琉球大学学術リポジトリ

特殊デイジタル計算機“遅延線路数ふるい”の論理および回路設計（摘要）

メタデータ	言語: 出版者: 琉球大学農家政工学部 公開日: 2011-04-28 キーワード (Ja): キーワード (En): 作成者: Kyan, Seiki, 喜屋武, 盛基 メールアドレス: 所属:
URL	http://hdl.handle.net/20.500.12000/19458

Logic and Circuits of a Delay-Line Number Sieve

By

Seiki KYAN*

Introduction

A delay-line number sieve is a special purpose digital computing device designed for solving a set of congruences into which problems involving Diophantine equations of second order, quadratic residues and other quadratic type problems can be transformed.

Because of the prohibitively long time required for the solution of this type of problem on general purpose computers it has long been desired to construct a special purpose computer for such problems.

A number of studies have been made on electronic number sieve theory and design at the University of California since 1947. They are described in Master's theses[1)~13)], and several different designs had been tried, but a completely successful one had not yet been made.

This paper describes logic and circuits of delay-line number sieve whose operation speed exceeds that of the sieve simulated in the I. B. M. 7090. That is,

$$6\times10^7 \quad \text{numbers/minute.}$$

The speed of sieve simulated in the I. B. M. 7090 computer is approximately

$$5\times10^5 \quad \text{numbers/minute.}^{14)}$$

I. Theory of Number Sieves

Sieve Problems.

Sieve problems in general can be expressed as follows[15)].

$$x\equiv a_{ij} \pmod{m_i} \qquad (1)$$

where $m_i=m_1, m_2m_3, \cdots, m_s$ are s positive integers relatively prime in pairs and $i=1, 2, 3, \cdots, s$; $j=1, 2, 3, \cdots, t_i<m_i$. For fixed i, the a_{ij} are the distinct non-negative integers less than m_i. The problems are to find all integers N between given limits, say

$$A\leq N<B,$$

such that N is a solution to s of the congruences.

It may be necessary to give a few examples in order to explain the principle of the sieve.

Sieve of Eratosthenes.

One of many such problems is the sieve of Eratosthenes. The problem here is to find all the primes p within the range of

$$A=B^{1/2}\leq p<B,$$

* Department of Electrical Engineering, Division of Agriculture, Home Economics & Engineering, University of the Ryukyus.

where $t_i=m_i-1$ for all i.

Let us, for example, find the primes p such that

$$6\leq p<36\,.$$

Congruences for the problem are;

$$\begin{aligned} &x\equiv 1 \pmod 2\\ &x\equiv 1,2 \pmod 3 \qquad \cdots\cdots(2)\\ &x\equiv 1,2,8,4 \pmod 5 \end{aligned}$$

The idea is to eliminate all the numbers which are divisible by any of these primes. Consider the following table where integers are displayed in the first row and moduli of the congruences in the first column. An intersection of an integer and a modulus will be filled by "1" if the integer is not divisible by the modulus and otherwise filled by "0". Fig. 1-1 is the resultant table.

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
3	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
5	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
c		x						x				x		x				x		x

m	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
2	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
3	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
5	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1
c				x						x		x						x		

Fig. 1-1. Table for congruences (2).

The numbers whose columns are filled with all ones are primes provided that they are within the range of $6\leq p<6^2=36$. (Marked by x in the last row c).

It should be noted that pattern of a raw is repetitive with the period of corresponding modulus.

Chinese remainder problem.

Another example is the so-called Chinese remainder problem which is to find an integer whose remainder is a if divided by A and b if divided by B, and c if divided by C.... etc. In terms of congruences, the problem can be expressed by a single remainder for all i in (1). And there will be only one solution among the numbers $N=\pi_1{}^i m_i$.

Let us, as an example, consider a problem in which we are to find a number whose remainder is 1 if divided by 2, 2 if divided by 3 and 3 if divided by 5. The congruences are;

$$\begin{aligned} &x\equiv 1 \pmod 2\\ &x\equiv 2 \pmod 3 \qquad \cdots\cdots(3)\\ &x\equiv 3 \pmod 5 \end{aligned}$$

If we make the similar table as the preceding paragraph by the same method, we get the table of Fig. 1-2.

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
3	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
5	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
c																				

m	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
2	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
3	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0
5	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0
c				x																

Fig. 1-2. Table for congruences (3).

We find that we have one integer whose column is filled by all ones, that it is unique within the range of $0 \leq N \leq 2 \times 3 \times 5 = 30$ and that it satisfies the congruences and therefore the original problem.

These two examples are rather extreme cases in that the remainders are only one less that the base number, that is $j = m_i - 1$, in the case of Sieve of Eratosthenes, and the remainder is only one for all i in the case of the Chinese remainder problem.

There are, however, very important sieve problems whose remainders are approximately $m_i/2$. They are generally called quadratic sieve problems. They include the Diophantine equations of second degree, residue systems and other quadratic type problems. It is for this type of problems that the number sieves are most useful.

Diophantine Equations.

A Diophantine equation is an ordinary polynomial equation with integer coefficients with the variables assuming only integral values.

Let us, as an example, consider a simple Diophantine equation of second degree in two variables:

$$x^2 + y^2 - 113 = 0 \quad \cdots\cdots (4)$$

The problem is to find the integers x and y which satisfy the equation (4). The equation can be easily transformed, as shown in Appendix I, into a set of congruences[16]. The congruences are;

$$\begin{aligned} &x = 1, 2 \pmod 3 \\ &x = 2, 3 \pmod 5 \\ &x = 0, 1, 2, 5, 6 \pmod 7 \quad \cdots\cdots (5) \\ &x = 0, 3, 4, 7, 8 \pmod{11} \end{aligned}$$

The corresponding table is shown in Fig. 1-3. Thus we find the roots to be 7 and 8. It should be noted that we did not need to use the (mod 11)-congruence to find the roots. Without 11's row, number 13 is added to the set of possible roots for the given equation but, on checking, we easily find that 13 is not a root of the equation. (For this particular example, however, we may not choose to use modulus 7 rather than modulus 11 because modulus 11 has 5 remainders which is less than 11/2 of maximum number of remainders so that we can exclude more than 50% of numbers under the base 11, whereas modulus 7 has 5 remainders which is to exclude only about 30%.) We can handle equations involving quite a large number by using limited numbers of moduli. The possible roots thus *sifted out* can be checked with

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
3	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1
5	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0	0	0	1	1	0
7	1	1	1	0	0	1	1	1	1	1	0	0	1	1	1	1	1	0	0	1
11	1	0	0	1	1	0	0	1	1	0	0	1	0	0	1	1	0	0	1	1
c								x	x											

Fig. 1-3. Table for congruences (5).

the given equation to get the right ones. This is why the process is called a number sieve.

History of Number Sieves.

The method explained in the preceding paragraphs is called graphical method proposed by Kraitchik in 1922 and was used by him to solve some problems in Number Theory[17].

Lehmer invented in 1925 an electro-mechanical device for this purpose which consisted of a set of motor-driven looped chains whose lengths correspond to the prime numbers for the moduli. The motor was stopped by relay switches when a solution was obtained[18]. A similar device using motion picture film[19] was built in 1936.

In 1933, he constructed another sieve called a photo-electric number sieve which consisted of a set of 30 gears whose numbers of teeth correspond to the moduli, optical system, a photo-electric cell, a relay switch, and a motor to drive the gears. The operation speed of this sieve was amazingly high for those days, namely

$$3.6\times10^5 \quad \text{number/minute.}$$

It was only when the faster and later models of general purpose computers became available that this speed was approached by other machines for this type of problem. However, it is still not practical to solve this kind of problem by the general purpose computers because of the extremely long time required for typical problems.

Delay-Line Number Sieve.

The system proposed in this paper consists of 31 delay-line registers whose lengths are proportional to the first 31 primes starting from 2, 3, 5, $\cdots$ to 113 and 127, and two binary counters to count solutions and also density of solutions.

The system is to have two different modes; *work* mode and *idle* mode. During the *work* mode, lines are connected in parallel as in Fig. 1-4; coincidence pulse from all the lines stops

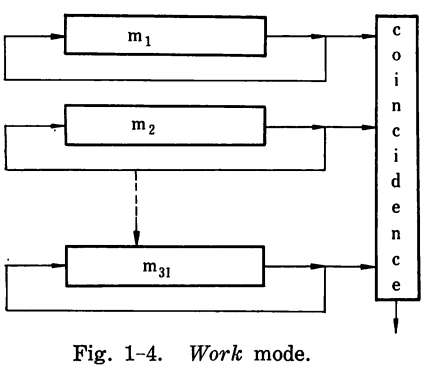


Fig. 1-4. *Work* mode.

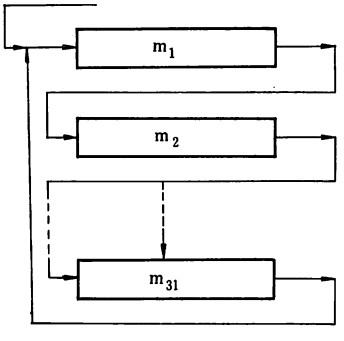


Fig. 1-5. *Idle* mode.

this mode and switches the system into the *idle* mode. During the *idle*, lines are connected in series as in Fig. 1-5 and the loading the problem may be performed while in the *idle* mode. Changing the mode from *idle* to *work* is done manually and the change from *work* to *idle* may also be done manually.

The system presents the following problems:

a) Design of reliable pulse regeneration circuit.

b) Design of an input device, specifying the problem to be solved.

c) Design of output device which will *count* solutions.

The following works have been done in this project.

1) New input logic was designed, and some modification was made on control unit of Gentner's logic[20], which are given in Chapter II of this thesis. Also, error-detection schemes are considered. Details are given in Chapter VI.

2) Pulse regenerative circuits were studied and actually built with the highest feasible pulse repetition rate of one megacycle for the available delay-line D-55. The effort was made to increase clock pulse rate because of the following reasons.

i) It would shorten the operation time which is inversely proportional to the clock pulse rate.

ii) It would cut down the cost of the system because of the less circuitry and fewer delay-lines.

iii) Reliability of the system would be increased because of the less active circuits and components which may be affected by temperature, aging and other factors.

3) A small system was built to test the new input logic. Details are given in Chapter IV.

4) A complete system with input, output, and control units was built (with last two longest lines) to test the stability and reliability. Description of the system is given in Chapter V.

5) Performance of the system was tested and some trial problems were solved. Results are given in Chapter V.

II. Logical Design

Input Logic.

During the *idle* mode all the lines are connected in series forming a large single register and loading is performed in serial fashion. Since the bits are to be stored dynamically, a marker is necessary to indicate the time to insert a bit so that the bits will be inserted sequentially, or in other words, a bit to be inserted at a certain time must be inserted right next to the bit inserted right next to the bit inserted previously.

Suppose there is a line A whose length is N in which N bits are to be stored in any given pattern and let us have another line B whose length is also N in which only a single bit is stored (both lines are times by the same clock pulse). If the output of the line B is *anded* with the input source as in Fig. 2-1, only one bit can be inserted in line A, which will be in synchronism with a bit in line B, since if other bits are inserted they will overlap and replace the one inserted previously.

