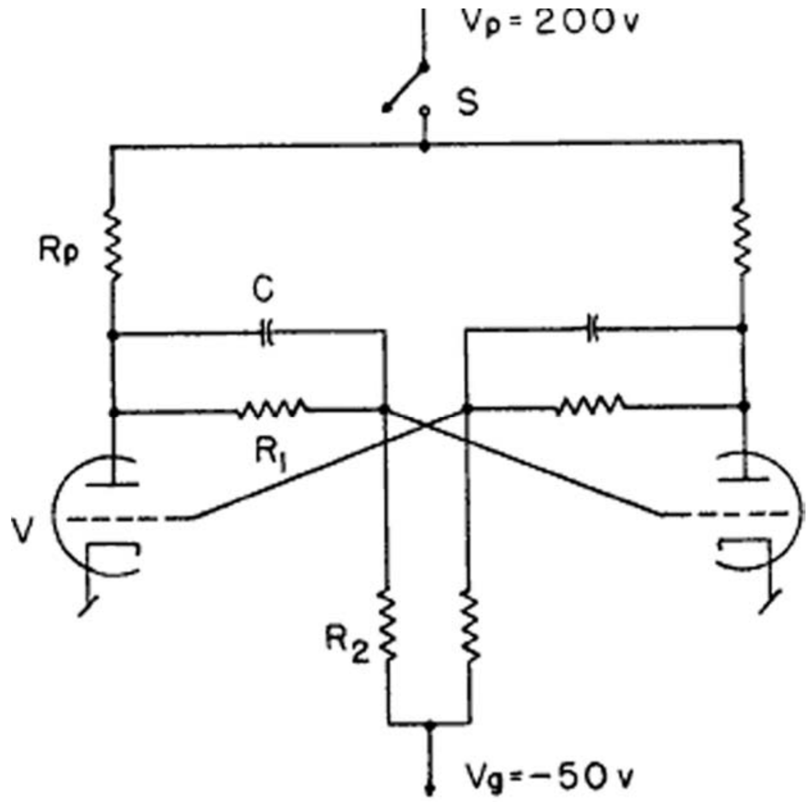
Flip-flop as Generator of Random Binary Digits

The aim of the present note is to show that a well known electronic element of digital computers, the flip-flop, may be used for generating a series of random binary digits with equal probabilities.

Let us consider a flip-flop as shown on fig. 1 and let A and B denote two possible stable states of the flip-flop. If we switch on the contact S, the flip-flop will be randomly set in one of its states A or B. We may obtain by the aid of the flip-flop a sequence of 2k random elements $X_1, X_2, \cdots, X_{2k}$, (abbreviated $\{X_{2k}\}$), where

$$X_j = \begin{cases} \text{A, if j-th switching on the contact } S \text{, set flip-flop in state A} \\ \text{B, if j-th switching on the contact } S \text{, set flip-flop in state B} \end{cases}$$

and $1 \leq j \leq 2k$.



Rp = 10 KΩ
R1 = 160 KΩ
R2 = 50 KΩ
C = 50 μμfd
V = ½ 6SN7

FIG. 1.

In this way we may obtain a finite random series of A and B which are statistically independent. One series produced by the aid of a flip-flop is given below:

AABAABBABBABBBABBAABABABBABAABABABBAA
BABABBBBBBBBBABBBABAABBB.

Let $\{Y_k\}$ be the sequence of k pairs of elements of $\{X_{2k}\}$ such that $Y_i = X_{2i-1}, X_{2i}$, where $1 \leq i \leq$ k. Omitting in $\{Y_k\}$ all elements of the form AA and BB we obtain a third sequence whose elements are the pairs AB and RA only, denoted in the following by 0 and 1 respectively.

Let $p_j(\text{A})$ and $p_j(\text{B})$ denote probabilities that j-th switching on of contact S set flip-flop in state A or B respectively and suppose that $p_j(\text{A})$ and $p_j(\text{B})$ *are* asymmetric, say $p_j(\text{A}) > p_j(\text{B})$. Supposing that the flip-flop does not change its properties during two successive switchings, we may write

(1) $$p_{2i-1}(\text{A}) = p_{2i}(\text{A})$$

(2) $$p_{2i-1}(\text{B}) = p_{2i}(\text{B}).$$

From 1 and 2 we have

(3) $$p_{2i-1}(\text{A}) \cdot p_{2i}(\text{B}) = p_{2i-1}(\text{B}) \cdot p_{2i}(\text{A}).$$

Because

(4) $$p_{2i-1}(\text{A}) \cdot p_{2i}(\text{B}) = p_i(0)$$

and

(5) $$p_{2i-1}(\text{B}) \cdot p_{2i}(\text{A}) = p_i(1),$$

therefore

(6) $$p_i(0) = p_i(1)$$

where $p_i(0)$ and $p_i(1)$ are probabilities of zeros and ones in the i-th place of the sequence $\{Y_k\}$.

The procedure above described may be used for production of binary random numbers by automatic digital computers. In this case the manual switch S must be replaced by an electronic switch, of course.

Z. PAWLAK

Warszawa, Poland