Proper families of discrete functions: equivalent definitions and properties

K. Tsaregorodtsev[1, 2]

[1]Lomonosov Moscow State University
Moscow, Russia

[2]JSC "NPK Kryptonite"

Seminar on Computer Algebra, May 16, 2023

Outline

Table of Contents

Quasigroups

Definition

Quasigroup is a (nonempty) set Q with a binary operation on it:

$$\circ \colon Q \times Q \to Q,$$

which obeys the following property: for each $a, b \in Q$ there exist unique $x, y \in Q$ such that:

$$a \circ x = b, \qquad y \circ a = b.$$

Equivalently, operations of left and right multiplication

$$L_a \colon Q \to Q,\ L_a(x) = a \circ x,$$

$$R_a \colon Q \to Q,\ R_a(y) = y \circ a,$$

are bijections on Q.
Essentially, "a group" without associativity and identity.
We are interested in finite quasigroups Q.

Latin squares

Informally: square table of size $k \times k$ filled with numbers $\{0, \ldots, k-1\}$, such that each number occurs *exactly once* in each row and each column.

Example: 5×5 latin square

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 3 & 4 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 1 & 2 & 0 \\ 4 & 2 & 0 & 1 & 3 \end{bmatrix}$$

Latin squares are multiplication tables of quasigroups.

d-Quasigroups

Definition

A pair (Q, g), where $g\colon Q^d \to Q$ is invertible in any variable, $d \geq 2$, Q is a nonempty finite set is called a d-quasigroup; g is called d-quasigroup operation.

Multiplication "tables" of d-quasigroups are *latin cubes.*

Remark

"Usual" quasigroup is a d-quasigroup with $d = 2$.

Quasigroup operation: example

$Q = \mathbb{E}_k$, $g(x_1, \ldots, x_d) = x_1 + \ldots + x_d + const$.

Notations to be used

Q	a set or quasigroup with a binary operation $\circ$
k	size of a "basic" set $k = \|Q\|$
$\mathbb{E}_k$	a set $\{0, \ldots, k-1\}$ (usually equipped with $+$ operation modulo k)
F	Family of functions $F\colon Q^n \to Q^n$
f_i	i-th function of a family F
n	size of a family
$Func(Q)$	a set of functions $f\colon Q \to Q$
$Perm(Q)$	a set of bijections on Q

Table of Contents

Shannon encryption

- Encrypting with one-time pad is perfectly secret:

$$m_i \to m_i \oplus k_i.$$

- Any quasigroup-based mapping is also OK:

$$m_i \to m_i \circ k_i,$$

  where $\circ$ is some quasigroup operation.
- Drawback: long keys.

More practical constructions

- Asymmetric primitives (DH-protocols, PKE schemes, FHE schemes, etc.) over non-associative structures, such as quasigroups / quasigroup rings[1].
- Stream-cipher-like constructions over quasigroups: Edon80[2], quasigroup string transformation[3].
- Hash functions[4].
- ZK-protocols, authentication schemes, ...

[1] Gribov, Zolotykh, and Mikhalev, "A construction of algebraic cryptosystem over the quasigroup ring"; Katyshev, Markov, and Nechaev, "Application of non-associative groupoids to the realization of an open key distribution procedure"; Katyshev, Zyazin, and Baryshnikov, "Application of non-associative structures for construction of homomorphic cryptosystems"; Markov, Mikhalev, and Nechaev, "Nonassociative Algebraic Structures in Cryptography and Coding".

[2] Gligoroski, Markovski, and Knapskog, "The stream cipher Edon80".

[3] Markovski and Bakeva, "Quasigroup string processing: Part 4".

[4] Gligoroski, Markovski, and Kocarev, "Edon-R, An Infinite Family of Cryptographic Hash Functions."; Gligoroski, Mihajloska, and Otte, "GAGE and InGAGE"; Gligoroski et al., "Cryptographic hash function Edon-R"'.