In order to insert a bit after another bit, it is clear that N of the line B must become

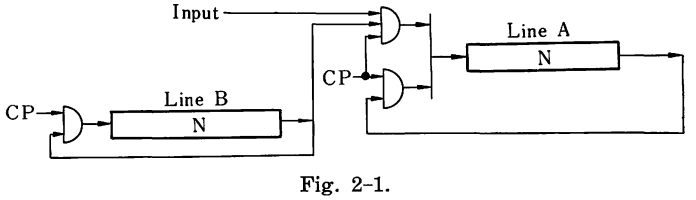


Fig. 2-1.

$N+1$ every time a bit is loaded. That is the line B will have two states.

State	Condition	Delay time of the line
1	Normal	N
2	A bit is being loaded.	$N+1$

Fig. 2-2 shows the logical diagram of the two different states.

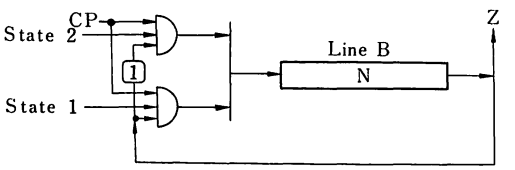


Fig. 2-2.

Let us have a single flip-flop to indicate two different conditions, which shall be denoted by FF-D hereafter. FF-D will be set when a bit is to be loaded and will be reset when a bit is to be loaded and will be reset when a bit has been loaded. The conditions required for the time when a bit is to be loaded are as follows:

a) A bit from outside world is ready to be loaded into the line. Since input data may be entered into the system asynchronously, a buffer is necessary to hold information temporarily.

b) There is an output from the line B which indicates possible time for bit insertion.

c) There is a clock pulse.

Therefore the set function for FF-D is

$$D_s=Z\cdot CP\cdot I_1\,,$$

where Z is the output of line B and I_1 is the signal to indicate that there is a bit ready to be inserted.

Fig. 2-3 is the logical diagram but scrutinizing the diagram, one can find out that a unit delay is necessary in the recirculating path of the line B as in Fig. 2-4 to match up with a unit delay assumed to be incorporated in the action of the FF-D and also reduction of delay-

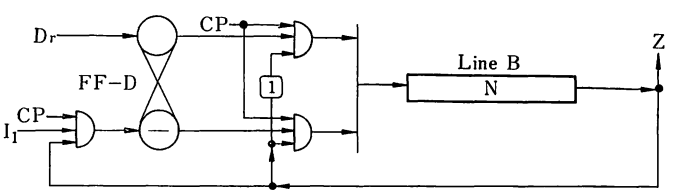


Fig. 2-3.

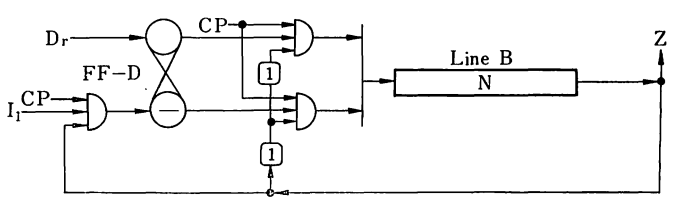


Fig. 2-4.

time of the line B to $N-1$ is necessary to make the normal path to be N. Otherwise FF-D output can not control the path of a bit in the line B.

D_r, the reset function of FF-D, has not been specified so far but the best time to reset is the very next clock pulse from the one which set the FF-D, thus to have the shortest waiting time for insertion of new bits into the line A.

Therefore,

$$D_r = D \cdot CP .$$

The input gate to the line A would be

$$A = I_2 \cdot CP ,$$

where I_2 is the input data signifying 1 or 0. I_2 should specify whether it is a one or a zero which is to be loaded whereas I_1 would only tell whether there is a bit or not waiting to be loaded. Thus, we will have two flipflops, one for a bit identity and the other for discriminating presence or absence of a bit. Former flipflop FF-A is simply set by 1 and reset by 0 of the input data and latter flipflop FF-B is set either 1 or 0 input, and reset when the loading of the information is completed. Thus,

$$\begin{aligned} A_s &= U \\ A_r &= V \\ B_s &= U + V \\ B_r &= D \cdot CP \cdot B , \end{aligned}$$

where U is input 1, and V input 0.

The complete input logic is as in Fig. 2-5.

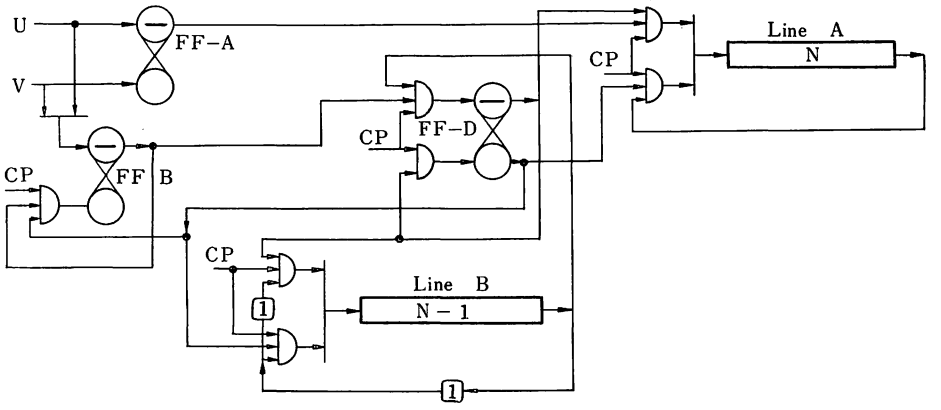


Fig. 2-5. Input Logic.

Practical Consideration of Unit Delays.

In practice, Unit delays in the preceding logic are best made with flipflops rather than with sections of a delay-line. Using sections of a delay-line would require additional amplifiers which consume power because of the terminating resistors of the lines. Distortion of the pulses due to dispersion and reflections of the line would make circuit design more difficult than it would be with flipflops.

Unit delays in the logic of previous section may be simply replaced with flipflops but some thought on the circuit would enable us to make it with a single flipflop which would be normally a unit delay and become a two-unit delay when loading is taking place.

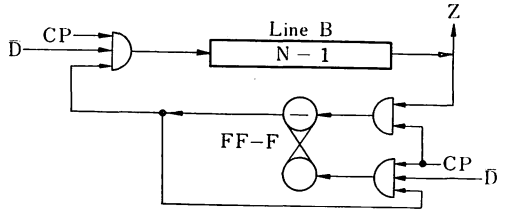


Fig. 2-6A.

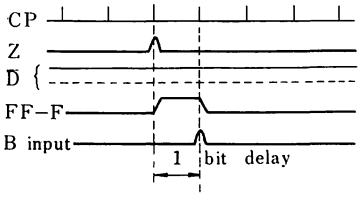


Fig. 2-6B.

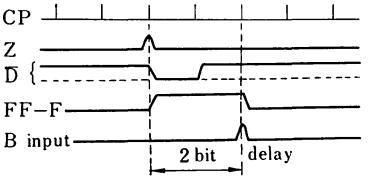


Fig. 2-6C.

Fig. 2-6A shows the logic with a flipflop and Fig. 2-6B and Fig. 2-6C show a sequence of operation during normal time, and during loading time respectively. The duration of FF-F output would be one bit time during normal time since signal $\bar{D}$ will be present at the time when the next clock pulse resets the flipflop. Therefore the input pulse to the line B will be delayed by one bit time. During the time when a bit is being loaded, however, duration of FF-F output will become two bit times because $\bar{D}$ will be absent at the next clock pulse time (FF-D is set by Z) and will become present at following clock pulse time (FF-D is reset by this time). If $\bar{D}$ were not applied to the input gate of the line B, two bits in a row would have been inserted in the line. However, the first bit which is delayed by one bit time is inhibited by $\bar{D}$ allowing the second bit which is delayed by 2 bit times to be entered into the line thus delaying 2 units during the time a bit is being loaded.

Beat Counter.

Number N in the lines A and B may be extended as large as necessary but it is much better from the economical standpoint as well as from the circuit reliability standpoint to have two or more lines in place of line B with lengths of $A, B, C, \cdots, M$ and get the Z output as the coincidence of all these lines. $A, B, C, \cdots, M$ must be such that

$$A \times B \times C \times \cdots \times M = N \qquad \text{(total length of main line)}$$

and that $A, B, C, \cdots, M$ are relatively prime in pairs.

Two lines with 33 bits and 61 bits have been chosen for our 31 lines making the total of 2013 bits as an optimum choice.

Control Unit and Over-All System Logic.

The control unit is almost the same as the one which was designed by Gentner[20] except for a minor modification on the reset function for FF-G which controls the mode of operation. The modification was made such that if there are two coincidences (solutions) on successive clock pulses and FF-G is reset by the first coincidence, it should be reset right back when set for the next solution, counting one bit on the *Result Counter*. Thus it would not miss solutions which are greater only by unity than other solutions as Gentner's did.

A single-bit insertion into the beat counter is made at the very beginning of the *idle* mode by $\bar{G}$ through a differentiator K whose time constant is considerably less than a unit clock

time. This is to set the FF-F_1 and FF-F_2 whenever FF-G is reset to *idle* mode. This bit must be erased during the *work* mode so that there is only one bit each present in the two lines of the beat counter during the *idle* mode. $\overline{G}$ applied to the input gates of the two lines are for erasing the bits during the *work* mode.

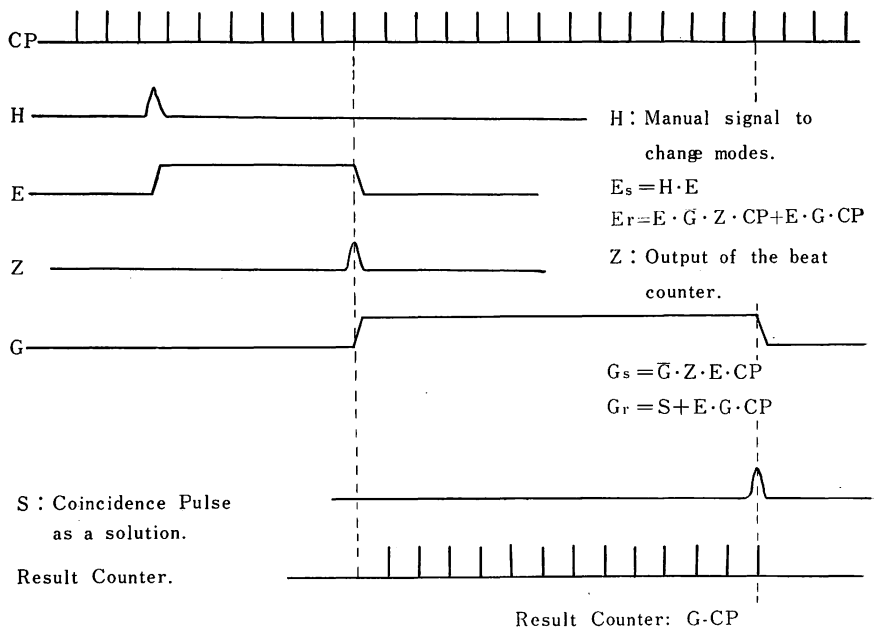


Fig. 2-8A. Sequence of operation from *idle* to *work* mode and then back to *idle* mode by coincidence output *S* counting the answer by *Result Counter*.

