The Diaconis Mind Reader

Mark Goresky, May 2008

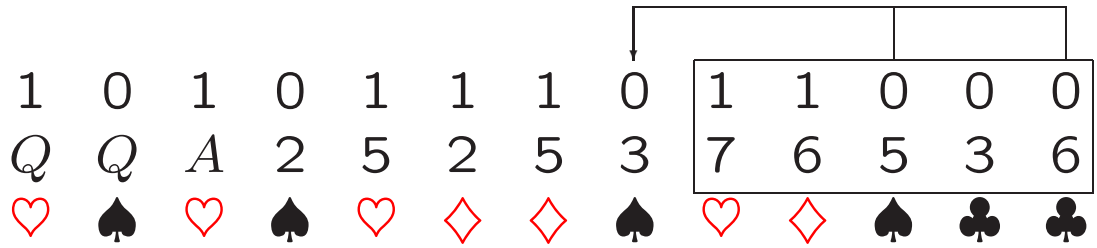
http://www.math.ias.edu/~goresky/preprints.html

00 = ♣, 01 = ♡, 10 = ♠, 11 = ♢.

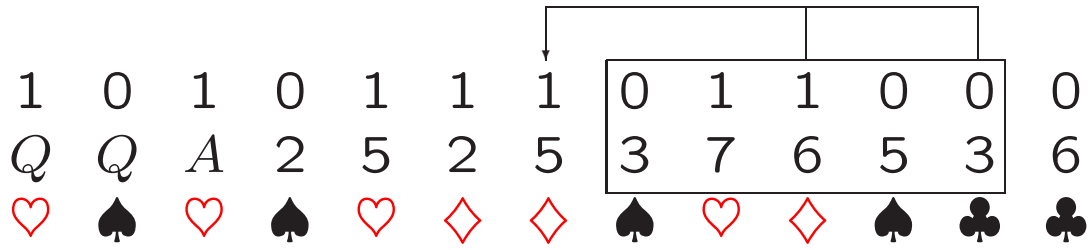
00 = ♣, 01 = ♡, 10 = ♠, 11 = ♢.

1	0	1	0	1	1	1	0	1	1	0	0	0
Q	Q	A	2	5	2	5	3	7	6	5	3	6
♡	♠	♡	♠	♡	♢	♢	♠	♡	♢	♠	♣	♣

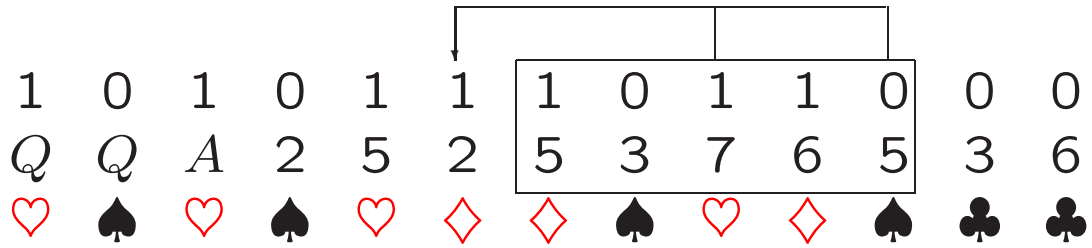
$00 = \clubsuit,\ 01 = \heartsuit,\ 10 = \spadesuit,\ 11 = \diamondsuit.$



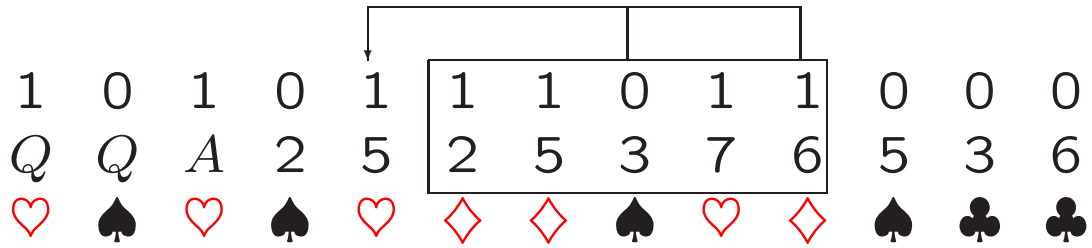
$00 = \clubsuit,\ 01 = \heartsuit,\ 10 = \spadesuit,\ 11 = \diamondsuit.$



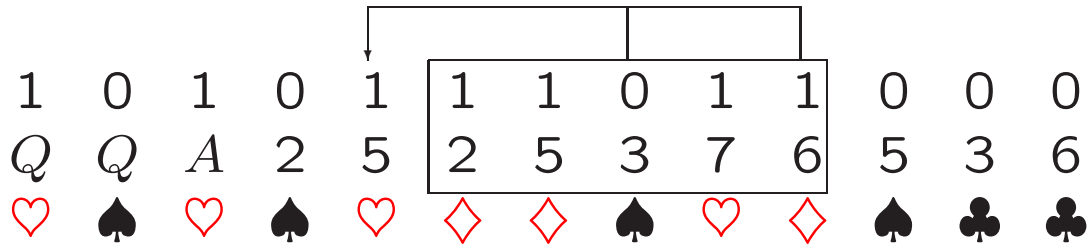
$00 = \clubsuit,\ 01 = \heartsuit,\ 10 = \spadesuit,\ 11 = \diamondsuit.$

