Noncommutative algebraic dynamics

Vladimir Anashin

Institute for Information Security

Lomonosov Moscow State University

Statement and motivation

Let $\mathcal{G} = \langle G, \Omega \rangle$ be a group G with a set of operators Ω; let $w(x)$ be a *polynomial* over $\mathcal{G}$; that is

$$w(x) = g_1 x^{n_1 \omega_1} g_2 x^{n_2 \omega_2} \dots g_k x^{n_k \omega_k} g_k,$$

where $n_i \in \mathbb{Z}$, $\omega_i \in \Omega$, $g_i \in G$.

Problem: under what conditions the transformation

$$a \mapsto w(a) \quad (a \in G)$$

is ergodic?

Statement and motivation

Motivation: there are ciphers that use a sequence $S_1, S_2, \ldots$ of permutations to encrypt a message

$$\alpha_1 \alpha_2 \ldots$$

(here α's are letters of a certain alphabet). Thus

$$S_1(\alpha_1) S_2(\alpha_2) \ldots$$

is an encrypted message; one uses a sequence of inverse permutations $S_1^{-1}, S_2^{-1}, \ldots$ to decrypt a message.

The cipher is provably secure whenever the sequence $S_1, S_2, \ldots$ is random.

Statement and motivation

Goal: we are seeking for an algorithm that produces pseudorandom sequence of permutations.

The trajectory

$$a_0 = a,\ a_1 = w(a_0),\ a_2 = w(a_1), \ldots,$$

where w is an ergodic polynomial over a group G , is a good candidate to a pseudorandom sequence of permutations.

Which groups?

Which groups admit ergodic polynomial transformations?

Which groups?

Which groups admit ergodic polynomial transformations?

E.g., these are *polynomially complete groups*; that is, groups G (with no non-identical operators) such that *every* map $G \to G$ could be represented by a polynomial.

Which groups?

Which groups admit ergodic polynomial transformations?

A group G is polynomially complete if and only G it is a finite simple non-Abelian group, or $|G| = 2$.

Which groups?

Which groups admit ergodic polynomial transformations?

A group G is polynomially complete if and only G it is a finite simple non-Abelian group, or $|G| = 2$.

To characterize ergodic polynomials on finite simple non-Abelian groups seems to be an infeasible problem!

Which groups?

Which groups admit ergodic polynomial transformations?

A group G is polynomially complete if and only G it is a finite simple non-Abelian group, or $|G| = 2$.

To characterize ergodic polynomials on finite simple non-Abelian groups seems to be an infeasible problem!

If $w(x)$ is an ergodic polynomial over a finite group G, if $G \triangleright N$, $n = |G : N|$, then $w^n(x)$ is ergodic on N. Moreover, G/N admits ergodic polynomial transform. If N is minimal and non-Abelian, then N is a Cartesian product of pairwise isomorphic finite simple non-Abelian groups.

Which groups?

Which groups admit ergodic polynomial transformations?

A group G is polynomially complete if and only G it is a finite simple non-Abelian group, or $|G| = 2$.

To characterize ergodic polynomials on finite simple non-Abelian groups seems to be an infeasible problem!

Hence, one could hope to characterize ergodic polynomials for a finite group G, *only if* G does not contain simple non-Abelian sections, that is, if G is a *solvable* group!

Ergodicity on Abelian groups

Theorem. *An ergodic polynomial over a finite Abelian group G with a set of operators Ω exists if and only if G is one of the following groups:*

(i) *a cyclic group with an arbitrary set of operators,*

(ii) *the Klein group K_4, with a certain operator from Ω inducing an involution on G,*

(iii) *a direct product of a group of type* (ii) *by a group of type* (i) *of odd order.*

Ergodicity on nilpotent groups

Theorem. *An ergodic polynomial over a finite nilpotent group G with a set of operators $\Omega = \{Id\}$ exists if and only if G is isomorphic to one of the following groups:*

- $\mathrm{C}_m(a)$, *a cyclic group of order* m (generated by a)*;*

Ergodicity on nilpotent groups

Theorem. *An ergodic polynomial over a finite nilpotent group G with a set of operators $\Omega = Aut(G)$ exists if and only if G is isomorphic to one of the following groups:*

