

THE UNIVERSITY OF MICHIGAN  
OFFICE OF RESEARCH ADMINISTRATION  
ANN ARBOR

THE THEORY OF ELECTRONIC RANDOM SELECTORS

Technical Report No. 115

2899-37-T

Cooley Electronics Laboratory  
Department of Electrical Engineering

By: G. A. Roberts

Approved by:



A. B. Macnee

Project 2899

TASK ORDER NO. EDG-3  
CONTRACT NO. DA-36-039 sc-78283  
SIGNAL CORPS, DEPARTMENT OF THE ARMY  
DEPARTMENT OF THE ARMY PROJECT NO. 3A99-06-001-01

December 1960



## TABLE OF CONTENTS

	Page
LIST OF ILLUSTRATIONS	iv
ABSTRACT	v
1. INTRODUCTION	1
2. THEORY OF ELECTRONIC RANDOM SELECTORS	1
2.1 Preliminary Discussion	1
2.2 Randomness Requirements	2
2.3 Probability-Control Circuit	3
2.3.1 Probability Control for Equal Probabilities	8
2.3.2 Probability Controls for Unequal Probabilities	8
2.4 Randomness Generation	11
2.4.1 Satisfaction of Randomness Requirement 3	11
2.4.2 $\epsilon$ and $Q$ for Several Distributions	13
2.4.3 The Satisfaction of Randomness Requirements 1 and 2	15
2.4.4 Determination of Minimum Allowable Time Between Questions	16
2.4.5 Random Selector With Random Source as an Integral Part of the Probability Control	17
2.5 Predictable Binary-Sequence Generators	19
3. SUMMARY	21
APPENDIX A	23
A.1 Derivation of $\epsilon$ and $Q$ for Uniform Distribution	23
A.2 Derivation of $\epsilon$ and $Q$ for Triangular Distribution	23
A.3 Derivation of $\epsilon$ and $Q$ for Exponential Distribution	25
A.4 Derivation of $\epsilon$ and $Q$ for Exponential Distribution Alternated	26
A.5 Derivation of $\epsilon$ and $Q$ for Normal Distribution	28
A.6 Derivation of $\epsilon$ and $Q$ for $\chi^2$ Distribution with $2N$ Degrees of Freedom	29
REFERENCES	30
DISTRIBUTION LIST	31

## LIST OF ILLUSTRATIONS

Figure		Page
1	Random selector	2
2	Transformation of the infinite time-domain into a finite space by the spinning disk	5
3	Probability-density function, $g(x)$ , over the finite space vs. $x$	6
4	Probability-density function, $f(t)$ , in the infinite time domain	7
5	The probability-density function, $g(t)$ , in the finite time domain obtained from Fig. 4 by rotating the disk at different speeds	7
6	Equally-likely random selector with $N$ possibilities	8
7	Binary random selector with adjustable probability	9
8	Binary random selector with continuously adjustable probability control	9
9	Waveform for voltage-adjustable random selector for small probability range	10
10	Probability-density curve wrapped around a cylinder	13
11	Peak-to-peak fractional error of the wrap-around probability-density as a function of the wrap-around factor $K$	14
12	Probability-density function	16
13	Full-wave rectified gaussian noise	17
14	Density functions for rectified and unrectified Gaussian noise	18
A.1	Uniform distribution	23
A.2	Triangular distribution	24
A.3	Exponential distribution	25
A.4	Exponential distribution alternated	26
A.5	Normal distribution	28
A.6	$\chi^2$ distribution with $2N$ degrees of freedom	29

### ABSTRACT

The basic theory of electronic random selectors is presented. An electronic random selector is a completely electronic device that makes a truly random selection of one item from a set of items.

Randomness requirements, probability control circuits, and randomness generation are discussed. A brief comment on predictable binary sequence generators is included.



## THE THEORY OF ELECTRONIC RANDOM SELECTORS

### 1. INTRODUCTION

In 1953 when the development of N. P. Psytar (Noise Programed Psycophysical Tester and Recorder) was begun at the University of Michigan there were no electronic machines which could produce truly random selections in response to a given request. Thus, as a part of the overall N. P. Psytar program electronic random selectors were developed.

An electronic random selector can usually be separated into two parts---a probability control circuit and a randomness generator. In line with this breakdown, the organization of this report consists of a discussion of the randomness requirements, probability control, randomness generation, and a brief comment on predictable binary-sequence generators.

### 2. THEORY OF ELECTRONIC RANDOM SELECTORS

#### 2.1 Preliminary Discussion

The input to a random selector is a request that a selection be made. This request is called a "question," and the time at which it is made is called the "question time." The output of a random selector is a selection from a set of possibilities. The probability of selection for each of the members of a set of possibilities is established prior to the "question time." Following this, the random selection is made in accordance with the established probabilities. For the purpose of analysis,

then, any random selector or random-number generator can be thought of as having two main parts: a probability control; and a randomness generator (See Fig. 1 ).

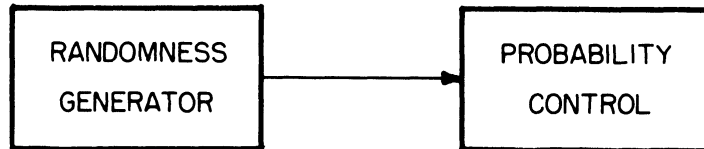


Fig. 1. Random selector.

A set of possibilities for a random selector might be, for example, the letters of the English alphabet; and the probability of any particular letter being selected could be equal to the frequency of its occurrence in the language.

The balance of this section is devoted to the expansion and clarification of the foregoing material in the following order: first, the randomness requirements are set forth; second, the theory of the probability control is described with the assumption that the input is a random function of time; third, the theory of generating this random input is described; and fourth, predictable binary-sequence generators are mentioned.

## 2.2 Randomness Requirements

In general three requirements must be met if selections are to be random:

1. The selections must be independent of one another. This means that the a priori probability of any selection must be the same as the conditional probability for all selections.
2. The selections must be independent of their applications. For this to be meaningful a universe of discourse must be



specified. Within this universe there is an experiment or test with events from which random selections are required. That the selections must be independent of their applications means that the events within this universe and the selections must be independent. Thus, the probability of any selection from the random selector must remain unchanged by any knowledge concerning the experimental or test events.

3. For each "question" one and only one selection can be made from  $N$  possibilities.<sup>1</sup> The probability of each of the  $N$  possibilities must depend on only the probability control. In effect, this requirement means that probabilities should not change unless the probability control is changed.

These requirements have been set forth to give sequences of selections that do not have predictable patterns and that have stable probabilities.

### 2.3 Probability-Control Circuit

The probability-control circuit is a device which, upon receiving a "question" input, makes one selection from a set of  $N$  possibilities. The probability of each selection is determined by the setting of each probability control. In some circuits the probabilities will be predetermined when the circuit is designed; manually operated controls will be provided in others so that an operator may adjust the probabilities.

It is meaningless to talk of a probability-control circuit if nothing is said of randomness. For instance, by improperly designing a random selector it would be possible to always make the same selection independently of the probability setting for that selection. A proper design

---

1. For other types of outputs, logic circuits can be employed to obtain the desired characteristics.

requires that the following conditions be met: (1) If the probability-control circuit does not have a built-in random source, then the "question times" must be randomly distributed in time. (In effect, the probability-control circuit transforms the random "question times" into random spatial selections.) (2) If the probability-control circuit has a built-in random source, then the "question times" need not be randomly distributed in time. But, depending upon the nature of the random source, certain restrictions on the input may be necessary.

Any random selector and probability control is dependent on time-varying factors. For this reason it is possible to describe all probability controls as spinning disks. This means that an analogy can be made between any electronic probability-control circuit and an appropriate mechanical spinning disk<sup>1</sup> (Refs. 1, 2).

The typical operation of a spinning-disk probability control is as follows: The disk has N segments, one for each selection, and is normally spinning. A selection is obtained by stopping the disk at a random time. The segment indicated by a fixed arrow indicates the selection. A set of selections is obtained by repeating this procedure for each additional member of the set.

Greater attention will now be given to the general theory of the probability of a selection. The above ideas should be kept in mind as background material, but they should not be allowed to confuse the new ones.