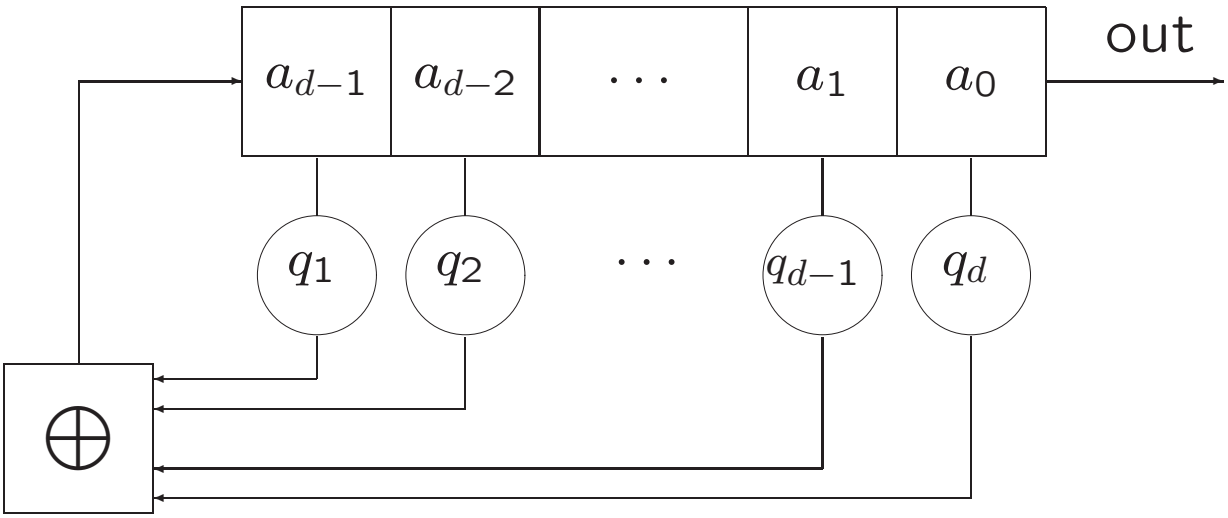


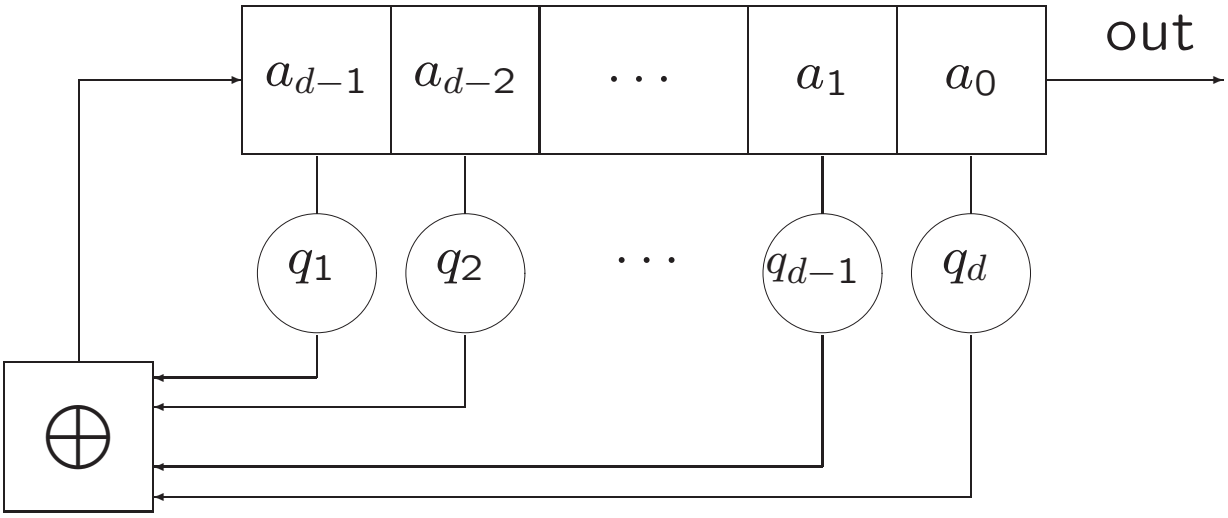
$00 = \clubsuit,\ 01 = \heartsuit,\ 10 = \spadesuit,\ 11 = \diamondsuit.$



$00 = \clubsuit$, $01 = \heartsuit$, $10 = \spadesuit$, $11 = \diamondsuit$.

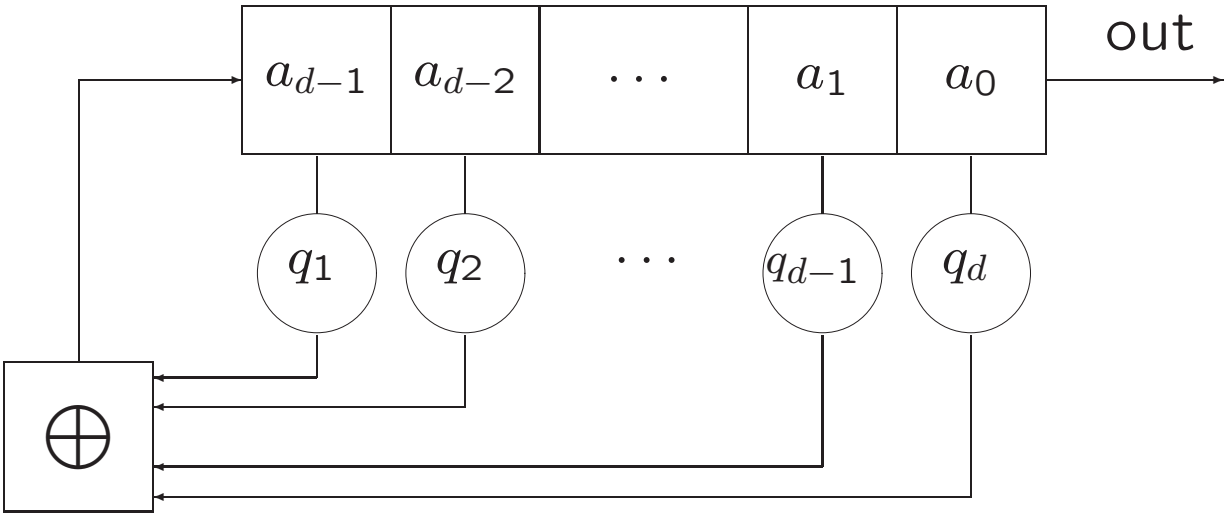






Connection polynomial:

$$q(x) = -1 + q_1 x + q_2 x^2 + \cdots + q_d x^d$$



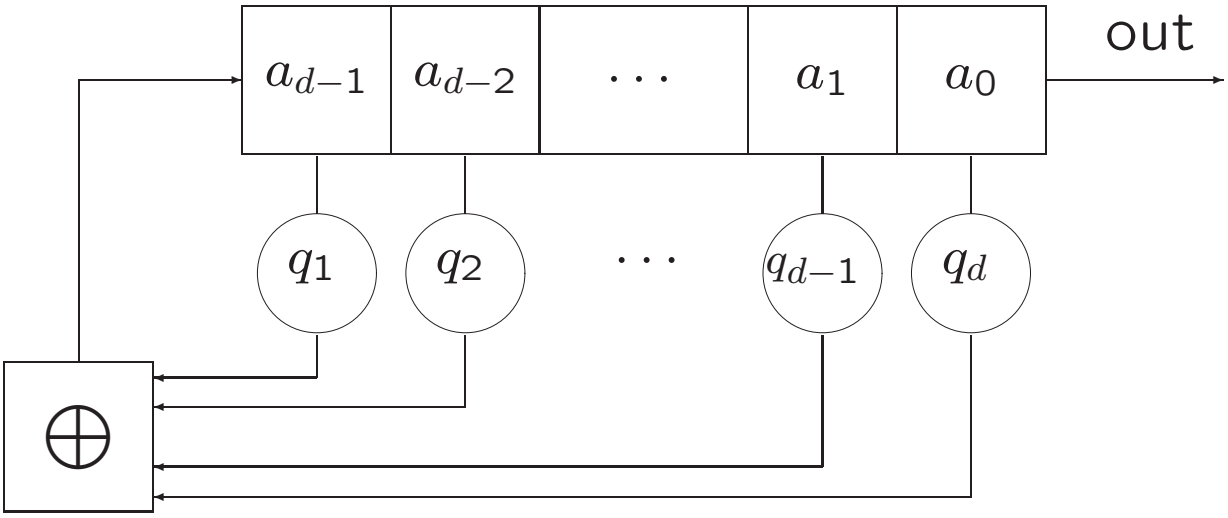
Connection polynomial:

$$q(x) = -1 + q_1 x + q_2 x^2 + \cdots + q_d x^d$$

"Initial" polynomial:

$$h(x) = \sum_{n=0}^{d-1} \left(\sum_{i=0}^{n} q_i a_{n-i} \right) x^n$$

$$\left\{ \begin{array}{c} \text{initial} \\ \text{loadings} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{polynomials of} \\ \text{degree} < d \end{array} \right\}$$



Connection polynomial:

$$q(x) = -1 + q_1 x + q_2 x^2 + \cdots + q_d x^d$$

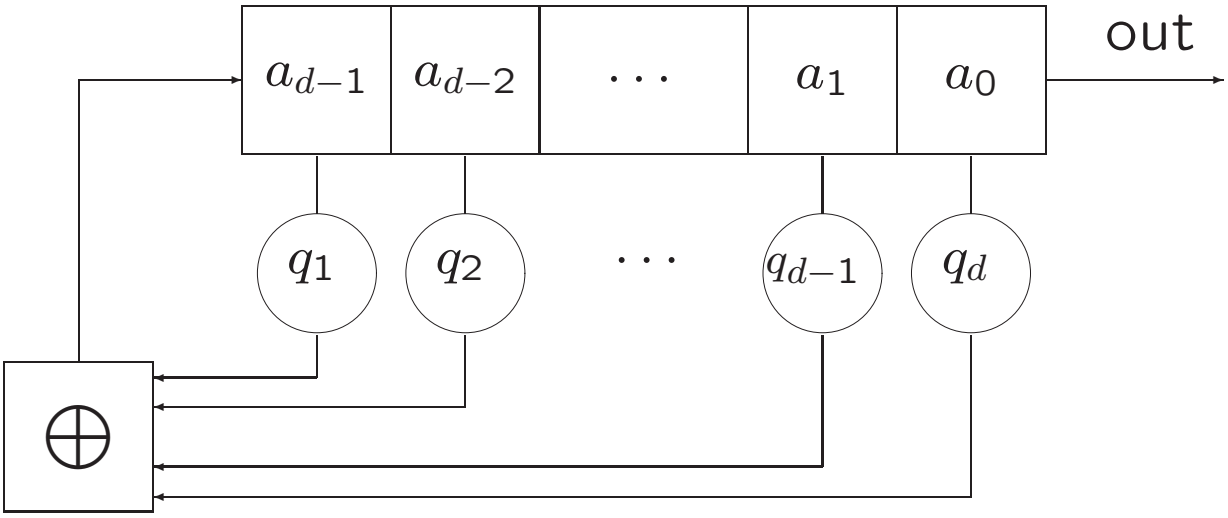
"Initial" polynomial:

$$h(x) = \sum_{n=0}^{d-1} \left(\sum_{i=0}^{n} q_i a_{n-i} \right) x^n$$

$$\left\{ \begin{array}{c} \text{initial} \\ \text{loadings} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{polynomials of} \\ \text{degree} < d \end{array} \right\}$$

Generating function of output sequence:

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$



Basic Fact

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \frac{h(x)}{q(x)}$$

1. $a(x) = h(x)/q(x)$.

1. $a(x) = h(x)/q(x)$.

2. The bit-wise sum of two periodic sequences $a_1(x)$ and $a_2(x)$ corresponds to

$$\frac{h_1(x)}{q_1(x)} + \frac{h_2(x)}{q_2(x)} = \frac{k(x)}{LCM(q_1, q_2)(x)}.$$

1. $a(x) = h(x)/q(x)$.

2. The bit-wise sum of two periodic sequences $a_1(x)$ and $a_2(x)$ corresponds to

$$\frac{h_1(x)}{q_1(x)} + \frac{h_2(x)}{q_2(x)} = \frac{k(x)}{LCM(q_1, q_2)(x)}.$$

3. Let $\alpha \in \mathbb{F}_{2^d}$ be a root of $q(x)$. Let

$$T : \mathbb{F}_{2^m} \to \mathbb{F}_2$$

be a linear surjective map. Then:

$$a_n = T(A\alpha^{-n})$$

for all $n \geq 0$. ($A \leftrightarrow$ initial loading)

1. $a(x) = h(x)/q(x)$.

2. The bit-wise sum of two periodic sequences $a_1(x)$ and $a_2(x)$ corresponds to

$$\frac{h_1(x)}{q_1(x)} + \frac{h_2(x)}{q_2(x)} = \frac{k(x)}{LCM(q_1, q_2)(x)}.$$

3. Let $\alpha \in \mathbb{F}_{2^d}$ be a root of $q(x)$. Let

$$T : \mathbb{F}_{2^m} \to \mathbb{F}_2$$

be a linear surjective map. Then:

$$a_n = T(A\alpha^{-n})$$

for all $n \geq 0$. ($A \leftrightarrow$ initial loading)

4. Maximal period ($= 2^d - 1$) occurs when $q(x)$ is a primitive polynomial ($\leftrightarrow \alpha$ is primitive).

1. $a(x) = h(x)/q(x)$.

