Arithmetic Correlations

Mark Goresky* and Andrew Klapper†

*partially supported by DARPA grant HR0011-04-1-0031

†partially supported by NSF grant CCF-0514660

Arithmetic Correlations

Mark Goresky* and Andrew Klapper†

*partially supported by DARPA grant HR0011-04-1-0031

†partially supported by NSF grant CCF-0514660

Let $\mathbf{c} = c_0, c_1, c_2, \cdots \quad c_i \in \mathbb{Z}/(p) \quad (p$ prime) eventually periodic sequence of period T.

Let $\mathbf{c} = c_0, c_1, c_2, \cdots \quad c_i \in \mathbb{Z}/(p) \quad (p \text{ prime})$ eventually periodic sequence of period T.

Let $\zeta = e^{2\pi i/p}$.

The *Imbalance* is the sum over one period,

$$Z(\mathbf{c}) = \sum_k \zeta^{c_k} = \sum_k e^{2\pi i c_k/p}$$

Let $\mathbf{c} = c_0, c_1, c_2, \cdots \quad c_i \in \mathbb{Z}/(p) \quad (p \text{ prime})$ eventually periodic sequence of period T.

Let $\zeta = e^{2\pi i/p}$.

The *Imbalance* is the sum over one period,

$$Z(\mathbf{c}) = \sum_k \zeta^{c_k} = \sum_k e^{2\pi i c_k/p}$$

Given two sequences of period T
$\mathbf{a} = a_0, a_1, \cdots, \quad \mathbf{b} = b_0, b_1, \cdots \quad a_i, b_i \in \mathbb{Z}/(p)$

Let $\mathbf{c} = c_0, c_1, c_2, \cdots \quad c_i \in \mathbb{Z}/(p) \quad (p \text{ prime})$ eventually periodic sequence of period T.

Let $\zeta = e^{2\pi i/p}$.

The *Imbalance* is the sum over one period,

$$Z(\mathbf{c}) = \sum_k \zeta^{c_k} = \sum_k e^{2\pi i c_k/p}$$

Given two sequences of period T
$\mathbf{a} = a_0, a_1, \cdots, \quad \mathbf{b} = b_0, b_1, \cdots \quad a_i, b_i \in \mathbb{Z}/(p)$

Their cross-correlation with shift τ is

$$\mathcal{C}_\tau(\mathbf{a}, \mathbf{b}) = \sum_{k=0}^{T-1} \zeta^{a_k} \zeta^{-b_{k+\tau}} = \sum_{k=0}^{T-1} \zeta^{a_k - b_{k+\tau}}$$

$$= Z(\mathbf{a} - \mathbf{b}^\tau)$$

where $\mathbf{b}^\tau = b_\tau, b_{\tau+1}, \cdots$ is the τ-shift of $\mathbf{b}$.

Let $\mathbf{c} = c_0, c_1, c_2, \cdots \quad c_i \in \mathbb{Z}/(p) \quad (p \text{ prime})$ eventually periodic sequence of period T.

Let $\zeta = e^{2\pi i/p}$.

The *Imbalance* is the sum over one period,

$$Z(\mathbf{c}) = \sum_k \zeta^{c_k} = \sum_k e^{2\pi i c_k/p}$$

Given two sequences of period T
$\mathbf{a} = a_0, a_1, \cdots, \quad \mathbf{b} = b_0, b_1, \cdots \quad a_i, b_i \in \mathbb{Z}/(p)$

Their cross-correlation with shift τ is

$$\mathcal{C}_\tau(\mathbf{a}, \mathbf{b}) = \sum_{k=0}^{T-1} \zeta^{a_k} \zeta^{-b_{k+\tau}} = \sum_{k=0}^{T-1} \zeta^{a_k - b_{k+\tau}}$$

$$= Z(\mathbf{a} - \mathbf{b}^\tau)$$

where $\mathbf{b}^\tau = b_\tau, b_{\tau+1}, \cdots$ is the τ-shift of $\mathbf{b}$.

