УДК 004.415.056.5(075) **Павлов І.М., Бірюков В.О.**

РОЗШАРУВАННЯ І ПУЧКИ ТОПОСІВ У ПІДОБ'ЄКТАХ МНОЖИН СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У статті, на базі математичного апарату теорії топосів, розглядається аналіз просторової побудови взаємно ворожих множин, які утворюються при впливі загроз на системи захисту інформації.

Ключові слова: множина, підмножина, об'єкти, підоб'єкти, система захисту інформації, топос, функції.

Вступ. На сьогоднішній день, при проектуванні систем захисту інформації, особливо які знаходяться у системах критичного застосування, обґрунтування структури і складу підсистем, показників їх ефективності, створення моделей захисту інформації не можливо без аналізу загроз, уразливостей систем захисту інформації. Все це необхідно вирішувати опираючись на придатний, для аналізу, математичний апарат (1 - 3).

Постановка проблеми. Процеси захисту інформації підвержені великому впливу випадкових факторів. Методи класичної теорії множин частіше практично не придатні для використання у якості основи науково-методичного базису рішення проблем захисту. Тому, при формуванні теорії захисту інформації, виникає актуальна задача розширення арсеналу класичної математичної теорії за рахунок використання теорії топосів, аналізу просторових взаємовідносин будь-яких множин підоб'єктів, визначення пучків та розшарувань над ними у множинах взаємно ворожих впливів. *Метою статті є* визначення підходів до аналізу розшарування та пучків у підоб'єктах множин ворожих впливів загроз та механізмів захисту інформації.

Основна частина. У основі пучка знаходиться теоретико-множинна структура розшарування.

Визначимо, що A - сукупність множин, які попарно не перетинаються, тобто елементами A є множини, які не мають загальних елементів. Як визначити ці множини?

Введемо множину *I* - міток, або індексів цих множин. Для кожного індексу $i \in I$ мається множина A_i, яка належить цієї сукупності, тоді:

$$\mathrm{A} = \{A_i : i \in I\}. \tag{1}$$

Згідно визначення - члени A попарно не перетинаються, це визначається умовою для будь-яких двох різних індексів $I, j \in I \Rightarrow A_i \cap A_j = \varnothing$. Наочно можна уявити, що множини A_i насаджені на елементи індексної множини *I*, як надано на рис. 1. Якщо визначити A як об'єднання усіх A_i, то:

$$\mathrm{A} = \{x : \text{для деякого } i, \text{при } x \in A_i\}.$$

Відповідно виникає відображення $p : A \to I$. Якщо $x \in A$, то оскільки множини A_i не перетинаються, існує рівно одна множина A_i, така, що $x \in A_i$.

Покладемо, що $p(x) = i$. Таким чином, усі елементи з A_i відображаються у *i*, усі елементи з A_j - у *j* і т.п. Множина A_i може бути представлена як прообраз при відображенні *p* множини $\{i\}$, тобто:

$$p^{-1}(\{i\}) = \{x : p(x) = i\} = A_i, \tag{2}$$

де A_i - шар над *i*, елементи з A_i - ростки у *i*, A - простір розшарування.

Якщо шари не пусті, то відображення *p* сур'єктивно. Для $p : A \to I$, то

$$A_i = p^{-1}(\{i\}) \text{ при } i \in I,$$

$$\mathrm{A} = \{p^{-1}(\{i\} : i \in I)\} = \{A_i : i \in I\}, \tag{3}$$

де A - розшарування множин над *I*, вихідна множина *A* – простір розшарування, вихідна функція *p* – відображення цього розшарування (так як ні у якому *x* функція *p* не може приймати двох різних значень, тобто шари не перетинаються).

Тому розшарування множин над *I* уявляє собою функцію, область значень якої є множина *I*.