2. The bit-wise sum of two periodic sequences $a_1(x)$ and $a_2(x)$ corresponds to

$$\frac{h_1(x)}{q_1(x)} + \frac{h_2(x)}{q_2(x)} = \frac{k(x)}{LCM(q_1, q_2)(x)}.$$

3. Let $\alpha \in \mathbb{F}_{2^d}$ be a root of $q(x)$. Let

$$T : \mathbb{F}_{2^m} \to \mathbb{F}_2$$

be a linear surjective map. Then:

$$a_n = T(A\alpha^{-n})$$

for all $n \geq 0$. ($A \leftrightarrow$ initial loading)

4. Maximal period ($= 2^d - 1$) occurs when $q(x)$ is a primitive polynomial ($\leftrightarrow \alpha$ is primitive).

5. The Massey-Berlekamp algorithm constructs the shift register for a given sequence

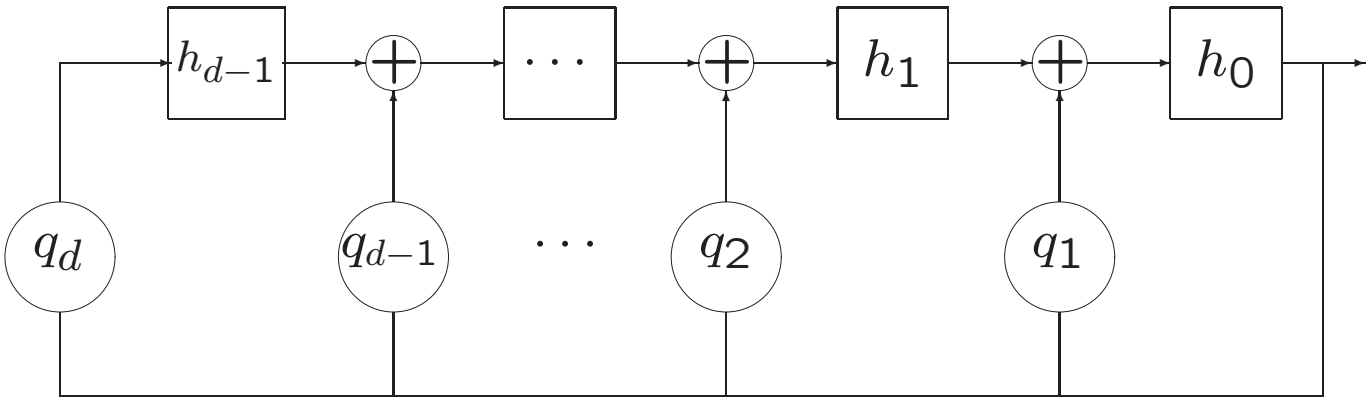
$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots .$$

Continued fraction expansion in $\mathbb{F}_2((x))$.

6. Similar results when cell contents in reasonable ring R.

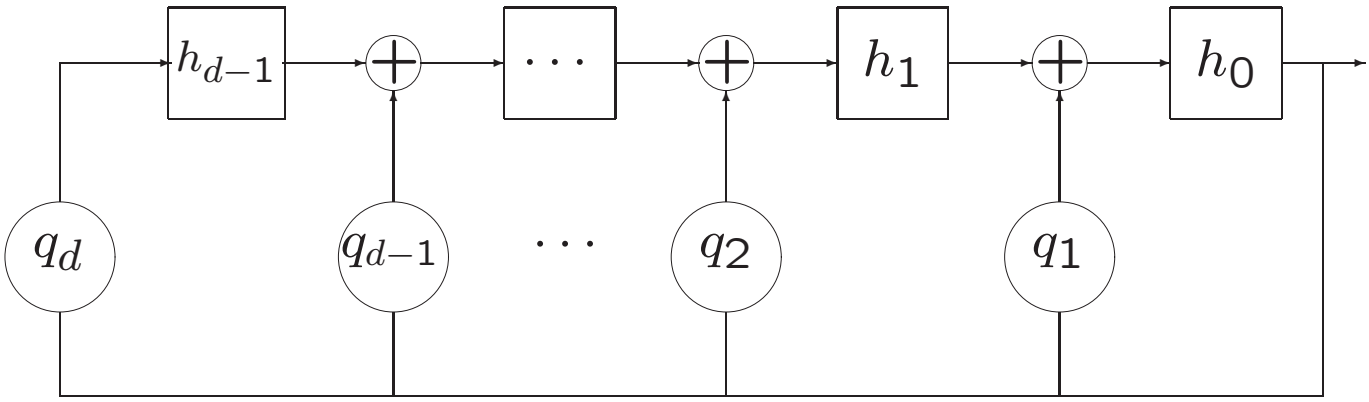
6. Similar results when cell contents in reasonable ring R.

7. Galois mode shift registers



6. Similar results when cell contents in reasonable ring R.

7. Galois mode shift registers

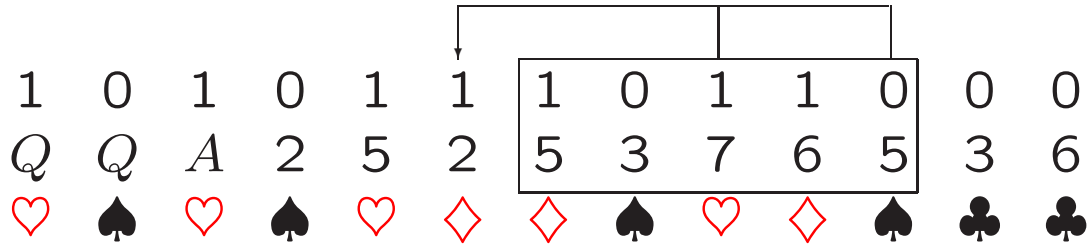


$$h(x) = h_0 + h_1 x + \cdots + h_{d-1} x^{d-1}$$
$$q(x) = -1 + q_1 x + \cdots + q_d x^d$$
$$a(x) = h(x)/q(x)$$

In summary, let

$$q(x) = -1 + x^3 + x^5$$

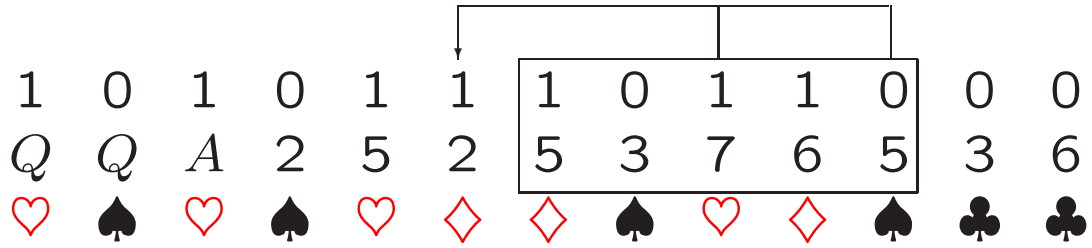
This is primitive. Use it for feedback taps.