The spinning disk may be considered as a device which transforms a part or all of the infinite time-domain into some finite space. A

---

1. Mechanical spinning-disk random selectors with which many people are familiar are roulette wheels and carnival wheels.

graphical interpretation is shown in Fig. 2. If the disk spins at a uniform rate it transforms the infinite time domain into a finite time domain

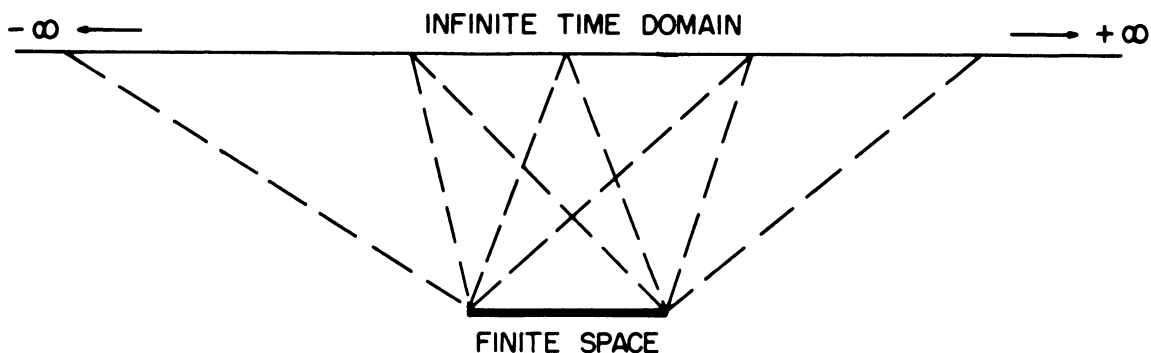


Fig. 2. Transformation of the infinite time-domain into a finite space by the spinning disk.

of duration  $T$ . The time for the disk to make one revolution is called the modulus period and is symbolized by  $T$ .

There is associated with each of the possible random selections a segment in the finite space. These segments are nonoverlapping because they correspond to the segments on the disk, which are nonoverlapping. A "question time" occurs in the infinite time domain, and the disk is stopped at this "question time." Corresponding to this time in the infinite space there is a point in the finite space which is the transform of the "question time." The segment of the finite space containing this point is the selection.

Over the finite space there is a probability-density distribution,  $g(x)$ , of the stopping point. An arbitrary function,  $g(x)$ , is shown in Fig. 3. The shape of the probability-density distribution is, of course, a function of the design of the equipment. More will be said about the actual formation of this probability-density distribution in section 2.3.

The segments shown in Fig. 3 identify the parts of the finite space corresponding to the possible selections. The probability of selecting

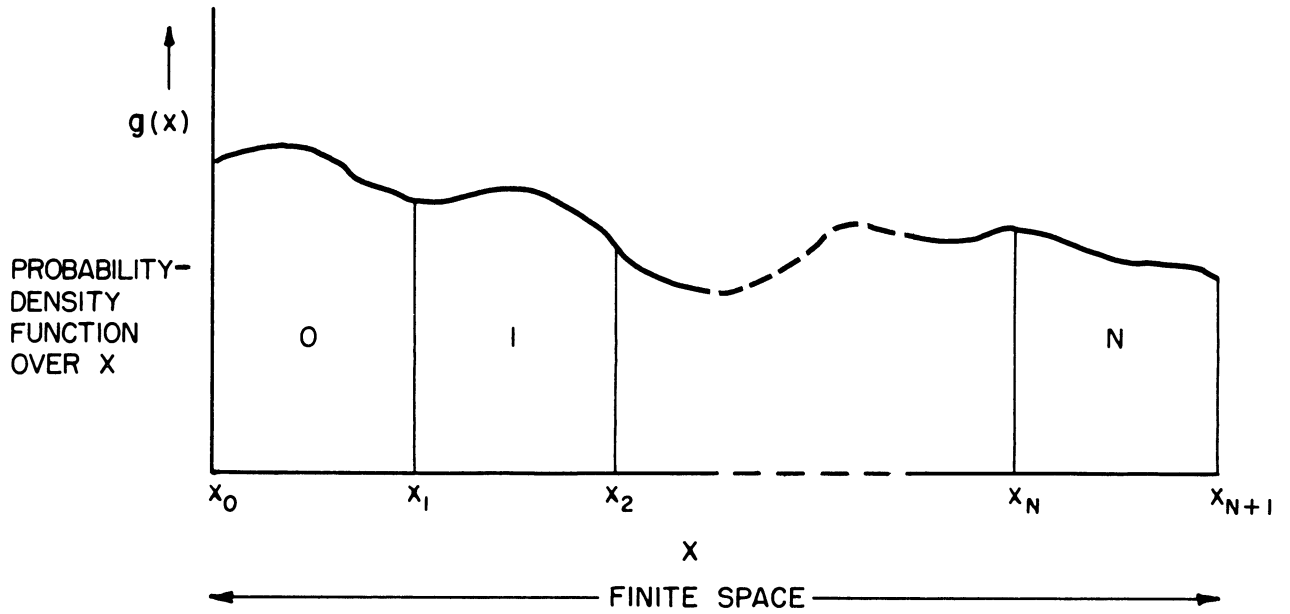


Fig. 3. Probability-density function,  $g(x)$ , over the finite space vs.  $x$ .

the  $i$ th segment,  $p_i$ , is given by

$$p_i = \int_{x_i}^{x_{i+1}} g(x) dx \quad (2.1)$$

where

$$\int_{x_0}^{x_{n+1}} g(x) dx = 1$$

and

- $x_i$  is the abscissa of the left-hand side of the  $i$ th segment,
- $x_{i+1}$  is the abscissa of the right-hand side of the  $i$ th segment,
- $g(x)$  is the probability-density function of the stopping point in the finite space, and
- $p_i$  is the probability of the  $i$ th segment being selected.

If the disk is spinning at a uniform rate, the finite space is a finite

time domain and  $x$  may be replaced by  $t$ .

The probability-density function,  $g(x)$  or  $g(t)$ , results from the transformation of some other probability-density function,  $f(t)$ , in the infinite time domain into the finite space.

Suppose that in the infinite time domain  $f(t)$  is described by the function in Fig. 4. Further suppose that a spinning disk has a constant speed and is phased such that the leading edge of the "0" segment coincides with  $t_1$ .

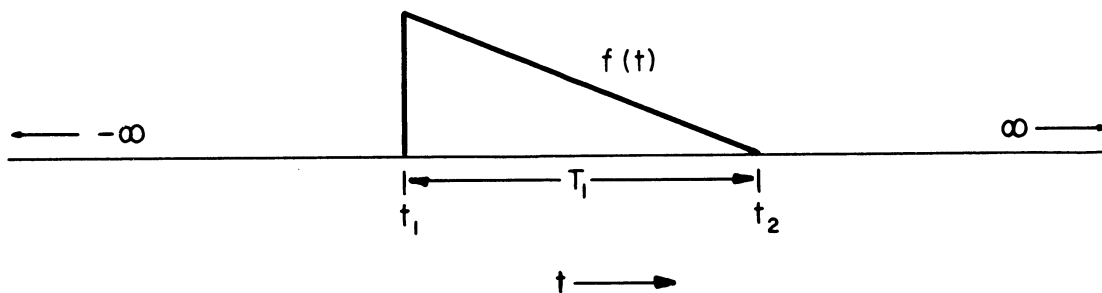


Fig. 4. Probability-density function,  $f(t)$ , in the infinite time domain.

coincides with  $t_1$ . The effect on  $g(t)$  of the disk rotating at three different speeds is shown in Fig. 5, where  $T$  is the time for one rotation. It should be obvious from these curves that the probability of a selection is influenced by the speed of rotation of the disk relative to the probability-density function  $f(t)$  for the particular conditions of the example. If it is possible to obtain a probability-density function  $g(t)$  in the

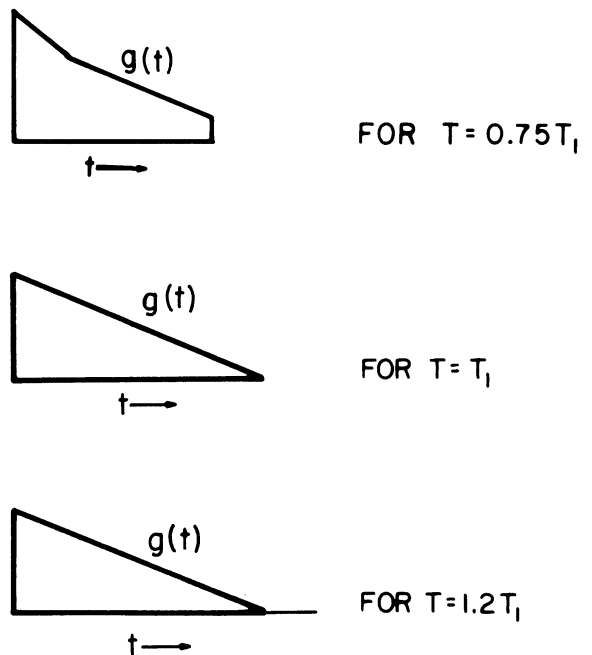


Fig. 5. The probability-density function,  $g(t)$ , in the finite time domain obtained from Fig. 4 by rotating the disk at different speeds.

finite space that is essentially uniform and not influenced by small changes in the speed of the disk, then a satisfactory probability control which will have stable probability settings can be designed. The method of obtaining such a uniform distribution is described in the section on randomness generation. For the present discussion it is assumed that a uniform density function is available in the finite space.