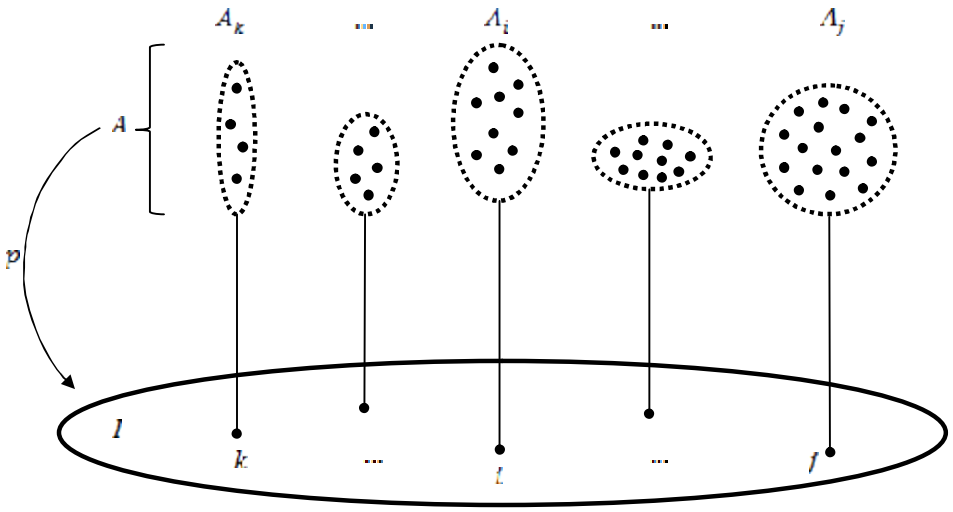


Рис. 1. Структура розшарування множин над базисним простором (базою)

Для визначення функції як розшарування позначимо відносну категорію $\mathrm{Set}\downarrow I$ як $\mathrm{Bn}(I)$. Таким чином, $\mathrm{Bn}(I)$-об'єкти, це пари (*A*,*f*), де $f: A \to I$ - теоретико-множинна функція, а $\mathrm{Bn}(I)$-стрілки $k:(A,f)\to(B,g)$ це функції $k: A \to B$, для яких діаграма, яка наведена на рис. 2. комутативна, тобто $g \circ k = f$. Це означає, що якщо $f(x) = i$ для $x \in A$, то $g(k(x)) = i$, тобто, якщо $x \in A_i$, то $k(x) \in B_i$. Таким чином, *k* відображає ростки у *i* розшарування (*A*,*f*) та ростки у *i* розшарування (*B*,*g*). Категорія $\mathrm{Bn}(I)$ є топосом. Його "множини" - це розшарування множин.

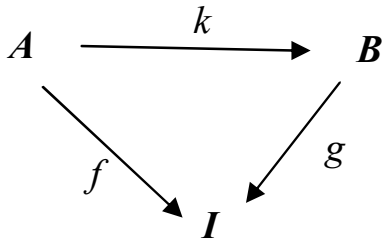
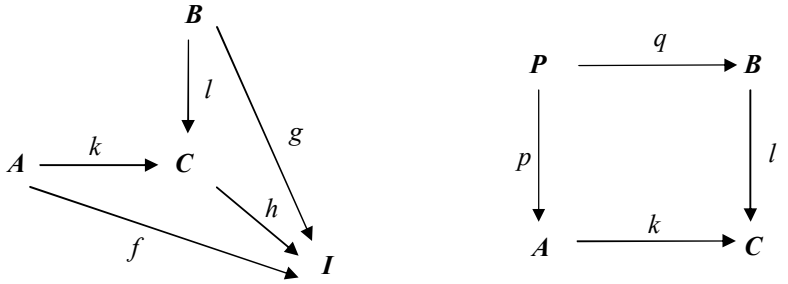


Рис. 2. Комутативна діаграма множин з функціями $g \circ k = f$

Кінцевим об'єктом множин у $\mathrm{Bn}(I)$ є тождествена функція $\mathrm{id}_I: I \to I$, і для вільного розшарування (*A*,*f*) єдиною стрілкою $(A,f)\to(\mathrm{id}_I)$ є сама функція $f: A \to I$. Шаром функції id_I над *i* служить множина $\mathrm{id}_I^{-1}(\{i\}) = \{i\}$, яка є кінцевим об'єктом у **Set**. Таким чином, кінцевий об'єкт у $\mathrm{Bn}(I)$ є розшаруванням над *I* кінцевих об'єктів з **Set**. Єдина стрілка $f:(A,f)\to(I,\mathrm{id}_I)$ може бути представлена як розшарування $\{f_i : i \in I\}$ відповідних єдиних **Set**- стрілок.