Algebraic structure and properties

- Hidden additional algebraic structure of quasigroups can drastically decrease the security of the cipher[5].
- Quasigroup is shapeless[6], if it is non-commutative, non-associative, it does not have neither left nor right unit, it does not contain proper sub-quasigroups, etc.
- In[7] quasigroups of sizes 2^ω are used, where ω is the length of the "word" to be processed (256 bit for the "usual" hash function).

[5] Slaminková and Vojvoda, "Cryptanalysis of a hash function based on isotopy of quasigroups"; Vojvoda, "Cryptanalysis of one hash function based on quasigroup".

[6] Gligoroski, Markovski, and Kocarev, "Edon-R, An Infinite Family of Cryptographic Hash Functions."

[7] Gligoroski, Markovski, and Kocarev, "Edon-R, An Infinite Family of Cryptographic Hash Functions."; Gligoroski et al., "Cryptographic hash function Edon-R"'.

Bottom line: what do we need?

- Moderately large quasigroups . . .
- . . . with some desirable properties, such as: polynomial completeness, minimal number of subquasigroups, quadraticity, small number of associative triples, etc.
- We are interested in *functional representation* of quasigroup operation: memory efficiency is needed.

Table of Contents

Proper family

A family of functions

Let Q be a finite nonempty set. A tuple of functions F:

$$F = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)),$$

where $f_i \colon Q^n \to Q$ is called a family of functions on Q^n.

Family F can be seen as a map $F \colon Q^n \to Q^n$.

Proper family

A family F is proper[a] if for any $\alpha \neq \beta \in Q^n$ it holds that

$$\exists i: \quad \alpha_i \neq \beta_i, \ f_i(\alpha) = f_i(\beta).$$

[a] Nosov, "Constructing a parametric family of Latin squares in the vector database", "Constructing Parametric Families of Latin Squares in the Boolean Database".

Example: constants

Proper family

A family F is proper if for any $\alpha \neq \beta \in Q^n$ it holds that

$$\exists i: \quad \alpha_i \neq \beta_i, \; f_i(\alpha) = f_i(\beta).$$

Essential (in)dependence

f_i does not depend essentially on x_i.

Constant family

$f_i \equiv const_i$ is proper.

Example: triangular family

Triangular family

Triangular family of size n is a family F such that

$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} const \\ f_2(x_1) \\ f3(x_1, x_2) \\ \vdots \\ f_n(x_1, \dots, x_{n-1}) \end{bmatrix}.$$

Triangular families are proper[8].

[8] Nosov and Pankratiev, “Latin squares over Abelian groups”.

Example: orthogonal families

Orthogonal families

Two functions $f, g\colon \mathbb{E}_k^n \to \mathbb{E}_k$ are **orthogonal**, if for any $x \in \mathbb{E}_k^n$ it holds that either $f(x) = 0$ or $g(x) = 0$.

Family of orthogonal functions

Let $F = (f_1, \ldots, f_n)$ be a family of pairwise orthogonal functions such that f_i does not depend essentially on x_i. Then F is proper[a]. For instance the family

$$\begin{aligned} f_1 &= \bar{x}_2 x_3 \cdots x_{n-1} x_n, \\ f_2 &= \bar{x}_3 x_4 \cdots x_n x_1, \\ &\vdots \\ f_n &= \bar{x}_1 x_2 \cdots x_{n-2} x_{n-1} \end{aligned} \tag{1}$$

on $\mathbb{E}_2^n$ is proper.

[a] Nosov and Pankratiev, "On functional representation of Latin squares".

Boolean case example

Quadratic family

The following Boolean family[a] is proper for any $n \geq 1$:

$$\begin{bmatrix} 0 \\ x_1 \\ x_1 \oplus x_2 \\ \vdots \\ x_1 \oplus x_2 \oplus \ldots \oplus x_{n-1} \end{bmatrix} \bigoplus \begin{bmatrix} \bigoplus_{i<j,\ i,j \neq 1}^{n} x_i x_j \\ \bigoplus_{i<j,\ i,j \neq 2}^{n} x_i x_j \\ \bigoplus_{i<j,\ i,j \neq 3}^{n} x_i x_j \\ \vdots \\ \bigoplus_{i<j,\ i,j \neq n}^{n} x_i x_j \end{bmatrix}; \tag{2}$$

[a] Tsaregorodtsev, "Properties of proper families of Boolean functions".

