

УДК 004.056

ПРОВЕРКА СООТВЕТСТВИЯ ОРИЕНТИРОВАННОГО ГРАФА АЛГЕБРАИЧЕСКОЙ РЕШЁТКЕ

С. В. Белим, Н. Ф. Богаченко

Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия

Рассмотрена проблема проверки изоморфности ориентированного графа диаграмме некоторой решётки. Исследованы три типа конечных решёток, используемых в моделях разграничения доступа. Построен алгоритм проверки соответствия ориентированного графа прямому произведению решётки подмножеств и линейной решётки. Алгоритм основан на анализе структуры двух множеств: множества вершин, покрывающих ровно одну вершину, и множества атомарных вершин. Доказано, что вычислительная сложность алгоритма проверки не превосходит $O(n^3)$.

Ключевые слова: *граф, теория решёток, мандатное разграничение доступа.*

DOI 10.17223/20710410/41/6

THE CHECK OF THE CORRESPONDENCE OF THE DIRECTED GRAPH TO THE ALGEBRAIC LATTICE

S. V. Belim, N. F. Bogachenko

*Dostoevsky Omsk State University, Omsk, Russia***E-mail:** belimsv@omsu.ru, nfbogachenko@mail.ru

The isomorphism check problem for a directed graph and a lattice diagram is considered in this paper. Three specific finite lattices used in the access control models are investigated. Special attention is paid to *MLS*-lattice which is the Cartesian product of the lattice of subsets and the linear lattice. Necessary and sufficient conditions for the isomorphism of a finite lattice S to the *MLS*-lattice are found. For the lattice S , these conditions define some limitations to the number of all nodes, of atomic nodes, and of nodes covered by each element of the lattice S . An algorithm which checks the correspondence of the directed graph to the *MLS*-lattice is offered. This algorithm is based on the structure of two sets: the set of the nodes which cover exactly one node and the set of the atomic nodes. The following conditions are checked: the number of nodes of the directed graph $n = 2^{n_1}n_2$; all nodes of the directed graph cover at least two others except the nodes $x_1, \dots, x_{n_1}, t, t_1, \dots, t_{n_2-1}$, wherein t is an outlet of the directed graph; the nodes $x_1, \dots, x_{n_1}, t_1, \dots, t_{n_2-1}$ cover exactly one node; the nodes $x_1, \dots, x_{n_1}, t_1$ are atomic nodes; the nodes $t_{n_2-1}, \dots, t_1, t$ form a chain $t_{n_2-1} \succ \dots \succ t_1 \succ t$ in which the nodes successively cover each other. We prove that the computing complexity of this algorithm does not exceed $O(n^3)$.

Keywords: *graph, lattice theory, mandatory access control.*

Введение

Работа посвящена проблеме поиска решётки, соответствующей заданному орграфу G . Данная проблема находит применение при построении и оптимизации структур, на которых строится политика безопасности компьютерных систем [1]. Можно выделить два случая:

- 1) Орграф G может быть дополнен до диаграммы некоторой решётки без добавления новых вершин. Необходимо определить соответствующую ему решётку. При этом под дополнением графа понимается построение его транзитивного замыкания — пополнение графа всеми дугами, соединяющими достижимые вершины.
- 2) Для построения диаграммы некоторой решётки необходимо дополнить орграф G как вершинами, так и рёбрами. В этом случае необходимо определить минимальную решётку, диаграмма которой включает данный орграф. Минимизируется число элементов решётки.

Остановимся на первой задаче, которая частично связана с пятой проблемой Бирхофа [2]. Различные вопросы, касающиеся графов, соответствующих решёткам, рассматриваются в [3–7]. Во всех этих работах авторы исходят из существования некоторой решётки, строят соответствующей ей граф и проводят его исследования. Актуальной представляется и обратная задача — исследовав свойства графа, сопоставить ему некоторую решётку. Нас интересует решётка, полученная в результате прямого произведения решётки подмножеств и линейной решётки. Основная цель исследования — построение и оценка вычислительной сложности алгоритма проверки соответствия ориентированного графа такой решётке.

