

THE THEORY OF PLAFALES. P VS NP PROBLEM SOLUTION

DMYTRO TOPCHYI

ABSTRACT. This paper is dedicated to a rigorous review of the theory of plafales, which describes the properties and applications of a new mathematical object. As a consequence of the created theory we give a proof of the equality of complexity classes P and NP.

2020 MSC. Primary: 00-02, 00A05. Secondary: 00A71, 18A05.

1. INTRODUCTION

The first edition of [1] is published in March 2011. The publication's goal is the creation of a new theory in mathematics, where the central object is plafal¹. The second edition of [2] is published in February 2013. After the report at the 42nd Polish Conference on Mathematics Applications [3], it is necessary to create applications based on the theory of plafales (so-called constructive approach of post-factum power). Here we will provide an appropriate overview of the research and development process of the theory of plafales.

Finite element method. There are created mathematical models of serendipity finite elements: a new approach to construction basis and field functions. A quadruple role of the basis functions of serendipity finite elements is structurally shown [4], [5].

IT (finite element method as algorithmic support). Due to solving the non-standard Dirichlet boundary value problem [4], using the components of the theory of plafales (to obtain the surface of the temperature field in a three-dimensional space), there is developed a software for testing non-stationary temperature fields [6].

Cryptography. In September 2014 there is created a symmetric-key algorithm "ECLECTIC-DT-1" [7]. Algorithm's characteristics: block length is 128 bits, key length is 256 bits, 14 rounds. Algorithm's indicators (upper bounds of practical security): $EDP \leq 2^{-714}$ (against differential cryptanalysis [8]), $ELP \leq 2^{-714}$ (against linear cryptanalysis [9]). In December 2018 the symmetric-key algorithm "STEEL" is created [10] (which is the modification of the algorithm "ECLECTIC-DT-1"). Algorithm's characteristics: block length is 128 bits, key length is 256 bits, 14 rounds. Algorithm's indicators: $EDP \leq 2^{-595}$, $ELP \leq 2^{-595}$.

Note 1. Editions [1], [2] are the basis of the theory of plafales. The theory of plafales has to be taken into consideration starting from this article.

Date: 12 January 2023.

Key words and phrases. Plafal, Plafale, The theory of plafales, P vs NP problem.

¹The singular form is plafal or plafale. The plural form is plafales.

2. CONCEPT OF THE PLAFAL

Now we introduce the following concept. For any simple graph $G(S, E)^2$ let there be a correspondence between each edge and an arbitrary object, and also between each vertex and an arbitrary object³. Object's essence is not taken into consideration: an arbitrary set, category, ∞ -cosmos [12], etc. Designation of plafal in general form is PF_j^i , where i is a number of graph's edges, j is a number of graph's vertices⁴ (examples of plafales are given in figures 1, 2).

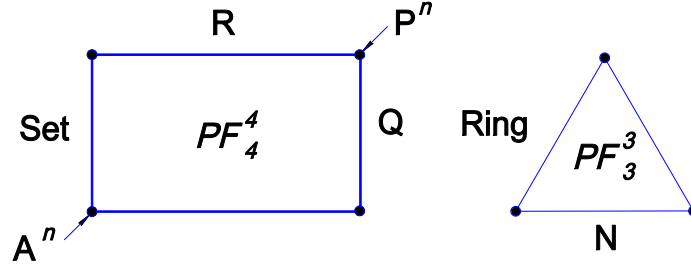


FIGURE 1. PF_4^4 . Edges: Set (the category of sets), \mathbb{R} is a set of real numbers, \mathbb{Q} is a set of rational numbers, $a \leftrightarrow A$. Vertices: \mathbb{A}^n is an affine space, \mathbb{P}^n is a projective space, $p \leftrightarrow P$ (for two vertices). PF_3^3 . Edges: \mathbb{N} is a set of natural numbers, Ring (the category of rings).

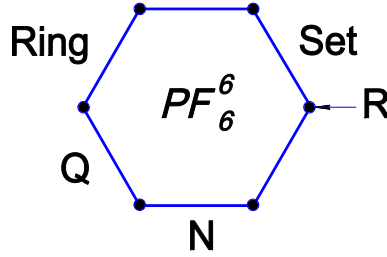


FIGURE 2. PF_6^6 .

²In the general case, a is an edge of $G(S, E)$, p is a vertex of $G(S, E)$. S is a set of vertices, E is a set of edges. $G(S, E)$ does not contain an isolated vertex.

³Let us remark that the above correspondences are not the graph's representation (the example of the graph's representation in the finite-dimensional vector space is given in [11]). This representation [11] is a special case of plafal, because instead of $G_a \subseteq V_w + V_q$ ($a \in E, w, q \in S, w \neq q$), for instance, it can be Ring (the category of rings).

⁴**Remark 1.** In the general case, A is an edge of plafal, P is a vertex of plafal. Between the edge A and two vertices P_1, P_2 , which are connected by A , there is not necessarily a logical relation. **Remark 2.** $a \leftrightarrow A$ (when the edge corresponds to itself); $p \leftrightarrow P$ (when the vertex corresponds to itself). **Remark 3.** Generally, we claim that $G(S, E) \equiv G(PF_j^i)$. **Remark 4.** The graph's properties, as a support of the plafal, are preserved.

Definition 2.1 (Labeled plafal). All or some of edges (vertices) are enumerated⁵. Designation is $PF_{j_l}^{i_k}$, k is a quantity of enumerated edges⁶: $\{\overline{i_1, i_k}\} \xrightarrow{\pi_1} \{\overline{1, i}\}$; l is a quantity of enumerated vertices⁷: $\{\overline{j_1, j_l}\} \xrightarrow{\pi_2} \{\overline{1, j}\}$, (figure 3). Here π_1, π_2 are substitutions.

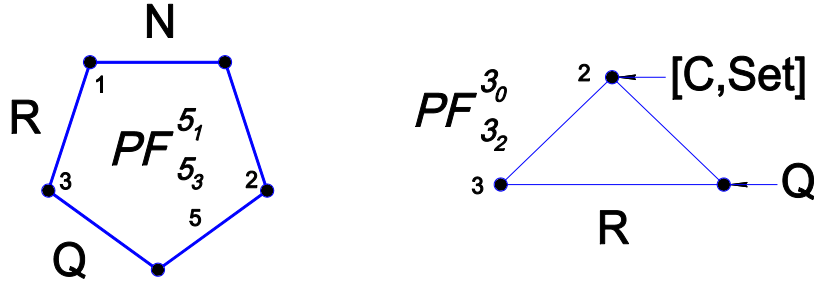


FIGURE 3. $PF_{5_3}^{5_1}$. One edge is enumerated, three vertices are enumerated. $PF_{3_2}^{3_0}$. Two vertices are enumerated.

Let's give a constructive example of using of the theory of plafales in cryptography [10]. For a byte $\{b_7b_6b_5b_4b_3b_2b_1b_0\}$ there is the correspondence that forms the plafal⁸: $b_{8-k} \leftrightarrow i_k, k \in M, M = \{1, 8\}$.

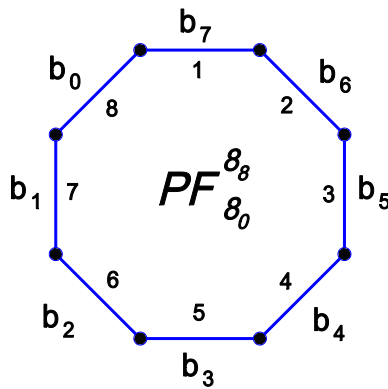


FIGURE 4. $PF_{8_0}^{8_8}$. Eight edges are enumerated.

