Latin Squares Specified by Systems of Boolean Functions

V.A. Nosov and A.E. Pankratiev

Moscow State University
Moscow, Russia

Omsk, August 22, 2009

Outline

Main concept

Definition

A Latin Square of order n is a square matrix with n^2 entries of n different elements, none of them occurring twice within any row or column of the matrix.

Example

$$\begin{array}{ccccc} 0 & 1 & 2 & \cdots & n-1 \\ 1 & 2 & 3 & & 0 \\ 2 & 3 & & & 1 \\ 3 & & & & 2 \\ \vdots & & & & \vdots \\ n-1 & 0 & 1 & \cdots & n-2 \end{array}$$

$$L(x, y) = x + y \pmod{n}$$

Main concept

Definition

A Latin Square of order n is a square matrix with n^2 entries of n different elements, none of them occurring twice within any row or column of the matrix.

Example

$$\begin{array}{|ccccc|} 0 & 1 & 2 & \cdots & n-1 \\ 1 & 2 & 3 & & 0 \\ 2 & 3 & & & 1 \\ 3 & & & & 2 \\ \vdots & & & & \vdots \\ n-1 & 0 & 1 & \cdots & n-2 \end{array}$$

$$L(x, y) = x + y \pmod{n}$$

Definition

A quasigroup is a groupoid (a set S equipped with a binary operation) such that, for any two elements $a, b \in S$, each of the equations $ax = b$ and $ya = b$ has exactly one solution (i.e., both the left and right inverse operations are uniquely defined).

Fact

Latin squares $\leftrightarrow$ *multiplication tables of finite quasigroups*

Basic notions and elementary facts

Definition

A quasigroup is a groupoid (a set S equipped with a binary operation) such that, for any two elements $a, b \in S$, each of the equations $ax = b$ and $ya = b$ has exactly one solution (i.e., both the left and right inverse operations are uniquely defined).

Fact

Latin squares $\leftrightarrow$ *multiplication tables of finite quasigroups*

Quadrangle criterion. Group Latin squares

Definition

A matrix $A = \{a_{ij}\}$ is said to satisfy the quadrangle criterion if, for any indices $i, j, k, l, i_1, j_1, k_1, l_1$, the equalities $a_{jk} = a_{j_1 k_1}$, $a_{ik} = a_{i_1 k_1}$, and $a_{il} = a_{i_1 l_1}$ imply $a_{jl} = a_{j_1 l_1}$.

Fact

The multiplication table of any finite group (its Cayley table) is a Latin square satisfying the quadrangle criterion.
Conversely, any Latin square satisfying the quadrangle criterion may be bordered in such a way as to present the Cayley table of some finite group.

Latin squares satisfying QC $\leftrightarrow$ multiplication tables of finite groups

Quadrangle criterion. Group Latin squares

Definition

A matrix $A = \{a_{ij}\}$ is said to satisfy the quadrangle criterion if, for any indices $i, j, k, l, i_1, j_1, k_1, l_1$, the equalities $a_{jk} = a_{j_1 k_1}$, $a_{ik} = a_{i_1 k_1}$, and $a_{il} = a_{i_1 l_1}$ imply $a_{jl} = a_{j_1 l_1}$.

Fact

The multiplication table of any finite group (its Cayley table) is a Latin square satisfying the quadrangle criterion.
Conversely, any Latin square satisfying the quadrangle criterion may be bordered in such a way as to present the Cayley table of some finite group.

Latin squares satisfying QC $\leftrightarrow$ multiplication tables of finite groups

Quadrangle criterion. Group Latin squares

Definition

A matrix $A = \{a_{ij}\}$ is said to satisfy the quadrangle criterion if, for any indices $i, j, k, l, i_1, j_1, k_1, l_1$, the equalities $a_{jk} = a_{j_1 k_1}$, $a_{ik} = a_{i_1 k_1}$, and $a_{il} = a_{i_1 l_1}$ imply $a_{jl} = a_{j_1 l_1}$.

Fact

The multiplication table of any finite group (its Cayley table) is a Latin square satisfying the quadrangle criterion.
Conversely, any Latin square satisfying the quadrangle criterion may be bordered in such a way as to present the Cayley table of some finite group.

