

ANL/ES-95

201  
6/17/80

mmw3

LD. 1352

ANL/ES-95

MASTER

**RANDOM NUMBERS SPRING  
FROM ALPHA DECAY**

by

**Norman A. Frigerio, L. P. Sanathanan,  
Mary Morley, Nancy A. Clark,  
and Sylvanus A. Tyler**



---

**ARGONNE NATIONAL LABORATORY, ARGONNE, ILLINOIS**  
**Prepared for the U. S. DEPARTMENT OF ENERGY**  
**under Contract W-31-109-Eng-38**

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

The facilities of Argonne National Laboratory are owned by the United States Government. Under the terms of a contract (W-31-109-Eng-38) among the U. S. Department of Energy, Argonne Universities Association and The University of Chicago, the University employs the staff and operates the Laboratory in accordance with policies and programs formulated, approved and reviewed by the Association.

#### MEMBERS OF ARGONNE UNIVERSITIES ASSOCIATION

The University of Arizona  
Carnegie-Mellon University  
Case Western Reserve University  
The University of Chicago  
University of Cincinnati  
Illinois Institute of Technology  
University of Illinois  
Indiana University  
The University of Iowa  
Iowa State University

The University of Kansas  
Kansas State University  
Loyola University of Chicago  
Marquette University  
The University of Michigan  
Michigan State University  
University of Minnesota  
University of Missouri  
Northwestern University  
University of Notre Dame

The Ohio State University  
Ohio University  
The Pennsylvania State University  
Purdue University  
Saint Louis University  
Southern Illinois University  
The University of Texas at Austin  
Washington University  
Wayne State University  
The University of Wisconsin-Madison

#### NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government or any agency thereof, nor any of their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Printed in the United States of America  
Available from  
National Technical Information Service  
U. S. Department of Commerce  
5285 Port Royal Road  
Springfield, VA 22161

NTIS price codes  
Printed copy: A04  
Microfiche copy: A01

ARGONNE NATIONAL LABORATORY  
9700 Cass Avenue  
Argonne, Illinois 60439

RANDOM NUMBERS SPRING  
FROM ALPHA DECAY

by

Norman A. Frigerio

L.P. Sanathanan  
Mary Morley

Nancy A. Clark\*  
Sylvanus A. Tyler

Division of Environmental Impact Studies  
and  
\*Applied Mathematics Division

DISCLAIMER

This book was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

May 1980

With a Dedication to Norman A. Frigerio

## CONTENTS

	<u>Page</u>
LIST OF FIGURES . . . . .	iv
LIST OF TABLES . . . . .	iv
DEDICATION . . . . .	v
ABSTRACT . . . . .	1
I. Introduction . . . . .	2
II. Strategy for Creating Almost Perfect Random Numbers . . . . .	7
III. The Brockwell-Moyal Model for Retroactive Decay and Its Validation . . . . .	11
IV. Insuring a Uniform Distribution of Random Numbers . . . . .	21
V. Statistical Tests on Random Numbers . . . . .	24
VI. Conclusion . . . . .	37
APPENDIX A. An Alternate Derivation of the Brockwell-Moyal Distribution . . . . .	38
APPENDIX B. Probabilities . . . . .	50
References . . . . .	51

## FIGURES

<u>Figure</u>	<u>Page</u>
1. Empirical Fit of the Brockwell-Moyal Distribution Obtained by Using System III . . . . .	17
2. Comparison of the Cumulative Frequency Distribution of the Observed Chi-Square Values and the Distribution Function of Chi-Square for 30 Degrees of Freedom Using System III . . . . .	19
3. Periodogram of Truly Random Numbers . . . . .	33
4. Comparison of Theoretical and Empirical Distribution Functions of Periodogram Ordinates for the Truly Random Numbers . . . . .	34
5. Comparison of Theoretical and Empirical Distribution Functions of the Four-tuples in the Unit Sphere for Truly Random Numbers . . . . .	35
6. Comparison of Theoretical and Empirical Distribution Functions of the Number of Five-tuples in the Unit Sphere for Truly Random Numbers . . . . .	36

## TABLES

<u>Table</u>	<u>Page</u>
1. Chi-Squared Comparisons of Theoretical and Experimental Distributions (System II) . . . . .	15
2. Distribution of Observed Counts for System III and the Fitted Brockwell-Moyal Distribution . . . . .	16
3. Chi Square Values for Tests with Given Degrees of Freedom . . .	27
4. Summary of Tests on System III Generator vs. Congruential Generators . . . . .	30
5. Deviation of Moments and Correlations from Expected Values for Random Numbers in the Interval . . . . .	31

## DEDICATION

NORMAN ALFRED FRIGERIO  
SEPTEMBER 4, 1929 - NOVEMBER 7, 1978

*This report is dedicated to the memory of our colleague Norm. It represents the completion of one of his final scientific endeavors. Excerpts from his personal memos form a part of this dedication to convey a glimpse of the genius, the style, and the undying humanity of this fine and unusual man.*



Philip F. Gustafson, Director  
Division of Environmental Impact Studies

78C141115. To Sylvanus Tyler, via mailbox.

Sylvanus, Sir:

Random Numbers, and Money, and Jobs, and all that sort of thing: Do you remember those random numbers I generated some years back using an alpha counter, for use with my Monte Carlo programs? Well, Nancy Clark and I kind of halfway wrote the system up, but we really didn't go any farther than that. We put the tapes in the Argonne Code Center (I think!). Anyway, a lot of people have called on me for copies of the tapes and I've sent copies to them along with some short descriptions. Nancy ran a whole battery of tests on them, and I guess between using them on various jobs and so forth they've pretty much been tested to death in a way. However, I never got around to really formalizing the thing. Now I find myself in a little bit of a bind for pressure. On the one hand I'm doing a massive accident analysis for USNRC in which I'm using these random numbers, and at the same time a whole bunch of people at NIH at WHO, Geneva, and so forth are bugging me to get the thing written up, documented and printed. So, apropos of our conversation Tuesday, that's the background behind it. As to time scale I promised them a report on this but it's hardly what you'd call a rush job.

History: Here's the history behind this thing. Many years ago in running Monte Carlo programs with random number generators I found, of course, that they certainly weren't perfect. In fact, for my purposes they were just barely good enough if I got the best generators, and the best generators I have ever gotten, I got from Nancy Clark. However, as I mentioned to you one day in a conversation in your office, I did find that one could get around their imperfection by averaging two runs, one done on a given random number string, and another using its one compliment. When I use random numbers in a Monte Carlo program, I use them as a series of fractions between 0 and 1. What led me to this was watching how the data set went and how it compared with experimental values. What I noticed was that as I would run more and more cases, the answer would asymptote to a common value. But even with the best random number generators I had, this asymptotic value was often slightly higher than the experimental one. And, by just about one standard deviation. At other times it would be slightly lower, and again by about one standard deviation. So, I reasoned that if this was due to some imperfection in the random number generator, it ought to flip its sign if I ran exactly the same run down the same random number string but used the ones compliment each time instead of the original random number. Sure

enough, this is exactly what happened. The two runs would mirror one another; they would asymptote to two different values, one slightly above and one slightly below the experimental value. Sure enough, if I averaged two such runs, I came out right on the button. Well, that was okay for what one might in medicine call "symptomatic" treatment, but it left me dissatisfied as to high quality stuff. So I figured I needed the best random number generator I could get, especially since NBS and I were comparing theoretical predictions and experimental values that were good out to 3 and 4 significant figures ....

The only natural process which everyone believes with almost complete firmness to be a truly random Poisson type of process is radioactive decay. In fact, I guess people think of this as the very paradigm of random processes. However, if you look in the literature, you'll see that this hasn't really been tested very much. The tests most everybody refers to occurred around the turn of the century, and people have done very little with it since. Not only that, the tests that do look good are all on alpha particle decays, and a number of people have reported rather strange looking gamma, beta, and so forth results. Well, that didn't surprise me at all. The very instrumental nature of trying to pick up gammas and betas and so forth I just knew was going to lead to trouble. They are just down too close to the natural noise level and what I think of as their "selectability". In other words, there are just too many energy losses, drifts, reflections, scatters, and all sorts of things and I just knew from long experience with this kind of particle that it was going to be more trouble than it was worth. An alpha decay, on the other hand, is very easy to pick out of any kind of a background. It's a lot like a supernova in the sky; it does things the other particles don't do, and it does them with a bang. But, even there, one has to stay away from sophisticated detectors. They may be sophisticated, but they're also wifty. So I went to the good old standby, a gas ionization detector chamber, which just goes boom, cleans itself up, heals itself again, and waits for the next one, and has never caused anybody any trouble. I then stuck a pure alpha source in there and counted for a fixed time period, or rather for a whole string of fixed time periods one after the other. In the original way in which I did this I fed the data into a multichannel analyzer of 4096 channels and then taped it back out again. This was operating in what's called multi-scaler mode, meaning each channel is a scaler for a fixed period of time, and then the analyzer switches to the next channel. This was okay, and those are the results you see in the first couple of manuscripts I've attached here. (Or, if I've forgotten to attach them, I'll send them later in the mail.) In order to speed things up, I then fed these into the Neurotron over at Applied Math, and it just wrote the counts through a buffer out onto tape. That way the thing could just run day and night, constantly writing tapes. That went on while I was overseas mostly, and Nancy Clark took care of it. She also took the tapes off, policed them up, and so forth. Then when I came back,

what I did was simply ask each counting interval whether the total number of counts was odd or even. If it was odd, I called that a 1 bit, and if it was even, I called that a 0 bit, and I just took these bits in order and made 31 bit words out of them by stringing them together one after the other and cutting them off every 31 bits. I didn't use 32 bits because although they speak of the IBM series of 32 bit machines, the first bit is a sign bit and that would have just confused things. This way they were all positive numbers between 0 and  $2^{31}-1$ , and one could make fractions out of them just by dividing. Actually the numbers I left on the tape are simply the 31 bit numbers themselves, so anybody can do with them what they like. In between these two ways of doing things, I ran off a few hundred thousand of them using the old IBM 1130 upstairs as an intermediate buffer. So there really are three sets of these, but it is only the last, and largest set that I think we need bother with. However, the other two sets still exist and sometimes it's nice to have them around to do some comparisons with or something. I asked Nancy Clark to put these tapes up at the Argonne Code Center, and I'm quite sure she did. However, when I went over to talk to Lou the other day we couldn't seem to find them. That doesn't mean the tapes are gone; I've got a set of them and Nancy has a set in the tape library. But, just in case they never got into the Argonne Code Center I'll put them in so that people can get the tapes from Margaret Butler and won't have to bother us. It makes her business look good. About a dozen people from all over have asked me for these tapes, and I've sent them to them, but oddly enough I've never gotten any reports back. On a couple of occasions I happened to meet somebody and talked to them about them, and they said they worked just fine, but I thought it was kind of too bad they never dropped me a line about it. Also, Nancy Clark ran a whole battery of tests on them, and those are the results that you also ought to see in some of the manuscripts I'm sending along.

What To Do -- Practical: I guess on the practical side the only thing to do is to look everything over, see if you're satisfied with the tests that have been done, and do anything you think appropriate. Then write the whole thing up as a little package. I leave it up to you whether we ought to put this out as an ANL report, or submit it to a journal for publication, or both. I suppose we could print up one of those tables of random numbers, but I leave that up to you. Myself, I would rather have a tape than a table, but I suppose there are people who can get hold of a table and use it, but can't get hold of the tapes. I don't know, so like I say, I leave that up to you. The programs we use for handling these don't amount to much; I'll get them and send them along too. About their only real utility is that they've got the formats in there for reading the tape.

What To Do Next -- Theoretical: I've talked to Herman Rubin and some other random number experts about this and they all seem quite pleased with the whole thing. They thought that the way I

went about removing bias was "wasteful", in that I didn't use every count or anything like it, but they certainly agreed that it really ought to remove any bias. To put it another way, how the heck could one group of counts know what the next group of counts was going to do to such an extent that it adjusted itself to be odd or even depending on what the other group was going to do. That ain't randomness, that's intelligence. Well, my feeling about it was it might be wasteful in a sense, but it really didn't amount to too much. I did the counts for one-fiftieth of a second, and with the source I was using this came out to a mean of about 23 counts per counting period. I could have used more or less, but this is where the theoretics came in. Herman Rubin told me that, if the distribution had been truly Poisson (that is to say, no deadtime at all), then the number of even bits minus the number of odd bits would just be probability of 0 quantity squared. Sure enough, I took the Poisson expression and expanded it and it works out! So, with the mean up around 23, this slight excess of one kind of bit over the other was vanishingly small. On the other hand, there wasn't much point in taking a lot more counts per unit interval because it wouldn't improve that any, and would just make life tougher on my machine and extend the time it took to get the data. But, therein lies the theoretics that I guess remains to be done. From the reprint attached I guess we're pretty sure that a Poisson with deadtime is a Brockwell-Moyal distribution. So, in all honesty and that sort of thing we ought to find out what the excess of odd or even bits is as predicted by this distribution. I would have done it; in fact I even tried, but the algebra got to be too much for me. I suppose if we can't solve it algebraically, we can always solve it numerically somehow. Of course, I do have the total number of odd and even bits in those tapes of random numbers, so we can then compare the two. But I guess there's a little bit of theoretical work to be done in the sense that we know these numbers are not quite perfect but we think we know how to predict what their imperfection is, and because of the nature of this prediction be able to say that one could reduce it to anything one wanted to. By the way, once you've got the equipment set up, running these numbers off is no great sweat. If I were to stick to just the parameters that I already use, and they are pretty optimum for the machinery I've got, you would get one bit every 50th of a second, or roughly one and a half random numbers a second. That means you get about 150,000 a day, or about 50 million a year. The machine just sits there and runs, and doesn't cost anything, and doesn't use up any computer time to speak of. So if anybody felt that he wanted 50 million of these things instead of the 120,000 I've got or something it would be no problem to get them. The main frame computer time required in reducing the tapes to random numbers is almost negligible. It would take about one hour of total main frame time to reduce the whole 50 million and write them onto a 6250 tape. Well, ten 6250 tapes to be exact for 50 million numbers.

L'Envoi: I guess about the only thing I've got to throw in here is that there always seems to be an argument between an

online generator and a generator that generates tapes. The idea is that an online generator somehow ought to be faster. I'm not talking about a computational pseudo random number generator; I'm talking about the kind of noise generators and so forth that people think of. My feeling about this is the whole thing is rather silly, and actually contraindicated. As things stand right now all major modern computers use no time at all on input-output of a tape because they have the necessary massive buffers to input them while the program is still running on the CPU, and in that sense don't waste any time at all. So, my feeling is that now that that's the situation, any kind of an online generator isn't faster, it's slower. A tape, in fact uses 0 CPU time to read itself into the memory. An online generator, no matter how fast it might be, uses all that time getting its number back over to the CPU whenever it's asked for. The very nature of that kind of a generator is, it can never be as fast as the random access time to memory with buffer, and I've certainly found that to be true on testing this out with a bunch of different machines.