⁵The camoufleur makes a graph labeling (see section 10).

⁶If $k < i$, then π_1 is an injection; if $k = i$, then π_1 is a bijection.

⁷If $l < j$, then π_2 is an injection; if $l = j$, then π_2 is a bijection.

⁸Edges $\{\overline{i_1, i_k}\}$ are sequential from north to northwest.

3. THE CATEGORY OF PLAFALES

Definition 3.1. Given plafales PF_j^i and $PF_{j'}^{i'}$, a plafal morphism g :

$\langle G(PF_j^i), PF_j^i \rangle \xrightarrow{g=\langle f, \Psi \rangle} \langle G(PF_{j'}^{i'}), PF_{j'}^{i'} \rangle$ is called an ordered pair of maps for which the following conditions hold:

- (1) $G(PF_j^i) \xrightarrow{f} G(PF_{j'}^{i'})$, f is a graph morphism [13];
- (2) $PF_j^i \xrightarrow{\Psi} PF_{j'}^{i'}$: $P \xrightarrow{\psi_{t'}} P'$ and $A \xrightarrow{\psi_{t''}} A'$; $P, A \in PF_j^i$, $P', A' \in PF_{j'}^{i'}$, $\Psi = \{\psi_t\}_{t \in \overline{\{1, (i+j)\}}}$ is a family of maps.

Example is given in figures 5, 6.

Plafales and plafal morphisms (as defined in def. 3.1) form the category **Plafales**, together with the componentwise compositions $\langle f, \Psi \rangle \circ \langle f', \Psi' \rangle = \langle f \circ f', \Psi \circ \Psi' \rangle$ and identities $id_{PF_j^i} = \langle id_{G(PF_j^i)}, id_P, id_A \rangle$.

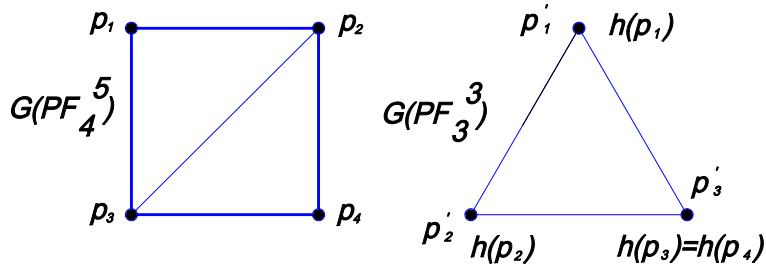


FIGURE 5. Condition 1. The image of $G(PF_4^5)$ under the strict homomorphism is $G(PF_3^3)$.

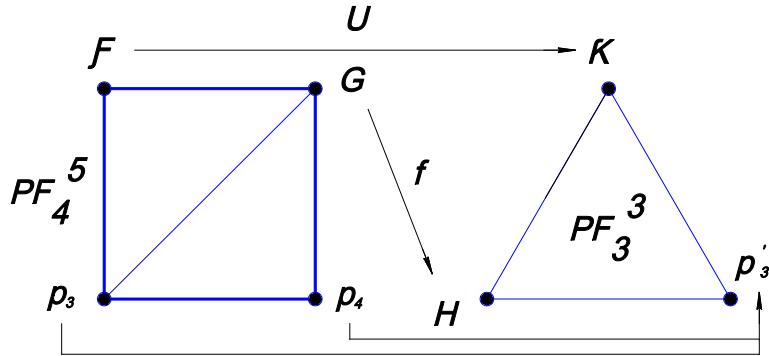


FIGURE 6. Condition 2. U is an accessible cosmological functor between ∞ -cosmoi which are accessible simplicially enriched categories; f is a homomorphism of groups.

Claim 3.2. *In **Plafales**, there're no initial and terminal objects.*

Proof. By definition 3.1 and due to the concept of the plafal, we have the following: the initial object must be $\langle \widehat{0}_{G(PF_j^i)}, \widehat{0}_C \rangle^9$, the terminal object must be $\langle \widehat{1}_{G(PF_j^i)}, \widehat{1}_C \rangle^{10}$. **a. Initial object.** Assume the converse. Consider the single plafal with the following configuration¹¹: $A \leftrightarrow \text{Ob}_{\text{Set}}$ and $P \leftrightarrow \text{Ob}_{\text{Ring}}$. Thus, we get two initial objects $\langle \widehat{0}_{G(PF_j^i)}, \widehat{0}_C = \emptyset \rangle$ and $\langle \widehat{0}_{G(PF_j^i)}, \widehat{0}_C = \mathbb{Z} \rangle^{12}$. Contradiction. **b. Terminal object.** In SiLlStG (The Category of Simple Loopless Graphs with Strict Morphisms) [14], there's no terminal object. This completes the proof of claim 3.2. \square

Given two plafales PF_1 and PF_2 , a product $PF^{prod} = PF_1 \times PF_2$ is defined by the graph product $G = G(PF_1) \times G(PF_2)$ [14] and existence of $P' \times P''$ (in accordance with G), $P' \in PF_1, P'' \in PF_2$; and for edges $A_j \in PF^{prod}$ we have the following: $A_j \leftrightarrow a$. Certainly, G is a simple graph and does not contain an isolated vertex.

Given two plafales PF_1 and PF_2 , a coproduct $PF^{coprod} = PF_1 \oplus PF_2$ is defined by the graph coproduct $G = G(PF_1) \oplus G(PF_2)$ (the disjoint union of graphs) [14] and existence of \coprod for $P, A \in PF_1, P', A' \in PF_2$.

Claim 3.3. *In **Plafales**, the product of any two plafales does not always exist.*

Proof. Consider the discrete category on the two-object set $\{B, A\}$ (this is most easily seen by thinking of $\{B, A\}$ as a discrete poset). The product $B \times A$ does not exist (the proof is trivial). Consider two plafales PF_1 and PF_2 with the following configurations: $P' \leftrightarrow B, P'' \leftrightarrow A, P' \in PF_1, P'' \in PF_2$. Then $B \times A$ does not exist at the $P' \times P''$. This completes the proof of claim 3.3. \square

Claim 3.4. *In **Plafales**, the coproduct of any two plafales does not always exist.*

Proof. Consider the category of fields. $P \leftrightarrow \mathbb{Q}, P' \leftrightarrow \mathbb{Z}/p\mathbb{Z}, P \in PF_1, P' \in PF_2$. Then $P \oplus P'$ does not exist. This completes the proof of claim 3.4. \square

Claim 3.5. ***Plafales** fails to have the following properties:*

- (S1) *NNO (a natural numbers object).*
- (S2) *AC (the axiom of choice).*
- (S3) *A subobject classifier is two-valued.*

Proof. SiLlStG (The Category of Simple Loopless Graphs with Strict Morphisms) fails to have the properties (S1), (S2), (S3) [14]. This completes the proof of claim 3.5. \square

Corollary 3.6. *Limits and colimits fail to exist, exponentiation with evaluation fails to exist, **Plafales** is not a topos. The proof is omitted.*

Remark 5. If the graph product G is a lexicographical product or of other types, then PF^{prod} will be defined in an analogous way.

⁹ $\widehat{0}_{G(PF_j^i)}$ is the initial object in the Categories of Graphs [14].

¹⁰ $\widehat{1}_{G(PF_j^i)}$ is the terminal object in the Categories of Graphs [14].

¹¹See remark 2.

¹² $\widehat{0}_C = \mathbb{Z}$ is the ring of integers.