2.3.1 Probability Control for Equal Probabilities. The spinning-disk probability control can be realized electronically in a number of ways. If  $N$  equally-likely selections are needed, then a modulus- $N$  counter (i.e., a counter with  $N$  states, 1, 2, 3, . . .  $N$ ) driven by a cyclic pulse generator is one of the best realizations (see Fig. 6).

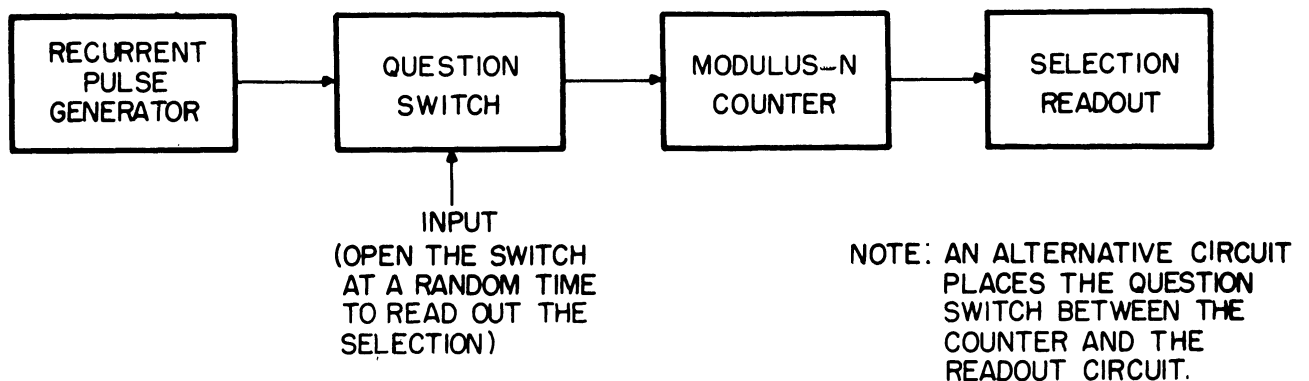


Fig. 6. Equally-likely random selector with  $N$  possibilities.

2.3.2 Probability Controls for Unequal Probabilities. If a binary selector with an adjustable probability is required, a modulus- $N$  counter driven by a recurrent pulse generator with a flip-flop readout can be used. If the flip-flop is placed in state A at the end of count  $N$  (i.e., just preceding count 0) and in state B at the end of count  $M$ , then the probability of selection A,  $P(A)$ , is

$$P(A) = \frac{M}{N} \quad (2.2)$$

and the probability of selection B,  $P(B)$ , is

$$P(B) = \frac{N-M}{N} = 1 - P(A) \quad (2.3)$$

assuming, of course, that  $f(t)$  is uniform. Note that the smallest increment of probability adjustment is  $1/N$ . See Fig. 7 for a block diagram.

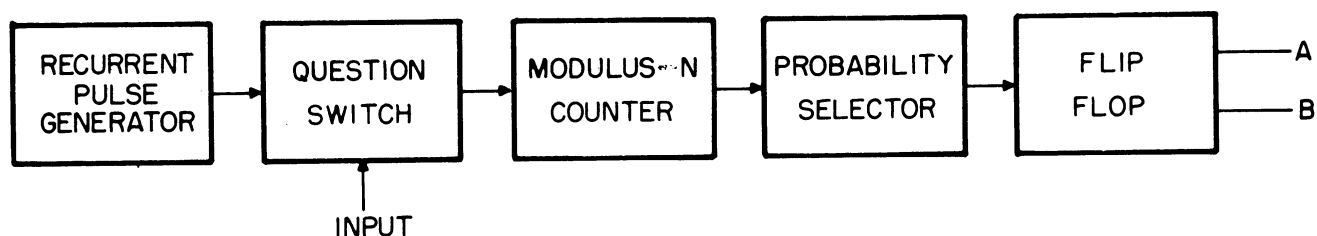


Fig. 7. Binary random selector with adjustable probability.

Continuous probability control may be desired in some applications. A realization for a spinning disk of this type may consist of a cyclic sawtooth generator, a Schmidt-trigger circuit, and a flip-flop (see Fig. 8). The probability of a selection A,  $P(A)$ , is given by Eq. 2.4,

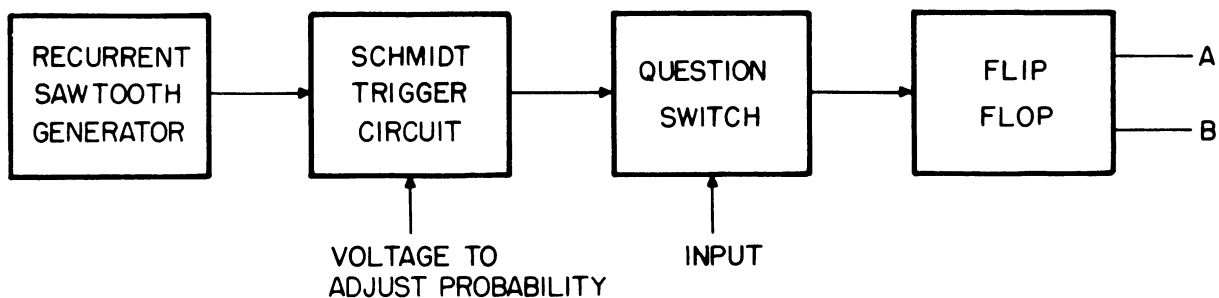


Fig. 8. Binary random selector with continuously adjustable probability control.

provided that the sawtooth waveform is linear and has a negligible retrace time.

$$P(A) = \frac{e_s - E_1}{E_2 - E_1} \quad (2.4)$$

where

$e_s$  is the trigger level of the Schmidt circuit ( $e_s$  is the parameter used to adjust the probability),

$E_2$  is the peak voltage of the sawtooth, and

$E_1$  is the minimum voltage of the sawtooth.

If the desired relationship between probability control voltage and probability is nonlinear, then the desired result can generally be achieved by modifying the waveform of the sawtooth generator.

If the probability range to be controlled by the voltage is small, then the waveform of the sawtooth generator should be modified as shown in Fig. 9.

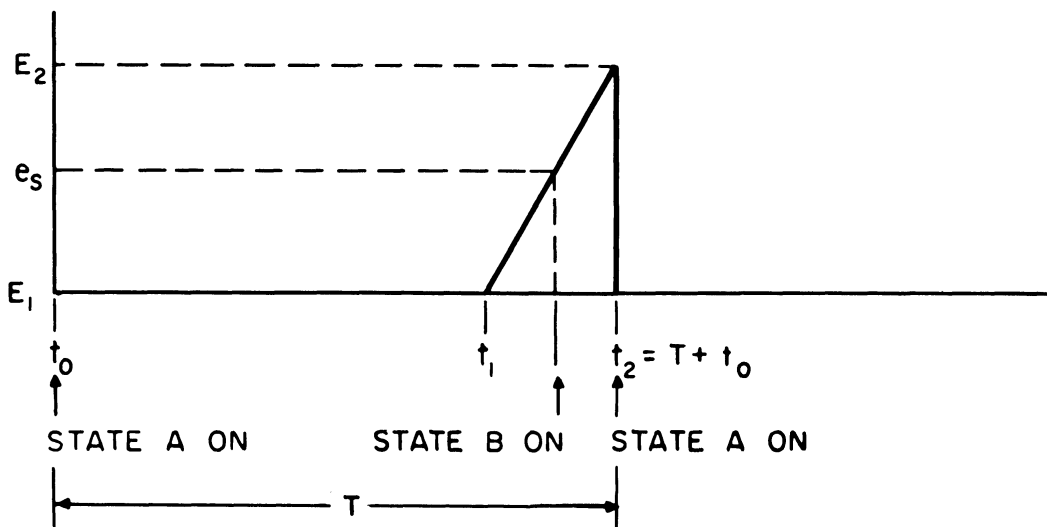


Fig. 9. Waveform for voltage-adjustable random selector for small probability range.



The probability of selection A,  $P(A)$ , for the waveform of Fig. 9 is

$$P(A) = \frac{t_1}{T} + \frac{e_s - E_1}{E_2 - E_1} \cdot \frac{t_2 - t_1}{T} \quad (2.5)$$

In general the binary adjustable-probability random selectors can be extended to have more possible selections by means of simple logical circuits.