Well, how does the whole thing strike you? Anyway, whether attached or under separate cover, you ought to be receiving (1) a bunch of manuscripts of this called "toward truly random numbers." (2) Nancy Clark's tests on it, (3) the tape library numbers, and various programs for getting hold of the numbers and so forth, and (4) any references I've got on recent work in this whole area by Herman Rubin or others.

78D221942. To Sylvanus Tyler.

Sylvanus, Sir:

Applications of the Brockwell-Moyal distribution in counting:  
I've attached a couple of things which pretty much represent the present state of the art, believe it or not. The deadtime correction equation that is found in all the handbooks is equations 2 and 3 on page 31 of the Radiological Health Handbook. This is what everybody uses unless they're very sophisticated. The same thing is repeated on page 121. As far as the more sophisticated goes, to the best of my ability to find out, the paper by Schiff in the 1936 Physical Review that I attached is pretty much state of the art. As near as I can make out what he did was take the Poisson, make some approximations, and correct the mean by an expression very similar to the one we used and which I put down there on the bottom of the first page. Then he just went ahead and used the  $\lambda$  that he got from that in the regular Poisson distribution. Numerically, this approach is pretty good and doesn't differ a great deal from the results I get with the BM. However, of course, it does differ, and it doesn't fit the observations either. So I'd say that between those two we probably already have more applications than we really want to use. My guess is that if we showed how to apply this to correct the determination of the deadtime, also called the resolving time and various other things, and also showed how to apply it to correcting observed count rates for deadtime, we would probably have helped out people quite a bit.

Something that occurs to me, and I'm just putting it down for the record so to speak, is that this doesn't just apply to a time situation; it applies to any kind of a resolution confusion in a string of otherwise random events. In fact, that's how B and M first got into this. They were analyzing bubble chamber photographs, and when two events were too close together they looked like one event on the photographic string of dots that you see. This probably has other applications, too, but they don't come to mind at the moment, and I rather suspect we probably have more here than we really need anyway.

Fred James: The third attachment is a piece of a draft that Fred James sent to me from Switzerland of a book he is writing on Monte Carlo. It contains that bias removal technique, which was explained to me by Herman Rubin years ago, but which I guess I never used because of some philosophical feeling that there really shouldn't be anything that is perfect, not even perfectly random. Anyway, it's passed along for your interest. Also, I did some kind of tests on all of this along the lines you were talking about; I just haven't found them yet, but when I do I'll pass them along. And, I'll get you all the tape numbers and things too, in case you want to run any tests on the various sets, means, and whatnot.

## RANDOM NUMBERS SPRING FROM ALPHA DECAY

Norman A. Frigerio, L.P. Sanathanan, Mary Morley,  
Nancy A. Clark, Sylvanus A. Tyler

### ABSTRACT

*Congruential random number generators, which are widely used in Monte Carlo simulations, are deficient in that the numbers they generate are concentrated in a relatively small number of hyper-planes. While this may not be a limitation in small Monte Carlo studies involving a few variables, it introduces a significant bias in large simulations requiring high resolution. This bias was recognized and assessed during preparations for an accident analysis study of nuclear power plants.*

*This report describes a random number device based on the radioactive decay of alpha particles from a U-235 source in a high-resolution gas proportional counter. The signals were fed to a 4096-channel analyzer and for each channel the frequency of signals registered in a 20,000-microsecond interval was recorded. The parity bits of these frequency counts (0 for an even count and 1 for an odd count) were then assembled in sequence to form 31-bit binary random numbers and transcribed to a magnetic tape. This cycle was repeated as many times as were necessary to create 3 million random numbers.*

*The frequency distribution of counts from the present device conforms to the Brockwell-Moyal distribution which takes into account the dead time of the counter (both the dead time and decay constant of the underlying Poisson process were estimated). Our analysis of the count data and our tests of randomness on a sample set of the 31-bit binary numbers indicate that this random number device is a highly reliable source of truly random numbers. Its use is, therefore, recommended in Monte Carlo simulations for which the congruential pseudorandom number generators are found to be inadequate.*

## RANDOM NUMBERS SPRING FROM ALPHA DECAY

## I. INTRODUCTION

The success of any large scale Monte Carlo study is critically dependent on the quality of the random number generator employed. Typically, a computer program based on some mathematical recurrence relation is used for generating random numbers. The resulting sequence of numbers is not truly random, but may satisfy various statistical criteria of randomness and, as such, the numbers of the sequence are referred to as pseudorandom numbers. The most widely used pseudorandom number generator is the multiplicative congruential generator due to Lehmer (1951) in which a new random integer is generated from the current random integer as follows:

$$\text{New } I = (K \times \text{old } I + C) \text{ modulo } M, \quad (1.1)$$

where  $I$  denotes an integer and  $K$ ,  $C$ , and  $M$  are arbitrarily chosen constants. Numerous papers have been written giving positive evaluations of congruential generators in terms of their statistical properties. Marsaglia (1968) pointed out that congruential generators are not as satisfactory as they were thought to be because they can be shown to generate certain nonrandom patterns. Specifically, letting  $n$ -tuples of these pseudorandom numbers represent points in the unit cube in  $n$ -space, Marsaglia proved that the points are not randomly dispersed throughout the  $n$ -cube and that, in fact, they are concentrated in a relatively small number of hyperplanes. As a consequence, there is a tendency for these  $n$ -tuples to form patterns that can jeopardize certain types of Monte Carlo studies. Furthermore, this defect cannot be corrected by changing the values of the parameters  $K$ ,  $C$ , and  $M$ . From a practical standpoint, in the operation of large Monte Carlo dose computation programs, Frigerio (1968,

1969, 1975) found that one of the best congruential random number generators, namely that given by 1.1 with  $K = 5^{15}$ ,  $C = 0$ , and  $M = 2^{47}$ , was inadequate as a generator since it produced bias errors up to 1.5%. Also, Coldwell (1974) pointed out that in simulating an ideal gas, particle configurations generated by taking successive pseudorandom numbers given by the IBM routine RANDU as particle coordinates behaved more like a crystal than an ideal gas. This behavior supports the theoretical result of Marsaglia (1968).

In view of the theoretical and practical shortcoming of the widely used congruential method, there is clearly a need to consider better random number generators. Several methods, which can be regarded basically as variants of the congruential method, have been proposed with the idea of getting numbers that are "more" random. For instance, MacLaren and Marsaglia (1965) suggest the use of two congruential generators in such a way that one generator is used to shuffle the sequence produced by the other. Marsaglia (1976) points out that this method has passed extensive tests for randomness and has not displayed regularities of the type observed for congruential generators used alone. He then conjectures that by doubling or tripling the time involved in using a single generator, it seems possible to produce satisfactory sequences for general Monte Carlo use. However, he adds that there is no guarantee that the combination method will be satisfactory for a new level of sophistication for simulation problems. Various criteria are used to judge the quality of a pseudorandom number generator. We shall focus on methods of generating uniformly distributed random numbers since random numbers conforming to other distributions can be generated by suitably transforming uniform random numbers.

In evaluating a pseudorandom number generator, we shall define the goal as that of generating a sequence which strongly resembles a sample realization of independent identically distributed random variables from the uniform distribution on the unit interval. The three criteria which are generally used in evaluating a pseudorandom number generator are as follows:

- (1) A generator based on a recurrence relation produces numbers that repeat at some point, i.e., are periodic. The period must be of adequate length.

- (2) The sequence of random numbers must conform to the uniform distribution on the unit interval.
- (3) Variables representing the numbers separated by different lags must be statistically independent.

Of the three criteria listed above, criterion (1) is the most clear-cut although in some cases determination of the length of period could be difficult. A method with unknown periodicity is usually eliminated from consideration. There exists, however, an extensive literature relating to periodicities for congruential sequences (Refs. 7, 10, 16, 25-28, 30, 36), and existing theorems do enable us to find methods with adequately long periods. We shall, therefore, restrict ourselves to generators which satisfy criterion (1) and evaluate them solely on the basis of criteria (2) and (3). Application of criteria (2) and (3) is somewhat vague since it is accomplished by subjecting the specific generator output to a battery of statistical tests, each of which merely provides evidence in support of or against randomness. Satisfactory statistical performance with respect to a few chosen tests does not thus establish randomness unequivocally. In practice, a given sequence is subjected to several different statistical tests and is considered random if it passes these tests satisfactorily. In addition to empirical tests of this type, there are theoretical tests by which one can analyze the characteristics of a sequence. The theoretical tests employ number-theoretical methods based on the recurrence rule used to form the given sequence. One of the most important theoretical tests is the spectral test devised by Coveyou and MacPherson (1967). The basis for the spectral test is the fact that any series of random variables is completely characterized by its spectrum which involves a Fourier transformation of the series. Coveyou and MacPherson essentially give a method for computing the Fourier coefficients associated with a given congruential generator and also show how to assess randomness on the basis of these Fourier coefficients. After analyzing the MacLaren-Marsaglia method involving two congruential generators and a wide variety of simple multiplicative congruence generators (of the type referred to at the beginning of this section), Coveyou and MacPherson concluded that:

*With respect to the spectral test, the simple multiplicative congruence method with a carefully chosen multiplier did as well as or better than any other existing method of generating a pseudo-uniform sequence.*

In view of the theoretical and practical inadequacy of multiplicative congruential generators referred to earlier, the above conclusion provides a compelling reason to search for more effective ways of generating random numbers.

Alternatives to the computer-based methods of producing random numbers are provided by physical processes which are generally referred to as "random number devices" (RND). Various physical processes have been suggested and they include radioactive decay, laser vacuum noise, and electronic noise. Such processes can be regarded as sources of truly random numbers in the sense that the output is unpredictable and irreproducible. By using an RND to generate random numbers one can avoid the theoretical problems encountered in the use of pseudorandom number generators. In practice, however, it is extremely difficult to construct a stable physical generator that is fast enough for on-line computer use. The feasibility of a generator based on electronic noise, that is fast enough for on-line computer use, has been demonstrated recently (Cohn 1969, 1971). However, owing to the imperfections of practical electronics and to certain theoretical considerations such as finite noise bandwidth, the above method cannot yield anything approaching a perfect set of random numbers. It must also be emphasized that any RND for on-line use must be monitored continually via tests of relevant frequency distributions generated by the process. The practical difficulty in instituting such a check prompted us to consider generating tapes of random numbers using an appropriate RND. Such sets of random numbers have the advantages of being thoroughly tested and of being completely known (which is an important consideration in debugging programs). Furthermore, in spite of the general feeling that an on-line generator, such as a noise generator, somehow ought to be faster, it is known from the experience of Frigerio that using a tape is in fact more efficient. Most modern computers use no CPU time at all on input-output of a tape because they have the necessary buffered capacity for input-output while the program is still running on the CPU. The supply of random numbers available on any particular tape would, of course, be subject to a limit. However, this is not a serious problem since additional tapes can be created by operating the RND for a longer period of time. It might also be pointed out that even a limited set of truly random numbers would be worthwhile to have since one can use it in conjunction with a congruential generator [as suggested by Rubin (Ref. 39) and Cook (Ref. 14)] to create a large set dependent on the limited set for its randomness.

The better pseudorandom number generators are probably adequate for most small scale Monte Carlo computations, although even here it is a good idea to try several of them. However, for large scale Monte Carlo studies requiring a high resolution, the limitations of pseudorandom number generators could be serious enough to warrant the use of a large set of truly random numbers. The following are some examples of large Monte Carlo studies performed at Argonne, for which the use of truly random numbers were especially important.

1. Simulation of accident experience in the nuclear and other industries to optimally predict the relative probabilities and interactions of human errors, mechanical failures, and natural events.
2. Simulation of the leakage and breakdown history of very large numbers of radioactive fuel elements and fuel containers stored at varying periods under varying conditions and for periods of time ranging into many centuries.
3. Simulation of an experiment to determine the optimal size and position of testing recorders and apparatus for the Argonne Magnetic Spark Chamber and to estimate the number of events that would go undetected between recorders.
4. Simulation of sparks on a particle track to test different circle-fitting methods.
5. Simulation of points on tracks in a non-uniform magnetic field which are then fitted with helices. Errors in measurement of these tracks are simulated by displacing the points randomly.
6. Calculation of energy loss for gamma rays incident on germanium crystals.
7. Simulation of a biological model for granulocyte maturation and release into the blood.
8. Simulation of counts of particles in a fluidized bed.
9. Simulation of birth and death processes.
10. Study of the effect of noise on a system by adding random magnitudes to parameters of a program.

The preceding was a discussion of our motivation for attempting to create a set of truly random numbers that can be labeled almost perfect. Our strategy for generating such a set and an assessment of the statistical performance of our random number generator are presented in the remainder of this report.

## II. STRATEGY FOR CREATING ALMOST PERFECT RANDOM NUMBERS

The need for considering truly random numbers in place of pseudorandom numbers is evident from the discussion in Section I. The difficulties associated with the construction of a reliable fast-enough random number device (RND) for on-line use, and the problems involved in the continual monitoring of such an RND have also been pointed out. These practical considerations prompted us to abandon the idea of an on-line physical generator. Instead, we focused on alternative methods of constructing an RND, with the idea of generating tapes of random numbers that would satisfy various accepted criteria of randomness. The advantage of this approach, as already pointed out, is that it provides the user with a thoroughly tested and completely known set of random numbers, with the same efficiency as that of an on-line generator (since most modern computers use no CPU time on input-output of a tape).

One of the paradigms of nuclear science is the process of radioactive decay, which is generally believed to be of the Poisson type. The Poisson model is taken typically to characterize a counting process with independent increments, i.e., such that the counts in two non-overlapping intervals are independent of each other. RND's based on the process of radioactive decay have been considered in the past (Shreider 1966 and Vincent 1970). A radioactive RND, in principle, consists of a source emitting radioactive particles and a counter which records the number of particles detected during a time interval of fixed length. Depending on whether or not the count is even or odd, the corresponding digit in the RND is set equal to zero or one. This results in strings of 0's and 1's constituting binary numbers which are then converted into decimal numbers. To insure that the final set of decimal numbers conforms to the uniform distribution, it is necessary to take certain steps which are discussed in Section IV. The above approach to the generation of truly random numbers is theoretically sound. However, translating this theory into hardware for large scale use has not been done before. The work reported here was undertaken to develop the necessary hardware and to produce acceptable sets of random numbers.