Latin squares satisfying QC $\leftrightarrow$ multiplication tables of finite groups

Classification of Latin squares

Definition

Let $(G, \cdot)$ and $(H, *)$ be two quasigroups. An ordered triple $(\theta,\ \varphi,\ \psi)$ of one-to-one mappings of the set G onto H is called an isotopism of $(G, \cdot)$ upon $(H, *)$ if $(x\theta) * (y\varphi) = (x \cdot y)\psi$ for all $x, y \in G$.
If $\theta = \varphi = \psi$, then the quasigroups are said to be isomorphic.

Definition

The conjugates of a Latin square $L = L(x, y)$ are the Latin squares ${}^{-1}L$, L^{-1}, L^{*}, $({}^{-1}L)^{*}$, and $(L^{-1})^{*}$, where L^{*} is the transpose of square L, and ${}^{-1}L$ (or L^{-1}) is the left (right) inverse of square L in the sense that ${}^{-1}L(L(x, y), y) = x$ (respectively, $L^{-1}(x, L(x, y)) = y$).

Classification of Latin squares

Definition

Let $(G, \cdot)$ and $(H, *)$ be two quasigroups. An ordered triple $(\theta,\ \varphi,\ \psi)$ of one-to-one mappings of the set G onto H is called an isotopism of $(G, \cdot)$ upon $(H, *)$ if $(x\theta) * (y\varphi) = (x \cdot y)\psi$ for all $x, y \in G$.
If $\theta = \varphi = \psi$, then the quasigroups are said to be isomorphic.

Definition

The conjugates of a Latin square $L = L(x, y)$ are the Latin squares ${}^{-1}L$, L^{-1}, L^*, $({}^{-1}L)^*$, and $(L^{-1})^*$, where L^* is the transpose of square L, and ${}^{-1}L$ (or L^{-1}) is the left (right) inverse of square L in the sense that ${}^{-1}L(L(x, y), y) = x$ (respectively, $L^{-1}(x, L(x, y)) = y$).

Classification of Latin squares (classes)

Definition

A set of Latin squares which comprises all the members of some isotopy class together with their conjugates is called a main class of Latin squares.

Fact

- *The set of all Latin squares of order n splits into disjoint main classes.*
- *Each main class is a union of complete isotopy classes.*
- *Each isotopy class splits into disjoint isomorphism classes.*

Classification of Latin squares (classes)

Definition

A set of Latin squares which comprises all the members of some isotopy class together with their conjugates is called a main class of Latin squares.

Fact

- *The set of all Latin squares of order n splits into disjoint main classes.*
- *Each main class is a union of complete isotopy classes.*
- *Each isotopy class splits into disjoint isomorphism classes.*

Motivation for study

Latin squares are widely used in

- experimental design;
- error-correcting codes;
- entertainment;
- cryptography.

It was demonstrated by C. Shannon* that stream ciphers based on Latin squares are, in a sense, "perfect."

* Shannon C., "Communication Theory of Secrecy Systems" // *Bell System Techn. J.*, **28**, 4 (1949), 656–715.

Motivation for study

Latin squares are widely used in

- experimental design;
- error-correcting codes;
- entertainment;
- cryptography.

It was demonstrated by C. Shannon* that stream ciphers based on Latin squares are, in a sense, "perfect."

* Shannon C., "Communication Theory of Secrecy Systems" // *Bell System Techn. J.*, **28**, 4 (1949), 656–715.

Some directions of research

- Constructing Latin Squares which have particular orders and differ from the already known examples.
- "Extending" (or "reducing") Latin squares of order n to Latin squares of order $n+1$ (respectively, $n-1$).
- Completing partially filled matrices to Latin squares.
- Classifying Latin squares of a given order n.
- Constructing (wide) parametric classes of Latin squares.
- Optimal (compact) specification of large Latin squares: constructive (analytical) methods.

Some directions of research

- Constructing Latin Squares which have particular orders and differ from the already known examples.
- "Extending" (or "reducing") Latin squares of order n to Latin squares of order $n+1$ (respectively, $n-1$).
- Completing partially filled matrices to Latin squares.
- Classifying Latin squares of a given order n.
- Constructing (wide) parametric classes of Latin squares.
- Optimal (compact) specification of large Latin squares: constructive (analytical) methods.

Some directions of research

- Constructing Latin Squares which have particular orders and differ from the already known examples.
- "Extending" (or "reducing") Latin squares of order n to Latin squares of order $n+1$ (respectively, $n-1$).
- Completing partially filled matrices to Latin squares.
- Classifying Latin squares of a given order n.
- Constructing (wide) parametric classes of Latin squares.
- Optimal (compact) specification of large Latin squares: constructive (analytical) methods.