It is possible to combine two or more binary random selectors in logical switching circuits to obtain probabilities smaller or larger than those readily achieved with the above random selectors. When this is done it is necessary that independent random sources be used for the individual binary random selectors.

#### 2.4 Randomness Generation

The randomness generator is responsible for the randomness of a random selector. Three requirements must be met.

1. The randomness source, in conjunction with the question input, must produce an input to the probability control in such a manner that the selections are independent of one another.
2. Similarly, the probability control input must be such that the selections are independent of their applications.
3. If the probability control does not contain a random source as an integral part, then the probability control settings should not be influenced by the choice of a randomness generator.

2.4.1 Satisfaction of Randomness Requirement 3. If  $g(t)$  is uniform, then requirement 3 is satisfied.

The combination of the question operation and the randomness source will produce some distribution  $f(t)$  in the infinite time domain. It is necessary to know whether  $f(t)$  produces a uniform distribution for  $g(t)$  in the finite time domain. When  $f(t)$  is segmented by the probability control, it is transformed to  $g(t)$ . This technique of segmenting  $f(t)$ , or for illustration wrapping it around a cylinder, is called the wrap-around effect.<sup>1</sup>

As an illustration of the wrap-around effect consider a cylinder of circumference  $T$  with a plot of  $f(t)$  to the same time scale around the cylinder as shown in Fig. 10. The sum of all the ordinates around the cylinder is  $g(t)$ . If  $f(t)$  is of the proper character, then  $g(t)$  will approach a uniform ordinate.

A measure is required to represent the closeness to a uniform distribution. The fractional peak-to-peak error  $\epsilon$  is such a measure and is defined as

$$\epsilon = \frac{g(t)_{\max} - g(t)_{\min}}{g(t)_{\text{avg}}} \quad (2.6)$$

Since the area under  $g(t) = 1$ , it is readily seen that  $g(t)_{\text{avg}} = 1/T$ . For convenience the period  $T$  will not be used. Instead, the period or circumference of the cylinder will be described as  $K\sigma$ , where  $K$  is a constant and  $\sigma$  is the standard deviation of  $f(t)$ . As a further simplification  $K$  will be used to represent the period; then comparisons can readily be made between different values of  $f(t)$ .

Thus the defining equation for  $\epsilon$  is

---

1. T. G. Birdsall originated this analysis.

$$\epsilon = K \left[ g(t)_{\max} - g(t)_{\min} \right] \quad (2.7)$$

The quality factor  $Q$  is defined as

$$Q = 1/\epsilon \quad (2.8)$$

Note that  $Q$  approaches  $\infty$  as  $g(t)$  approaches a uniform distribution.

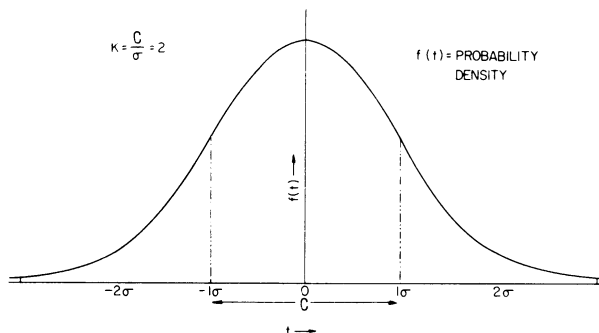
2.4.2  $\epsilon$  and  $Q$  for Several Distributions. The maximum value of the fractional peak-to-peak error,  $\epsilon$ , is derived for the following distributions:

1. Uniform distribution.
2. Triangular distribution.
3. Exponential distribution.
4. Exponential distribution alternated.
5. Normal distribution.
6.  $\chi^2$  distribution with  $N$  degrees of freedom.

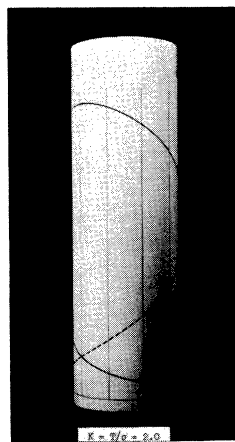
See Appendix A for the derivations.

The results of these derivations are plotted in Fig. 11, with  $\epsilon$  as a function of  $K$  for  $\sigma = 1$ .

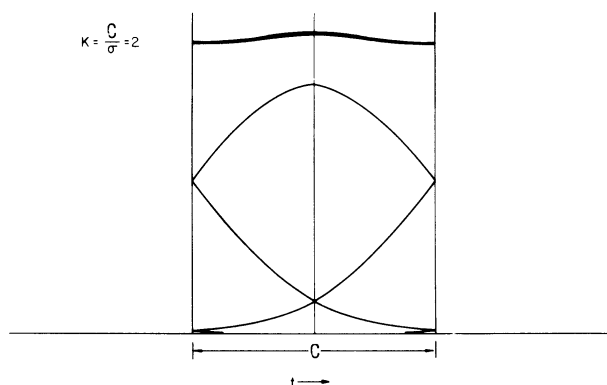
These curves may be somewhat deceptive; therefore particular attention should be given to the



(a) Segmented normal delay distribution function.



(b) Cylindrical wrap-around representation.



(c) Wrap-around effect for a normal delay distribution function.

Fig. 10. Probability-density curve wrapped around a cylinder.

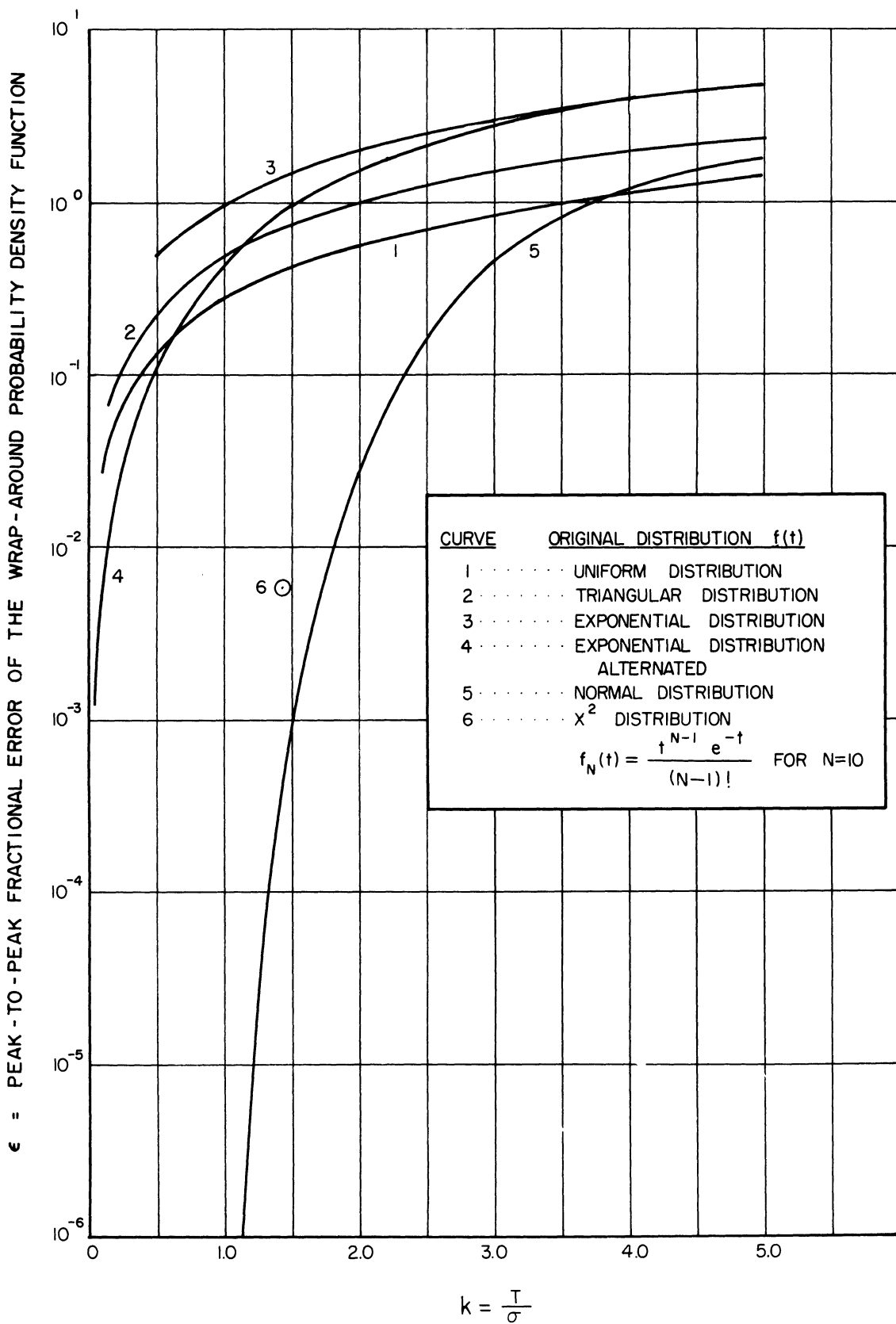


Fig. 11 Peak-to-peak fractional error of the wrap-around probability-density as a function of the wrap-around factor K.

following values of  $\sigma$ . For curves 1, 2, 3, 5, and 6,  $\sigma$  is the calculated standard deviation of  $f(t)$ . For the case of curve 4 it is not easy to calculate  $\sigma$  of  $f(t)$ . Therefore, in this case the  $\sigma$  calculated is for the exponential before alternation. Actually this is more informative because the improvement resulting from alternating the exponential is seen by comparing curves 3 and 4.