We began our experimentation using a simple procedure (System I)--namely, a system consisting of a Cs-137 gamma source and a NaI crystal

counter (Frigerio 1973). The counts were fed into a 400-channel analyzer operated in time mode. Each channel recorded counts for 10 sec in chronological sequence, and at the end of a 4000-sec sweep, the memory was dumped onto paper tape and the cycle repeated. This system has two drawbacks. Firstly, it is slow in that each channel gives rise to only one useful bit, depending on whether its content was odd or even and, hence, one can only generate  $10^4$  bits per day. Secondly, gamma Compton events create an energy spectrum which is continuous into the noise level. Thus, instantaneous count rate depends critically on the stability of a discriminator--a classic example of "the house built on shifting sands." Since subsequent count distribution analyses would depend heavily on the average count rate, we abandoned this system.

Further trials with beta and gamma systems indicated that counts were too dependent on equipment shifts, temperature, slow chemical changes, backscatter, etc. to give the kind of precision and reproducibility that we required. A large part of this was a consequence of the continuous Compton and/or beta distributions, which formed the baseline against which counts were measured. Even a small shift in the energy window used for the isolation of counts resulted in a discernible change in count rate. Pile-up and pulse-size effects were also aggravated by the presence of electron noise, and of "useless" counts, in the lower regions of the continuum.

A more successful system (System II), which we tried, employed a U-235 alpha-particle source in a high-resolution, gas, proportional counter, with the signals fed to a 4096-channel analyzer (Frigerio 1965, 1973). Each channel recorded counts for 16,650 microsec, with an additional 16 microsec per count period allowed for baseline restoration and address shift. At the end of a 4096-channel sweep the memory was dumped onto a magnetic tape and the cycle repeated. This system produced about  $2 \times 10^5$  bits per day. In addition, the natural energy separation of the 5.5-MeV alpha events from noise and other signals was so great that the count rate was independent of electronic parameters to at least the  $1 \times 10^{-6}$  level. Channels 1 and 4096 were reserved for start and stop signals, so 4094 useful bits were obtained per cycle.

To be sure that a system of the above type is operating properly, it is necessary to analyze the frequency distribution of counts generated by the system. Theoretically, a radioactive decay process is expected to conform to a Poisson distribution. However, a distinction has to be made between the statistics of counting and the statistics of decay. Even if one radioactive decay does not affect the probability of another decay, it may easily affect the probability of its detection in any real system (Evans 1962, Fry 1965, Frigerio 1968 and Schiff 1936). In order for a counter to register a particle, that particle must be preceded by a certain small interval during which no particle arrives at the counter. The length of this blank interval is called the resolving time or dead time of the counter. The effect of dead time has been taken into account by Schiff (1936) and more recently by Brockwell and Moyal (1966).

Our next step was to fit the Brockwell-Moyal distribution to the frequency data from the alpha-counting system just described (Frigerio 1973). By means of a memory oscilloscope the experimental dead time was found to be  $8.81 \pm 0.03$   $\mu$ sec. Results of our fit, along with a discussion of the Brockwell-Moyal distribution are presented in Section III. These results show excellent agreement between data and theory, indicating proper functioning of the system.

The above system still appeared to have some disadvantages. The tape transfer system was slower than necessary, the dead time was long, and the use of a 60-cycle clock driven from the power lines made the system mean somewhat subject to powerline fluctuations and impulses. Therefore, System III was devised to operate from a crystal-controlled 50-cycle clock, with a dead time of only 0.8 microseconds, and to feed an IBM-1130 computer directly via an analog-digital hybrid link (Duparc 1953). Counts were written directly onto the 1130 disc in buffered sets of 316 16-bit words, each word containing the counts recorded in a 20,000-microsecond interval. This system was capable of accumulating nearly 50 counts per second, i.e., about 3.8 million useful parity bits per day. A day's running time, in fact, produced 3,791,052 counts at an average rate of 24.415761 events per 20,000-microsec count period. Dead time, measured by the two-source method, was 0.80 microsec with a standard deviation of about 0.01 microsec. However, oscilloscopic measurement gave a short-term value of  $0.8 \pm 0.1$  microsec because of pulse jitter.

This jitter was apparently fixed at about 0.1 microsec, and was not observed with the earlier alpha system because of the much slower rise and decay times of the long dead-time pulses.

The frequency data from System III was subjected to extensive tests (details of which can be found in Section III). The results enabled us to conclude that the system was functioning properly and that we finally had a feasible mechanism for generating random numbers.

System III was used to accumulate 3,791,052 counts, containing a total of  $9.2 \times 10^7$  events (Ref. 3a), at an average count rate of 24.31576 events per 20-millisecond count time. The parity bits of these counts (0 for an even count and 1 for an odd count) were then assembled in sequence to form 122,292 31-bit binary random number words, and these were transcribed to magnetic tape (Ref. 3b). Conversion of these binary numbers to decimal numbers and properties of the resulting numbers that are dependent on the parameters of the counting process employed are discussed in Section IV. The set of random numbers that we generated was further subjected to a battery of tests for randomness and uniformity of distribution. The results are given in Section V. The present tape set passed all of these tests among which are twelve chi-square tests, tests of moments, serial correlation tests, and a periodogram analysis. [An additional set of  $2\frac{1}{2}$  million random numbers was also generated but not analyzed (Ref. 3c).]

Six other laboratories have obtained copies of this tape set of random numbers which seem to be producing good results. Generating additional random numbers poses no problem. Once the equipment is set up, running the numbers off is easily accomplished. Resorting to the same parameters as before (which are optional for our equipment) we can produce one bit every 50th of a second. The machine can thus generate about 150,000 bits a day, or about 50 million a year. The machine runs at no cost and the computer time required to reduce the tapes to random numbers is almost negligible.

### III. THE BROCKWELL-MOYAL MODEL FOR RADIOACTIVE DECAY AND ITS VALIDATION

In the previous section we described the alpha-counting system that we developed for the purpose of generating truly random numbers. It is possible to spot anomalies in the system by analyzing the frequency data it generates. An analysis of our data showed that our system was functioning properly. Details of this analysis are presented in this section, along with a discussion of the theoretical model behind the analysis.

The rationale for using a radioactive decay process for generating random numbers has already been discussed. Basically, it is the Poisson nature of the process that justifies its use as an RND. A confirmation of the Poisson process would not only provide justification for using this type of RND, but also provide evidence for the proper functioning of the system.

Theoretically, the number of radiated particles emanating from a radioactive source during a time interval of fixed length is expected to follow a Poisson distribution. However, recent work (Anderson 1972) questions this hypothesis on the basis of count data from several beta and gamma systems. Part of this discrepancy can be traced to the difference between the statistics of counting and the statistics of decay. Counting mechanisms generally have a positive resolving time, so not all particles arriving are registered (counted). A distinction has to be made between the process represented by the number of arriving particles. The experimenter observes only the latter and is required to use it to infer the properties of the underlying decay process.

Specifically, in order for a counter to register a particle, that particle must be preceded by a certain small interval during which no particle arrives at the counter. The length of this blank interval is called the resolving time or dead time of the counter. It is necessary to take the effect of dead time into account before we can determine the properties of a given radioactive decay process, including the decay constant (which is defined as the mean number of particles arriving at the counter per unit time). Efforts along these lines have been made by Schiff (1936), who used the relationship between the expected number of particles arriving in a given period and the expected

number that registered to obtain estimates of the actual counts from the observed counts. He then used estimated actual counts to determine the decay constant. Estimating the actual counts, however, can be done only with the knowledge of the parameters of the process and Schiff suggests assuming approximate parameter values for this purpose. A more rigorous approach is possible by considering the probability distribution of the observed counts.

The process considered here is similar to the one considered by Brockwell and Moyal (1966) in the context of bubble chamber measurements. The latter arises when a particle travels through a chamber generating events (formation of a bubble) at random. The distances between successive bubbles are used to estimate the velocity of the particle whose track is observed. However, owing to the nonzero diameter  $d$  of the bubble, only those distances ( $Y_i$ ) which are greater than the bubble diameter are observed. Hence, in order to estimate velocity, a knowledge of the distribution of the number of  $Y_i$ 's greater than  $d$  is required. This distribution was derived by Brockwell and Moyal (1966) and can be applied to the present situation, since the registered particles correspond to interarrival times (time between arrivals of successive particles) that are greater than the resolving time. Brockwell and Moyal (1966) first determine the probability generating function for the process constituted by the  $Y_i$ 's and then use it to find the distribution of the number of  $Y_i$ 's greater than  $d$ . In Appendix A we present a different approach, one which leads to a specific joint distribution and a related method of estimating the process parameters.

The Brockwell-Moyal distribution reduces to:

$$P(m) = \sum_{s=m}^{\lfloor t/d \rfloor} \frac{(-1)^{s-m} e^{-sd\lambda} \lambda^s [t - sd]^s}{m!(s-m)!} \quad \text{for } m \leq t/d, \quad (3.1)$$

where  $P(m)$  is the probability of  $m$  particles being registered at the counter in time  $t$ ,  $d$  is the resolving time or dead time,  $\lfloor t/d \rfloor$  is the greatest integer  $\leq t/d$ , and  $\lambda$  is the mean relaxation time ( $\lambda$  can also be defined as the intensity parameter of the Poisson process for the actual counts).

The following analysis pertains to data generated by System II. The mean  $\bar{m}$  was 20.391059 events per 1.050  $\mu\text{sec}$  for 872,022 runs (213 cycles of 4094 counts each). From a comparison of mean and variance (which are theoretically the same under the Poisson distribution) computed from the data, it was evident that the Poisson distribution provided a poor fit for this data. This was confirmed by a  $\chi^2$  value of 229 which was computed using 38 categories formed by grouping  $m$  values from 0 to 4 and  $m$  values greater than 40. With 36 degrees of freedom, the observed  $\chi^2$  leads to the rejection of the Poisson hypothesis at a significance level less than 0.001.

Next, we tried the Brockwell-Moyal (BM) distribution and obtained the following results: The dead time for System II, as measured with a memory oscilloscope, was  $8.81 \pm 0.03 \mu\text{sec}$ . Assuming this  $d$  value,  $\lambda$ , was estimated from the data using the equation

$$\bar{M} = \lambda(t - d) e^{-\lambda d}, \quad (3.2)$$

where  $\bar{M}$  is the mean of the observed counts. The right-hand side (RHS) of (3.2) is the mean of the BM distribution and thus the above method of estimation reduces to the method of moments. Solution of (3.2) involves an iterative procedure which is outlined in Appendix A.

Expected values based on the fitted distribution were computed and compared with the observed counts. The resulting  $\chi^2$  value was 26.90 with a  $P$  value of 0.86 for 36 degrees of freedom, indicating an excellent fit.

We also carried out the following second-order diagnostic check. The 213 counting cycles, each consisting of 4094 counts, were treated as subsampled. The BM distribution with the same  $d$  and  $\lambda$  values as those applicable to the entire data was fitted to each of the 213 subsamples.  $\chi^2$  values were computed in each case and the distribution of observed  $\chi^2$  values was compared with the theoretical  $\chi^2$  distribution with 25 degrees of freedom (the same 25 categories were used). Results are presented in Table 1 and show a remarkable agreement between observed and theoretical values. Besides confirming the excellent fit of the BM distribution to the data, this second-order check confirms that the system experienced hardly any fluctuation throughout the observation time.

In the present situation, since  $d$  was determined experimentally, it was necessary to estimate only  $\lambda$ . One can obviate the need for determining  $d$  experimentally by estimating  $d$  and  $\lambda$  simultaneously from the data. Methods of doing so are discussed in Appendix A. Even when the experimental value of  $d$  is available, it is helpful to estimate  $d$  and see how well the two values agree. A quick check of this type was made by varying the value of  $d$  (as shown in Table 1) and determining the  $d$  value with minimum  $\chi^2$ . This method yielded an estimated value of  $\hat{d} = 8.82 \mu\text{sec}$ , which agrees well with the oscilloscope value.

As pointed out in Section II, System II was revised in order to correct certain drawbacks. The following analysis pertains to data from System III. Dead time for System III, as measured by the two-source method, was  $0.80 \pm 0.01 \mu\text{sec}$ . However, oscilloscopic measurement gave a short-term value of  $0.8 \pm 0.1 \mu\text{sec}$  because of pulse jitter. The jitter was apparently fixed at  $0.1 \mu\text{sec}$ . This had not been observed with System II, probably because of much slower pulse rises and decay times.

System III was used to collect 3,791,052 counts at an average rate  $\bar{M}$ , of 24.415761 events per 20,000  $\mu\text{sec}$ . By using (3.2)  $\lambda$  was estimated to be 0.001219. The frequency data from System III were also subjected to the same tests as before. For the BM distribution with  $d = 0.8 \mu\text{sec}$ , the  $\chi^2$  value was 29.3 for 30 degrees of freedom, leading to a P value of 0.5 and, hence, the plausibility of the BM distribution is supported. By contrast the  $\chi^2$  value with the Poisson was 44.3 ( $P < 0.05$ ), leading to the rejection of the Poisson hypothesis.

