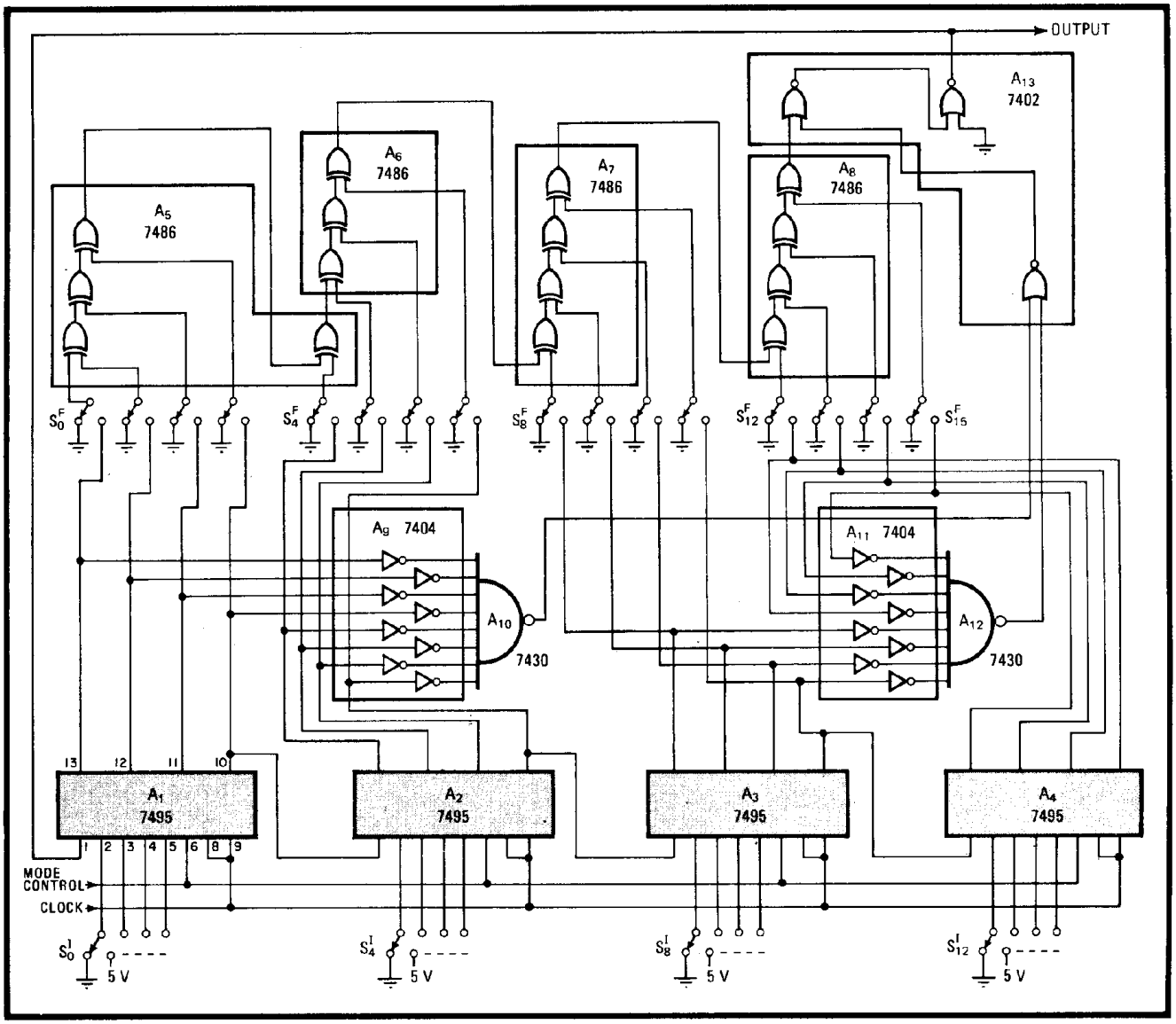
Pseudorandom generator has programmable sequence length

by Ajit Pal
Indian Statistical Institute, Calcutta, India

Providing a pseudorandom binary sequence of order i in the range of 2 to 16, this generator will find many uses in fault-detection and speech-scrambling equipment. Any sequence having a maximum length of $2^{16}-1$ can be generated. If the sequence can be selected electronically, instead of mechanically by means of a manual-switching arrangement as shown, the unit will be extremely useful in automatic-test environments.

The pseudo-random sequence is produced with the aid of a 16-bit shift register and appropriate circuitry for providing a feedback signal to the register's first stage. A_1–A_4 are the 4-bit registers that comprise the 16-bit stage, wired to shift bits from left to right on every system clock. A_5–A_7, connected at the register's outputs, and A_8 are exclusive-OR gates used to generate the feedback signal, which is determined by switches S_i^F. The switch positions are set in accordance with the primitive polynomial of the binary sequence to be generated. Note that the settings of the switches in the figure correspond to a sequence of length $2^{15}-1$, or an equivalent primitive polynomial of $x^{15}+x+1$.

A_9–A_{13} detect the all-zero condition of A_1–A_4 and ensure that the register will not be locked in that state on power-up or during normal operation. The mode control input otherwise allows A_1–A_4 to be set at any point in the sequence as determined by the S_i^I switches. □



Selection. Switches S_i^F and A_5–A_8 derive suitable feedback signal so that shift register A_1–A_4 can generate a pseudorandom binary sequence of selectable length. A_9–A_{13} detect register's all-zero state and prevent register lock-up by generating logic 1 bit to A_1–A_4 input during power-initialization period. Switches S_i^I initialize registers at any point in a sequence that may extend to $2^{16}-1$ bits.