There is another way to say this:

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \qquad \in \mathbb{Z}(p)[[x]]$$
$$b^\tau(x) = b_\tau + b_{\tau+1} x + b_{\tau+2} x^2 + \cdots \qquad \in \mathbb{Z}(p)[[x]]$$

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \qquad \in \mathbb{Z}(p)[[x]]$$
$$b^\tau(x) = b_\tau + b_{\tau+1} x + b_{\tau+2} x^2 + \cdots \qquad \in \mathbb{Z}(p)[[x]]$$

Then $\mathbf{a} - \mathbf{b}^\tau$ is the coefficient sequence of
$c(x) = a(x) - b^\tau(x) \qquad \in \mathbb{Z}/(p)[[x]]$

so: $\mathcal{C}_\tau(\mathbf{a}, \mathbf{b}) = Z(c) = \sum_{k=0}^{T-1} \zeta^{c_k} = \sum_{k=N}^{N+T-1} \zeta^{c_k}.$

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \qquad \in \mathbb{Z}(p)[[x]]$$
$$b^\tau(x) = b_\tau + b_{\tau+1} x + b_{\tau+2} x^2 + \cdots \qquad \in \mathbb{Z}(p)[[x]]$$

Then $\mathbf{a} - \mathbf{b}^\tau$ is the coefficient sequence of
$c(x) = a(x) - b^\tau(x) \qquad \in \mathbb{Z}/(p)[[x]]$

so: $\mathcal{C}_\tau(\mathbf{a}, \mathbf{b}) = Z(c) = \sum_{k=0}^{T-1} \zeta^{c_k} = \sum_{k=N}^{N+T-1} \zeta^{c_k}.$

Arithmetic analog:

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \qquad \in \mathbb{Z}_p.$$
$$\beta^\tau = b_\tau + b_{\tau+1} p + b_{\tau+2} p^2 + \cdots \qquad \in \mathbb{Z}_p.$$

$$\gamma = \alpha - \beta^\tau = \gamma_0 + \gamma_1 p + \gamma_2 p^2 + \cdots \qquad \in \mathbb{Z}_p.$$

Note: $\gamma = \alpha - \beta^\tau$ is *eventually* periodic.

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \qquad \in \mathbb{Z}(p)[[x]]$$
$$b^\tau(x) = b_\tau + b_{\tau+1} x + b_{\tau+2} x^2 + \cdots \qquad \in \mathbb{Z}(p)[[x]]$$

Then $\mathbf{a} - \mathbf{b}^\tau$ is the coefficient sequence of
$c(x) = a(x) - b^\tau(x) \qquad \in \mathbb{Z}/(p)[[x]]$

so: $\mathcal{C}_\tau(\mathbf{a}, \mathbf{b}) = Z(c) = \sum_{k=0}^{T-1} \zeta^{c_k} = \sum_{k=N}^{N+T-1} \zeta^{c_k}.$

Arithmetic analog:

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \qquad \in \mathbb{Z}_p.$$
$$\beta^\tau = b_\tau + b_{\tau+1} p + b_{\tau+2} p^2 + \cdots \qquad \in \mathbb{Z}_p.$$

$$\gamma = \alpha - \beta^\tau = \gamma_0 + \gamma_1 p + \gamma_2 p^2 + \cdots \qquad \in \mathbb{Z}_p.$$

Note: $\gamma = \alpha - \beta^\tau$ is *eventually* periodic.

Set $\mathcal{C}_\tau^{arith}(\mathbf{a}, \mathbf{b}) = Z(\gamma) = \sum_{k=N}^{N+T-1} \zeta^{\gamma_k}.$
(sum over periodic part)

- Averaged over all pairs of sequences,

$$E(\mathcal{C}_\tau(\mathbf{a},\mathbf{b})) = \begin{cases} T & (\mathbf{a}=\mathbf{b} \text{ and } \tau = 0) \\ 0 & (\mathbf{a}\neq\mathbf{b} \text{ or } \tau \neq 0) \end{cases}$$

- Averaged over all pairs of sequences,

$$E(\mathcal{C}_\tau(\mathbf{a},\mathbf{b})) = \begin{cases} T & (\mathbf{a}=\mathbf{b} \text{ and } \tau = 0) \\ 0 & (\mathbf{a}\neq\mathbf{b} \text{ or } \tau \neq 0) \end{cases}$$

- RMS cross-correlation is

$$\sqrt{E(\mathcal{C}_\tau(\mathbf{a},\mathbf{b})^2)} = \begin{cases} \mathrm{T} & (\mathbf{a}=\mathbf{b} \text{ and } \tau = 0) \\ \sqrt{2T} & (\mathbf{a}=\mathbf{b}, \tau \neq 0, p = 2) \\ \sqrt{T} & (\text{otherwise}) \end{cases}$$