Some directions of research

- Constructing Latin Squares which have particular orders and differ from the already known examples.
- "Extending" (or "reducing") Latin squares of order n to Latin squares of order $n+1$ (respectively, $n-1$).
- Completing partially filled matrices to Latin squares.
- Classifying Latin squares of a given order n.
- Constructing (wide) parametric classes of Latin squares.
- Optimal (compact) specification of large Latin squares: constructive (analytical) methods.

Some directions of research

- Constructing Latin Squares which have particular orders and differ from the already known examples.
- "Extending" (or "reducing") Latin squares of order n to Latin squares of order $n+1$ (respectively, $n-1$).
- Completing partially filled matrices to Latin squares.
- Classifying Latin squares of a given order n.
- Constructing (wide) parametric classes of Latin squares.
- Optimal (compact) specification of large Latin squares: constructive (analytical) methods.

Some directions of research

- Constructing Latin Squares which have particular orders and differ from the already known examples.
- "Extending" (or "reducing") Latin squares of order n to Latin squares of order $n+1$ (respectively, $n-1$).
- Completing partially filled matrices to Latin squares.
- Classifying Latin squares of a given order n.
- Constructing (wide) parametric classes of Latin squares.
- Optimal (compact) specification of large Latin squares: constructive (analytical) methods.

Consider an $(n \times n)$-matrix $L = L(x, y)$ specified by the formula

$$L(x,y) = \pi(x+y) + x \quad \text{or} \quad L(x,y) = \pi(x+y) - x.$$

Here, $x, y \in \{0, 1, \ldots, n-1\}$, the sum $x + y$ is considered modulo n and π is a mapping $\mathbb{Z}_n \to \mathbb{Z}_n$.
Denote by π^+ (respectively, π^-) the class of mappings π for which the matrix defined above is a Latin square.

Fact

A mapping $\pi = \pi(z)$ belongs to π^+ (respectively, π^-) if and only if

1. *$\pi(z)$ is bijective and*
2. *$\sigma(z) = \pi(z) + z$ (respectively, $\sigma(z) = \pi(z) - z$) is bijective as well.*

Consider an $(n \times n)$-matrix $L = L(x, y)$ specified by the formula

$$L(x, y) = \pi(x + y) + x \quad \text{or} \quad L(x, y) = \pi(x + y) - x.$$

Here, $x, y \in \{0, 1, \ldots, n-1\}$, the sum $x + y$ is considered modulo n and π is a mapping $\mathbb{Z}_n \to \mathbb{Z}_n$.
Denote by π^+ (respectively, π^-) the class of mappings π for which the matrix defined above is a Latin square.

Fact

A mapping $\pi = \pi(z)$ belongs to π^+ (respectively, π^-) if and only if

1. *$\pi(z)$ is bijective and*
2. *$\sigma(z) = \pi(z) + z$ (respectively, $\sigma(z) = \pi(z) - z$) is bijective as well.*

Constructing non-group Latin squares of large prime orders

Consider an $(n \times n)$-matrix $L = L(x, y)$ specified by the formula

$$L(x, y) = \pi(x + y) + x \quad \text{or} \quad L(x, y) = \pi(x + y) - x.$$

Here, $x, y \in \{0, 1, \ldots, n-1\}$, the sum $x + y$ is considered modulo n and π is a mapping $\mathbb{Z}_n \to \mathbb{Z}_n$.
Denote by π^+ (respectively, π^-) the class of mappings π for which the matrix defined above is a Latin square.

Fact

A mapping $\pi = \pi(z)$ belongs to π^+ (respectively, π^-) if and only if

1. *$\pi(z)$ is bijective and*
2. *$\sigma(z) = \pi(z) + z$ (respectively, $\sigma(z) = \pi(z) - z$) is bijective as well.*

Constructing non-group Latin squares of large prime orders

Fix a prime $p > 5$ and let s be a primitive root in $\mathbb{Z}_p^*$.
Then $\exists l > 2$, $m \geq 2$: $p - 1 = l \cdot m$. Denote $k = s^m$.
Note that $\mathrm{ord}(k) = l > 2$, hence, $k \neq \pm 1$.
Consider the permutation

$$\pi = (0)(1\ k\ k^2\ \dots\ k^{l-1})(s\ sk\ \dots\ sk^{l-1})\ \dots\ (s^{m-1}\ s^{m-1}k\ \dots\ s^{m-1}k^{l-1})$$

Introduce $\varepsilon = (\varepsilon_0, \dots, \varepsilon_{m-1})$, where $\varepsilon_0 = 1$ and $\varepsilon_i = \pm 1$, $i = \overline{1, m-1}$.
Denote by π_ε the permutation obtained from π by reversing all cycles that correspond to $\varepsilon_i = -1$ (excluding the cycle (0)).