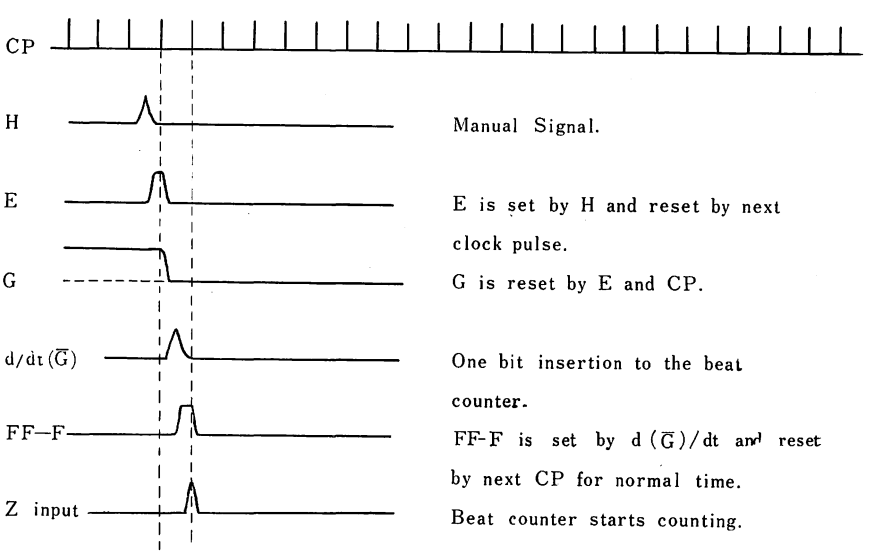


Fig. 2-8B. Sequence of one bit insertion to the beat counter at the beginning of *idle* mode.

Fig. 2-8A shows the sequence of operation from *idle* mode to *work* mode and then back to *idle* mode by coincidence output S counting the answer by the *Result Counter*.

Fig. 2-8B shows the sequence of one bit insertion to the beat counter at the beginning of *idle* mode.

Fig. 2-9 shows the complete over-all system logic of the number sieve.

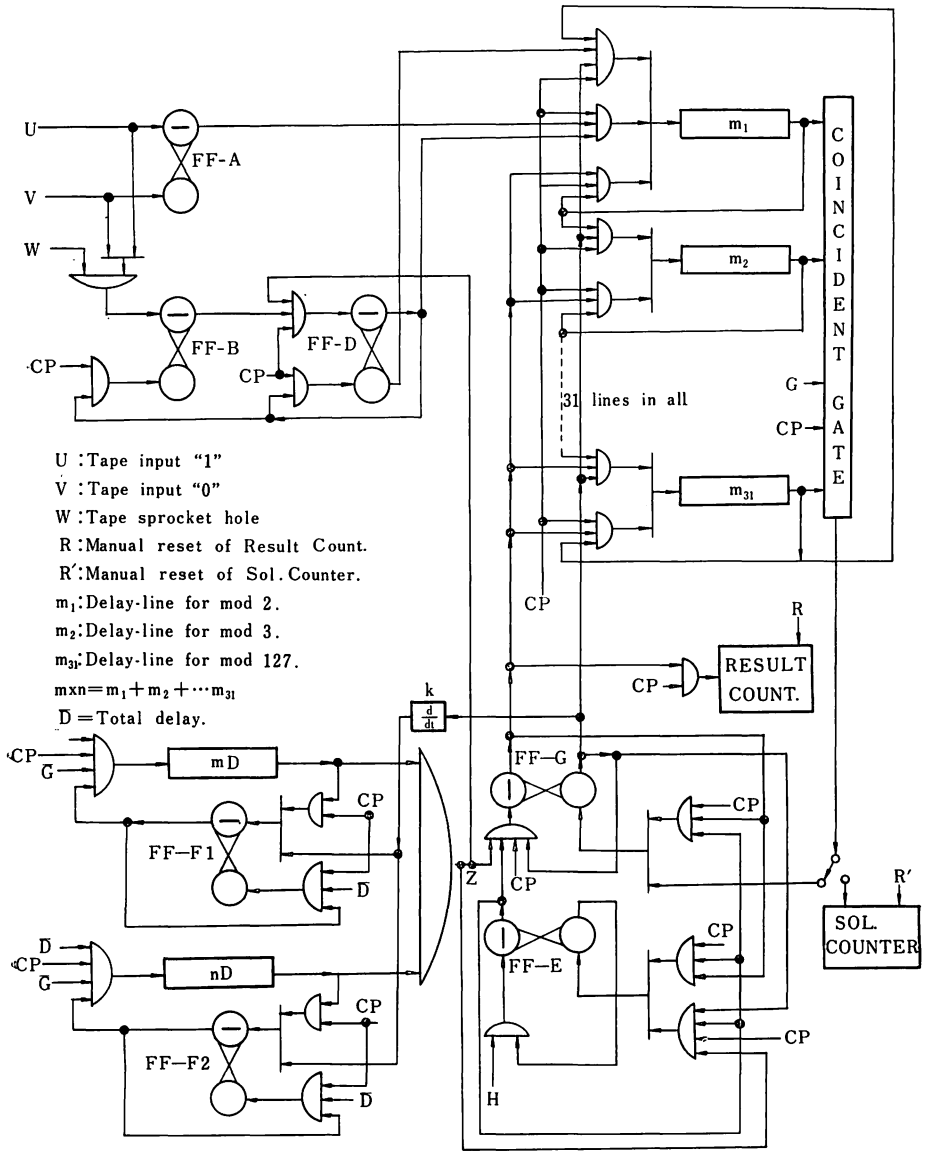


Fig. 2-9. Complete over-all system logic.

III. Delay-line Register

Experiments on Delay-line DL-55.

Before the circuit design was attempted, several experiments on the delay-lines to be used in the system were performed in order to find the optimum pulse repetition rate and pulse width for the system.

For the pulse representation, the "Return to zero" (RZ) method was chosen because of the simplicity of its sensing circuit.

The characteristics of the delay-line were calculated and measured by Rea, which are given in Appendix II of this thesis.

Fig. 3-1 shows the layout of the experiments and Figs. 3-2A, B, C, ···, G show the wave-

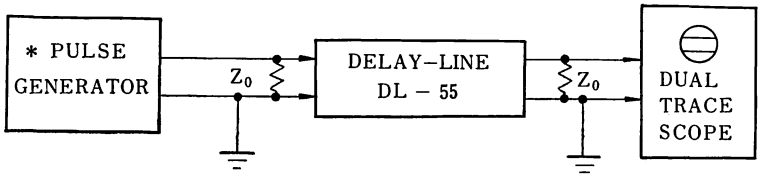


Fig. 3-1.

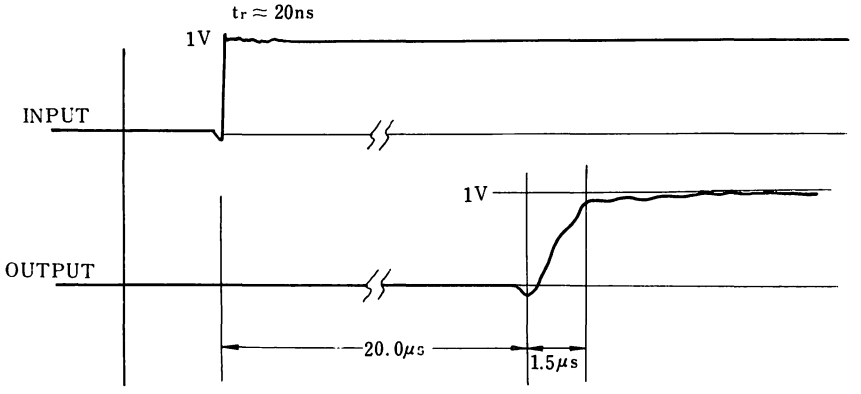


Fig. 3-2A.

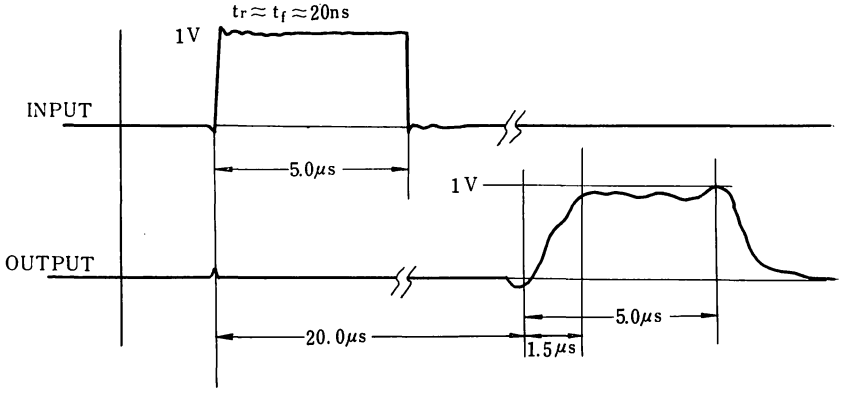


Fig. 3-2B.

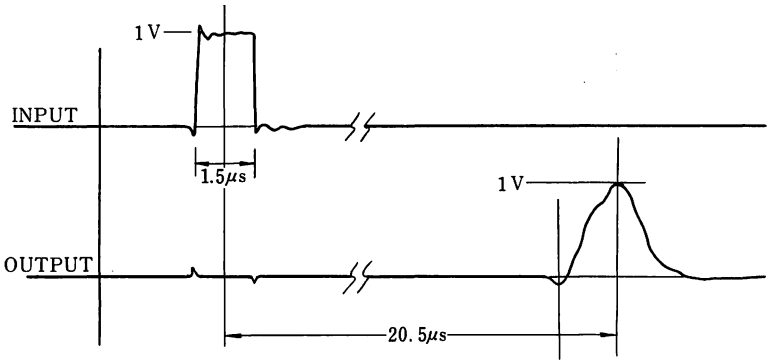


Fig. 3-2C.

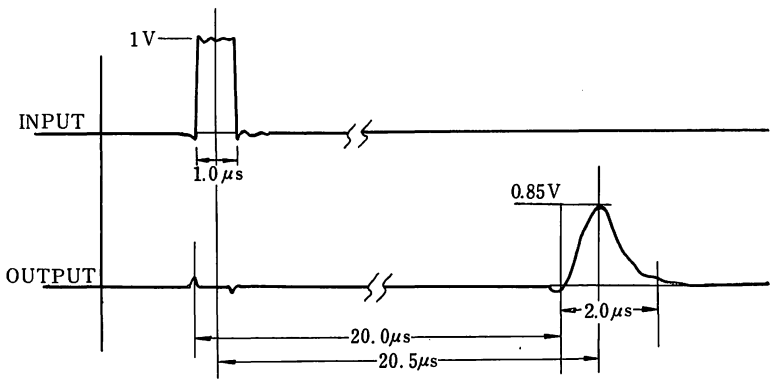


Fig. 3-2D.