We also used a normed measure of the following type as a supplement in assessing goodness of fit. Consider the measure

$$I = \frac{\sum_{i=1}^r \text{Min} (O_i, E_i)}{T}, \quad (3.3)$$

where  $T$  is the total number of observations,  $r$  is the number of categories,

Table 1. Chi-Squared Comparisons of Theoretical and Experimental Distributions (System II)

<i>Test for Minimum d</i>		<i>Comparison of Distributions</i>		
<i>d/t</i>	$\chi^2$	<i>P</i>	$\chi^2$ , <i>theory</i>	$\chi^2$ , <i>experiment</i>
0.0 (Poisson)	228.9	0.99	11.5	10.3
$1.0 \times 10^{-8}$	228.9	0.98	12.7	12.9
$6 \times 10^{-5}$	186.4	0.95	14.6	14.9
0.00036	47.85	0.90	16.5	16.6
0.00040	39.07	0.80	19.0	19.6
0.00048	28.58	0.70	20.9	20.9
0.00049	27.94	0.50	24.3	23.8
0.00050	27.45	0.30	28.2	27.6
0.00051	27.12	0.20	30.7	30.1
0.00052	26.93	0.10	34.4	34.0
0.00053	26.90	0.05	37.6	37.5
0.00054	26.96	0.02	41.6	41.3
0.00055	27.01	0.01	44.3	43.3
0.00056	27.28			
0.00057	27.71			
0.00058	28.28			
0.00060	30.94			

*In testing for minimum d/t 38 groupings were used; k = 0-4, 35 groupings of  $\Delta k = 1$ , and k = 41- $\infty$ . Allowing one restriction on total and one on mean afforded 36 degrees of freedom.*

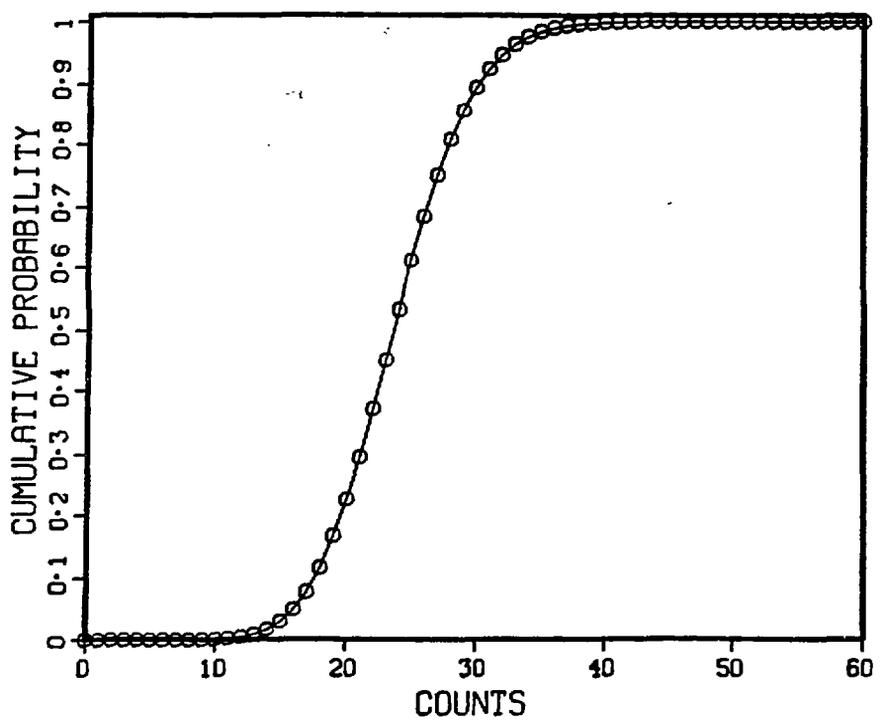
*In comparison of distributions 27 groupings were used; k = 0-9, 25 groupings of  $\Delta k = 1$ , and k = 35- $\infty$ . Restrictions as above afforded 25 degrees of freedom.*

$O_i$  is the observed number in the  $i^{\text{th}}$  category and  $E_i$  is the corresponding expected number. (A program to compute the BM probabilities is included in Appendix B.) Then  $I$  is a normed measure between 0 and 1 such that  $I = 1$  implies perfect agreement between data and theory and 0 represents perfect disagreement.

Table 2 shows the distribution of observed counts and the fitted BM distribution. The value of  $I$  is 0.9990 indicating a very high degree of conformity of our data to the BM distribution which can also be seen in Figure 1. The corresponding  $I$  value with respect to the best fitting Poisson is 0.9877, which is also reasonably high. The fact that we are able to reject a distribution with such a high  $I$  value shows that our sample provides a high degree of discrimination between alternative distributions. It is

Table 2. Distribution of Observed Counts for System III  
and the Fitted Brockwell-Moyal Distribution

<i>m</i>	<i>Observed Frequency</i>	<i>Expected Frequency</i>	<i>m</i>	<i>Observed Frequency</i>	<i>Expected Frequency</i>
0	3	0	30	146,784	146,570
1	0	0	31	113,998	114,656
2	0	0	32	86,960	86,882
3	0	0	33	63,595	63,836
4	1	1	34	45,725	45,519
5	8	7	35	31,846	31,528
6	31	30	36	21,082	21,229
7	110	106	37	13,901	13,907
8	350	324	38	9,010	8,870
9	889	876	39	5,497	5,512
10	2,231	2,129	40	3,344	3,339
11	4,773	4,702	41	2,041	1,973
12	9,486	9,517	42	1,122	1,138
13	17,857	17,779	43	628	641
14	30,812	30,838	44	326	353
15	49,880	49,919	45	202	190
16	75,712	75,751	46	113	100
17	107,983	108,180	47	47	51
18	145,926	145,896	48	20	26
19	186,293	186,391	49	23	12
20	226,066	226,202	50	0	6
21	261,899	261,422	51	0	2
22	288,424	288,369	52	0	1
23	304,320	304,240	53	0	0
24	306,008	307,586	54	0	0
25	299,309	298,505	55	0	0
26	278,861	278,529	56	0	0
27	250,707	250,243	57	0	0
28	216,926	216,783	58	0	0
29	180,871	181,307	59	0	0



Solid line: Theory

Open circles: Observed cumulative frequencies

Fig. 1. Empirical Fit of the Brockwell-Moyal Distribution  
Obtained by Using System III.

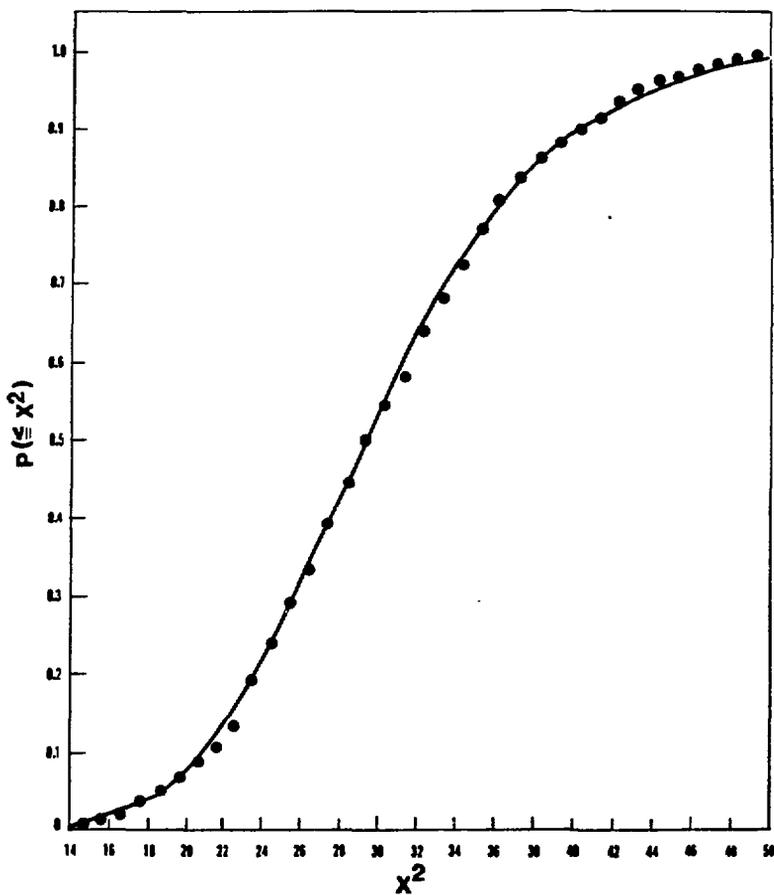
also to be noted that the  $d$  value in this case is only 0.8  $\mu\text{sec}$ , which accounts for the rather small difference in  $I$  values between the Poisson and the corresponding BM distribution. For larger values of  $d$ , the disparity between the two distributions would be more pronounced.

The second-order diagnostic check, described earlier, was also performed using data from System III.  $\chi^2$  values were computed for 600 subsamples (cycles) each consisting of 6320 counts. Results are presented in Figure 2 along with the theoretical  $\chi^2$  distribution of 30 degrees of freedom. Considering that the cumulative distribution form used here amplifies small discrepancies and that a small deviation in one direction must await a compensating deviation in the opposite direction for the points to conform to the theoretical curve, the agreement we see is quite remarkable.

As before,  $d$  was estimated from data (using the minimum  $\chi^2$  approach. Other approaches are given in Appendix A). The  $\chi^2$  values gave a flat minimum for  $d = 0.7$  to  $0.9 \mu\text{sec}$ , probably reflecting the jitter referred to earlier. A comparison of theoretical moments with sample moments (results shown in Appendix A) again indicated close agreement between theory and data.

The validation of the BM distribution using counts generated by this system has essentially the following implication for random number generation. It strongly supports the assumption of independent interarrival times (which is the basis for the BM distribution as pointed out in Appendix A) and, hence, the randomness of the numbers generated (in the sense of zero serial correlation). It also attests to the proper functioning of the equipment without which the theoretical expectation of randomness is not necessarily fulfilled.

In a broader perspective, our experimental validation of the BM distribution demonstrates its applicability to any radioactive counting situation. Conversely, the applicability of the Poisson is refuted, even for dead times in the sub-microsecond range. Since earlier reports of non-Poisson behavior were based on counting systems with dead times of at least 8  $\mu\text{sec}$ , much of the discrepancy observed could be explained by the effect of dead time. As a corollary, the underlying Poisson distribution of decay, on which the BM distribution is based, is confirmed for alpha decay. For beta-gamma decay,



Solid line: Theoretical cumulative  $\chi^2$ -distribution

Points: Observed cumulative frequencies

Fig. 2. Comparison of the Cumulative Frequency Distribution of the Observed Chi-Square Values and the Distribution Function of Chi-Square for 30 Degrees of Freedom Using System III.

however, the situation is vastly complicated, not only by instrumental considerations, but also by the possibility of other effects (Anderson 1972, Bainbridge 1951 and Emeury 1972). Thus, while correction via the above distribution should certainly be applied to beta-gamma studies of radioactive decay, it is doubtful that this alone will provide a satisfactory solution of the problem. The BM distribution may well provide a good model for counting effects in other contexts which otherwise mask the underlying statistics.

Thus far, we have been concerned with the randomness of the numbers (i.e., the statistical property of independence among variables representing the numbers separated by different lags) generated by our system. The above validation of the BM distribution provides strong evidence for the random nature of our numbers, which is further confirmed through direct tests of randomness discussed in Section V. However, it does not shed any light on the distribution of the random numbers generated. The objective, as pointed out in Section I, is to create uniformly distributed random numbers. The distributional aspect of our random number generator is discussed in Section IV.

#### IV. INSURING A UNIFORM DISTRIBUTION OF RANDOM NUMBERS

In the previous section we focused on the criterion of randomness in evaluating our RND. In this section we turn to the second criterion--namely, that the sequence of random numbers must conform to the uniform distribution on the unit interval.

Consider a sequence of independent identically distributed random variables  $X_i$  such that each  $X$  takes the value 1 with probability 1/2 and the value 0 with probability 1/2. Define a random variable  $Z$  of the form

$$Z = \sum_i X_i 2^{-i} , \quad (4.1)$$

where the summation extends over  $n$  terms in the  $X_i$  sequence. One can regard  $Z$  as a random number whose binary digits correspond to  $X_i$ 's. As  $n$  approaches infinity, the distribution function  $F_n(z)$  of  $Z$  approaches (Shreider 1966) the uniform distribution function  $F(z)$  and

$$|F(z) - F_n(z)| < \frac{1}{2^n} . \quad (4.2)$$

In the present case, the parity bits of radioactive decay counts (0 for an even count and 1 for an odd count) were grouped into 31-bit binary words and transcribed to a tape. These 31-bit binary words can in turn be converted into numbers between 0 and 1 using equation (4.1) and  $n$  equal to 31 (comparable with the bit size of the computer). In view of (4.2) the resulting sequence of random numbers can be expected to conform to a uniform distribution, provided the probability of an even count is the same as that of an odd count. These probabilities are evaluated as follows: let  $M$  denote the total number of particles registered at the counter in time  $t$ . Then (Parzen 1962)

$$P[M \text{ is even}] - P[M \text{ is odd}] = \sum_m (-1)^m P[M=m] , \quad (4.3)$$

where  $P[M=m]$  is given by the Brockwell-Moyal distribution defined in Section

III, equation (3.1). From (4.3) and (3.1) it follows that

$$P[M \text{ is even}] - P[M \text{ is odd}] = \sum_{m=0}^{[t/d]} \sum_{s=0}^{[t/d]} \frac{(-1)^s e^{-sd\lambda} \lambda^s (t - sd)^s}{m!(s - m)!}, \quad (4.4)$$

where  $d$  is the resolving time or dead time,  $[t/d]$  is the greatest integer  $\leq t/d$  and  $\lambda$  is the mean relaxation time (See Section III for definitions of these parameters). The RHS of (4.4) can be rewritten as

$$\sum_{s=0}^{[t/d]} (-1)^s e^{-sd\lambda} \lambda^s (t - sd)^s \sum_{m=0}^s \frac{1}{m!(s - m)!}. \quad (4.5)$$

But

$$\sum_{m=0}^s \frac{1}{m!(s - m)!} = \frac{1}{s!} \sum_{m=0}^s \frac{s!}{m!(s - m)!} = \frac{2^s}{s!}. \quad (4.6)$$

Thus, from (4.5) and (4.6) we have

$$p[M \text{ is even}] - P[M \text{ is odd}] = \sum_{s=0}^{[t/d]} \frac{[-2 e^{-\lambda d} \lambda (t - sd)]^s}{s!}. \quad (4.7)$$

As  $d \rightarrow 0$ , the BM distribution approaches the Poisson distribution with intensity parameter  $\lambda$ . In this limiting situation

$$P[M \text{ is even}] - P[M \text{ is odd}] = \sum_{s=0}^{\infty} \frac{[-2\lambda t]^s}{s!} = e^{-2\lambda t}. \quad (4.8)$$

It is evident from (4.8) that the bias between the probabilities for an even and an odd count can be reduced by increasing  $\lambda t$ , the mean count. In order to generate uniformly distributed random numbers one must therefore choose  $t$  (the time spent on finding one binary digit) so that the average number of particles counted during this period is reasonably large. The bias in probabilities for System III computed on the basis of (4.7) is  $-1.7 \times 10^{-9}$ . We consider this amount as negligible. The actual frequencies of even and odd counts are 1,895,329 and 1,896,671, respectively. However, even if the system has a non-

negligible bias it is possible to generate uniformly distributed random numbers using a bias-removing technique such as the following (Shreider 1966, pp. 22).

Let  $X_i$ 's represent the original sequence of 1's and 0's. Define  $Y_i$  such that

$$Y_i = \begin{cases} 1 & \text{if } X_i = 1, X_{i+1} = 0 \\ 0 & \text{if } X_i = 0, X_{i+1} = 1 \end{cases} .$$

If  $X_i = X_{i+1}$ , then  $Y_i$  is determined from a later pair  $X_{i+k}, X_{i+k+1}$  whose values are distinct. Denoting the probability that  $X_i = 1$  by  $u$  we see that

$$P(Y_i = 1) = \frac{u(1-u)}{u(1-u) + (1-u)u} = \frac{1}{2} .$$

The average number of steps required to find a suitable pair is

$$\frac{u^2 + (1-u)^2 [1 + 2u(1-u)]}{2u(1-u)} . \quad (4.9)$$

In particular, if  $u \sim 1/2$ , the above method involves discarding approximately 50 percent of the binary digits. In the present case the bias was so small as to obviate the need for a bias-removing technique.