4. A CANVAS OF THE PLAFALES

Definition 4.1. A canvas of the plafales PF_r^U is an algebraic surface of the first order (plane) which contains $r \in \mathbb{Z}_+ \cup \{0\}$ plafales¹³. If $r = 0$, then PF_0^U is called an empty canvas of the plafales. ${}^pPF_j^i$ (${}^pPF_{j_i}^{i_k}$) is a plafal with an assigned number, $1 \leq p \leq r$.

Definition 4.2. PF^p is an adherent point of PF_r^U . Types: limit point PF^{pl} ; isolated point PF^{pis} . $S(PF^p)$ is the set of all adherent points. $S(PF^{pl}) \subset S(PF^p)$ is the set of all limit points. $S(PF^{pis}) \subset S(PF^p)$ is the set of all isolated points.

Definition 4.3. Interior region of the plafal PF^I is the set of all points located inside of plafal. Exterior region of the plafal PF^E is the set of all points located outside of plafal¹⁴.

Definition 4.4. PF^{Ip} is an adherent point of PF^I . Types: interior limit point PF^{Ipl} ; interior isolated point PF^{Ipis} . PF^{Ep} is an adherent point of PF^E . Types: exterior limit point PF^{Epl} ; exterior isolated point PF^{Epis} .

4.1. Special points.

Definition 4.5. Special limit point (imaginary point) PF^{spl} is a type of PF^{pl} ¹⁵ for which the following correspondence holds:

$$(4.1) \quad PF^{spl} \leftrightarrow [u_1 \cdot c_1(t) \quad W_i^{spl} \cdot c_1(t)],$$

u_1 is a unique parameter¹⁶, $W_i^{spl} = (m_i(x, y, t) \pm 1)$ is a characteristic function¹⁷, $[u_1 \cdot c_1(t) \quad W_i^{spl} \cdot c_1(t)]$ is a state matrix, $c_1(t) = 1$ (see section 5).

Definition 4.6. Special isolated point PF^{spis} is a type of PF^{pis} ¹⁸ for which the following correspondence holds:

$$(4.2) \quad PF^{spis} \leftrightarrow [u_2 \cdot c_2(t) \quad W_i^{spis} \cdot c_2(t)],$$

u_2 is a unique parameter¹⁹, $W_i^{spis} = (n_i(x, y, t) \pm 1)$ is a characteristic function²⁰, $[u_2 \cdot c_2(t) \quad W_i^{spis} \cdot c_2(t)]$ is a state matrix, $c_2(t) = 1$ (see section 5).

¹³The other types of algebraic surfaces are not considered in this paper. PF_r^U is \mathbb{R}^2 equipped with the metric topology. The induced topology on \mathbb{R}^2 defines on $R(K) = \bigcup_{I \in K} \Delta_I \subset \mathbb{R}^2$ the structure of compact space, $\Delta_I = \text{conv}(e_i \mid i \in I, I \subset \{1, 2\})$ is a simplex spans the vectors e_1, e_2 . This compact space $|K|$ is the geometric realization of a 1-dimensional simplicial complex $K = G(S, E)$ [15].

¹⁴ $|K|$ is the Jordan curve, $PF^I = \text{Int } |K|$, $PF^E = \text{Ext } |K|$.

¹⁵ $PF^{spl} \notin |K|$, $S(PF^{spl})$ is the set of all imaginary points.

¹⁶ $u_1 \in \{a \in \mathbb{R}, \text{color}, \dots\}$, u_1 is a same for $S(PF^{spl})$.

¹⁷The coordinates of PF^{spl} are (x, y) , t is a time. $\forall PF^{spl} \exists! W_i^{spl}; W_1^{spl}, \dots, W_k^{spl}$ is a collection of characteristic functions. In the general case, $W_i^{spl} = (m_i(x, y, t) \pm 1)$. If $PF^{spl} \in PF^I$, then $W_i^{spl} = (m_i(x, y, t) + 1)$. If $PF^{spl} \in PF^E$, then $W_i^{spl} = (m_i(x, y, t) - 1)$.

¹⁸ $PF^{spis} \notin |K|$, $S(PF^{spis})$ is the set of all special isolated points.

¹⁹ $u_1 \neq u_2$, u_2 is a same for $S(PF^{spis})$.

²⁰ $\forall PF^{spis} \exists! W_i^{spis}; W_1^{spis}, \dots, W_l^{spis}$ is a collection of characteristic functions. In the general case, $W_i^{spis} = (n_i(x, y, t) \pm 1)$. If $PF^{spis} \in PF^I$, then $W_i^{spis} = (n_i(x, y, t) + 1)$. If $PF^{spis} \in PF^E$, then $W_i^{spis} = (n_i(x, y, t) - 1)$.

Definition 4.7. Flickering point PF^{spf} is a point of PF_r^U for which the following correspondence holds²¹:

$$(4.3) \quad PF^{spf} \leftrightarrow [u_3 \quad W_i^{spf}],$$

$u_3 = (u_1 \cdot c_1(t) + u_2 \cdot c_2(t))$ ²², $W_i^{spf} = (h_i(x, y, t) \pm 1) = (W_i^{spl} \cdot c_1(t) + W_i^{spis} \cdot c_2(t))$ is a characteristic function²³, $[u_3 \quad W_i^{spf}]$ is a state matrix.

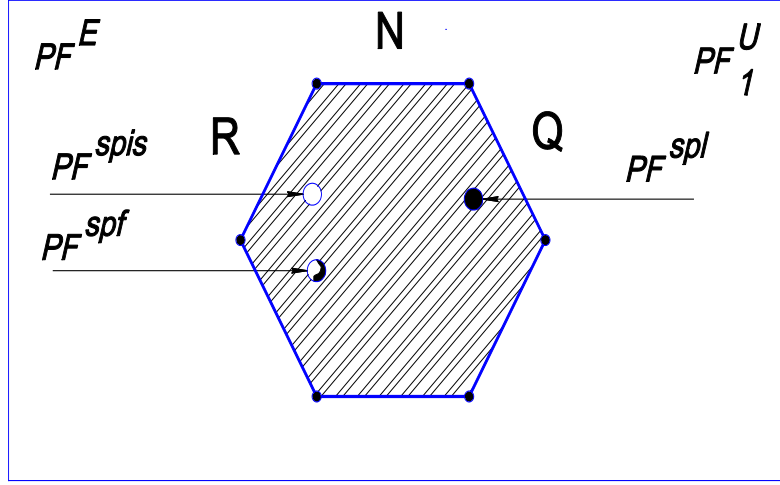


FIGURE 7. The canvas of the plafales PF_1^U : interior region of the plafal, exterior region of the plafal, special limit point, special isolated point, flickering point.

5. ABSOLUTE TRANSITIONS

Definition 5.1. For given PF^{spl} and PF^{spis} let an absolute transition t^{aslis} :

$\langle (x, y), PF^{spl} \rangle \xrightarrow{t^{aslis} = \langle p, h^{aslis} \rangle} \langle (x, y), PF^{spis} \rangle$ be an ordered pair of maps for which the following conditions hold:

- (1) $(x, y) \xrightarrow{p} (x, y)$ (i.e. PF^{spl} and PF^{spis} have the same coordinates);
- (2) $PF^{spl} \xrightarrow{h^{aslis}} PF^{spis}$.

²¹ $PF^{spf} \notin |K|$, $S(PF^{spf})$ is the set of all flickering points. PF^{spf} is an intermediate point in the transition between PF^{spl} and PF^{spis} (see section 5), i.e. PF^{spf} is a superposition of the states PF^{spl} and PF^{spis} , where $c_i(t)$ are the probabilities of the states PF^{spl} and PF^{spis} at the PF^{spf} .