- Averaged over all pairs of sequences,

$$E(\mathcal{C}_\tau(\mathbf{a},\mathbf{b})) = \begin{cases} T & (\mathbf{a}=\mathbf{b} \text{ and } \tau = 0) \\ 0 & (\mathbf{a}\neq\mathbf{b} \text{ or } \tau \neq 0) \end{cases}$$

- RMS cross-correlation is

$$\sqrt{E(\mathcal{C}_\tau(\mathbf{a},\mathbf{b})^2)} = \begin{cases} \mathsf{T} & (\mathbf{a}=\mathbf{b} \text{ and } \tau = 0) \\ \sqrt{2T} & (\mathbf{a}=\mathbf{b}, \tau \neq 0, p=2) \\ \sqrt{T} & (\text{otherwise}) \end{cases}$$

- Average Arithmetic cross-correlation is:

$$E(\mathcal{C}_\tau^{arith}(\mathbf{a},\mathbf{b})) = \begin{cases} T & (\mathbf{a}=\mathbf{b}, \tau = 0) \\ T/p^{T-\mathsf{gcd}(\tau,T)} & (\mathbf{a}=\mathbf{b}, \tau \neq 0) \\ T/p^T & (\text{otherwise}) \end{cases}$$

- Averaged over all pairs of sequences,

$$E(\mathcal{C}_\tau(\mathbf{a},\mathbf{b})) = \begin{cases} T & (\mathbf{a}=\mathbf{b} \text{ and } \tau=0) \\ 0 & (\mathbf{a}\neq\mathbf{b} \text{ or } \tau\neq 0) \end{cases}$$

- RMS cross-correlation is

$$\sqrt{E(\mathcal{C}_\tau(\mathbf{a},\mathbf{b})^2)} = \begin{cases} \mathsf{T} & (\mathbf{a}=\mathbf{b} \text{ and } \tau=0) \\ \sqrt{2T} & (\mathbf{a}=\mathbf{b}, \tau\neq 0, p=2) \\ \sqrt{T} & (\text{otherwise}) \end{cases}$$

- Average Arithmetic cross-correlation is:

$$E(\mathcal{C}_\tau^{arith}(\mathbf{a},\mathbf{b})) = \begin{cases} T & (\mathbf{a}=\mathbf{b}, \tau=0) \\ T/p^{T-\mathsf{gcd}(\tau,T)} & (\mathbf{a}=\mathbf{b}, \tau\neq 0) \\ T/p^T & (\text{otherwise}) \end{cases}$$

- RMS Arithmetic cross-correlation is:

$$\sqrt{E(\mathcal{C}_\tau^{arith}(\mathbf{a},\mathbf{b})^2)} = \begin{cases} T & (\mathbf{a}=\mathbf{b}, \tau=0) \\ \sqrt{2T}e_1 & (\mathbf{a}=\mathbf{b}, \tau\neq 0, p=2) \\ \sqrt{T}e_2 & (\mathbf{a}=\mathbf{b}, \tau\neq 0, p>2) \\ \sqrt{T}e_3 & (\mathbf{a}\neq\mathbf{b}) \end{cases}$$

$(e_1, e_2, e_3 \sim 1)$

m-sequences

Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in \mathbb{Z}/(p)[[x]]$.

m-sequences

Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in \mathbb{Z}/(p)[[x]]$.

Reduce to lowest terms:

$$a(x) = \frac{a_0 + a_1 x + \cdots + a_{T-1} x^{T-1}}{1 - x^T} = \frac{-h(x)}{q(x)}$$

m-sequences

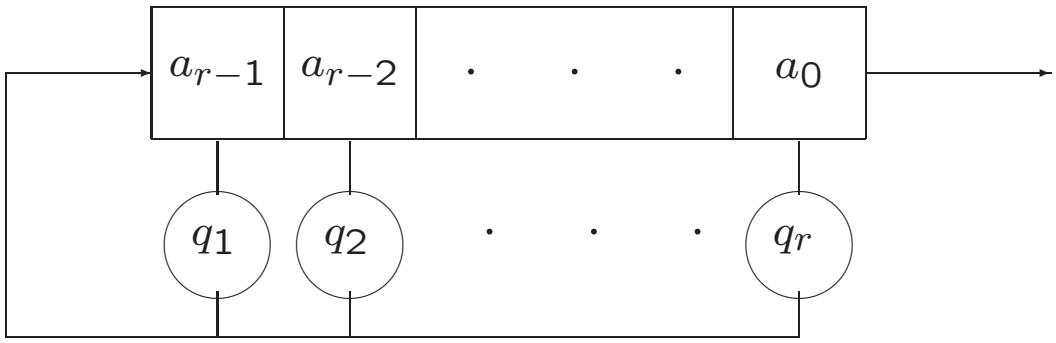
Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in \mathbb{Z}/(p)[[x]]$.