Theorem (Budagyan)

For $\varepsilon \neq (1, \dots, 1)$, formula $L(x, y) = \pi_\varepsilon(x + y) + x$ defines a non-group Latin square of order p (the quadrange criterion is violated).

Constructing non-group Latin squares of large prime orders

Fix a prime $p > 5$ and let s be a primitive root in $\mathbb{Z}_p^*$.
Then $\exists l > 2$, $m \geq 2$: $p - 1 = l \cdot m$. Denote $k = s^m$.
Note that $\mathrm{ord}(k) = l > 2$, hence, $k \neq \pm 1$.
Consider the permutation

$$\pi = (0)(1\ k\ k^2\ \ldots\ k^{l-1})(s\ sk\ \ldots\ sk^{l-1})\ \ldots\ (s^{m-1}\ s^{m-1}k\ \ldots\ s^{m-1}k^{l-1})$$

Introduce $\varepsilon = (\varepsilon_0, \ldots, \varepsilon_{m-1})$, where $\varepsilon_0 = 1$ and $\varepsilon_i = \pm 1$, $i = \overline{1, m-1}$.
Denote by π_ε the permutation obtained from π by reversing all cycles that correspond to $\varepsilon_i = -1$ (excluding the cycle (0)).

Theorem (Budagyan)

For $\varepsilon \neq (1, \ldots, 1)$, formula $L(x, y) = \pi_\varepsilon(x + y) + x$ defines a non-group Latin square of order p (the quadrange criterion is violated).

Constructing non-group Latin squares of large prime orders

Fix a prime $p > 5$ and let s be a primitive root in $\mathbb{Z}_p^*$.
Then $\exists l > 2,\ m \geq 2$: $p - 1 = l \cdot m$. Denote $k = s^m$.
Note that $\mathrm{ord}(k) = l > 2$, hence, $k \neq \pm 1$.
Consider the permutation

$$\pi = (0)(1\ k\ k^2\ \ldots\ k^{l-1})(s\ sk\ \ldots\ sk^{l-1})\ \ldots\ (s^{m-1}\ s^{m-1}k\ \ldots\ s^{m-1}k^{l-1})$$

Introduce $\varepsilon = (\varepsilon_0, \ldots, \varepsilon_{m-1})$, where $\varepsilon_0 = 1$ and $\varepsilon_i = \pm 1$, $i = \overline{1, m-1}$.
Denote by π_ε the permutation obtained from π by reversing all cycles that correspond to $\varepsilon_i = -1$ (excluding the cycle (0)).

Theorem (Budagyan)

For $\varepsilon \neq (1, \ldots, 1)$, formula $L(x, y) = \pi_\varepsilon(x + y) + x$ defines a non-group Latin square of order p (the quadrange criterion is violated).

Constructing non-group Latin squares of large prime orders

Fix a prime $p > 5$ and let s be a primitive root in $\mathbb{Z}_p^*$.
Then $\exists l > 2$, $m \geq 2$: $p - 1 = l \cdot m$. Denote $k = s^m$.
Note that $\mathrm{ord}(k) = l > 2$, hence, $k \neq \pm 1$.
Consider the permutation

$$\pi = (0)(1\ k\ k^2\ \ldots\ k^{l-1})(s\ sk\ \ldots\ sk^{l-1})\ \ldots\ (s^{m-1}\ s^{m-1}k\ \ldots\ s^{m-1}k^{l-1})$$

Introduce $\varepsilon = (\varepsilon_0, \ldots, \varepsilon_{m-1})$, where $\varepsilon_0 = 1$ and $\varepsilon_i = \pm 1$, $i = \overline{1, m-1}$.
Denote by π_ε the permutation obtained from π by reversing all cycles that correspond to $\varepsilon_i = -1$ (excluding the cycle (0)).

Theorem (Budagyan)

For $\varepsilon \neq (1, \ldots, 1)$, formula $L(x, y) = \pi_\varepsilon(x + y) + x$ defines a non-group Latin square of order p (the quadrange criterion is violated).