Curve 6 has only one point shown. A great deal of work is required to calculate  $\Delta f(t)$  for this distribution. However, it was deemed desirable to give the reader some idea of the position of this curve since it is a realizable practical distribution. The significance of curve 6 for  $N = 10$  is that it is close to the normal distribution and is readily generated. Note that if  $N$  is varied curve 6 will have upper and lower bounds given by curves 3 and 5 when  $N = 0$  and  $N = \infty$ .

Curve 1 is drawn as a continuous curve. Actually  $\epsilon$  goes to zero when  $\lambda$  is equal to an integral multiple of  $T$ .

Several general statements can be made regarding the magnitude of  $\epsilon$  with respect to the shape of  $f(t)$ . For a symmetrical distribution  $\epsilon$  will be smaller than for a skewed distribution. As the wrap-around duration  $T$  is made smaller,  $\epsilon$  will decrease.

2.4.3 The Satisfaction of Randomness Requirements 1 and 2. To determine that conditions 1 and 2 are satisfied it is necessary to analyze the randomness source, the probability control, and the universe of discourse relative to one another. Now it will be assumed that the wrap-around probability-density function  $g(t)$  is uniform. The method of analysis will be described by means of a typical example. For other applications the reader will have to carefully form his own analysis procedure.

Example: this example is concerned with the design of equipment

for a psychophysical experiment. The universe of discourse consists of (a) individuals that are subjects and called observers, (b) a set of signals, and (c) random selection equipment to select signals to present to the observers. The random selector has as a randomness generator a noise source that produces output pulses with the density function of curve 6, Fig. 11. The original source of these pulses is a counter of pulses generated by the decay of a radioactive element. Every tenth pulse is used as an output pulse. The probability control is driven by a stable oscillator, and  $K = T/\sigma$  is selected so that  $g(t)$  is essentially uniform. There is no known causal relationship between the radiation from the radioactive element and the oscillator, and therefore the selections are independent of one another. There is no causal relationship between the noise source and the observer, and therefore the selections are independent of their application. Thus, in this application all three requirements are satisfied.

#### 2.4.4 Determination of Minimum Allowable Time Between Questions.

An important practical design factor is the maximum rate of making selections. This is of course related to  $f(t)$ . If  $f(t)$  has a positive tail that extends to infinity, then an allowable probability of failure to make a selection (Fig. 12, crosshatched region),  $P_F(T_1)$ , must be chosen. Consider the  $f(t)$  shown in Fig. 12.

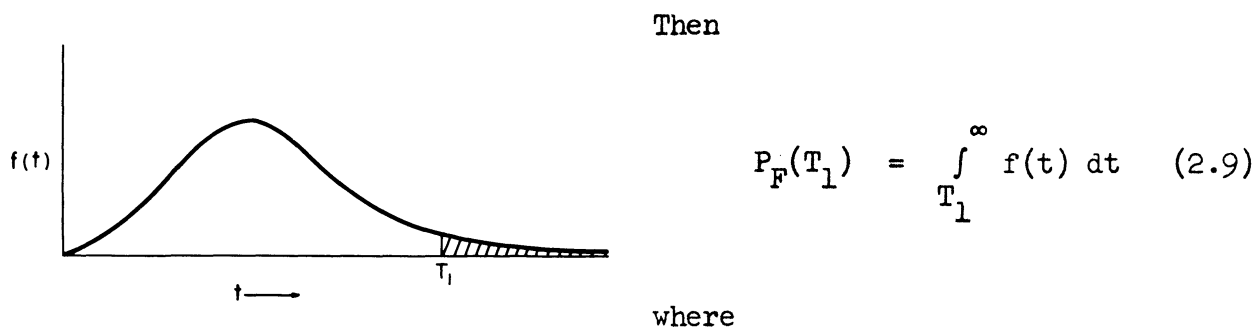


Fig. 12. Probability-density function.

$P_F(T_1)$  = probability of failure to make a selection

$T_1$  = minimum time allowed between question pulses.

Generally  $P_F(T_1)$  will be chosen to be a very small probability. However, if  $f(t)$  has a positive tail that terminates at time  $T_2$ , then it is possible to make  $P_F(T_1) = 0$ , provided  $T_1 > T_2$ . The selection of a value for  $P_F(T_1)$  will depend upon the application of the random selector.

2.4.5 Random Selector With Random Source as an Integral Part of the Probability Control. When the circuit design is such that the random source and probability control cannot be physically separated, then the random selector falls in this category. Randomness conditions 1 and 2 must be satisfied, and condition 3 does not apply. As an illustration of this type of random selector consider the following example. A Gaussian noise source is full-wave rectified, and this voltage waveform is then used in the circuit of Fig. 8 in place of the recurrent sawtooth generator. Photographs of typical samples of full-wave rectified Gaussian noise are shown in Fig. 13. The amplitude density function of this full-wave recti-

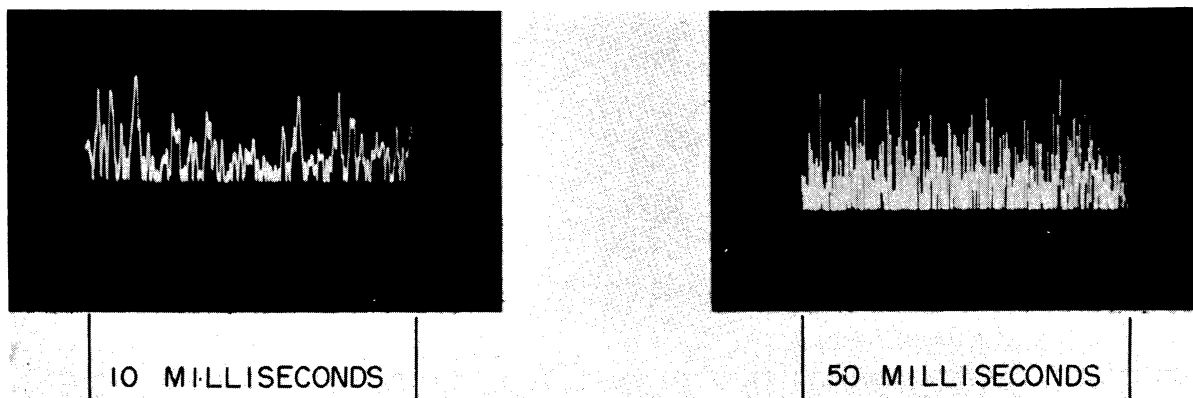


Fig. 13. Full-wave rectified gaussian noise.

fied noise voltage is

$$D_e = \frac{2}{\sqrt{2\pi} \sigma} e^{-\frac{e^2}{2\sigma^2}} \quad 0 < e < \infty \quad (2.10)$$

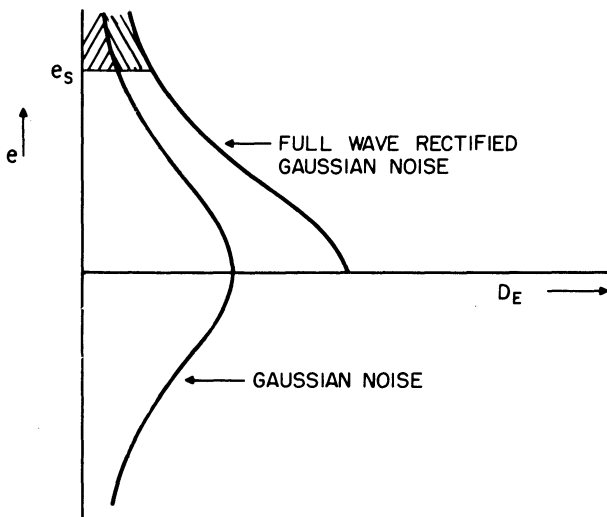
where

$D_e$  = probability density of the full-wave rectified Gaussian noise voltage

$\sigma$  = standard deviation or RMS noise voltage

$e$  = voltage measured from the base line of the noise voltage.