Multivariate quasigroup representation

- Assume that $|Q| = k^n$ for some $k, n \in \mathbb{N}$;
- elements of Q can be represented by n-tuples $(x_1, \ldots, x_n)$, $x_i \in \mathbb{E}_k$,
- quasigroup operation $\circ\colon Q \to Q$ can be treated as a $2n$-ary vector function from the k-valued logic; $z = x \circ y$ can be written in the form:

$$\begin{aligned} z_1 &= f_1(x_1, \ldots, x_n, y_1, \ldots, y_n) \\ z_2 &= f_2(x_1, \ldots, x_n, y_1, \ldots, y_n) \\ &\vdots \\ z_n &= f_n(x_1, \ldots, x_n, y_1, \ldots, y_n) \end{aligned} \tag{3}$$

  with $f_i \in P_k^{2n}$;
- in practice the most interesting case is $k = 2^t$ for some $t \in \mathbb{N}$, in particular $k = 2$ (Boolean representation).

Proper families specify quasigroups

- Assume that $h_1, \ldots, h_n$ are 3-quasigroup operations on $\mathbb{E}_k$, $g_1, \ldots, g_n$ are n-ary k-valued functions, $\pi_1, \ldots, \pi_n$ are k-valued functions of arity 2;
- consider a particular case of the relations (3):

$$\begin{aligned} z_1 &= h_1(x_1, y_1, g_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))) \\ z_2 &= h_2(x_2, y_2, g_2(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))) \\ &\vdots \\ z_n &= h_n(x_n, y_n, g_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n))) \end{aligned} \tag{4}$$

Theorem

The relations (4) **specify a quasigroup operation** *for any choice of the internal functions* $\pi_1, \ldots, \pi_n$ *if and only if the family* $(g_1, \ldots, g_n)$ **is proper**[a].

[a] Galatenko, Nosov, and Pankratiev, "Latin squares over quasigroups".

Benefits of proper family-based specification

Transition from specification (3) to proper family-based specification may reduce generality, however there are several essential advantages:

- unlike many existing constructions proper families can be used to generate d-quasigroups for any $d \geq 2$;
- transition from Cayley tables to proper families significantly decreases memory load;
- still the number of quasigroups and d-quasigroups generated is large (depends on the cardinality of the image of the corresponding proper family[9]).

[9] Galatenko et al., "Generation of n-quasigroups with the use of proper families of functions".

Table of Contents

Properness-preserving transformations: shifts

Theorem

For any $\alpha = (a_1, \ldots, a_n) \in Q^n$ *let us define the shift transformations*[a]*:*

$$x \in Q^n \to L_\alpha(x) = (a_1 \circ x_1, \ldots, a_n \circ x_n),$$

$$x \in Q^n \to R_\alpha(x) = (x_1 \circ a_1, \ldots, x_n \circ a_n).$$

If $F(x) = (f_1(x), \ldots, f_n(x))$ *is proper, then* $T_\alpha(F(T_\beta(x)))$ *is proper, where* $T \in \{L, R\}$, $\alpha, \beta \in Q^n$.

[a] Nosov and Pankratiev, "Latin squares over Abelian groups".

Properness-preserving transformations: reencoding

Theorem

For any $\Psi = (\psi_1, \dots, \psi_n) \in Func(Q, Q)^n$ *let us define the reencoding transformations:*

$$x \in Q^n \to \Psi(x) = (\psi_1(x_1), \dots, \psi_n(x_n)).$$

Let $\Phi \in Func(Q)^n$, $\Psi \in Perm(Q)^n$. *If* $F(x) = (f_1(x), \dots, f_n(x))$ *is proper, then* $\Phi(F(\Psi(x)))$ *is proper.*

If $\Phi, \Psi \in Perm(Q)^n$, then this transformation is called "reencoding".

