Can quasigroup transformations of random variables be spoofed?

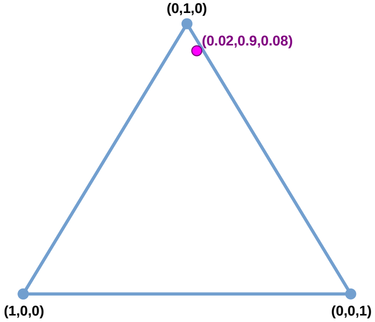
Alexey D. Yashunsky

Keldysh Institute of Applied Mathematics
Moscow, Russia

July 8, 2019

Random variables

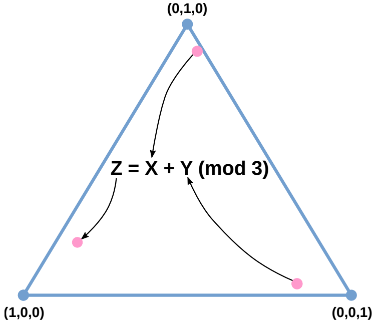
- $E_k = \{0, 1, 2, \ldots, k-1\}$
- $\mathrm{P}\{X = 0\} = p_0, \ldots, \mathrm{P}\{X = k-1\} = p_{k-1}$
- $p_0 \geq 0, \ldots, p_{k-1} \geq 0, \quad \sum_{i=0}^{k-1} p_i = 1$
- $X \sim \mathbf{p} = (p_0, \ldots, p_{k-1}) \in \mathbf{S}^{(k)}, \quad \mu(\mathbf{p}) = \{i \in E_k \mid p_i > 0\}$



Algebraic transformations

- $X \sim (p_0, p_1, p_2)$,
  $Y \sim (q_0, q_1, q_2)$
- $Z = X + Y \pmod 3$

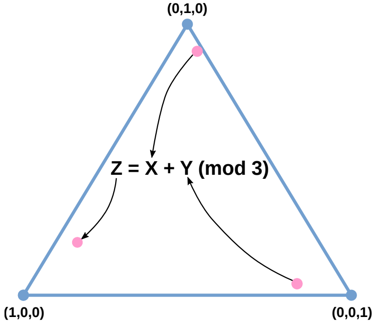
$$Z \sim (p_0 q_0 + p_1 q_2 + p_2 q_1,\\ p_0 q_1 + p_1 q_0 + p_2 q_2,\\ p_0 q_2 + p_1 q_1 + p_2 q_0)$$



Algebraic transformations

- $X \sim (p_0, p_1, p_2)$,
  $Y \sim (q_0, q_1, q_2)$
- $Z = X + Y \pmod 3$

$$Z \sim (p_0 q_0 + p_1 q_2 + p_2 q_1,\; p_0 q_1 + p_1 q_0 + p_2 q_2,\; p_0 q_2 + p_1 q_1 + p_2 q_0)$$



- $X_1 \sim \mathbf{p}^{(1)}, \dots, X_n \sim \mathbf{p}^{(n)}$
- $f(x_1, \dots, x_n) \colon E_k^n \to E_k$
- $f(X_1, \dots, X_n) \sim \widehat{f}(\mathbf{p}^{(1)}, \dots, \mathbf{p}^{(n)})$
- $\widehat{f}(\mathbf{p}^{(1)}, \dots, \mathbf{p}^{(n)}) \colon \left(\mathbf{S}^{(k)}\right)^n \to \mathbf{S}^{(k)}$

Identities

$$(r_0, \ldots, r_{k-1}) = \mathbf{r} = \widehat{f}(\mathbf{p}^{(1)}, \ldots, \mathbf{p}^{(n)})$$

$$r_i = \sum_{f(j_1,\ldots,j_n)=i} p^{(1)}_{j_1} \cdots p^{(n)}_{j_n}$$

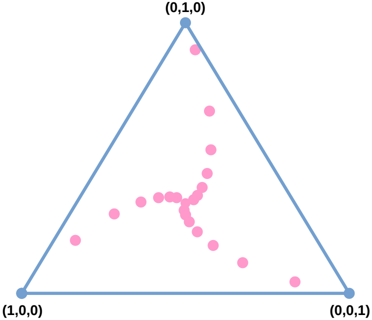
$$x \circ y = y \circ x \qquad \mathbf{p} \mathbin{\widehat{\circ}} \mathbf{q} = \mathbf{q} \mathbin{\widehat{\circ}} \mathbf{p}$$

$$x \circ (y \circ z) = (x \circ y) \circ z \qquad \mathbf{p} \mathbin{\widehat{\circ}} (\mathbf{q} \mathbin{\widehat{\circ}} \mathbf{r}) = (\mathbf{p} \mathbin{\widehat{\circ}} \mathbf{q}) \mathbin{\widehat{\circ}} \mathbf{r}$$

$$x \backslash (x \circ y) = y \qquad \mathbf{p} \mathbin{\widehat{\backslash}} (\mathbf{p} \mathbin{\widehat{\circ}} \mathbf{q}) \neq \mathbf{q}$$