This function and the original unrectified density function are plotted in Fig. 14.



The probability of selection B,  $P(B)$ , is given by Eq. 2.11

$$P(B) = \int_{e_s}^{\infty} \frac{2}{\sqrt{2\pi} \sigma} e^{-\frac{e^2}{2\sigma^2}} de, \quad 0 < e_s, \quad (2.11)$$

where

$P(B)$  = probability of selecting B

$e_s$  = Schmitt circuit trigger level.

Fig. 14. Density functions for rectified and unrectified Gaussian noise.

It is important to note two problems with this type of random selector.

The probability  $P(B)$  is sensitive to (1) changes in the shape of the density function, and (2) changes in the ratio of  $e_s$  to  $\sigma$ .

To obtain the required independence of selections it is necessary that the noise source be independent of the questioning time and independent of the application. To obtain independence among selections



the time between question pulses must exceed a minimum time  $T_3$ .  $T_3$  is determined by the maximum allowable correlation between selections. The correlation function for the noise is then determined by the impulse-response function of the network which determines the spectral distribution of the gaussian noise.

## 2.5 Predictable Binary-Sequence Generators

A predictable binary-sequence generator is a device which produces a sequence of  $M$  binary digits in a deterministic manner. If the design and the stored contents or initial conditions of the device are known, then the output is predictable for a person with this information, but may be unpredictable for a person without this information. Examples of possible predictable sequence generators are:

1. Printed random-number tables.
2. Random-number routines for digital computers.
3. Punched paper tape.
4.  $n$ -stage shift register with feedback loops.
5.  $2^n$ -modulus counters with a suitable output matrix switch.

If a shift-register generator or similar sequence generator produces a periodic sequence of period  $2^n = M$ , then by proper design it is possible to match the statistics up to the  $n$ th order. This means that the probability of a particular subsequence of  $K$  digits, for  $0 < K \leq n$ , is the same as the probability of any other subsequence of  $K$  digits. An example is illustrated below:

Sequence	01110001'01110001'01110001'01110001'0
Period	$2^n$ , $n = 3$
Probability of a $K$ -tuple	$= P(K) = \frac{1}{2^K}$ for $0 < K \leq n$

By actual count:

Sub sequence	Number of Subsequences	Probability
0	4	0.5
1	4	0.5
00	2	0.25
01	2	0.25
10	2	0.25
11	2	0.25
000	1	0.125
001	1	0.125
010	1	0.125
011	1	0.125
100	1	0.125
101	1	0.125
110	1	0.125
111	1	0.125
0000	0	0.000
0001	1	0.125
0010	1	0.125
0011	0	0.000
0100	0	0.000
0101	1	0.125
0110	0	0.000
0111	1	0.125
1000	1	0.125
1001	0	0.000
1010	0	0.000
1011	1	0.125
1100	1	0.125
1101	0	0.000
1110	1	0.125
1111	0	0.000

etc.

For  $n = 3$  there are  $2^{2^3} = 256$  different binary sequences, but there are only 16 ways in which the above sequence can be written and still retain the desired properties.

The importance of the sequence generator is that by proper design the statistical properties are like those of the truly-random binomial distribution with  $p = 0.5$ . It should be noted that this statement is true

for  $0 < K \leq n$  but does not hold for  $K > n$ .

Thus, for applications in which it is desirable to have repeatable experiments or where the statistics must have precise values in the experiment, this type of device may be used as a random selector. As an example, psychologists often want random sequences in which the statistics up through the fourth are precisely matched. They do not want the fluctuations that result from sample variance, and of course sample variance is present in a truly random sequence. It is extremely important that the use of the sequence generator for a random selector satisfy the randomness requirements given on p. 11.

For instance, consider the psychophysical experiment described on p. 16. If a binary sequence generator is used for the random source and if the sequence complexity is such that the observer cannot remember the sequence, then the output will meet the randomness test. Now, if instead, the observer has an identical sequence generator, then he can predict the sequence, and randomness requirement 2 fails.

To ensure independence it is possible to randomly change the code on the sequence generator after every  $\sqrt{2^n}$  digits for a sequence of length  $2^n$ .

### 3. SUMMARY

The basic requirements for randomness have been presented. Techniques for building random selectors have been described. However, no circuit details are given. The actual circuits used in N.P. Psytar are to be presented in a subsequent report (Ref. 3).



## APPENDIX A

### THE DERIVATION OF $\epsilon$ AND $Q$ FOR SEVERAL TYPES OF DISTRIBUTION

#### A.1 Derivation of $\epsilon$ and $Q$ for Uniform Distribution

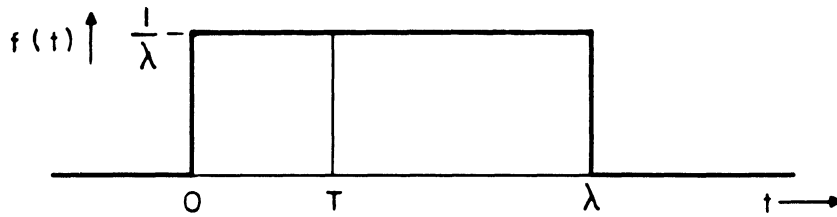


Fig. A.1. Uniform distribution.

Let

$$\lambda = NT + a \quad 0 < a < T$$

$$u = \lambda/2; \text{ mean time of the distribution}$$

$$\sigma = \lambda \frac{\sqrt{3}}{6}$$

$$g(t)_{\max} - g(t)_{\min} = \Delta g(t) = (N + 1) \frac{1}{\lambda} - N \frac{1}{\lambda} = \frac{1}{\lambda}$$

for

$$\sigma = 1; \quad K = T; \quad \lambda = 2\sqrt{3}$$

$$\epsilon = K \frac{1}{\lambda} = \frac{K}{2\sqrt{3}}$$

$$Q = \frac{2\sqrt{3}}{K}$$

#### A.2 Derivation of $\epsilon$ and $Q$ for Triangular Distribution

$$f(t) = \frac{2}{NT+a} - \left( \frac{t}{NT+a} \cdot \frac{2}{NT+a} \right)$$

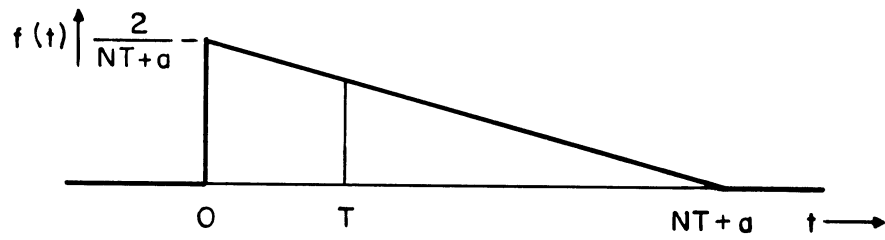


Fig. A.2. Triangular distribution.

$$\mu = E(t) = \int_{-\infty}^{\infty} t f(t) dt$$

$$\sigma^2 = E(t-\mu)^2 = \int_{-\infty}^{\infty} t^2 g(t) dt - \mu^2$$

Let

$$\lambda = NT + a$$

then

$$\mu = \lambda/3$$

$$\sigma^2 = \lambda^2/18$$

$$\sigma = \frac{\lambda}{3\sqrt{2}}$$

Assume  $a = 0$

$$f(t) = \frac{2}{NT} \left(1 - \frac{t}{NT}\right) \quad 0 < t < NT$$

$$= \frac{2}{NT} \left(1 - \frac{iT+t'}{NT}\right) \quad \left\{ \begin{array}{l} 0 < t' < T \\ i = 0, 1, 2, \dots, N-1 \end{array} \right\}$$

$$g(t) = \sum_{i=0}^{N-1} f(t)$$

$$= \frac{2}{NT} \left[ N - \frac{t'}{T} - \frac{1}{N} \cdot \frac{N(N-1)}{2} \right]$$

$$g(t) = \frac{1}{NT} \left[ N + 1 - 2 \frac{t'}{T} \right] \quad 1 < N$$

$$g(t)_{\max} - g(t)_{\min} = \Delta g(t) = 2/NT = 2/\lambda$$

For

$$\sigma = 1; \quad \lambda = 3\sqrt{2}; \quad K = T$$

$$\epsilon = K 2/\lambda = \frac{K\sqrt{2}}{3}$$

$$Q = \frac{3\sqrt{2}}{2K}$$

Using this same procedure, it is possible to evaluate  $\epsilon$  or  $Q$  for the symmetrical triangular distribution.

