14P

Technical Memorandum No. 33-185

14P

The Role of Pseudorandom Codes in Communications

Robert C. Titsworth

FACILITY FORM 602

N64-28965 (ACCESSION NUMBER)

(THRU)

14 (PAGES)

1 (CODE)

CR-58240 (NASA CR OR TMX OR AD NUMBER)

08 (CATEGORY)

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

August 3, 1964

OTS PRICE

XEROX $ 1.60 ph.

MICROFILM $

Technical Memorandum No. 33-185

The Role of Pseudorandom Codes in Communications

Robert C. Titsworth

M. Easterling, Chief
Communications Systems Research

JET PROPULSION LABORATORY
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

August 3, 1964

Copyright © 1964
Jet Propulsion Laboratory
California Institute of Technology

Prepared Under Contract No. NAS 7-100
National Aeronautics & Space Administration

CONTENTS

The Role of Pseudorandom Codes in Communications 1

References 6

Table 1. Summary of minimax sequences 7

FIGURES

1. Autocorrelation functions of pseudorandom binary sequences: (a) pseudonoise, (b) difference set, (c) optimal-minimax 8

2. Pseudorandom sequence generator: (a) feedback type, (b) output-logic type 8

3. Sequence generation by logical combination of component pseudorandom sequences for ranging or Boolean multiplex telemetry 8

4. The single-channel ranging receiver with clock-acquiring loop 9

5. Acquisition diagram for the clock-acquiring ranging receiver 9

ABSTRACT

28965

Periodic sequences having certain inherent random-like statistics are called pseudorandom sequences. The most important randomness criterion, insofar as communications of a Gaussian channel is concerned, is the resemblance which the cyclic autocorrelation function of a sequence bears to that of a sequence of coin-tosses. The match between these two correlation functions is a function of the cycle length of the periodic code, and can be measured in degrees of phase-orthogonality. Many communications systems use this phase-orthogonality for information distinguishability in many diverse ways, depending on particular applications. This report summarizes the kinds of pseudorandom sequences, and the differing criteria under which they are studied, and indicates applications wherein they have been found useful

Author

THE ROLE OF PSEUDORANDOM CODES IN COMMUNICATIONS*

If all the different cyclic sequences composed of s different states and of period p were to be examined term by term, it is natural to suppose that some of them, over a certain portion of their period, would appear to have little organized behavior. Some of the sequences would appear to be governed by probabilities of occurrence and transition, rather than by the algorithm which deterministically produced them, so that they have a random-like behavior. On the other hand, other sequences would look neither particularly random nor particularly deterministic, and another group would seem every deterministic indeed.

In many applications it would be extremely convenient to generate sequences which only appear to be random, even if, upon closer and longer observation, certain regularities become evident.

Periodic sequences having certain structurally inherent random-like statistics are called *pseudorandom* sequences. More specifically, a pseudorandom sequence of events is one particular (deterministic) sequence which *represents* the whole ensemble of random sequences, insofar as certain of its statistics are concerned. That is, an experiment to be subjected to an ensemble of random sequences of events or numbers, in which the conclusions drawn from the output behavior are governed by this set of statistics, could equally as well be subjected to only the pseudorandom sequence, and the outcome would then be guaranteed to behave as if the entire ensemble had been tested. Other definitions of pseudorandomness can also be formulated for a given application, according to the specific requirement as to the degree of randomness.

A *pseudorandom code* is a cyclic (perhaps nonlinear) binary code with a single generator (i.e., all code words are cyclic shifts of each other), and the generator sequence satisfies certain randomness criteria. Correlation between code words is defined as the number of places where the two words agree, minus the number of places where they disagree. Since there is only one generator in the code, correlations between words are terms in the cyclic autocorrelation function of the generator sequence. The most important randomness criteria, insofar as communications in the additive Gaussian channel is concerned, is the resemblance which the cyclic autocorrelation function of a word bears to that of a sequence of coin-tosses. In this

---

* This paper was first presented at the International Symposium on Global Communications, Philadelphia, Pennsylvania, June 2-5, 1964.

discussion, we shall restrict $a_n = \pm 1$, so that the sequence autocorrelation is

$$R(m) = \sum_{n=1}^{p} a_n a_{n+m}.$$

Because of their noise-like correlation function, such codes are nearly orthogonal ones and, in some cases, even *beyond* orthogonal (*i.e.*, all "out-of-phase" autocorrelation values are nonpositive).