1. Решёточный граф

Определение 1. Частично упорядоченное множество S называется решёткой, если для любых двух его элементов $x, y \in S$ в множестве S можно найти их точную верхнюю и точную нижнюю грани: $\sup\{x, y\}, \inf\{x, y\} \in S$.

Орграф $G = (V, E)$, не содержащий ориентированных циклов, задаёт отношение частичного порядка на множестве своих вершин: $v_1 \geq v_2$ ($v_1, v_2 \in V$) тогда и только тогда, когда в орграфе существует ориентированный путь $p(v_1, v_2)$. Очевидно, что полученное множество не всегда является решёткой.

Определение 2. Ориентированный граф будем называть решёточным, если его вершины образуют решётку с отношением порядка « $\geq$ », порождённым ориентированными путями орграфа.

Имея в распоряжении матрицу смежности орграфа, несложно доказать следующий факт.

Теорема 1. Трудоемкость проверки, является ли орграф решёточным, не превышает $O(n^4)$.

Рассмотрим далее некоторые частные решения задачи восстановления решётки. На сегодняшний день в моделях безопасности компьютерных систем получили широкое распространение три решётки:

- 1) Линейная решётка. Под линейно упорядоченным множеством B понимается множество, для любых двух элементов которого определено отношение порядка. Как легко показать, такое множество образует решётку: если $a \geq b$, то $\sup\{a, b\} = a$ и $\inf\{a, b\} = b$. Решётка данного вида является наиболее распространённой в системах защиты информации, она описывает уровни доступа к данным. Если $B = \{0, 1, \dots, m-1\}$, то линейная решётка обозначается $SL(m)$.
- 2) Решётка подмножеств. Пусть задано множество A мощности n . Рассмотрим множество всех его подмножеств $2^A = \{X : X \subseteq A\}$. Введём на множестве 2^A отношение порядка: $\forall X_1, X_2 \in 2^A (X_1 \geq X_2 \Leftrightarrow X_1 \supseteq X_2)$. Легко доказать, что

отношение $X_1 \supseteq X_2$ есть отношение нестрогого порядка, а множество 2^A частично упорядоченное: так, не для любой пары элементов определено отношение порядка. Наибольшую нижнюю и наименьшую верхнюю грани определим на основе операций пересечения и объединения множеств: $\inf\{X_1, X_2\} = X_1 \cap X_2$, $\sup\{X_1, X_2\} = X_1 \cup X_2$. Также нетрудно доказать, что $(2^A, \supseteq, \cup, \cap)$ — решётка. Примерами её использования в реальных компьютерных системах может служить множество атрибутов файла и зависимость выходной величины от подмножества множества входных элементов. Если $A = \{1, 2, \dots, n\}$, то решётка подмножеств обозначается $SX(n)$ и содержит 2^n элементов.

3) *MLS*-решётка — прямое (декартово) произведение первых двух решёток.

Алгебраическая решётка используется в моделях безопасности для задания уровней секретности информации и уровней доверия к пользователям и называется решёткой ценностей. Рассмотрим задачу проверки соответствия указанным решёткам заданного решёточного графа. Для этого потребуется ряд определений и теорема об изоморфности *MLS*-решётке.

2. Исследование *MLS*-решётки

Из определения решётки нетрудно вывести, что любое конечное подмножество решётки имеет точную верхнюю и нижнюю грани. В частности, точную верхнюю и нижнюю грань имеет любое подмножество конечной решётки S (в частности, вся S). Обозначим $\sup S = I$, $\inf S = O$ — таким образом, любой элемент конечной решётки S меньше или равен I и больше или равен O .

Определение 3. Будем говорить, что элемент y решётки S покрывает элемент x этой решётки (обозначается $y \succ x$), если $y > x$ и не существует такого $z \in S$, что $y > z > x$.

