U.D.C. 681.325.36:〔621.382.23:621.391.822〕

ダイオードノイズを利用した乱数発生装置

Random Number Generator Using a Diode Noise

石田正次* 佐藤利男** 鈴木亀二郎***
Masatsugu Ishida Toshio Sato Kamejiro Suzuki
下田昭一郎**** 川瀬哲郎****
Shoichiro Shimoda Tetsuo Kawase

In statistic simulation by means of electronic computers random numbers are used as a factor for contingency. A random number generator introduced here is intended for feeding random numbers to electronic computers. Different from the random number generation by means of software, this machine depends on totally physic probability phenomena and by processing the phenomena generates random numbers. It is expected that problems inherent to software random number generation can be solved by the use of this physic generator.

This article introduces a random number generator, completed by Hitachi to the order of the Statistic Mathematics Institute, which has a transfer speed about 100 times that of similar devices for laboratory use.

1．緒　　言

統計シミュレーションの初期においては,確率現象の源として,既成の乱数表が利用されたこともあったが，これでは必要な結果を得るのに十分なだけの乱数を用意することが困難であり，しかも乱数を計算機の中に記憶させるための労力がたいへんであるので，この方法は，非常に特別な場合以外は用いられなくなった。

これに代わる方法には，ソフトウェアによる乱数発生方式，いわゆる擬似乱数がある。これは計算機でできるいくつかの演算を組み合わせて，乱数と見なしうるような数列を次々と作りながら計算を進める方法であるが，周期性その他の難点があり，大規模なシミュレーションを行なう場合は常に問題となるところである。大規模な統計シミュレーションでは，規則性をもたぬ長大な乱数列を速い速度で必要とし，ソフトウェア方式でこれを実現することはきわめて困難である。これを解決する方法として，物理的確率現象から乱数を得る方式が注目されたわけである。この方式の特徴はすべて乱数源のもつ確率法則に支配されるので，乱数源の選択と処理を適切に行なえば，統計的シミュレーション用の乱数として，都合のよい出力を得ることができる。この方式の乱数発生装置を擬似乱数発生装置と区別するために，工学的乱数発生装置と呼んでいる。

2．工学的乱数発生装置の動向

工学的乱数発生装置の歴史をたどると，昭和31年統計数理研究所において，放射性同位元素を乱数源とした装置が第1号機として出現している。この装置は計数装置の性能上，0.5秒に一字(6ビット）程度の乱数発生速度であり，統計的シミュレーションを行なうためには，あまりにもおそすぎた。計算機の演算速度が速くなればこれに見合うような乱数発生装置を作らねばならない。

次に考え出されたのは熱雑音が純粋の確率事象にきわめて近いことを利用し，これを乱数源としたものであって周波数帯域の選択いかんによって，いくらでもスピードアップできることに着目したものである。第2号機として完成されたこの装置は，統計数理研究所指導のもとに，富士計器株式会社製作という形で共同開発された。この装置の乱数発生スピードは，0.5msに1字（6ビット）程度の出力を得ることができ，HIPAC 103を処理装置とし，アナログコンピュータ，特殊関数発生器など数多くの付属設備を含んだシミュレーション用計算機システムとして，同種システムの母体を作り上げることに成功した。このシステムによって得られた演算結果は，擬似乱数のそれより数段高い精度のものである。

標本分布を求めるような，いわば純粋の数理統計の問題においては，要求される精度からみて，まず必要とされるのは超高速の計算機である。一般に確率事象の精度は近似的に繰り返し回数の平方根に比例し，結果を1けたよけいに出そうとすると，計算時間は約100倍かかることを意味する。電子計算機の演算速度が急速に向上している現在，乱数発生装置に対して高速処理能力が要求されるようになった。

3．乱数発生装置の仕様

ここで本装置の機能仕様の一部を抜粋し，前項の装置性能と比較してみよう。

(1) 乱数形式……2進乱数
(2) 乱数転送速度……200Kバイト/s
(3) 〝0〞〝1〞等確率出現性および独立性 …統計的にみて妥当であること。

この仕様は，先に述べた工学的乱数発生装置2号機に比べ，転送速度は約100倍，情報量は約130倍の能力をもつ必要があることを示している。具体的に解説すれば，2進乱数とは〝0〞または〝1〞の信号が統計的にみて等確率でしかも独立に出現しなければならないことを意味している。また転送速度200Kバイト/sとは,5μsに1バイト（8ビットパラレル）の速度で乱数を転送しなければならないことである。

4．乱数発生装置

4.1 概　　要

本装置の外観は**図1**に，ブロックダイヤグラムは**図2**に示すとおりである。**図2**に従い動作概要を説明する。本装置は乱数源としてツェナダイオードより発生するダイオードノイズを用いている。この出力を(2)に示す増幅器にて広帯域増幅し，(4)に示すカウ

