Outline

1 Background
   - Pseudorandom Sequences
   - Algebra

2 Generation Primitives
   - Linear Feedback Shift Registers
   - Feedback with Carry Shift Registers

3 Complexity Measures
   - Linear and $N$-adic Complexity
   - Extended Complexity Measures
   - Results and Future Work
Outline

1. Background
   - Pseudorandom Sequences
     - Algebra

2. Generation Primitives
   - Linear Feedback Shift Registers
   - Feedback with Carry Shift Registers

3. Complexity Measures
   - Linear and $N$-adic Complexity
   - Extended Complexity Measures
   - Results and Future Work
Random Sequences

What is a random sequence?

A sequence which is output by a truly random source.

What is a truly random source?

- non-deterministic
- equally likely selection for each symbol of the alphabet.

Examples:

- Rolling an unbiased die
- The points in time at which a radioactive source decays
- Time difference between mouse movements
Random Sequences

What is a random sequence?

A sequence which is output by a truly random source.

What is a truly random source?

- non-deterministic
- equally likely selection for each symbol of the alphabet.

Examples:

- Rolling an unbiased die
- The points in time at which a radioactive source decays
- Time difference between mouse movements
Pseudorandom Sequences

Appear random and generated by expanding a seed (PRNGs).

Examples:
- Roll a die a bunch of times. Store the values generated in a list and reproduce.
- Use a mathematical formula: \( s_{n+1} = a \cdot s_n + c \mod m, \) with \( 0 < a, s_0, c < m. \)

Advantages:
- Efficient
- Deterministic: Can be reproduced with the same seed.
Randomness Tests

Kolmogorov’s test: A given sequence $S$ is random if

$$|S| \leq \text{Smallest program that outputs } S.$$ 

Golomb’s randomness postulates for binary strings over $\{-1, 1\}$

R-1 A balance of $-1$s and $1$s.

R-2 Two runs of length $k$ for each run of length $k + 1$.

R-3 A two level auto-correlation function.

$$\frac{1}{n} \sum_{i=1}^{n} a_i a_{i+\tau} = \begin{cases} 
1 & \text{if } \tau = 0; \\
K & \text{if } 0 < \tau < n.
\end{cases}$$
Stream cipher:
- Private key cryptosystem.
- Encrypts one symbol at a time.
- Uses pseudorandom sequences.

Let $M$: message, $K$: key stream, $C$: cipher
- Sender: Send the cipher $C = M \oplus K$ across the channel.
- Receiver: Extract the message $M = C \oplus K$.

Sequences should satisfy
- Randomness Properties.
- Large period.
- Fast generation.
- Resistance to specific attacks (Berlekamp-Massey).
1 Background
   - Pseudorandom Sequences
   - Algebra

2 Generation Primitives
   - Linear Feedback Shift Registers
   - Feedback with Carry Shift Registers

3 Complexity Measures
   - Linear and $N$-adic Complexity
   - Extended Complexity Measures
   - Results and Future Work
A (commutative) ring is a set $R$ with two binary operations $\ast$ and $+$ on $R$ such that the following properties hold:

1. $\forall a, b \in R$, $a + b = b + a$ and $ab = ba$.
2. $\forall a, b, c \in R$, $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$.
3. $\exists e_+, e_* \in R$ such that $\forall a \in R$, $ae_* = a$ and $a + e_+ = a$.
4. For each $a \in R$, $\exists -a$ such that $a + (-a) = e_+$.
5. $\forall a, b, c \in R$, $a(b + c) = ab + ac$.

$R$ is a field if it is a ring and for each $a \neq 0 \in R$, $\exists a^{-1}$ so that $aa^{-1} = e_*$.

**Theorem**

For each $q = p^i$, where $p$ is a prime and $i \geq 1$, there exists a finite field $\mathbb{F}_q$ with $q$ elements. These are all the finite fields.

$\mathbb{F}_q[x]$ is the ring of polynomials with coefficients in $\mathbb{F}_q$. 
Definition

A sequence $S = s_0, s_1, s_2, \cdots$ is eventually periodic with period $T$ if $s_{n+T} = s_n$ holds for all $n \geq n_0$ for some $n_0 \geq 0$. $S$ is periodic if $n_0 = 0$.

