Distribution of short subsequences of inversive generator

László Mérai

(joint work with Igor Shparlinski)

Austrian Academy of Sciences
Johann Radon Institute for Computational and Applied Mathematics
Linz, Austria

6th International Conference on Uniform Distribution Theory

Inversive generator

Let $\mathcal{R}$ be a (finite, commutative, unitary) ring and define the sequence (u_n) by

$$u_n = \psi(u_{n-1}), \quad n \geq 1 \quad \text{with} \quad \psi(x) = \frac{a}{x} + b, \quad a, b \in \mathcal{R}.$$

Inversive generator

Let $\mathcal{R}$ be a (finite, commutative, unitary) ring and define the sequence (u_n) by

$$u_n = \psi(u_{n-1}), \quad n \geq 1 \quad \text{with} \quad \psi(x) = \frac{a}{x} + b, \quad a, b \in \mathcal{R}.$$

or in general

$$u_n = \psi(u_{n-1}), \quad n \geq 1 \quad \text{with} \quad \psi(x) = \frac{ax+b}{cx+d}, \quad a, b, c, d \in \mathcal{R}.$$

with an initial value $u_0 \in \mathcal{R}$.

Inversive generator

Let $\mathcal{R}$ be a (finite, commutative, unitary) ring and define the sequence (u_n) by

$$u_n = \psi(u_{n-1}), \quad n \geq 1 \quad \text{with} \quad \psi(x) = \frac{a}{x} + b, \quad a, b \in \mathcal{R}.$$

or in general

$$u_n = \psi(u_{n-1}), \quad n \geq 1 \quad \text{with} \quad \psi(x) = \frac{ax + b}{cx + d}, \quad a, b, c, d \in \mathcal{R}.$$

with an initial value $u_0 \in \mathcal{R}$.

- The sequence (u_n) can be finite, or
- ultimately periodic, as $\mathcal{R}$ is finite.

Inversive generator

Let $\mathcal{R}$ be a (finite, commutative, unitary) ring and define the sequence (u_n) by

$$u_n = \psi(u_{n-1}), \quad n \geq 1 \quad \text{with} \quad \psi(x) = \frac{a}{x} + b, \quad a, b \in \mathcal{R}.$$

or in general

$$u_n = \psi(u_{n-1}), \quad n \geq 1 \quad \text{with} \quad \psi(x) = \frac{ax+b}{cx+d}, \quad a, b, c, d \in \mathcal{R}.$$

with an initial value $u_0 \in \mathcal{R}$.

- The sequence (u_n) can be finite, or
- ultimately periodic, as $\mathcal{R}$ is finite.

For computational aspect, there are two interesting cases:

- $\mathcal{R} = \mathbb{F}_q$, typically prime field: q is large prime.
- $\mathcal{R} = \mathbb{Z}_{p^t}$, p is small, typically $p = 2$.

Examples for inversive generator

Let $t \geq 3$ and

$$\psi(x) = \frac{ax+b}{cx+d}, \quad a, b, c, d \in \mathbb{Z}_{2^t}.$$

Assume, that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mod 2.$$

Examples for inversive generator

Let $t \geq 3$ and

$$\psi(x) = \frac{ax+b}{cx+d}, \quad a, b, c, d \in \mathbb{Z}_{2^t}.$$

Assume, that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mod 2.$$

Then ψ defines a permutation on $\mathbb{Z}_{2^t}^*$.

Examples for inversive generator

Let $t \geq 3$ and

$$\psi(x) = \frac{ax+b}{cx+d}, \quad a,b,c,d \in \mathbb{Z}_{2^t}.$$

Assume, that

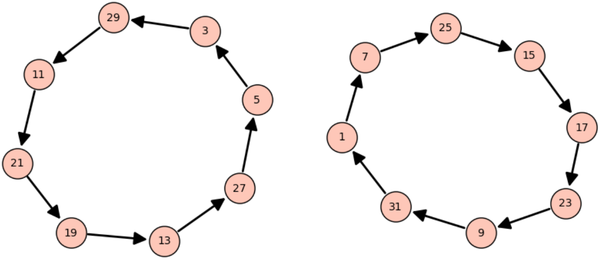
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mod 2.$$

Then ψ defines a permutation on $\mathbb{Z}_{2^t}^*$.

