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 $X_1, X_2, \ldots, X_{2k}$ (abbreviated $\{X_{2k}\}$), where

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

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

![Fig. 1](image)

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:

\[
AABBBABBABBBABBBABBAABABBAABBBAA
\]

\[
BABBBABBABBBABBBABBBABBAABBBBA
\]

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

\[
\begin{align*}
(1) & \quad p_{2i-1}(A) = p_{2i}(A) \\
(2) & \quad p_{2i+1}(B) = p_{2i}(B).
\end{align*}
\]

From 1 and 2 we have

\[
\begin{align*}
(3) & \quad p_{2i-1}(A) \cdot p_{2i}(B) = p_{2i-1}(B) \cdot p_{2i}(A).
\end{align*}
\]

Because

\[
\begin{align*}
(4) & \quad p_{2i-1}(A) \cdot p_{2i}(B) = p_i(0) \\
(5) & \quad p_{2i-1}(B) \cdot p_{2i}(A) = p_i(1),
\end{align*}
\]

therefore

\[
(6) \quad p_i(0) = p_i(1)
\]

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

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.

Warszawa, Poland

Z. Pawlak