In Sections III and IV we have essentially dealt with methods of insuring that a radioactive decay counting system generates uniformly distributed random numbers. Section III was devoted to the aspect of randomness and Section IV to the distributional aspect. Results of applying the relevant checks to our RND are also given in these sections. Both Systems II and III were judged to be highly satisfactory with regard to both these aspects. System III is, however, more efficient from a practical point of view and is the one that we employed to generate the present tapes of random numbers. A sample from this set of random numbers was further subjected to a battery of tests for randomness and uniformity of distribution. Results of these tests are given in Section V.

## V. STATISTICAL TESTS ON RANDOM NUMBERS

Kendall and Smith (1939) developed a series of tests for testing the "Randomness" of a sequence of numbers. These tests fall into four categories--namely, frequency tests, serial tests, gap tests and poker tests--and have been used widely for testing several random number generators (see e.g., Rand Corporation 1955). More recently, MacLaren and Marsaglia (1965) proposed a more stringent battery of tests designed to evaluate various congruential generators and to weed out the bad ones. This battery consists of tests of uniformity of single numbers, pairs, and triples, and tests based on the maximum of  $n$  random numbers, minimum of  $n$  and sum of  $n$ , for  $n = 2, 3, 4, 6$ , and  $12$ . The above battery of tests has also been employed successfully by Van Gelder (1967) for evaluating other types of pseudorandom number generators. We follow a similar procedure here for evaluating our RND. Following the approach used by Van Gelder, we chose a battery of primary tests on the basis of which we can judge the performance of our RND in an absolute sense and also in relation to some good "congruential estimators." A few tests that are secondary or confirmatory in nature were also selected.

The following twelve primary tests were selected with a view to determining whether a string of random numbers behaves statistically like numbers independently sampled from a uniform distribution.

- (a) Three chi-square tests of uniformity of single numbers, pairs and triples. The first of these tests is based on  $2^{10} = 1024$  cells (we can thus classify numbers using the first ten bits), the second on  $2^5 \times 2^5 = 1024$  cells (the first five bits being used in classification), and the third on  $2^3 \times 2^3 \times 2^3 = 512$  cells (the first 3 bits being used in classification).
- (b) A run test based on the frequencies of runs (up or down) of lengths 1, 2, 3, 4 and greater than 4, where a run length is defined as follows: The sequence 4 7 3 11 2 1 gives rise to the sequence + - + - - and, hence, to runs of lengths 1, 1, 1, and 2. Levene and Wolfowitz (1944) showed that the expected number  $e_k$  of runs of length  $k$  in a sequence of length

N is given by:

$$e_k = 2N \frac{k^2 + 3k + 1}{(k + 3)!} - 2 \frac{k^3 - 3k^2 - k - 4}{(k + 3)!} \quad (k \leq N - 2) . \quad (5.1)$$

The runs are classified according to their lengths and, therefore, are not strictly independent of each other. In this case, Levene and Wolfowitz suggested a  $\chi^2$  test involving the covariance matrix of the  $e_k$ 's. However, the usual  $\chi^2$  test is applicable here in an approximate way (as borne out by the conformity of our observed  $\chi^2$  values to the  $\chi^2$  distribution assumed here). We have, therefore, simplified our analysis by computing the usual  $\chi^2$  based only on the observed and expected frequencies. This remark also applies to all tests described in (c) and (d) which also involve runs.

- (c) A chi-square test based on the frequencies of runs of the same leading bit, for lengths 1, ..., 9 and greater than 9. Here  $e_k$  (defined in (b)) is equal to  $N/2^{k+1}$ .
- (d) A chi-square test based on the frequencies of lengths of runs of matched or mixed two leading bits for lengths 1, ..., 9, and  $> 9$ . The expected number  $e_k$ , in this case, is also equal to  $N/2^{k+1}$ .
- (e) Six chi-square tests based on the frequencies of runs of length  $k$  for  $k = 1$  or  $2, 3, \dots, \geq 11$ , where run lengths are defined as follows:

For the first test, run length is the length of the series until a zero bit is found in each bit position of the most significant 10-bit byte of the random number.

Run length is defined similarly for the 2nd and 3rd tests in this set, the difference being that instead of examining the most significant 10-bit byte, we examine the next 10-bit byte for the second test and the next 10-bit byte for the third test.

The remaining three tests in this set are also defined similarly, the difference being that instead of requiring that a zero bit be found in each position, we require that a one be found in each bit position.

For all of the above six tests, the expected number  $e_k$  of runs of length  $k$  in a sequence of  $N$  numbers is given by:

$$e_k = \frac{N}{\sum_{j=1}^m (-1)^{j+1} \binom{m}{j} \left(\frac{1}{1-0.5^2}\right)} \left[ \left(1 - 0.5^k\right)^m - \left(1 - 0.5^{k-1}\right)^m \right],$$

where  $m$  is the number of bits in the byte.

For testing purposes, we divided the set of 122,292 31-bit numbers into ten consecutive sets of 12,229 numbers each. These eleven sets (the whole set and the ten subsets) were subjected to the above battery of twelve chi-square tests. The sample sizes were large enough to permit frequency tests for single numbers and pairs involving an examination of more than the high order two or three bits (As pointed out in (a), with 1024 cells, we need to examine the first ten bits for single numbers and for pairs we need to examine the first five bits. The disadvantage of having, say, only ten cells is that only the first decimal digit of the random numbers is tested, and one-digit accuracy is usually not adequate).

The results of the above tests are summarized in Table 3. A total of 132 (12 × 11) chi-square values were produced. Corresponding to each of these  $\chi^2$  values there is a percentile  $\alpha$  which represents the probability that a random sample would give a worse (larger) value of  $\chi^2$ . The resulting 132  $\alpha$  values are not mutually independent, but each one is uniformly distributed under the hypothesis that the random numbers are independent and uniformly distributed. The 132  $\alpha$  values can be conveniently summarized by the numbers that fall below 0.5, below 0.05, below 0.025, and below 0.005. The theoretical average values for these numbers are 66, 6.6, 3 and 0.6. The observed numbers are 61, 5, 2, and 1, which are in agreement with the expected values. The performance of the present generator can, therefore, be considered satisfactory on the basis of the twelve  $\chi^2$  tests. To get a better picture of its performance we also

Table 3. Chi Square Values for Tests with Given Degrees of Freedom

		<i>Degrees of Freedom</i>											
		1023	1023	511	4	9	9	9	9	9	9	9	9
<i>Set</i>	<i>Freq.</i>	<i>Pairs</i>	<i>Triples</i>	<i>Runs Up/Down</i>	<i>Runs Hi/Low</i>	<i>Runs Mid/Extr</i>	<i>High 10 Bits</i>		<i>Middle 10 Bits</i>		<i>Low 10 Bits</i>		
							<i>And to 0's</i>	<i>Or to 1's</i>	<i>And to 0's</i>	<i>Or to 1's</i>	<i>And to 0's</i>	<i>Or to 1's</i>	
First	12229	1030.2	990.4	485.2	3.17	6.22	5.13	8.80	7.11	8.55	10.98	5.30	7.93
Second	"	1040.3	1063.9	540.2	2.00	7.05	7.36	12.26	5.42	8.01	8.99	8.42	10.83
Third	"	984.2	1004.3	567.0	7.82	5.08	9.24	8.24	9.05	6.47	7.17	9.16	7.73
Fourth	"	1091.2	1011.3	471.1	1.31	11.52	13.09	10.08	<u>18.61</u>	12.18	<u>16.98</u>	6.53	12.84
Fifth	"	1054.5	1078.5	492.2	2.75	<u>2.06</u>	13.73	9.63	<u>26.45</u>	<u>1.94</u>	10.86	8.92	4.43
Sixth	"	1041.8	1048.2	469.1	3.24	4.27	4.41	13.30	6.82	4.37	8.13	7.16	8.05
Seventh	"	1027.7	1025.4	479.6	2.06	5.88	6.07	6.58	7.36	11.87	7.16	13.38	8.82
Eighth	"	976.7	977.8	461.3	8.54	10.01	4.33	4.26	11.81	13.97	5.21	8.79	<u>18.13</u>
Ninth	"	954.5	1019.7	538.0	0.82	9.99	7.12	6.43	7.81	8.50	3.38	16.04	6.28
Tenth	"	1016.3	<u>1116.5</u>	562.5	1.26	8.18	9.97	7.92	13.89	5.71	<u>2.29</u>	7.41	8.31
Whole	122292	989.2	1020.9	518.8	6.83	5.34	14.03	10.46	10.84	8.91	9.41	7.76	16.77

Note: Chi square values underlined are outside the 90% probability interval.

Chi Square Values for n Degrees of Freedom at Selected Probabilities

<i>n</i>	<i>p Values</i>								
	<i>p=0.995</i>	<i>.975</i>	<i>.95</i>	<i>.50</i>	<i>.05</i>	<i>.025</i>	<i>.005</i>	<i>.10</i>	
4	0.207	0.484	0.712	3.357	9.48	11.14	14.86	7.78	
9	1.735	2.532	3.321	8.343	16.92	19.02	23.59	14.68	
511	431.8	449.7	458.9	510.5	564.42	575.05	597.9	552.22	
1023	910.	936.3	949.3	1022.5	1098.24	1113.05	1144.	1081.20	

compared it with other generators. The generators chosen for comparison were congruential generators of the multiplicative or mixed type, since these are presently the most widely used generators.

A wide variety of congruential generators was subjected to the same twelve tests described above, on the basis of which we identified the following as being reasonably good:

1.  $x_{k+1} = (2^7 + 1) x_k + 1 \pmod{2^{35}}$
2.  $x_{k+1} = 2^7 + 1) x_k + 1 \pmod{2^{47}}$
3.  $x_{k+1} = (2^{10} + 1) x_k + 1 \pmod{2^{47}}$
4.  $x_{k+1} = 5^{15} x_k \pmod{2^{47}}$
5.  $x_{k+1} = 5^{15} x_k \pmod{2^{35}}$
6.  $x_{k+1} = 3^{29} x_k \pmod{2^{47}}$

Generator 1 has been favorably reported by Allard, Dobell and Hull (1963) and generator 4 is one of the "traditional" generators. Generator 4 has also been judged as satisfactory by Coveyou and MacPherson (1967) on the basis of their spectral test. Also, judging by the maximum attainable performance for a simple multiplicative congruential estimator in terms of the spectrum, the spectral graphs by Coveyou and MacPherson indicate that generator 4 is probably the best in that class. They show a slight improvement over this generator by going to a mixed generator with the same multiplier and 1 as the constant.

We also included the following "bad" (as indicated by our tests) generators for contrast:

7.  $x_{k+1} = (2^{17} + 1) x_k + 1 \pmod{2^{47}}$
8.  $x_{k+1} = (2^{17} + 1) x_k + 1 \pmod{2^{35}}$

Of the twelve tests described earlier, eight (consisting of all tests under (a), (b), (c) and two tests under (e) restricted to the high order 10 bits) were performed on three consecutive strings of length 10,240 from each

of the above eight generators. The results of these tests are summarized in Table 4 along with the results pertaining to the first three of the twelve samples of the present generator. Results pertaining to all twelve samples were presented earlier and indicate a satisfactory performance by the present generator. For purposes of comparison, however, we can include only three of these twelve samples, since only three samples were taken from the other generators. It should also be pointed out that the sample size chosen for the present generator was 12,229 compared to 10,240 for the other generators. However, this difference in sample size cannot affect our conclusions since both sample sizes are large enough for the  $\chi^2$  approximations to work well under the null hypothesis concerning the random numbers and any deviation from the null would only put the present generator at a disadvantage in terms of a higher  $\chi^2$  value resulting from a larger sample size.

There are  $3 \times 8 = 24$   $\chi^2$  values for each of the nine generators (the present generator plus the eight congruential estimators chosen for comparison) and corresponding to each of these  $\chi^2$  values there is a percentile  $\alpha$  (defined earlier). As before, we can conveniently summarize these  $\alpha$  values for each generator by the numbers that fall below 0.5, below 0.05, below 0.025 and below 0.005.

From the above summary it can be seen that the present generator performs as well as the better congruential generators, namely 4 and 6, on the basis of the eight tests that were performed on all of them. A set of secondary and confirmatory tests were also run on the present generator and the results are summarized below.

The first through fourth moments and the serial correlation coefficients for lags of 1 through 9 were computed for each set of random numbers. For these computations, the interval of the random numbers was translated from  $[0, 1]$  to  $[-.5, .5]$ . These quantities are shown in Table 5 along with their 2 sigma limits.

Of the forty-four moments computed, there was only one outside the 2 sigma limits and of the ninety-nine serial correlation coefficients there was only one outside the  $2\sigma$  limits. We also subjected the present set of random

Table 4. Summary of Tests on System III Generator vs. Congruential Generators

Generator	Number of Failures at the Level of:			
	0.5	0.10	0.025	0.005
$x_{k+1} = (2^7 + 1) x_k + 1 \pmod{2^{35}}$	17	5	2	2
$x_{k+1} = (2^7 + 1) x_k + 1 \pmod{2^{47}}$	17	4	0	0
$x_{k+1} = (2^{10} + 1) x_k + 1 \pmod{2^{47}}$	17	6	1	1
$x_{k+1} = 5^{15} x_k \pmod{2^{47}}$	12	1	0	0
$x_{k+1} = 5^{15} x_k \pmod{2^{35}}$	12	4	0	0
$x_{k+1} = 3^{29} x_k \pmod{2^{47}}$	9	2	0	0
$x_{k+1} = (2^{17} + 1) x_k + 1 \pmod{2^{47}}$	17	10	6	3
$x_{k+1} = (2^{17} + 1) x_k + 1 \pmod{2^{35}}$	21	18	19	19
System III generator	10	2	0	0
Theoretical averages	12	2.4	0.6	0.12

numbers to a 'white noise' test by treating it as a time series and doing a periodogram analysis. The periodogram of a series  $\{x_t\}$  is defined as:

$$I(\alpha) = \frac{1}{\pi} \sum_{-n}^n c_k \cos k\alpha, \quad (5.1)$$

where  $c_k$  is a covariance-type expression defined by

$$c_k = \frac{1}{n} \sum_{t=1}^{n-k} x_t x_{t+k}.$$

When data are independent random numbers drawn from a normal distribution, the periodogram ordinates at the Fourier frequencies (which are given by  $\frac{2\pi j}{n}$  for  $0 \leq j \leq n/2$ ) other than 0 and  $\pi$ , are independently exponentially distributed (see e.g., Bloomfield 1976). Even when the underlying distribution is non-normal, the distribution of the periodogram ordinates can still be seen to be approximately exponential for large  $n$ .

