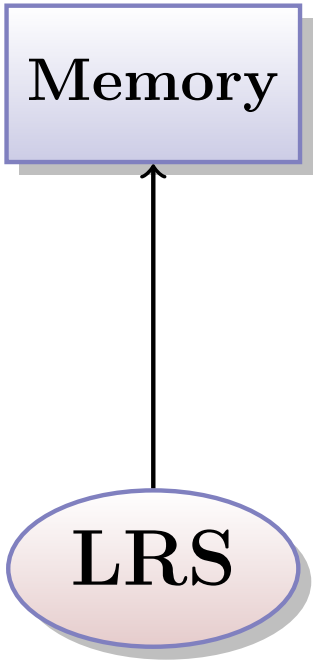
Equidistant filters based on skew ML-sequences over fields

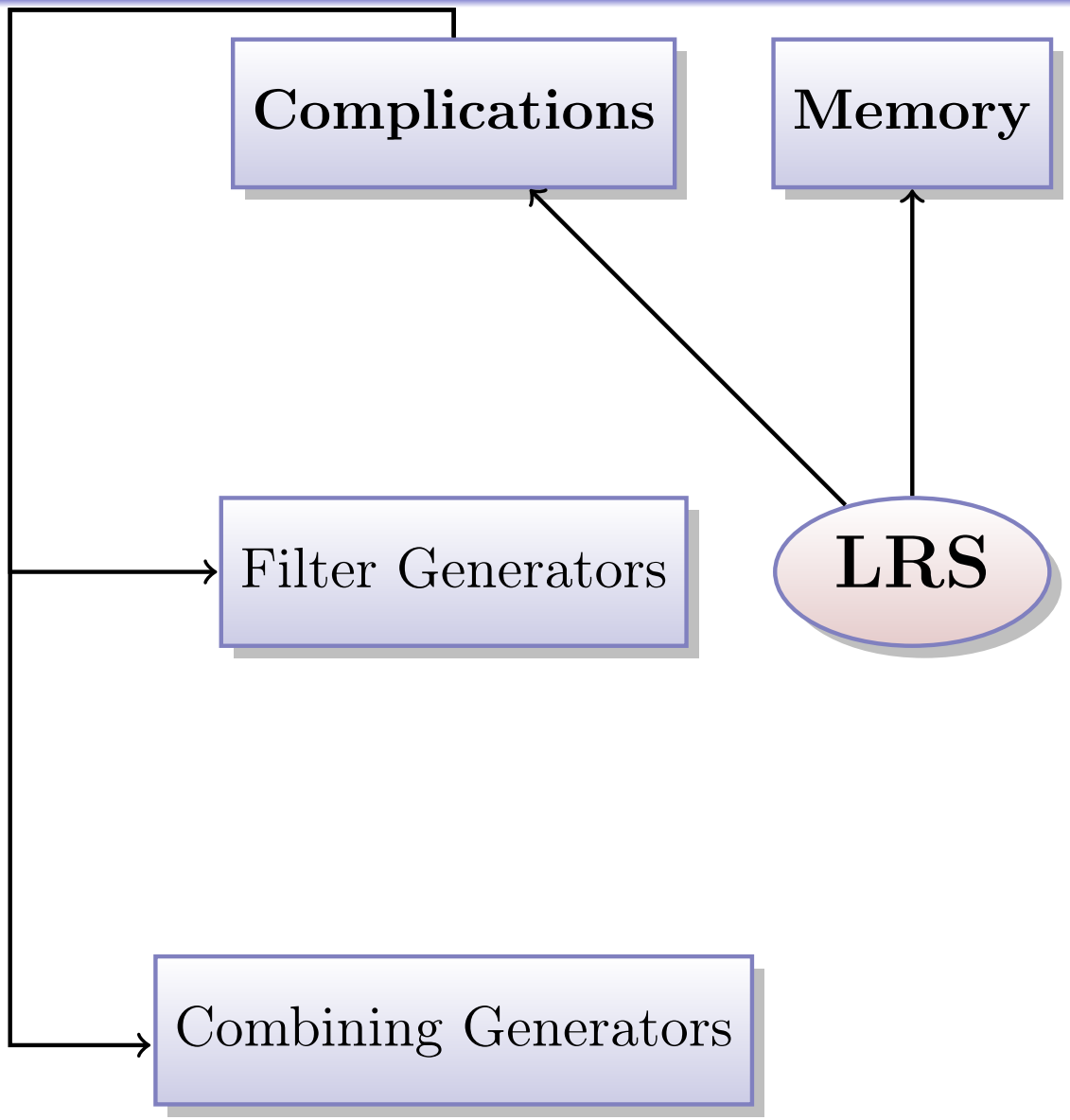
M.A. Goltvanitsa