- $\mathrm{C}_m(a)$, *a cyclic group of order* m (generated by a);
- $\mathrm{D}_n^k = \mathrm{gp}\,(u, v \parallel v^{2^n} = 1,\ v^u = v^{-1},\ u^2 = v^{2^k})$, *where* $n = 1, 2, 3, \ldots$, *and* $k \in \{n, n-1\}$ *for* $n > 1$ *and* $k = 1$ *for* $n = 1$ (Note: $\mathrm{D}_1^1 = \mathrm{K}_4$, $\mathrm{D}_2^1 = \mathrm{Q}_8$ — quaternion group of order 8, D_n^{n-1} — generalized quaternion group of order 2^{n+1}, $\mathrm{D}_n^n = \mathrm{D}_{2^{n+1}}$ — dihedral group of order 2^{n+1});
- $H \times \mathrm{C}_m(a)$, *where* $H \in \{\mathrm{D}_n^k\}$ *and* m *is odd.*

Ergodicity on nilpotent groups

Theorem. *An ergodic polynomial over a finite nilpotent group G with a set of operators $\Omega = End(G)$ exists if and only if G is isomorphic to one of the following groups:*

- $\mathrm{C}_m(a)$, *a cyclic group of order* m (generated by a);
- $\mathrm{D}_n^k = \mathrm{gp}\,(u, v \parallel v^{2^n} = 1,\ v^u = v^{-1},\ u^2 = v^{2^k})$, *where* $n = 1, 2, 3, \ldots$, *and* $k \in \{n, n-1\}$ *for* $n > 1$ *and* $k = 1$ *for* $n = 1$ (Note: $\mathrm{D}_1^1 = \mathrm{K}_4$, $\mathrm{D}_2^1 = \mathrm{Q}_8$ — quaternion group of order 8, D_n^{n-1} — generalized quaternion group of order 2^{n+1}, $\mathrm{D}_n^n = \mathrm{D}_{2^{n+1}}$ — dihedral group of order 2^{n+1});
- $\mathrm{SD}_n = \mathrm{gp}\,(u, v \parallel u^2 = v^{2^n} = 1,\ v^u = v^{2^{n-1}-1})$, *where* $n = 3, 4, 5, \ldots$ (a semidihedral group);
- $H \times \mathrm{C}_m(a)$, *where* $H \in \{\mathrm{D}_n^k, \mathrm{SD}_n\}$ *and* m *is odd.*

Ergodicity on solvable groups

- $M(m,k,s) = \mathrm{C}_k(d) \leftthreetimes \mathrm{C}_m(c) = \mathrm{gp}\,(c,\, d \parallel c^m = d^k = 1,\, d^c = d^s)$, where $m, k = 2, 3, 4, \ldots$, $s \not\equiv 1 \pmod{k}$, $s^m = 1 \pmod{k}$, m and k are coprime;

Ergodicity on solvable groups

- $M(m,k,s) = \mathrm{C}_k(d) \leftthreetimes \mathrm{C}_m(c) = \mathrm{gp}\,(c,\, d \parallel c^m = d^k = 1,\, d^c = d^s)$, where $m, k = 2, 3, 4, \ldots$, $s \not\equiv 1 \pmod{k}$, $s^m = 1 \pmod{k}$, m and k are coprime;
- $A(r) = K_4 \leftthreetimes \mathrm{C}_{3^r}(b) = \mathrm{gp}\,(b,\, u,\, v \parallel b^{3^r} = u^2 = v^2 = 1,\, uv = vu,\, u^b = v,\, v^b = uv)$;

Ergodicity on solvable groups

- $M(m,k,s) = \mathrm{C}_k(d) \leftthreetimes \mathrm{C}_m(c) = \mathrm{gp}\,(c,\, d \parallel c^m = d^k = 1,\, d^c = d^s)$, where $m, k = 2, 3, 4, \ldots$, $s \not\equiv 1 \pmod{k}$, $s^m = 1 \pmod{k}$, m and k are coprime;
- $A(r) = K_4 \leftthreetimes \mathrm{C}_{3^r}(b) = \mathrm{gp}\,(b,\, u,\, v \parallel b^{3^r} = u^2 = v^2 = 1,\, uv = vu,\, u^b = v,\, v^b = uv)$;
- $\mathrm{S}(r) = \mathrm{A}(r) \leftthreetimes \mathrm{C}_2(a)$, where $b^a = b^{-1}$, $u^a = u$, $v^a = uv$;