Интервалом $[x, y]$ для элементов $x, y \in S$, $x \leq y$, называется множество таких элементов $z \in S$, что $x \leq z \leq y$. Таким образом, y покрывает x в точности тогда, когда интервал $[x, y]$ содержит лишь сами элементы x и y .

Лемма 1. Пусть S — конечная решётка, $x, y \in S$, $x < y$. Тогда найдётся такой $z \in [x, y]$, что $z \succ x$.

Доказательство. Пусть y не покрывает x . Тогда по определению можно построить такой y_1 , что $x < y_1 < y$. По построению $y_1 \in [x, y]$. Если y_1 также не покрывает x , можем аналогично построить y_2 , такой, что $x < y_2 < y_1$. При этом, поскольку $y_1 < y$, y_2 также лежит в интервале $[x, y]$. Продолжая аналогичные построения, получаем цепочку $y_1 > y_2 > y_3 > \dots$ различных элементов, лежащих в интервале $[x, y]$.

Но поскольку решётка S конечна, в интервале $[x, y]$ может лежать лишь конечное число различных элементов, то есть в какой-то момент мы не сможем построить очередной y_i . Это означает, что y_{i-1} покрывает x . ■

Заменив в доказательстве знаки всех неравенств, можно сформулировать двойственное утверждение: в любом интервале $[x, y]$ конечной решётки S , $x < y$, найдётся такой $z \in [x, y]$, что $z \prec y$.

Определение 4. Элемент $a \in S$ называется атомарным элементом решётки S , имеющей инфинум $O = \inf S$, если $a \succ O$.

Отметим, что атомарные элементы не могут покрывать отличных от O элементов решётки, так как если атомарный элемент a покрывает какой-то отличный от O элемент b , то $a > b > O$ и a не покрывает O .

Определение 5. Пусть S, S' — решётки. Отображение $\psi : S \rightarrow S'$ называется порядковым гомоморфизмом решёток, или изотонным отображением, если $x \leq y$ влечёт за собой $\psi(x) \leq \psi(y)$ для любых $x, y \in S$.

Таким образом, изотонное отображение сохраняет порядок элементов решётки.

Определение 6. Прямым произведением решёток A и B называется решётка $S = A \times B$, определённая на декартовом произведении множеств A и B следующим образом. Для $a, a' \in A, b, b' \in B$ полагаем $(a, b) \leq (a', b')$ в точности тогда, когда $a \leq a'$ и $b \leq b'$.

При этом супремумом и инфинумом элементов $(a, b), (a', b') \in A \times B$ будут соответственно $(\sup\{a, a'\}, \sup\{b, b'\})$ и $(\inf\{a, a'\}, \inf\{b, b'\})$. Если решётки A и B имеют нижние грани, то $\inf(A \times B) = (\inf A, \inf B)$.

Отметим, что элемент (a, b) решётки $A \times B$ покрывает элемент (a', b') той же решётки в том и только в том случае, когда

$$a \succ a', b = b' \quad \text{или} \quad a = a', b \succ b'. \quad (1)$$

Действительно, если выполнена, например, первая пара условий, то $(a, b) > (a', b')$ и если найдётся такой $(x, y) \in A \times B$, что $(a, b) > (x, y) > (a', b')$, то $a > x > a'$, что противоречит условию $a \succ a'$. Обратно, предположим, что для $(a, b) > (a', b')$ условие (1) не выполняется. Тогда либо $a > a', b > b'$, либо $b = b'$, но a не покрывает a' , либо $a = a'$, но b не покрывает b' . В первом случае $(a, b) \geq (a, b') > (a', b')$, во втором случае найдётся такой $x \in A$, что $a > x > a'$, и тогда $(a, b) > (x, b) > (a', b')$, аналогично в третьем случае $(a, b) > (a, y) > (a', b')$ для такого $y \in B$, что $b > y > b'$. Так или иначе, получаем, что при невыполнении условия (1) элемент (a, b) решётки $A \times B$ не может покрывать её элемент (a', b') .