### A.3 Derivation of $\epsilon$ and $Q$ for Exponential Distribution

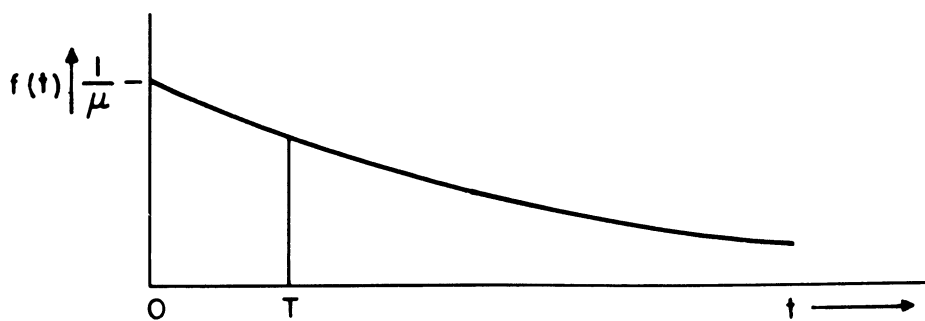


Fig. A.3. Exponential distribution.

$$g(t) = 1/\mu e^{-\frac{t}{\mu}} \quad \text{Note } \sigma = \mu$$

$$g(t) = \sum_{i=0}^{\infty} \frac{1}{\mu} e^{-\frac{1}{\mu} (i + \frac{t'}{T})T} \quad 0 < t' < T$$

$$= \frac{1}{\mu} \cdot \frac{e^{-\frac{t'}{\mu}}}{1 - e^{-\frac{T}{\mu}}}$$

$$g(t)_{\max} - g(t)_{\min} = \Delta g(t) = \frac{1}{\mu} = \frac{1}{\sigma}$$

For

$$\sigma = 1; \quad K = T$$

$$\epsilon = K$$

or

$$Q = 1/K$$

#### A.4 Derivation of $\epsilon$ and $Q$ for Exponential Distribution Alternated

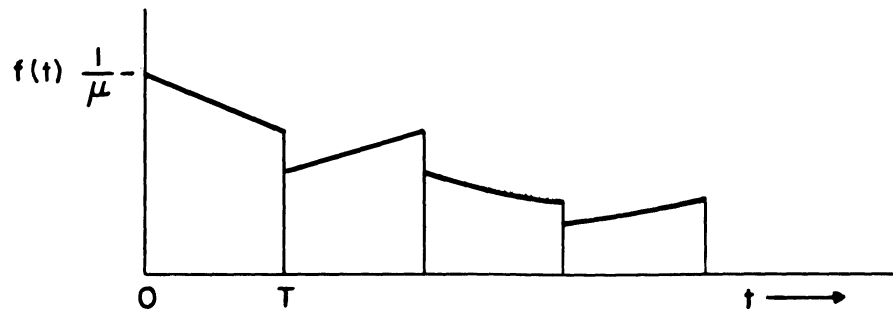


Fig. A.4. Exponential distribution alternated.

$$f(t) = \frac{1}{\mu} e^{-\left(i + \frac{t'}{2T}\right) \frac{2T}{\mu}} \quad \left. \begin{array}{l} i = 0, 1, 2, \dots \\ 0 < t' < T \\ t = i2T + t' \end{array} \right\}$$



$$f(t) = \frac{1}{\mu} e^{-(i+1 - \frac{t'}{2T}) \frac{2T}{\mu}} \quad \left\{ \begin{array}{l} i = 0, 1, 2 \dots \\ 0 < t' < T \\ t = (i+1) 2T - t' \end{array} \right\}$$

where  $\mu$  is the mean for the nonalternated exponential distribution.

$\sigma^2$  is the variance for the nonalternated exponential distribution.

$$g(t) = \sum_{i=0}^{\infty} \left[ \frac{1}{\mu} e^{-(i + \frac{t'}{2T}) \frac{2T}{\mu}} + \frac{1}{\mu} e^{-(i+1 - \frac{t'}{2T}) \frac{2T}{\mu}} \right] \quad 0 < t' < T$$

$$g(t) = \frac{1}{\mu} \sum_{i=0}^{\infty} \left[ e^{-i \frac{2T}{\mu}} e^{-\frac{t'}{\mu}} + e^{-(2T - t') \frac{1}{\mu}} \right]$$

$$= \frac{1}{\mu} \frac{e^{\left(\frac{T}{\mu} - \frac{t'}{\mu}\right)} + e^{-\left(\frac{T}{\mu} - \frac{t'}{\mu}\right)}}{e^{\frac{T}{\mu}} - e^{-\frac{T}{\mu}}}$$

$$= \frac{1}{\mu} \frac{\cosh \frac{1}{\mu} (T - t')}{\sinh \frac{T}{\mu}}$$

$$g(t)_{\max} - g(t)_{\min} = \Delta g(t) = \frac{1}{\mu} \left( \frac{1}{\tanh \frac{T}{\mu}} - \frac{1}{\sinh \frac{T}{\mu}} \right)$$

Let

$$\mu = 1; \quad \sigma = 1; \quad K = T$$

$$\epsilon = K \left( \frac{1}{\tanh K} - \frac{1}{\sinh K} \right) = K \left( \frac{\cosh K - 1}{\sinh K} \right)$$

or

$$Q = \frac{1}{K} \left( \frac{\sinh K}{\cosh K - 1} \right)$$

For small K (neglecting third- and higher-order factors) we obtain

$$\epsilon = K^2/2$$

A.5 Derivation of  $\epsilon$  and Q for Normal Distribution

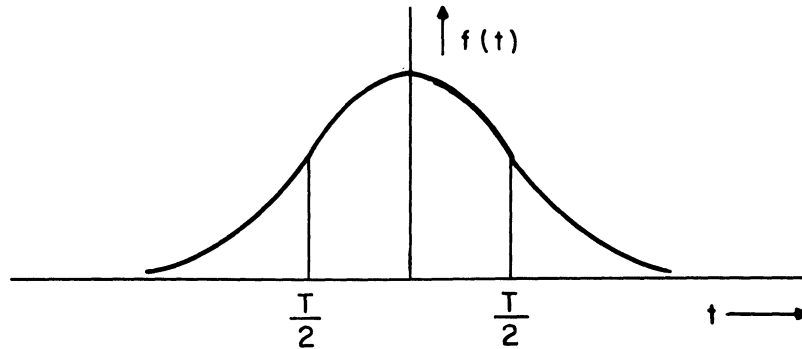


Fig. A.5. Normal distribution.

$$f(t) = \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} \quad \sigma = 1$$

$$\Delta g(t) = \frac{1}{\sqrt{2\pi}} + 2 \sum_{i=1}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{(iK)^2}{2}} - 2 \sum_{i=1}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{[(i - \frac{1}{2})K]^2}{2}}$$

For

$$\left\{ \begin{array}{l} i = 0, 1, 2, \dots \\ K = T \end{array} \right\}$$

$$= \frac{1}{\sqrt{2\pi}} \left[ 1 + 2 \sum_{i=1}^{\infty} \left( e^{-\frac{(iK)^2}{2}} - e^{-\frac{[(i - \frac{1}{2})K]^2}{2}} \right) \right]$$

This numerical evaluation is most easily obtained by means of tables.

A.6 Derivation of  $\epsilon$  and  $Q$  for  $\chi^2$  Distribution with  $2N$  Degrees of Freedom

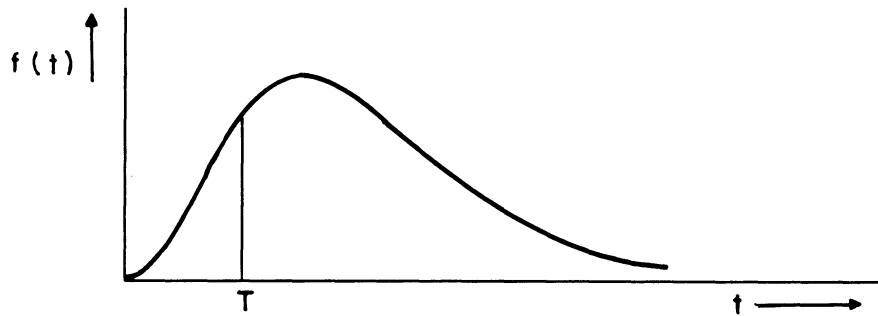


Fig. A.6.  $\chi^2$  distribution with  $2N$  degrees of freedom.

$$f(t) = \frac{t^{N-1} e^{-t}}{(N-1)!} \quad \begin{array}{l} \mu = N \\ \sigma = \sqrt{N} \end{array}$$

$\Delta g(t)$  is not easy to express for all  $N$  and is also difficult to calculate. As  $N \rightarrow \infty$ ;  $g(t)$  approaches the normal distribution.