* 文部省統計数理研究所
** 日立製作所神奈川工場
*** 日立製作所旭工場
**** 日立電子エンジニアリング株式会社

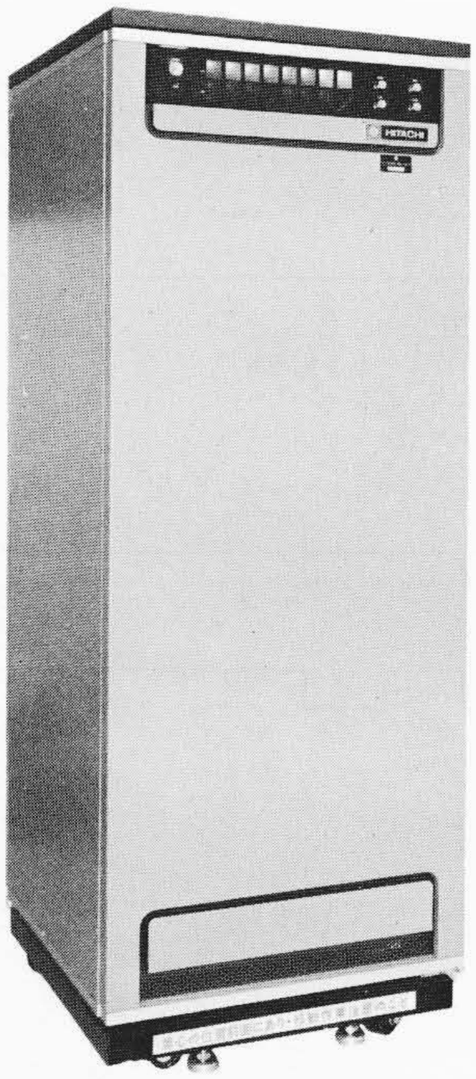


図1　乱数発生装置の外観

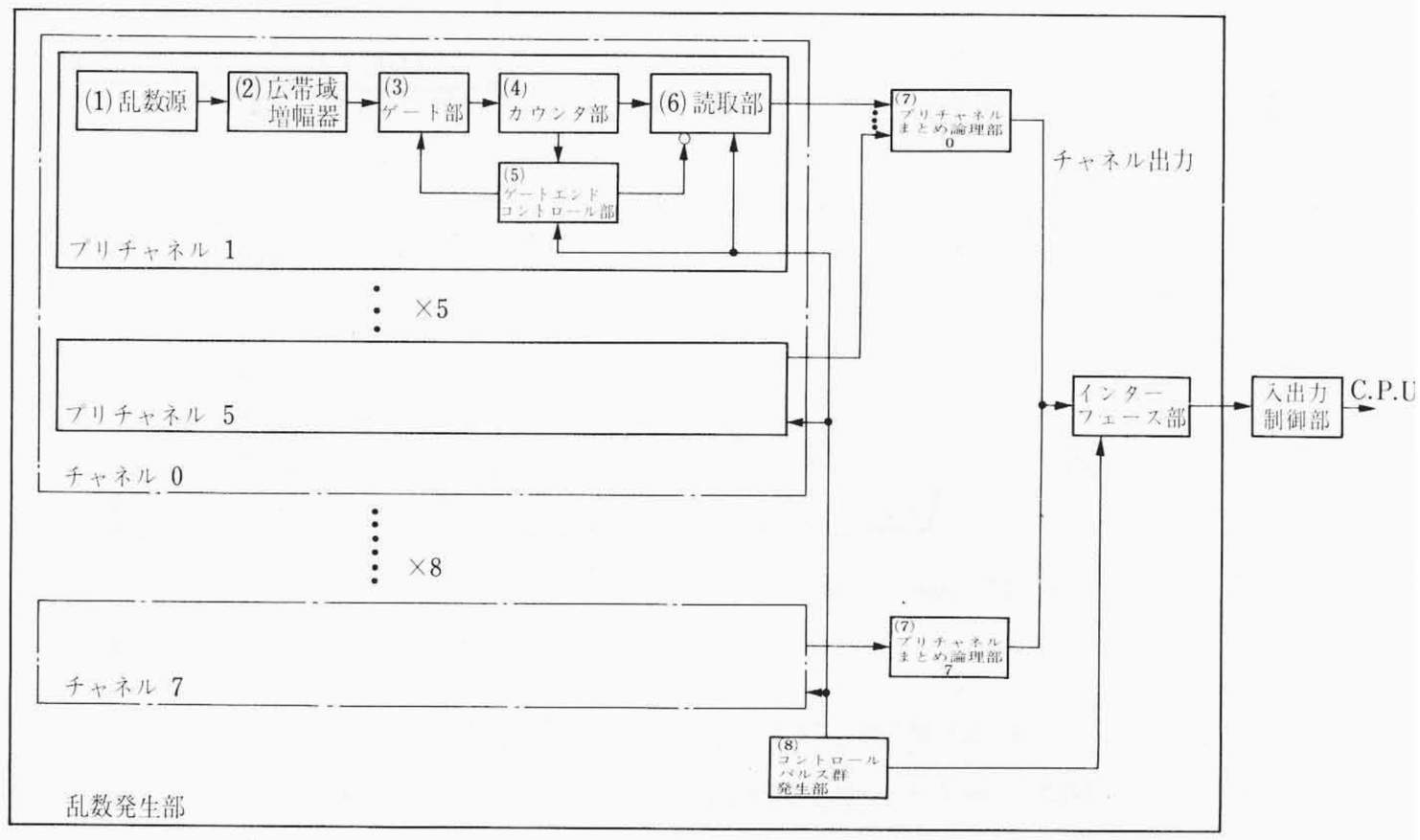


図2　乱数発生装置ブロックダイヤグラム

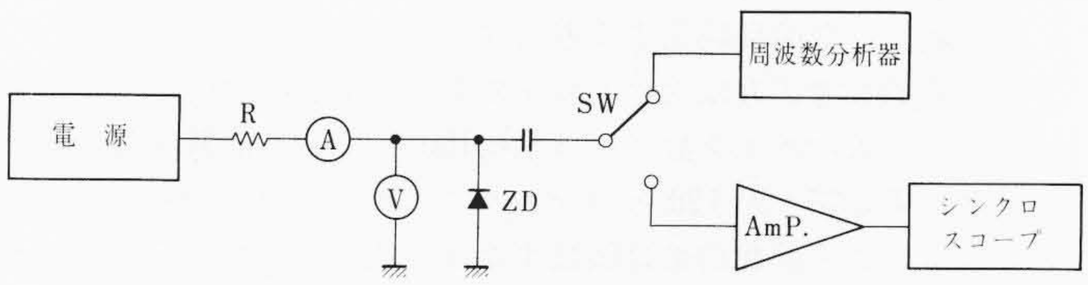
ンタおよび(3), (5)に示すゲート部，ゲートエンドコントロール部により単位時間あたりのランダムパルス数が，偶数であるか，奇数であるかを弁別する。しかる後，(6)の読取部より，偶数は〝0〞，奇数は〝1〞のように出力を読み取り，2進乱数を発生させるものである。また後述する理由により，(7)に示すプリチャネルまとめ部により，5個のプリチャネルの情報を順次とり出し，1チャネル分の出力を得ている。(8)に示すコントロールパルス群発生部はこれらのタイミングを制御する。さらに，このチャネルを8個もち，8ビットパラレルのバイト出力を得る。これら一連の動作を行なう部分を乱数発生部と呼び，この出力は入出力制御部を介して電子計算機の入出力チャネルに接続される。

4.2 乱　数　源

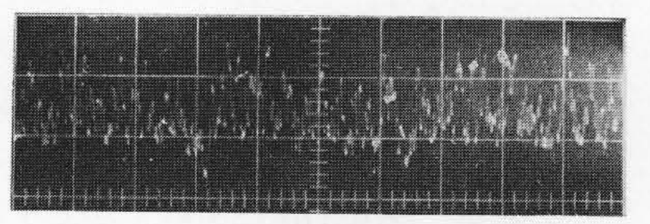
工学的に乱数を作る場合は乱数源となるものが時間的に安定で，電圧や周囲温度などの外乱条件の変化に無関係でなければならない。また乱数源の中で起こる確率現象を簡単なしかも確実な装置によって計算に便利な形の乱数に変換できるということもたいせつな条件である。これらの条件を満足する乱数源として，われわれの身辺には，放射性物質，熱雑音などさまざまなものが考えられる。