Определение 7. Решётки S и S' называются изоморфными, если существует биективное изотонное отображение $\psi : S \rightarrow S'$. Это отображение называется изоморфизмом решёток S и S' .

Любая линейная решётка B при $|B| = m$ изоморфна решётке $SL(m)$. Любая решётка 2^A при $|A| = n$ изоморфна решётке $SX(n)$. Отметим также, что если решётка A изоморфна A' , а B изоморфна B' , то и $A \times B$ изоморфна $A' \times B'$ — их изоморфизм получается как прямое произведение изоморфизмов решёток-сомножителей.

Напомним, что цепью в частично упорядоченном множестве S называется его вполне упорядоченное подмножество; так, конечная цепь длины m представляет собой набор элементов $b_1, \dots, b_m$, таких, что $b_1 \leq b_2 \leq \dots \leq b_m$. Будем говорить, что элементы $b_1, \dots, b_m$ последовательно покрывают друг друга, если $b_1 \prec b_2 \prec \dots \prec b_m$.

Теорема 2. Конечная решётка S изоморфна MLS -решётке, то есть прямому произведению полной решётки подмножеств на линейную решётку $SX(n) \times SL(m)$ для некоторых $m, n \geq 1$, тогда и только тогда, когда она удовлетворяет следующим трём условиям:

- 1) $|S| = 2^n m$;
- 2) если $m \geq 2$, то в точности $n + 1$ элементов решётки S являются атомарными; в случае $m = 1$ атомарны в точности n элементов S ;
- 3) каждый элемент решётки S , кроме указанных далее $n + m$ элементов, покрывает по крайней мере два других. Исключения из этого условия составляют цепь из m последовательно покрывающих друг друга элементов S , начинающаяся с её инфинума O (каждый из них, кроме O , покрывает лишь предшествующий элемент цепи), а также n атомарных элементов, не входящих в эту цепь.

Доказательство. Проверим сначала выполнение условий 1–3 для решётки $T(n, m) = SX(n) \times SL(m)$. Условие 1 следует из того, что $|SX(n)| = 2^n$, $|SL(m)| = m$.

При $m = 1$ атомарными элементами решётки $T(n, 1) = SX(n) \times SL(1) = SX(n)$ являются в точности 1-элементные подмножества множества $N = \{1, \dots, n\}$, которых ровно n , что даёт выполнение условия 2.

Покажем, что при $m = 1$ все элементы решётки $SX(n)$, кроме атомарных и O (соответствующего пустому множеству), покрывают по крайней мере два других элемента $SX(n)$ (ранее показано, что атомарные элементы покрывают только O). Действительно, такие элементы являются k -элементными подмножествами множества N , $k \geq 2$. Из определения покрытия следует, что k -элементное множество покрывает все свои $(k-1)$ -элементные подмножества. Число таких подмножеств равно $C_k^{k-1} = k \geq 2$, что и требуется. Таким образом, при $m = 1$ условия 2 и 3 проверены.

Проверим условие 2 для решётки $T(n, m)$ при $m \geq 2$. Из условия (1) следует, что элемент $(a, b) \in T(n, m)$ является атомарным (то есть покрывает $(\emptyset, 0)$) тогда и только тогда, когда a атомарен в $SX(n)$ и $b = 0$, либо $a = \emptyset$ и b атомарен в $SL(m)$. Таким образом, атомарными в $T(n, m)$ являются в точности $n+1$ элементов $(\{1\}, 0), \dots, (\{n\}, 0), (\emptyset, 1)$, что доказывает выполнение условия 2.

Осталось проверить выполнение условия 3 при $m \geq 2$. Прежде всего заметим, что указанная в условии цепь из m последовательно покрывающих друг друга элементов получится, если рассмотреть элементы $(\emptyset, 0), \dots, (\emptyset, m-1)$. Действительно, согласно условию (1), $(\emptyset, k) \succ (a, b)$ для некоторого $(a, b) \in T(n, m)$ равносильно тому, что $a = \emptyset$ (так как $a \prec \emptyset$ невозможно) и $b \prec k$, то есть $(a, b) = (\emptyset, k-1)$ — предыдущий элемент цепи. Таким образом, указанные элементы действительно образуют цепь и каждый элемент цепи (кроме $(\emptyset, 0)$, являющегося инфинумом $T(n, m)$) покрывает ровно один элемент $T(n, m)$ (предыдущий элемент цепи).