Reduce to lowest terms:

$$a(x) = \frac{a_0 + a_1 x + \cdots + a_{T-1} x^{T-1}}{1 - x^T} = \frac{-h(x)}{q(x)}$$

- $q(x) = -1 + q_1 x + \cdots + q_r x^r$
  is the connection polynomial of a LFSR
  that generates the sequence $\mathbf{a}$.



m-sequences

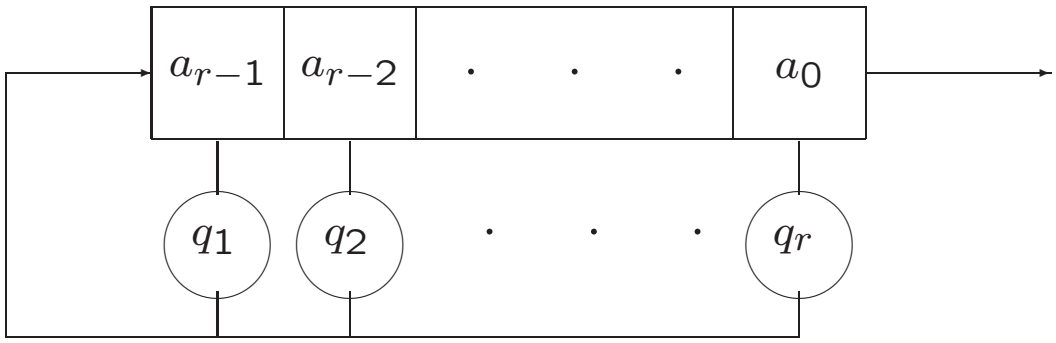
Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \in \mathbb{Z}/(p)[[x]]$.

Reduce to lowest terms:

$$a(x) = \frac{a_0 + a_1 x + \cdots + a_{T-1} x^{T-1}}{1 - x^T} = \frac{-h(x)}{q(x)}$$

- $q(x) = -1 + q_1 x + \cdots + q_r x^r$
  is the connection polynomial of a LFSR
  that generates the sequence $\mathbf{a}$.



- **m-sequence** $\Leftrightarrow$ $q(x)$ is a primitive polynomial

ℓ-sequences

Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$.

ℓ-sequences

Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$.

Reduce to lowest terms:

$$\alpha = \frac{a_0 + a_1 p + \cdots + a_{T-1} p^{T-1}}{1 - p^T} = \frac{-h}{q}$$

ℓ-sequences

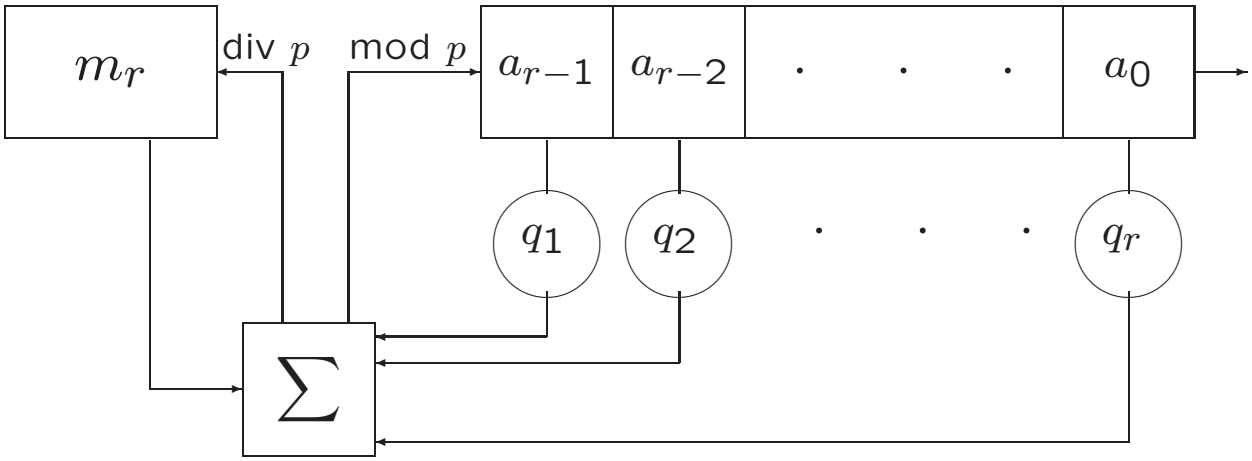
Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$.