放射性物質から放射される粒子の時間間隔は指数分布に従うといわれている。いま1位の数 t に着目し，その出現率を求めてみれば明らかなように，1回の粒子カウント数の平均を100とか200というように十分大きくすれば，t は実用上十分な程度の等分布をするのがわかる。しかし，この結果をそのまま実用化するためには，いくつかの問題がある。それは計数装置の性能に関するもので，たとえばG－M管を用いたとすると，10^{-4} 秒程度の休止時間があるので，これ以下の時間間隔ではいってきた粒子は計数されない。このことは高速で乱数を作り得ないことを示している。[1]

熱雑音はいわゆる白色雑音に近く，高い周波数帯域まで周波数スペクトラムが得られ，出力が前者に比べて非常に小さいという欠点を除けば速度の点で非常に有利となる。熱雑音を発生する素子として，ノイズダイオード（真空管），抵抗，半導体などがあげられる。ノイズダイオードは高圧電源を必要とすることや，発熱を考えると，電子計算機と同居する装置としては好ましくないし，



(a) ツェナーダイオード雑音測定ブロックダイヤフラム



2MHz　　7MHz

(0.5MHz/div)

(b) ノイズ波形周波数分析結果代表例

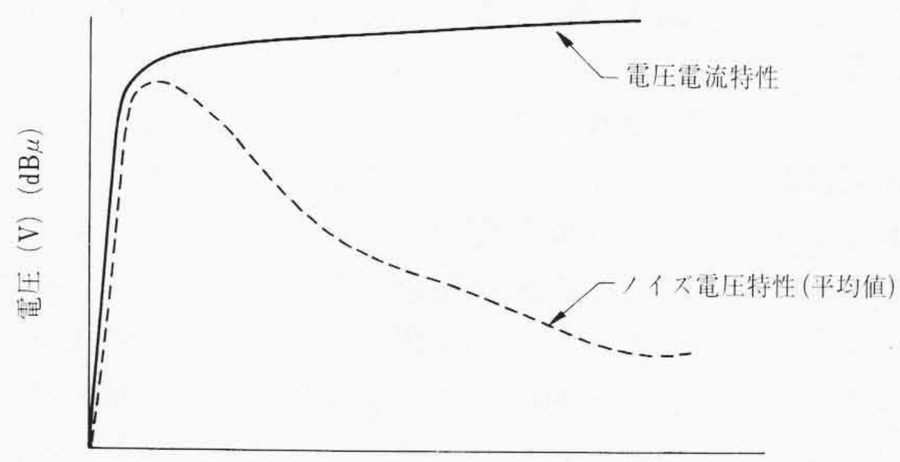
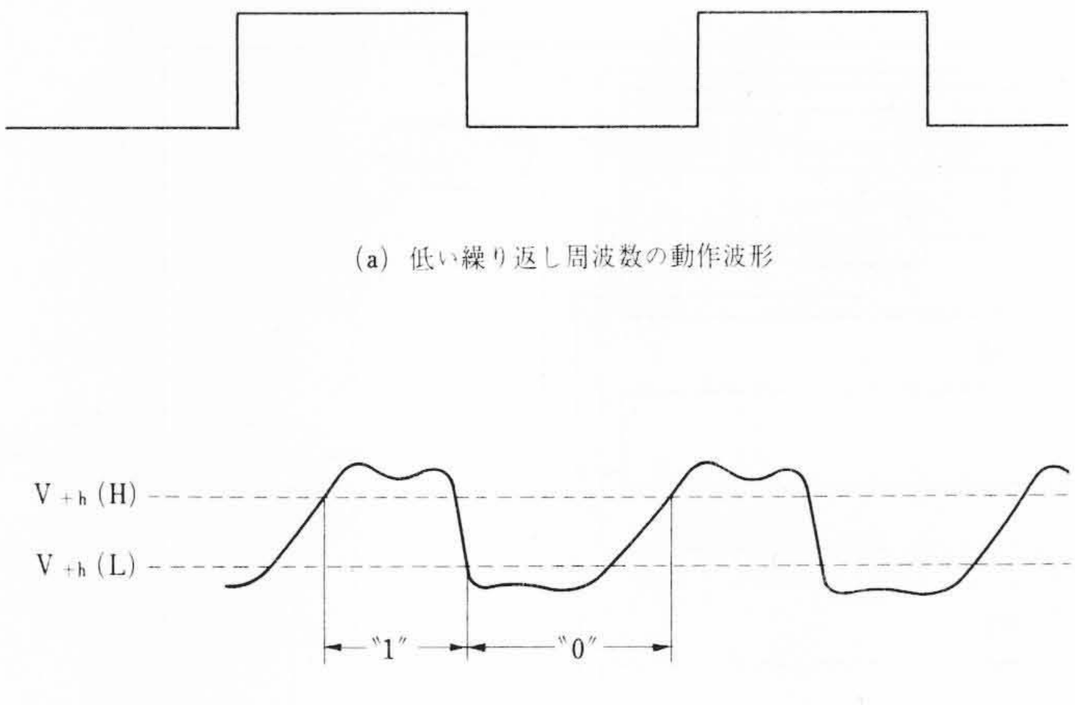