Remark

Shifts are special case of these transformations.

Properness-preserving transformations: renumbering

Theorem

For any $\sigma \in Perm(n)$ *let us define the renumbering transformation:*

$$F \to \sigma(F),$$

$$f_i(x_1, \ldots, x_n) \to f_{\sigma(i)}(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

If $F(x)$ *is proper, then* $\sigma(F)$ *is proper*[a].

[a] Nosov and Pankratiev, "Latin squares over Abelian groups".

Properness-preserving transformations: "projections"

Theorem

For any $i \in \{1, \dots, n\}$ and any $a \in Q$ the family F' obtained from proper family F by substituting the value a for the variable x_i and cancelling the function f_i is a proper family[a] *of size $(n-1)$ (projection):*

$$F'(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) = \Pi_a^i(F) = \begin{bmatrix} f_1(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ \vdots \\ f_{i-1}(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ f_{i+1}(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \\ \vdots \\ f_n(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_n) \end{bmatrix}.$$

[a] Nosov and Pankratiev, "Latin squares over Abelian groups".

General type of bijective transformations

- Let Φ, Ψ be bijective transformations of Q^n: $\Phi, \Psi \in Perm(Q^n)$.
- Consider the stabilizer of the set of all proper families in $Perm(Q^n)$, i.e.

$$\{(\Phi, \Psi) \in Perm(Q^n) \mid \Phi(F(\Psi(x))) \text{ is proper for any proper } F\colon Q^n \to Q^n\}.$$

- Then Φ and Ψ must be isometries of $\mathbb{E}_k^n$ (Hamming metric).
- Isometries of $\mathbb{E}_k^n$ are reencodings and renumberings.
- These two classes preserve properness.
- Hence, no other transformations in the stabilizer of the set of proper functions: only reencodings and renumberings.

Table of Contents

Boolean cube $\mathbb{B}_n$ and USO

Boolean cube $\mathbb{B}_n$:

- vertices: $V = \{\alpha \in \mathbb{E}_2^n\}$;
- edges: $\{\alpha, \beta\} \in E$ iff $\rho(\alpha, \beta) = 1$ (Hamming distance).

Definition

Unique sink orientation (USO)[a] of $\mathbb{B}_n$ is an orientation of the edges of $\mathbb{B}_n$ such that in every subcube of $\mathbb{B}_n$ there is exactly one vertex for which all adjoining edges are oriented inward (i.e. towards that vertex).

[a] Szabo and Welzl, "Unique sink orientations of cubes".

USO: example

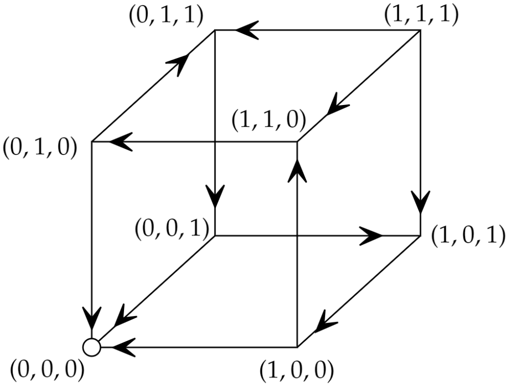


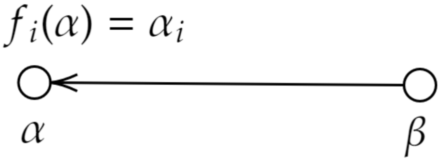
Figure: USO of a 3d-cube $\mathbb{B}_3$

Graph of a family $\Gamma(F)$

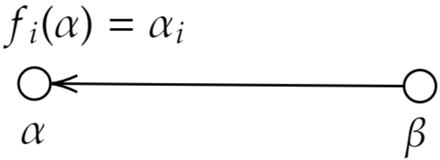
The graph of a family

Given a Boolean family F, we can construct the graph (the family graph $\Gamma(F)$).