Ergodicity on solvable groups

- $M(m,k,s) = \mathrm{C}_k(d) \leftthreetimes \mathrm{C}_m(c) = \mathrm{gp}\,(c,\, d \parallel c^m = d^k = 1,\, d^c = d^s)$, where $m, k = 2, 3, 4, \ldots$, $s \not\equiv 1 \pmod{k}$, $s^m = 1 \pmod{k}$, m and k are coprime;
- $A(r) = K_4 \leftthreetimes \mathrm{C}_{3^r}(b) = \mathrm{gp}\,(b,\, u,\, v \parallel b^{3^r} = u^2 = v^2 = 1,\, uv = vu,\, u^b = v,\, v^b = uv)$;
- $\mathrm{S}(r) = \mathrm{A}(r) \leftthreetimes \mathrm{C}_2(a)$, where $b^a = b^{-1}$, $u^a = u$, $v^a = uv$;
- $\mathrm{H}(r) = \mathrm{Q}_8 \leftthreetimes \mathrm{C}_{3^r}(b) = \mathrm{gp}\,(b, u, v \parallel b^{3^r} = u^4 = v^4 = 1, u^2 = v^2, u^b = v^{-1}, v^b = uv^{-1})$;

Ergodicity on solvable groups

- $M(m,k,s) = \mathrm{C}_k(d) \leftthreetimes \mathrm{C}_m(c) = \mathrm{gp}\,(c,\, d \parallel c^m = d^k = 1,\, d^c = d^s)$, where $m, k = 2, 3, 4, \ldots$, $s \not\equiv 1 \pmod{k}$, $s^m = 1 \pmod{k}$, m and k are coprime;
- $A(r) = K_4 \leftthreetimes \mathrm{C}_{3^r}(b) = \mathrm{gp}\,(b,\, u,\, v \parallel b^{3^r} = u^2 = v^2 = 1,\, uv = vu,\, u^b = v,\, v^b = uv)$;
- $\mathrm{S}(r) = \mathrm{A}(r) \leftthreetimes \mathrm{C}_2(a)$, where $b^a = b^{-1}$, $u^a = u$, $v^a = uv$;
- $\mathrm{H}(r) = \mathrm{Q}_8 \leftthreetimes \mathrm{C}_{3^r}(b) = \mathrm{gp}\,(b, u, v \parallel b^{3^r} = u^4 = v^4 = 1, u^2 = v^2, u^b = v^{-1}, v^b = uv^{-1})$;
- $\mathrm{Q}_1(r) = \mathrm{H}(r) \leftthreetimes \mathrm{C}_2(a)$, where $b^a = b^{-1}$, $u^a = u$, $v^a = uv$;

Ergodicity on solvable groups

- $M(m,k,s) = \mathrm{C}_k(d) \leftthreetimes \mathrm{C}_m(c) = \mathrm{gp}\,(c,\, d \parallel c^m = d^k = 1,\, d^c = d^s)$, where $m, k = 2, 3, 4, \ldots$, $s \not\equiv 1 \pmod{k}$, $s^m = 1 \pmod{k}$, m and k are coprime;
- $A(r) = K_4 \leftthreetimes \mathrm{C}_{3^r}(b) = \mathrm{gp}\,(b,\, u,\, v \parallel b^{3^r} = u^2 = v^2 = 1,\, uv = vu,\, u^b = v,\, v^b = uv)$;
- $\mathrm{S}(r) = \mathrm{A}(r) \leftthreetimes \mathrm{C}_2(a)$, where $b^a = b^{-1}$, $u^a = u$, $v^a = uv$;
- $\mathrm{H}(r) = \mathrm{Q}_8 \leftthreetimes \mathrm{C}_{3^r}(b) = \mathrm{gp}\,(b, u, v \parallel b^{3^r} = u^4 = v^4 = 1, u^2 = v^2, u^b = v^{-1}, v^b = uv^{-1})$;
- $\mathrm{Q}_1(r) = \mathrm{H}(r) \leftthreetimes \mathrm{C}_2(a)$, where $b^a = b^{-1}$, $u^a = u$, $v^a = uv$;
- $\mathrm{Q}_2(r) = \mathrm{gp}\,(a,\, b,\, u,\, v \parallel b^{3^r} = v^4 = 1, b^a = b^{-1}, u^a = u^{-1}, v^a = uv, u^b = v^u = v^{-1}, v^b = uv^{-1}, a^2 = u^2 = v^2)$

Ergodicity on solvable groups

Theorem. *An ergodic polynomial over a finite solvable group G with a set of operators $\Omega = \{Id\}$ exists if and only if $G = B \leftthreetimes A$, where orders of A and B are coprime, and*

$$A \in \{\mathrm{E}, \mathrm{S}(r), \mathrm{Q}_1(r), \mathrm{Q}_2(r)\}$$

$$B \in \{\mathrm{E}, \mathrm{C}_k, \mathrm{M}(m, k, s)\}$$

Ergodicity on solvable groups

Theorem. *An ergodic polynomial over a finite solvable group G with a set of operators $\Omega = Aut(G)$ exists if and only if $G = B \leftthreetimes A$, where orders of A and B are coprime, and*

$$A \in \{\mathrm{E}, \mathrm{S}(r), \mathrm{Q}_1(r), \mathrm{Q}_2(r), \mathrm{A}(r), \mathrm{D}_n^k\}$$

$$B \in \{\mathrm{E}, \mathrm{C}_k, \mathrm{M}(m, k, s)\}$$

Note: In this case action A on B is specified; not every action is admitted.