図3　ツェナダイオード雑音特性測定

抵抗の熱雑音はその発生レベルが低く実用的ではない。

ここでわれわれは，ツェナダイオードがある種のバイアス条件のもとで雑音を発生する[2]ことに着目し，**図3**（a）に示す方法で，このダイオードノイズがわれわれの利用する範囲内で，白色雑音とみなすことができることを確認した。**図3**（b）はツェナダイオードの雑音を周波数分析した代表例であり，**図3**（c）はツェナ電流と雑音発生量の代表的特性を示したものである。



(a) 低い繰り返し周波数の動作波形

(b) 高い繰り返し周波数の動作波形

図4　バイナリカウンタ出力波形

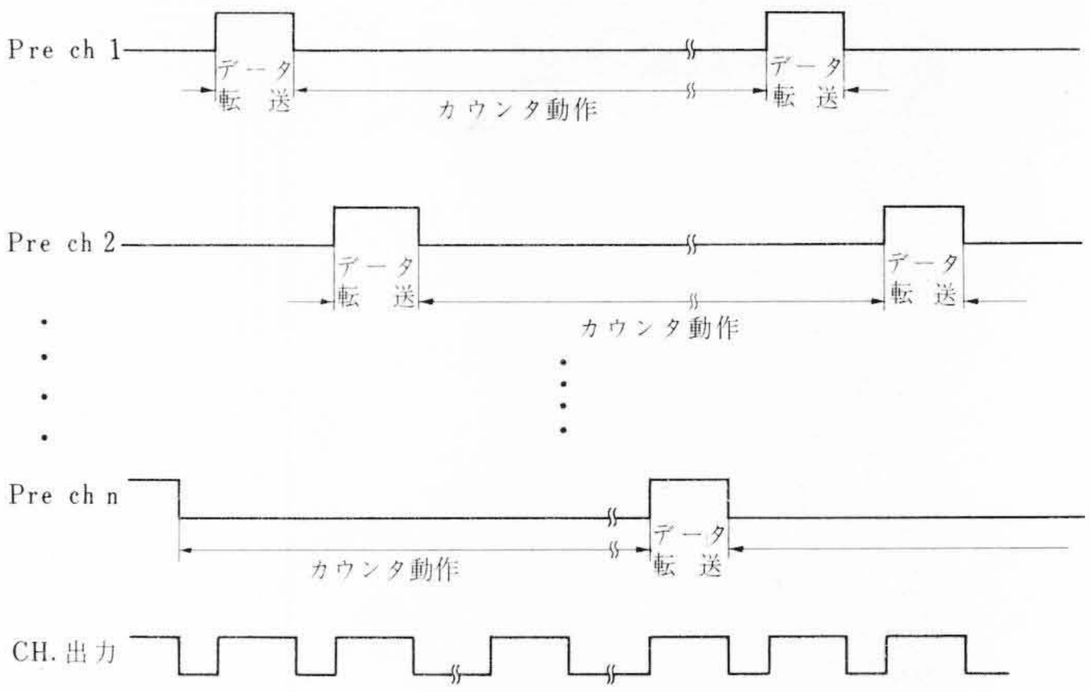


図5　プリチャネルスキャニング方式

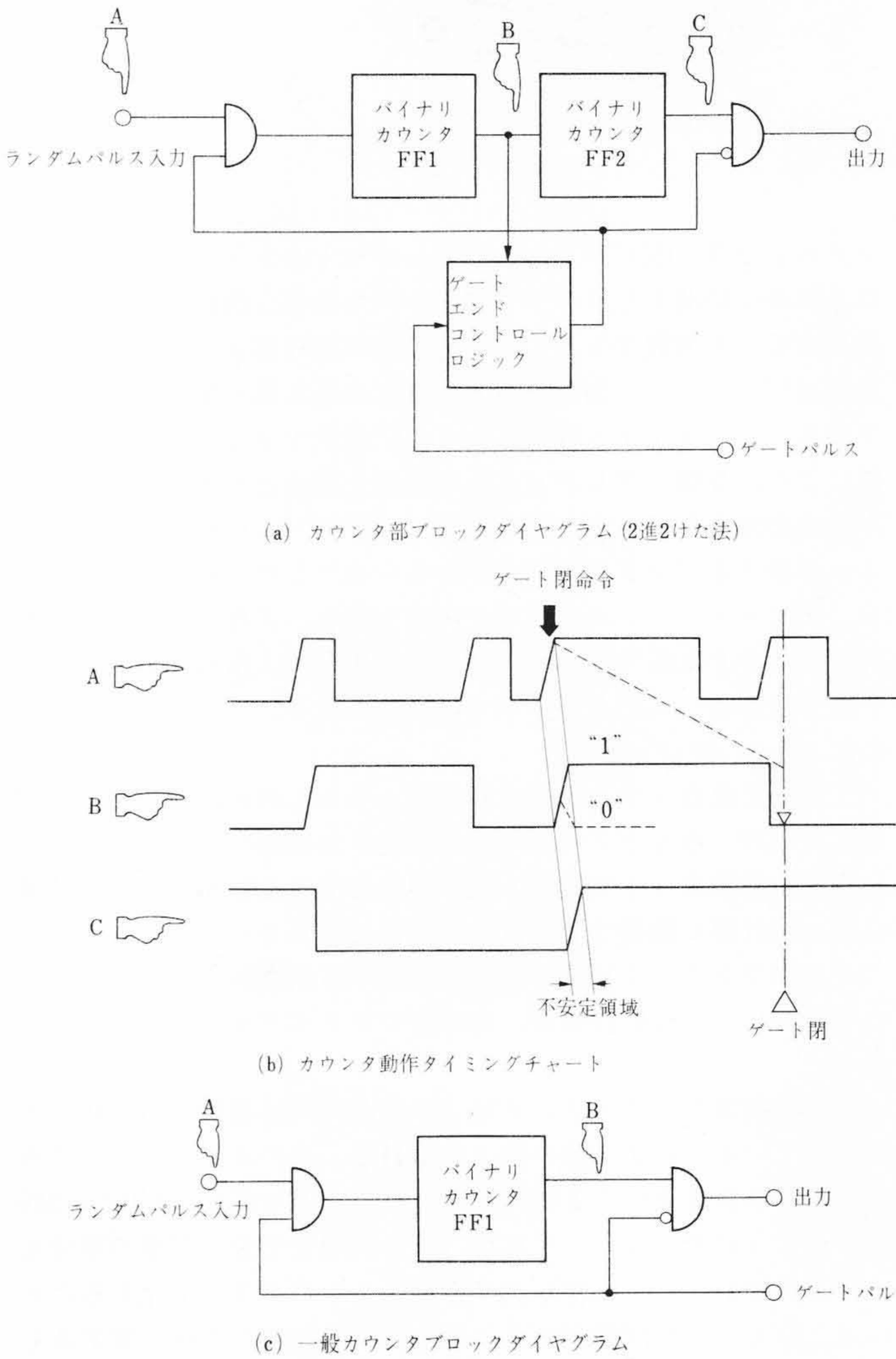
4.3 カウンタ

白色雑音を2進乱数化する方式は，動作概要の項でも触れたが，この基本的な考え方は次のとおりである。単位時間内にはいってくるランダムパルスを数多く（平均100とか200）計数すれば，その計数結果は75とか120というように，かなりの変動幅をもつことになる。この計数結果は偶数または奇数のいずれかであり，その出現は確率事象に支配される。また計数パルス数変動幅が十分大であれば，偶数，奇数の出現確率は50%に収束する。

この単純に見える動作を電気回路に置き換えると，次に述べるような問題点を含むことになる。その第一はパルスの立ち上り時間に関するものであって，**図4**に示すように1：1の時間比をもつパルスをバイナリカウンタに与えたときの出力波形は，低い周波数において，く形波と見なせるが，周波数が高くなるにつれ，三角波に近づく。この結果，**図4**（b）に図解するように〝1〟の時間間隔と〝0〟の時間間隔が異なることになる。