Constructing non-group Latin squares of large prime orders

Fix a prime $p > 5$ and let s be a primitive root in $\mathbb{Z}_p^*$.
Then $\exists l > 2,\ m \geq 2$: $p - 1 = l \cdot m$. Denote $k = s^m$.
Note that $\mathrm{ord}(k) = l > 2$, hence, $k \neq \pm 1$.
Consider the permutation

$$\pi = (0)(1\ k\ k^2\ \dots\ k^{l-1})(s\ sk\ \dots\ sk^{l-1})\ \dots\ (s^{m-1}\ s^{m-1}k\ \dots\ s^{m-1}k^{l-1})$$

Introduce $\varepsilon = (\varepsilon_0, \dots, \varepsilon_{m-1})$, where $\varepsilon_0 = 1$ and $\varepsilon_i = \pm 1$, $i = \overline{1, m-1}$.
Denote by π_ε the permutation obtained from π by reversing all cycles that correspond to $\varepsilon_i = -1$ (excluding the cycle (0)).

Theorem (Budagyan)

For $\varepsilon \neq (1, \dots, 1)$, formula $L(x, y) = \pi_\varepsilon(x + y) + x$ defines a non-group Latin square of order p (the quadrange criterion is violated).

Constructing classes of Latin squares

Let us turn once again to the simplest

Example

0	1	$\cdots$	$n-1$
1	2		0
$\vdots$			$\vdots$
$n-1$	0	$\cdots$	$n-2$

$$L(x,y) = x + y \pmod{n}$$

and introduce some "disturbance" (or "remainder") into this formula:

$$L(x,y) = x + y + f(x,y)$$

Below we treat this formula in "vector" form.

Constructing classes of Latin squares

Let us turn once again to the simplest

Example

$$\begin{array}{|cccc|}\hline 0 & 1 & \cdots & n-1 \\ 1 & 2 & & 0 \\ \vdots & & & \vdots \\ n-1 & 0 & \cdots & n-2 \\ \hline\end{array}$$

$$L(x,y) = x + y \pmod{n}$$

and introduce some "disturbance" (or "remainder") into this formula:

$$L(x,y) = x + y + f(x,y)$$

Below we treat this formula in "vector" form.

Constructing classes of Latin squares

Let us turn once again to the simplest

Example

$$\begin{array}{|cccc|} \hline 0 & 1 & \cdots & n-1 \\ 1 & 2 & & 0 \\ \vdots & & & \vdots \\ n-1 & 0 & \cdots & n-2 \\ \hline \end{array}$$

$$L(x, y) = x + y \pmod{n}$$

and introduce some “disturbance” (or “remainder”) into this formula:

$$L(x, y) = x + y + f(x, y)$$

Below we treat this formula in “vector” form.

Latin squares over Abelian groups

Fix a finite Abelian group G and let $H = G^n = G \times G \times \cdots \times G$.
Define a square L of size $|H| \times |H|$ over H as follows.

- "Enumerate" rows and columns of L by elements of H;
- Define the entry $L(x, y) = (z_1, \ldots, z_n)$ at row $x = (x_1, \ldots, x_n) \in H$ and column $y = (y_1, \ldots, y_n) \in H$ by the formulas

$$
\begin{aligned}
z_1 &= x_1 + y_1 + f_1(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) \\
z_2 &= x_2 + y_2 + f_2(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) \\
&\vdots \\
z_n &= x_n + y_n + f_n(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)).
\end{aligned}
$$

Here, $p_i : \; G \times G \to G; \quad f_i : \; G^n \to G, \quad i = \overline{1, n}.$

Latin squares over Abelian groups

Question

What are necessary/sufficient conditions on functions f_i for L to be a Latin square?

Proper families of functions

Definition

Functions $f_1, f_2, \ldots, f_n$ of variables $p_1, p_2, \ldots, p_n$ form a proper family if, for any distinct n-tuples $p' = (p'_1, p'_2, \ldots, p'_n)$ and $p'' = (p''_1, p''_2, \ldots, p''_n)$, there is an index α, $1 \leq \alpha \leq n$, such that $p'_\alpha \neq p''_\alpha$, while $f_\alpha(p') = f_\alpha(p'')$.