Покажем, что все элементы $T(n, m)$, кроме её инфинума, атомарных элементов и элементов рассмотренной выше цепи, покрывают по крайней мере два других элемента $T(n, m)$. Пусть $(a, b) \in T(n, m)$ — такой элемент ($a \subseteq N$, $b \in \{0, \dots, m-1\}$). По построению это равносильно тому, что $|a| \geq 2$ при $b = 0$ и $a \neq \emptyset$ при $b \geq 1$. В первом случае, как мы видели при рассмотрении случая $m = 1$, найдутся такие $x, y \in SX(n)$, $x \neq y$, что $a \succ x$, $a \succ y$. Тогда $(a, 0) \succ (x, 0)$ и $(a, 0) \succ (y, 0)$. Во втором случае найдётся хотя бы один $x \in SX(n)$, такой, что $a \succ x$ (возможно, $x = \emptyset$), и тогда $(a, b) \succ (x, b)$ и $(a, b) \succ (a, b-1)$.

Докажем теперь обратное утверждение теоремы — если решётка S удовлетворяет условиям 1–3 при некоторых $m, n \geq 1$, то она изоморфна $SX(n) \times SL(m)$.

Обозначим через $A = \{a_0, \dots, a_n\}$ множество атомарных элементов S ($A = \{a_1, \dots, a_n\}$ в случае $m = 1$). Если $m = 1$, указанная в условии 3 цепь по построению состоит только из элемента $O = \inf S$. В случае $m \geq 2$ эта цепь включает в себя m элементов, из которых ровно один (следующий за O) является атомарным; без ограничения общности считаем, что это a_0 . Обозначим эту цепь $B = \{b_0, \dots, b_{m-1}\}$, $b_0 \prec b_1 \prec \dots \prec b_{m-1}$ (при этом $b_0 = O$, $b_1 = a_0$). Обозначим $A^* = A \setminus \{a_0\}$ ($A^* = A$ при $m = 1$). Отметим, что, независимо от значения m , $|A^*| = n$.

Зададим отображение $\psi : S \rightarrow 2^{A^*} \times B$ следующим образом. Каждому элементу $s \in S$ сопоставим упорядоченную пару, состоящую из подмножества всех элементов A^* , меньших или равных s , а также максимального элемента цепи B , меньшего или равного s :

$$\psi(s) = (\{a \in A^* : a \leq s\}, \max\{b \in B : b \leq s\}).$$

Докажем, что отображение ψ является изоморфизмом решёток.

Покажем сначала, что ψ изотонно. Пусть $p, p' \in S$, $p \leq p'$. Обозначим $\psi(p) = (P, b)$, $\psi(p') = (P', b')$. Если для некоторого $a \in A^*$ выполнено $a \in P$, то $a \leq p \leq p'$ и $a \in P'$. Отсюда $P \subseteq P'$. Далее, из $b \leq p$ следует $b \leq p'$, поэтому $b \leq b'$. Тогда $(P, b) \leq (P', b')$ в решётке $2^{A^*} \times B$.

Покажем, что ψ инъективно. Пусть $\psi(p) = \psi(p') = (L, b_j)$ для $p, p' \in S$, выведем отсюда, что $p = p'$. Доказательство будем вести индукцией по сумме $|L| + j$.

При $|L| + j = 0$ имеем $\psi(p) = \psi(p') = (\emptyset, O)$, откуда следует, что в S нет ни одного атомного элемента, меньше или равного p или p' . Но тогда $p = p' = O$, так как если, например, $p > O$, то по лемме 1 в S найдётся элемент, меньший или равный p и покрывающий O .