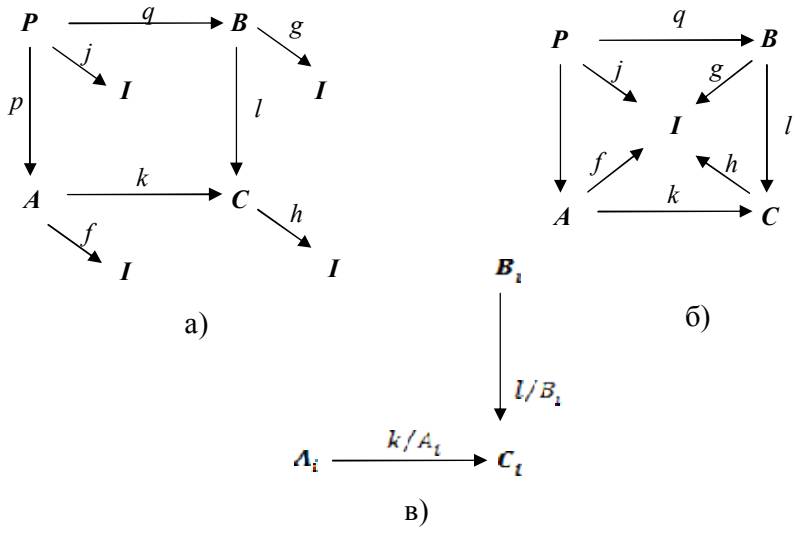
Розкриємо зворотній образ множин. Для даних $\mathrm{Bn}(I)$ - стрілок $k:(A,f)\to(C,h)$ та $l:(B,g)\to(C,h)$ с комутативною у **Set** діаграмою, яка надана на рис. 3а., побудуємо у **Set** зворотній образ стрілок *k* і *l*, який наданий декартовим квадратом (рис. 3 б).



а) б)

Рис. 3. а) Комутативна діаграма множин $k:(A,f)\to(C,h)$ та $l:(B,g)\to(C,h)$;
б) зворотній образ стрілок *k* і *l*, який наданий декартовим квадратом

Тоді діаграма, яка надана на рис. 4а, буде уявляти собою зворотній образ у $\mathrm{Bn}(I)$ стрілок *k* і *l*, де $j=f\circ p=h\circ k\circ p=h\circ l\circ q=g\circ q$. Цю діаграму правильніше зображати у вигляді, який наданий на рис. 4 б. У подальшому, якщо A_i,B_i,C_i - шари над *i* розшарувань *f*, *g*, *h* відповідно, то областю визначення зворотнього образу пари (рис. 4 в) $\langle k/A_i,l/B_i\rangle$ (де пара уявляє собою обмеження функцій *k*, *l* над множинами A_i, B_i, відповідно), буде служити множина $\{\langle x,y\rangle : x\in A_i, y\in B_i \text{ та } k(x)=l(y)\}$ яка співпадає з множиною $\{\langle x,y\rangle : x\in A, y\in B \text{ та } j\langle x,y\rangle = i\} = j^{-1}(\{i\})$, тобто з шаром над і розшарування $j:P\to I$.



а) б) в)

Рис. 4. а, б) зворотний образ у $\mathrm{Bn}(I)$ стрілок *k* і *l*, де $j=f\circ p=h\circ k\circ p=h\circ l\circ q=g\circ q$;
в) області визначення зворотного образу пари $\langle k/A_i,l/B_i\rangle$

Таким чином, зворотнім образом у $\mathrm{Bn}(I)$ є розташування зворотних образів у **Set**. Класифікатором підоб'єктів для $\mathrm{Bn}(I)$ є розшарування двоелементних множин, тобто розшарування **Set**-класифікаторів.

Визначимо (рис. 5) Ω рівнянням $\Omega = (2 \times I, p)$, де p_i - проекція на другий множник, $p_I(\langle x, y \rangle) = y$.