Examples

- Families of constant functions.
- Families of "triangular" form:
  $f_1 \equiv \mathrm{const},\ f_2 = f_2(p_1),\ f_3 = f_3(p_1, p_2),\ \ldots,\ f_n = f_n(p_1, p_2, \ldots, p_{n-1})$.
- "Clique" families:
  $f_1 = \overline{x_2}x_3 \cdots x_n,\ f_2 = \overline{x_3}x_4 \cdots x_n x_1,\ \ldots,\ f_n = \overline{x_1}x_2 \cdots x_{n-1},\ n \geq 3$.

Proper families of functions

Definition

Functions $f_1, f_2, \dots, f_n$ of variables $p_1, p_2, \dots, p_n$ form a proper family if, for any distinct n-tuples $p' = (p'_1, p'_2, \dots, p'_n)$ and $p'' = (p''_1, p''_2, \dots, p''_n)$, there is an index α, $1 \le \alpha \le n$, such that $p'_\alpha \neq p''_\alpha$, while $f_\alpha(p') = f_\alpha(p'')$.

Examples

- Families of constant functions.
- Families of "triangular" form:
  $f_1 \equiv \mathrm{const},\ f_2 = f_2(p_1),\ f_3 = f_3(p_1, p_2),\ \dots,\ f_n = f_n(p_1, p_2, \dots, p_{n-1})$.
- "Clique" families:
  $f_1 = \overline{x_2} x_3 \cdots x_n,\ f_2 = \overline{x_3} x_4 \cdots x_n x_1,\ \dots,\ f_n = \overline{x_1} x_2 \cdots x_{n-1},\ n \ge 3$.

Proper families of functions

Theorem (NP)

Formulas

$$z_1 = x_1 + y_1 + f_1(p_1(x_1, y_1), \dots, p_n(x_n, y_n))$$
$$z_2 = x_2 + y_2 + f_2(p_1(x_1, y_1), \dots, p_n(x_n, y_n))$$
$$\vdots$$
$$z_n = x_n + y_n + f_n(p_1(x_1, y_1), \dots, p_n(x_n, y_n))$$

determine a Latin square for any functions $p_1, p_2, \dots, p_n$ if and only if the family $F = \{f_1, f_2, \dots, f_n\}$ is proper.

The graph of essential dependence of a family of functions

We restrict our presentation to the case of Boolean functions (the Abelian group G coincides with $\mathbb{Z}_2$) and investigate such families of terms of graphs.

Definition

The graph of essential dependence of a family of functions $F = \{f_i\}_{i=1}^n$, $f_i = f_i(z_1, \ldots, z_n)$, is a directed graph $G_F = (V, E)$ defined on the set of vertices $V = \{1, 2, \ldots, n\}$, where two vertices i, j are connected by a (directed) edge $(i, j) \in E$ if and only if f_j essentially depends on x_i.

Remark

The graph of essential dependence of a proper family is free of loops.

Theorem (NP)

A family of linear functions $F = \{f_1, f_2, \ldots, f_n\}$ *is proper if and only if its graph of essential dependence* G_F *contains no cycles.*

Remark

The class of functions in which a family is proper if and only if its graph of essential dependence contains no cycles can be significantly extended to the class of the so-called H*-functions.*

Graphs of proper families of functions

Theorem (NP)

A family of linear functions $F = \{f_1, f_2, \dots, f_n\}$ *is proper if and only if its graph of essential dependence* G_F *contains no cycles.*

Remark

The class of functions in which a family is proper if and only if its graph of essential dependence contains no cycles can be significantly extended to the class of the so-called H*-functions.*

Graphs of proper families of functions

Question

What directed graphs are the graphs of essential dependence of some proper families of functions?

Remark

- *Any directed graph without cycles is the graph of essential dependence of a proper family of functions.*
- *A complete graph on n vertices ($n \geq 3$) is the graph of essential dependence of a proper family of functions.*

Clearly, any directed graph G without loops and multiple edges can be embedded in the graph of essential dependence of some proper family. However, in such embedding, the original graph G may be augmented with a large number of new edges. Moreover, the proper family which has a complete graph of essential dependence may have little in common with the family of functions that realizes the original graph G.

Graphs of proper families of functions

Question

What directed graphs are the graphs of essential dependence of some proper families of functions?