Distribution algebras

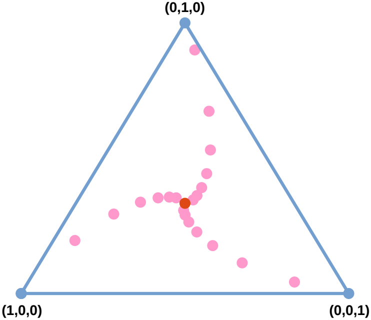
- $B = \{f_i\colon E_k^{n_i} \to E_k\}_{i \in I}, \quad \mathbf{G} \subseteq \mathbf{S}^{(k)}$
- $\mathcal{H} = \left\{ \mathbf{H} \;\middle|\; \begin{array}{l} \mathbf{G} \subseteq \mathbf{H}; \quad \forall \mathbf{h}^{(1)}, \ldots, \mathbf{h}^{(n)} \in \mathbf{H}, \\ f \in B \Rightarrow \widehat{f}(\mathbf{h}^{(1)}, \ldots, \mathbf{h}^{(n)}) \in \mathbf{H} \end{array} \right\}$
- $V_B(\mathbf{G}) = \bigcap_{\mathbf{H} \in \mathcal{H}} \mathbf{H}$



Limit points

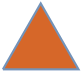
$\rho(\mathbf{g}, \mathbf{h})$ – a metric on $\mathbf{S}^{(k)}$

$$\lambda(\mathbf{G}) = \{\mathbf{q} \mid \forall \varepsilon > 0\ \exists \mathbf{g} \in \mathbf{G} \colon 0 < \rho(\mathbf{q}, \mathbf{g}) < \varepsilon\}$$



$$|\mu(\mathbf{p})| > 1, B = \{1, +, \times, x^2, \ldots, x^{k-1}\}$$

$$\lambda(V_B(\{\mathbf{p}\})) = \mathbf{S}^{(k)}$$



Quasigroup transformations

Markovski, Gligoroski, Bakeva '99

- $B = \{\circ_1, \ldots, \circ_l\} \subset$ binary quasigroup operations on E_k
- $|\mu(\mathbf{p})| = k$
- $\mathbf{C} = \{(\ldots((\mathbf{p} \,\widehat{\circ}_{j_1}\, \mathbf{p}) \,\widehat{\circ}_{j_2}\, \mathbf{p}) \ldots \widehat{\circ}_{j_m}\, \mathbf{p})\}_{m \in \mathbb{N}, j_1, \ldots, j_m \in \{1, \ldots, l\}}$

$\lambda(\mathbf{C}) = \left\{ \left(\frac{1}{k}, \ldots, \frac{1}{k} \right) \right\}$

$\mathbf{C} \subseteq V_B(\{\mathbf{p}\})$

Quasigroup transformations

Markovski, Gligoroski, Bakeva '99

- $B = \{\circ_1, \ldots, \circ_l\} \subset$ binary quasigroup operations on E_k
- $|\mu(\mathbf{p})| = k$
- $\mathbf{C} = \{(\ldots((\mathbf{p} \,\widehat{\circ}_{j_1}\, \mathbf{p}) \,\widehat{\circ}_{j_2}\, \mathbf{p}) \ldots \widehat{\circ}_{j_m}\, \mathbf{p})\}_{m \in \mathbb{N}, j_1, \ldots, j_m \in \{1, \ldots, l\}}$

$\lambda(\mathbf{C}) = \left\{\left(\frac{1}{k}, \ldots, \frac{1}{k}\right)\right\}$

$\mathbf{C} \subseteq V_B(\{\mathbf{p}\})$

Yashunsky '13

- $B = \{\circ_1, \ldots, \circ_l\} \subset$ binary quasigroup operations on E_k
- $|\mu(\mathbf{p})| > \frac{k}{2}$

$\lambda(V_B(\{\mathbf{p}\})) = \left\{\left(\frac{1}{k}, \ldots, \frac{1}{k}\right)\right\}$

$f(x_1, \ldots, x_n)\colon E_k^n \to E_k$ is an *n-ary quasigroup operation* if $\forall i = 1, \ldots, n, \forall \alpha_1, \ldots, \alpha_{n-1} \in E_k$ the function

$$\varphi(x) = f(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_i, \ldots, \alpha_n)$$

is a permutation on E_k.

n-ARY QUASIGROUP TRANSFORMATIONS

$f(x_1,\dots,x_n)\colon E_k^n \to E_k$ is an *n-ary quasigroup operation* if $\forall i = 1,\dots,n, \forall \alpha_1,\dots,\alpha_{n-1} \in E_k$ the function

$$\varphi(x) = f(\alpha_1,\dots,\alpha_{i-1},x,\alpha_i,\dots,\alpha_n)$$

is a permutation on E_k.

