ZASTOSOWANIA MATEMATYKI
VII (1963)

S. K. ZAREMBA (Swansea)

MINIMUM-AUTOCORRELATION SEQUENCES

M. T. G. Hughes and A. R. M. Noton [1] proposed a new method of evaluating in the presence of internal noise the response of a linear control system to a unit impulse. This method consists of feeding white noise into the system and estimating the cross-covariance function of the input-and-output process; this function is precisely the required response multiplied by the variance of the input. It is easy to see how the effect of the noise in the system is reduced by this procedure.

In the model which is adopted in practice, time is discretized. The input becomes then a sequence $\{x_t\}$ of impulses; it is convenient to make $x_t = \pm 1$ for every t, the mean being 0, so that var $x_t = 1$. The response in question is now a sequence; if this sequence is denoted by $\{h_k\}$, and if the noise in the system is ignored, the output is given by

$$y_t = \sum_{l=0}^{+\infty} h_l x_{t-l}.$$

The cross-covariance function of $\{x_t, y_t\}$ is estimated by means of

$$\overline{x_t y_{t+k}} = \sum_{l=0}^{+\infty} h_l \cdot \overline{x_t x_{t+k-l}}, \tag{1}$$

where the bars denote temporal averages. The expectation of the right-hand side is 0 for negative values of k and h_k for $k \geqslant 0$. The actual values of (1) will be nearest to their respective expectations if the averages $\overline{x_t x_{t+m}}$ are as near as possible to 0 for all $m \neq 0$.

It was never proposed to use an actual white noise generator as a source of input. The input is in fact determinate. Thus we are faced with the problem of devising a finite sequence $\{x_t\}$ of length, say, N composed of equal numbers of $+1$'s and -1's in such a way as to minimize the absolute values of the averages

$$\overline{x_t x_{t+k}}. \tag{2}$$

In practice one assumes that the response h_k becomes negligible for lags exceeding some specified number. Then the absolute values of (2) need to be minimized only for values of k which are smaller than this number, and this makes the problem more tractable.

Once an input sequence has been fixed and registered in some form or other, it is likely to be repeated a number of times during the same experiment in order to average out, as far as possible, the noise in the system. It is, therefore, reasonable, and it also proves convenient, to interpret (2) as

$$R_k = \frac{1}{N}\sum_{t=0}^{N} x_t x_{t+k}, \tag{3}$$

where the indices are reduced modulo N. Thus, $\bar{x}_t$ being equal to 0, $\{R_k\}$ is the circular sample covariance function of $\{x_t\}$, and at the same time its circular sample autocorrelation function, since $R_0 = 1$.

In what follows it will be more convenient to deal with sequences of 0's and 1's. Obviously, replacing 0 by -1 does not affect the circular sample autocorrelation function, which in any case will be denoted by $\{R_k\}$.

Given an arbitrary positive integer r, form the sequence of all the integers from 0 to 2^r-1, writing them consecutively in binary notation; the sequence of the $N = r2^r$ digits, taken in the order in which they are written, will be denoted by S_r. It may be worth recalling that it was with this kind of finite sequences that normal sequences of digits were built up on a decimal base by D. G. Champernowne [2]; for later developments see A. G. Postnikov [3].

It will be convenient to write S_r in 2^r columns, each of them being composed of the successive binary digits of the corresponding integer from 0 to 2^{r-1}. The matrix formed in this manner will be described as *the matrix of* S_r. For instance, that of S_4 will be

$$\begin{bmatrix} 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}.$$

The ordinal number of the row in which a digit is situated will be described as its *depth*. Two ordered pairs of digits will be said to have *the same relative position* if the depths of the corresponding digits are the same, and if the difference, reduced modulo 2^r, of the ordinal number of the column containing the first digit and of that containing the second is the same in both pairs. There are, obviously, 2^r pairs of digits in any given relative position. The pairs $(0, 0)$ and $(1, 1)$ will be called *homogeneous*, and the pairs $(0, 1)$ and $(1, 0)$ *heterogeneous*.

LEMMA. *The set of all the pairs of digits of S_r being in an arbitrarily given relative position which involves different depths of the two elements is composed of equal numbers of homogeneous and heterogeneous pairs.*

Proof. Let p and q with $p < q$ be the respective depths of the digits in the given relative position. It is easily seen that the row no. p is composed of runs of 2^{r-p} equal digits. To the elements of any of these runs (of zeros or of units) there corresponds a sequence of consecutive elements of the row no. q which form with them pairs in the given relative position. But every row contains equal numbers of 0's and 1's, and the row no. q has a period of 2^{r-q+1}, which divides 2^{r-p}. Hence any 2^{r-p} consecutive elements of this row include equal numbers of 0's and 1's, so that the 2^{r-p} pairs under consideration consist of equal numbers of homogeneous and heterogeneous pairs. Since the set of all the pairs in the given relative position is composed of 2^p similar sets, this completes the proof.