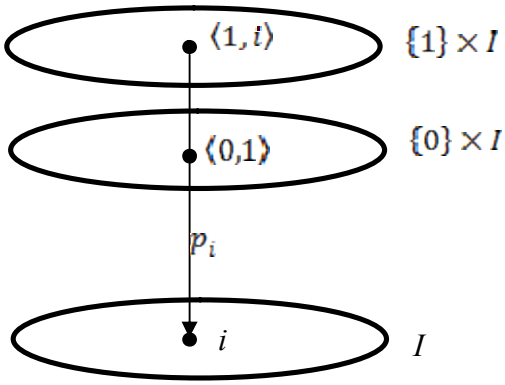


Рис. 5. Об'єднання ізоморфних множин, які не перетинаються

Множину $2 \times I$ можна представити як об'єднання множин, які не перетинаються,

$$\{0\} \times I = \{\langle 0, i \rangle : i \in I\} \text{ та } \{1\} \times I = \{\langle 1, i \rangle : i \in I\}, \quad (4)$$

кожне з яких ізоморфно. А шаром над *i* є двоелементна множина:

$$\Omega_i \{\langle 0, i \rangle, \langle 1, i \rangle = 2 \times \{i\}\}. \quad (5)$$

Стрілкою класифікатора $T : 1 \to \Omega$ може розглядатися розшарування класифікованих функцій true. Визначимо $T : I \to 2 \times I$ рівнянням $T(i) = \langle 1, i \rangle$.

Візьмемо монострілку $k : (A, f) \to (B, g)$ у $\mathrm{Bn}(I)$ (рис. 6).

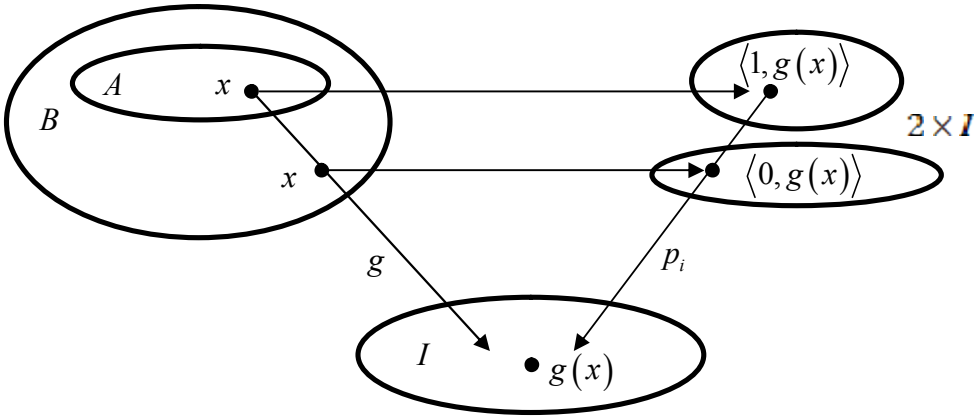


Рис. 6. Розподіл підмножин множин

Тоді $k : A \to B$ буде монострілкою у **Set** і можна рахувати, що *k* є включенням, тобто $A \subseteq B$ і $f(x) = g(x)$ для усіх $x \in A$.

Для визначення характеристичної стрілки $\chi_k : (B, g) \to \Omega = (2 \times I, p_I)$, щоб побудувати комутативну діаграму, наведену на рис. 7., при $x \in A$, або $x \notin A$ визначимо 1 або 0 у залежності від того, який випадок має місце. Для чого зробимо вибір у відповідному правому шарі (рис. 6).

При цьому повинно виконуватися рівняння $p_I \circ \chi_k = g$. Формально $\chi_k : B \to 2 \times I$ дорівнює добутку $\langle \chi_A, g \rangle : B \to 2 \times I$, де $\chi_A : B \to 2$ - звичайна характеристична функція множини *A*, тобто:

$$\chi_k(x)=\begin{cases}\langle 1, g(x)\rangle, & \text{якщо } x\in A,\\ \langle 0, g(x)\rangle, & \text{якщо } x\notin A.\end{cases} \tag{6}$$

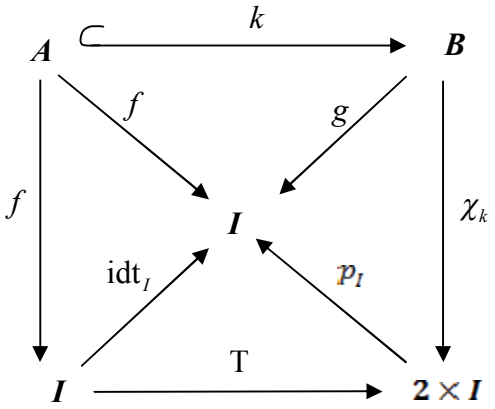


Рис. 7. Комутативна діаграма декартового квадрату множин для $\chi_k:(B,g)\to\Omega=(2\times I, p_I)$