If ψ is a permutation of $\mathbb{Z}_{2^t}^*$, then $(u_n) = (\psi^n(u))$ is purely periodic.

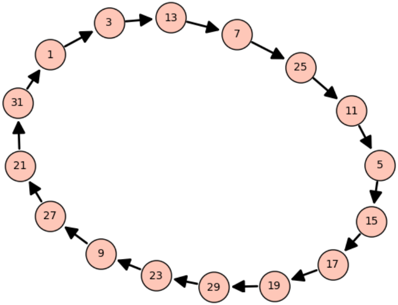
Its period length is $\tau = 2^k$ for some $0 \leq k \leq t-1$.

Examples for inversive generator



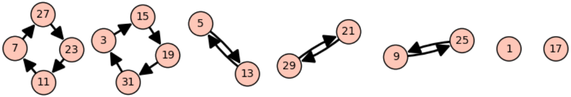
$$\psi(x) = \frac{x+2}{2x+3} \mod 2^5, \quad u_n = \psi(u_{n-1}), \quad n \geq 1.$$

Examples for inversive generator



$$\psi(x) = \frac{2x+1}{x} \mod 2^5, \quad u_n = \psi(u_{n-1}), \quad n \geq 1.$$

Examples for inversive generator



$$\psi(x) = \frac{x+4}{2x+3} \mod 2^5, \quad u_n = \psi(u_{n-1}), \quad n \geq 1.$$

Distribution for inversive generator

Assume, that ψ is a permutation of $\mathbb{Z}_{2^t}^*$ and let (u_n) be defined as

$$u_n = \psi(u_{n-1}), \quad n \geq 1$$

with initial value $u_0 \in \mathbb{Z}_{2^t}^*$ and period length τ.

Distribution for inversive generator

Assume, that ψ is a permutation of $\mathbb{Z}_{2^t}^*$ and let (u_n) be defined as

$$u_n = \psi(u_{n-1}), \quad n \geq 1$$

with initial value $u_0 \in \mathbb{Z}_{2^t}^*$ and period length τ.

Our goal is to study the discrepancy $D_N(u_n)$ of

$$u_0/2^t, \ldots, u_{N-1}/2^t \in [0, 1), \quad N \leq \tau.$$

Distribution for inversive generator

Assume, that ψ is a permutation of $\mathbb{Z}_{2^t}^*$ and let (u_n) be defined as

$$u_n = \psi(u_{n-1}), \quad n \geq 1$$

with initial value $u_0 \in \mathbb{Z}_{2^t}^*$ and period length τ.

Our goal is to study the discrepancy $D_N(u_n)$ of

$$u_0/2^t, \ldots, u_{N-1}/2^t \in [0,1), \quad N \leq \tau.$$

As usual, the main tool is to bound

$$\sum_{n=0}^{N-1} \exp\left(h\frac{2\pi i u_n}{2^t}\right), \quad \gcd(h,2) = 1.$$

Distribution for inversive generator

Niederreiter, Winterhof '05:

$$\sum_{n=0}^{N-1} \exp\left(h\frac{2\pi i u_n}{2^t}\right) \ll 2^{\frac{3}{4}t} N^{\frac{1}{2}} \tau^{-\frac{1}{2}}, \quad 1 \le N \le \tau,$$

where τ is the period length and $\gcd(h, 2) = 1$.

Distribution for inversive generator

Niederreiter, Winterhof '05:

$$\sum_{n=0}^{N-1} \exp\left(h\frac{2\pi i u_n}{2^t}\right) \ll 2^{\frac{3}{4}t} N^{\frac{1}{2}} \tau^{-\frac{1}{2}}, \quad 1 \le N \le \tau,$$

where τ is the period length and $\gcd(h, 2) = 1$.