Пусть утверждение выполнено для всех $|L| + j < k$, $k > 0$. Покажем его выполнение при $|L| + j = k$. Предположим противное: $\psi(p) = \psi(p') = (L, b_j)$, но $p \neq p'$. Обозначим $q = \sup(L \cup \{b_j\})$ (поскольку $p \neq p'$, без ограничения общности можно полагать $q \neq p$). По построению получаем $q \leq p$ (супремум элементов из $L \cup \{b_j\}$ меньше или равен их верхней грани) и, с учётом неравенства, $q < p$. Тогда по лемме 1 в интервале $[q, p]$ найдётся такой элемент r , что $r \succ q$. Заметим, что, исходя из построения q , $\psi(q) \geq (L, b_j)$. Тогда ввиду доказанной изотонности ψ получаем $\psi(q) = (L, b_j)$ в силу неравенства $q \leq p$ и затем $\psi(r) = (L, b_j)$ в силу неравенств $q \leq r \leq p$.

Поскольку $L \neq \emptyset$ или $b_j \neq O$, имеем $q \neq O$, а значит, r не атомарен. Кроме того, $r \notin B$, так как каждый элемент B , отличный от O , покрывает предшествующий в цепи, поэтому q также лежит в B , и $\psi(r) \neq \psi(q)$, поскольку $\psi(r) = (\cdot, r)$, а $\psi(q) = (\cdot, q)$. Тогда по условию 3 теоремы r покрывает по крайней мере два разных элемента S , и найдётся такой $t \in S$, $t \neq q$, что $r \succ t$. При этом $\psi(t) \leq \psi(r) = (L, b_j)$, но $\psi(t) \neq (L, b_j)$, так как в противном случае получим $t \geq q$ (из тех же соображений, из которых $p \geq q$), и тогда $r > t > q$, что противоречит тому, что r покрывает q . Таким образом, получили, что $\psi(t) < (L, b_j)$. Обозначим $\psi(t) = (M, b_i) < (L, b_j)$.

Из последнего неравенства следует, что $|M| + i < k$. Тогда для любой верхней грани t' множества $M \cup \{b_i\}$, меньше или равной t , из $t' \leq t$ ввиду изотонности ψ получим $\psi(t') \leq (M, b_i)$. С другой стороны, для t' , являющегося верхней гранью $M \cup \{b_i\}$, по построению $\psi(t') \geq (M, b_i)$. Отсюда $\psi(t') = (M, b_i) = \psi(t)$, и $t' = t$ в силу предположения индукции. Заметим теперь, что t является верхней гранью (M, b_i) по построению. Тогда $\sup(M, b_i) \leq t$ и из проведённых рассуждений следует, что $t = \sup(M, b_i)$.

Но q также является верхней гранью $M \cup \{b_i\}$, и тогда $q \geq \sup(M, b_i) = t$. Получаем $r > q > t$ ($t \neq q$ по построению), а это противоречит тому, что r покрывает t . Инъективность ψ доказана.

Сюръективность ψ следует из его инъективности (дающей $|\psi(S)| = |S|$) и условия 1 теоремы (дающего $|S| = |2^{A^*} \times B|$). Таким образом, ψ задаёт изоморфизм решёток S и $2^{A^*} \times B$, последняя из которых изоморфна $SX(n) \times SL(m)$. ■

Сделаем замечание о структуре рассматриваемых теоремой 2 решёток, которое понадобится в дальнейшем.

Следствие 1. Решётки $SX(n) \times SL(2)$ и $SX(n+1)$, $n \geq 1$, эквивалентны.

Доказательство. Применим к решётке $S = SX(n) \times SL(2)$ прямое утверждение теоремы 2. Согласно условию 1, $|S| = 2^n \cdot 2 = 2^{n+1}$. Согласно условию 2, S содержит ровно $n+1$ атомарных элементов. Наконец, указанная в условии цепь из двух элементов, помимо O , содержит элемент, покрывающий его, то есть атомарный. Таким образом, согласно условию 3, исключениями из правила, согласно которому каждый

элемент S должен покрывать два других её элемента, являются в точности O и все атомарные элементы S .