先に述べた2進乱数化方式を別の角度から見ると，固定周波数のパルスをランダムな時間間隔でくぎり，その時間内にはいってきたパルスをバイナリカウントし，〝1〟であるか〝0〟であるかを判別するのと等価である。したがって〝1〟を捕える確率と〝0〟を捕える確率はその時間比に比例するから，**図4**（b）のような波形は，出力結果が必然的に〝0〟に多くかたよることになる。

このほかに，プリント基板パターンのインダクタンス，キャパシタンスが周波数によってインピーダンス差となって表われ，見掛け上スレッシホールドレベルを変化させ，カウンタを反転させる条件が不安定になることも重大な問題の一つである。ことにスレッシホールドレベル付近でゲートが閉じ，カウンタを停止させようとするとき，入力パルス条件によってカウンタを反転させたり，させなかったりすることになる。通常のカウンタであれば，計数結果±1という値は許容誤差として認められるが，乱数化用カウンタでは偶数，奇数を判断しているのであるから，この問題は非常に重要な誤差の原因となる。

これらの問題点の対策の第一は，カウンタの入力情報となるランダムパルスの最高繰り返し周波数を低く押え，出力パルス波形の立ち上り，立ち下り時間が無視できるような，く形波にしようという試みである。この方式は単位時間内にはいってくるランダムパルスの平均入力数および最小と最大入力数との差，言い換えればパルス数のランダム性が減少し，時間的に隣合った出力ビットの独立性が犯されることになる。この独立性を保証するためには，カウンタに割り当てられているカウント時間を長くする必要



(a) カウンタ部ブロックダイヤグラム（2進2けた法）

(b) カウンタ動作タイミングチャート

(c) 一般カウンタブロックダイヤグラム

図6　2進2けた読取方式

があるが，乱数発生速度が低下し仕様を満足することができない。ここで乱数転送速度を保証し，上記の対策を同時に行なうために**図5**に示すプリチャネルスキャニング方式を採用している。