Reduce to lowest terms:

$$\alpha = \frac{a_0 + a_1 p + \cdots + a_{T-1} p^{T-1}}{1 - p^T} = \frac{-h}{q}$$

- $q = -1 + q_1 p + \cdots + q_r p^r \quad \in \mathbb{Z}$
  is the connection integer of an FCSR
  that generates the sequence $\mathbf{a}$.



ℓ-sequences

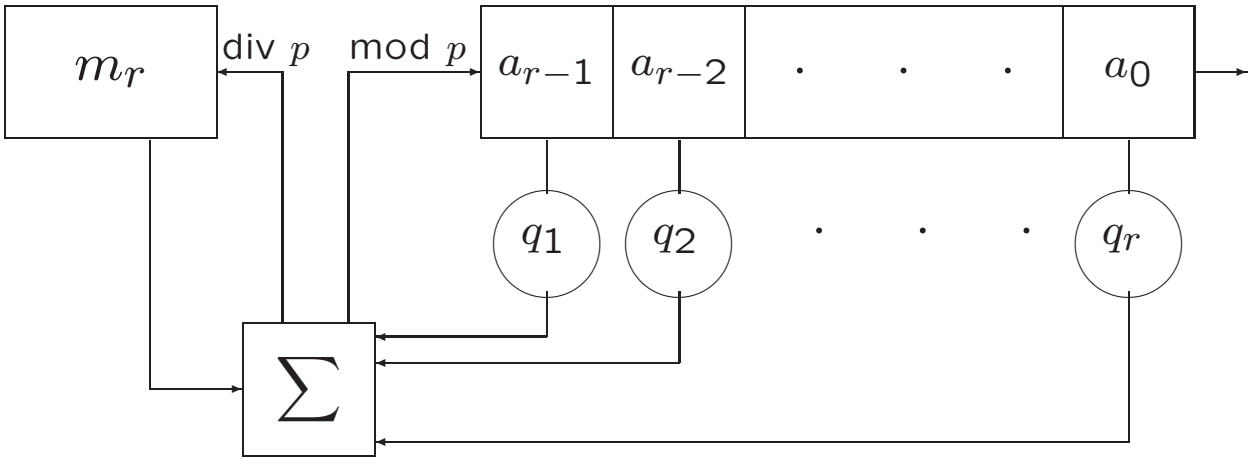
Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$.

Reduce to lowest terms:

$$\alpha = \frac{a_0 + a_1 p + \cdots + a_{T-1} p^{T-1}}{1 - p^T} = \frac{-h}{q}$$

- $q = -1 + q_1 p + \cdots + q_r p^r \quad \in \mathbb{Z}$
  is the connection integer of an FCSR
  that generates the sequence $\mathbf{a}$.



