \triangleq \deg(B)$. It is well-known that the common factor $G(x)$ of $A(x)$ and $B(x)$ of highest degree can be computed via a procedure consisting of a finite sequence of polynomial divisions that we shall call the basic Euclid's algorithm to avoid confusion with the extended Euclid's algorithm which yields not only the greatest common divisor $gcd(A, B) = G$, but also polynomials X and Y such that

$$AX + BY = G \qquad (1)$$

with $\deg(X) < b–g$ and $\deg(Y) < a–g$, $g \triangleq \deg(G)$, provided $a > g$ and $b > g$. It is worth noting that $gcd(A, B) = G$ is only unique up to a multiplicative constant, but can be made unique by requiring

it to be monic, i.e. to have a highest-order coefficient that is equal to unity.

It is the purpose of this Letter to prove that, with a slight modification of the starting and terminating conditions, simultaneous computation of G and X or Y can be carried out by the basic version of Euclid's algorithm. Before developing the new procedure, the standard algorithms are briefly reviewed in the following where *Quot*(N, D) and *Rem*(N, D) denote, respectively, the quotient and remainder polynomials obtained by dividing $N(x)$ by $D(x)$ with both polynomials arranged in descending powers of x.

Basic Euclid's algorithm: Set $S_0 = A$, $S_1 = B$ and perform successively the divisions S_{i-2}/S_{i-1} to obtain $S_i = Rem(S_{i-2}, S_{i-1})$, for i = 2,3,..., I+1, until a remainder $S_{I+1} = 0$ is obtained. As is well known, the last non-zero remainder S_I yields $gcd(A, B) = C = S_I$.

Extended Euclid's algorithm: At the same time that $gcd(A, B)$ is being computed via the preceding basic algorithm, polynomials X_i and Y_i can be computed recursively for i = 2,3,..., I, using $Q_i = Quot(S_{i-2}/S_{i-1})$, $X_i = X_{i-2} - Q_i X_{i-1}$ and $Y_i = Y_{i-2} - Q_i Y_{i-1}$ initialised with $X_0 = Y_1 = 1$ and $X_1 = Y_0 = 0$. A solution to eqn. 1 is then $G = S_I$, $X = X_I$ and $Y = Y_I$.

The main results of this Letter are now stated in the form of two algorithms.

Algorithm GX: Set $R_0 = x^b A + 1$ and $R_1 = x^b B$. Start the divisions R_{i-2}/R_{i-1} of the basic Euclid's algorithm to obtain $R_i = Rem(R_{i-2}, R_{i-1})$ for i = 2,3,... and stop the divisions when the degrees of the remainder polynomials R_i satisfy $\deg(R_I) \geq b$ and $\deg(R_{I+1}) < b$ for some I. Then

$$R_I = x^b G + X \tag{2}$$

and since $\deg(X) < b$, R_I yields G and X at once.

Outline of proof: The first step is to prove that the polynomials R_i generated by the algorithm GX are related to the above-mentioned polynomials S_i and X_i by

$$R_i = x^b S_i + X_i \qquad i = 0, 1, ..., I + 1 \tag{3}$$

This is readily checked for $i = 0$ and $i = 1$. Let us assume that eqn. 3 is true for the integers i–1 and i, ($1 \leq i \leq I$). Then, using elementary polynomial arithmetic, we can prove that eqn. 3 necessarily holds for the next i+1. Therefore, eqn. 3 is proved by mathematical induction. To achieve the proof, the integer I evidenced in algorithm GX can easily be shown to be identical with the integer I in the standard Euclid's algorithm; then, remembering that $S_I = G$ and $X_I = X$, it is sufficient to set $i = I$ in eqn. 3 to obtain eqn. 2.

Remarks: (i) As long as our purpose is limited to obtaining G and X that satisfy eqn. 1, each R_i can be multiplied by any arbitrary nonzero constant; these constants may be chosen to save numerical work or to make G monic.

(ii) If, for some I, $\deg(R_I) = b$, then the next division to get R_{I+1} is superfluous, since it is necessary that $\deg(R_{I+1}) < b$. In this case, up to a multiplicative constant (see remark (i)) $R_I = x^b + X$, which implies that A and B are relatively prime, and eqn. 1 reduces to $AX+BY = 1$, known as the Bezout identity.

Example 1 : Let $A = 2x^4 + 7x^3 + 8x^2 + 5x + 2$ and $B = x^3 + 3x^2 + 3x + 2$. Since $\deg(B) = 3$, set $R_0 = x^3 A + 1$ and $R_1 = x^3 B$. By successive divisions we obtain the following sequence of remainders:

$$R_2 = \mathrm{Rem}(R_0, R_1) = -x^5 - 2x^4 + 1$$
$$R_3 = \mathrm{Rem}(R_1, R_2) = x^4 + 2x^3 + x + 1$$
$$R_4 = \mathrm{Rem}(R_2, R_3) = x^2 + x + 1$$

The procedure is stopped at this stage because $\deg(R_4) < 3$. Comparing $R_3 = x^3(x+2)+x+1$ with eqn. 2, we get $G = x+2$ and $X = x+1$.

Remark : Once G and X are known, Y can be readily obtained from eqn. 1 as $Y = (G-AX)/B$. However, if Y is needed but not X, it is better to calculate Y directly, using the following algorithm.