Introduction: Pseudo-random Sequences Generation

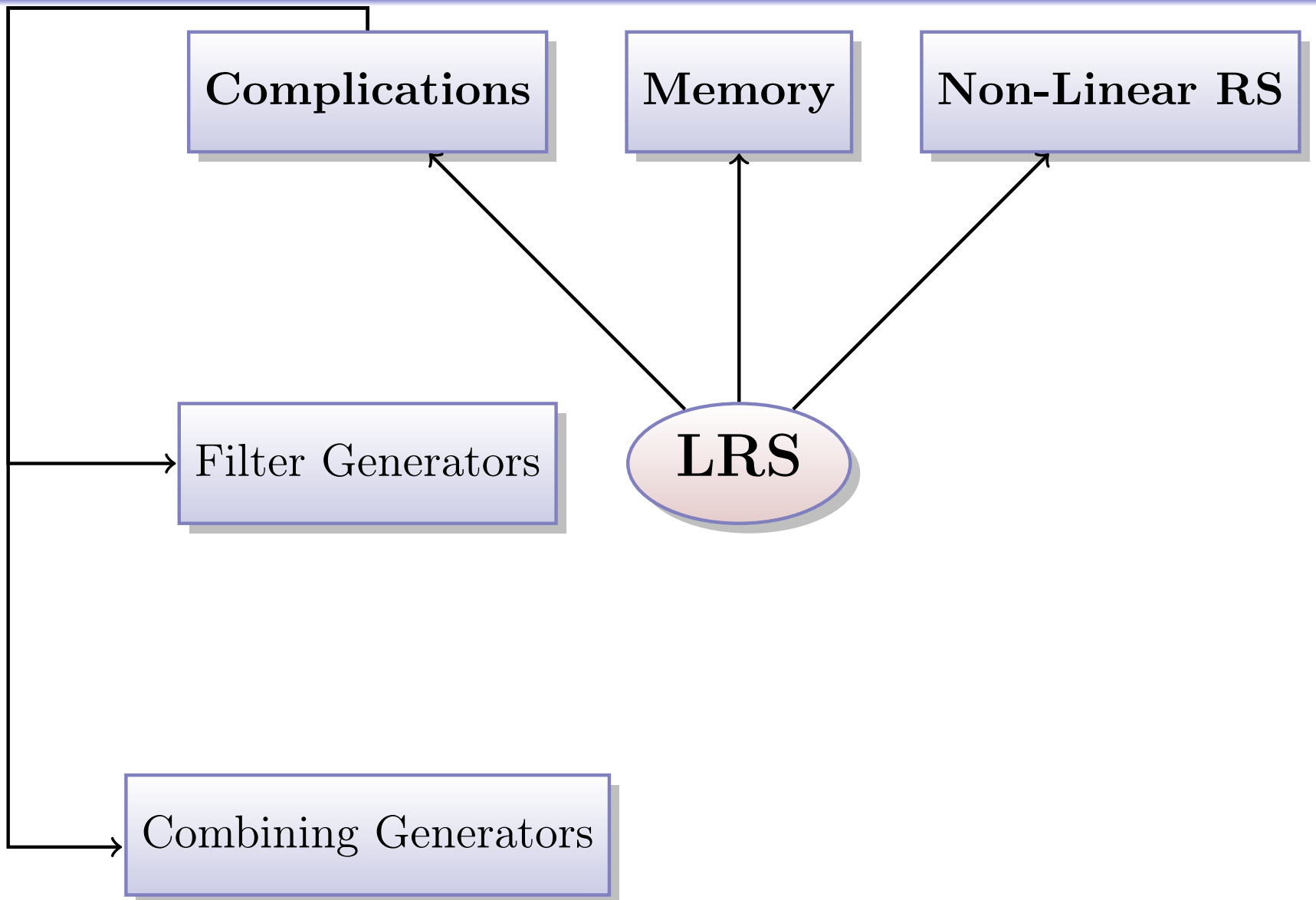
Introduction: Pseudo-random Sequences Generation