- $h < q$ and $h \leftrightarrow$ initial loading

ℓ-sequences

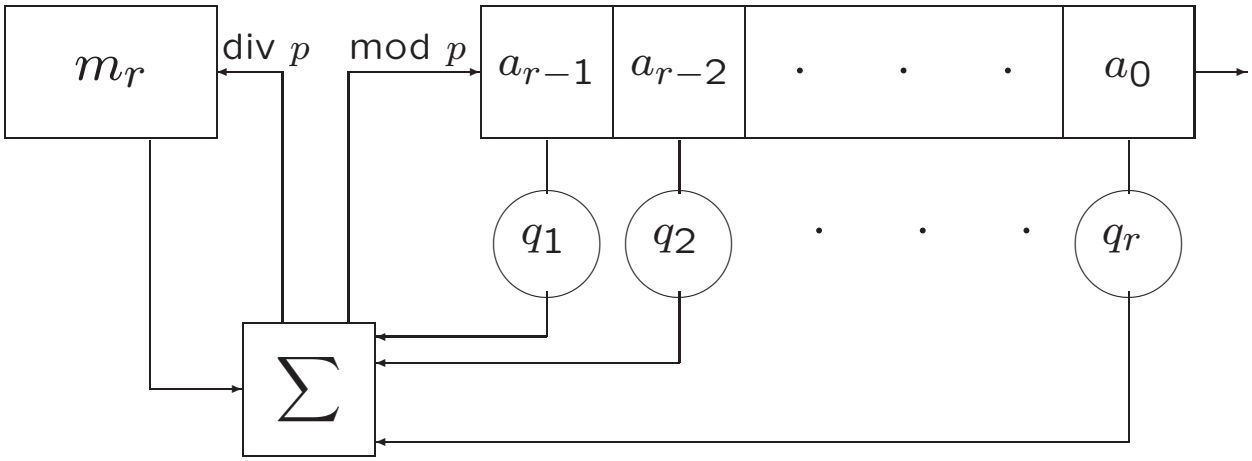
Let $\mathbf{a} = a_0, a_1, a_2, \cdots$ be T-periodic, $\quad a_i \in \mathbb{Z}/(p)$.

Set $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$.

Reduce to lowest terms:

$$\alpha = \frac{a_0 + a_1 p + \cdots + a_{T-1} p^{T-1}}{1 - p^T} = \frac{-h}{q}$$

- $q = -1 + q_1 p + \cdots + q_r p^r \quad \in \mathbb{Z}$
  is the connection integer of an FCSR
  that generates the sequence $\mathbf{a}$.



- $h < q$ and $h \leftrightarrow$ initial loading

- ℓ-**sequence** $\Leftrightarrow$ p is a primitive root modulo q.

Shift and add sequences

Let $\mathbf{a} = a_0, a_1, \cdots$ be T-periodic. $(a_i \in \mathbb{Z}/(p))$

It is a **shift and add sequence** if for any shift τ,

$$\mathbf{a} + \mathbf{a}^{\tau} = \begin{cases} \mathbf{a}^{\tau'} & \text{some shift } \tau', \text{ or} \\ 0 \end{cases}$$

Shift and add sequences

Let $\mathbf{a} = a_0, a_1, \cdots$ be T-periodic. $(a_i \in \mathbb{Z}/(p))$
It is a **shift and add sequence** if for any shift τ,

$$\mathbf{a} + \mathbf{a}^\tau = \begin{cases} \mathbf{a}^{\tau'} & \text{some shift } \tau', \text{ or} \\ 0 \end{cases}$$

Theorem. *(Zierler) The sequence* $\mathbf{a}$ *is a shift and add sequence if and only if it is an m-sequence.*

Shift and add sequences

Let $\mathbf{a} = a_0, a_1, \cdots$ be T-periodic. $(a_i \in \mathbb{Z}/(p))$
It is a **shift and add sequence** if for any shift τ,

$$\mathbf{a} + \mathbf{a}^\tau = \begin{cases} \mathbf{a}^{\tau'} & \text{some shift } \tau', \text{ or} \\ 0 \end{cases}$$

Theorem. *(Zierler) The sequence* $\mathbf{a}$ *is a shift and add sequence if and only if it is an m-sequence.*

Arithmetic shift and add

(Shift and add with carry)

Shift and add sequences

Let $\mathbf{a} = a_0, a_1, \cdots$ be T-periodic. $(a_i \in \mathbb{Z}/(p))$
It is a **shift and add sequence** if for any shift τ,

$$\mathbf{a} + \mathbf{a}^\tau = \begin{cases} \mathbf{a}^{\tau'} & \text{some shift } \tau', \text{ or} \\ 0 \end{cases}$$

Theorem. *(Zierler) The sequence* $\mathbf{a}$ *is a shift and add sequence if and only if it is an m-sequence.*

Arithmetic shift and add

(Shift and add with carry)

Let $\mathbf{a} = a_0, a_1, \cdots$ be T-periodic $(a_i \in \mathbb{Z}/(p))$
It is an **arithmetic shift and add** sequence if, $\forall \tau$,

$$\text{periodic part of } (\alpha + \alpha^\tau) = \text{shift of } \alpha$$

where $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$.