In summary, let

$$q(x) = -1 + x^3 + x^5$$

This is primitive. Use it for feedback taps.

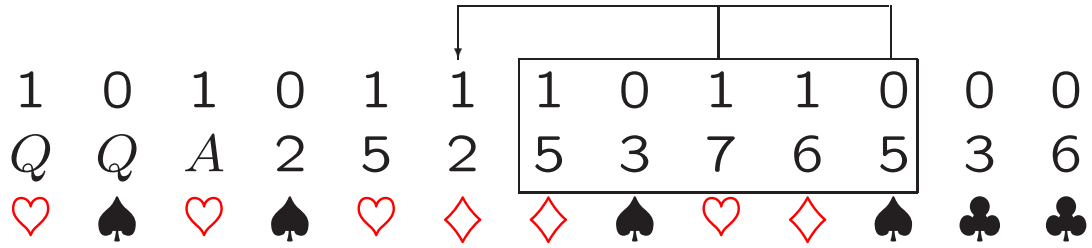


This generates an LFSR sequence of period 31

In summary, let

$$q(x) = -1 + x^3 + x^5$$

This is primitive. Use it for feedback taps.



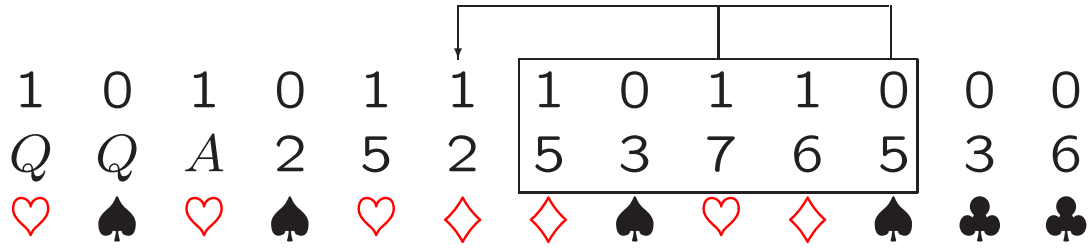
This generates an LFSR sequence of period 31

Good for magic

In summary, let

$$q(x) = -1 + x^3 + x^5$$

This is primitive. Use it for feedback taps.



This generates an LFSR sequence of period 31

Good for magic

Bad for cryptography

Summation combiner = sum-with-carry

$$
\begin{array}{cccccccccc}
1 & 1^{1} & 0^{1} & 0^{1} & 0 & 1 & 1^{1} & 0^{1} & 1^{1} & \cdots \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \cdots \\
\hline
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & \cdots
\end{array}
$$

Summation combiner = sum-with-carry

$$\begin{array}{cccccccccc} 1 & 1^{1} & 0^{1} & 0^{1} & 0 & 1 & 1^{1} & 0^{1} & 1^{1} & \cdots \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \cdots \\ \hline 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & \cdots \end{array}$$

$$a = a_0 2^0 + a_1 2^1 + a_2 2^2 + \cdots \in \mathbb{Z}_2$$

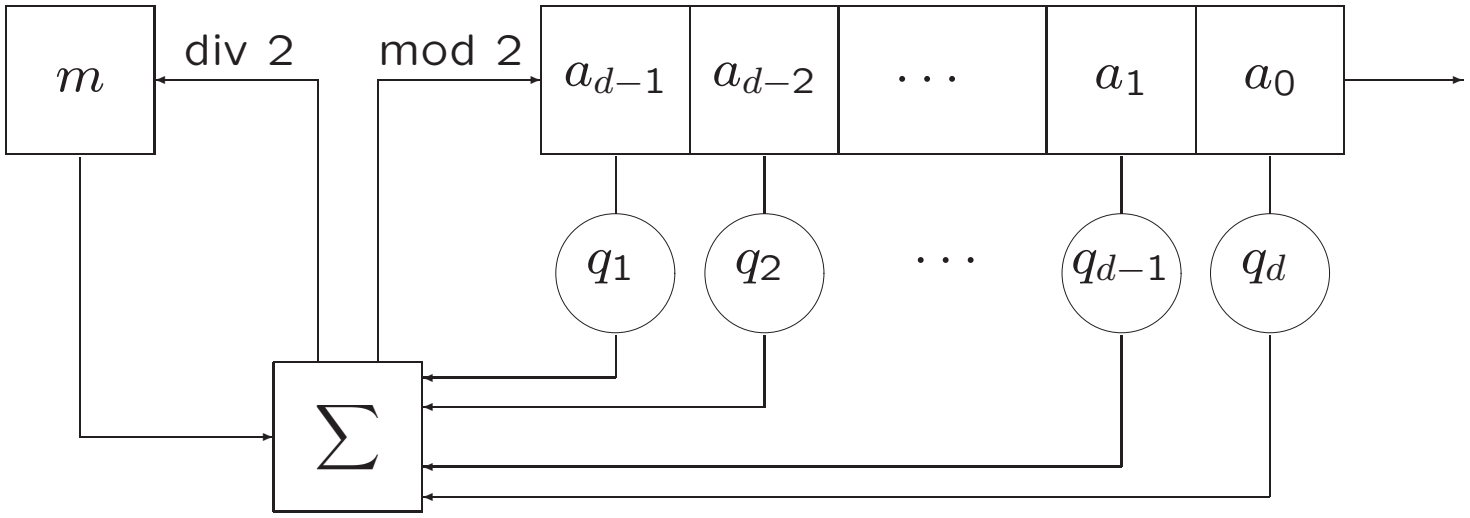
Summation combiner = sum-with-carry

$$
\begin{array}{l}
2^0+2^1+0\ +0\ +0\ +2^5+2^6+0\ +2^8+\cdots \\
2^0+0\ +2^2+0\ +2^4+2^5+0\ +2^7+2^8+\cdots \\
\hline
0\ +0\ +0\ +2^3+2^4+0\ +0\ +0\ +2^8+\cdots
\end{array}
$$