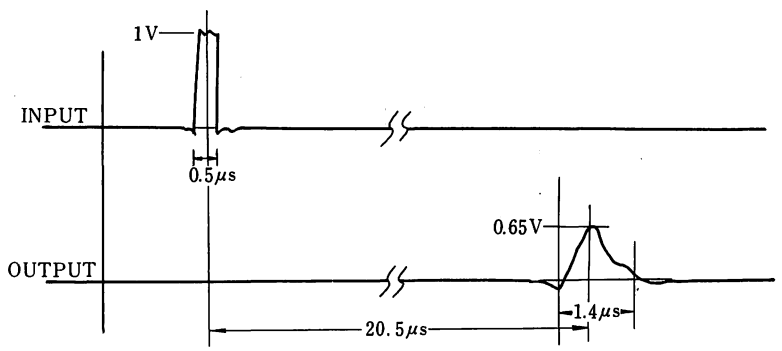


Fig. 3-2E.

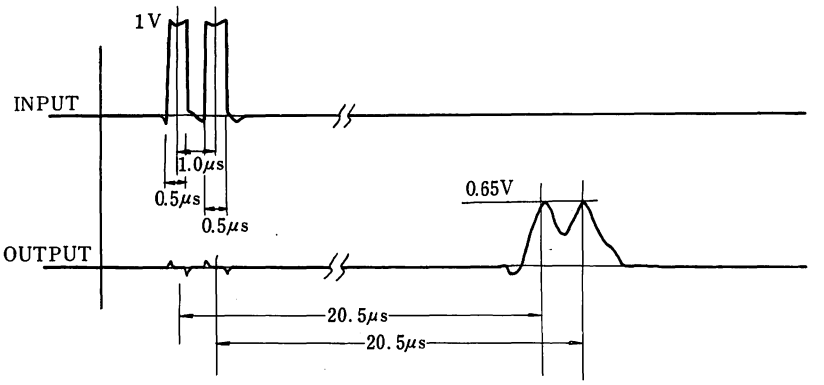


Fig. 3-2F.

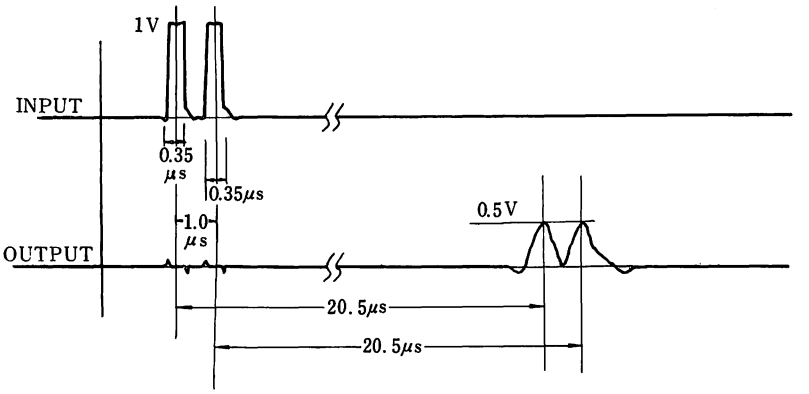


Fig. 3-2G.

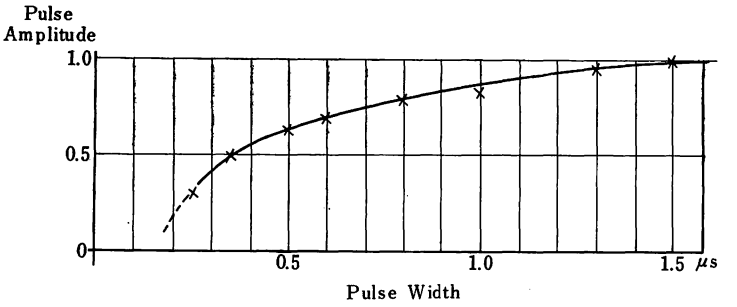


Fig. 3-3.

forms of output from a 126-section delay-line (one box) with inputs of various widths. Fig. 3-2C is the waveform with the narrowest input pulse width for the maximum output amplitude. As the pulse width is further narrowed, the output amplitude is reduced. Figs. 3-2D, and E show the consequent waveforms as the pulse width is narrowed. Fig. 3-3 shows the relation between pulse width and the output amplitude.

From Fig. 3-3, it is clear that pulse widths in the neighborhood of 0.5 microsecond are still capable of delivering more than 1/2 of the input amplitude to the output of the line. Thus, we can use a one megacycle pulse repetition rate, increasing operational time by the factor of 3 and decreasing components by approximately 1/3 compared with previous designs[21].

Fig. 3-2F, G are additional experiments using the Berkeley Double Pulse Generator to determine the optimum pulse width for one megacycle pulse repetition rate.

It was found that discrete pulses with no overlapping are obtained with 0.35 microsecond pulse width. Further decreasing the pulse width only resulted in decreasing amplitude of output sharply without affecting the dispersion giving no improvement in pulse resolution.

Another important factor on determing the frequency and the pulse width is the Signal-to-Noise ratio. The noise which seems to be caused by the stray capacitance between input and output and also by reflections was observed, its amplitude being approximately 5% of the input and pulse width being approximately 20 nanosecond when input risetime is approximately 20 nanosecond. Choosing the pulse width of 0.35 microsecond gives a Signal-to-Noise ratio of $5.5/0.5=11$, which is reasonably good for reliable operation.

Design of Pulse Regenerative Circuits.

Previous work by Rea and Gentner used a blocking oscillator as a regenerative amplifier. There are a few drawbacks in their circuits.

a) Level shift problem.

As the amplifier is capacitively coupled, the d-c component is lost and even with a d-c restorer circuits as commonly used in television, there is a considerable shift due to the random pattern of the bits, which cause difficulty in applying the proper bias to the first stage amplifier. As a matter of fact, Gentner's delay-line register encountered with erroneous bit generation when two or more lines were connected in series.

b) Pulse repetition rate.

Pulse repetition rate is too slow. Their circuit is designed for approximately 330 kilocycle whereas the experiments on the delay-lines indicate a one megacycle pulse repetition rate is quite feasible as noted above. However, blocking oscillators at this high frequency are not practical because of duty cycle limitations and the design difficulty due to ringing phenomena at such frequencies.

From the experiments on delay-lines, it is known that the noise from the delay-line has a very short pulse width with about 5% amplitude of the input. This noise may be removed not only by threshold techniques but also by using storage-delay time inherent with saturated transistors.

Therefore, the amplifier of the first stage should be normally "ON" in slightly saturated condition so that the noise pulses of short duration may be filtered out by the amplifier. In fact, later experiments showed that this method is quite effective in removing the noise due to the leakage capacitance of the delay-line.

Since first stage amplifier is to be normally "ON", it should be applied with positive pulses to its base if PNP transistors are to be used, and then the following pulse shaper has to triggered by negative pulses.

Coupling between two regenerative amplifiers is done by direct coupling. This was chosen because of the following reasons.

1. It would reduce the level shift problem due to the capacitive coupling which was the main difficulty of amplifiers of previous design.

2. It would reduce the intercoupling between the stages since direct coupling requires a

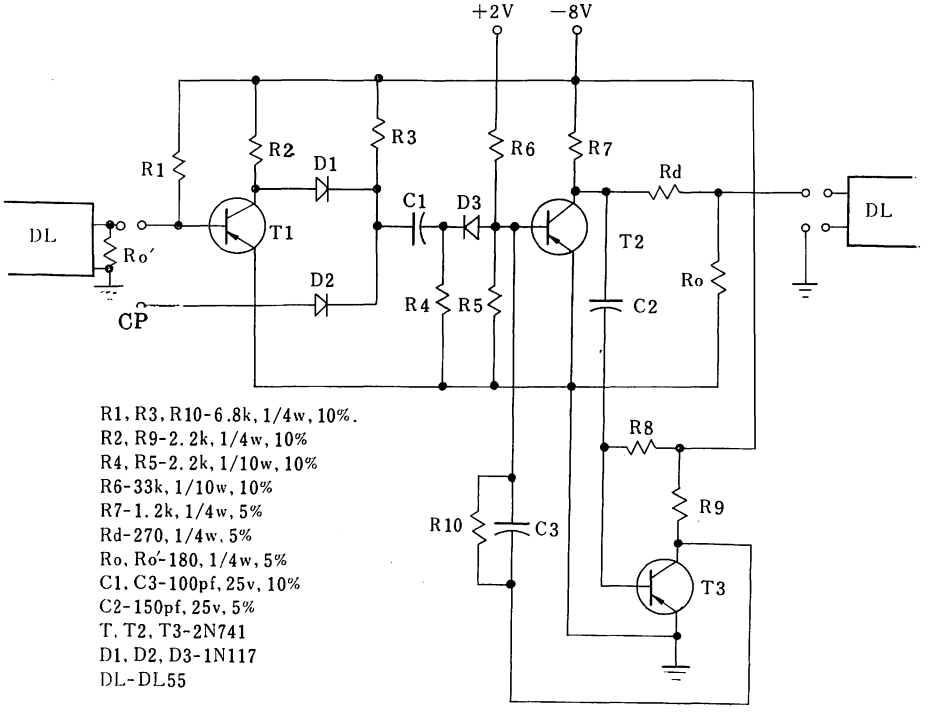
very low amplitude of output. Voltage swing at the input of the delay-line is only 1/2 volt.

3. Its operating speed can be very high, because of the small voltage changes and high frequency transistor used in this method.

4. There will be very little loss of power in changing and discharging stray capacitances, because of the very low voltage swing.

Fig. 3-4 shows the circuit diagram of the pulse regenerating amplifier. Calculation of the parameters is shown in the Appendix III.

It was found that the pulse regenerating amplifier will self-oscillate if it is connected directly to the delay-line probably due to the reflections from the delay-line although it is terminated with R_0. This self-oscillation is stopped simply by inserting a damping resistor Rd as in Fig. 3-4, instead of inserting an amplifier for isolation.



R1, R3, R10-6.8k, 1/4w, 10%.
R2, R9-2.2k, 1/4w, 10%
R4, R5-2.2k, 1/10w, 10%
R6-33k, 1/10w, 10%
R7-1.2k, 1/4w, 5%
Rd-270, 1/4w, 5%
Ro, Ro′-180, 1/4w, 5%
C1, C3-100pf, 25v, 10%
C2-150pf, 25v, 5%
T, T2, T3-2N741
D1, D2, D3-1N117
DL-DL55

Fig. 3-4. Pulse regenerating circuit.

Experiments of Delay-line Resistors.