Shift and add sequences

Let $\mathbf{a} = a_0, a_1, \cdots$ be T-periodic. $(a_i \in \mathbb{Z}/(p))$
It is a **shift and add sequence** if for any shift τ,

$$\mathbf{a} + \mathbf{a}^\tau = \begin{cases} \mathbf{a}^{\tau'} & \text{some shift } \tau', \text{ or} \\ 0 \end{cases}$$

Theorem. *(Zierler) The sequence* $\mathbf{a}$ *is a shift and add sequence if and only if it is an m-sequence.*

Arithmetic shift and add

(Shift and add with carry)

Let $\mathbf{a} = a_0, a_1, \cdots$ be T-periodic $(a_i \in \mathbb{Z}/(p))$
It is an **arithmetic shift and add** sequence if, $\forall \tau$,

$$\text{periodic part of } (\alpha + \alpha^\tau) = \text{shift of } \alpha$$

where $\alpha = a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p$.

Theorem. *The sequence* $\mathbf{a}$ *is an arithmetic shift and add sequence if and only if it is an* ℓ*-sequence.*

Summary of properties

m-sequence	ℓ-sequence

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry
Period:	
$T = p^r - 1$	$T = q - 1$

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry
Period:	
$T = p^r - 1$	$T = q - 1$
Connection element:	
polynomial $q(x)$	integer q

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry
Period:	
$T = p^r - 1$	$T = q - 1$
Connection element:	
polynomial $q(x)$	integer q
Primitive element:	
$\alpha \in \mathbb{F}_{p^r}$ root	$p \in \mathbb{Z}/(q)$

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry
Period:	
$T = p^r - 1$	$T = q - 1$
Connection element:	
polynomial $q(x)$	integer q
Primitive element:	
$\alpha \in \mathbb{F}_{p^r}$ root	$p \in \mathbb{Z}/(q)$
Reduction mapping:	
$\mathbb{F}_{p^r} \stackrel{Tr}{\rightarrow} \mathbb{F}_p$	$\mathbb{Z}/(q) \stackrel{mod}{\rightarrow} \mathbb{F}_p$

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry
Period:	
$T = p^r - 1$	$T = q - 1$
Connection element:	
polynomial $q(x)$	integer q
Primitive element:	
$\alpha \in \mathbb{F}_{p^r}$ root	$p \in \mathbb{Z}/(q)$
Reduction mapping:	
$\mathbb{F}_{p^r} \stackrel{Tr}{\rightarrow} \mathbb{F}_p$	$\mathbb{Z}/(q) \stackrel{mod}{\rightarrow} \mathbb{F}_p$
Output sequence:	
$a_n = Tr(\alpha^n)$	$a_n = p^{-n} \pmod{q} \pmod{p}$

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry
Period:	
$T = p^r - 1$	$T = q - 1$
Connection element:	
polynomial $q(x)$	integer q
Primitive element:	
$\alpha \in \mathbb{F}_{p^r}$ root	$p \in \mathbb{Z}/(q)$
Reduction mapping:	
$\mathbb{F}_{p^r} \stackrel{Tr}{\rightarrow} \mathbb{F}_p$	$\mathbb{Z}/(q) \stackrel{mod}{\rightarrow} \mathbb{F}_p$
Output sequence:	
$a_n = Tr(\alpha^n)$	$a_n = p^{-n} \pmod q \pmod p$
Auto-correlation:	
$\lvert\mathcal{C}_\tau(\mathbf{a}, \mathbf{a})\rvert \leq 1$	$\lvert\mathcal{C}_\tau^{arith}(\mathbf{a}, \mathbf{a})\rvert \leq 1$ $\mathcal{C}_\tau^{arith}(\mathbf{a}, \mathbf{a}) = 0$ for $p = 2$

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry
Period:	
$T = p^r - 1$	$T = q - 1$
Connection element:	
polynomial $q(x)$	integer q
Primitive element:	
$\alpha \in \mathbb{F}_{p^r}$ root	$p \in \mathbb{Z}/(q)$
Reduction mapping:	
$\mathbb{F}_{p^r} \stackrel{Tr}{\rightarrow} \mathbb{F}_p$	$\mathbb{Z}/(q) \stackrel{mod}{\rightarrow} \mathbb{F}_p$
Output sequence:	
$a_n = Tr(\alpha^n)$	$a_n = p^{-n} \pmod q \pmod p$
Auto-correlation:	
$\lvert\mathcal{C}_\tau(\mathbf{a},\mathbf{a})\rvert \leq 1$	$\lvert\mathcal{C}_\tau^{arith}(\mathbf{a},\mathbf{a})\rvert \leq 1$ $\mathcal{C}_\tau^{arith}(\mathbf{a},\mathbf{a}) = 0$ for $p = 2$
Occurrences of a block $\mathbf{b}$, $s = T/(p^{\lvert\mathbf{b}\rvert})$	
$N(\mathbf{b}) \in \{s, s+1\}$	$N(\mathbf{b}) \in \{s, s+1\}$