Theorem

- $B = \{f_1,\dots,f_l\} \subset$ *quasigroup operations on* E_k
- $B \ni f, f$ *has arity* > 1
- $\mathbf{G} \subset \mathbf{S}^{(k)}$, $|\mathbf{G}| < \infty$, $\forall \mathbf{g} \in \mathbf{G}\colon |\mu(\mathbf{g})| > \frac{k}{2}$

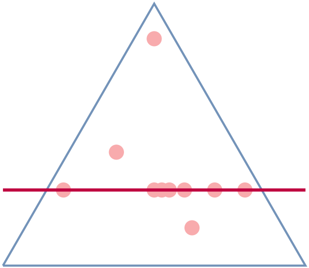
$$\lambda(V_B(\{\mathbf{G}\})) = \left\{\left(\frac{1}{k},\dots,\frac{1}{k}\right)\right\}$$

Some geometry

Affine hull: $\mathrm{Aff}(\mathbf{H}) = \left\{ \sum \alpha_i \mathbf{h}^{(i)} \mid \lambda_i \in \mathbb{R}, \mathbf{h}^{(i)} \in \mathbf{H}, \sum \alpha_i = 1 \right\}$

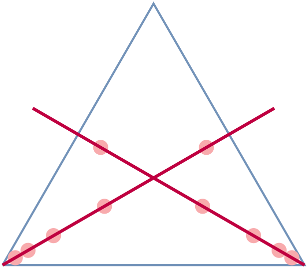
Essentially flat set $\mathbf{H}$

$$\exists \mathbf{H}',\ |\mathbf{H}'| < \infty :$$
$$\mathbf{S}^{(k)} \not\subset \mathrm{Aff}(\mathbf{H} \setminus \mathbf{H}')$$



X-set $\mathbf{H}$

$$\mathbf{H} \subseteq \mathbf{H}' \cup \mathbf{H}''$$
$$\mathbf{S}^{(k)} \not\subset \mathrm{Aff}(\mathbf{H}'), \mathrm{Aff}(\mathbf{H}'')$$



Single limit point

Theorem

- $\mathbf{H} \subset \mathbf{S}^{(k)},\ V_B(\mathbf{H}) = \mathbf{H}$
- $\lambda(\mathbf{H}) = \{\mathbf{q}\}$
- $|\mu(\mathbf{q})| = k$
- $B \ni f, f$ *has arity* > 1
- $\mathbf{H}$ *is neither essentially flat, nor an X-set*

$\mathbf{q} = \left(\frac{1}{k}, \ldots, \frac{1}{k}\right),\ B \subset$ *quasigroup operations on* E_k

Binary case

Yashunsky '18

- $\mathbf{H} \subset \mathbf{S}^{(2)},\ V_B(\mathbf{H}) = \mathbf{H}$
- $\lambda(\mathbf{H}) = \{\mathbf{q}\}$
- $|\mu(\mathbf{q})| = 2$
- $B \ni f, f$ has arity > 1

$$\mathbf{q} = \left(\tfrac{1}{2}, \tfrac{1}{2}\right), \quad f \in B \Rightarrow f = x_1 + \cdots + x_n + c \pmod 2$$

Binary case

Yashunsky '18

- $\mathbf{H} \subset \mathbf{S}^{(2)}, \ V_B(\mathbf{H}) = \mathbf{H}$
- $\lambda(\mathbf{H}) = \{\mathbf{q}\}$
- $|\mu(\mathbf{q})| = 2$
- $B \ni f, f$ has arity > 1

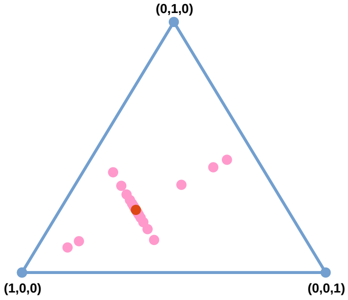
$\mathbf{q} = \left(\frac{1}{2}, \frac{1}{2}\right), \quad f \in B \Rightarrow f = x_1 + \cdots + x_n + c \pmod 2$

$\mathbf{H} \subset \mathbf{S}^{(2)}$ is essentially flat or an X-set $\Rightarrow |\mathbf{H}| = 1$

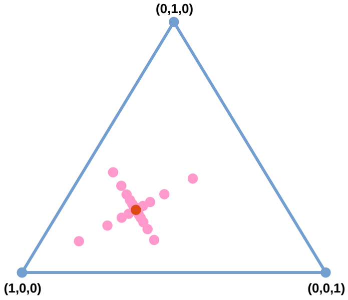
Exceptions

$$B = \{f\}$$

f	0	1	2
0	0	0	0
1	2	2	1
2	1	1	2



H is essentially flat



H is an X-set

Thank you!