Remark

- *Any directed graph without cycles is the graph of essential dependence of a proper family of functions.*
- *A complete graph on n vertices ($n \geq 3$) is the graph of essential dependence of a proper family of functions.*

Clearly, any directed graph G without loops and multiple edges can be embedded in the graph of essential dependence of some proper family. However, in such embedding, the original graph G may be augmented with a large number of new edges. Moreover, the proper family which has a complete graph of essential dependence may have little in common with the family of functions that realizes the original graph G.

Graphs of proper families of functions

Question

What directed graphs are the graphs of essential dependence of some proper families of functions?

Remark

- *Any directed graph without cycles is the graph of essential dependence of a proper family of functions.*
- *A complete graph on n vertices ($n \geq 3$) is the graph of essential dependence of a proper family of functions.*

Clearly, any directed graph G without loops and multiple edges can be embedded in the graph of essential dependence of some proper family. However, in such embedding, the original graph G may be augmented with a large number of new edges. Moreover, the proper family which has a complete graph of essential dependence may have little in common with the family of functions that realizes the original graph G.

Graphs of proper families of functions

Problem

Construct an embedding of a given graph G into some larger graph G' which can be treated the graph of essential dependence of a proper family of functions $F' = \{f_i'\}$ in such a way that the structure of graph G be preserved.

This is particularly important when the original graph G arises as the graph of essential dependence of some given family of functions $F = \{f_i\}$. In this case, it is desirable that functions f_i' most closely resemble the original functions f_i in the sense that, for a certain evaluation of the newly introduced variables, functions f_i' treated as functions of the original variables coincide with functions f_i.

Graphs of proper families of functions

Problem

Construct an embedding of a given graph G into some larger graph G' which can be treated the graph of essential dependence of a proper family of functions $F' = \{f_i'\}$ in such a way that the structure of graph G be preserved.

This is particularly important when the original graph G arises as the graph of essential dependence of some given family of functions $F = \{f_i\}$. In this case, it is desirable that functions f_i' most closely resemble the original functions f_i in the sense that, for a certain evaluation of the newly introduced variables, functions f_i' treated as functions of the original variables coincide with functions f_i.

Graphs of proper families of functions

Definition

Let C be a directed cycle in an arbitrary directed graph $G(V, E)$. The collapse of cycle C is the operation of passing from graph $G(V, E)$ to a new graph $G^C(V^C, E^C)$ obtained from $G(V, E)$ by deleting all edges involved in the cycle C and identifying all vertices visited by cycle C.

Theorem (NP)

Suppose that a finite directed graph $G(V, E)$ without loops and multiple edges is proper (i.e., can be considered the graph of essential dependence of a proper family of functions). Then the collapse of any irreducible simple cycle $C \in G$ gives a graph G^C that contains multiple edges.

Graphs of proper families of functions

Theorem (NP)

Let $G(V, E)$ be an arbitrary directed graph without loops and multiple edges on n vertices $V = \{1, 2, \ldots, n\}$.
Then there exists a larger proper graph $G'(V', E')$ on $n' \leq n + \lceil \log_2 n \rceil$ vertices $V' = \{1, 2, \ldots, n'\}$ such that its subgraph induced by the vertex subset $V \subseteq V'$ coincides with G.
Moreover, for any family of functions $F = \{f_i\}_{i=1}^{n}$ realizing the original graph G, one can find a proper family of functions $F' = \{f_i'\}_{i=1}^{n'}$ which realizes graph G' and such that for every i, $1 \leq i \leq n$, there exists an evaluation of arguments $x_{n+1}, \ldots, x_{n'}$ such that f_i' as a function of n arguments $x_1, \ldots, x_n$ coincides with f_i.

Graphs of proper families of functions

Remark

If the set V of vertices of the original graph $G(V, E)$ can be partitioned into two subsets $V = V_0 \sqcup V_1$ in such a way that any directed cycle of graph $G(V, E)$ contains vertices of both subsets V_0, V_1, then the graph $G'(V', E')$ mentioned above can be constructed using only one additional vertex.

References

- Dénes J. and Keedwell A., *Latin squares and their applications*, Budapest, (1974).
- Hall, M., *Combinatorial theory*, Blaisdell, Massachusetts, (1967).
- Budagyan, L., "Construction of non-group Latin squares of arbitrarily large orders", Proc. conf. "Mathematics and Security of Information Technologies", (Moscow, October 23–24, 2003), 410–412.
- Nosov, V. A. and Pankratiev, A. E., "Latin squares over Abelian groups" // *J. Math. Sci.*, **149**, 3, (2008), 1230–1234.