- Vertices: $V = \{\alpha \in \mathbb{E}_2^n\}$.
- Given $\alpha \neq \beta$, $\rho(\alpha, \beta) = 1$, $\alpha_i \neq \beta_i$, we add an edge $(\beta, \alpha) \in E$ iff $f_i(\alpha) = \alpha_i$.



Fixed points



- What if α is a fixed point of the mapping $x \to F(x)$?
- Then $f_i(\alpha) = \alpha_i$ for any $1 \leq i \leq n$.
- Hence, α is a *sink* of $\Gamma(F)$.

Geometric characterization

Theorem

Graph $\Gamma(F)$ of a Boolean family F is USO iff F is proper[a].

[a] Tsaregorodtsev, "One-to-one correspondense between proper families of boolean functions and unique sink orientations of cubes".

- One-to-one correspondence between algebraic and geometric objects.
- "Translate" results from one language to another: randomized algorithms for proper families generation (MCMC)[10], estimates for the number of boolean proper families[11], construction of new classes of proper families.

[10] Galatenko et al., "Generation of proper families of functions"; Schurr, "Unique sink orientations of cubes".

[11] Tsaregorodtsev, "Properties of proper families of Boolean functions".

Example of "translation"

Recursively combed cube orientation

An orientation of $\mathbb{B}_n$ is recursively combed if there is at least one dimension along which all the edges go into the same direction and the two $(n-1)$-dimensional cube orientations resulting from the removal of all edges along that dimension are again recursively combed.

Recursively triangle families

$F\colon \mathbb{E}_k^n \to \mathbb{E}_k^n$ is recursively triangle, if there exists i, such that $f_i \equiv const_i$, and $\Pi_a^i(F)$ are recursively triangle for any $a \in \mathbb{E}_k$.

Theorem

Recursively triangle families are proper.

Table of Contents

Fixed points of proper families

Fixed points, boolean case

Boolean family F is proper iff for F and any of its *projections* there exists a unique fixed point.

This "fixed point" characterization gives rise to another alternative characterization, known as **HUFP (hereditarily unique fixed point) Boolean networks.**
There exist a generalization to the case of k-valued logic[12]:

Fixed points

Family $F\colon \mathbb{E}_k^n \to \mathbb{E}_k^n$ is proper iff for any reencoding $x \to \Phi(F(\Psi(x)))$ (i.e., $\Phi, \Psi \in Perm(Q)^n$) any of its *projections* has a unique fixed point.

[12] Galatenko et al., "Generation of proper families of functions".

Boolean network

- Essentially the same object as Boolean family of functions (i.e., $F\colon \mathbb{E}_2^n \to \mathbb{E}_2^n$).
- HUFP (hereditarily unique fixed point) Boolean network: F and all of its projections has unique fixed point.
- i.e., HUFP Boolean networks $=$ Boolean proper families.
- i.e., yet another language for the same object.

Global interaction graphs

Let F be a Boolean family of size n. Let us define the global interaction graph $G(F)$:

- Vertices: $V = \{1, \ldots, n\}$.
- Edges: $i \to j$ iff f_j depends essentially on x_i.
- Equivalently: discrete derivative of f_j w.r.t. x_i is not zero.

Theorem

If $G(F)$ is acyclic, then F is HUFP Boolean network.

Equivalently: if F is triangle Boolean family, then F is proper.

Local interaction graphs

Let F be a Boolean family of size n. Let us define local interaction graph $G(F, \alpha)$, where $\alpha \in \mathbb{E}_2^n$:

- Vertices: $V = \{1, \ldots, n\}$.
- Edges: $i \to j$ iff f_j depends essentially on x_i "locally in α":

$$f_j(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n) \neq f_j(\alpha_1, \ldots, \alpha_i \oplus 1, \ldots, \alpha_n).$$

Theorem

If $G(F, \alpha)$ is acyclic for every $\alpha \in \mathbb{E}_2^n$, then F is HUFP Boolean network.