Функція $\mathrm{T}: I\to 2\times I$ має наступну властивість: її значення $\mathrm{T}(i)=\langle 1,i\rangle$ є ростком у i. Функція з базисної множини I у просторі розшарування, яка обирає один росток з кожного шару, ще має назву січення цього розшарування. Іншою мовою, $s: I\to A$ є січенням розшарування $f: A\to I$, якщо $s(i)\in A_i=f^{-1}(\{i\})$ для усіх $i\in I$, тобто якщо $f(s(i))=i$ для усіх $i\in I$.

Під пучком розуміється розшарування, яке має деякі додаткові топологічні структури [4, 5]. Визначимо, що I - топологічний простір і Θ - сукупність його відкритих множин. Тоді пучком над I називають пару (A, p), де A – топологічний простір і $p: A\to I$ - безперервне відображення, яке є локальним гомеоморфізмом. Тобто кожна точка $x\in A$ має відкриту площину U, яка гемеоморфно відображається функцією p на множину $p(U)=\{p(y): y\in U\}$, яка є відкритою у I. Об'єктами категорії **Top** (I) пучків над I служать пари (A, p), які є пучками, а стрілками $k:(A,p)\to(B,g)$ - безперервні відображення $k: A\to B$ такі, що діаграма, яка наведена на рис. 8 а комутативна. Таке відображення k є відкритим.

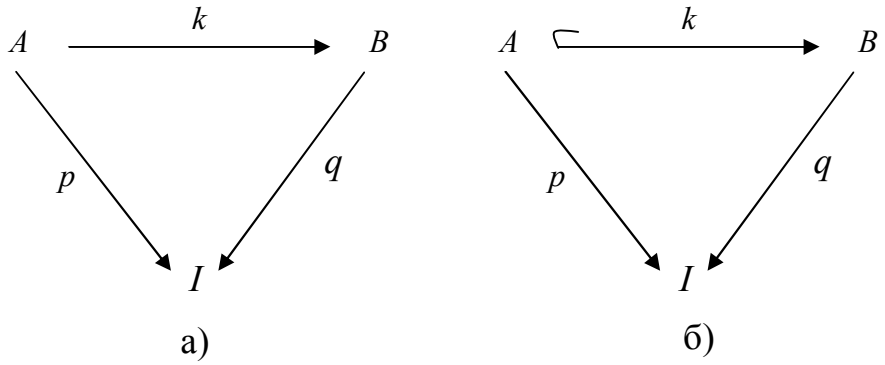


Рис. 8. Комутативні діаграми об'єктів категорії **Top** (I)

Категорію **Top** (I) є топосом і ще її називають просторовим топосом. Його кінцевим об'єктом служить функція $\mathrm{id}_I: I\to I$. Об'єкт класифікації Ω топосу **Top** (I) називають

пучком ростків відкритих у *I* множин. Побудова цього пучка ілюструє наступний загальний метод утворення розшарувань над *I*. У деякій множині *X* кожна точка $i \in I$ визначає відношення еквівалентності $\square_i$ на *X*. Шар над *i* визначається як фактор-множина $X / \square_i$ класів еквівалентності відносно $\square_i$.

У випадку об'єкту класифікації у якості *X* береться сукупність Θ усіх відкритих у *I* множин. Для кожного $i \in I$ відношення $\square_i$ визначається наступним чином:

$U \square_i V$ якщо і тільки якщо існує деяка відкрита множина W, така, що $i \in W$ і $U \cap W = V \cap W$. Тоді $\square_i$ є відношення еквівалентності. Тобто інтуїтивно еквівалентність $U \square_i V$ означає, що точки з *U*, які близькі до *i* співпадають з точками з *V*, які близькі до *i*, тобто поблизу і множини *U* і *V* не різняться або пропозиція "$U = V$" "локально істина" у *i*.