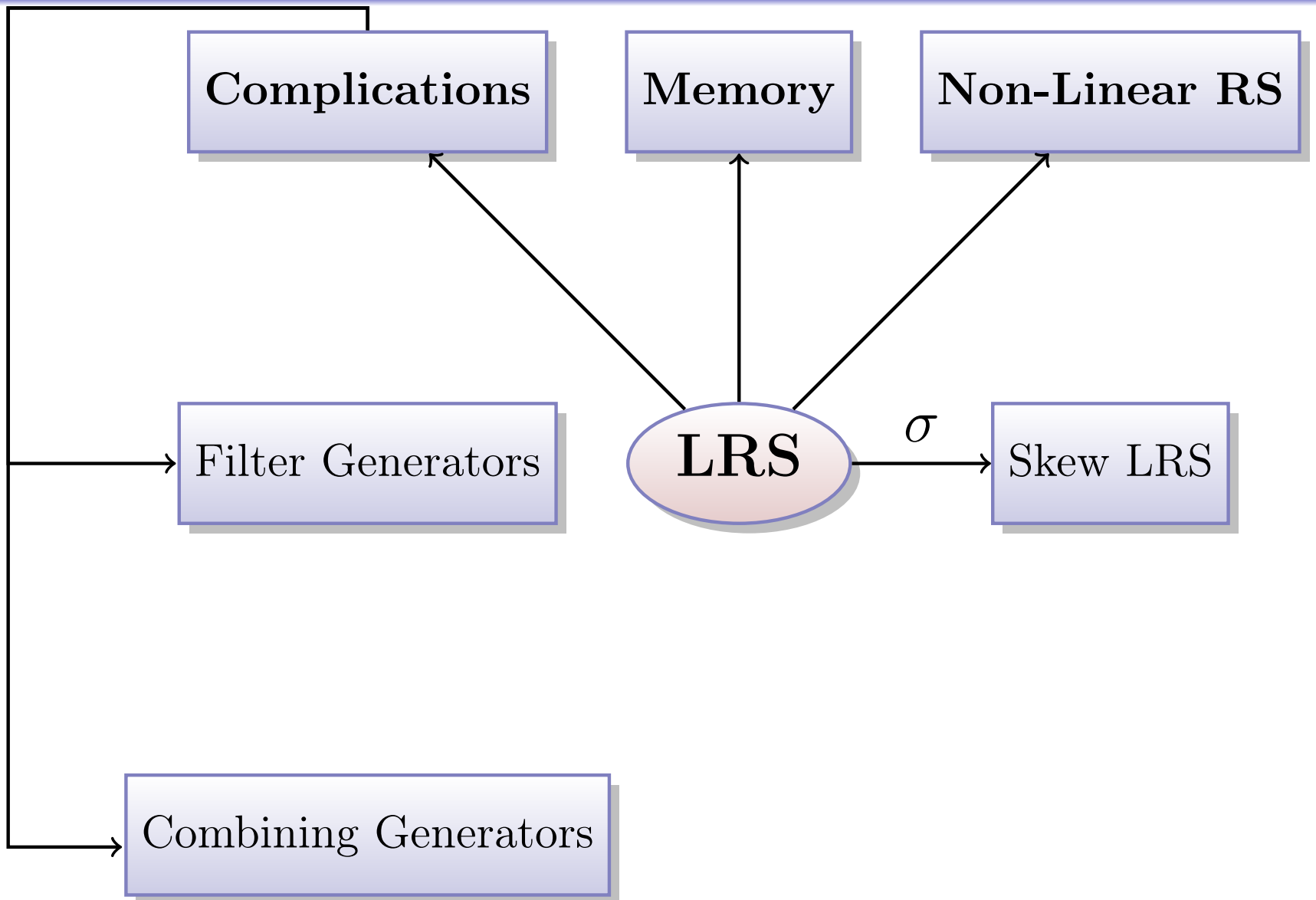
Introduction: Pseudo-random Sequences Generation