Теперь, применяя к S обратное утверждение теоремы 2, получаем с учётом доказанного, что S изоморфна $SX(n+1) \times SL(1)$, то есть $SX(n+1)$. ■

Оценим сложность проверки указанных в теореме 2 условий при определении структуры данной конечной решётки S . Решётку будем полагать заданной её матрицей инцидентности, то есть матрицей, для каждой пары элементов решётки указывающей, какой из них больше (либо что они несравнимы).

Теорема 3. Для проверки изоморфизма конечной решётки S , заданной своей матрицей инцидентности, произведению решёток $SX(n) \times SL(m)$ при каких-либо (неизвестных заранее) $m, n \geq 1$ достаточно выполнить $O(|S|^2)$ операций.

Доказательство. Будем проверять выполнение условий теоремы 2 для каких-либо m, n . Для этого определим элементы решётки S , покрывающие ровно один её элемент (а также определим инфинум S), затем выделим среди них атомарные элементы (что даст возможное значение n) и определим, удовлетворяют ли оставшиеся m элементов указанной в условии 3 теоремы 2 структуре.

Обозначим множество элементов S , покрывающих ровно один другой её элемент, через P . Покажем, что для определения принадлежности заданного элемента $p \in S$ множеству P достаточно совершить два прохода по набору $L(p) = \{q \in S : q < p\}$ элементов S , строго меньших p (они получаются из строки, соответствующей p в матрице инцидентности S). При этом если таких элементов нет ($L(p) = \emptyset$), то $p = O$. Если такой элемент только один, то $L(p) = \{O\}$ и p атомарен, так как если бы нашёлся такой $q \in S$, что $p > q > O$, то $O, q \in L(p)$. Множество атомарных элементов S обозначим A .

Рассмотрим случай $|L(p)| \geq 2$. Заметим, что $p \in P$ тогда и только тогда, когда в множестве $L(p)$ содержится его супремум (который p и покрывает). Действительно, если $r = \sup L(p)$, $r \in L(p)$, то $r < p$, и если найдётся такой $s \in S$, что $r < s < p$, то по построению $s \in L(p)$, и тогда $s \leq r$ — противоречие, означающее, что $r < p$. При этом для любого другого $r' \in L(p)$, $r' \neq r$, получается $r' < r < p$, что делает невозможным $r' < p$.

Обратно, пусть в $L(p)$ содержится ровно один элемент r , покрываемый p . Тогда в $L(p)$ не найдётся элемента, большего r , так как если $s > r$, $s \in L(p)$, то $p > s > r$ и p не покрывает r . Предположим сначала, что r является верхней гранью $L(p)$. Тогда $r = \sup L(p)$ (как и требуется), так как в противном случае найдётся меньшая верхняя грань $r' = \sup L(p)$, но тогда из $r \in L(p)$ следует $r \leq r'$ — противоречие. Если же предположить, что r не является верхней гранью $L(p)$, придём к противоречию. Действительно, в этом случае в $L(p)$ найдётся элемент s , $s \neq r$, не меньший чем r . По замечанию к лемме 1 тогда получим, что в интервале $[s, p]$ найдётся такой элемент r' , что $r' < p$. При этом из $r' > s$ следует $r' \neq r$, и приходим к противоречию с тем, что p покрывает лишь один элемент решётки S .

Итак, мы показали, что условие $p \in P$ равносильно тому, что множество $L(p)$ содержит свой супремум (достаточно проверить содержание им своей верхней грани, так как в предыдущем абзаце показано, что любая верхняя грань $L(p)$, лежащая в $L(p)$, является его супремумом). Построим алгоритм, проверяющий условие наличия верхней грани множества $L(p)$ в нём самом.

За первый проход по множеству $L(p)$ находится его максимум q (элемент множества $L(p)$, не меньший никакого другого элемента этого множества).