The result is nontrivial if

$$\tau \gg 2^{\frac{3}{4}t} \quad \text{and} \quad N \gg 2^{\frac{3}{2}t}\tau^{-1}.$$

Distribution for inversive generator

Niederreiter, Winterhof '05:

$$\sum_{n=0}^{N-1} \exp\left(h\frac{2\pi i u_n}{2^t}\right) \ll 2^{\frac{3}{4}t} N^{\frac{1}{2}} \tau^{-\frac{1}{2}}, \quad 1 \le N \le \tau,$$

where τ is the period length and $\gcd(h,2) = 1$.

The result is nontrivial if

$$\tau \gg 2^{\frac{3}{4}t} \quad \text{and} \quad N \gg 2^{\frac{3}{2}t}\tau^{-1}.$$

For example, if (u_n) has large period length: $\tau \gg 2^t$, then one needs $N \gg 2^{\frac{t}{2}}$.

Distribution for inversive generator

Niederreiter, Winterhof '05:

$$\sum_{n=0}^{N-1} \exp\left(h\frac{2\pi i u_n}{2^t}\right) \ll 2^{\frac{3}{4}t} N^{\frac{1}{2}} \tau^{-\frac{1}{2}}, \quad 1 \leq N \leq \tau,$$

where τ is the period length and $\gcd(h, 2) = 1$.

The result is nontrivial if

$$\tau \gg 2^{\frac{3}{4}t} \quad \text{and} \quad N \gg 2^{\frac{3}{2}t}\tau^{-1}.$$

For example, if (u_n) has large period length: $\tau \gg 2^t$, then one needs $N \gg 2^{\frac{t}{2}}$.

Can we do more?

Inversive generator, special cases

Proposition

Assume, that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *has eigenvalue with multiplicity. Then*

$$u_n \equiv \frac{\alpha n + u_0}{\beta n + 1} \mod 2^t, \quad \textit{for } n \geq 0.$$

Inversive generator, special cases

Proposition

Assume, that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *has eigenvalue with multiplicity. Then*

$$u_n \equiv \frac{\alpha n + u_0}{\beta n + 1} \mod 2^t, \quad \textit{for } n \geq 0.$$

If $\beta = 0$, we have a linear generator $(\alpha n + u_0)$.

Inversive generator, special cases

Proposition

Assume, that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *has eigenvalue with multiplicity. Then*

$$u_n \equiv \frac{\alpha n + u_0}{\beta n + 1} \mod 2^t, \quad \textit{for } n \geq 0.$$

If $\beta = 0$, we have a linear generator $(\alpha n + u_0)$.

If $\beta \neq 0$, $S_h(N)$ is a Kloosterman sum.

Inversive generator, special cases

Proposition

Assume, that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *has eigenvalue with multiplicity. Then*

$$u_n \equiv \frac{\alpha n + u_0}{\beta n + 1} \mod 2^t, \quad \textit{for } n \geq 0.$$

If $\beta = 0$, we have a linear generator $(\alpha n + u_0)$.

If $\beta \neq 0$, $S_h(N)$ is a Kloosterman sum.

Korolev '16:

$$\sum_{\substack{c \leq n < N+c \\ 2 \nmid n}} \exp\left(\frac{an^{-1} + bn}{2^t}\right) = o(N)$$

for $2^{c(t^{2/3})} \leq N \leq 2^{t/2}$.

Explicit inversive generator

Assume, that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is diagonalizable over $\mathbb{Z}_{2^t}$. Then

$$u_n \equiv \frac{\alpha}{g^n + \beta} + \gamma \mod 2^t, \quad n \geq 0, \quad \text{with } g, \alpha, \beta, \gamma \in \mathbb{Z}.$$

Explicit inversive generator

Assume, that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is diagonalizable over $\mathbb{Z}_{2^t}$. Then

$$u_n \equiv \frac{\alpha}{g^n + \beta} + \gamma \mod 2^t, \quad n \geq 0, \quad \text{with } g, \alpha, \beta, \gamma \in \mathbb{Z}.$$

Explicit inversive generator

Assume, that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is diagonalizable over $\mathbb{Z}_{2^t}$. Then

$$u_n \equiv \frac{\alpha}{g^n + \beta} + \gamma \mod 2^t, \quad n \geq 0, \quad \text{with } g, \alpha, \beta, \gamma \in \mathbb{Z}.$$

Theorem (M., Shparlinski)

For odd α write $\tau = 2^{t-\nu+1}$.