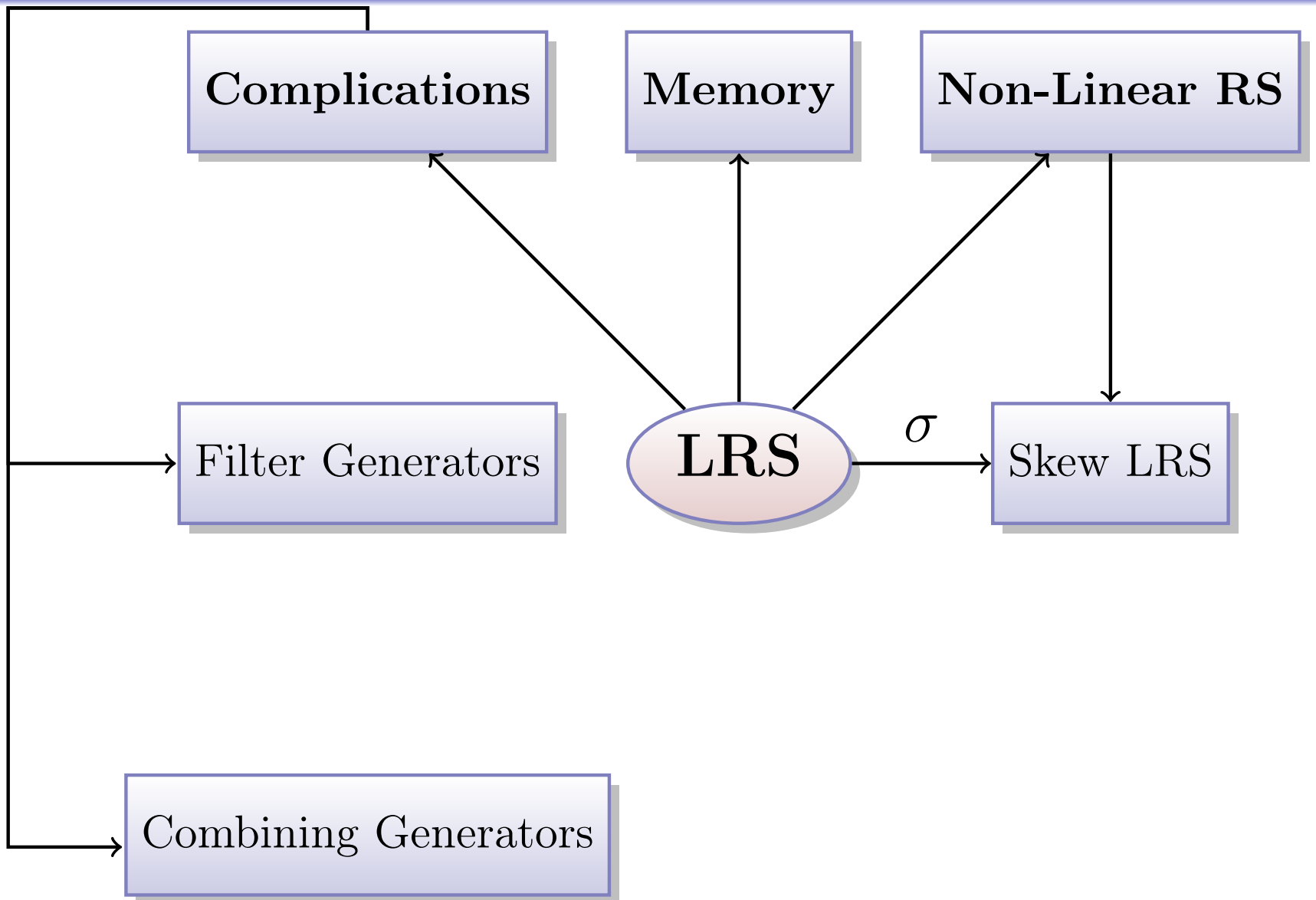
Introduction: Pseudo-random Sequences Generation