Table 5. Deviation of Moments and Correlations from Expected Values  
for Random Numbers in the Interval  $(-\frac{1}{2}, +\frac{1}{2})$

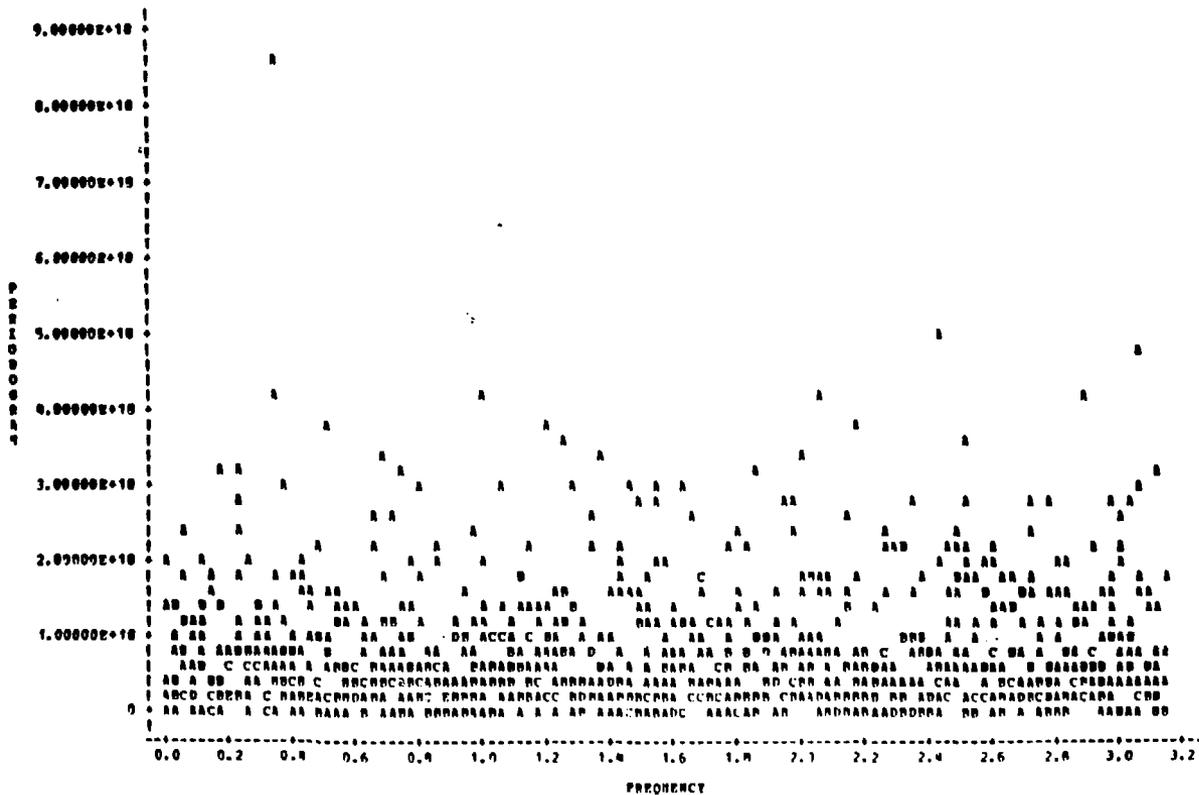
<i>Set</i>	<i>First Moment</i>	<i>Second Moment</i> -.0833	<i>Third Moment</i>	<i>Fourth Moment</i> -.0125	<i>Largest Correlation Coefficient of Lags [1-9]</i>	<i>Smallest Correlation Coefficient of Lags [1-9]</i>
First 12229	.00300	.00012	.00039	.000006	.00106	-.00137
Second "	-.00270	-.00051	-.00076	-.000121	.00101	<u>-.00159</u>
Third "	-.00118	-.00113	-.00016	-.000288	.00101	-.00095
Fourth "	.00023	.00102	.00011	.000202	.00132	-.00132
Fifth "	.00440	.00002	.00051	-.000020	.00100	-.00134
Sixth "	.00125	.00000	.00032	.000013	.00119	-.00141
Seventh "	-.00408	-.00027	<u>-.00086</u>	.000050	.00104	-.00032
Eighth "	-.00261	.00048	-.00037	.000086	.00129	-.00085
Ninth "	.00112	-.00005	.00029	-.000037	.00058	-.00081
Tenth "	.00323	-.00066	.00036	-.000148	.00106	-.00123
Whole 122292	.00027	-.00007	-.00002	-.000027	.00030	-.00045
2σ for N=12229	.00522	.00135	.000085	.000301	.00151	.00151
2σ for N=122292	.00165	.00043	.00027	.000095	.00047	.00047

Note: Values underlined are outside the two standard deviation interval from the expected value.

In the present case, a sample of 2048 random numbers (in their original form of 31 bit words) was used as input into the SAS routine SPECTRA (Barr 1976) and the following results were obtained.

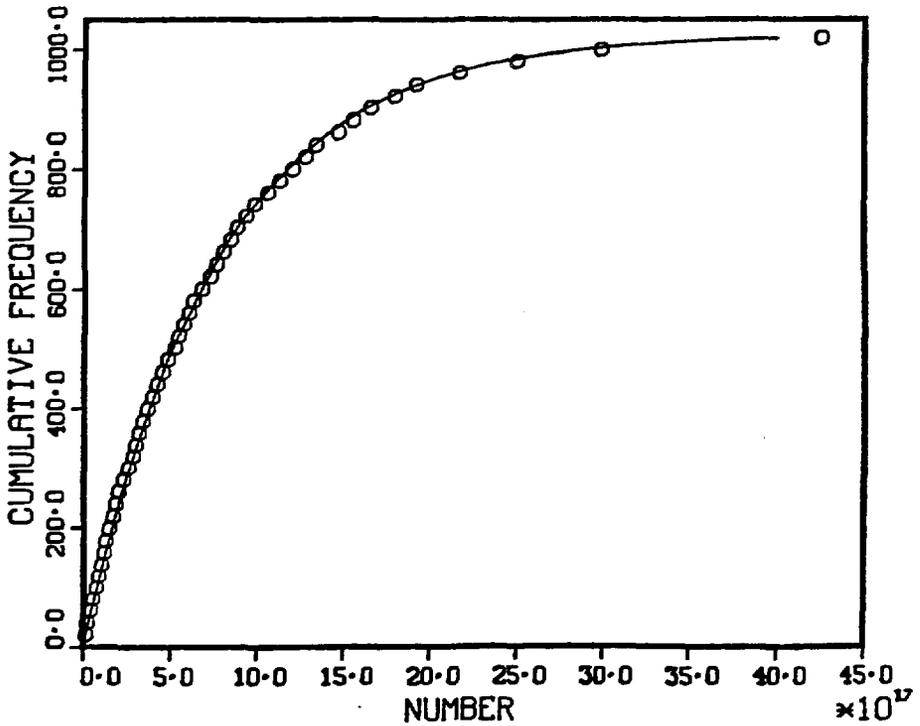
Visually, the periodogram (shown in Fig. 3) strongly resembles that of white noise. This is confirmed by Figure 4 showing close agreement between the empirical cumulative distribution function of the periodogram ordinates and the corresponding theoretical distribution function. In addition, Fisher's test of significance based on the largest peak in a periodogram, and Bartlett's Kolmogorov-Smirnov test both support the "white noise" hypothesis (Fisher's kappa equals 21.7926 and Bartlett's statistic equals 0.0298, both of which are not significant at the five percent level).

A further test of a confirmatory nature was performed on the present set of random numbers involving runs of shorter length. One hundred and twenty subsamples of a thousand or fewer  $n$ -tuples for  $n = 2, \dots, 5$  (the exact number is determined by the size of  $n$ ) were analyzed as follows: for each sample, the number  $X$  of  $n$ -tuples lying within the unit  $n$ -dimensional hypersphere was determined. The variable  $X$  has a binomial distribution with probability  $\frac{2}{n} \frac{\pi^{n/2}}{\Gamma(n/2)}$ . A comparison of the theoretical distribution function with the empirical distribution function of the  $X$  values (Figs. 5 and 6 for  $n = 4$  and 5, respectively) also leads to the conclusion that the present set of numbers is adequately random.



A = 1 observation, B = 2 observations, etc.

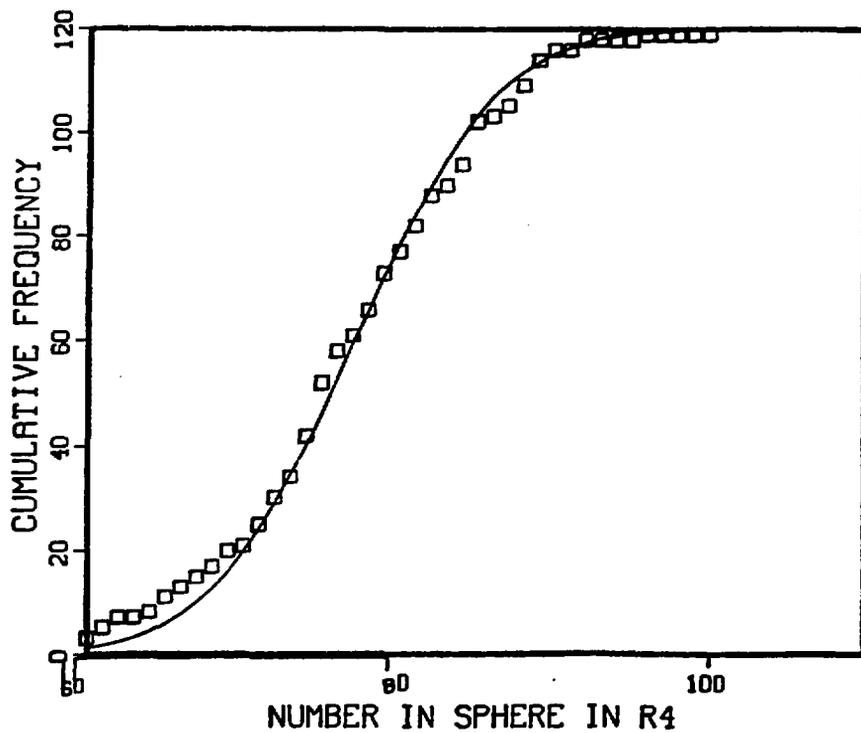
Fig. 3. Periodogram of Truly Random Numbers.



Solid line: Theory

Open circles: Empirical

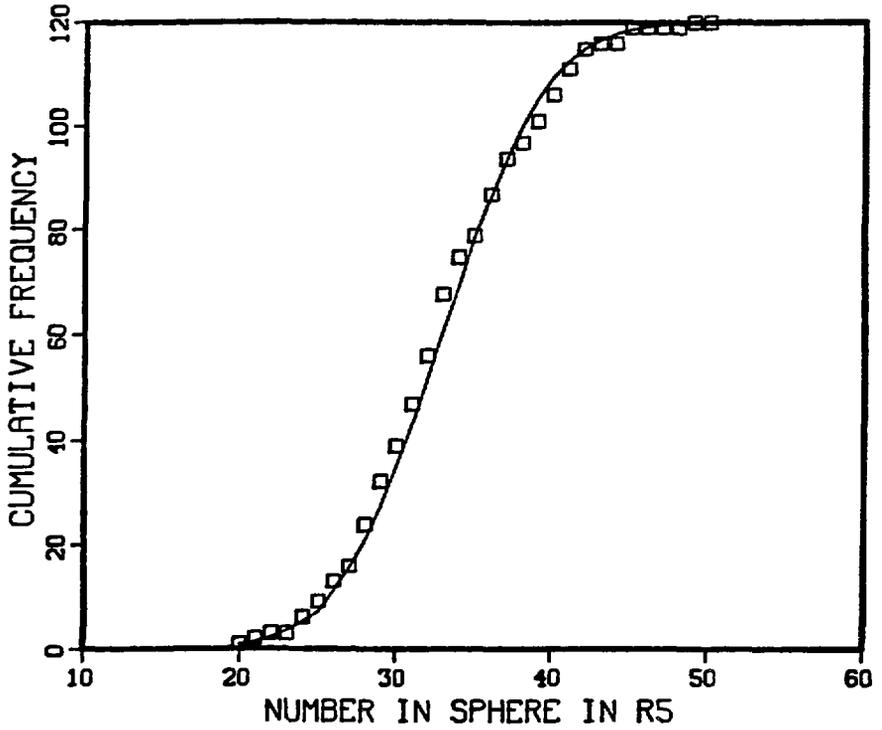
Fig. 4. Comparison of Theoretical and Empirical Distribution Functions of Periodogram Ordinates for the Truly Random Numbers.



Solid line: Theory

Open squares: Empirical

Fig. 5. Comparison of Theoretical and Empirical Distribution Functions of the Four-tuples in the Unit Sphere for Truly Random Numbers.



Solid line: Theory

Open squares: Empirical

Fig. 6. Comparison of Theoretical and Empirical Distribution Functions of the Number of Five-tuples in the Unit Sphere for Truly Random Numbers.

## VI. CONCLUSION

The need for a physical random number device (RND) to generate random numbers for large Monte Carlo studies became evident in an experiment on gamma and neutron interactions, performed at Argonne in collaboration with the National Bureau of Standards. Pseudorandom number generators of the congruential type caused a significant bias in the experimental and theoretical results. This behavior of congruential pseudorandom numbers can be explained by the theorem (Marsaglia 1968) that these numbers are concentrated in a relatively small number of hyperplanes. Other pseudorandom number generators, devised to correct this defect, may not be satisfactory for the degree of resolution required in any specific simulation problem. Use of an RND to generate random numbers for large Monte-Carlo studies is therefore desirable, provided the device is stable enough to give valid results.

The alpha counting system, referred to as System III here, is a highly reliable mechanism for generating truly random numbers because:

1. the generated count data conforms to the theoretically predicted Brockwell-Moyal distribution for a random Poisson process with dead time; and
2. the 31-bit binary numbers generated by the system satisfy accepted standards of "randomness" as judged by the results of a battery of statistical tests performed on a sample set of these numbers.

We, therefore, recommend the use of truly random numbers generated by System III in Monte-Carlo simulations for which the congruential pseudorandom number generators are found to be inadequate.