But it is easily seen that NR_k is equal to the difference between the numbers of homogeneous and heterogeneous pairs in the right-hand side of (3). Now these N pairs can be separated into r sets of pairs being in the same relative position. Moreover, if k is not a multiple of r, the depths of the two digits in any pair are different. Hence the following:

PROPOSITION 1. *The circular sample autocorrelation function of S_r takes the value* 0 *for all the lags which are not divisible by r.*

Thus, in principle, S_r is a solution of our problem. However, since R_r is easily seen to be large, applications would entail inordinately long sequences of digits. On the other hand, the author is inclined to doubt the existence of sequences which would be much shorter than S_r and would have zero covariances for all lags other than multiples of r, or even only for lags smaller than this number. It is, therefore, proposed to explore sequences in which the covariances which matter are not necessarily all equal exactly to 0, but are, on the whole, much smaller in absolute value than one would expect them to be if the sequences were chosen at random.

The two kinds of solution which will be suggested arise out of S_r by appropriate permutations of the columns of its matrix. Columns beginning with a 0 will be described as *white*, and those beginning with a 1 as *black*. Thus the matrix of S_r consists of 2^{r-1} white columns preceding as many black columns. Beginning with the first two, adjacent columns will be formed into pairs. Hence both columns forming a pair are always of the same colour; this will be regarded as the colour of the pair. S_r is now transformed into a new sequence S_r^* by re-ordering the columns of its matrix in the following manner: at the beginning we put the first pair of white columns, then the last pair of black columns, and further the second white pair followed by the last-but-one black pair etc., alternating white and black pairs in such a way that the order of the white pairs remains unchanged in comparison with S_r, while that of the black pairs is reversed (without changing the order within the pairs). Thus, for instance, the matrix of S_4^* is

$$\begin{bmatrix} 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&0&1&1&0&0&1&1&1&1&0&0&1&1&0&0 \\ 0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix}.$$

PROPOSITION 2. *The circular sample autocorrelation function of S_r^* takes the value* 0 *for all the lags which are not divisible by r, while*

$$R_r = -4/N.$$

Proof. With the exception of the last row, digits situated in the same depth and belonging to the same pair of columns are clearly equal. On the other hand, no pair of adjacent elements of the last row is homogeneous. It follows that if the relative position of two elements is such that one, and only one, of them is situated in the last row, then the set of all the pairs of digits in the same relative position is composed of equal numbers of homogeneous and heterogeneous pairs.

The relative position of any other pair of digits will be characterized by depths p and q $(p < q < r)$ and by a specified difference between the ordinal numbers of the corresponding columns. Pairs in which the digit at a depth p belongs to a white column will be considered first; of course, the argument which follows will also apply, with obvious modifications, to pairs in which this digit belongs to a black column. Further, pairs of digits in which this element belongs to the first column of a pair will be considered first, the same argument applying also to pairs of digits in which the digit in depth p belongs to the second column of the pair. The other digit of the pair belongs to a column of constant colour. If this colour is again white, it suffices to note that if we discard the last row of the matrix and take one column from each pair, we obtain the first half, i.e. the first 2^{r-2} columns, of the matrix of S_{r-1}, and the argument of the Lemma shows that the numbers of homogeneous and heterogeneous pairs of digits will be equal. The same argument applied to the case of the column containing the digit at a depth q being black, since the period of the digits of black columns situated at a given depth is equal to that of the digits of white columns at the same depth. Thus we find again that for lags which are not divisible by r the values of $\{R_k\}$ are equal to 0.

There remains to consider the correlation of lag r. The relevant pairs of digits are situated in adjacent columns of the matrix of S_r^* and in the same row. In the first row, pairs of 0's and pairs of 1's alternate invariably. In consequence, the first row contains 2^{r-1} homogeneous pairs of consecutive digits and as many heterogeneous pairs, so that its contribution to R_r is 0. The picture in the next $r-2$ rows is similar, but with a growing number of exceptions. It is easy to see that the passage from a white to a black column always involves a change in the value of the digit; this is an immediate consequence of a skew symmetry of the matrix of S_r whereby, for any t ($1 \leqslant t \leqslant 2^r$), the column no. 2^r-t+1 can be obtained from the column no. t by replacing in it all the 0's by 1's and all the 1's by 0's. It follows that the passage from a black column to a white one also involves a change unless the digit in the white column has changed in comparison with the preceding white column. But in the second row there are two such changes (we regard it as having a cyclic order), so that the number of homogeneous pairs exceeds that of heterogeneous pairs by 4. In general, in the row no. p ($1 < p < r$) there are 2^{p-1} changes of digits within the white columns. Thus the contribution of the first $r-1$ rows to R_r amounts to

$$\sum_{p=2}^{r-1} 2^p = 2^r-4.$$

But in the last row all the pairs of consecutive digits are heterogeneous, so that its contribution to R_r is -2^r. The total having to be divided by N, we find $R_r = -4/N$, which completes the proof.