Certain pseudorandom sequences are ideal in that the correlation values between distinct shifts are maximally distinguishable from the no-shift value (Fig. 1a). These are the so-called *pseudonoise* (Ref. 1) sequences, and there are 5 known classes of them, all of whose periods p are congruent to 3 modulo 4: (1) linear shift-register sequences, period $p = 2^n - 1$, (2) the Gordon-Mills-Welch extensions of these, also of period $p = 2^n - 1$, (3) Legendre (or quadratic residue) sequences for prime $p \equiv 3 (\mathrm{mod}\ 4)$, (4) twin-prime (or Jacobi residue) sequences, $p = t(t + 2)$, when both t and $t + 2$ are prime, and (5) Hall sequences, p a prime of the form $4x^2 + 27$.

Used as telemetry codes, it has recently been shown (Ref. 2) that, when bandwidth is no constraint, pseudonoise codes are optimal. Because the available periods of such sequences of this ideal type grow relatively sparse as p grows large, it is often desirable to include a wider class of sequences into what we term "pseudorandom."

Containing the ideal class is the set of sequences which possess two-level autocorrelation functions but not necessarily of the ideal type (Fig. 1b). These sequences correspond to difference sets and certain symmetric block designs (Ref. 3).

Another class which is under recent consideration, and which also includes the ideal set, is the set of "optimal" sequences (Ref. 4). A code belongs to this class if, for a fixed but arbitrary period p, the code is most nearly ideal (Fig. 1c, for example). The maximum out-of-phase autocorrelation value is minimized over all sequences having period p, and this maximum occurs the least number of times per period.

Still another class to consider is the set of sequences which, while perhaps not optimal, yet possess out-of-phase autocorrelation values whose maximum values are less than or equal to $p (\mathrm{mod}\ 4)$. This is the *least possible value* for their particular period (if the sequence is not pseudonoise). They are "minimax" sequences. Some of them (Fig. 1c) generate codes which are also transorthogonal.

A minimax sequence is easily recognized, for all one must do is compute its autocorrelation function and check to make sure that its maximum out-of-phase value is the proper value. Judging whether a given sequence is optimum, however, is somewhat more of a problem, in that the form of the best autocorrelation function is often unknown. Perhaps the strongest result (Ref. 4) at present is that *if a sequence* $\{a_n\}$ *has a balance of* + 1's *and* − 1's *per period, and if the number of different out-of-phase autocorrelation values is 2 or less, minimally separated* (by 4), *then the sequence is both optimum and minimax.*

Several analytic and iterative methods by which optimal and minimax sequences can be made have been studied. It has been found that the quadratic residue sequences for all prime-length periods are minimax-optimal, and that the Jacobi-residue sequences for periods equal to the product of primes separated by 2, 4, or 6 give minimax sequences. For a separation of 2 these are pseudonoise. For separation 4, the autocorrelation function has only 3 levels, with minimum separation, but an imbalance of 3. For separation 6, there are 4 levels, each with minimum separation. Various cases in which shorter sequences have been combined term-by-term, or combined in a Kronecker product, also produce many minimax, near-optimal (or optimal?) sequences of longer periods.