²² $c_2(t) = 1 - c_1(t)$, $0 < c_1(t) < 1$.

²³ $\forall PF^{spf} \exists! W_i^{spf}; W_1^{spf}, \dots, W_s^{spf}$ is a collection of characteristic functions. In the general case, $W_i^{spf} = (h_i(x, y, t) \pm 1)$. If $PF^{spf} \in PF^I$, then $W_i^{spf} = (h_i(x, y, t) + 1)$. If $PF^{spf} \in PF^E$, then $W_i^{spf} = (h_i(x, y, t) - 1)$.

5.1. There's a transition from the special limit point to the special isolated point without returning back.

$$PF^{spl} \xrightarrow{h^{aslis}=f^{asfis} \circ g^{aslf}} PF^{spis}, T_1 \leq t \leq T_2^{24}:$$

$$(5.1) \quad PF^{spl} \xrightarrow{g^{aslf}} PF^{spjf} \xrightarrow{f^{asfis}} PF^{spis}.$$

Using (4.1), (4.2), (4.3) in (5.1), we get (5.2), (5.3).

$$(5.2) \quad \begin{aligned} PF^{spjf} \xrightarrow{g^{aslf}} PF^{spis} : [u_3 \quad W_i^{spjf}] &= [u_1 \cdot c_1(t) \quad W_i^{spl} \cdot c_1(t)] \cdot g^{aslf} = \\ &= [u_1 \cdot c_1(t) \quad W_i^{spl} \cdot c_1(t)] \cdot \begin{bmatrix} 1 & \frac{W_i^{spl} \cdot c_1(t)}{u_1 \cdot c_1(t)} \\ \frac{u_2 \cdot c_2(t)}{W_i^{spl} \cdot c_1(t)} & \frac{W_i^{spis} \cdot c_2(t)}{W_i^{spl} \cdot c_1(t)} \end{bmatrix}, \\ c_1(t) &= \begin{cases} 1, & t \leq T_1, \\ \frac{T_2-t}{T_2-T_1}, & T_1 < t < T_2, \end{cases} \quad c_2(t) = \begin{cases} 0, & t \leq T_1, \\ \frac{t-T_1}{T_2-T_1}, & T_1 < t < T_2, \end{cases} \\ \lim_{t \rightarrow T_1} c_1(t) &= 1, \quad \lim_{t \rightarrow T_1} c_2(t) = 0. \end{aligned}$$

$$(5.3) \quad \begin{aligned} PF^{spjf} \xrightarrow{f^{asfis}} PF^{spis} : [u_2 \cdot c_2(t) \quad W_i^{spis} \cdot c_2(t)] &= [u_3 \quad W_i^{spjf}] \cdot f^{asfis} = \\ &= [u_3 \quad W_i^{spjf}] \cdot \begin{bmatrix} \frac{u_2 \cdot c_2(t)}{u_3} & 0 \\ 0 & \frac{W_i^{spis} \cdot c_2(t)}{W_i^{spjf}} \end{bmatrix}, \\ c_1(t) &= \begin{cases} \frac{T_2-t}{T_2-T_1}, & T_1 < t < T_2, \\ 0, & t \geq T_2, \end{cases} \quad c_2(t) = \begin{cases} \frac{t-T_1}{T_2-T_1}, & T_1 < t < T_2, \\ 1, & t \geq T_2, \end{cases} \\ \lim_{t \rightarrow T_2} c_1(t) &= 0, \quad \lim_{t \rightarrow T_2} c_2(t) = 1. \end{aligned}$$

Definition 5.2. For given PF^{spis} and PF^{spl} let an absolute transition t^{asisl} :

$\langle (x, y), PF^{spis} \rangle \xrightarrow{t^{asisl}=\langle p, h^{asisl} \rangle} \langle (x, y), PF^{spl} \rangle$ be an ordered pair of maps for which the following conditions hold:

- (1) $(x, y) \xrightarrow{p} (x, y)$ (i.e. PF^{spis} and PF^{spl} have the same coordinates);
- (2) $PF^{spis} \xrightarrow{h^{asisl}} PF^{spl}$.

5.2. There's a transition from the special isolated point to the special limit point without returning back.

$$PF^{spis} \xrightarrow{h^{asisl}=f^{asfl} \circ g^{asif}} PF^{spl}, T_1 \leq t \leq T_2^{25}:$$

$$(5.4) \quad PF^{spis} \xrightarrow{g^{asif}} PF^{spjf} \xrightarrow{f^{asfl}} PF^{spl}.$$

²⁴ $PF^{spl} \rightarrow PF^{spjf}$ at time T_1 , $PF^{spjf} \rightarrow PF^{spis}$ at time T_2 .

²⁵ $PF^{spis} \rightarrow PF^{spjf}$ at time T_1 , $PF^{spjf} \rightarrow PF^{spl}$ at time T_2 .

Using (4.1), (4.2), (4.3) in (5.4), we get (5.5), (5.6).

$$\begin{aligned}
PF^{spis} \xrightarrow{g^{asisf}} PF^{spf} : [u_3 \quad W_i^{spf}] &= [u_2 \cdot c_2(t) \quad W_i^{spis} \cdot c_2(t)] \cdot g^{asisf} = \\
&= [u_2 \cdot c_2(t) \quad W_i^{spis} \cdot c_2(t)] \cdot \begin{bmatrix} \frac{u_1 \cdot c_1(t)}{u_2 \cdot c_2(t)} & \frac{W_i^{spl} \cdot c_1(t)}{u_2 \cdot c_2(t)} \\ \frac{u_2 \cdot c_2(t)}{W_i^{spis} \cdot c_2(t)} & 1 \end{bmatrix}, \\
c_1(t) &= \begin{cases} 0, & t \leq T_1, \\ \frac{t-T_1}{T_2-T_1}, & T_1 < t < T_2, \end{cases} & c_2(t) = \begin{cases} 1, & t \leq T_1, \\ \frac{T_2-t}{T_2-T_1}, & T_1 < t < T_2, \end{cases} \\
(5.5) & \qquad \qquad \qquad \lim_{t \rightarrow T_1} c_1(t) = 0, \quad \lim_{t \rightarrow T_1} c_2(t) = 1.
\end{aligned}$$

$$\begin{aligned}
PF^{spf} \xrightarrow{f^{asfl}} PF^{spl} : [u_1 \cdot c_1(t) \quad W_i^{spl} \cdot c_1(t)] &= [u_3 \quad W_i^{spf}] \cdot f^{asfl} = \\
&= [u_3 \quad W_i^{spf}] \cdot \begin{bmatrix} \frac{u_1 \cdot c_1(t)}{u_3} & 0 \\ 0 & \frac{W_i^{spl} \cdot c_1(t)}{W_i^{spf}} \end{bmatrix}, \\
c_1(t) &= \begin{cases} \frac{t-T_1}{T_2-T_1}, & T_1 < t < T_2, \\ 1, & t \geq T_2, \end{cases} & c_2(t) = \begin{cases} \frac{T_2-t}{T_2-T_1}, & T_1 < t < T_2, \\ 0, & t \geq T_2, \end{cases} \\
(5.6) & \qquad \qquad \qquad \lim_{t \rightarrow T_2} c_1(t) = 1, \quad \lim_{t \rightarrow T_2} c_2(t) = 0.
\end{aligned}$$