Summary of properties

m-sequence	ℓ-sequence
Characterization:	
shift-and-add	shift-and-add with carry
Period:	
$T = p^r - 1$	$T = q - 1$
Connection element:	
polynomial $q(x)$	integer q
Primitive element:	
$\alpha \in \mathbb{F}_{p^r}$ root	$p \in \mathbb{Z}/(q)$
Reduction mapping:	
$\mathbb{F}_{p^r} \stackrel{Tr}{\to} \mathbb{F}_p$	$\mathbb{Z}/(q) \stackrel{mod}{\to} \mathbb{F}_p$
Output sequence:	
$a_n = Tr(\alpha^n)$	$a_n = p^{-n} \pmod q \pmod p$
Auto-correlation:	
$\lvert\mathcal{C}_\tau(\mathbf{a},\mathbf{a})\rvert \leq 1$	$\lvert\mathcal{C}_\tau^{arith}(\mathbf{a},\mathbf{a})\rvert \leq 1$ $\mathcal{C}_\tau^{arith}(\mathbf{a},\mathbf{a}) = 0$ for $p = 2$
Occurrences of a block $\mathbf{b}$, $s = T/(p^{\lvert\mathbf{b}\rvert})$	
$N(\mathbf{b}) \in \{s, s+1\}$	$N(\mathbf{b}) \in \{s, s+1\}$
Decimations:	
$\mathbf{a} \neq \mathbf{a}^\tau$ for $(\tau, T) = 1$	$\mathbf{a} \neq \mathbf{a}^\tau$ for $(\tau, T) = 1$ and $q > 13$ (conj.)

Generalizations

- Replace $\mathbb{Z}/(p)$ with $\mathbb{Z}/(N)$

Generalizations

- Replace $\mathbb{Z}/(p)$ with $\mathbb{Z}/(N)$
- Replace $\mathbb{Z}/(p)$ with $\mathbb{F}_{p^r}$

Generalizations

- Replace $\mathbb{Z}/(p)$ with $\mathbb{Z}/(N)$
- Replace $\mathbb{Z}/(p)$ with $\mathbb{F}_{p^r}$

alphabet	m-sequence	ℓ-sequence
$\mathbb{Z}/(N)$		N-adic numbers

Generalizations

- Replace $\mathbb{Z}/(p)$ with $\mathbb{Z}/(N)$
- Replace $\mathbb{Z}/(p)$ with $\mathbb{F}_{p^r}$

alphabet	m-sequence	ℓ-sequence
$\mathbb{Z}/(N)$	Galois rings interesting	N-adic numbers

Generalizations

- Replace $\mathbb{Z}/(p)$ with $\mathbb{Z}/(N)$

- Replace $\mathbb{Z}/(p)$ with $\mathbb{F}_{p^r}$

alphabet	m-sequence	ℓ-sequence
$\mathbb{Z}/(N)$	Galois rings interesting	N-adic numbers
$\mathbb{F}_{p^r}$	m-sequences	

Generalizations

- Replace $\mathbb{Z}/(p)$ with $\mathbb{Z}/(N)$

- Replace $\mathbb{Z}/(p)$ with $\mathbb{F}_{p^r}$

alphabet	m-sequence	ℓ-sequence
$\mathbb{Z}/(N)$	Galois rings interesting	N-adic numbers
$\mathbb{F}_{p^r}$	m-sequences	p-adic fields interesting

Generalizations

- Replace $\mathbb{Z}/(p)$ with $\mathbb{Z}/(N)$

- Replace $\mathbb{Z}/(p)$ with $\mathbb{F}_{p^r}$

alphabet	m-sequence	ℓ-sequence
$\mathbb{Z}/(N)$	Galois rings interesting	N-adic numbers
$\mathbb{F}_{p^r}$	m-sequences	p-adic fields interesting