Iterative computer methods (Ref. 5) have been used to find optimal and minimax sequences of a given period when theoretic considerations have failed to produce results. These methods start with an arbitrary or randomly chosen sequence of the proper period, and change elements, one at a time, until any further change would result in a worse sequence. The goodness criterion here is taken as the sth even moment of the autocorrelation function about some value, say −1, −2, etc. These methods produce minimax sequences (many of which are also optimum) for every period length up through 63, with the exception of $p = 40$, 48, 52, and 56 (see Table 1). Note also from Table 1 that the optimal-length 14 sequence has 3-level autocorrelation but is *not* balanced, which indicates that balance is not necessary to optimality. The optimal-length 27 sequence has maximum out-of-phase correlation equal to 3, and is the first sequence whose length is of the form $4N + 3$ not to be pseudonoise. The minimax sequence of length 36 was found by backtrack programming; this approach has not yet been applied to the cases $p = 40$, 48, 52, or 56.

It has not yet been shown that it is impossible to have minimax sequences of period $4N$ for any N, but it has been shown (Ref. 6) that there are none of the difference-set type, except for $N = 1$, up through $N = 36 (p = 144)$ — with a conjecture that there are no more for *any* N.

The fact that any periodic sequence is readily generated by (perhaps nonlinear) feedback shift-register techniques (Ref. 7) is, at this point, extremely fortunate. There are generally two methods used for such

generation, depending on the flexibility of the application desired and the ease with which each method applies itself to a particular case. The first method (Fig. 2a) is one in which all computation is done in the feedback logic itself. The other method eases some of the burden on the feedback logic and places it on the output logic (Fig. 2b). The feedback logic then merely generates a sequence of the proper period, and the output logic transforms it into the desired one.

Certain combinations of several pseudorandom sequences by a Boolean function (Fig. 3) yield extremely long codes with amazing synchronization properties, even in extremely noisy environments (Ref. 8). These Boolean combination codes are also applicable to telemetry systems wherein commutation is replaced by a passive logic function (Ref. 9). All that really need be noted here is that the component codes at the input of the logic in one system are data codes and, in the other, synchronization words. The shift-register generators can also be viewed this way: namely, that all inputs to the logic are cyclic shifts of the same sequence.

In the unconstrained channel with white, additive Gaussian noise, it has long been recognized that the best possible ranging receiver is a set of correlators, or filters matched to each possible (assumed discrete) time-shifted return of the transmitted code. For a long code, this requires a prohibitive amount of receiver equipment, and, with only one correlator, serial operation requires an extremely long time to determine range.

Therefore, when the amount of receiver equipment is limited, matched filtering is no longer the optimal detection scheme. A better scheme is one which, by the use of a Boolean function, combines several "component" sequences to generate the transmitted signal. The receiver (Fig. 4) quickly acquires the phase of each component separately and computes the range therefrom. This method was first suggested by Golomb (Ref. 10), and an operational model, built by Easterling (Ref. 11) had amazing success ranging the Courier satellite (Ref. 12). Easterling's receiver made use of the fact that one of the components was a clock sequence, and the receiver synchronized itself to the component.

These Boolean combination codes allow the determination of range as one of $p_1 \, p_2 \cdots p_n$ values after searching only through $p_1 + p_2 \cdots + p_n$ of them. The ratio of the time required to acquire the phase of a code by serial cross-correlation with each of its components to the time required for serial correlation with the code itself can be made extremely small. In fact, a code long enough to measure the range of a spacecraft somewhere within an ambiguity region of 10^4 km to an accuracy of a few tens of meters requires a transmitted code of about 10^5 in length, made of 5 short sequences, at a saving factor of about 1000 over the longer method.

The acquisition diagram for such a scheme is shown in Fig. 5. Besides the number of components and their periods, the Boolean function itself may be optimized with certain parameters under the control of the designer. The best Boolean function is a majority-vote logic in which the degree of majority required is set by the design parameters. For the clock-loop receiver, these design parameters are the initial value of clock-loop correlation and the amount by which this correlation drops when the second component is sought.

A random number generator for digital computers based on a linear pseudonoise sequence has recently been programmed (Ref. 13). The output sequence of numbers fulfills the requirements of speed, uniform distribution, and "whiteness" (uncorrelated samples) needed for many Monte Carlo experiments.