The first experiment was with a single line storing 21 bits. It stored a random pattern without changing the contents for 8 hours. Level shift was checked by oscilloscope, which showed considerable improvement over the Rea-Gentner's results. Voltage required is 8 v±20% for the supply voltage and 2 v±20% for the bias voltage and the clock pulse can be from 1 v to 10 v without any appreciable difference. Clock pulse frequency was adjusted to 21/20.5 megacycle (the measured delay in one delay box was 20.5 microseconds) so that a single line contains 21 bits. Frequency tolerance is ±1.5%. The maximum storage capability was found to be better than 26 bits per line but it is to be used with 21 bits per line for reliable operation.

The second experiment was with 6 lines in series with 6 regenerative amplifiers which formed a 126-bit delay-line registor with 21/20.5 megacycle pulse repetition rate as in Fig. 3-5. It also stored a random pattern for several hours without change.

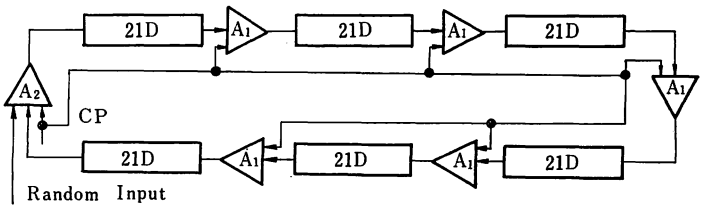


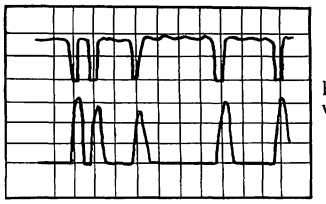
Fig. 3-5. 126-bit delay-line registor.

It was also learned that some adjustment has to be made on each bias resistor R1 in order to have optimum results. This is due to the somewhat different characteristics of the individual delay-lines and also of the transistors of the amplifier.

It is necessary to have accurate resistors R7, Rd and Ro and capacitor C2 in order to have uniform output so as to have a fixed resistor R1 as well as to select delay-lines of uniform characteristics. Although adjusting R1 is not a difficult task, it is better to eliminate these adjustments if possible.

It was observed in both experiments that the noise was completely eliminated.

Fig. 3-6 shows the picture of pulses; lower trace is unshaped pulse at the collector of T1, upper trace is shaped pulses at the collector of T2.



horiz. 0.5 micro-second/section
verti. 1.0 volt/section

Fig. 3-6.

IV. Circuit Design of Input Logic

Beat Counter.

Fig. 4-1 shows the circuit diagram of one line of the beat counter mentioned in earlier chapter. Flipflops were designed in conventional way[22] except that a delay of about 0.15 microseconds in transistor T4 was provided so that the logical sequence shown in Fig. 2-6B and C will take place definitely. T4's base resistor R11 and capacitor C4 are for this purpose.

Input Flipflops.

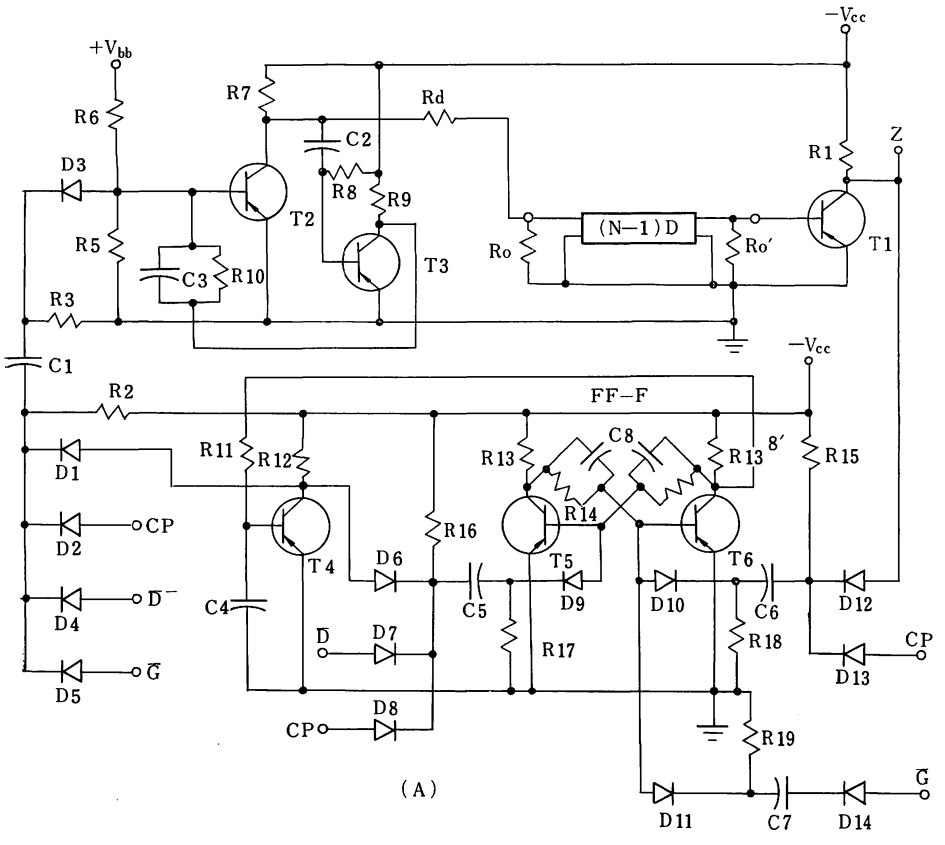
Fig. 4-3 is the logical diagram for loading a single line of 22 bits. Flipflops B and D were designed as in Fig. 4-2A and were built in a card (Vector Board 3″×4″). Pictures in Fig. 4-5A and B show the circuit cards for Fig. 4-1 circuit and Fig. 4-2 circuit and Fig. 4-2 circuit respectively.

Time delay for D and $\bar{D}$ was achieved by C7, R14, and C7', R14' as in the previous circuit.

Flipflop A was built in a separate card with two AND gates for the beat counter and for the coincidence of the two lines (113D and 127D) to be used for the following experiments in the Chapter 5. All flipflops were designed to have 0.1 microsecond rise time or better.

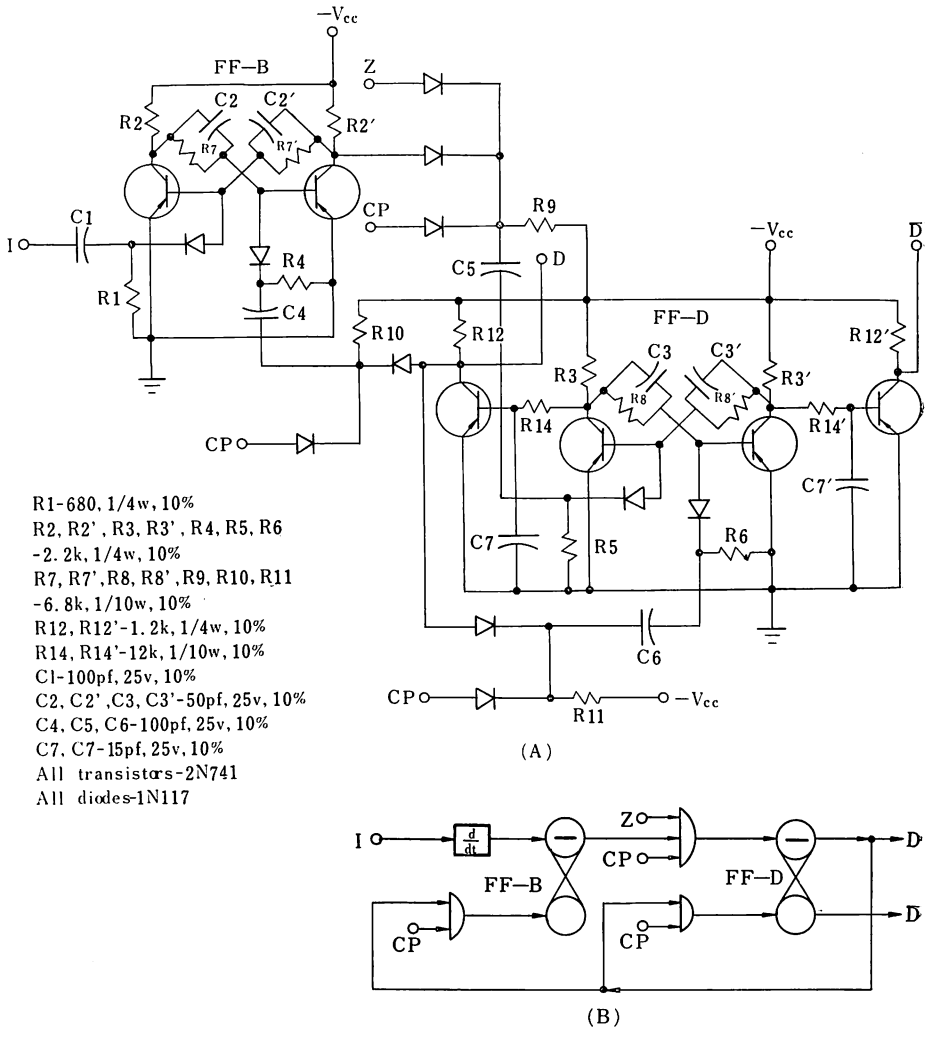
Experiment on Input Unit.

Fig. 4-3 shows the logical diagram of input unit for a single 22-bit line. S1 and S2 are the manual switch to set and reset the flipflop A for 1 and 0. S3 is the manual switch to



R1 through R10; C1, C2, C3,
Rd, Ro, Ro' are same as Figure 3-4.
R11-12k, 1/10w, 10%
R12-1.2k, 1/4w, 10%
R13, R13', R17, R18, R19
-2.2k, 1/4 w, 10%
R14, R15, R16-6.8k, 1/10w,
10%
C4-15pf, 25v, 10%
C5, C6, C7—100pf, 25V, 10%
C8, C8'-50pf, 25v, 10%

Fig. 4-1. Circuit diagram of the beat counter.



R1-680, 1/4w, 10%
R2, R2', R3, R3', R4, R5, R6
-2.2k, 1/4w, 10%
R7, R7', R8, R8', R9, R10, R11
-6.8k, 1/10w, 10%
R12, R12'-1.2k, 1/4w, 10%
R14, R14'-12k, 1/10w, 10%
C1-100pf, 25v, 10%
C2, C2', C3, C3'-50pf, 25v, 10%
C4, C5, C6-100pf, 25v, 10%
C7, C7'-15pf, 25v, 10%
All transistors-2N741
All diodes-1N117

Fig. 4-2. Circuit diagram of flip-flop B and D.