The generating function of an $S = s_0, s_1, \cdots$ is

$$
\sum_{i=0}^{\infty} s_i x^i.
$$

Closed forms for some well known sequences:

- $1, 1, 1, \cdots$: $\frac{1}{1 - x}$.

- $1, 2, 3, \cdots$: $\frac{1}{(1 - x)^2}$.

- $0, 1, 1, 2, 3, 5, \cdots$: $\frac{1}{1 - x - x^2}$. 
Consider $S$ below with preperiod $n_0 + 1$ and period $T$

$$s_0, s_1, \ldots, s_{n_0}, (s_{n_0+1}, \ldots, s_{n_0+T})^\infty.$$ 

The generation function of $S$ is

$$G(S)$$

$$= s_0 + s_1 x + \cdots + s_{n_0} x^{n_0} + \frac{s_{n_0+1} x^{n_0+1} + \cdots + s_{n_0+T} x^{n_0+T}}{1 - x^T}$$

$$= \frac{(1 - x^T)(s_0 + s_1 x + \cdots + s_{n_0} x^{n_0}) + s_{n_0+1} x^{n_0+1} + \cdots + s_{n_0+T} x^{n_0+T}}{1 - x^T}$$

$$= \frac{u(x)}{g(x)} \quad \text{for some } u(x), g(x) \in \mathbb{F}_q[x].$$
Outline

1. Background
   - Pseudorandom Sequences
   - Algebra

2. Generation Primitives
   - Linear Feedback Shift Registers
   - Feedback with Carry Shift Registers

3. Complexity Measures
   - Linear and $N$-adic Complexity
   - Extended Complexity Measures
   - Results and Future Work
Definition of LFSRs

\[ g_i, a_j \in \mathbb{F}_q, \text{ field} \]

![Diagram of LFSR](image)

- \( a_r = g_1 a_{r-1} + \cdots + g_r a_0 \)
- Output \( A = a_0, a_1, \cdots, a_{r-1}, a_r, a_{r+1}, \cdots \)
- Analysis:
  - generating function \( A(x) = \sum_i a_i x^i \)
  - connection polynomial \( g(x) = -1 + g_1 x + g_2 x^2 + \cdots + g_r x^r \)
Properties of LFSRs

LFSR sequences are eventually periodic.

The generating function of LFSR sequences is rational

\[ A(x) = \frac{u(x)}{g(x)}, \quad u(x) \in \mathbb{F}_q[x] \]

- Periodic iff \( \deg(u) < \deg(g) \)
- If \( \gcd(u, g) = 1 \) period is the smallest \( T \) such that \( g(x) | x^T - 1 \).
- m-sequence: If \( g(x) \) primitive, period = \( q^r - 1 \)
- m-sequences: uniform – each nonzero \( r \)-tuple occurs once (R1,R2,R3)
rand() and random()

rand() uses multiplicative congruential generator:

\[ s_{n+1} = a \cdot s_n \mod m, \text{ where } m \text{ is prime and } a \neq 0. \]

Source: National Energy Research Scientific Computing Center

“the low dozen bits generated by the rand subroutine go through a cyclic pattern, while all the bits generated by the random subroutine are usable”

Source: Comments from the GNU source file random_r.c

“The random number generation technique is a linear feedback shift register approach, employing trinomials (since there are fewer terms to sum up that way). In this approach, the least significant bit of all the numbers in the state table will act as a linear feedback shift register, and will have period \(2^{\text{deg}} - 1\) (where deg is the degree of the polynomial being used, assuming that the polynomial is irreducible and primitive).”
Outline

1. Background
   - Pseudorandom Sequences
   - Algebra

2. Generation Primitives
   - Linear Feedback Shift Registers
   - Feedback with Carry Shift Registers

3. Complexity Measures
   - Linear and $N$-adic Complexity
   - Extended Complexity Measures
   - Results and Future Work
$N \in \mathbb{Z}, \; N \geq 2.$