To indicate in detail the role pseudorandom codes play in all communications systems would be impossible here. But most of these systems make use of the "phase-orthogonality" of pseudorandom sequences, and some of them can be listed: (1) search and tracking radar, (2) range-gated radar for precision planetary and lunar work, (3) precision ranging of planetary and lunar spacecraft, (4) coded telemetry, (5) multiplexed telemetry by Boolean functions, (6) data synchronization, and self-acquirable codes, and (7) multiple-address key sequences.

REFERENCES

1. Golomb, S. W., *Sequences with Randomness Properties,* The Martin Co., Baltimore, 1955.

2. Balakrishnan, A. V., "A Contribution to the Sphere-Packing Problem of Communications Theory," *J. Math. Anal. and Appl.,* Vol. 3, 1961, pp. 485-506.

3. Hall, M., Jr., *Projective Planes and Related Topics,* published lecture notes, California Institute of Technology, Pasadena, 1954.

4. Titsworth, Robert C., "Optimum and Minimax Sequences," *Proc. Int. Telem. Conf.,* London, 1963, pp. 581-589.

5. Titsworth, Robert C., *Correlation Properties of Cyclic Sequences,* Ph. D. Dissertation, California Institute of Technology, Pasadena, 1962.

6. Turyn, R. J., *Optimal Codes Study – Final Report,* Sylvania Electronic Systems, Waltham, Mass., 1960.

7. Golomb, S. W., Welch, L. R., and Goldstein, R. M., *Cycles from Non-Linear Shift-Registers,* Report 20-389, Jet Propulsion Laboratory, Pasadena, August 31, 1959.

8. Titsworth, Robert C., "Optimal Ranging Codes," *Trans. PTG-SET,* Vol. SET-10, No. 1, March 1964.

9. Titsworth, Robert C., "A Boolean Function Multiplexed Telemetry System," *Trans. PTG-SET,* Vol. SET-9, No. 2, June 1963, pp. 42-45.

10. Golomb, S. W., "Deep Space Range Measurement," Research Summary No. 36-1, Jet Propulsion Laboratory, Pasadena, 1960, pp. 39-42.

11. Easterling, M. F., "Acquisition Ranging Codes and Noise," Research Summary, No. 36-2, Jet Propulsion Laboratory, Pasadena, 1960, pp. 31-36.

12. Easterling, M. F., "A Skin Tracking Radar Experiment Involving the Courier Satellite", *IRE Transactions of PTG-SET,* June 1962, pp. 76-84.

13. Titsworth, Robert C., "Random Numbers Generated by Linear Recurrence, Mod 2," Space Programs Summary No. 37-27, Vol. IV, June 30, 1964.