Ergodicity on solvable groups

Theorem. *An ergodic polynomial over a finite solvable group G with a set of operators $\Omega = End(G)$ exists if and only if $G = B \leftthreetimes A$, where orders of A and B are coprime, and*

$$A \in \{\mathrm{E}, \mathrm{S}(r), \mathrm{Q}_1(r), \mathrm{Q}_2(r), \mathrm{A}(r), \mathrm{D}_n^k, \mathrm{SD}_m\}$$

$$B \in \{\mathrm{E}, \mathrm{C}_k, \mathrm{M}(m, k, s)\}$$

Ergodicity on pro-2-group D_∞

$$\mathrm{D}_\infty \cdots \xrightarrow{\varphi_{n+1}} \mathrm{D}_{2^n} \xrightarrow{\varphi_n} \mathrm{D}_{2^{n-1}} \xrightarrow{\varphi_{n-1}} \ldots \xrightarrow{\varphi_4} \mathrm{D}_8$$

$$\mathrm{Ker}\,\varphi_n = Z(\mathrm{D}_{2^n}) = \{1, v^{2^{n-2}}\}$$

$$\mathrm{D}_{2^n} = (\mathbb{Z}/2^{n-1}\mathbb{Z})^+ \leftthreetimes (\mathbb{Z}/2\mathbb{Z})^+$$

$$\mathrm{D}_\infty = \mathbb{Z}_2^+ \leftthreetimes (\mathbb{Z}/2\mathbb{Z})^+$$

Ergodicity on pro-2-group D_∞

$$\mathrm{D}_\infty \cdots \xrightarrow{\varphi_{n+1}} \mathrm{D}_{2^n} \xrightarrow{\varphi_n} \mathrm{D}_{2^{n-1}} \xrightarrow{\varphi_{n-1}} \ldots \xrightarrow{\varphi_4} \mathrm{D}_8$$

$$\operatorname{Ker} \varphi_n = Z(\mathrm{D}_{2^n}) = \{1, v^{2^{n-2}}\}$$

$$\mathrm{D}_{2^n} = (\mathbb{Z}/2^{n-1}\mathbb{Z})^+ \leftthreetimes (\mathbb{Z}/2\mathbb{Z})^+$$

$$\mathrm{D}_\infty = \mathbb{Z}_2^+ \leftthreetimes (\mathbb{Z}/2\mathbb{Z})^+$$

Theorem. *A polynomial over the group* D_∞ *with the set of operators* $Aut(\mathrm{D}_\infty)$ *is ergodic* (with respect to the Haar measure) *if and only if it is ergodic on* D_8.

Some applications

In computer programs, realization of a certain operations depend on the value of the one-bit registers, called “flags."

For instance, if the value of a flag is equal to 0, then addition is carried out, and if it is 1, then subtraction is carried out.

Some applications

This way, the $*$ operation of the dihedral group appears in computer calculations:

If ε, ξ are values of flags, a, b are n-bit words in the alphabet $\{0, 1\}$, then $(\varepsilon, a) * (\xi, b) = (\varepsilon \oplus \xi, b + (-1)^{\xi} a)$, where $\oplus$ is addition modulo 2.

Some applications

Automorphisms are special word substitutions; these could be implemented as subroutines or via look-up tables.

Some applications

This way, a polynomial over a dihedral group D_{2^n} with the set of operators $Aut(\mathrm{D}_{2^n})$ could be implemented as a computer program that produces a pseudorandom sequence of group elements.

This sequence could be treated as a sequence of permutations, or as a sequence of $(n+1)$-bit words.

Some applications

The results presented in the talk expand the set of instructions that could be used to develop computer programs that produce uniformly distributed sequences.

Earlier results on ergodic transformations of $\mathbb{Z}_2$ could be applied to develop programs based on arithmetic and/or bitwise logical instructions only; results presented now add operations with flags to the list of possible instructions.