Клас еквівалентності $[U]_i = \{V : U \square_i V\}$ називають ростком місцевості *U* у *i*. Це сукупність точок з *U* близьких до *i* [6]. У якості шару над *i* візьмемо множину $\Omega_i = \{\langle i, [U]_i \rangle : U$ відкрито у $I\}$. Тоді об'єкт Ω у **Top** (*I*) визначається як відповідна функція $p : \text{Ł} \to I$, де Ł - об'єднання шарів Ω_i, а *p* для значень аргументу, які належать Ω_i, дає *i*. Надамо пояснення до рис. 9. Топологія на Ł визначається базою, яка складається з усіх множин:

$$[U, V] = \{\langle i, [U]_i \rangle : i \in V\}, \tag{7}$$

де *V* відкрито і $U \subseteq V$. Відображення *p* тоді стає локальним гомеоморфізмом, а кожен шар - дискретним простором у відносній топології.

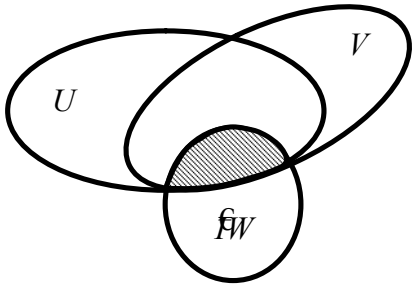


Рис. 9. Об'єднання шарів множин

Властивості ростків:

1. $[U]_i = [I]$ тоді і тільки тоді, коли $i \in U$.
2. $[I]_i = \Theta_i$.
3. $[I]_i = [\varnothing]_i$ тоді і тільки тоді, коли і відокремлено від *U* (тобто існує $V \in \Theta_i$, таке, що $U \bigcap V = \varnothing$).

Розглянемо істинні значення $s : 1 \to \Omega$. Стрілки такого вигляду є безперервними січеннями розшарування Ω, які ще мають назву глобального січення пучка. Для відкритої у *I* підмножини *U* визначимо $S_U : I \to$ Ł рівнянням $S_U(i) = \langle i, [U]_i \rangle$. Рівняння S_U є безперервним глобальним січенням, тобто $S_U : 1 \to \Omega$. У силу першої властивості рівняння $S_U(i) = \langle i, [U]_i \rangle$ має місце тоді і тільки тоді, коли $i \in U$. Крім того, якщо $s : 1 \to \Omega$ - вільне безперервне січення Ω і $U = \{i : s(i) = \langle i, [I]_i \rangle\}$, то множина *U* відкрита $\left(U = S^{-1}(I, \text{Ł})\right)$ і $S_U = s$.

Таким чином, істинні значення у **Top** (*I*) – це у сутності відкриті підмножини простору *I*, у той час як у **Bn** (*I*) ними були усі підмножини у *I*.

Стрілка $\mathrm{T}:1\to\Omega$ визначається як безперервне січення $\mathrm{T}:I\to\mathbb{C}$ для якого $\mathrm{T}(i)=\langle i,[I]_i\rangle$ при усіх $i\in U$. Нехай k – монострілка, для якої діаграма, наведена на рис. 8 б комутативна і A - відкрита підмножина у B. Характеристичну стрілку $\chi_k:(B,q)\to\Omega$ побудуємо наступним чином. Нехай $i\in B$, тоді виберемо площину S точки x, у якій q є локальним геоморфізмом (рис. 10). Тоді значення функції $\chi_k:B\to I$ у точці x покладемо рівним ростку відкритої множини $q(A\cap S)$ у $q(x)$, тобто: $\chi_k(x)=\langle q(x),[q(A\cap S)]_{q(x)}\rangle$.