5.3. There're the transitions from the special limit point to the special isolated point and instantaneous returning back to the special limit point. Combining (5.1) – (5.6), we obtain (5.7).

$$(5.7) \quad \begin{cases} PF^{spl} \xrightarrow{h^{aslis}=f^{asfis} \circ g^{asfl}} PF^{spis}, & T_1 \leq t \leq T_2, \\ PF^{spis} \xrightarrow{h^{asisl}=f^{asfl} \circ g^{asisf}} PF^{spl}, & T_2 \leq t \leq T_3. \end{cases}$$

5.4. There're the transitions from the special isolated point to the special limit point and instantaneous returning back to the special isolated point. Combining (5.1) – (5.6), we obtain (5.8).

$$(5.8) \quad \begin{cases} PF^{spis} \xrightarrow{h^{asisl}=f^{asfl} \circ g^{asisf}} PF^{spl}, & T_1 \leq t \leq T_2, \\ PF^{spl} \xrightarrow{h^{aslis}=f^{asfis} \circ g^{asfl}} PF^{spis}, & T_2 \leq t \leq T_3. \end{cases}$$

5.5. There're $n \leq \infty$ transitions from the special limit (isolated) point to the special isolated (limit) point. Using (5.7), (5.8), we obtain (5.9).

$$(5.9) \quad \begin{cases} PF^{spl}(PF^{spis}) \rightarrow PF^{spis}(PF^{spl}), & T_i \leq t \leq T_{i+1}, \\ PF^{spis}(PF^{spl}) \rightarrow PF^{spl}(PF^{spis}), & T_{i+2} \leq t \leq T_{i+3}, \\ |T_{j+1} - T_j| = \gamma, & \gamma \in \mathbb{Z}_+ \cup \{0\}. \end{cases}$$

Claim 5.3. PF^{spl} , PF^{spis} and morphisms t^{aslis} , t^{asisl} (in accordance with (5.9)) form the category **Plafales-AT**.

Proof. $id = id_{PF^{spl}} = id_{PF^{spis}} = \langle (x, y), \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \rangle$, $t^{aslis} \circ id = t^{aslis}$, $id \circ t^{aslis} = t^{aslis}$, $t^{asisl} \circ id = t^{asisl}$, $id \circ t^{asisl} = t^{asisl}$. \square

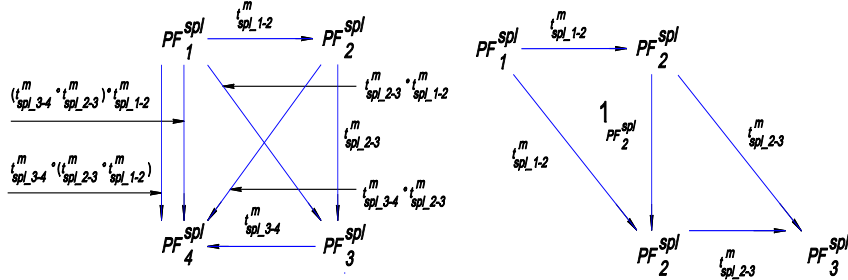
6. MOVING TRANSITIONS

Definition 6.1. For given $PF_1^{spl}, PF_2^{spl} \in S(PF^{spl})$ let a moving transition t_{spl}^m : $\langle (x, y), PF_1^{spl} \rangle \xrightarrow{t_{spl}^m = \langle p, h_{spl}^m \rangle} \langle (x', y'), PF_2^{spl} \rangle$ be an ordered pair of maps for which the following conditions hold:

- (1) $(x, y) \xrightarrow{p} (x', y')$ (i.e. PF_1^{spl} and PF_2^{spl} have different coordinates²⁶);
- (2) $PF_1^{spl} \xrightarrow{h_{spl}^m} PF_2^{spl}$: $[u_1 \cdot c_1(t) \quad W_2^{spl} \cdot c_1(t)] = [u_1 \cdot c_1(t) \quad W_1^{spl} \cdot c_1(t)] \cdot h_{spl}^m = [u_1 \cdot c_1(t) \quad W_1^{spl} \cdot c_1(t)] \cdot \begin{bmatrix} 1 & 0 \\ 0 & \frac{W_2^{spl} \cdot c_1(t)}{W_1^{spl} \cdot c_1(t)} \end{bmatrix}$.

Claim 6.2. $S(PF^{spl})$ and morphisms t_{spl}^m form the category *Plafales-MT-spl*.

Proof. $id = \langle (x, y), \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \rangle$. We get the following commutative diagrams:



□

Definition 6.3. For given $PF_1^{spis}, PF_2^{spis} \in S(PF^{spis})$ let a moving transition t_{spis}^m :

$\langle (x, y), PF_1^{spis} \rangle \xrightarrow{t_{spis}^m = \langle p, h_{spis}^m \rangle} \langle (x', y'), PF_2^{spis} \rangle$ be an ordered pair of maps for which the following conditions hold:

- (1) $(x, y) \xrightarrow{p} (x', y')$ (i.e. PF_1^{spis} and PF_2^{spis} have different coordinates);
- (2) $PF_1^{spis} \xrightarrow{h_{spis}^m} PF_2^{spis}$: $[u_2 \cdot c_2(t) \quad W_2^{spis} \cdot c_2(t)] = [u_2 \cdot c_2(t) \quad W_1^{spis} \cdot c_2(t)] \times h_{spis}^m = [u_2 \cdot c_2(t) \quad W_1^{spis} \cdot c_2(t)] \cdot \begin{bmatrix} 1 & 0 \\ 0 & \frac{W_2^{spis} \cdot c_2(t)}{W_1^{spis} \cdot c_2(t)} \end{bmatrix}$.

Claim 6.4. $S(PF^{spis})$ and morphisms t_{spis}^m form the category *Plafales-MT-spis*. The proof is omitted.

Definition 6.5. For given $PF_1^{spf}, PF_2^{spf} \in S(PF^{spf})$ let a moving transition t_{spf}^m :

$\langle (x, y), PF_1^{spf} \rangle \xrightarrow{t_{spf}^m = \langle p, h_{spf}^m \rangle} \langle (x', y'), PF_2^{spf} \rangle$ be an ordered pair of maps for which the following conditions hold:

²⁶In particular, $x = x'$ or $y = y'$.

- (1) $(x, y) \xrightarrow{p} (x', y')$ (i.e. PF_1^{spf} and PF_2^{spf} have different coordinates);
(2) $PF_1^{spf} \xrightarrow{h_{spf}^m} PF_2^{spf} : [u_3 \quad W_2^{spf}] = [u_3 \quad W_1^{spf}] \cdot h_{spf}^m = [u_3 \quad W_1^{spf}] \cdot \begin{bmatrix} 1 & 0 \\ 0 & \frac{W_2^{spf}}{W_1^{spf}} \end{bmatrix}$.

Claim 6.6. $S(PF^{spf})$ and morphisms t_{spf}^m form the category **Plafales-MT-spf**. The proof is omitted.

By definitions 6.1, 6.3, we have the following:

Definition 6.7. For given $p_1, p_2 \in S(PF^{splis})$ ²⁷ let a moving transition t_{splis}^m :

$\langle (x, y), p_1 \rangle \xrightarrow{t_{splis}^m = \langle p, h_{splis}^m \rangle} \langle (x', y'), p_2 \rangle$ be an ordered pair of maps for which the following conditions hold:

- (1) $(x, y) \xrightarrow{p} (x', y')$ (i.e. p_1 and p_2 have different coordinates);
(2) $p_1 \xrightarrow{h_{splis}^m} p_2$ ²⁸.