Table 1. Summary of minimax sequences

p	R_M	R_{min}	D	N	No. of levels	Generation method
3	−1	−1	1	0	2	linear shift register (opt)
4	0	−4	0	2	3	2 ⊗ 2 (opt)
5	1	−3	1	2	3	quadratic residue (opt)
6	2	−2	0	1	3	3 ⊗ 2 (opt)
7	−1	−1	1	0	2	linear shift register (opt)
8	0	−4	0	5	3	$s = 1$ (opt)
9	1	−3	1	4	3	$s = 1$ (opt)
10	2	−2	0	4	3	$s = 1$ (opt)
11	−1	−1	1	0	2	quadratic residue (opt)
12	0	−4	0	8	3	$s = 1$ (opt)
13	1	−3	1	6	3	$s = 1$ (opt)
14	2	−2	2	4	3	$s = 1$ (opt)
15	−1	−1	1	0	2	linear shift register (opt)
16	0	−4	0	11	3	$s = 1$ (opt)
17	1	−3	1	8	3	$s = 1$ (opt)
18	2	−2	0	4	3	$s = 1$ (opt)
19	−1	−1	1	0	2	quadratic residue (opt)
20	0	−4	0	14	3	$s = 1$ (opt)
21	1	−3	1	10	3	$s = 1$ (opt)
22	2	−2	0	5	3	$s = 1$ (opt)
23	−1	−1	1	0	2	quadratic residue (opt)
24	0	−4	4	21	3	$s = 1$ (opt?)
25	1	−3	1	12	3	$s = 1$ (opt)
26	2	−2	0	6	3	$s = 1$ (opt)
27	3	−5	1	2	4	$s = 1$ (opt)
28	0	−4	2	21	3	4 * 7 (opt?)
29	1	−3	1	14	3	quadratic residue (opt)
30	2	−2	2	8	3	$s = 4$ (opt?)
31	−1	−1	1	0	2	linear shift register (opt)
32	0	−8	0	24	4	$s = 1$ (opt?)
33	1	−3	3	18	3	$s = 2$ (opt?)
34	2	−6	0	10	4	$s = 4$
35	−1	−1	1	0	2	Jacobi (opt)
36	0	−4	4	27	3	backtrack (opt?)
37	1	−3	1	18	3	$s = 1$ (opt)
38	2	−6	0	11	4	$s = 4$
39	3	−5	3	6	4	$s = 2$
40						
41	1	−3	1	20	3	quadratic residue (opt)
42	2	−6	0	14	4	$s = 4$
43	−1	−1	1	0	2	quadratic residue (opt)
44	0	−4	2	33	3	11 * 4 (opt?)
45	1	−7	1	24	4	$s = 4$
46	2	−6	2	18	4	$s = 2$
47	−1	−1	1	0	2	quadratic residue (opt)
48						
49	1	−7	1	36	3	7 ⊗ 7
50	2	−6	2	16	4	$s = 4$
51	3	−5	3	12	4	$s = 2$
52						
53	1	−3	1	26	3	quadratic residue (opt)
54	2	−6	4	21	4	$s = 2$
55	3	−5	5	10	4	Jacobi (opt?)
56						
57	1	−19	1	36	4	19 ⊗ 3
58	2	−6	0	20	4	$s = 4$
59	−1	−1	1	0	2	quadratic residue (opt)
60	0	−4	2	45	3	15 * 4 (opt?)
61	1	−3	1	30	3	quadratic residue (opt)
62	2	−6	0	25	4	$s = 4$
63	−1	−1	1	0	2	linear shift register (opt)

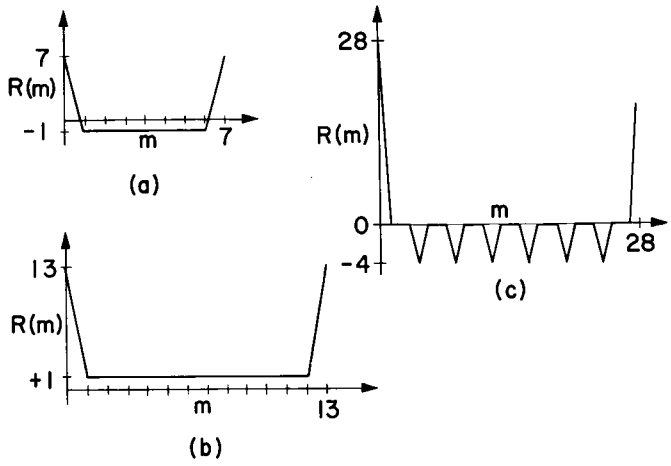
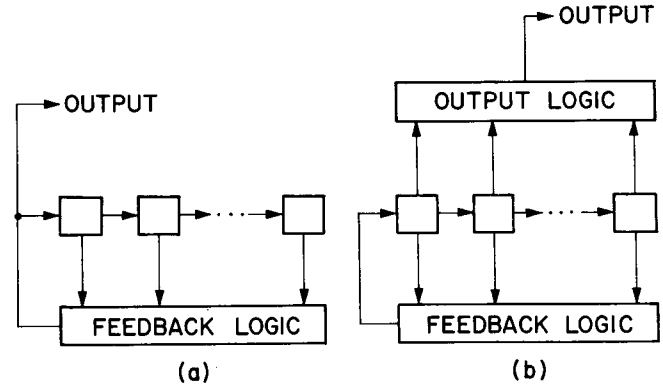