Introduction: Pseudo-random Sequences Generation



Introduction: Pseudo-random Sequences Generation



- $R < S, \quad R = \mathrm{GF}(q), \quad S = \mathrm{GF}(q^n);$

- $R < S, \quad R = \mathrm{GF}(q), \quad S = \mathrm{GF}(q^n);$
- $\mathrm{Aut}(S/R) = \langle \sigma \rangle, \ \ \mathrm{ord}\, \sigma = n \ \ (\sigma(s) = s^q : \ \forall s \in S);$

- $R < S, \quad R = \mathrm{GF}(q), \quad S = \mathrm{GF}(q^n)$;
- $\mathrm{Aut}(S/R) = \langle \sigma \rangle, \ \ \mathrm{ord}\, \sigma = n \ \ (\sigma(s) = s^q : \ \forall s \in S)$;
- For every endomorphism $\psi \in Q = \mathrm{End}({}_R S)$ there exist $s_0, \ldots, s_{n-1} \in S$ such that $\psi(z) = \sum_{j=0}^{n-1} s_j \sigma^j(z) \ \forall z \in S$;

- $R < S, \quad R = \mathrm{GF}(q), \quad S = \mathrm{GF}(q^n)$;
- $\mathrm{Aut}(S/R) = \langle \sigma \rangle, \ \ \mathrm{ord}\, \sigma = n \ \ (\sigma(s) = s^q : \ \forall s \in S)$;
- For every endomorphism $\psi \in Q = \mathrm{End}({}_R S)$ there exist $s_0, \ldots, s_{n-1} \in S$ such that $\psi(z) = \sum_{j=0}^{n-1} s_j \sigma^j(z) \ \forall z \in S$;

Skew LRS Definition

A sequence v over S is said to be a ***skew LRS*** of order m iff there exist $\psi_0, \ldots, \psi_{m-1} \in \mathrm{End}({}_R S)$ such that
$v(i+m) = \psi_{m-1}(v(i+m-1)) + \ldots + \psi_1(v(i+1)) + \psi_0(v(i)), \ i \geq 0.$
$\Psi(x) = x^m - \psi_{m-1} x^{m-1} - \ldots - \psi_1 x - \psi_0$ —characteristic polynomial of LRS v.

- $R < S, \quad R = \mathrm{GF}(q), \quad S = \mathrm{GF}(q^n)$;
- $\mathrm{Aut}(S/R) = \langle \sigma \rangle, \ \ \mathrm{ord}\, \sigma = n \ \ (\sigma(s) = s^q : \ \forall s \in S)$;
- For every endomorphism $\psi \in Q = \mathrm{End}({}_R S)$ there exist $s_0, \ldots, s_{n-1} \in S$ such that $\psi(z) = \sum_{j=0}^{n-1} s_j \sigma^j(z) \ \forall z \in S$;

Skew LRS Definition

A sequence v over S is said to be a ***skew LRS*** of order m iff there exist $\psi_0, \ldots, \psi_{m-1} \in \mathrm{End}({}_R S)$ such that
$v(i+m) = \psi_{m-1}(v(i+m-1)) + \ldots + \psi_1(v(i+1)) + \psi_0(v(i)), \ i \geq 0.$
$\Psi(x) = x^m - \psi_{m-1} x^{m-1} - \ldots - \psi_1 x - \psi_0$ —characteristic polynomial of LRS v.

- if $\psi_j = s_j \in S$, that is $\psi_j(z) = s_j \cdot z$ then v is a *classic LRS*.
- The period $T(v) \leq \tau = q^{mn} - 1$, $\mathrm{rank}_S\, v = km, \ k \in \overline{1, n}$
- There are methods for construction LRS v with $\mathrm{rank}_S\, v = mn$.