The curve of  $\epsilon$  as a function of  $K$  is not so good as the normal distribution.

Note: When  $N = 1$ ,  $f(t)$  is the exponential distribution.

If numerical calculation of  $\epsilon$  is desired for small  $\epsilon$ , then a digital computer should be used.

$\epsilon$  as a function of  $K(\sigma = 1)$  is plotted for each of the above wrap-around distributions in the text in Fig. 11.

## REFERENCES

1. G. A. Roberts, "Spinning Disk Random Selectors," Cooley Electronics Laboratory Technical Memorandum No. 39, The University of Michigan, Ann Arbor, April 1957.
2. R. R. McPherson, "Use of Hewlett-Packard Model 522B Electronic Counter as a 'Spinning Disk' Random-Number Selector," Cooley Electronics Laboratory Technical Memorandum No. 29, The University of Michigan, Ann Arbor, July 1956.
3. G. A. Roberts, "N. P. Psytar: Noise Programmed Psychophysical Tester and Recorder," Cooley Electronics Laboratory Technical Memorandum No. 86, The University of Michigan, Ann Arbor, March 1961.

DISTRIBUTION LIST

<u>COPY NO.</u>		<u>COPY NO.</u>	
1-2	Commanding Officer, U. S. Army Signal Research and Development Laboratory, Fort Monmouth, New Jersey, ATTN: Senior Scientist, Countermeasures Division	28	Chief, Bureau of Naval Weapons, Code RRR-E, Department of the Navy, Washington 25, D. C.
3	Commanding General, U. S. Army Electronic Proving Ground, Fort Huachuca, Arizona, ATTN: Director, Electronic Warfare Department	29	Chief of Naval Operations, EW Systems Branch, OP-35, Department of the Navy, Washington 25, D. C.
4	Chief, Research and Development Division, Office of the Chief Signal Officer, Department of the Army, Washington 25, D. C., ATTN: SIGEB	30	Chief, Bureau of Ships, Code 691C, Department of the Navy, Washington 25, D. C.
5	Commanding Officer, Signal Corps Electronics Research Unit, 9560th USASRU, P. O. Box 205, Mountain View, California	31	Chief, Bureau of Ships, Code 684, Department of the Navy, Washington 25, D. C.
6	U. S. Atomic Energy Commission, 1901 Constitution Avenue, N.W., Washington 25, D. C., ATTN: Chief Librarian	32	Chief, Bureau of Naval Weapons, Code RAAV-33, Department of the Navy, Washington 25, D. C.
7	Director, Central Intelligence Agency, 2430 E. Street, N.W., Washington 25, D. C., ATTN: OCD	33	Commander, Naval Ordnance Test Station, Inyokern, China Lake, California, ATTN: Test Director-Code 30
8	Signal Corps Liaison Officer, Lincoln Laboratory, Box 73, Lexington 73, Massachusetts, ATTN: Col. Clinton W. Janes	34	Director, Naval Research Laboratory, Countermeasures Branch, Code 5430, Washington 25, D. C.
9-18	Commander, Armed Services Technical Information Agency, Arlington Hall Station, Arlington 12, Virginia	35	Director, Naval Research Laboratory, Washington 25, D. C., ATTN: Code 2021
19	Commander, Air Research and Development Command, Andrews Air Force Base, Washington 25, D. C., ATTN: RDTC	36	Director, Air University Library, Maxwell Air Force Base, Alabama, ATTN: CR-4987
20	Directorate of Research and Development, USAF, Washington 25, D. C., ATTN: Chief, Electronic Division	37	Commanding Officer-Director, U. S. Naval Electronic Laboratory, San Diego 52, California
21-22	Commander, Wright Air Development Center, Wright Patterson Air Force Base, Ohio, ATTN: WCOSI-3	38	Office of the Chief of Ordnance, Department of the Army, Washington 25, D. C., ATTN: ORDTU
23	Commander, Wright Air Development Center, Wright-Patterson Air Force Base, Ohio, ATTN: WCLGL-7	39	Chief, West Coast Office, U. S. Army Signal Research and Development Laboratory, Bldg. 6, 75 S. Grand Avenue, Pasadena 2, California
24	Commander, Air Force Cambridge Research Center, L. G. Hanscom Field, Bedford, Massachusetts, ATTN: CROTLR-2	40	Commanding Officer, U. S. Naval Ordnance Laboratory, Silver Springs 19, Maryland
25	Commander, Rome Air Development Center, Griffiss Air Force Base, New York, ATTN: RCSSLD	41-42	Chief, U. S. Army Security Agency, Arlington Hall Station, Arlington 12, Virginia, ATTN: IADEV
26	Commander, Air Proving Ground Center, ATTN: Adj/Technical Report Branch, Eglin Air Force Base, Florida	43	President, U. S. Army Defense Board, Headquarters, Fort Bliss, Texas
27	Commander, Special Weapons Center, Kirtland Air Force Base, Albuquerque, New Mexico	44	President, U. S. Army Airborne and Electronics Board, Fort Bragg, North Carolina
		45	U. S. Army Antiaircraft Artillery and Guided Missile School, Fort Bliss, Texas
		46	Commander, USAF Security Service, San Antonio, Texas, ATTN: CLR

DISTRIBUTION LIST (Continued)

<u>COPY NO.</u>		<u>COPY NO.</u>	
47	Chief, Naval Research, Department of the Navy, Washington 25, D. C., ATTN: Code 931	61	Commanding Officer, U. S. Naval Air Development Center, Johnsville, Pennsylvania, ATTN: Naval Air Development Center Library
48	Commanding Officer, U. S. Army Security Agency, Operations Center, Fort Huachuca, Arizona	62	Commanding Officer, U. S. Army Signal Research and Development Laboratory, Fort Monmouth, New Jersey, ATTN: U. S. Marine Corps Liaison Office, Code AO-4C
49	President, U. S. Army Security Agency Board, Arlington Hall Station, Arlington 12, Virginia	63	President, U. S. Army Signal Board, Fort Monmouth, New Jersey
50	Operations Research Office, John Hopkins University, 6935 Arlington Road, Bethesda 14, Maryland, ATTN: U. S. Army Liaison Officer	64-73	Commanding Officer, U. S. Army Signal Research and Development Laboratory, Fort Monmouth, New Jersey
51	The John Hopkins University, Radiation Laboratory, 1315 St. Paul Street, Baltimore 2, Maryland, ATTN: Librarian	ATTN:	1 Copy - Director of Research 1 Copy - Technical Documents Center ADT/E 1 Copy - Chief, Countermeasures Systems Branch, Countermeasures Division
52	Stanford Electronics Laboratories, Stanford University, Stanford, California, ATTN: Applied Electronics Laboratory Document Library	1 Copy	- Chief, Detection and Location Branch, Countermeasures Division
53	HRB-Singer, Inc., Science Park, State College, Pennsylvania, ATTN: R. A. Evans, Manager, Technical Information Center	1 Copy	- Chief, Jamming and Deception Branch, Countermeasures Division
54	ITF Laboratories, 500 Washington Avenue, Nutley 10, New Jersey, ATTN: Mr. L. A. DeRosa, Div. R-15 Lab.	1 Copy	- File Unit No. 2, Mail and Records, Countermeasures Division
55	The Rand Corporation, 1700 Main Street, Santa Monica, California, ATTN: Dr. J. L. Hult	1 Copy	- Chief, Interference Reduction Branch, Electromagnetic Environment Division
56	Stanford Electronics Laboratories, Stanford University, Stanford, California ATTN: Dr. R. C. Cumming	3 Copies	- Chief, Security Division (for retransmittal to BJSM)
57	Willow Run Laboratories, The University of Michigan, P. O. Box 2008, Ann Arbor, Michigan, ATTN: Dr. Boyd	74	Director, National Security Agency, Fort George G. Meade, Maryland, ATTN: TEC
58	Stanford Research Institute, Menlo Park, California, ATTN: Dr. Cohn	75	Dr. H. W. Farris, Director, Cooley Electronics Laboratory, The University of Michigan, Ann Arbor, Michigan
59-60	Commanding Officer, U. S. Army Signal Missile Support Agency, White Sands Missile Range, New Mexico, ATTN: SIGWS-EW and SIGWS-FC	76-99	Cooley Electronics Laboratory Project File, The University of Michigan, Ann Arbor, Michigan
		100	Project File, The University of Michigan Office of Research Administration, Ann Arbor, Michigan

Above distribution is effected by Countermeasures Division, Surveillance Department, USASRDL, Evans Area, Belmar, New Jersey. For Further information contact Mr. I. O. Myers, Senior Scientist, Telephone PProspect 5-3000, Ext. 61252.