Algorithm GY: Set $R_0 = x^a A$ and $R_I = x^a B+1$. Start the divisions R_{i-2}/R_{i-1} of the basic Euclid's algorithm to obtain $R_i = Rem(R_{i-2}, R_{i-1})$, for i = 2,3,... and stop the divisions when the degrees of the remainder polynomials R_i satisfy $\deg(R_I) \geq a$ and $\deg(R_{I+1}) < a$ for some I. Then

$$R_I = x^a G + Y \tag{4}$$

and since $\deg(Y) < a$, R_I yields G and Y at once.

Outline of proof: The proof, similar to that of algorithm GX, is based on the expression of R_i which is now given by

$$R_i = x^a S_i + Y_i \qquad i = 0, 1, ..., I + 1 \tag{5}$$

Hence, setting $i = I$ gives eqn. 4.

Example 2: Let A and B be the polynomials of example 1. Since $\deg(A) = 4$, set $R_0 = x^4 A$ and $R_1 = x^4 B + 1$. By successive divisions we obtain the following sequence of remainders:

$$R_2 = -x^6 - 2x^5 - 2x - 1$$
$$R_3 = x^5 + 2x^4 - 2x^2 - 3x$$
$$R_4 = -2x^3 - 3x^2 - 2x - 1$$

The procedure is stopped at this stage because $\deg(R_4) < 4$. Comparing $R_3 = x^4(x+2)-x(2x+3)$ with eqn. 4 yields $G = x+2$ and $Y = -x(2x+3)$.

Example 3: Let $f(x) = c_0+c_1x+c_2x^2+...$ be a power series in the indeterminate x over a field and let N be a non-negative integer. From [2] it is known that the extended Euclid's algorithm applied to x^{N+1} and $c_N x^N + ... + c_0$ yields Nth order Padé approximation S_i/Y_i to $f(x)$. Thus, producing a Padé approximation via algorithm GY is straightforward.

To get third order Padé approximations to e^x (a standard example) let us apply the algorithm GY to $A = x^4$ and $B = x^3/6+x^2/2+x+1$. Set $R_0 = x^8$ and $R_1 = x^4 B+1$. To save numerical work we could (but do not) drop multiplicative constants in the remainders which are obtained in succession as

$$R_2 = 3[x^4(x^2 + 4x + 6) - 2x + 6]$$
$$R_3 = [x^4(2x + 6) + x^2 - 4x + 6]/3$$
$$R_4 = 3[x^4(6) - x^3 + 3x^2 - 6x + 6]/2$$

On account of eqn. 5, four third order Padé approximations S_i/Y_i are available from R_i, i = 1, 2, 3, 4. For instance, the (1,2) approximation extracted from R_3 is $S_3/Y_3 = (2x+6) / (x^2-4x+6)$ which agrees with a well-known result in the literature.

Conclusion: The proposed variation of Euclid's algorithm automates the calculation of X_i and/or Y_i polynomials associated with the extended algorithm. Since this method involves only remainder calculations, it is very easy to use.

10 April 1997
Electronics Letters Online No: 19970658

L.C. Calvez, S. Azou and P. Vilbé (*Laboratoire d'Electronique et Systèmes de Télécommunications (LEST), URA CNRS no. 1329, Université de Bretagne Occidentale (UBO), 29285 Brest Cedex, France*)

References

1 SUGIYAMA, Y., KASAHARA, M., HIRASAWA, S., and NAMEKAWA, T.: 'A method for solving key equation for decoding Goppa codes', *Information and Control*, 1975, **27**, pp. 87–99

2 MCELIECE, R.J., and SHEARER, J.B.: 'A property of Euclid's algorithm and an application to Padé approximation', *SIAM J. Appl. Math.*, 1978, **34**, (4), pp. 611–615

3 SUGIYAMA, Y.: 'An algorithm for solving discrete-time Wiener-Hopf equations based upon Euclid's algorithm', *IEEE Trans. Inf. Theory*, 1986, **32**, (3), pp. 394–409

4 DEMEURE, C.J., and MULLIS, C.T.: 'The Euclid algorithm and the fast computation of cross-covariance and autocovariance sequences', *IEEE Trans. Acoust., Speech, Signal Process.*, 1989, **37**, (4), pp. 545–552

5 PALMER, R.D., and CRUZ, J.R.: 'An ARMA spectral analysis technique based on a fast Euclidean algorithm', *IEEE Trans. Acoust., Speech, Signal Process.*, 1989, **37**, (10), pp. 1532–1536

6 DEMEURE, C.J., and MULLIS, C.T.: 'A Newton-Raphson method for moving-average spectral factorisation using the Euclid algorithm', *IEEE Trans. Acoust., Speech, Signal Process.*, 1990, **38**, (10), pp. 1697–1709

7 CALVEZ, L.C., VILBE, P., and SEVELLEC, M.: 'Efficient evaluation of model-reduction related integrals via polynomial arithmetic', *Electron. Lett.*, 1992, **28**, (7), pp. 659–661

8 DERRIEN, A., NOUET, C., VILBE, P., and CALVEZ, L.C.: 'Orthogonal sets for efficient model-order reduction via a Gauss-Newton method', *Electron. Lett.*, 1994, **30**, (7), pp. 544–546