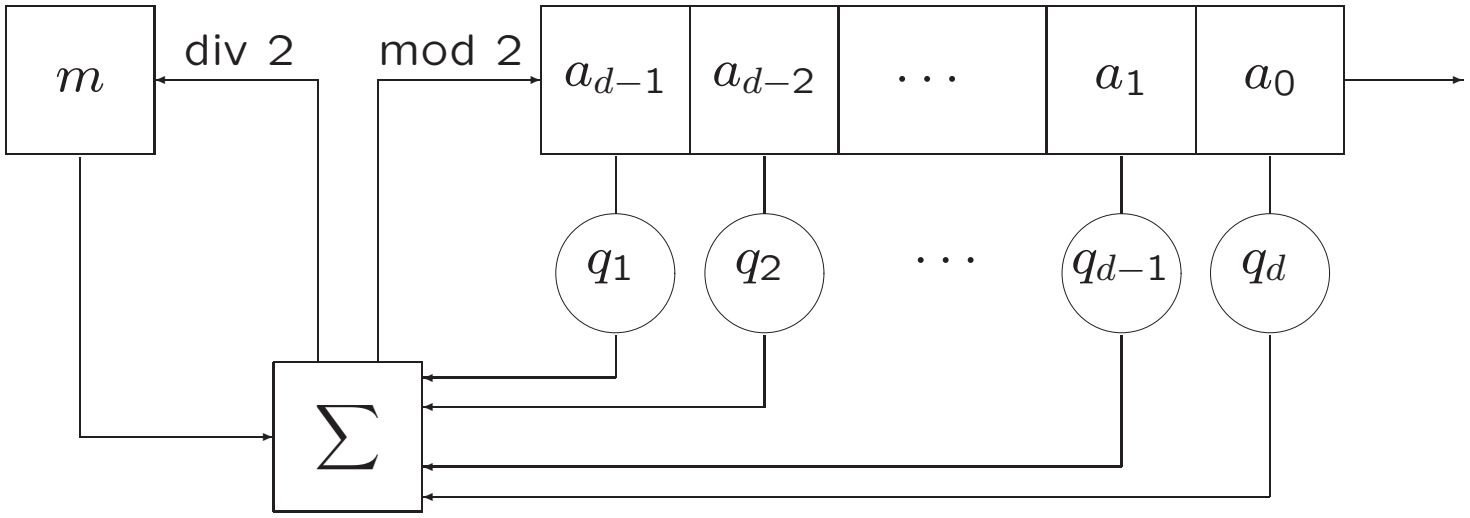
$$a = a_0 2^0 + a_1 2^1 + a_2 2^2 + \cdots \in \mathbb{Z}_2$$

From here on:

Joint work with Andy Klapper (U. Kentucky)



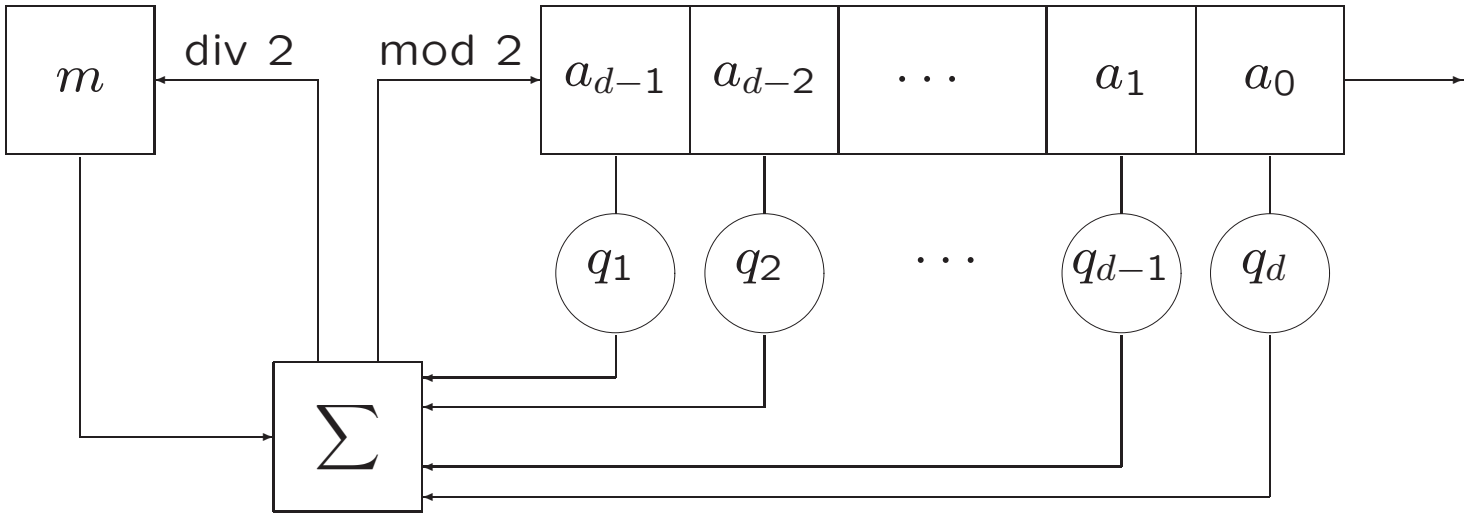
Feedback with carry shift register



Feedback with carry shift register

Connection integer:

$$q = -1 + q_1 2 + q_2 2^2 + \cdots + q_d 2^d$$



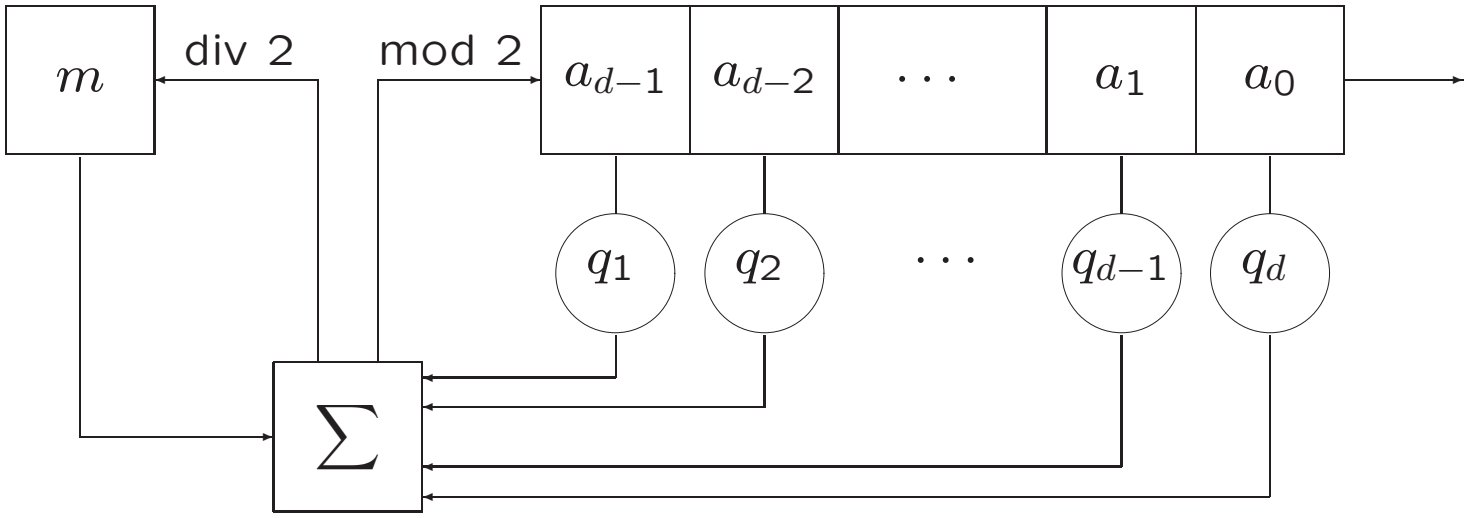
Feedback with carry shift register

Connection integer:

$$q = -1 + q_1 2 + q_2 2^2 + \cdots + q_d 2^d$$

"Initial" integer:

$$h = \sum_{n=0}^{d-1} \left(\sum_{i=0}^{n} q_i a_{n-i} \right) 2^n - m 2^d$$



Feedback with carry shift register

Connection integer:

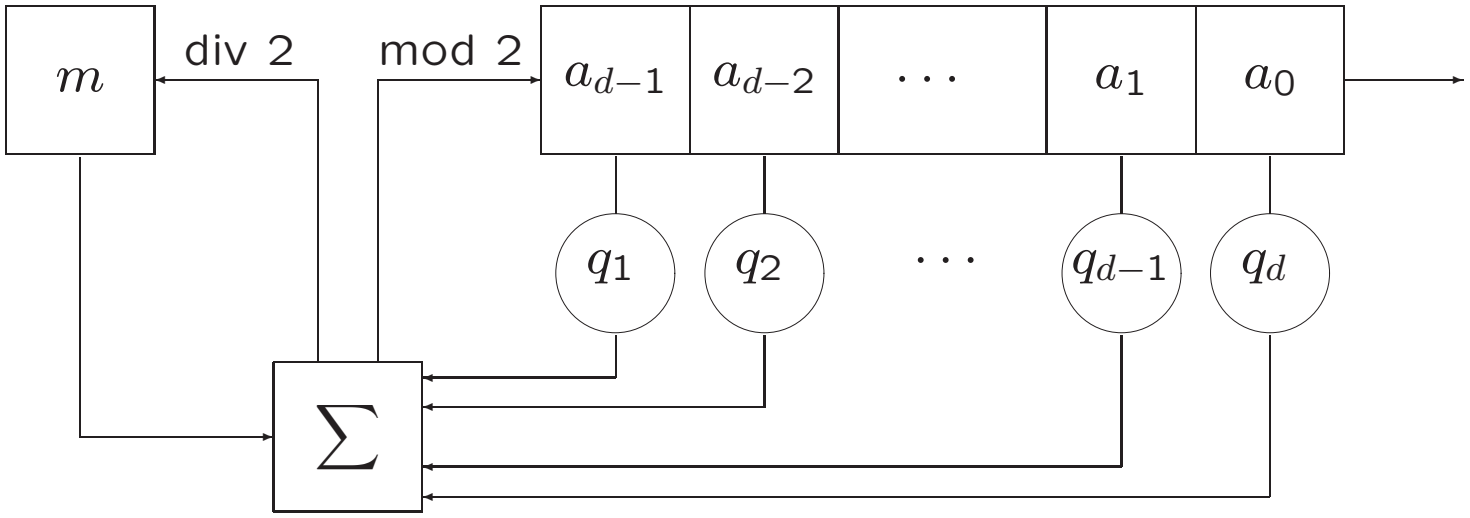
$$q = -1 + q_1 2 + q_2 2^2 + \cdots + q_d 2^d$$

"Initial" integer:

$$h = \sum_{n=0}^{d-1} \left(\sum_{i=0}^{n} q_i a_{n-i} \right) 2^n - m 2^d$$

Generating "series":

$$a = a_0 + a_1 2 + a_2 2^2 + \cdots$$



Feedback with carry shift register

Main fact:

$$\mathbf{a} = a_0 + a_1 2 + a_2 2^2 + \cdots = \frac{h}{q}$$

1. $a = h/q \in \mathbb{Z}_2$.

1. $a = h/q \in \mathbb{Z}_2$.

2. The sum-with-carry of two sequences a_1 and a_2 corresponds to

$$\frac{h_1}{q_1} + \frac{h_2}{q_2} = \frac{k}{LCM(q_1, q_2)}$$

1. $a = h/q \in \mathbb{Z}_2$.

2. The sum-with-carry of two sequences a_1 and a_2 corresponds to

$$\frac{h_1}{q_1} + \frac{h_2}{q_2} = \frac{k}{LCM(q_1, q_2)}$$

3. Let $(\mathrm{mod}\, 2) : \mathbb{Z}/(q) \to \mathbb{Z}/(2)$. Then

$$a_n = (A2^{-n}) \ (\mathrm{mod}\, q) \ (\mathrm{mod}\, 2).$$

($A \leftrightarrow$ initial loading)

1. $a = h/q \in \mathbb{Z}_2$.

2. The sum-with-carry of two sequences a_1 and a_2 corresponds to

$$\frac{h_1}{q_1} + \frac{h_2}{q_2} = \frac{k}{LCM(q_1, q_2)}$$

3. Let $(\mathrm{mod}\, 2) : \mathbb{Z}/(q) \to \mathbb{Z}/(2)$. Then

$$a_n = (A2^{-n}) \ (\mathrm{mod}\, q) \ (\mathrm{mod}\, 2).$$

($A \leftrightarrow$ initial loading)

4. Maximal period ($= q - 1$) occurs when 2 is a primitive root modulo q.

1. $a = h/q \in \mathbb{Z}_2$.