Claim 6.8. $S(PF^{splis})$ and morphisms t_{splis}^m form the category **Plafales-MT-splis**. The proof is omitted.

By definitions 6.1, 6.5, we have the following:

Definition 6.9. For given $p_1, p_2 \in S(PF^{splf})$ ²⁹ let a moving transition t_{splf}^m :

$\langle (x, y), p_1 \rangle \xrightarrow{t_{splf}^m = \langle p, h_{splf}^m \rangle} \langle (x', y'), p_2 \rangle$ be an ordered pair of maps for which the following conditions hold:

- (1) $(x, y) \xrightarrow{p} (x', y')$ (i.e. p_1 and p_2 have different coordinates);
(2) $p_1 \xrightarrow{h_{splf}^m} p_2$ ³⁰.

Claim 6.10. $S(PF^{splf})$ and morphisms t_{splf}^m form the category **Plafales-MT-splf**. The proof is omitted.

$$^{27}S(PF^{splis}) = S(PF^{spl}) \cup S(PF^{spis}).$$

$$^{28}PF^{spl} \xrightarrow{h_{splis}^m} PF^{spis} : \begin{bmatrix} u_2 \cdot c_2(t) & W_i^{spis} \cdot c_2(t) \\ u_1 \cdot c_1(t) & W_i^{spl} \cdot c_1(t) \end{bmatrix} = \begin{bmatrix} u_1 \cdot c_1(t) & W_i^{spl} \cdot c_1(t) \\ 0 & \frac{W_i^{spis} \cdot c_2(t)}{W_i^{spl} \cdot c_1(t)} \end{bmatrix} \cdot h_{splis}^m =$$

$$PF^{spis} \xrightarrow{h_{splis}^m} PF^{spl} : \begin{bmatrix} u_1 \cdot c_1(t) & W_i^{spl} \cdot c_1(t) \\ u_2 \cdot c_2(t) & W_i^{spis} \cdot c_2(t) \end{bmatrix} = \begin{bmatrix} u_2 \cdot c_2(t) & W_i^{spis} \cdot c_2(t) \\ 0 & \frac{u_1 \cdot c_1(t)}{u_2 \cdot c_2(t)} \end{bmatrix} \cdot h_{splis}^m =$$

$$= h_{spl}^m; \text{ if } p_1 = p_2 = PF^{spis}, \text{ we have } h_{splis}^m = h_{spis}^m.$$

$$^{29}S(PF^{splf}) = S(PF^{spl}) \cup S(PF^{spf}).$$

$$^{30}PF^{spl} \xrightarrow{h_{splf}^m} PF^{spf} : \begin{bmatrix} u_3 & W_i^{spf} \\ u_1 \cdot c_1(t) & W_i^{spl} \cdot c_1(t) \end{bmatrix} = \begin{bmatrix} u_1 \cdot c_1(t) & W_i^{spl} \cdot c_1(t) \\ 0 & \frac{u_3}{u_1 \cdot c_1(t)} \end{bmatrix} \cdot h_{splf}^m =$$

$$PF^{spf} \xrightarrow{h_{splf}^m} PF^{spl} : \begin{bmatrix} u_1 \cdot c_1(t) & W_i^{spl} \cdot c_1(t) \\ u_3 & W_i^{spf} \end{bmatrix} = \begin{bmatrix} u_3 & W_i^{spf} \\ 0 & \frac{u_1 \cdot c_1(t)}{u_3} \end{bmatrix} \cdot h_{splf}^m =$$

$$= \begin{bmatrix} u_3 & W_i^{spf} \\ 0 & \frac{u_1 \cdot c_1(t)}{u_3} \end{bmatrix} \cdot \begin{bmatrix} u_1 \cdot c_1(t) & W_i^{spl} \cdot c_1(t) \\ 0 & \frac{u_3}{u_1 \cdot c_1(t)} \end{bmatrix}; \text{ if } p_1 = p_2 = PF^{spl}, \text{ we have } h_{splf}^m = h_{spl}^m; \text{ if } p_1 =$$

$$= p_2 = PF^{spf}, \text{ we have } h_{splf}^m = h_{spf}^m.$$

By definitions 6.3, 6.5, we have the following:

Definition 6.11. For given $p_1, p_2 \in S(PF^{spisf})$ ³¹ let a moving transition t_{spisf}^m :

$\langle (x, y), p_1 \rangle \xrightarrow{t_{spisf}^m = \langle p, h_{spisf}^m \rangle} \langle (x', y'), p_2 \rangle$ be an ordered pair of maps for which the following conditions hold:

- (1) $(x, y) \xrightarrow{p} (x', y')$ (i.e. p_1 and p_2 have different coordinates);
- (2) $p_1 \xrightarrow{h_{spisf}^m} p_2$ ³².

Claim 6.12. $S(PF^{spisf})$ and morphisms t_{spisf}^m form the category **Plafales-MT-spisf**. The proof is omitted.

By definitions 6.1, 6.3, 6.5, 6.7, 6.9, 6.11, we have the following:

Definition 6.13. For given $p_1, p_2 \in S(PF^{splisf})$ ³³ let a moving transition t_{splisf}^m :

$\langle (x, y), p_1 \rangle \xrightarrow{t_{splisf}^m = \langle p, h_{splisf}^m \rangle} \langle (x', y'), p_2 \rangle$ be an ordered pair of maps for which the following conditions hold:

- (1) $(x, y) \xrightarrow{p} (x', y')$ (i.e. p_1 and p_2 have different coordinates);
- (2) $p_1 \xrightarrow{h_{splisf}^m} p_2$.

Claim 6.14. $S(PF^{splisf})$ and morphisms t_{splisf}^m form the category **Plafales-MT-splisf**. The proof is omitted.

Corollary 6.15. **Plafales-MT-spl**, **Plafales-MT-spis**, **Plafales-MT-spf**, **Plafales-MT-splis**, **Plafales-MT-splf**, **Plafales-MT-spisf** are the subcategories of **Plafales-MT-splisf**. The proof is streightforward.

By definitions 5.1, 5.2, 6.7, we have the following:

Claim 6.16. $S(PF^{splis})$ and morphisms t^{aslis} , t^{asisl} , t_{splis}^m form the category **Plafales-splis**. The proof is left to the reader.

Corollary 6.17. **Plafales-MT-splis** and **Plafales-AT** are the subcategories of **Plafales-splis**. The proof is streightforward.

Claim 6.18. A singleton $\{x\}$ with $id_{\{x\}}$ is a skeleton of **Plafales-MT-splisf** and **Plafales-splis**. The proof is trivial.

6.1. An ensemble of the special points (SP).

Definition 6.19. An ensemble of the special points $PF_{sp}^{ens} \subset S(PF^{splisf})$ is a plane curve with the following configuration: each point is a special point.