- $g_1, g_2, \ldots, g_r \in S = \{0, 1, \ldots, N - 1\}$.
- State change: define $a_r \in S$ and $m_r \in \mathbb{Z}$ by

$$a_r + Nm_r = m_{r-1} + g_1 a_{r-1} + \cdots + g_r a_0.$$

- Connection number: $g = -1 + g_1 N + g_2 N^2 + \cdots + g_r N^r$. 
Ring of \(N\)-adic integers

\[
\mathbb{Z}_N = \left\{ \sum_{i=0}^{\infty} a_i N^i = \alpha(A, N) : a_i \in S \right\}
\]

- **Addition:** To add \(\sum a_i N^i + \sum b_i N^i = \sum c_i N^i:\)

  \[
c_0 + Nd_1 = a_0 + b_0, \quad 0 \leq c_0 < N \\
c_1 + Nd_2 = a_1 + b_1 + d_1, 0 \leq c_1 < N \\
-1 = (N - 1) + (N - 1)N + (N - 1)N^2 + \cdots
\]

- **Multiplication is similar**

- **\(A = \sum a_i N^i \in \mathbb{Z}_N\) is invertible iff \(\gcd(a_0, N) = 1\)**
Properties of FCSRs

For an $r$-stage FCSR let $w = \sum_{i=1}^{r} g_i$. Denote $z_{r-1}:$ initial memory, $z$: memory in any state.

- Periodic state $\Rightarrow 0 \leq z < w$.
- $z_{r-1} \geq w$ or $z_{r-1} < 0 \Rightarrow$ within $\lceil \log_N(|z_{r-1}|) \rceil + r$ steps $0 \leq z < w$.

So FCSR sequences are eventually periodic.

- $N$-adic number $\alpha(A, N) = u/g$, some $u \in \mathbb{Z}$, and $\gcd(g, N) = 1$.
- Periodic iff $-g \leq u \leq 0$
- If $\gcd(u, g) = 1$, period is the smallest $T$ such that $g|(N^T - 1)$.
- $\ell$-sequence: When $g = p^t$, $p$ a prime, period $= (p - 1)p^{t-1}$. 
Outline

1 Background
   - Pseudorandom Sequences
   - Algebra

2 Generation Primitives
   - Linear Feedback Shift Registers
   - Feedback with Carry Shift Registers

3 Complexity Measures
   - Linear and $N$-adic Complexity
   - Extended Complexity Measures
   - Results and Future Work
The linear complexity $\lambda(A)$ of a sequence $A = (a_0, a_1, \cdots)$ over $F_q$ is the length of smallest LFSR that can generate $A$.

Let $A$ be a periodic sequence with period $T$. Let $a(x) = a_0 + a_1 x + \cdots + a_{T-1} x^{T-1}$. Then

$$\sum_{i=0}^{\infty} a_i x^i = \frac{a(x)}{1 - x^T} = \frac{u(x)}{g(x)}, \quad \gcd(u(x), g(x)) = 1.$$ 

- $g(x)$ is called the minimal connection polynomial.
- $\lambda(A) = T - \deg(\gcd(a(x), 1 - x^T)) = \deg(g(x)).$
**N-adic Complexity**

**Definition**

The $N$-adic span $\Lambda_N(A)$ of an $N$-ary, eventually periodic sequence $A = (a_0, a_1, \cdots)$ is the smallest value of $\Lambda$ among all FCSRs that output $A$.

\[
\Lambda = r + \max(\lfloor \log_N(\sum_{i=0}^{r} g_i) \rfloor + 1, \lfloor \log_N(|m|) \rfloor + 1) + 1
\]

**Definition**

Let $\alpha(A, N) = -p/q$, with $\gcd(p, q) = 1$. The the $N$-adic complexity of $A$ is the real number $\phi_N(A) = \log_N(\max(|p|, |q|))$.

\[
|\Lambda_N(A) - 2) - \phi_N(A)| \leq \log_N(\phi_N(A)) + 1
\]
Why Study Complexity Measures?