2. The sum-with-carry of two sequences a_1 and a_2 corresponds to

$$\frac{h_1}{q_1} + \frac{h_2}{q_2} = \frac{k}{LCM(q_1, q_2)}$$

3. Let $(\mathrm{mod}\, 2) : \mathbb{Z}/(q) \to \mathbb{Z}/(2)$. Then

$$a_n = (A2^{-n}) \ (\mathrm{mod}\, q) \ (\mathrm{mod}\, 2).$$

($A \leftrightarrow$ initial loading)

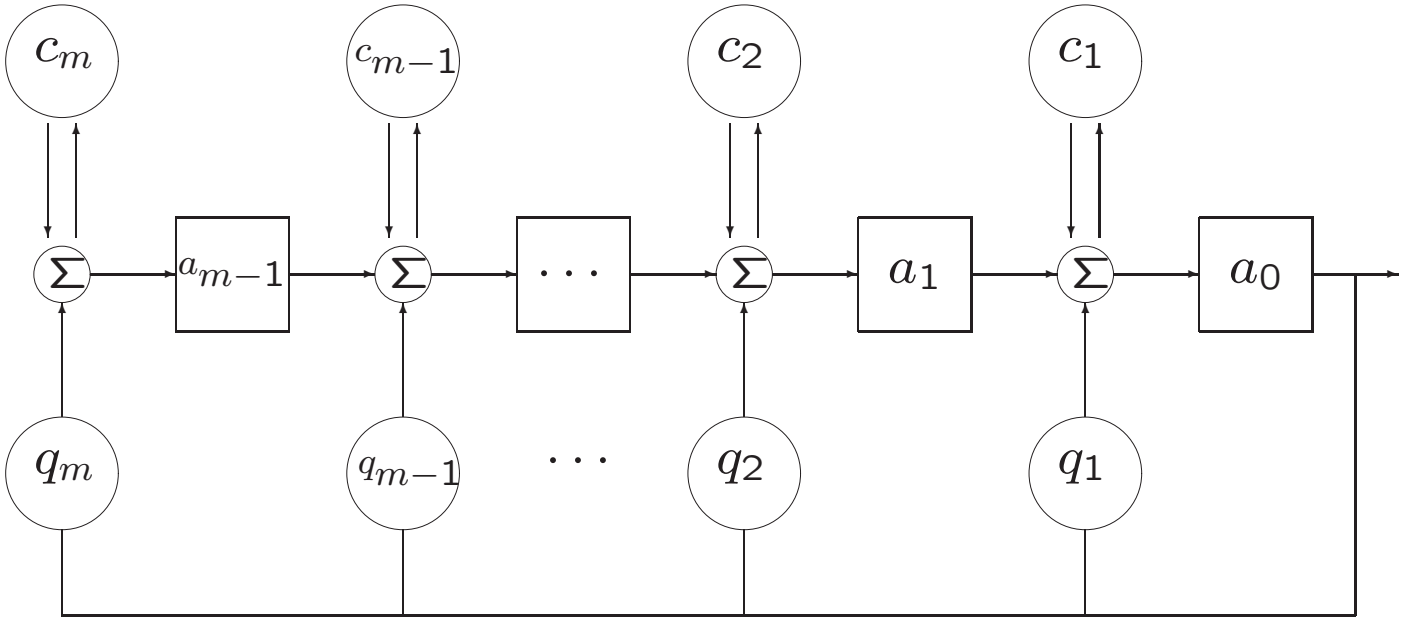
4. Maximal period ($= q - 1$) occurs when 2 is a primitive root modulo q.

5. Continued fraction expansion in $\mathbb{Z}_2$ does not converge, but (Mahler-deWeger) approximation lattices may be used to construct the FCSR for a given sequence.

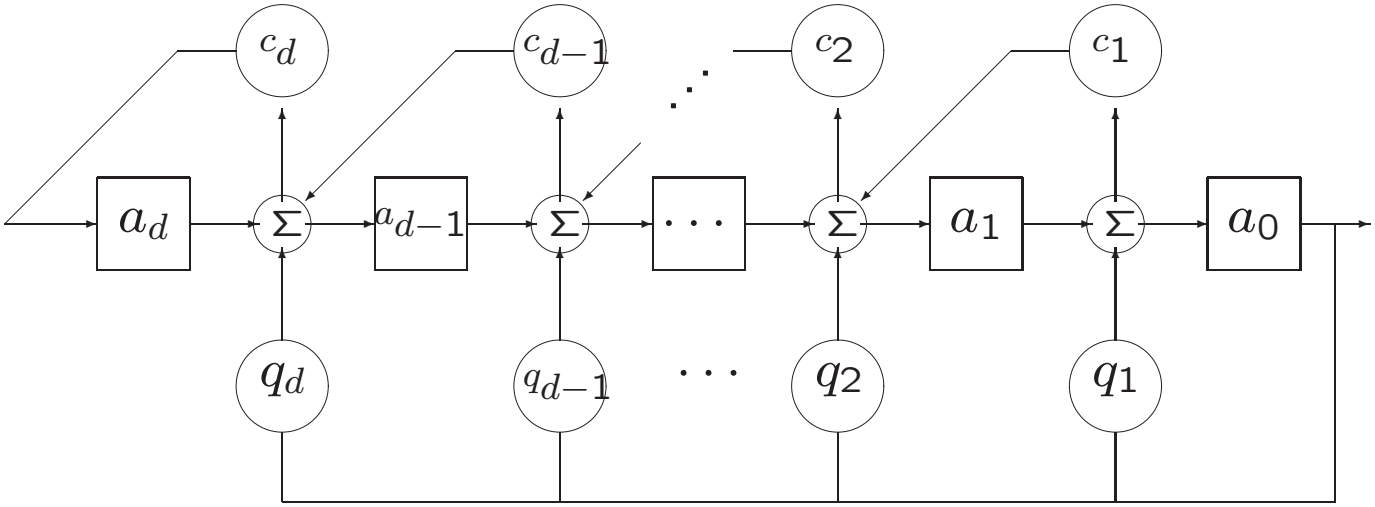
6. Similar results for cell contents in reasonable ring R.

6. Similar results for cell contents in reasonable ring R.

7. Galois mode FCSR



Many further variations, e.g. ramified extension of 2-adic numbers:



Amusing fact: a U.S. deck has 52 cards.
53 is prime and 2 is primitive mod 53.

Amusing fact: a U.S. deck has 52 cards.
53 is prime and 2 is primitive mod 53.

So it is possible to carry out the Diaconis mind-dreader, using a full deck of 52 cards, with the FCSR sequence for

$$q = 53 = -1 + 2 + 4 + 16 + 32.$$