Local interaction graphs-2

Using the notion of local interaction graphs, we can introduce a class of **locally triangle** families (for any $k \geq 2$):

Definition

$F: \mathbb{E}_k^n \to \mathbb{E}_k^n$ is locally triangle, if $G(F, \alpha)$ is acyclic for every $\alpha \in \mathbb{E}_k^n$, where local dependence of f on x_i in α is interpreted as:

$$\exists b\colon f(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n) \neq f(\alpha_1, \ldots, b, \ldots, \alpha_n).$$

Theorem

Locally triangle families are proper.

Remark

Each recursively triangular family is locally triangle.

Local interaction graphs-3

Theorem

If for any t, $1 \leq t \leq n$ there are at most $2^t - 1$ points α such that $G(F, \alpha)$ has a cycle of length at most t, then F is HUFP Boolean network.

- It is not known whether this fact is a criterion.
- The intuitive interpretation / "translation" to the proper family language is yet to be discovered.

Table of Contents

Proper permutations

Let $F\colon Q^n \to Q^n$ be proper, $(Q,+)$ is a quasigroup. Then

$$\sigma_F(x)\colon x \to x + F(x), \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \to \begin{bmatrix} x_1 + f_1(x_1,\dots,x_n) \\ \vdots \\ x_n + f_n(x_1,\dots,x_n) \end{bmatrix}$$

is a permutation: $\sigma_F \in Perm(Q^n)$.

Proper permutations-2

Let $F\colon Q^n \to Q^n$ be proper. Consider $\sigma_F^{-1} \in Perm(Q^n)$.

Theorem

If $(Q, +)$ is a group (i.e., $+$ is associative), then $G\colon Q^n \to Q^n$ of the form

$$G(x) = (-x) + \sigma_F^{-1}(x)$$

is also proper.

I.e., for the proper F there exists G "dual" to F in the sense that

$$\sigma_F^{-1}(x) = \sigma_G(x).$$

Proper permutations-3

- The set of all proper permutations $\mathcal{S}^{\mathrm{prop}}$ **is not** a subgroup of $Perm(Q^n)$.
- It acts transitively on Q^n.
- In the case $Q = \mathbb{E}_2$ it is known[13] that σ_F generates $Perm(\mathbb{E}_2^n)$.

Theorem

Let $F = (f_1, \ldots, f_n)$ be a proper family of Boolean functions. Then for any $A \in \{0,1\}^n$ the number of solutions of the equation $F(x) = A$ is even[a].

[a] Tsaregorodtsev, “Properties of proper families of Boolean functions”.

Number of fixed points of π_F

From the theorem above it follows that $\pi_F(x) = x + F(x)$ has an even number of fixed points.

[13] Schurr, “Unique sink orientations of cubes”.

Table of Contents

Recognizing properness

Theorem

Given a Boolean family F by its CNF, the problem of recognizing properness is coNP-complete[a]*.*

[a] Nosov, "Constructing Parametric Families of Latin Squares in the Boolean Database".

- Hence, no generic fast algorithm for deciding properness so far.
- This is also true for $k \geq 3$.
- Some special algorithms for the *classes* of families, e.g.:
  - linear families[14];
  - monotonic functions[15];
  - ...

[14] Nosov and Pankratiev, "Latin squares over Abelian groups".

[15] Rykov, "On the algorithms for checking the properness of a function family".

Recognizing properness-2

Let F be a Boolean family of size n.

- Algorithm "by definition": $\mathcal{O}(4^n)$ operations of calculating $F(x)$ (count $F(x)$ and $F(y)$ for each pair $x, y \in \mathbb{E}_2^n$).
- Optimized version (algorithm[16] for recognizing USO property): $\mathcal{O}(3^n)$ operations.

[16] Bosshard and Gärtner, *Pseudo Unique Sink Orientations*.

Number of proper families

Size n	$\Delta(n)$	$\Delta^{\mathtt{rec}}(n)$	$\Delta^{\mathtt{loc}}(n)$	$T(n)$
$n = 1$	2	2	2	2
$n = 2$	12	12	12	12
$n = 3$	488	680	680	744
$n = 4$	481776	3209712	3349488	5541744

Table: Number of triangle, recursively/locally triange and proper Boolean families of size n.