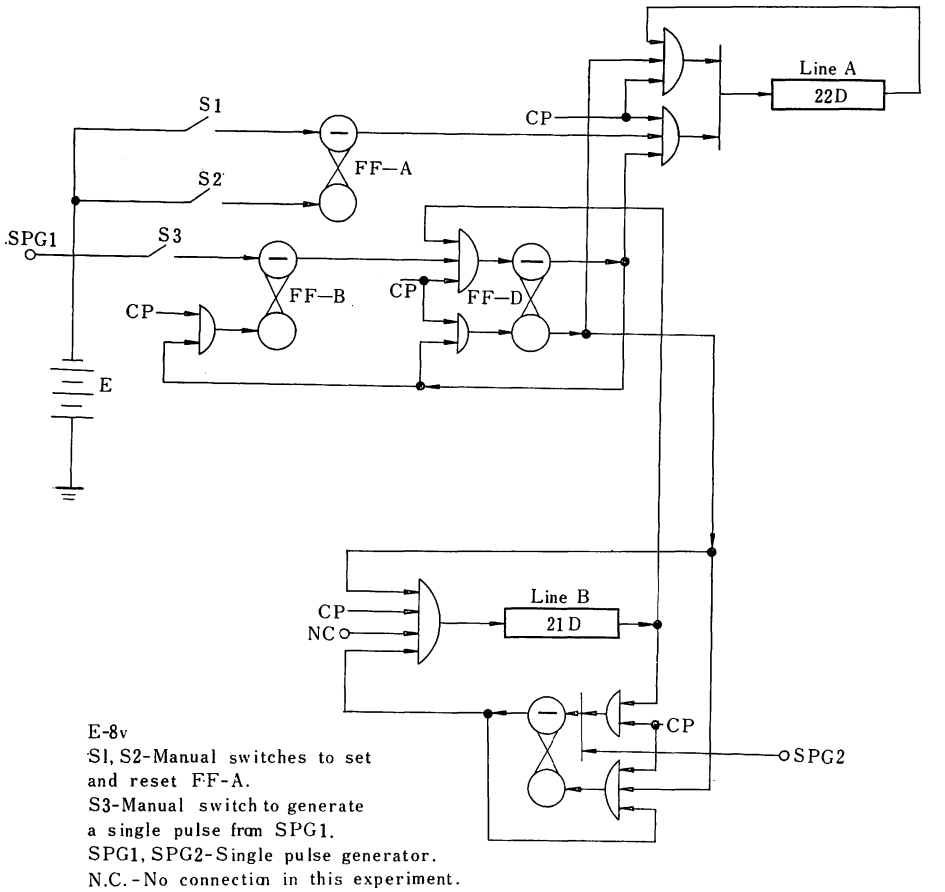


Fig. 4-3. Logic diagram of input unit for a single 22D line.

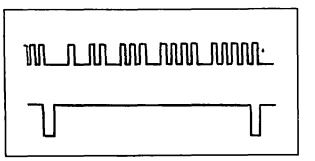


Fig. 4-4. Stored bit pattern in 22D line.
(10110111011111011111000)

generate a single pulse from a pulse generator.

The picture in Fig. 4-4 shows one of the stored bit patterns in the 22-bit line.

It was found necessary to have a time delay of 0.1 microseconds for D and $\overline{D}$, for proper bit insertion. Without delay and with the speed-up capacitors across the 12 k resistor R14 and R14′, it was found that erasing the bits by $\overline{D}$ did not occur and the insertion process inserted two bits at a time instead of just one bit.

The picture in Fig. 4-6A shows the waveforms at the various points of the beat counter which are shown in Fig. 4-6B. The picture is actually same as Fig. 2-6B.

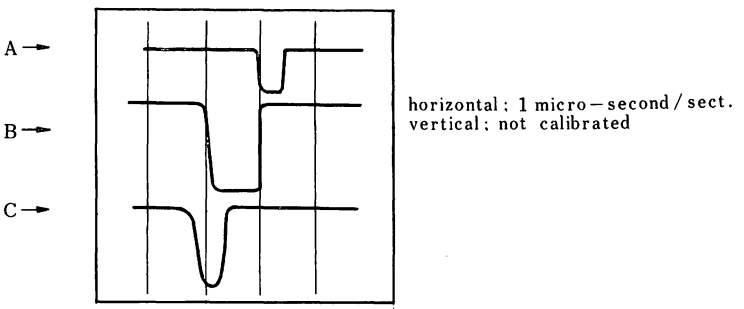


Fig. 4-6A. Waveforms of the beat counter.

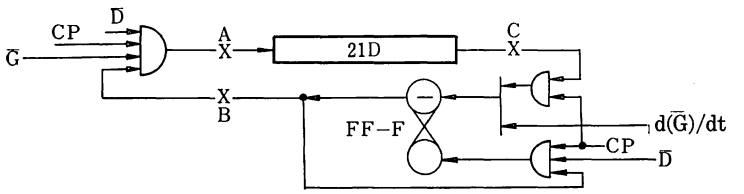


Fig. 4-6B. The points at which above pictures were taken.

V. Construction of Over-All System

Logical Interconnections.

Over-all system for this experiment is shown in Fig. 5-1. It uses the last two lines, 113-bit and 127-bit. When connected in series during the *idle* mode, it becomes a 240-bit delay-line registor. Therefore, the beat counter may have two lines of 15-bit and 16-bit making $15\times16=240$. The input data was fed by two manual switches for 1 and 0, and a single pulse generator for the presence-of-bit signal. These are to be replaced by a tape reader and its auxiliary circuits[23].

Physical Layout.

Fig. 5-2 shows the physical layout of the system. It was designed so that the wiring becomes minimum.

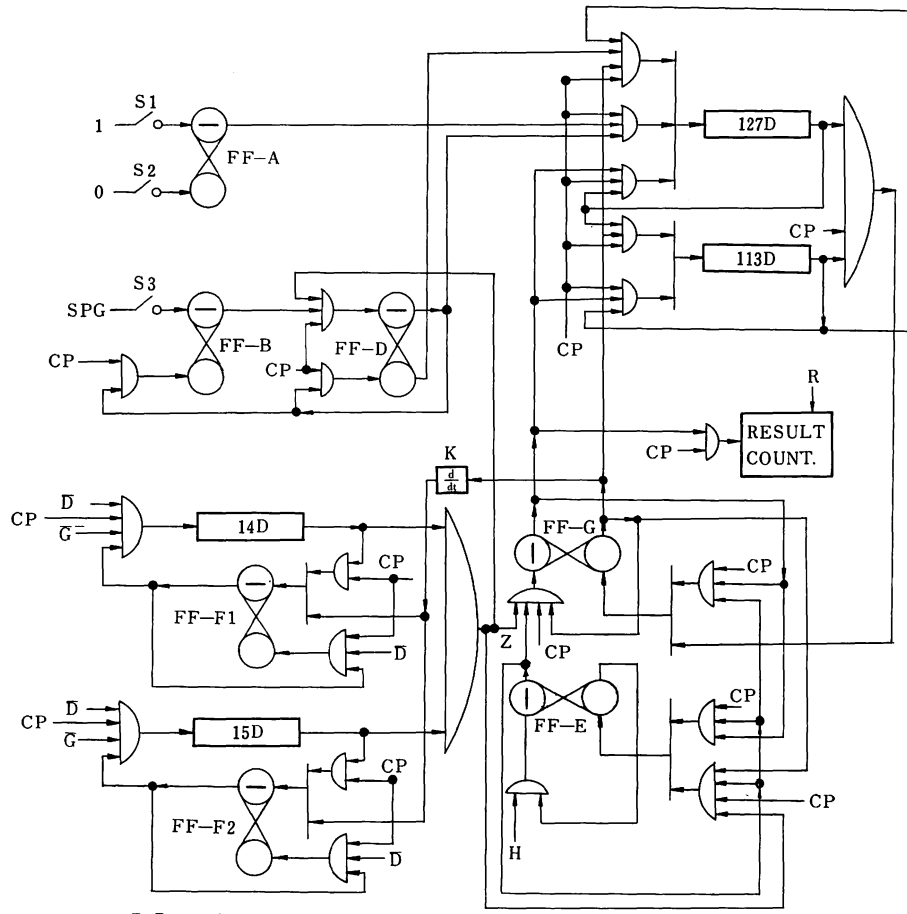
Loading.

Loading was performed by hand. The beat counter was observed working correctly although at the beginning of the operation, the following procedure had to be used:

1) When power is turned on, it may happen that the beat counter contains no bit and FF-G is on the *idle* mode. In this case, a bit has to be inserted by some means into the beat counter because without Z output, loading can not be done. To insert a bit by switching the system from the *work* mode to the *idle* mode is impossible in this case because FF-G is initially in the *idle* mode and there is no Z output to switch the flipflop into the *work* mode.

2) Another case is that when the beat counter happens to contain initially more than one bit. In this case, all it has to be done is to switch the flipflop into the *work* mode once and switch back to the *idle* mode again.

3) The last case is that when FF-G is initially on the *work* mode. In this case, no bit will be present in the beat counter because of the $\overline{G}$ application to the input gates of the two lines of the beat counter. However, by switching the FF-G to the *idle* mode, which can be



R-Reset input
SPG-Single pulse generator
CP-Clock Pulses

Fig. 5-1. Logical block diagram for the final experiment.

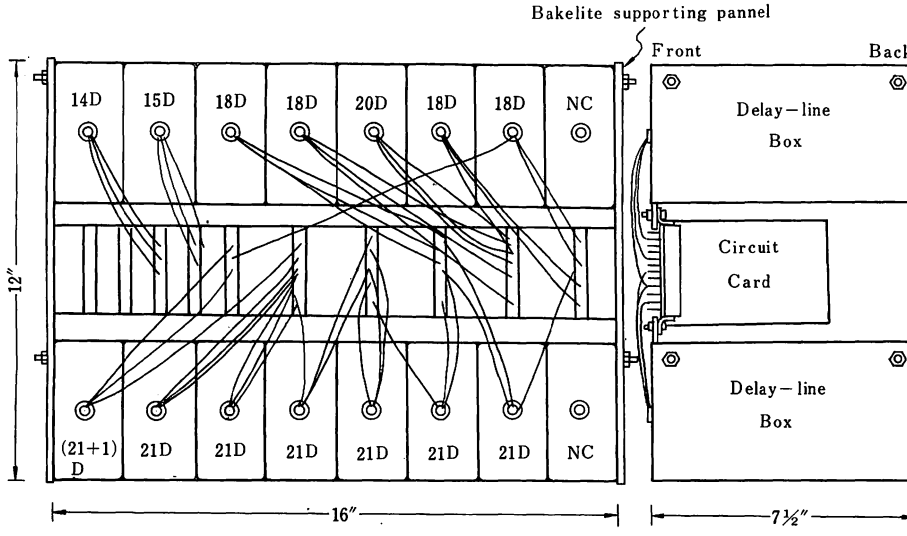


Fig. 5-2. Physical lay-out of the system.

done without, a single bit will be inserted into the beat counter.