Answer: Shift Register Synthesis Algorithms

Input: First few symbols, usually, linear in the complexity.
Output: Shift Register that outputs the sequence

<table>
<thead>
<tr>
<th>Algorithm</th>
<th># Symbols $t \geq$</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berlekamp-Massey (Massey)</td>
<td>$2\lambda$</td>
<td>$O(t^2)$</td>
</tr>
<tr>
<td>Rational Approximation ($N = 2$, Klapper and Goresky)</td>
<td>$2[\phi_2] + 2$</td>
<td>$O(t^2 \log t \log \log t)$</td>
</tr>
<tr>
<td>Rational Approximation ($N &gt; 2$, Xu)</td>
<td>$6(3 + [\phi_N])$</td>
<td>$O(t^2 + tN^2 \log^3 N)$</td>
</tr>
<tr>
<td>Euclidean Approximation ($N$ not a square, Arnault et al.)</td>
<td>$2[\phi_N] + 3$</td>
<td>$O(t^2)$</td>
</tr>
</tbody>
</table>
1 Background
   - Pseudorandom Sequences
   - Algebra

2 Generation Primitives
   - Linear Feedback Shift Registers
   - Feedback with Carry Shift Registers

3 Complexity Measures
   - Linear and N-adic Complexity
   - Extended Complexity Measures
   - Results and Future Work
In practice, if an attacker can recover a prefix of the keystream, then the system is vulnerable.

Attacker: Run shift register synthesis algorithms on finite prefixes.

Thus every prefix should have $\lambda$ as high as possible.

**Definition (Rueppel)**

The $n$th linear complexity $\lambda_n(A)$ is defined as the length of the shortest LFSR whose first $n$ terms are $a_0, a_2, \ldots, a_{n-1}$. The sequence $\lambda_1(A), \lambda_2(A), \ldots$ of integers is called the linear complexity profile of $A$.

Example: Let $A = (0, \cdots, 0, 1)^\infty$ with period $T$.

Then $\lambda(A) = T$ but $\lambda_n(A) = 0$, for $n = 1 \cdots T - 1$.

Similar measures for $N$-adic complexity.
In practice, if an attacker can recover all but a few symbols of the keystream then the system is insecure.

Attacker: Try all one symbol changes of the known keystream. Choose the one that leads to a message that makes sense.

**Definition (Ding)**

The $k$-error linear complexity $\lambda_{k}^{err}(A)$ of a periodic sequence $A$ is the smallest linear complexity that can be obtained by changing $k$ or fewer symbols of a single period and repeating the period.

Example: Let $A = (0, \cdots, 0, 1)^{\infty}$. Then $\lambda_{1}^{err}(A) = \lambda_{1}^{del}(A) = 0$. Similarly we have $\lambda_{k}^{del}(A)$, $\lambda_{k}^{ins}(A)$, and $\lambda_{k}^{oper}(A)$.

Similar measures for $N$-adic complexity and finite sequences.
Number of Changes Needed to Lower the Complexity

**Definition**

\[ \text{minsub}(A) \] is the minimum number of substitutions required to modify a single period so that the linear complexity of the modified sequence is less than the original sequence.

Similarly \( \text{mindel}(A) \), \( \text{minins}(A) \) and \( \text{minoper}(A) \).

For \( i \in \mathbb{N} \) with radix \( p \) form \( i = \sum_{j=0}^{l-1} i_j p^j \) define \( \text{Prod}(i) = \prod_{j=0}^{l-1} (i_j + 1) \).

**Theorem (Kurosawa et al.)**

For a periodic sequence \( A \) with period \( T = p^d \), \( d \in \mathbb{Z}^+ \), we have

\[ \text{minsub}(A) = \text{Prod}(T - \lambda(A)) \]

Similarly \( \text{minsub}_N(A) \), \( \text{mindel}_N(A) \), \( \text{minins}_N(A) \), and \( \text{minoper}_N(A) \) for \( \phi_N(A) \).
1. Background
   - Pseudorandom Sequences
   - Algebra

2. Generation Primitives
   - Linear Feedback Shift Registers
   - Feedback with Carry Shift Registers

3. Complexity Measures
   - Linear and $N$-adic Complexity
   - Extended Complexity Measures
   - Results and Future Work
Problems on Complexity Measures

1. Determine counting functions and expected values.
2. Determine good upper and lower bounds.
3. Investigate the asymptotic behavior for nonperiodic sequences.
4. Design efficient algorithms to compute a complexity measure.
5. Design efficient algorithms to find the smallest generator.
6. Construct sequences with high complexity and error complexity.