Example of skew LRS

- $R = \mathrm{GF}(2) < S = R[x]/x^{32} + x^7 + x^3 + x^2 + 1 = \mathrm{GF}(2^{32})$;
- $s = [x^{i_1} + x^{i_2} + \ldots + x^{i_l}] \leftrightarrow 2^{i_1} + 2^{i_2} + \ldots + 2^{i_l} \in \overline{0, 2^{32} - 1}$;

Example of skew LRS

- $R = \mathrm{GF}(2) < S = R[x]/x^{32} + x^7 + x^3 + x^2 + 1 = \mathrm{GF}(2^{32})$;
- $s = [x^{i_1} + x^{i_2} + \ldots + x^{i_l}] \leftrightarrow 2^{i_1} + 2^{i_2} + \ldots + 2^{i_l} \in \overline{0, 2^{32} - 1}$;
- **Classic LRS** u over S:

  $u(i + 8) = 3u(i + 7) + 17u(i + 4) + 209u(i + 1) + 5u(i)$.

Example of skew LRS

- $R = \mathrm{GF}(2) < S = R[x]/x^{32} + x^7 + x^3 + x^2 + 1 = \mathrm{GF}(2^{32})$;
- $s = [x^{i_1} + x^{i_2} + \ldots + x^{i_l}] \leftrightarrow 2^{i_1} + 2^{i_2} + \ldots + 2^{i_l} \in \overline{0, 2^{32} - 1}$;
- **Classic LRS** u over S:

  $u(i+8) = 3u(i+7) + 17u(i+4) + 209u(i+1) + 5u(i)$.
- **Skew LRS** v over S:

$$\begin{aligned} v(i+8) = {} & 3v(i+7) + 6v(i+7)^2 + 9v(i+7)^4 + v(i+7)^8 + v(i+7)^{16} \\ & +17v(i+4) \quad + \quad 1029v(i+4)^4 + 27v(i+4)^8 + \\ & +209v(i+1) + 11v(i+1)^2 + \\ & +5v(i) \quad + \quad +30v(i)^{16} \end{aligned}$$

Previous Investigations

- *Kurakin V. L., Mikhalev A. V., Nechaev A. A., and Tsypyschev V. N.* The trinomial LRS of order 16 over $\mathrm{GF}(2^{16})$ of period $2^{256} - 1$.

Previous Investigations

- *Kurakin V. L., Mikhalev A. V., Nechaev A. A., and Tsypyschev V. N.* The trinomial LRS of order 16 over $\mathrm{GF}(2^{16})$ of period $2^{256} - 1$.
- *Zeng, G., He, K.C., Han, W.*

$$u(i+m) = \&_{\vec{s}} v(i+k) + \sigma^l(v(i)).$$

Previous Investigations

- *Kurakin V. L., Mikhalev A. V., Nechaev A. A., and Tsypyschev V. N.* The trinomial LRS of order 16 over $\mathrm{GF}(2^{16})$ of period $2^{256} - 1$.
- *Zeng, G., He, K.C., Han, W.*