各プリチャネルは，1個ごとに独立した乱数発生源とカウンタを持つことにより，プリチャネル単体で処理速度の遅い，言い換えれば，ランダムパルス最高繰り返し周波数を制限し，カウント

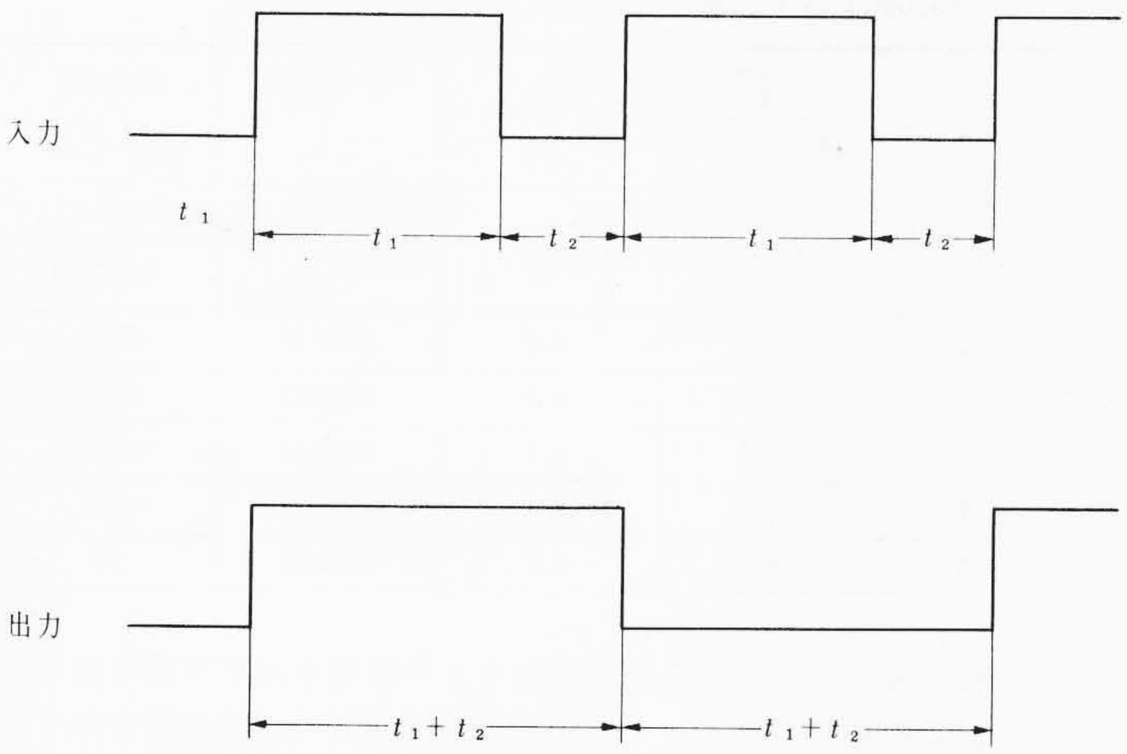


図7　バイナリカウンタのパルス比補正

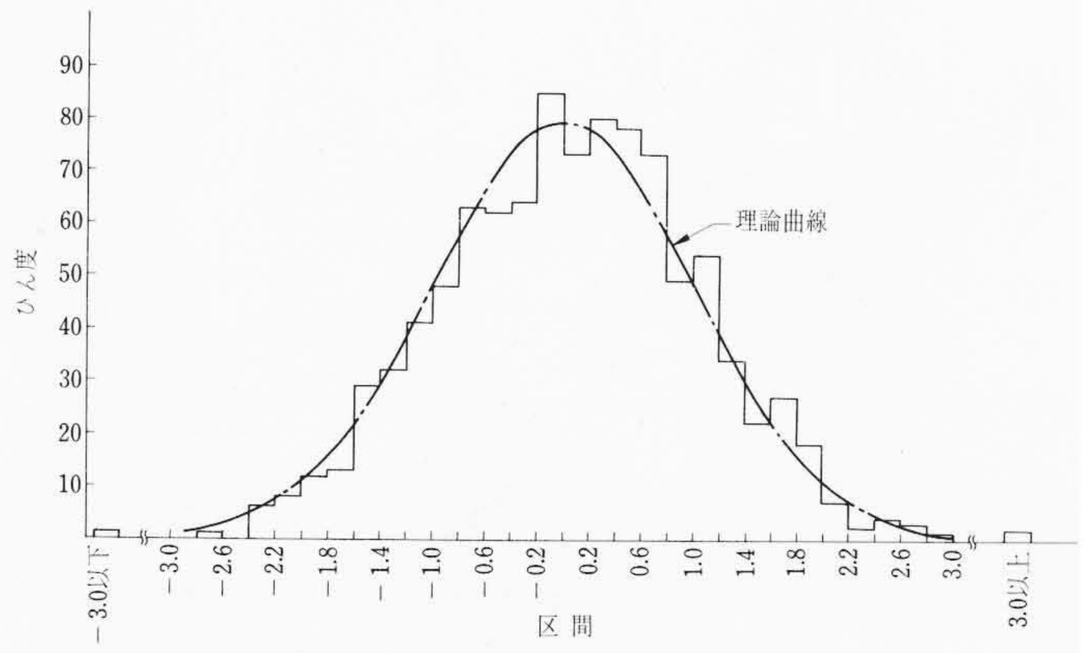


図8　バイトパターン等確率出現性テスト結果

時間を長く設定した乱数発生装置を構成している。このプリチャネルを n 個もち，順次ゲートパルスのスキャニング操作を行なうことによりデータを読み取り，プリチャネル単体の転送速度の n 倍をチャネル転送速度として得ている。