Remarks on machinery

In study of ergodic transformations of $\mathbb{Z}_p$ we used the 4p4-adic differential calculus; for instance:

A polynomial $f(x) \in \mathbb{Z}_p[x]$ preserves the Haar measure if and only if

- *f is bijective modulo p* (i.e., on $\mathbb{Z}_p/p\mathbb{Z}_p$), *and*
- *f' vanishes modulo p nowhere on $\mathbb{Z}_p$.*

Remarks on machinery

Given $f(x) \in \mathbb{Z}_p[x]$, for all $h \in \mathbb{Z}_p$,

$$f(x+h) \equiv f(x) + hf'(x) \pmod{p^{\operatorname{ord}_p h + 1}}$$

Remarks on machinery

Given $f(x) \in \mathbb{Z}_p[x]$, for all $h \in \mathbb{Z}_p$,

$$f(x+h) \equiv f(x) + hf'(x) \pmod{p^{\operatorname{ord}_p h + 1}}$$

If A is a minimal normal subgroup of a finite group G, and if A is Abelian, then A is the additive group of a vector space over $\mathbb{Z}/p\mathbb{Z}$.

Remarks on machinery

Given $f(x) \in \mathbb{Z}_p[x]$, for all $h \in \mathbb{Z}_p$,

$$f(x+h) \equiv f(x) + hf'(x) \pmod{p^{\operatorname{ord}_p h + 1}}$$

Given $w(x) \in G[x]$ (a polynomial over a group G), for all $h \in A$,

$$w(xh) = w(x)h^{w'(x)},$$

where $w'(x) \in End(A)$, the *Fox derivative* of $w(x)$.

Remarks on machinery

Given $f(x) \in \mathbb{Z}_p[x]$, for all $h \in \mathbb{Z}_p$,

$$f(x+h) \equiv f(x) + hf'(x) \pmod{p^{\operatorname{ord}_p h + 1}}$$

Given $w(x) \in G[x]$ (a polynomial over a group G), for all $h \in A$,

$$w(xh) = w(x)h^{w'(x)},$$

where $w'(x) \in End(A)$, the *Fox derivative* of $w(x)$.

$\frac{\partial x}{\partial x} = 1$;

$\frac{\partial g}{\partial x} = 0$ for any $g \in G$;

$\frac{\partial uv}{\partial x} = \frac{\partial u}{\partial x}v + \frac{\partial v}{\partial x}$ for any $u, v \in G[x]$.

Remarks on machinery

Given $f(x) \in \mathbb{Z}_p[x]$, for all $h \in \mathbb{Z}_p$,

$$f(x+h) \equiv f(x) + hf'(x) \pmod{p^{\operatorname{ord}_p h + 1}}$$

Given $w(x) \in G[x]$ (a polynomial over a group G), for all $h \in A$,

$$w(xh) = w(x)h^{w'(x)},$$

where $w'(x) \in End(A)$, the *Fox derivative* of $w(x)$.

Example: Let $w(x) = ax^2bx^{-1}c$, then

$$w(xh) = w(x)h^{xbx^{-1}c + bx^{-1}c - x^{-1}c}$$

Remarks on machinery

Given $f(x) \in \mathbb{Z}_p[x]$, for all $h \in \mathbb{Z}_p$,

$$f(x+h) \equiv f(x) + hf'(x) \pmod{p^{\operatorname{ord}_p h + 1}}$$

Given $w(x) \in G[x]$ (a polynomial over a group G), for all $h \in A$,

$$w(xh) = w(x)h^{w'(x)},$$

where $w'(x) \in End(A)$, the *Fox derivative* of $w(x)$.

Theorem: *A polynomial $w(x) \in G[x]$ is bijective on G if and only if*

- *w is bijective modulo A* (i.e., on G/A)*, and*
- *w' is a non-singular linear transformation of A.*

Remarks on machinery

Given $f(x) \in \mathbb{Z}_p[x]$, for all $h \in \mathbb{Z}_p$,

$$f(x+h) \equiv f(x) + hf'(x) \pmod{p^{\operatorname{ord}_p h + 1}}$$

Given $w(x) \in G[x]$ (a polynomial over a group G), for all $h \in A$,

$$w(xh) = w(x)h^{w'(x)},$$

where $w'(x) \in End(A)$, the *Fox derivative* of $w(x)$.

'Template theorem': *Let $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots E$, let all $G_i/G_{i+1} = A_i$ be Abelian groups. A polynomial $w(x) \in G[x]$ 'preserves measure' on G whenever $w(x)$ is bijective on A_1, and $w'(x) \in \operatorname{Aut} A_i$ for all x, $i = 2, 3, 4, \ldots$.*