$$u(i+m) = \&_{\vec{s}} v(i+k) + \sigma^l(v(i)).$$

- *Goltvanitsa M.A.*

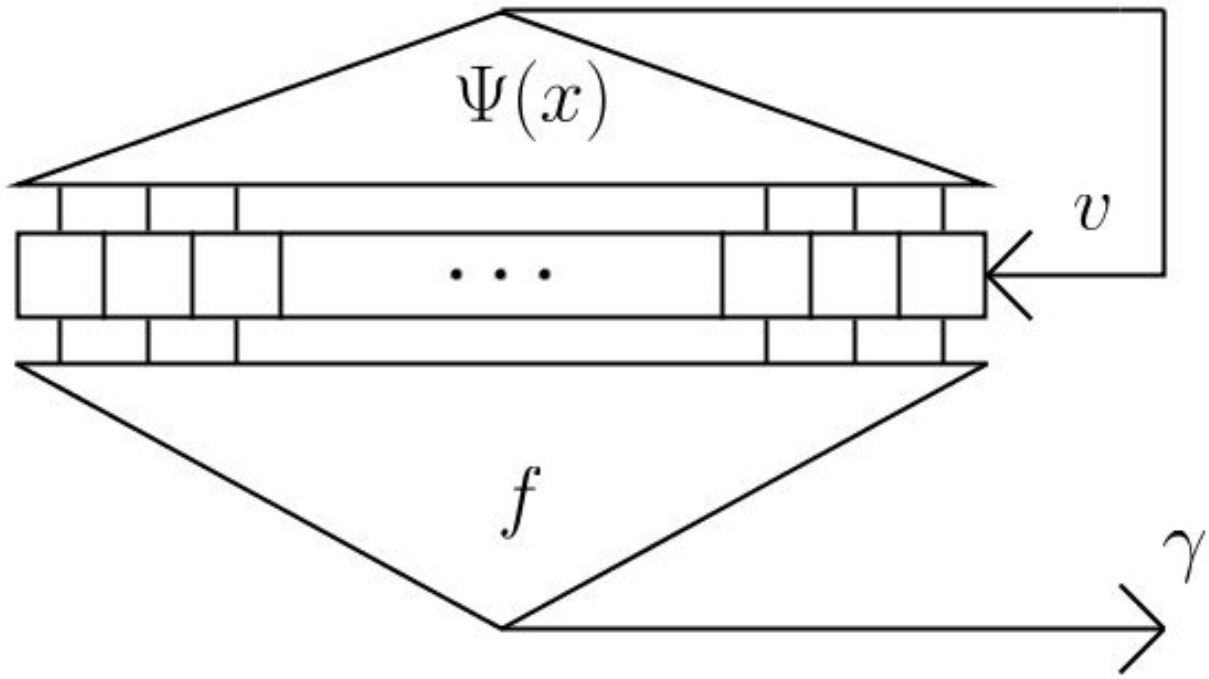
$$u(i+m) = \sum_{j \in W_1} s_j v(i+j) + \sum_{j \in W_2} s_j \sigma^l(v(i+j))$$

Skew LRS is a Promising Source of PRSG

- There exist wide classes of skew MP LRS oriented toward fast software implementation.
- Design advantages
- High linear complexity
- High linear complexity of complications

Goltvanitsa, M.A.

- Digit sequences of skew LRS of maximal period over Galois rings // Mat. Vopr. Kriptogr. — 2015. — V. 6. — I. 2. — P. 19-27.
- The first digit sequence of skew LRS of maximal period over Galois rings // Mat. Vopr. Kriptogr. — 2016. — V. 7. — I. 3. — P. 5-18.



$$\gamma(i) = f(v(i), v(i+1), \ldots, v(i+m-1)),$$
$$v(i+m) = \psi_{m-1}(v(i+m-1)) + \ldots + \psi_1(v(i+1)) + \psi_0(v(i)),$$
$$\psi_0, \ldots, \psi_{m-1} \in Q.$$

Equidistant phases product

- Let v be a skew MP LRS of order m.
- $y(i) = v(i) \cdot v(i+k) \cdot \ldots \cdot v(i+k(t-1)),\ k \in \mathbb{N},\ 2 \leq t < m$

For the case, where v is a classic MP LRS the sequence y was investigated earlier by many authors. Among them are:
V.I. Nechaev, A.A. Nechaev, A.S. Kuzmin, V.L. Kurakin, R.Ruepel, R.V. Bogonatov, N. Kolokotronis, K. Liminiotis, N. Kaloupsidis.

- The basic estimation for classic MP LRS v $\operatorname{rank}_S y \geq \binom{m}{t}$

Trace representation

- $R = \mathrm{GF}(q) < S = \mathrm{GF}(q^n)$
- $S < K = \mathrm{GF}(q^{mn})$

Theorem 1

Let v be a skew MP LRS of order m over S. Then there exist $\theta \in K$ and unique tuple $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1})$ such that

$$v(i) = \mathrm{tr}_S^K(\varepsilon_0\theta^i) + \mathrm{tr}_S^K(\varepsilon_1\theta^{iq}) + \ldots + \mathrm{tr}_S^K(\varepsilon_{n-1}\theta^{iq^{n-1}}).$$

Linear complexity

- $R = \mathrm{GF}(q) < S = \mathrm{GF}(q^n) < K = \mathrm{GF}(q^{mn})$;
- $v(i) = \mathrm{tr}_S^K(\sum_{j=0}^{n-1} \varepsilon_j \theta^{iq^j})$, $N(v) = \{j \in \overline{0, n-1} : \ \varepsilon_j \neq 0\}$;
- $|N(v)| = n_0$;
- $y(i) = v(i)v(i+k)\dots v(i+k(t-1))$, $2 \leq t < m$.