The value of R_r in S_r^* is satisfactory, but R_{2r} is easily seen to be large, so that N is still large in comparision with the number of consecutive values of the sample autocorrelation function which are negligible. Despite the fact that sequences of the type of S_r^* do not appear to be altogether useless, it was felt that other ways of permuting the columns of the matrix of S_r should be explored. One of them consists of fixing an odd integer p and taking out of the matrix S_r the columns whose ordinal numbers are the successive multiples of p reduced modulo 2^r; the elements of the resulting matrix, taken column after column, form a new sequence $S_r^{(p)}$. In other terms, we write in binary notation the successive multiples of p reduced modulo 2^r, and the $r2^r$ consecutive digits form $S_r^{(p)}$.

PROPOSITION 3. *For any odd p and any integer r bigger than* 1, *the circular sample autocorrelation function of $S_r^{(p)}$ takes the value* 0 *for all lags which are not divisible by r.*

Proof. In view of the nature of the permutation of columns which transforms the matrix of S_r into that of $S_r^{(p)}$, it is clear that two pairs of digits are in the same relative position after this transformation if and only if they were previously in the same relative position. Consequently, the Lemma also applies to sets of pairs of digits being in the same relative position in $S_r^{(p)}$, and Proposition 3 follows therefrom in the same way as Proposition 1.

Of course, the values of the circular sample autocorrelation function of $S_r^{(p)}$ for lags which are multiples of r depend on the values of r and p.

No general theory is offered for the optimum choice of p when r is given; this can be done by inspection in each particular case. Let it be only noted that $r = 7$ and $p = 15$ seems to be a particularly practical combination (Table 1) from the view point of applications suggested in [1]. Indeed, for $S_7^{(15)}$, we have

$$R_7 = -1/224; \quad R_{14} = 1/16.$$

TABLE 1

Table of the sequence $S_7^{(15)}$ (to be read downwards column after column, from left to right)

0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0
0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1	0	1	0	1
0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1
1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
0	0	0	0	0	0	0	0	0	0	0	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	1	1	1	1	1	1	1	1	1	1

This is easily verified without a tedious count by studying, for R_7, the effect, on the last four binary digits of a number, of adding to it 15, and then considering separately the effect on the other digits of a binary unit being carried over; similar considerations yield the value of R_{14}. In this way it can also be seen that in $S_r^{(p)}$, p being any odd number, R_{2r} is always bigger than R_r.

The values of R_7 and R_{14} can be compared with those likely to be obtained if a sequence of $7 \times 2^7 = 896$ binary digits were formed at random. The values of the sample autocorrelation function corresponding to various lags, and computed on the assumption that the mean of the digits is $\frac{1}{2}$, would be uncorrelated and approximately normally distributed (cf. [4]) with a variance equal to 1/896, and consequently a standard deviation of $896^{-\frac{1}{2}} > 1/30$. Now R_7 is much smaller than this value, while R_{14} is smaller than twice this standard deviation; a value bigger than this would be expected among 20 values of the sample autocorrelation function of a random sequence of 896 binary digits.

It may also be noted that, for $S_7^{(15)}$, the value of

$$\sum_{k=1}^{20} R_k^2,$$

which reduces to $R_7^2+R_{14}^2$, is less than one-fifth of the expected value of the same expression in the corresponding random sequence. With a view to possible applications, a table od $S_7^{(15)}$ is given above.

It is perhaps worth pointing out that errors in the evaluation of $\{h_k\}$ arising out of *one* value of $\{R_k\}$ appreciably differing from 0 can be corrected with very little effort. For instance, in the case of $S_7^{(15)}$, with the 0's replaced by -1's, if we assume that h_k is negligible for $k > 20$ and accept R_7 as sufficiently near to 0, but wish to correct the error arising out of the value of R_{14}, we find, according to (1),

$$\overline{x_t y_{t+k}} = \sum_{l=0}^{+\infty} h_l R_{k-l} \simeq h_k R_0 + h_{k+14} R_{14}, \qquad 0 \leqslant k \leqslant 6;$$

$$\overline{x_t y_{t+k}} \simeq h_k R_0 = h_k, \qquad 7 \leqslant k \leqslant 13;$$

$$\overline{x_t y_{t+k}} \simeq h_{k-14} R_{14} + h_k R_0, \qquad 14 \leqslant k \leqslant 20.$$

Thus h_7, h_8, h_9, h_{10}, h_{11}, h_{12}, h_{13} require no correction at all, while the other values of $\{h_k\}$ are given by

$$h_k = \frac{\overline{x_t y_{t+k}} - R_{14} \overline{x_t y_{t+k\pm 14}}}{R_0^2 - R_{14}^2},$$

the sign in front of 14 being + for $0 \leqslant k \leqslant 6$ and − for $14 \leqslant k \leqslant 20$.

