5 Feedback with Carry Shift Registers

First, the definition of a *finite state machine* according to Golomb's famous book *Shift Register Sequences* is given.

Definition 5.1. A *finite state machine* consists of a finite collection of *states* $K = \{K_i\}$, sequentially accepts a sequence of *inputs* from a finite set $A = \{a_i\}$, and produces a sequence of *outputs* from a finite set $B = \{b_i\}$

A *feedback with carry shift register* is a feedback shift register which uses a linear combination each state toA description of N-ary feedback with carry shift registers is defined here. The definition of the register follows the one given in Andrew Klapper's book.

Definition 5.2. Let $q_0, q_1, \ldots, q_m \in \mathbb{Z}/(p)$ for $p \in \mathbb{Z}$ and assume that $q_0 \not\equiv 0 \pmod{p}$. An *algebraic feedback shift register* (or *AFSR*) over ($\mathbb{Z}$,p,S) of length m with *multipliers* or *taps* $q_0, q_1, \ldots, q_m$ is a discrete state machine whose states are collections

$$(a_0, a_1, \ldots, a_{m-1}; z) \textit{ where } a_i \in S \textit{ and } z \in \mathbb{Z}$$

consisting of cell contents a_i and memory z. The state changes according to the following rules:

1. Compute
$$\sigma = \sum_{i=1}^{m} q_i a_{m-i} + z.$$
2. Find $a_m \in S$ such that $-q_0 a_m \equiv \sigma \pmod{p}$. That is $a_m \equiv -q_0^{-1}\sigma \pmod{p}$.
3. Replace $(a_0, \ldots, a_{m-1})$ by $(a_1, \ldots, a_m)$ and replace z by $\sigma(\text{div}p) = (\sigma + q_0 a_m)/p$.

References