³¹ $S(PF^{spisf}) = S(PF^{spis}) \cup S(PF^{spf})$.

$$\begin{aligned} & \supset PF^{spis} \xrightarrow{h_{spisf}^m} PF^{spf} : \left[\begin{array}{cc} u_3 & W_i^{spf} \end{array} \right] = \left[\begin{array}{cc} u_2 \cdot c_2(t) & W_i^{spis} \cdot c_2(t) \end{array} \right] \cdot h_{spisf}^m = \\ & = \left[\begin{array}{cc} u_2 \cdot c_2(t) & W_i^{spis} \cdot c_2(t) \end{array} \right] \cdot \left[\begin{array}{cc} \frac{u_3}{u_2 \cdot c_2(t)} & 0 \\ 0 & \frac{W_i^{spf}}{W_i^{spis} \cdot c_2(t)} \end{array} \right]; \end{aligned}$$

$$\begin{aligned} & PF^{spf} \xrightarrow{h_{spisf}^m} PF^{spis} : \left[\begin{array}{cc} u_2 \cdot c_2(t) & W_i^{spis} \cdot c_2(t) \end{array} \right] = \left[\begin{array}{cc} u_3 & W_i^{spf} \end{array} \right] \cdot h_{spisf}^m = \\ & = \left[\begin{array}{cc} u_3 & W_i^{spf} \end{array} \right] \cdot \left[\begin{array}{cc} \frac{u_2 \cdot c_2(t)}{u_3} & 0 \\ 0 & \frac{W_i^{spis} \cdot c_2(t)}{W_i^{spf}} \end{array} \right]; \text{ if } p_1 = p_2 = PF^{spis}, \text{ we have } h_{spisf}^m = h_{spis}^m; \text{ if } p_1 = \\ & = p_2 = PF^{spf}, \text{ we have } h_{spisf}^m = h_{spf}^m. \end{aligned}$$

³³ $S(PF^{splisf}) = S(PF^{spl}) \cup S(PF^{spis}) \cup S(PF^{spf})$.

6.2. Dynamical system of the SP.

Definition 6.20. A dynamical system of the SP is a tuple $S^* = \langle T, S(PF^{splisf}), \Phi \rangle$, $(T \times S(PF^{splisf})) \supseteq S^* \xrightarrow{\Phi = \langle \Psi, \Upsilon \rangle} S(PF^{splisf})$, Ψ is a family of maps of the points (x, y) on the plane PF_r^U , $\Upsilon = \{\Upsilon', h_{splisf}^m\}$ is a family of maps³⁴, $S(PF^{splisf})$ is a phase space, $t \in T$.

As an example, let $S(PF^{splisf}) = PF_{sp}^{ens}$ be an unit circle, the position of the point on the unit circle is determined by the angle φ , dynamical system with discrete time is determined by $\Psi = \Psi(\varphi) = 2 \cdot \varphi \pmod{2\pi}$. Therefore, we have

$$S^* \xrightarrow{\Phi = \langle \Psi(\varphi), \Upsilon' \rangle} S(PF^{splisf}).$$

Claim 6.21. S^* with $\Upsilon = \{h_{splisf}^m\}$ can be determined by Υ' .

Proof. It is sufficient to consider the single h_{splisf}^m between two points p_1, p_2 (as defined in def. 6.13). Therefore, we have

$$\langle (x, y), p_1(t_1) \rangle \xrightarrow{\Phi = \langle p, h_{splisf}^m \rangle} \langle (x', y'), p_2(t_2) \rangle.$$

Thus we have $S^* = \langle T = \{t_1, t_2\}, \{p_1, p_2\}, \Phi \rangle$. It is easily shown that S^* can be determined by

$$\begin{cases} \langle (x, y), p_1 \rangle \xrightarrow{\langle p, id \rangle} \langle (x, y), p_1 \rangle, & t \leq t_1, \\ \langle (x', y'), p_2 \rangle \xrightarrow{\langle p', id \rangle} \langle (x', y'), p_2 \rangle, & t_2 \leq t. \end{cases}$$

□

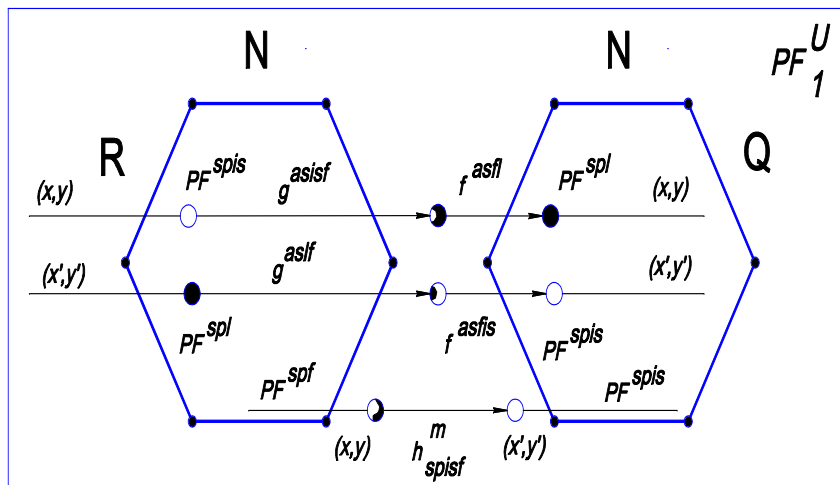


FIGURE 8. Absolute transitions. Moving transitions.

³⁴ $\Upsilon' = \{id = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, h^{aslis}, h^{asisl}, f^{asfis}, f^{asfl}, g^{asif}, g^{aslf}\}$. See sections 5, 6.

7. PLAFALES OPERATIONS

In this section we will consider the basic plafales operations.

7.1. Elementary operations. 1. Vertex deletion ${}^P PF_{ji}^{ik} - P$; 2. Edge deletion ${}^P PF_{ji}^{ik} - A$; 3. Edge addition ${}^P PF_{ji}^{ik} + A$; 4. Subplafal contraction ${}^P PF_{ji}^{ik} \setminus {}^P PF_{ji}^{ik}$; 5. Vertex breeding ${}^P PF_{ji}^{ik} \uparrow P$; 6. Complement plafal $\overline{{}^P PF_{ji}^{ik}}$. The operations are illustrated in figure 9.

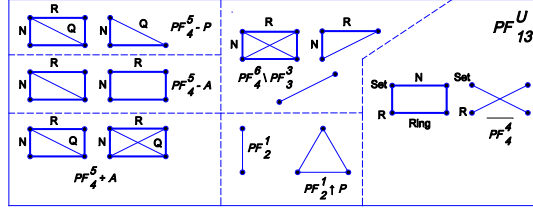


FIGURE 9. Elementary operations.

7.2. Advanced operations.

Definition 7.1. Union of plafales. Given plafales PF_1, \dots, PF_n , a union of plafales $PF_{S_n}^{un} = \bigcup_{i=1}^n PF_i$ is defined by the union of graphs³⁵ $G = \bigcup_{i=1}^n G(PF_i)$, if there exist: $P' \cup P''$ (at the common vertex) and $A' \cup A''$ (at the common edge), where $P', A' \in PF_{j'}$; $P'', A'' \in PF_{j''}$.

Definition 7.2. Docking of plafales. Given plafales PF_1, \dots, PF_n , a docking of plafales $PF_{S_n}^{doc} = \bigcup_{i=1}^n PF_i$ is defined by the union of graphs $G = \bigcup_{i=1}^n G(PF_i)$, for all common edges $a_1, \dots, a_k, \dots, a_m$ and vertices $p_1, \dots, p_l, \dots, p_q$, which are obtained by G , we have the following: $A' \leftrightarrow A_k, A'' \leftrightarrow A_k, P' \leftrightarrow P_l, P'' \leftrightarrow P_l$, where $P', A' \in PF_{j'}$; $P'', A'' \in PF_{j''}$.

Definition 7.3. Docking• of plafales. Given plafales PF_1, \dots, PF_n , a docking• of plafales $PF_{S_n}^{doc\bullet} = \bigcup_{i=1}^n PF_i$ is defined by the union of graphs $G = \bigcup_{i=1}^n G(PF_i)$, for all common edges $a_1, \dots, a_k, \dots, a_m$ and vertices $p_1, \dots, p_l, \dots, p_q$, which are obtained by G , we have the following: $A' \leftrightarrow A_k, A'' \leftrightarrow A_k, P' \leftrightarrow P_l, P'' \leftrightarrow P_l$, if there exist: $A_s = A''' \cup A''''$ and $P_t = P''' \cup P''''$; $P', P''', A', A'''' \in PF_{j'}$; $P'', P'''' \in PF_{j''}$.