Theorem 2

Let $[R(\theta^k) : R] = \mu, n|\mu, \nu = \frac{\mu}{n}$.

1. If $\mathrm{char}R \neq 2$, $t = 2$, and k satisfies the condition $[R(\theta^{2k}) : R] = [R(\theta^k) : R]$, then $\mathrm{rank}_S\, y = \dfrac{mn_0(mn_0+1)}{2}$.
2. In the case where $\mathrm{char}R = 2$, we have $\mathrm{rank}_S\, y \geq n_0^t \binom{\nu}{t} \left(\frac{m}{\nu}\right)^t + (n_0)_t \left(\binom{m}{t} - \binom{\nu}{t}\left(\frac{m}{\nu}\right)^t\right) + \binom{n_0}{t} m$

Theorem 3 (Periodic properties)

The period $T(y)$ of the sequence y satisfies the condition

$$T(y)|\frac{\tau}{(q-1,t)}.$$

If $t=2$, then

$$T(y)=\frac{\tau}{(q-1,2)}.$$

In the case where $\mathrm{char}R=2$ and $[R(\theta^k):R]=\mu,n|\mu,\nu=\frac{\mu}{n}$.

1. $\frac{\tau}{(q^n-1,t)}|T(y)$
2. if $3\leq t<m,\ n_0\geq 2$, then

$$\frac{\tau}{(q^\lambda-1,t)}|T(y), \tag{1}$$

where λ is equal to greatest common divisor of all elements from the set $\{j_b-j_a:\ j_a,j_b\in N(v),\ a,b\in\overline{1,n_0},\ j_a<j_b\}\cup\{n\}$.

- $R = \mathrm{GF}(q) < S = \mathrm{GF}(q^n) < K = \mathrm{GF}(q^{mn})$;
- $v(i) = \mathrm{tr}_S^K(\sum_{j=0}^{n-1} \varepsilon_j \theta^{iq^j}),\ N(v) = \{j \in \overline{0, n-1} :\ \varepsilon_j \neq 0\}$, $n_0 = |N(v)|$;
- $y(i) = v(i)v(i+k)\dots v(i+k(t-1)),\ 2 \leq t < m$.

Consequence

Let $[R(\theta^k) : R] = \mu, n | \mu, \nu = \frac{\mu}{n}$ and $\mathrm{char} R = 2,\ 3 \leq t < m$. Then if any of the conditions

1. $n_0 \geq 2$ and n is prime;
2. $n_0 > \frac{n}{2}$;

is fulfilled, then the period of sequence y reaches the maximal value, that is

$$T(y) = \frac{\tau}{(q-1, t)}. \tag{2}$$

Consider the sequence

$$z(i) = \sum_{j=0}^{N-1} h_j y(i+j) + g(v(i), v(i+1), \ldots, v(i+m-1)),$$

where $h_j \in S,\ \deg g < s$

Theorem 4

Let $[R(\theta^k) : R] = \mu, n|\mu, \nu = \frac{\mu}{n}$. In the case where $\mathrm{char} R = 2$

$\mathrm{rank}_S\, z \geq$

$$n_0^t \binom{\nu}{t} \left(\frac{m}{\nu}\right)^t + (n_0)_t \left(\binom{m}{t} - \binom{\nu}{t} \left(\frac{m}{\nu}\right)^t \right) + \binom{n_0}{t} m - (N-1).$$

In the case where $\mathrm{char} R \neq 2, t = 2$ and k satisfies condition $[R(\theta^k) : R] = [R(\theta^{2k}) : R]$:

$$\mathrm{rank}_S\, z \geq \frac{m n_0 (m n_0 - 1)}{2} - (N-1).$$