第2に見掛け上のスレッシホールドレベルの変化に対する対策として，2進2けた法を採用した。これは，先に述べた乱数発生装置第2号機において，微分トリガ形フリップフロップのトリガ点変動および入力パルスの〝0〟〝1〟比アンバランスに対する対策として，石田および富士計器株式会社池田氏が考案し，すでに実績のある方式である。今回の場合は，カウンタ形式が多少異なるが，方式的に非常に有効であり，論理的に等価動作を行なわせ実用化している。

2進2けた法の動作概要は**図6**（a）のブロックダイヤグラムおよび**図6**（b）のタイミングチャートに示すとおりである。**図6**（c）は一般のカウンタブロックダイヤグラムを示したものである。まず最初に**図6**（c）の構成によるカウンタを用いランダムパルスの2進乱数化を行なったとするとパルス立ち上り動作時つまり**図6**（b）の⬇の個所にてゲート閉命令が発せられたとすると，先に述べたように，見掛け上のスレッシホールドレベルが不安定な状態にあるので，バイナリカウンタ（ＦＦ1）の出力が〝1〟側へ反転するか〝0〟側に保持されるかは明らかではなく，カウンタのくせに支配されることになる。このような状態を避けるためには，パルス立ち上り時にゲート閉の行なわれないことが望ましい。ここで，たとえパルス立ち上り時にゲート閉命令が発せられても，ゲートを閉じず，出力段が完全に安定となるまでゲート開を保持し，出力段が安定領域に存在していることを確認してゲート閉を行なうことが必要となる。このために**図6**（a）に示すような論理構成によりゲートタイミングの補正を行なっている。これはバイナリカウンタを2段シリーズ（2進2けたカウント）に接続すれば**図6**（b）のB，C波形の関係のように，前段の立ち下り領域においては後段は必ず安定領域にあるという原理を利用したものである。つまりゲート閉命令が発せられてもすぐにはゲート閉を行なわず，前段のカウンタが立ち下るまでゲートを開放保持し，立ち下り情報により実際にゲートを閉じる方式とすれば，後段からは常に安定領域にある出力を得ることができる。この機能をゲートエンドコントロールロジックと呼んでいる。カウント機能系に着目すれば2進カウンタ1けた目（ＦＦ1）は，ゲート閉最適タイミング情報をゲートエンドコントロールロジックに提供し，実際の出力は2進カウンタ2けた目（ＦＦ2）より取り出すことができる。またこの方式は**図7**に示すように，入力パルス比補正の効果を有し，1個のバイナリカウンタと論理回路の組合せによる〝0〟〝1〟出現比補正弁別方式より時間的にも構造的にもはるかにすぐれている。

5．乱数発生装置出力の概要

5.1　等確率出現性の問題

本装置の出力は毎回8ビットであるので，これを1組にみれば，出現パターンの数は，

$$2^8=256$$

であり，乱数発生装置としては，このパターンが等しい確率で出現することが望ましい。この様子をみるためにわれわれは出現パターンのテストをχ^2表示で行なっている。つまり，各パターンの平均出現度数を100回とし，全体で25,600の出力をもって1回の為行と考え，各回ごとに

$$\chi^2=\sum_{i=1}^{256}\frac{(Fi-100)^2}{100}$$

ここに，Fiは25,600回のうち各パターンの出現度数を計算し，これを1,000回行なってヒストグラムを作成する。この方法がテストの内容である。

この結果の一例は**図8**に示すとおりである。表の横軸はχ^2をガウス形に変換したもので，

$$\sqrt{2\chi^2}-\sqrt{2n-1}$$

ここに，nは自由度であって，出現パターンの数より1だけ小さい数である。

により求められる。

この表でみれば，分布がやや右傾しているが，これは波形のひずみなどによる影響と考えられる。この程度のひずみは，他の乱数に比べて非常に小さいものではあるが，なお大形のシミュレーションのためには，今後さらに検討を要することになろう。

5.2　独立性の問題

乱数発生装置の出力を2回分取り出した場合，前と後(あと)の結果は独立でなければならない。もし独立であれば，2回の出力を二けたの数と考えれば，

００，０１，１０，１１

の4個のパターンの出現確率は等しくなるはずである。このテストを前項に述べた等確率出現性テストと同時に行なえば，25,600回の出力は2けたの数12,800個と考えられ，したがって各パターンの理論出現度数は3,200となりχ^2値は次式で与えられる。