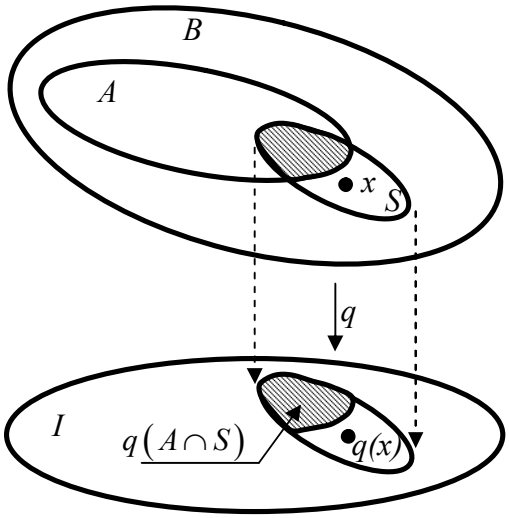


Рис. 10. Ростки відкритої множини $q(A\cap S)$ у $q(x)$
під час безперервного січення множин

Інтуїтивно, росток множини $q(A\cap S)$ у $q(x)$, де q - локальний геоморфізм, уявляє у I множину точок з A близьких до x. Він дає міру віддаленості x від A. У той-же час, як у теорії множин, допускається тільки дві можливості: або $x\in A$, або $x\notin A$ - у топологічному контексті можливо більш тонка різниця по ступені близькості x до A. Розглядаються ростки у $q(x)$ як міра ступені близькості x до відкритих підмножин у B. Визначимо на $\Omega_{q(x)}$ частковий порядок наступною умовою: $[U]_{q(x)}\sqsubseteq[V]_{q(x)}$ тоді і тільки тоді, коли існує відкрита підмножина $W\subseteq I$ таке, що $q(x)\in W$ і $U\cap W\subseteq V\cap W$.

Тобто $[U]_{q(x)}\sqsubseteq[V]_{q(x)}$, якщо пропозиція $U\subseteq V$ локально істинна у $q(x)$. Чім більше, у смислі цього порядку, росток множини $q=(A\cap S)$, тим ближче x до A, то $q(x)\in q(A\cap S)$ і згідно першої властивості ростків росток множини $q(A\cap S)$ стає самим великим з можливих, тобто $[q(A\cap S)]_{q(x)}\subseteq[I]_{q(x)}$.

У іншому граничному випадку, коли x відділено від A, росток буде найменшим з можливих, тобто $[q(A\cap S)]_{q(x)}\subseteq[\varnothing]_{q(x)}$. З іншого боку, коли x знаходиться на кордоні, росток $[q(A\cap S)]$ розташований суворо між ростками множин $\varnothing$ та I, тобто $[\varnothing]\subset[q(A\cap S)]\subset[I]$.

У вільному топосі експоненціал Ω^a є аналогом множини 2^A для категорії Set [7, 8]. У зв'язку з ізоморфізмом $2^A\cong P(A)$ виникає питання зможуть властивості об'єкту Ω^a бути аналогічними властивостям "множини-ступені" множини a.

Для множин A і B існує бієктивна відповідність між функціями з B у $P(A)$ і відношеннями з B у A. Функція $f: B \to P(A)$ визначає відношення $R_f \subseteq B \times A$, яке задається еквівалентністю:

$$xR_f y \Rightarrow y \in f(x), \tag{8}$$

де $x \in B$, $y \in A$. Зворотньо, відношення $R_f \subseteq B \times A$ визначає функцію $f_R: B \to P(A)$, яка задається рівнянням $f_R(x) = \{y : y \in A \text{ і } xRy\}$. Ці два відображення (одне переводить R у f_R, а інше f у R_f) є зворотнім одного до іншого, і встановлюють ізоморфізм.

Розглянемо відношення належності $\in_A$ з $P(A)$ у A. Це відношення має усю інформацію про те, які підмножини множини A які елементи мають. Точніше $\in_A = \{\langle U, x\rangle : U \subseteq A, x \in A \text{ і } x \in U\}$.

Переходячи від $P(A)$ до 2^A і замінюючи умову "$x \in U$" на умову "$\chi_U(x) = 1$" отримуємо відношення $\in_A$ яке ізоморфно множині: $\in'_A = \{\langle \chi_U, x\rangle : U \subseteq A, x \in A \text{ і } \chi_U(x) = 1\} \subseteq 2^A \times A$.

Характеристична функція підмножини $\in'_A$ множини $2^A \times A$ уявляє собою стрілку значення $\mathrm{ev}: 2^A \times A \to 2$ так як $\mathrm{ev}(\chi_U, x) = \chi_U(x)$. Таким чином, можна охарактеризувати $\in'_A$ (і з точністю до ізоморфізму $\in_A$) за допомогою декартового квадрату, який наведений на рис. 11 а.