Number of proper families-2

Theorem

Let $T(n)$ be the number of Boolean proper families of size n. Then[a] *there exist $B \geq A > 0$ such that for $n \geq 2$:*

$$n^{A \cdot 2^n} \leq T(n) \leq n^{B \cdot 2^n}.$$

[a] Tsaregorodtsev, "Properties of proper families of Boolean functions".

Alternative characterization of triangular families

$\Delta(n)$ is *A250110*-oeis sequence.

Alternative characterization of triangular families

There is a bijection between Triangular Boolean families of size n and *Conditional Preference networks* (CP-nets) of size n.

CP-net

Conditional Preference Network (CP-net) is a graphical model to represent user's conditional ceteris paribus (all else being equal) preference statements.

The result can be generalized to the case of k-valued logic.

Almost all Boolean proper families are not triangular

Theorem

Let $\Delta(n)$ be the number of triangular Boolean families of size n. Then it holds that

$$\frac{\Delta(n)}{T(n)} = o\left(\frac{1}{n^{D \cdot 2^n}}\right) \text{ as } n \to \infty,$$

for some $D > 0$.

Recurrence for the number of recursively triangle proper families

Theorem

Let $\Delta^{\texttt{rec}}(n)$ be the number of recursively triange families of size n over k-valued logic. Then it holds that

$$\Delta^{\texttt{rec}}(n) = \sum_{j=1}^{n} (-1)^{j+1} \cdot k^j \cdot \binom{n}{j} \Delta^{\texttt{rec}}(n-j)^{k^j}.$$

Self-duality and properness

Theorem

F is proper iff any of the projections $\Pi_{i_1,\dots,i_k}^{a_1,\dots,a_k}(F)$ **is not** *self-dual.*

Slight generalization of the Theorem[17].

[17] Richard, "Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks".

Concluding remarks

What have we discussed today:

- the notion of proper family and some classes ((recursive/locally) triangle, orthogonal);
- how proper families helps in generating large classes of quasigroups;
- some "geometric" properties: isometries, alternative characterization via USO and HUPF for Boolean proper families;
- some "algebraic" properties: the set of "proper permutations" is closed under inversion; acts transitively; even number of fixed points in Boolean case;
- other properties: deciding properness is hard in general; bounds on the number of Boolean proper families.

Thank you for your attention!

Bibliography I

- Bosshard, Vitor and Bernd Gärtner. *Pseudo Unique Sink Orientations*. 2017. arXiv: 1704.08481 [math.CO].
- Galatenko, A. V., V. A. Nosov, and A. E. Pankratiev. "Latin squares over quasigroups". In: *Lobachevskii Journal of Mathematics* 41 (2020), pp. 194–203.
- Galatenko, A. V. et al. "Generation of n-quasigroups with the use of proper families of functions". In: *Discrete mathematics* 35.1 (2023). In russian, pp. 35–53.
- Galatenko, A. V. et al. "Generation of proper families of functions". In: *Intellektual'nye Sistemy. Teoriya i Prilozheniya (Intelligent Systems. Theory and Applications)* 25.4 (2021). In russian, pp. 100–103.
- Gligoroski, D., S. Markovski, and S. J. Knapskog. "The stream cipher Edon80". In: *New stream cipher designs*. Springer, 2008, pp. 152–169.
- Gligoroski, D., S. Markovski, and L. Kocarev. "Edon-R, An Infinite Family of Cryptographic Hash Functions.". In: *International Journal of Security and Networks* 8.3 (2009), pp. 293–300.
- Gligoroski, D., H. Mihajloska, and D. Otte. "GAGE and InGAGE". In: *Submission to the NIST's Lightweight Standardization Process*. 2019.