APPENDIX A. AN ALTERNATE DERIVATION OF THE  
BROCKWELL-MOYAL DISTRIBUTION

1. Notation

- $N$  = total number of particles arriving at the counter in time  $t$   
 $M$  = total number of particles registered at the counter in time  $t$   
 $d$  = resolving time or dead time  
 $t_1$  = time before arrival of the first particle  
 $t_2$  = time between arrivals of the first and second particles  
 $t_n$  = time between arrivals of the  $(n - 1)^{\text{st}}$  and  $n^{\text{th}}$  particles

Next, we derive the joint distribution of  $N$  and  $M$ , which, in turn, is used to obtain the marginal distribution of  $M$  and also to get the conditional expectation of  $N$  given  $M$ .

2. Joint Distribution of  $N$  and  $M$

All modern theories of radioactive decay are based on the assumption that in an assembly of nuclei of a given element all the nuclei are identical, independent, and have the same probability of decaying in unit time. It then follows that a radioactive decay process generates events according to the Poisson law. It also follows that the inter-arrival times  $t_1, \dots, t_n, \dots$  are independent identically distributed random variables, each with the exponential distribution. The registered particles correspond to interarrival times that are greater than  $d$ . We note that

$$N = n \Leftrightarrow t_1 + \dots + t_n \leq t \text{ and } t_1 + \dots + t_{n+1} > t ,$$

and that

$$M = m \text{ given } N = n \Leftrightarrow m \text{ of the } n \text{ } t\text{'s are } \geq d \text{ and } n - m \text{ of the } t\text{'s are } < d .$$

It, therefore, follows that

$$P(N=n \text{ and } M=m) = P(t_1 + \dots + t_n \leq t, t_1 + \dots + t_{n+1} > t \text{ such that } m \text{ of the } t\text{'s are } \geq d \text{ and the remaining are } < d). \quad (\text{A.1})$$

The RHS of (A.1) can be evaluated by considering a specific set of  $m$   $t$ 's such that they are  $\geq d$  and such that the other constraints are satisfied, and then multiplying the resulting probability by  $\binom{n}{m}$ . This is valid since all sets

of  $t$ 's selected in the above manner lead to the same probability and there are  $\binom{n}{m}$  ways of selecting them.

Let  $s_0$  be the set of constraints defined by

$$t_1 \geq d, \dots, t_m \geq d, t_{m+1} < d, \dots, t_n < d,$$

$$t_1 + \dots + t_n \leq t, \text{ and } t_1 + \dots + t_{n+1} > t.$$

It follows that

$$P(N=n \text{ and } M=m) = \binom{n}{m} \int_{\substack{t_1, \dots, t_{n+1} \in s_0 \\ \prod_{i=1}^{n+1} \lambda^{n+1} e^{-\lambda t_i} dt_1 \dots dt_{n+1}}} . \quad (\text{A.2})$$

The multiple integral appearing in (A.2), which is henceforth denoted by  $I_0$ , can be evaluated step by step as follows:

Step 0: Integration with respect to  $t_{n+1}$  yields

$$I_0 = \lambda^n \int_{\substack{t_1, \dots, t_n \in s_1 \\ e^{-\lambda(t_1 + \dots + t_n)} f_1(t_1, \dots, t_n) dt_1 \dots dt_n}} ,$$

where

$$s_1 = t_1 \geq d, \dots, t_m \geq d, t_{m+1} < d, \dots, t_n < d, \text{ and } t_1 + \dots + t_n \leq t,$$

and

$$f_1 = \int_{t_{n+1} > t - (t_1 + \dots + t_n)} \lambda e^{-\lambda t_{n+1}} dt_{n+1} = e^{-\lambda[t - (t_1 + \dots + t_n)]} .$$

Therefore,

$$I_0 = \lambda^n e^{-\lambda t} I ,$$

where

$$I = \int_{t_1, \dots, t_n \in s_1} dt_1 \dots dt_n .$$

Step 1: Integration with respect to  $t_1$  yields

$$I = \int_{t_2, \dots, t_n \in S_2} f_2(t_2, \dots, t_n) dt_2 \dots dt_n,$$

where

$$s_2 = t_2 \geq d, \dots, t_m \geq d, t_{m+1} < d, \dots, t_n < d, \text{ and } t_2 + \dots + t_n + d \leq t,$$

and

$$f_2 = \int dt_1 = t - (t_2 + \dots + t_n + d).$$

$$t_1 \geq d$$

$$t_1 < t - (t_2 + \dots + t_n)$$

Therefore,

$$I = \int_{t_2, \dots, t_n \in S_2} [t - (t_2 + \dots + t_n + d)] dt_2 \dots dt_n$$

Step 2: Integration with respect to  $t_2$  yields

$$I = \int_{t_3, \dots, t_n \in S_3} \frac{[t - (t_3 + \dots + 2d)]^2}{2} dt_3 \dots dt_n,$$

where

$$s_3 = t_3 \geq d, \dots, t_m \geq d, t_{m+1} < d, \dots, t_n < d, \text{ and } t_3 + \dots + t_n + 2d \leq t.$$

Step m: Integration with respect to  $t_m$  yields

$$I = \int_{t_{m+1}, \dots, t_n \in S_{m+1}} \frac{[t - (t_{m+1} + \dots + md)]^m}{m!} dt_{m+1} \dots dt_n,$$

where

$$s_{m+1} = t_{m+1} < d, \dots, t_n < d, \text{ and } t_{m+1} + \dots + md < t.$$

Step  $m + 1$ : Integration with respect to  $t_{m+1}$  can be done more simply by considering  $t_{m+1} \geq d$  and then taking the complement. This yields

$$\int \frac{[t - (t_{m+1} \dots md)]^m}{m!} dt_{m+1} = \int \frac{[t - (t_{m+1} \dots md)]^m}{m!} dt_{m+1} - \int \frac{[t - (t_{m+1} + \dots md)]^m}{m!} dt_{m+1}$$

$$\begin{array}{l} t_{m+1} < d \\ t_{m+1} < t - (t_{m+2} + \dots md) \\ t_{m+1} < t - (t_{m+2} + \dots md) \end{array} \quad \begin{array}{l} t_{m+1} + \dots md < t \\ t_{m+1} \geq d \end{array}$$

$$= \frac{[t - (t_{m+2} + \dots md)]^{m+1}}{(m+1)!} - \frac{[t - (t_{m+2} + \dots (m+1)d)]^{m+1}}{(m+1)!}.$$

Therefore,

$$I = I_{m+1,1} - I_{m+1,2},$$

with

$$I_{m+1,1} = \int \frac{[t - (t_{m+2} + \dots md)]^{m+1}}{(m+1)!} dt_{m+2},$$

$$t_{m+2}, \dots, t_n \in s_{m+2,1}$$

and

$$I_{m+1,2} = \int \frac{[t - (t_{m+2} + \dots (m+1)d)]^{m+1}}{(m+1)!} dt_{m+2}$$

$$t_{m+2}, \dots, t_n \in s_{m+2,2}$$

where

$$s_{m+2,1} = t_{m+2} < d, \dots, t_n < d, t_{m+2} + \dots t_n + md \leq t$$

and

$$s_{m+2,2} = t_{m+2} < d, \dots, t_n < d, t_{m+2} + \dots t_n + (m+1)d \leq t.$$

Step m + 2: Using the same approach as in Step m + 1, we have

$$I_{m+1,1} = \int_{t_{m+3}, \dots, t_n \in s_{m+3,1}} \frac{[t - (t_{m+3} + \dots md)]^{m+2}}{(m+2)!} dt_{m+3} \dots dt_n$$

$$- \int_{t_{m+3}, \dots, t_n \in s_{m+3,2}} \frac{[t - (t_{m+3} + \dots (m+1)d)]^{m+2}}{(m+2)!} dt_{m+3} \dots dt_n,$$

and

$$I_{m+1,2} = \int_{t_{m+3}, \dots, t_n \in s_{m+3,2}} \frac{[t - (t_{m+3} + \dots (m+1)d)]^{m+2}}{(m+2)!} dt_{m+3} \dots dt_n$$

$$- \int_{t_{m+3}, \dots, t_n \in s_{m+3,3}} \frac{[t - (t_{m+3} + \dots (m+2)d)]^{m+2}}{(m+2)!} dt_{m+3} \dots dt_n,$$

where

$$s_{m+3,1} = t_{m+3} < d, \dots, t_n < d, t_{m+3} + \dots t_n + md \leq t,$$

$$s_{m+3,2} = t_{m+3} < d, \dots, t_n < d, t_{m+3} + \dots (m+1)d \leq t, \text{ and}$$

$$s_{m+3,3} = t_{m+3} < d, \dots, t_n < d, t_{m+3} + \dots (m+2)d \leq t.$$

Therefore,

$$I = I_{m+2,1} - 2I_{m+2,2} + I_{m+2,3},$$

where

$$I_{m+2,1} = \int_{t_{m+3}, \dots, t_n \in S_{m+3,1}} \frac{[t - (t_{m+3} + \dots + md)]^{m+2}}{(m+2)!} dt_{m+3} \dots dt_n,$$

$$I_{m+2,2} = \int_{t_{m+3}, \dots, t_n \in S_{m+3,2}} \frac{[t - (t_{m+3} + \dots + (m+1)d)]^{m+2}}{(m+2)!} dt_{m+3} \dots dt_n,$$

and

$$I_{m+2,3} = \int_{t_{m+3}, \dots, t_n \in S_{m+3,3}} \frac{[t - (t_{m+3} + \dots + (m+2)d)]^{m+2}}{(m+2)!} dt_{m+3} \dots dt_n.$$

Proceeding in the above manner yields the final step:

$$\begin{aligned} P(N=n, M=m) &= \binom{n}{m} \lambda^n e^{-\lambda t} \sum_{\substack{r < n-m \\ d(m+r) \leq t}} (-1)^r \frac{[t - (m+r)d]^n}{n!} \binom{n-m}{r}, \\ &= \frac{\lambda^n e^{-\lambda t}}{m!} \sum_{\substack{r < n-m \\ r \leq t/d-m}} \frac{[t - (m+r)d]^n}{r!(n-m-r)!} \quad \text{for } n \geq m, \\ &= 0 \text{ otherwise.} \end{aligned} \tag{A.3}$$

The expression,  $\binom{a}{b}$ , is equal to  $\frac{a!}{b!(a-b)!}$ , where  $a \geq b$ .

### 3. Marginal Distribution of M

$$\begin{aligned}
 P(M=m) &= \sum_{N=m}^{\infty} P(M=m, N=n) \\
 &= e^{-\lambda t} \sum_{n=m}^{\infty} \binom{n}{m} \lambda^n \sum_{\substack{0 < r \leq n-m \\ (m+r)d \leq t}} (-1)^r \frac{[t - (m+r)d]^n}{n!} \binom{n-m}{r}.
 \end{aligned} \tag{A.4}$$

Reverse the order of summation.

Let  $r = 0$ . Summation with respect to  $n$  then gives

$$\begin{aligned}
 \frac{e^{-\lambda t}}{m!} \sum_{n=m}^{\infty} \frac{\lambda^n [t - md]^n}{(n-m)!} &= \frac{e^{-\lambda t}}{m!} \lambda^m [t - md]^m e^{\lambda(t-md)} \\
 &= \frac{e^{-\lambda md} \lambda^m [t - md]^m}{m!}.
 \end{aligned} \tag{A.5}$$

The  $r^{\text{th}}$  term is

$$\begin{aligned}
 (-1)^r \frac{e^{-\lambda t}}{m!r!} \sum_{n=m+r}^{\infty} \frac{\lambda^n [t - (m+r)d]^n}{(n-m-r)!} \\
 &= \frac{(-1)^r e^{-\lambda t} \lambda^{m+r}}{m!r!} [t - (m+r)d]^{m+r} e^{\lambda[t - (m+r)d]} \\
 &= \frac{(-1)^r \lambda^{m+r} [t - (m+r)d]^{m+r} e^{-(m+r)d\lambda}}{m!r!}.
 \end{aligned} \tag{A.6}$$

Therefore,

$$P(M=m) = \sum_{r=0}^{\lfloor t/d \rfloor - m} \frac{(-1)^r e^{-(m+r)d\lambda} \lambda^{m+r} [t - (m+r)d]^{m+r}}{m!r!} \quad \text{for } m \leq t/d \quad (\text{A.7})$$

$$= 0 \text{ otherwise,}$$

where  $\lfloor t/d \rfloor$  is the greatest integer  $\leq t/d$ .

Equation (A.7) is the same as the expression derived by Brockwell and Moyal (1966) and can be rewritten as follows:

$$P(M=m) = \sum_{s=m}^{\lfloor t/d \rfloor} \frac{(-1)^{s-m} e^{-sd\lambda} \lambda^s [t - sd]^s}{m!(s-m)!} \quad \text{for } m \leq t/d \quad (\text{A.8})$$

$$= 0 \text{ otherwise.}$$

#### 4. Conditional Expectation of N Given M = m

$$\begin{aligned} E(N|M=m) &= \sum_{n=m}^{\infty} n P(N=n|M=m) \\ &= \frac{1}{P(M=m)} \sum_{n=m}^{\infty} n P(N=n, M=m) \\ &= \frac{1}{P(M=m)} \sum_{r=0}^{\lfloor t/d \rfloor - m} (-1)^r \frac{e^{-\lambda t}}{m!r!} \sum_{n=m+r}^{\infty} \frac{\lambda^n n [t - (m+r)d]^n}{(n-m-r)!}. \quad (\text{A.9}) \end{aligned}$$

$$\sum_{n=m+r}^{\infty} \frac{\lambda^n n [t - (m+r)d]^n}{(n-m-r)!} = \lambda^{m+r} (m+r) [t - (m+r)d]^{m+r} \\ + \sum_{n=m+r+1}^{\infty} \frac{\lambda^n (m+r+n-m-r) [t - (m+r)d]^n}{(n-m-r)!}, \quad (\text{A.10})$$

$$= \lambda^{m+r} [t - (m+r)d]^{m+r} e^{\lambda[t-(m+r)d]} [m+r + \lambda(t - (m+r)d)]. \quad (\text{A.11})$$

Therefore,

$$E(N|M=m) = \frac{1}{P(M=m)} \sum_{r=0}^{[t/d]-m} (-1)^r e^{-(m+r)d\lambda} \lambda^{m+r} [t - (m+r)d]^{m+r} [m+r + \lambda(t - (m+r)d)] \\ = \frac{1}{P(M=m)} \sum_{s=m}^{[t/d]} \frac{(-1)^{s-m} e^{-sd\lambda} \lambda^s [t - sd]^s [s + \lambda(t - sd)]}{m!(s-m)!}. \quad (\text{A.12})$$

### 5. Estimation of $\lambda$ and $d$

In Section III we used the first moment (given by equation (3.2) of the distribution of  $M$  as a basis for estimating  $\lambda$  given  $d$ ). For estimating  $\lambda$  and  $d$  simultaneously, we can again use the method of moments. Equating the first two factorial moments of  $M$  [expressions for moments are given by Brockwell and Moyal (1966)] to the corresponding sample moments, we have

$$\bar{M} = \lambda(t - d) e^{-\lambda d}, \quad (\text{A.13})$$

$$\bar{\bar{M}} - \bar{M} = \lambda^2(t - 2d)^2 e^{-2\lambda d}, \quad (\text{A.14})$$

where  $\bar{M}$  is the average observed count and  $\bar{\bar{M}}$  is the sample second moment or the average of the squares of observed counts. From (A.13) and (A.14) we have

$$\frac{\bar{M} - \bar{M}}{\bar{M}^2} = \frac{(t - 2d)^2}{(t - d)^2} . \quad (\text{A.15})$$

Since the LHS of (A.15) is always positive or zero, (A.15) implies

$$\frac{t - 2d}{t - d} = \frac{\sqrt{\bar{M}} \cdot \bar{M}}{\bar{M}} \quad (\text{A.16})$$

From (A.16) the solution for  $d$  is given by

$$d = \frac{t(C - 1)}{C - 2} , \quad (\text{A.17})$$

where

$$C = \frac{\sqrt{\bar{M}} - \bar{M}}{\bar{M}}$$

Given  $d$ , we can obtain  $\lambda$  by solving (A.13) iteratively as follows:

From (A.13) we have

$$\lambda(t - d) = \bar{M} e^{\lambda d} . \quad (\text{A.18})$$

Using  $\bar{M}$  as the initial value of  $\lambda$  and substituting it in the RHS of (A.18), we obtain a new value of  $\lambda$  using the LHS. This, in turn, is substituted in the RHS and the procedure is repeated until convergence in the  $\lambda$  values is attained.