Fig. 1. Autocorrelation functions of pseudorandom binary sequences:
(a) pseudonoise
(b) difference set
(c) optimal-minimax

Fig. 2. Pseudorandom sequence generator:
(a) feedback type
(b) output-logic type



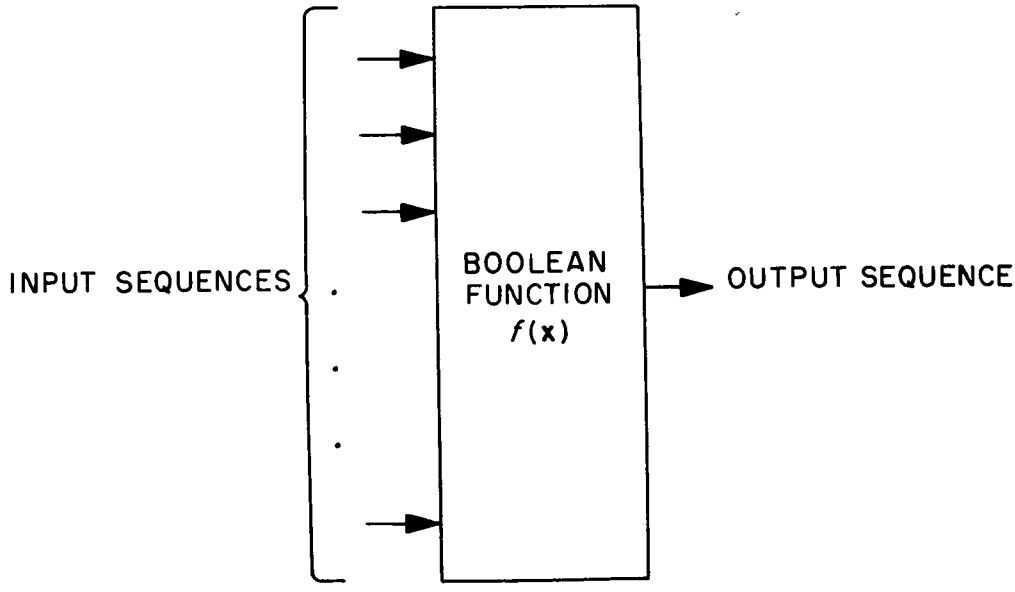


Fig. 3. Sequence generation by logical combination of component pseudorandom sequences for ranging or Boolean multiplex telemetry