$$\chi^2=\sum_{i=1}^{4}\frac{(Fi-3,200)^2}{3,200}$$

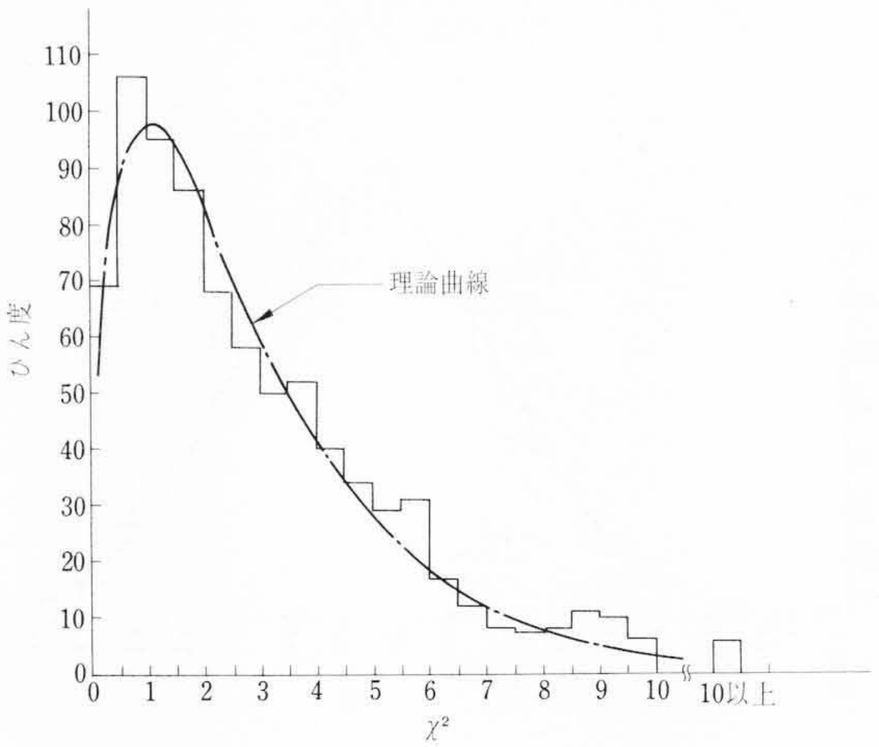


図9　2進2けた組合せテスト結果

図10　2進乱数プラグインパネル試験器

ここに，Fiは００，０１，１０，１１の出現度数

この結果を1回の為行と考え，1,000回行なった結果を示すと**図9**になる。

5.3　プリチャネルの特性

各プリチャネルを一つのブロックと考えると，おのおののブロックは独立に2進乱数を発生している。したがって，これらを単独の乱数発生器と考えると，その出力は統計的にみて，等確率出現性，独立性を満足していなければならない。これらは前項と同様χ^2表示で行なうことができ等確率出現性は次のように示される。

$$\chi^2=\frac{\left(n_0-\frac{N}{2}\right)^2}{\frac{N}{2}}+\frac{\left(n_1-\frac{N}{2}\right)^2}{\frac{N}{2}}$$

$$N=n_1+n_0$$

ここに，N：総ビット数

n_0：〝0〞出現度数

n_1：〝1〞出現度数

となり，このχ^2値を理論χ^2値(一般的に5％値)と比較することにより等確率出現性の判定を行なうことができる。具体的に等確率出現性を満足する〝1〞の出現度数範囲を，

$N=10,000$

理論χ^2値(自由度1，5％)$=3.841\fallingdotseq 4$

として概算すると，

$4,900<n_1<5,100$

を得る。これは総ビット数10,000の2進乱数の〝1〞の出現度数は，4,900～5,100の間になければならないことを意味する。ただし，この判定基準は，理論χ^2値を5％に選んでいるため，理論上5％の危険率を有することになる。ここで10,000ビット試験法を1回の為行と考え，これを1,000回行なった結果を示すと**表1**になる。また，この結果は総ビット数$N=10,000,000$の試験を行なっていると解釈してもさしつかえないから，これを1回の為行と考え，その理論値と測定結果を同時に示した。

表1　10,000ビット試験1,000回為行結果（代表例）

Prech. No. ＼ 理論値	10,000パルステスト $4,900<n_1<5,100$ 満足する(％)	満足しない(％)	〝1〞累積数 $\sum n_1$	累積偏差 $\sum\frac{n}{2}-\sum n_1$
	95.45	4.55	危険率5％〔$\chi^2 0.05(\phi=1)$〕	
			4996861～5003139	$>\pm 3139$
01	95.6	4.4	4999750	+240
02	95.8	4.2	4999243	+857
03	95.3	4.7	5001686	−1686
04	96.4	3.6	5000343	−343
05	94.3	5.7	5000050	−50

6．監視・保守機能

本装置は方式上純粋の確率現象に基づいた再現性の無い乱数列を発生するため，非常に低い確率でしか存在しないような特異なパターンの数列をも発生することがありうる。この場合装置故障によるものか確率的要素により発生したものかを判定することはきわめてむずかしい。たとえばオール〝0〞のパターンをかなり長いビットにわたり送出し続けた場合はカウント結果がオール偶数であるのか，ダイオードノイズが停止しカウンタが動作しなくなったのか判別しがたい。ここで乱数の転送状況を〝1〞〝0〞出力ともにランプ表示し，その輝度を比較し，簡易に偏(かたよ)りを判定できるとともに，常時ランダムパルスのレベルを監視し，レベルが低下すると直ちに警報を送出し，データ送出を停止する機能をあわせ持つよう工夫してある。

本装置の最小乱数発生系列はプリチャネルであることは前にも述べたが，このプリチャネルが**5.3**で述べた特性を満足していることが必要となる。ここで定期点検時に各プリチャネルの特性を容易に把握(はあく)できるよう**図10**に示す専用試験器を開発し，保守点検の能率化を図っている。この試験器は10,000ビットテストのほかにパルスランダム性測定，平均入力パルス数算出，アラーム機能チェック，累積偏差測定などの機能を有し，特性劣化の原因となる要素を事前にチェックすることができる。

7．結　　言

以上，統計数理研究所納め乱数発生装置の方式概要について述べた。本装置の特色をまとめると，

(1)　本装置の出力は物理的確率現象を乱数源とし，純粋の確率法則に支配された周期性のない乱数を得る。

(2)　乱数発生用のプログラム作成などの準備作業なしに任意の長さの乱数列を得ることができる。

(3)　高速度（200Kバイト/s）の発生速度を有する。

(4)　統計シミュレーション用乱数として，必要な特性を有する。

終わりに，本装置の開発に関し終始ご指導，ご協力を賜わった統計数理研究所の各位に対し，厚くお礼申し上げる。

参　考　文　献

(1) 石田：科学基礎論研究　17．2．29（1965）

(2) 川瀬：工学的手法による乱数発生装置　電子通信学会交換研究会資料ＳＥ72－2