Explicit inversive generator

Assume, that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is diagonalizable over $\mathbb{Z}_{2^t}$. Then

$$u_n \equiv \frac{\alpha}{g^n + \beta} + \gamma \mod 2^t, \quad n \geq 0, \quad \text{with } g, \alpha, \beta, \gamma \in \mathbb{Z}.$$

Theorem (M., Shparlinski)

For odd α write $\tau = 2^{t-\nu+1}$.
Let $t > 16\nu$. Then for $2^{8\nu} < N \leq 2^{t/2}$,

$$\sum_{n=0}^{N-1} \exp\left(h \frac{2\pi i u_n}{2^t}\right) \ll N^{1-\varepsilon\left(\frac{\log N}{t}\right)^2}, \quad 2 \nmid h$$

for some $\varepsilon > 0$.

Explicit inversive generator – Discrepancy bound

Let $D_N(u_n)$ be the discrepancy of the sequence

$$u_0/2^t, \ldots, u_{N-1}/2^t \in [0,1).$$

Reminder:

$$D_N(u_n) = \sup_{I \subset [0,1)} \left| \frac{\#\{u_n \in I : 0 \leq n < N\}}{N} - |I| \right|.$$

Explicit inversive generator – Discrepancy bound

Let $D_N(u_n)$ be the discrepancy of the sequence

$$u_0/2^t, \dots, u_{N-1}/2^t \in [0,1).$$

Reminder:

$$D_N(u_n) = \sup_{I \subset [0,1)} \left| \frac{\#\{u_n \in I : 0 \le n < N\}}{N} - |I| \right|.$$

Corollary (M., Shparlinski)

For odd α write $\tau = 2^{t-\nu+1}$.
Let $t > 32\nu$. Then for $2^{8\nu} < N \le 2^{(\frac{1}{2}-\delta)t}$, with $0 < \delta < 1/2$,

$$D_N(u_n) \ll_\delta N^{-\varepsilon' \left(\frac{\log N}{t}\right)^2},$$

for some $\varepsilon' = \varepsilon'(\delta) > 0$.

Idea of the proof

- Dealing with exponential terms
  Let τ_s be the order of g modulo 2^s. Then

$$g^{\tau_s} = 1 + v2^s$$

Idea of the proof

- Dealing with exponential terms
  Let τ_s be the order of g modulo 2^s. Then

  $$g^{\tau_s} = 1 + v2^s$$

  and

  $$g^{n\cdot\tau_s} \equiv 1 + v\binom{n}{1}2^s + \cdots + v^k\binom{n}{k}2^{ks} \mod 2^t$$

  where $(k+1)s \geq t$.

Idea of the proof

- Dealing with exponential terms
  Let τ_s be the order of g modulo 2^s. Then

$$g^{\tau_s} = 1 + v2^s$$

  and

$$g^{n\cdot\tau_s} \equiv 1 + v\binom{n}{1}2^s + \cdots + v^k\binom{n}{k}2^{ks} \mod 2^t$$

  where $(k+1)s \geq t$.

  Thus $g^{n\cdot\tau_s}$ can be approximated by $f(n\,2^s)$ with $f(x) \in \mathbb{Q}[x]$.

Idea of the proof

- Dealing with exponential terms
  Let τ_s be the order of g modulo 2^s. Then

$$g^{\tau_s} = 1 + v2^s$$

  and

$$g^{n\cdot\tau_s} \equiv 1 + v\binom{n}{1}2^s + \cdots + v^k\binom{n}{k}2^{ks} \mod 2^t$$

  where $(k+1)s \geq t$.
  Thus $g^{n\cdot\tau_s}$ can be approximated by $f(n\,2^s)$ with $f(x) \in \mathbb{Q}[x]$.

- Shift and average method:

$$\sum_{n=0}^{N-1} \exp\left(h\frac{2\pi i u_n}{2^t}\right) \approx \frac{1}{2^s}\sum_{n=0}^{N-1}\sum_{x=0}^{2^s-1} \exp\left(h\frac{2\pi i u_{n+x\cdot\tau_s}}{2^t}\right)$$

Thank you!