У подальшому, якщо $R \subseteq B \times A$ - вільне відношення, то $\langle x, y\rangle \in R$ тоді і тільки тоді, коли $y \in f_R(x)$, а також $\langle f_R(x), y\rangle \in \in_A$.

Тобто, R є прообразом множини $\in_A$ при відображенні $f_R \times 1_A$, який переводить пару $\langle x, y\rangle$ у пару $\langle f_R(x), y\rangle$.

Таким чином, діаграма, яка наведена на рис. 11 б, у якій g визначає обмеження $f_R \times \mathrm{id}_A$ на R, є декартовим квадратом.

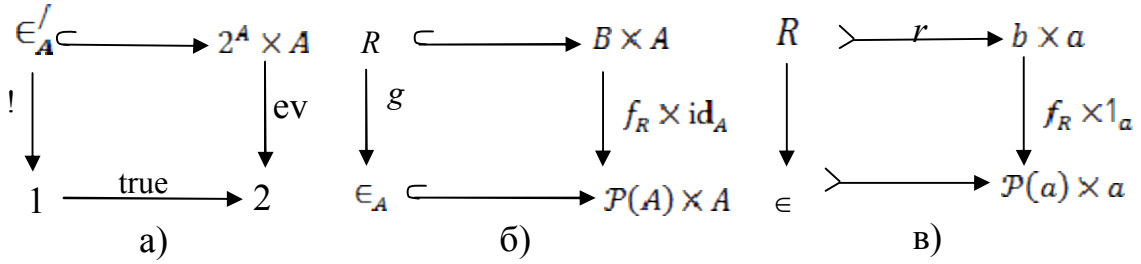


Рис. 11.Декартові квадрати для:
а) $\mathrm{ev}: 2^A \times A \to 2$; б) $f_R \times \mathrm{id}_A$; в) $\in : \in_A \mapsto P(a) \times a$

Для цього R функція f_R – єдина функція, для якої квадрат декартовий.

Визначаємо, що категорія ε має об'єкти-ступені, якщо для кожного ε-об'єкту існують ε-об'єкти $P(a)$ та $\in_A$ і монострілка $\in : \in_A \mapsto P(a) \times a$, такі, що для вільного ε-об'єкту b і відношення $r: R \mapsto b \times a$ існує єдина ε-стрілка $f_r: b \to P(a)$, для якої квадрат, наведений на рис. 11 в є декартовим при деякій ε-стрільці $R \to \in_A$.

Заключення.

У подальшому виникає питання визначення об'єктів-ступенів у топосах, принципів згортання та побудови образів стрілок у взаємно загрозливих множинах. Усі ці питання необхідно розглядати у комплексі послідовно розкриваючи кроки побудови моделей взаємовідносин таких множин.

ЛІТЕРАТУРА

1. Бірюков В.О. Композиція і категорії функцій систем загроз в областях систем захисту інформації / В.О. Бірюков, І.М. Павлов. – Захист інформації. – № 1. – 2013. – С. 28 – 37.
2. Павлов І.М. Морфізм функцій і бієктивність об'єктів при проекції множин загроз та областей систем захисту інформації / І.М. Павлов. – Сучасна спеціальна техніка. – № 1. – 2013. – С. 36 – 45.
3. Павлов І.М. Проектування комплексних систем захисту інформації / І.М. Павлов, В.О. Хорошко. – К.: 2011. – 245 с.
4. Manes E. G. Category Theory Applied to Computation and Control, Lecture Notes in Computer Science, Vol. 25, Springer-Verlag, 1996.
5. Аксиоматична теорія множин: навч. посіб. / М.М. Попов. – Чернігівський національний університет (ЧНУ). – 2011. – 79 с.
6. Grayson. R. Heyting-valued models for intuitionistic set theory. – Lecture Notes in Mathematics. 2002, p. 402.
7. Topos di Grothendieck e topos di Lawvere e Tierney. Rendiconti de Matematica, 7, 1974, 513 – 553.
8. Modeles dun Categorie Logique dans des Topos de P re faisceaux et d'Ensembles de Heyting, Memoire de La Maitrise es Sciences, Universite de montreal, 1975.

Надійшла: 02.04.2013 р.

Рецензент: д.т.н., проф. Толюпа С.В.