Using the method of moments we obtained the estimates,  $\hat{\lambda} = 0.001213$ , and  $\hat{d} = 0.6$ . By a search process, Butler (Ref. 9) found the maximum likelihood estimates to be  $\hat{\lambda} = 0.001213$ , and  $\hat{d} = 0.58$ . The close agreement between the numerical estimates given by the two methods is due to the large sample employed in the estimation. The maximum likelihood method is computationally involved; so we propose the method below as a compromise between statistical and computational efficiency. Even when the method of moments is adequate, an alternative method, such as the following, affords a comparison between the second moment of the observed distribution and the fitted distribution.

The method proposed here is based on the conditional expectation,  $E(N|M)$ , of  $N$  given  $M$ . If  $N$  is observable, then the maximum likelihood estimate of  $\lambda$  would be  $\bar{N}$ , the average of the  $N$  values. Since  $N$  is not observable directly, but can only be inferred through  $M$ , we use  $E(N|M)$  in place of  $N$  [this is akin to the "Missing Information Principle" (Sanathanan and Blumenthal 1978 for maximum likelihood estimation)], i.e., the estimating equation for  $\lambda$  is given by

$$\lambda = \frac{1}{n} \sum_{i=1}^n E(N|M_i), \quad (\text{A.19})$$

where  $n$  is the number of observations and  $M_i$ 's are the observed counts. The estimating equation for  $d$  can be taken to be (A.13) which is based on the first moment of  $M$ .

The LHS of (A.19) is given by (A.12) which involves  $\lambda$  and  $d$ . (A.13) also involves  $\lambda$  and  $d$ . The following iterative procedure yields the solution for  $\lambda$  and  $d$ . Rewrite (A.13) as

$$(t - d) = \frac{\bar{M} e^{\lambda d}}{\lambda}. \quad (\text{A.20})$$

Using trial values for  $\lambda$  and  $d$  ( $\bar{M}$  and that given by (A.17), respectively) and substituting in the RHS of (A.19) and in the RHS of (A.20), we obtain revised values of  $\lambda$  and  $d$ . We repeat this cycle until convergence in the  $\lambda$  and  $d$  values is obtained.

## 6. Comparison of Theoretical and Sample Moments

Expressions for the factorial moment of  $M$  have been derived by Brockwell and Moyal (1966) and are given by

$$\begin{aligned} E[M(M-1)\dots(M-k+1)] &= \lambda^k (t - kd)^k e^{-k\lambda d}, \quad 1 \leq k \leq t/d \\ &= 0, \quad k > t/d \end{aligned}$$

Computations using the above result for the BM distribution with  $d = 0.8$ ,

$t = 2000$  and  $\lambda = 0.01213$  yielded  $E(M) = 24.26$ ,  $E(M^2) = 612.83$ ,  $E(M^3) = 16,067.27$ , and  $E(M^4) = 436,112.75$ .

Corresponding moments computed from the data from System III are 24.26, 612.85, 16068.30 and 436,161.69, respectively. In all cases the ratio of the theoretical moment to the corresponding sample moment is between 0.999 and 1.001, indicating very close agreement between the observed and fitted distributions.

## APPENDIX B. PROBABILITIES

```

-----
CARD
NUMBER                                FORTRAN SOURCE LISTING
-----
 1 C PROGRAM TO CALCULATE BLACKWELL-MOYAL PROBABILITIES
 2 C FORTRAN TRANSLATION BY MARY MORLEY OF A PL1 PROGRAM BY
 3 C JAMES BUTLER
 4     REAL*16 LANDA,D,X,MU,T,SUM3,SUM4,PROBB,PROBB2
 5     REAL*8 XMFAC(61),XMF
 6     READ(5,1006) LANDA,TOTAL
 7     T=2.0Q-2
 8     D=.8Q-6
 9     X=D/T
10 C SUM3 ADDS UP THE PROBABILITIES TIMES THE TOTAL
11 C IT SHOULD ADD UP TO 3.792E6; SUM4 WILL BE THE SUM OF THE
12 C EVEN PROBABILITIES MINUS THE ODD PROBABILITIES, THIS IS ALSO
13 C MULTIPLIED BY THE TOTAL SO THE DEAS IS OUT OF 3.792E6 NOT OUT OF 1
14     SUM3=0Q0
15     SUM4=0Q0
16     MU=LANDA*T*QEXP(-1*LANDA*D)
17 C XMFAC'S ARE THE INVERSE FACTORIALS XMFAC(I)=(I-1)!
18     READ(5,1001) (XMFAC(I),I=1,61)
19     DO 11 K=1,61
20     KM1=K-1
21     XMF=XMFAC(K)
22 C SUBROUTINE DTIME DOES THE ACTUAL CALCULATIONS OF THE PROBABILITIES.
23     CALL DTIME(XMF,KM1,PROBB,MU,X)
24     PROBB2=PROBB*TOTAL
25     SUM3=SUM3+(-1)**K*PROBB2
26     SUM4=SUM4+PROBB2
27     WRITE(6,1002) KM1,PROBB,PROBB2
28     11 CONTINUE
29     WRITE(6,1003) SUM3,SUM4
30     1001 FORMAT(D21.15)
31     1002 FORMAT(' ',16,X,F12.8,X,F20.1)
32     1003 FORMAT(' ',F20.8,X,F20.8)
33     1006 FORMAT(F9.4,2X,E7.3)
34     STOP
35     END

36     SUBROUTINE DTIME(XMF,KM1,PROBB,MU,X)
37     REAL*16 MU,KK,TERM1,TERM2,ONE,LOW,ABS,MU,X,SUM,PROBB
38     REAL*8 XMF
39     LOW=2Q00**(-250)
40     IX=2Q0
41     ONE=1Q00
42     TERM1=ONE
43     TERM2=ONE
44     SUM=0Q00
45     M=0
46     MU=0Q00
47     KK=KM1
48     ICOUNT=0
49     20 ABS=ABS(TERM2)
50     IF (ABS .LE. LOW) GO TO 24
51     ICOUNT=ICOUNT+1
52     IF (ICOUNT .GT. IX) GO TO 24
53     TERM2=TERM1*(ONE-(MU+KK)*X)**(M+KM1)
54     SUM=SUM+TERM2
55     MU=MU+ONE
56     M=M+1
57     TERM1=-1*TERM1*MU/MU
58     GO TO 20
59     24 K1=KM1/2
60     K2=KM1-K1
61     PROBB=MU**K1*XMF*(MU**K2*SUM)
62     RETURN
63     END
-----

```

## REFERENCES

1. Allard, J. L., A. R. Dobell, and T. E. Hull. 1963. *Mixed congruential random number generators for decimal machines*. J. of ACM. 10:131-141.
2. Anderson, J. L. 1972. *Non-Poisson distributions observed during counting of certain carbon-14 labeled organic (sub) monolayers*. J. Phys. Chem. 76:3603.
3. Argonne Tape Library, (a) Tape Nos. 103511, 103914-103916, 103928, 104094, 104095, 104118, 104120. (b) Tape No. 097143. (c) Tape No. 139820.
4. Bainbridge, K. T., M. Goldhaber, and E. Wilson. 1951. *Influence of the chemical state on the lifetime of an isomer*. Phys. Rev. 84:1260-1261.
5. Barr, A. J., J. Goodnight, J. Sall, and J. Helwig. 1976. *A user's guide to SAS 76*. SAS Institute Inc. Raleigh, N.C. 329 pp.
6. Bloomfield, Peter. 1976. *Fourier analysis of time series*, Wiley. New York. 289 pp.
7. Bofinger V. and J. Bofinger. 1958. *On a periodic property of pseudo-random sequences*. J. of ACM. 5:261-265.
8. Brockwell, P. J. and J. E. Moyal. 1966. *A stochastic population process and its application to bubble chamber measurements*. J. Appl. Prob. 3:280-284.
9. Butler, J. 1975. Argonne National Laboratory. Unpublished manuscript.
10. Certain, J. 1958. *On the sequence of pseudo-random numbers of maximal length*. J. of ACM. 5:353-356.
11. Cohn, C. E. 1969. *Reactor-noise studies with an on-line digital computer*. Nuclear Applications. 6:391-393.
12. Cohn, C. E. 1971. *The performance of random bit generators*. Stimulation. 17:234-236.
13. Coldwell, R. I. 1974. *Correctional defects in the standard IBM 360 random number generators and the classical ideal gas correlation function*. J. of Comp. Phys. 14:223-226.
14. Cook, J. A. 1975. Argonne National Laboratory. Personal communication.
15. Coveyou, R. R. and R. D. MacPherson. 1967. *Fourier analysis of uniform number generators*. J. of ACM. 14:100-119.

16. Duparc, H. J., G. G. Lekerkerker, and W. Permans. 1953. *Reduced sequences of integers and pseudo-random numbers*. Mathematic Centrum Report, 1953-002. Amsterdam.
17. Emery, G. T. 1972. *Perturbation of nuclear decay rates*. Ann. Rev. Nucl. Sci. 22:165-202.
18. Evans, R. D. 1962. *The atomic nucleus*. Chap. 26-28, MacGraw Hill. New York. 972 pp.
19. Frigerio, N. A. 1965. *Low scatter, lightweight fission spectrometer*. Rev. of Sci. Inst. 36:1048-1049.
20. Frigerio, N. A. 1968. *Toward the production of truly random numbers*. In Report ANL-7535, Argonne National Laboratory.
21. Frigerio, N. A. and M. H. Branson. 1969. *Current research in depth dose computations*. In: *Proc. Sym. Neutrons in Radiobiology*, CONF-691106, USAEC. Oak Ridge, Tenn. pp. 95-115.
22. Frigerio, N. A. 1973. *Poisson and non-poisson behavior of radioactive systems*. Nuclear Instruments and Methods. 114:175-177.
23. Frigerio, N. A. and N. A. Clark. 1975. *A random number set for Monte Carlo computations*. Tran. American Nuclear Society. 22:283-284.
24. Fry, T. C. 1965. *Probability and its engineering uses*, 2nd ed., Van Nostrand. Princeton, N.J. 462 pp.
25. Fuller, A. T. 1976. *The period of pseudo-random numbers generated by Lehmer's congruential method*. Comp. J. (6B). 19:173-177.
26. Greenberger, M. 1961. *An a priori determination of serial correlation in computer generated random numbers*. Math. Comp. 15:383-389.
27. Hull, T. E. and A. R. Dobell. 1962. *Random number generators*. SIAM Review. 4:230-254.
28. Junosca, M. 1953. *Random number generators on the BRL high speed computing machines*. Ballistic Research Labs, Report N. 855, Aberdeen Proving Ground, Md.
29. Kendall, M. G. and B. B. Smith. 1939. *Tables of random sampling numbers*. Cambridge University Press. 60 pp.
30. Knuth, D. E. 1969. *The art of computer programming*. Addison-Wesley Publishing Company. Reading, Mass. 624 pp.
31. Lehmer, D. H. 1951. *Proc. 2nd symposium on large-scale digital computing machinery*. Harvard University Press. pp. 142-145.
32. Levene, H. and J. Wolfowitz. 1944. *The covariance matrix of runs up and down*. Ann. of Math. Stat. 15:58-69.

33. MacLaren, M. D. and G. Marsaglia. 1965. *Uniform random number generators*. J. of ACM. 12:83-89.
34. Marsaglia, G. 1968. *Random numbers fall mainly in the planes*. Proc. Nat. Acad. Sci. USA. 61:25-28.
35. Marsaglia, G. 1976. *Random number generators*. In: *Encyclopedia of Computer Sciences*. Anthony Ralston, ed. Petrocelli Books, New York. pp. 1192-1197.
36. Moshman, J. 1954. *The generation of pseudo-random numbers on a decimal calculator*. J. of ACM. 11:88-91.
37. Parzen, E. 1962. *Stochastic processes*. Holden Day Inc. San Francisco, Cal. 324 pp.
38. Rand Corporation. 1955. *A million random digits with 100,000 normal deviates*. Free Press. Blencoe, Ill. XXV:400,200.
39. Rubin, H. 1976. Purdue University. Personal communication.
40. Sanathanan, L. and Blumenthal. 1978. *The logistic model for dichotomous response*. J. of American Statistical Association, 73:794-799.
41. Schiff, L. I. 1936. *Statistical analysis of counter data*. Phys. Rev. 50:88-96.
42. Shreider, Y. A. ed. 1966. *The Monte-Carlo method (the method of statistical trials)*. Pergamon Press, Oxford. 370 pp.
43. Van Gelder, A. 1967. *Some new results in pseudo-random number generators*. J. of ACM. 14:785-792.
44. Vincent, C. H. 1970. *The generation of truly random numbers*. J. of Physics E. 3:594-598.