Alternatively, if h_k is assumed to be negligible for $k > 20$, it may be plausible also to assume that, for $k \geqslant 14$, h_k is sufficiently small to make $R_{14} h_k$ negligible; then no corrections are needed for the first 14 values of $\{h_k\}$, and the corrections to the next 7 values are simplified. As a matter of fact, corrections arising out of two or even three values of $\{R_k\}$ differing too much from 0 would not be very laborious, and this, evidently, widens the scope of the whole method.

The author wishes to stress that he does not claim to have necessarily found the best solution of the problem of finding minimum-autocorrelation sequences of binary digits; indeed, he would welcome a better solution than his own, let alone one which could be proved to be the best possible in some well-defined sense.

References

[1] M. T. G. Hughes and A. R. M. Noton, *The measurement of control characteristics by means of a cross-correlator*, Proc. of the Institution of Electrical Engineers, 109, Part B, No. 43, pp. 77-83.

[2] D. G. Champernowne, *The construction of decimals normal in the scale of ten*, J. London Math. Soc. 8 (1933), pp. 254-260.

[3] А. Г. Постников, *Арифметическое моделирование случайных процессов*, Труды Математического Института имени В. А. Стеклова, Москва 1960.

[4] Z. A. Łomnicki and S. K. Zaremba, *On some moments and distributions occurring in the theory of linear stochastic processes, I*, Monatsh. Math. 61 (1957), pp. 318-358.

Received on 1. 12. 1962

S. K. ZAREMBA (Swansea)

CIĄGI O MINIMALNEJ AUTOKORELACJI

STRESZCZENIE

Charakterystyczną cechą liniowych układów sterowania jest ich odpowiedź na impuls jednostkowy. Przy jej doświadczalnym wyznaczaniu możliwe są zniekształcenia przez szum wewnętrzny. Można temu w zasadzie w znany sposób zaradzić przez wielokrotne wprowadzanie na wejściu białego szumu.

Za M. T. G. Hughesem i A. R. M. Notonem proponuję użyć za sygnał wejściowy skończony ciąg złożony z zer i jedynek, taki żeby jego funkcja autokorelacji przyjmowała wartości równe lub możliwie bliskie zeru.

Następnie podaję prosty sposób budowy takiego ciągu, oznaczonego w pracy przez S_r i dowodzę, że S_r ma pożądane własności. Okazuje się jednak, że ciągi S_r byłyby zbyt długie dla zastosowania w praktyce. Aby temu zaradzić, podaję dwa sposoby permutowania wyrazów ciągu S_r, co prowadzi do dwóch wariantów, z których zwłaszcza drugi (ciąg $S_r^{(p)}$) zachowuje korzystne własności ciągu S_r przy niezbyt wielkiej liczbie wyrazów.

W pracy podano ciąg o 896 wyrazach i opisano sposób jego używania.

С. К. ЗАРЭМБА (Свапсии)

ПОСЛЕДОВАТЕЛЬНОСТИ С МИНИМАЛЬНОЙ АВТОКОРРЕЛЯЦИЕЙ

РЕЗЮМЕ

Характеристической чертой линейных схем управления является реакция на единичный импульс. Во время её экспериментального определения возможны искажения, связанные с внутренними шумами. Этого можно избежать путем многократного введения на входе „белого шума".

Согласно М. Т. Г. Юзу и А. Р. М. Нотону предлагаю в качестве входного сигнала использовать конечную последовательность составленную из нулей и единиц. Функция корреляции этой последовательности должна принимать значения равные или возможно близкие к нулю.

Привожу далее простой способ построения такой последовательности обозначенной в работе S_r и доказываю, что S_r обладает всеми необходимыми свойствами. Однако, оказывается, что последовательности S_r слишком длинны для их практического использования. Чтобы этого избегать, привожу два способа перестановки членов последовательности S_r, что ведет к двум вариантам, из которых особенно второй (последовательность $S_r^{(p)}$) сохраняет выгодные свойства последовательности S_r при небольшом количестве членов.

В работе приводится последовательность с 896 членами и описывается способ ей использования.