Although these procedures once done have not to be repeated, it is rather tedious thing to do. These problems may be overcome with an additional manual switch would set the FF-G on the work mode at the beginning of the operation, thus greatly simplifying the starting procedures: Press the switch to set the system into the *work* mode if it is not so initially, and then press the *work-idle* mode switch to set it on the *idle* mode. Fig. 5-3A shows this manual switch. Automatic setting maybe done by the method shown in Fig. 5-3B. The

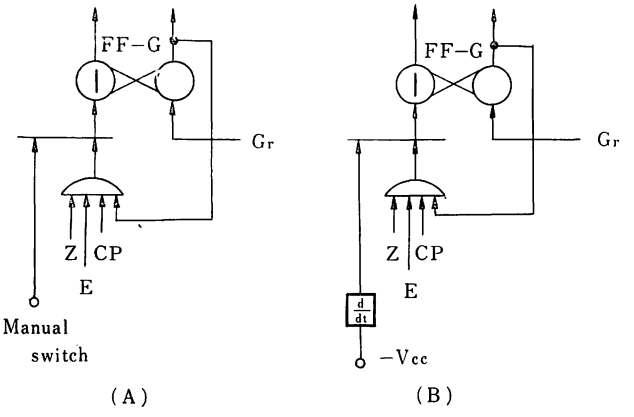


Fig. 5-3.

method is to give the set signal from transistorized power supply voltage through a differentiator of longer time constant than the rise time of the supply voltage.

Solving some problems.

The several test programs were loaded and their results are given in this section.

Problem 1.

Line 127; 0000000....all zeros....000001
Line 113; 0000000....all zeros....000001

As H switch was pressed for the *work* mode, mode indicator light blinked and the result counter showed 14351 which is the multiple of 113 and 127. Switch H was pressed 100 times without resetting the counter. The counter showed 1435100.

The problem is the equivalence of

$$x \equiv 0 \pmod{113}$$
$$x \equiv 0 \pmod{127}.$$

Problem 2.

$$x \equiv 0, 126 \pmod{127}$$
$$x \equiv 0, 112 \pmod{113}$$

Answers: 1, 016
13, 334
14, 350
14, 351

Check: $1,016 \equiv 112 \pmod{113}$
$\equiv 0 \pmod{127}$

$$
\begin{aligned}
13,334 &\equiv 0 \pmod{113}\\
&\equiv 126 \pmod{127}\\
14,350 &\equiv 112 \pmod{113}\\
&\equiv 0 \pmod{127}\\
14,351 &\equiv 0 \pmod{113}\\
&\equiv 0 \pmod{127}
\end{aligned}
$$

All existing solutions were detected and solutions which differ just by one were also detected satisfying the stringent requirement on the logic stated in Chapter 2.

Problem 3.

$$
\begin{aligned}
x &\equiv 0, 70 \pmod{113}\\
x &\equiv 0, 70 \pmod{127}
\end{aligned}
$$

Answers: 70
635
13, 786
14, 351

Check: All checked to be correct.

Problem 4.

$$
\begin{aligned}
x &\equiv 1, 21 \pmod{113}\\
x &\equiv 15, 40 \pmod{127}
\end{aligned}
$$

Answers: 4, 993
8, 270
10, 962
14, 239

Check: All checked to be correct.

Problem 5.

$$
\begin{aligned}
x &\equiv 0, 108 \pmod{113}\\
x &\equiv 0, 28, 119 \pmod{127}
\end{aligned}
$$

Answers: 4, 859
5, 080
6, 215
11, 295
14, 125
14, 351

Check: All the answers checked to be correct, and there is no correct, and there is no other solution within the limit of

$$0 \leq N \leq \prod_{1}^{s} m_i = 14,351 .$$

VI. Error Detection Schemes

Check During the Idle Mode.

Check for errors during the *idle* mode immediately after loading may be performed by loading the same program twice. It is clear that the bits stored by the first loading will coincide with the bits being inserted the second time if the loading were performed correctly both times. Therefore, detection can be made by bit-by-bit comparision to see if the bit at the point k in the line as in Fig. 6-1 is same as the bit at the point L which is just being inserted. If it does not coincide, it means loading has not been done perfectly which may be the consequence of the malfunction of any one of the 106 amplifier in the main line, or malfunction of loading system.

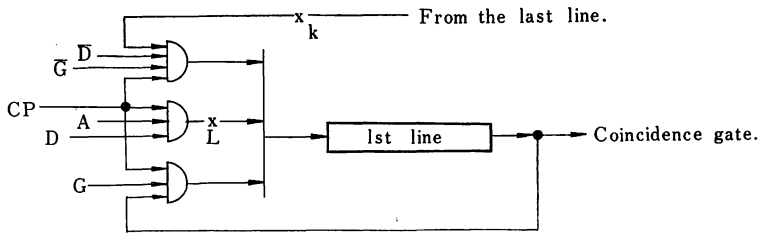


Fig. 6-1.

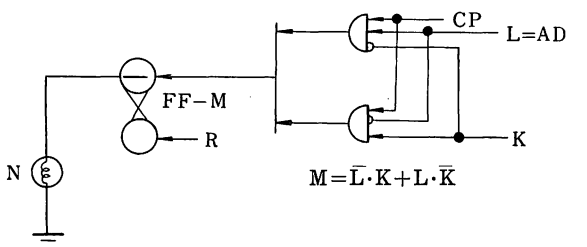


Fig. 6-2.

Fig. 6-2 shows the logic diagram of the system. It should be noted that L in Fig. 6-2 is A·D not A·D·CP as in Fig. 6-1. Therefore, it is necessary to have a coincident gate to get the signal from A and D to feed to L in Fig. 6-2. R is to reset flipflop FF-M manually at the beginning of the second loading. The light N will become ON when an error is detected.

Check During the Work Mode.

Probably the simplest check during the *work* mode is to check by oscilloscope. Each line may be checked for correct bit patterns at any time during the *work* mode by oscilloscope with high impedance probe. Isolating amplifier may be needed between the probe and the lines. The selection of the lines to be checked may be done simply by a mechanical selection switch such as rotary switch. The important problem of providing a synchronizing signal appropriate to each line is being studied by Brent Miller.

VII. Conclusion

From the experiments on Chapter 5, it is safe to say the system can be extended into full lines (31 lines) without too much difficulty. However, following cautions must be taken

in assembling the complete system.

a) Ground lines should be made with larger wires and one point connection should be maintained wherever possible.

b) Shielding the line from the amplifier to the delay-line may not be necessary because of the low voltage swing and low impedance of the delay-line, but should avoid the inter-coupling between the lines by proper layout.

c) Physical layout should be made also for the convenient maintenance and operation.

d) Isolation low pass filter should be made between AC line and the system to filter the high frequency noise generated by near-by instruments when they are turned on or off.

APPENDIX I

TRANSFORMATION OF A DIOPHANTINE EQUATION INTO CONGRUENCES

A Given Equation.

$$x^2+y^2=113$$

Method.

We may choose 7 as an "excluding number". We construct the following table.

$x=0$	1	2	3	4	5	6	
$x^2=0$	1	4	9	16	25	36	
$=0$	1	4	2	2	4	1	(mod 7)
$N=113=1$							(mod 7)
$N-x^2=1$	0	−3	−1	−1	−3	0	
$=1$	0	4	6	6	4	0	(mod 7)
x	x	x			x	x	

$N-x^2$ to be perfect square number y^2, its residues must be restricted to numbers 0, 1, 2 and 4. Therefore, acceptable residues of 7 are 1, 0, 4, 4, 0 out of 1, 0, 4, 6, 6, 4, 0. Their corresponding numbers for x are 0, 1, 2, 5 and 6.

Therefore, congruence is;

$$x=0, 1, 2, 5, 6 \pmod 7 .$$

Similarly, we can get following congruences;

$$x=0, 1 \pmod 2$$
$$x=1, 2 \pmod 3$$
$$x=0, 3, 4, 7, 8 \pmod{11} .$$

(mod 2)-congruence is useless because it does not exclude any number at all. This is why it was not used in Chapter 1.

APPENDIX II

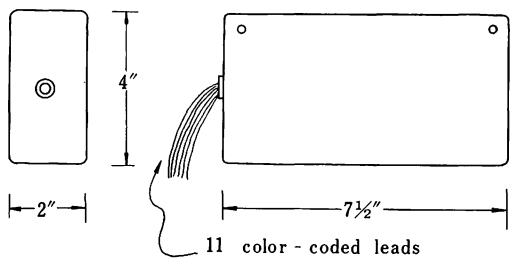
DELAY-LINE CHARACTERISTICS

Manufacturers.

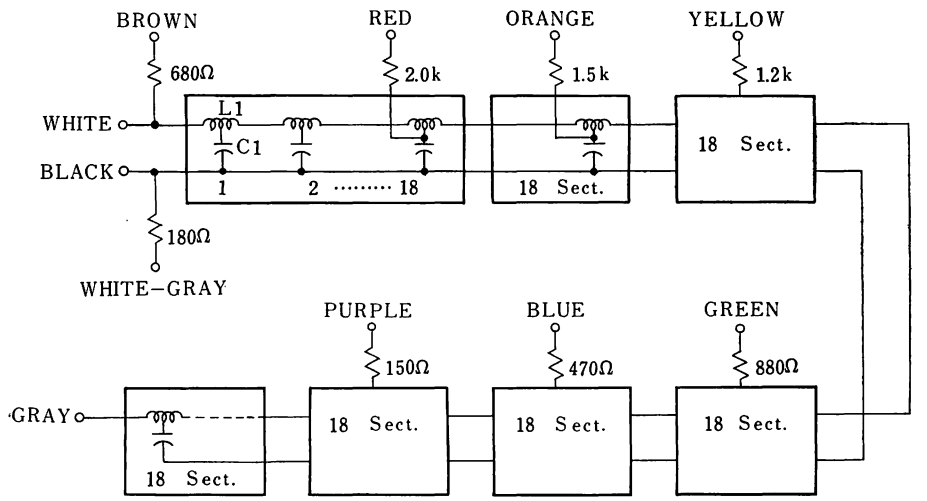
a. Brubaker Electronics—part number DL55.

b. Capehart-Farnsworth—part number 801882.

Physical Dimension



Schematic Diagram



126 T sections in all in one box.

Parameters.

C1: Capacitance of a T section.
Measured value: 980 picofarads.

L1: Inductance of a T section.
Measured value: 15 microhenrys.

Calculated C and L.

$C = C1/m = 770$ picofarads.

$L = \frac{4mL1}{m^2+1} = 25.2$ microhenrys.

$m = 1.27$, the value which yields the flattest possible delay versus frequency curve.

fo: Cut-off frequency.

$fo = \frac{1}{2\pi\sqrt{LC}} = 2.3$ megacycles.

Zo: Characteristic impedance.

$Zo = \sqrt{\frac{L}{C}}$ (for $f \ll fo$) $= 181$ ohms.

Zo measured: 185 ohms.

t_s: Delay time for a T section.

t_s=1.20 LC=0.167 microseconds.

t_d: Delay of 126 sections, or one DL55 line.

t_d=126t_s=21.1 microseconds.

t_d measured: 20.5 microseconds.

t_r: Rise time (10%-90%).

t_r=0.86 microseconds (measured).

APPENDIX III

REGENERATION CIRCUIT

The diagram on page 51 shows the regeneration circuit designed for this sieve.

T2 is kept normally off by R6 and R5, and T3 normally on by R8. During this normal condition, C2 is charged to Ec as in Fig. 8-2B.

As a negative trigger is applied to the base of T2, T2 turns on grounding the capacitor C2 as in Fig. 8-2D switching the base of T3 to positive potential. T3 then turns off and is kept off until capacitor C2 discharges through R8 down to the potential which is sufficiently negative to turn T3 on.