Special cases can also be considered if the general ones are hard.
Let \( N_{(n,k)}(c) \) denote the number of sequences \( A \) with \( \lambda_{(n,k)}^{err}(A) = c \).

**Theorem (Gustavson)**

\[
N_{(n,0)}(0) = 1. \text{ If } 1 \leq c \leq n \text{ then,}
N_{(n,0)}(c) = (q - 1)q^{\min(2c-1,2n-2c)}.
\]

**Theorem (Rueppel)**

*If* \( T = 2^d \), *then the expected linear complexity* \( E_0 \) *of a random periodic T-periodic binary sequence is given by*

\[
E_0 = T - 1 + 2^{-T}.
\]
Asymptotic Behavior

- Ultimately nonperiodic sequences: linear complexity increases unboundedly.

- Normalized linear complexity: $\delta_n(A) = \lambda_n(A)/n$

- $\delta_n(A)$ does not have a single limit but a set of accumulation points.

- Dai et al.: Set of accumulation points for normalized $\lambda$ is
  $\Delta = [B, 1 - B]$

- Klapper: Set of accumulation points for normalized $\phi_N$ is
  $\Delta_N = [B, 1 - B]$ when $N$ is a power of 2 or 3

- Sequences exist for each $B \in [0, 1/2]$ with $\Delta = [B, 1 - B]$ and $\Delta_N = [B, 1 - B]$. 
Theorem (Kavuluru and Klapper)

Let \( A \) be a sequence over \( \mathbb{F}_q \) of period \( T \). Then

1. \( \lambda_{k}^{\text{oper}}(A) \geq \min(\lambda(A), T/k - \lambda(A)) \) if the number of deletions is greater than or equal to the number of insertions.

2. \( \lambda_{k}^{\text{oper}}(A) \geq \min(\lambda(A), (T + 1)/k - \lambda(A)) \) if the number of deletions is less than the number of insertions.

Corollary

Let \( A \) be a not all zero sequence of period \( T \). Then

\[
\min_{\text{oper}}(A) > \frac{T}{2\lambda(A)}.
\]
Lower Bounds on $k$-operation $N$-adic Complexity

**Theorem (Kavuluru and Klapper)**

Let $A$ be a sequence over $\{0, \cdots, N-1\}$ of period $T$. Then

1. $\phi_{N,k}^{\text{oper}}(A) > \min(\phi_{N}(A), T/k + \log_{N}((N-1)/N(N+1)) - \phi_{N}(A))$ if the number of deletions is greater than the number of insertions.

2. $\phi_{N,k}^{\text{oper}}(A) > \min(\phi_{N}(A), \log_{N}(N^T - 1) - (k-1)T/k - \phi_{N}(A) - 1)$ if the number of deletions is equal to the number of insertions.

3. $\phi_{N,k}^{\text{oper}}(A) > \min(\phi_{N}(A), (T+1)/k + \log_{N}((N-1)/N(N+1)) - \phi_{N}(A))$ if the number of deletions is less than the number of insertions.

**Corollary**

Let $A$ be an $N$-ary periodic sequence with period $T$. We have

$$\text{minoper}_{N}(A) > \frac{T}{2\phi_{N}(A) + 3}.$$
## Problem Space

<table>
<thead>
<tr>
<th>Settings</th>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>LFSRs, FCSRs, AFSRs</td>
<td>Counting functions</td>
</tr>
<tr>
<td>Sequences, Multisequences</td>
<td>Expected values</td>
</tr>
<tr>
<td>Periodic, Finite Length</td>
<td>Complexity bounds</td>
</tr>
<tr>
<td>Conventional, $k$-error, $k$-insert</td>
<td>Complexity computation</td>
</tr>
<tr>
<td>$k$-delete, $k$-operation, $minerror$</td>
<td>Shift register synthesis</td>
</tr>
<tr>
<td>arithmetic $k$-error</td>
<td>Asymptotic behavior</td>
</tr>
<tr>
<td>Special Cases: $k = 1, 2, T = p^d$</td>
<td>Fix $\mathbb{F}_q$, $N$, or $(R, \pi, S)$</td>
</tr>
</tbody>
</table>
Thank You