Bibliography II

- Gligoroski, D. et al. "Cryptographic hash function Edon-R'". In: *2009 Proceedings of the 1st International Workshop on Security and Communication Networks*. IEEE. 2009, pp. 1–9.
- Gribov, Aleksei Viktorovich, Pavel Andreevich Zolotykh, and Aleksandr Vasil'evich Mikhalev. "A construction of algebraic cryptosystem over the quasigroup ring". In: *Matematicheskie Voprosy Kriptografii [Mathematical Aspects of Cryptography]* 1.4 (2010), pp. 23–32.
- Katyshev, Sergey Yu., Viktor T. Markov, and Alexander A. Nechaev. "Application of non-associative groupoids to the realization of an open key distribution procedure". In: *Discrete Math. Appl.* 25.4 (1 2015), pp. 9–24.
- Katyshev, Sergey Yur'evich, Andrey Valentinovich Zyazin, and Andrei Vladimirovich Baryshnikov. "Application of non-associative structures for construction of homomorphic cryptosystems". In: *Matematicheskie Voprosy Kriptografii [Mathematical Aspects of Cryptography]* 11.3 (2020), pp. 31–39.
- Markov, V. T., A. V. Mikhalev, and A. A. Nechaev. "Nonassociative Algebraic Structures in Cryptography and Coding". In: *Journal of Mathematical Sciences* 245.2 (2020), pp. 178–197.
- Markovski, Smile and Verica Bakeva. "Quasigroup string processing: Part 4". In: *Contributions, Section of Natural, Mathematical and Biotechnical Sciences* 27.1-2 (2017).

Bibliography III

Nosov, V. A. "Constructing a parametric family of Latin squares in the vector database". Russian. In: *Intellektual'nye Sistemy. Teoriya i Prilozheniya (Intelligent Systems. Theory and Applications)* 8.1-4 (2006). In russian, pp. 517–529. ISSN: 2075-9460; 2411-4448.

— . "Constructing Parametric Families of Latin Squares in the Boolean Database". Russian. In: *Intellektual'nye Sistemy. Teoriya i Prilozheniya (Intelligent Systems. Theory and Applications)* 4.3-4 (1999). In russian, pp. 307–320. ISSN: 2075-9460; 2411-4448.

Nosov, V. A. and A. E. Pankratiev. "Latin squares over Abelian groups". In: *Journal of Mathematical Sciences* 149 (2008), pp. 1230–1234.

— . "On functional representation of Latin squares". In: *Intellektual'nye Sistemy. Teoriya i Prilozheniya (Intelligent Systems. Theory and Applications)* 12.1-4 (2008). In russian, pp. 317–332. ISSN: 2075-9460; 2411-4448.

Richard, Adrien. "Fixed point theorems for Boolean networks expressed in terms of forbidden subnetworks". In: *Theoretical Computer Science* 583 (2015), pp. 1–26.

Rykov, D. O. "On the algorithms for checking the properness of a function family". In: *Intellektual'nye Sistemy. Teoriya i Prilozheniya (Intelligent Systems. Theory and Applications)* 14.1-4 (2010). In russian, pp. 261–276.

Bibliography IV

- Schurr, Ingo A. "Unique sink orientations of cubes". PhD thesis. ETH Zurich, 2004.
- Slaminková, I. and M. Vojvoda. "Cryptanalysis of a hash function based on isotopy of quasigroups". In: *Tatra Mountains Mathematical Publications* 45.1 (2010), pp. 137–149.
- Szabo, T. and E. Welzl. "Unique sink orientations of cubes". In: *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*. IEEE. 2001, pp. 547–555.
- Tsaregorodtsev, K. D. "One-to-one correspondense between proper families of boolean functions and unique sink orientations of cubes". In: *Applied discrete mathematics* 48 (2020). In russian, pp. 16–21.
- — ."Properties of proper families of Boolean functions". In: *Discrete mathematics* 33.1 (2021). In russian, pp. 91–102.
- Vojvoda, M. "Cryptanalysis of one hash function based on quasigroup". In: *Tatra Mountains Mathematical Publications* 29.173 (2004), pp. 173–181.