Definition 7.4. Intersection of plafales. Given plafales PF_1, \dots, PF_n , an intersection of plafales $PF_{S_n}^{in} = \bigcap_{i=1}^n PF_i$ is defined by the intersection of graphs $G = \bigcap_{i=1}^n G(PF_i)$, if there exist: $P' \cap P''$ (at the common vertex) and $A' \cap A''$ (at the common edge), where $P', A' \in PF_{j'}$; $P'', A'' \in PF_{j''}$.

Definition 7.5. Merger of plafales. Given two plafales PF_1, PF_2 , a merger of plafales $PF_{S_2}^m = \bigcap_{i=1}^2 PF_i$ is defined by the intersection of graphs $G = \bigcap_{i=1}^2 G(PF_i)$, for all edges $a_1, \dots, a_k, \dots, a_m$ and vertices $p_1, \dots, p_l, \dots, p_q$, which are obtained by G , we have the following: $A' \leftrightarrow A_k, A'' \leftrightarrow A_k, P' \leftrightarrow P_l, P'' \leftrightarrow P_l$, where $P', A' \in PF_1$; $P'', A'' \in PF_2$.

³⁵No three of which do not have a common edge.

Definition 7.6. Merger• of plafales. Given two plafales PF_1, PF_2 , a merger• of plafales $PF_{S^2}^m \bullet = \bigcap_{i=1}^2 PF_i$ is defined by the intersection of graphs $G = \bigcap_{i=1}^2 G(PF_i)$, for all edges $a_1, \dots, a_k, \dots, a_m$ and vertices $p_1, \dots, p_l, \dots, p_q$, which are obtained by G , we have the following: $A' \leftrightarrow A_k, A'' \leftrightarrow A_k, P' \leftrightarrow P_l, P'' \leftrightarrow P_l$, if there exist: $A_s = A''' \cap A''''$ and $P_t = P''' \cap P''''$; $P', P''', A', A'''' \in PF_1$; P'', P'''' , $A'', A'''' \in PF_2$.

Definition 7.7. Product• of plafales. Given two plafales PF_1 and PF_2 , a product of plafales $PF^{prod} \bullet = PF_1 \times PF_2$ is defined by the graph product [14] and existence of $P' \times P''$ (in accordance with the graph product), $P' \in PF_1, P'' \in PF_2$; and for edges $a_j \in (G(PF_1) \times G(PF_2))$ we have the following: the camoufleur³⁶ makes the correspondences.

Definition 7.8. Decomposition of plafales. Given plafales PF_1, \dots, PF_n , a decomposition of plafales $PF_{S^n}^d \bullet$ is defined by the decomposition of graphs [16], [17], [18] and for all edges and vertices, which are obtained by the decomposition of graphs, we have the following: the camoufleur makes the correspondences.

Remark 6. G (as defined in def. 7.1 – 7.7) is a simple graph and does not contain an isolated vertex. Decomposition of graphs are the simple graphs and do not contain the isolated vertices.

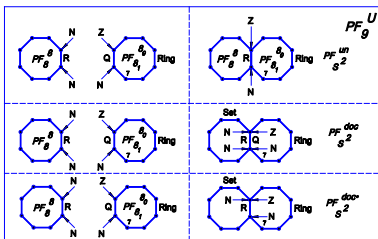


FIGURE 10. Union of plafales, docking of plafales, docking• of plafales.

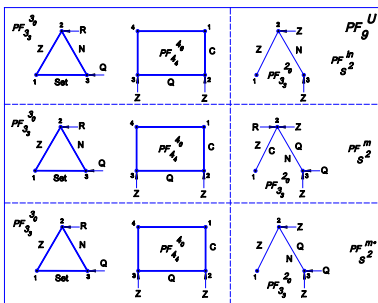


FIGURE 11. Intersection of plafales, merger of plafales, merger• of plafales.

³⁶See section 10.

REFERENCES

- [1] Topchy D. The theory of plafales. UK, Best Global Publishing, 2011, 634 p.
- [2] Topchy D. The theory of plafales. UK, Best Global Publishing, 2013, 695 p.
- [3] Topchy D. The theory of plafales: applications of new cryptographic algorithms and platforms in military complex, IT, banking system, financial market. 42nd Polish Conference on Mathematics Applications. Warsaw, Polish Academy of Sciences, 2013, pp. 58.
- [4] Topchy D. Models of the serendipity family, methods and software for testing non-stationary physical fields. Ph. D. thesis. Mykolaiv, 2017, 152 p. DOI: 10.13140/RG.2.2.20314.77769
- [5] Topchy D. The theory of plafales: quadruple role of the basis functions of serendipity finite elements. Review of the results. Scientific Works of Vinnytsia National Technical University, 2016, no. 2, pp. 72-78.
- [6] Topchy D. The software “Testing of non-stationary temperature fields with dynamic thermo-elements”. Electronic scientific journal “Branch aspects of technical sciences”, Publishing house INGN, 2015, iss. 4 (46), pp. 27-37.
- [7] Topchy D. The theory of plafales: cryptographic complex “ECLECTIC-DT-1”. UK, Chipmunkpublishing, 2015, 65 p.
- [8] Lai X., Massey J. L., Murphy S. Markov ciphers and differential cryptanalysis. Advances in Cryptology, EUROCRYPT’91, Proceedings. Springer Verlag, 1991, pp. 17-38.
- [9] Matsui M. Linear cryptanalysis methods for DES cipher. Advances in Cryptology, EUROCRYPT’93, Proceedings. Springer Verlag, 1994, pp. 386-397.
- [10] Topchy D. The theory of plafales: symmetric-key algorithm “STEEL”. RG, 2018, 72 p. DOI: 10.13140/RG.2.2.10943.97445
- [11] Gelfand I. M., Ponomarev V. A. Gabriel’s theorem is also true for representations of equipped graphs by relations. *Funct. Anal. Appl.*, 1981, vol. 15, iss. 2, pp. 71-72.
- [12] Riehl E., Verity D. *Elements of ∞ -Category Theory*. Cambridge University Press, 2018-2021, 592 p.
- [13] Ehrig H., Ermel C., Golas U., Hermann F. *Graph and Model Transformation. General Framework and Applications*. Springer, 2015, 472 p.
- [14] Plessas D. J. *The Categories of Graphs*. Graduate Student Theses, Dissertations, Professional Papers. Montana, 2011, 123 p.
- [15] Ayzenberg A. *Combinatorics, topology and algebra of simplicial complexes*. Steklov Institute of Mathematics, 2015-2016, 90 p.
- [16] Arumugam S., Sahul Hamid I., Abraham V. M. Decomposition of Graphs into Paths and Cycles. *Journal of Discrete Mathematics*, 2013, vol. 2013, Article ID 721051, 6 pages.
- [17] Tyshkevich R. I., Skums P. V., Suzdal S. V. Algebraic graph decomposition theory. *Proceedings of the Institute of Mathematics*, 2010, vol. 18, iss. 1, pp. 99-115.
- [18] Golovchenko E. N. Survey of graph partitioning algorithms. *Keldysh Institute of Applied Mathematics*, 2020, preprint 2, 38 p.

E-mail address: `dima.topchy@gmail.com`