Duration to keep T3 off which is in turn to keep T2 on is entirely determined by C2 and R8.

Base potential of T3 is calculated as follows.

$$Eb3=-Ec+(Ec+Vcc)\left(1-Exp\left(-\frac{t}{C2\ R8}\right)\right) \quad \cdots\cdots\cdots\cdots\cdots\cdots (6)$$

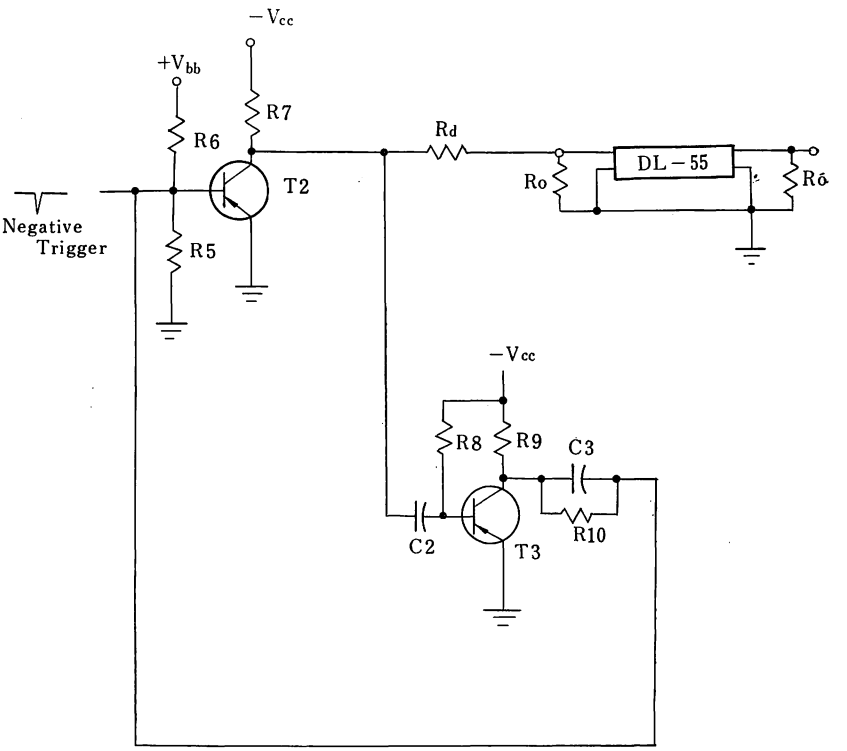


Fig. 8-1.

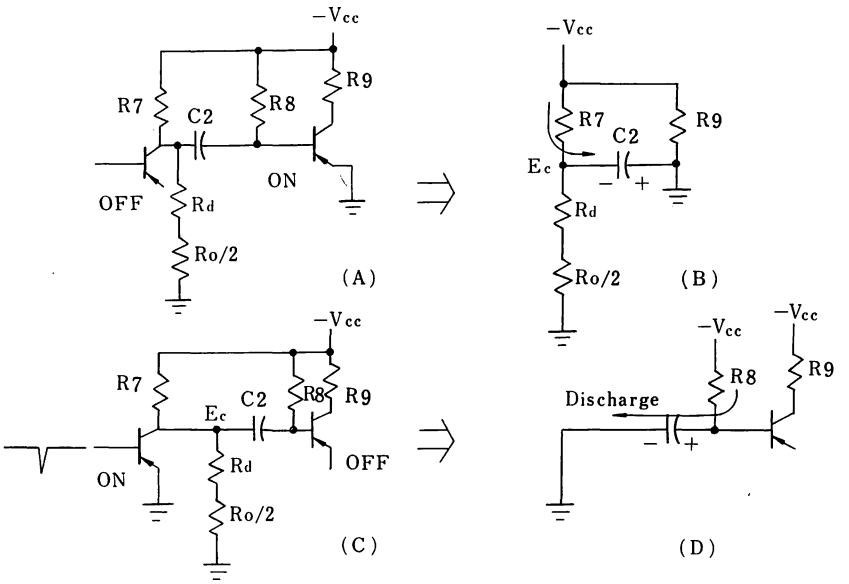


Fig. 8-2.

Where

$$Ec=\frac{Vcc(Ro/2+Rd)}{R7+Rd+Ro/2}.$$

Therefore, C2 and R8 may be determined from the following equation.

$$C2\ R8=To/\ln\left[\frac{1}{1-\frac{Eb3o+Ec}{Ec+Vcc}}\right] \quad \text{.....(7)}$$

Taking Eb3o=0v, and experimentally determined To=0.35 microseconds, we get from equation (7),

$$C2\ R8=0.35/\ln(1.14)=\frac{0.35}{0.131} \quad \text{.....(8)}$$

Now, determining R8, the collector current Ic of T3 was chosen to be 3.6 milliamperes for proper switching time. Hence R9 becomes 2.2 k.

For this value of Ic, Ib is found to be 0.25 milliamperes from the data sheet of Motorola transistor 2N741. Twice this value, 0.44 mA is provided by R8 which is 18 k.

Therefore, from the equation (8), we calculate the value of C2.

$$C2=\frac{0.35}{0.131}\cdot\frac{1}{18}\ \text{(microfarads)}$$
$$=148\ \text{picofarads.}$$

150 pf was used for C2 in the circuits.

R7 was initially chosen to be 1.2 k to provide about 6.7 milliamperes collector current of T2, which is sufficient to switch in 1/10 microseconds for the 50 pf wiring capacitance. The current to be used in charging 50 pf wiring capacitance is

$$\frac{C\Delta V}{\Delta t}=\frac{50\times10^{-12}\times8}{0.5\times10^{-6}}=0.8\,\mathrm{mA}.$$

6 times this value was taken for the collector current of T2.

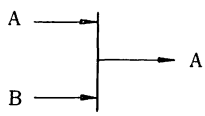
Damping resistor Rd was experimentally determined to stop oscillation mentioned in Chapter 3. It is about 270 ohms.

R10 is to provide base current Ib2 of T2 which is sufficient to switch T2 in 1/10 microseconds and R3 in Fig. 3-4 is also determined for proper switching. R10 and R3 which are 6.8 k will provide about 10 times as large base current necessary to give required collector current.

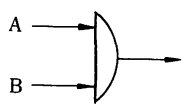
Speed-up capacitance C3 was determined emprically to be 50 picofarads.

APPENDIX IV

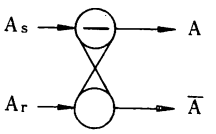
TABLE OF SYMBOLS



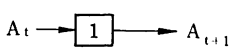
"OR" GATE



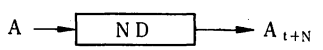
"AND" GATE



FLIPFLOP



UNIT DELAY



N–BIT DELAY

Footnotes

1) Cunningham, J. L., "Design of Control Circuits for an Electronic Number Sieve," unpublished Master's Thesis, University of California, Berkeley, 1948.
2) St. Clair, H. K., "The Design of High Frequency Counters," unpublished Master's Thesis, University of California, Berkeley, 1948.
3) Dell, H. R., "The Electrical Design of Electronic Number Sieve," unpublished Master's Thesis, University of Calif. 1949.

4) Haanstra, J. W., "A new Design for an Electronic Number Sieve," unpublished Master's Thesis, University of Calif. 1950.
5) Michelson, J. R., "The Design of Sectionalized Ring Counters," unpublished Master's Thesis, University of California, Berkeley, 1950.
6) Nina, J. P., "The Design and Development of a 137-stage Matrix Decoder," unpublished Master's Thesis, University of California, Berkeley, 1951.
7) Mesiano, C. E., "The Design of Control Circuits for an Electronic Sieve Computer," unpublished Master's Thesis, University of California, Berkeley, 1951.
8) Arsenault, W. R., "Analysis and Development of an Electronic Number Sieve," unpublished Master's Thesis, University of California, 1952.
9) Boyson, J. A., "Engineering Design of an Electronic Number Sieve," unpublished Master's Thesis, University of Calif. 1952.
10) Rea, D. E., "Pulse Circuitry for a Delay-line Number Sieve," unpublished Master's Thesis, University of California, Berkeley, 1960.
11) Gentner, O., "Logical Circuitry for a Delay-line Number Sieve," unpublished Master's Thesis, University of Calif., Berkeley, 1960.
12) Paulson, D. H., "Paper Tape Reader for a Delay-line Number Sieve," unpublished Master's Thesis, University of Calif. Berkeley, 1961.
13) Gentner, O., "Delay-line Number Sieve Report," unpublished Master's Thesis, University of California, Berkeley, 1961.
14) Estimated by Prof. Lehmer, D. H., Mathematics Department, University of California, Berkeley.
15) Lehmer, D. H., "The sieve problem for all-purpose computers," Mathematical Tables and Aides to Computation, v. 7, 1953, p. 6-14.
16) Lehmer, D. H., "The Mechanical Combination of Linear Forms," American Mathematical Monthly, v. 35, 1928, p. 114-121.
17) *Ibid.*
18) *Ibid.*
19) Lehmer, D. H., "Photo-Electric Number Sieve," American Mathematic Monthly, v. 40, No. 7, 1933, p. 401-406.
20) Gentner, "Logical Circuitry...."
21) Rea, *loc. cit.*
22) Pressman, A. I., "Design of Transistorized Circuits for Digital Computers," 1961, p. 278-307.
23) Paulson, *loc. cit.*
24) Graduate Student, Electrical Engineering Department, University of California, Berkeley.

特殊デイジタル計算機"遅延線路数ふるい"の論理および回路設計 (摘要)

喜屋武盛基

いわゆる万能デイジタル計算機 (general purpose digital computer) は文字通り万能でありあらゆる種類の演算から言語の翻訳などに至るまで適当なプログラミングにより行なうことができる。しかしこの型の計算機はある種の計算にはまったく不向きで，その驚くべき早さの演算能力をもってしても相当長い時間を必要とすることが知られている。整数論の二次不定方程式やその他の平方剰余の問題を解くのに使はれる連立合同式の解法がその一つである。

この種の計算を万能計算機に行なわせるには経済的に不可能なことなので，この計算だけを行なわせる特殊目的のデジタル計算機の開発が数年前から試みられている。

この論文では“数ふるい”と称する連立合同式を解くことのみを目的とする電子計算機の論理設計と回路試作について論じている。

この計算機の記憶装置（メモリ）としては LC 遅延線路を主体として 20.5μs の長さの遅延線路に 21 ビットのパルスをたくわえまた 1 ビットの記憶にはフリップフロップを用いて行なった。演算をコントロールする主要部分である計数回路には遅延線路を用いた特殊な設計のビート計数回路を用いて信頼度を高めることができた。このため高価な電子管式計数器の使用をはぶくことができた。

試作機の全記憶容量は 240 ビットである。この容量の範囲で可能な種々の連立合同式の計算を行なわせて正しい結果を得ることができた。

最後に誤動作自動検出装置について論じ，その論理設計も行なった。