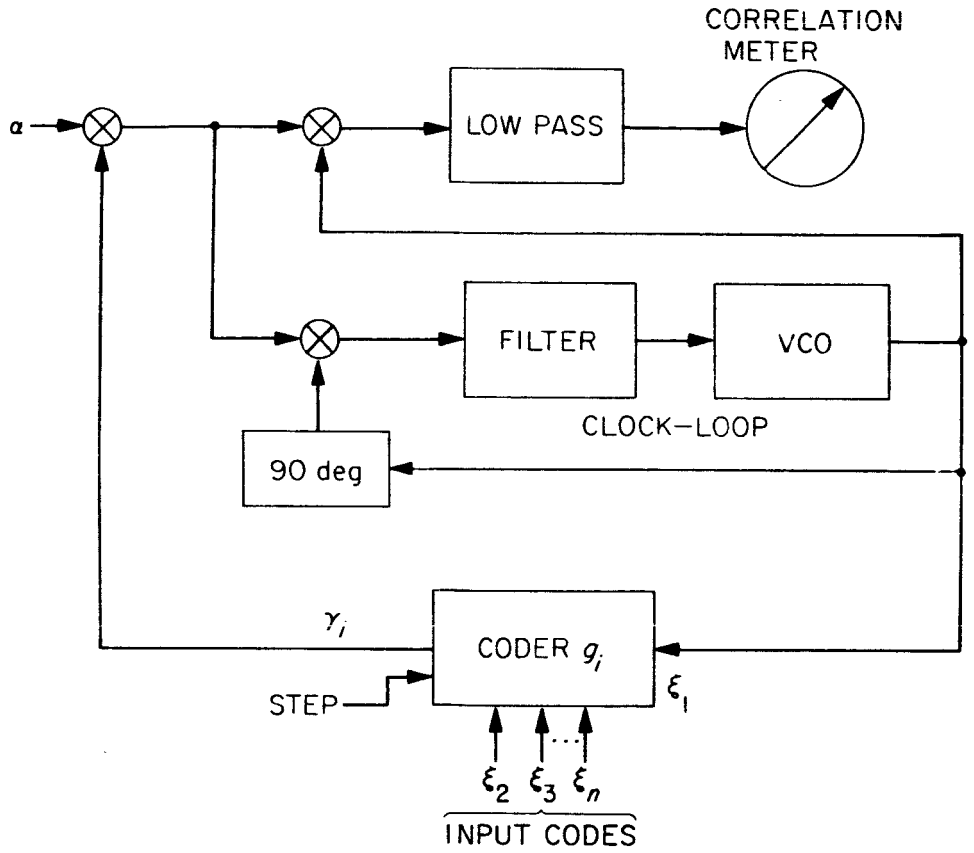


Fig. 4. The single-channel ranging receiver with clock-acquiring loop

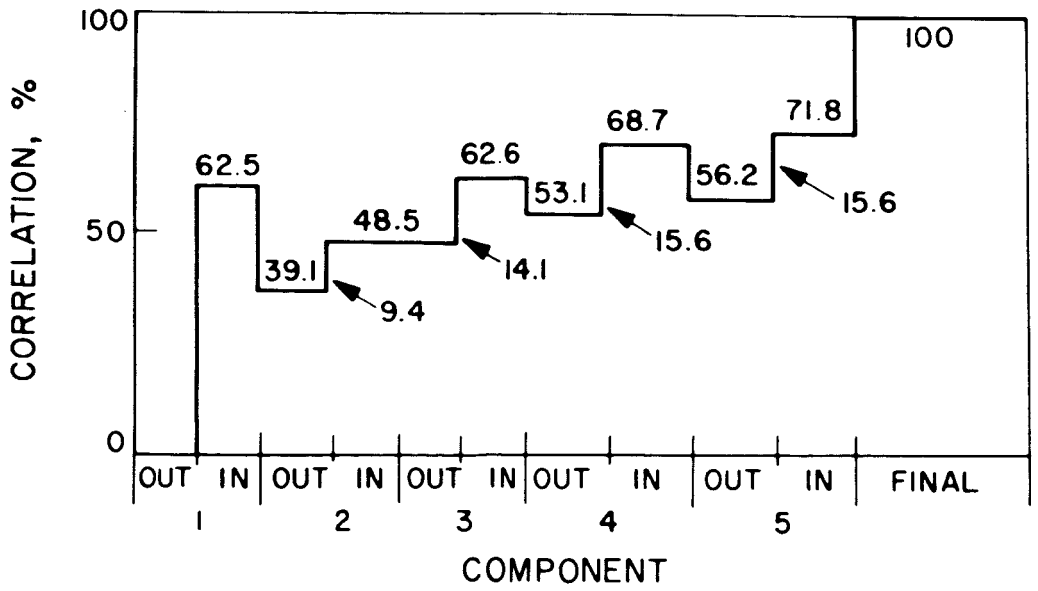


Fig. 5. Acquisition diagram for the clock-acquiring ranging receiver