За второй проход проверяем, является ли найденный максимум q верхней гранью $L(p)$, сравнивая его с остальными элементами. Если q не является верхней гранью $L(p)$, то $L(p)$ не содержит своей верхней грани, так как если r — верхняя грань $L(p)$, $r \in L(p)$, $r \neq q$, то $r > q$, что противоречит максимальности q .

Итак, два прохода по множеству $L(p)$ для каждого элемента $p \in S$ позволяют определить принадлежность $p \in P$ для всех p и, таким образом, дают множество P .

Если все элементы P атомарны, то, согласно условию 2 теоремы 2, возможны лишь случаи $m = 1$ или 2 (второй из которых сводится к первому ввиду доказанной в следствии теоремы 2 изоморфности решёток $SX(n+1)$ и $SX(n) \times SL(2)$). В этом случае берём, согласно условию 2 теоремы 2, $n = |A| - 1$, и если $|S| = 2^n$, то, применяя теорему с $m = 1$, получаем, что S изоморфна $SX(n)$. Если же $|S| \neq 2^n$, то, согласно условию 1 теоремы 2 (n определяется условием 2 однозначно), S не может быть изоморфна никакому произведению полной решётки подмножеств на линейную.

Рассмотрим случай, когда не все элементы P атомарны. Обозначим $B^* = P \setminus A$. Предполагая изоморфность S нужному прямому произведению, из условия 2 теоремы 2 вновь получаем $n = |A| - 1$ и, согласно условию 3, $m = |B^*| + 2$ (к неатомарным элементам P добавляется один атомарный, входящий в цепь из условия 3, и O). Теперь можем проверить равенство из условия 1: $|S| = 2^n m$ — если оно не выполнено, то требуемого изоморфизма нет.

Если это равенство выполнено, осталось проверить, что элементы B^* образуют указанную в условии 3 цепь, последовательно покрывая друг друга. Для этого на этапе построения записываем элементы B^* в массив, индексированный количеством элементов S , меньших заданного элемента B^* . Покажем, что если элементы B^* образуют требуемую цепь, эти индексы не могут совпадать друг с другом и образуют полный набор целых чисел от 2 до m .

Действительно, если $B^* = \{b_2, \dots, b_{m-1}\}$, $O \prec b_1 \prec b_2 \prec b_3 \prec \dots \prec b_{m-1}$, где b_1 — атомарный элемент, входящий в цепь, то каждый b_i превосходит i элементов $O, b_1, b_2, \dots, b_{i-1}$. Для того чтобы показать, что b_i не может превосходить никаких других элементов S , предположим противное и выберем минимальный b_i , превосходящий какой-то элемент, кроме указанных. Обозначим такой элемент q . Тогда по замечанию к лемме 1 найдётся элемент $r \in [q, b_i]$, такой, что $r \prec b_i$. При этом $r \neq b_{i-1}$, так как в противном случае $q \leq r < b_{i-1}$, что противоречит минимальности выбранного b_i . Но тогда получаем, что b_i покрывает два разных элемента из S (r и b_{i-1}) — противоречие с условием 3 теоремы 2.

Итак, если указанные условия на индексы элементов B^* не выполнены, то S не изоморфна требуемому прямому произведению. Если условия выполнены, то для проверки условия 3 теоремы 2 и доказательства изоморфизма S решётке $SX(n) \times SL(m)$ с вычисленными выше n, m остаётся лишь проверить, что каждый следующий элемент массива больше предыдущего (что делается прямыми сравнениями за один проход по массиву). Действительно, в этом случае элементы B^* образуют цепь и каждый следующий элемент покрывает предыдущий, так как если $p > q$, но p не покрывает q , то есть $p > r > q$ для некоторого $r \in S$, то $L(p) \supseteq L(q) \cup \{q, r\}$ и $|L(p)| \geq |L(q)| + 2$, но по условиям на индексы $|L(p)| = |L(q)| + 1$.

Отдельно нужно рассмотреть минимальный элемент $b_2 \in B^*$ (с индексом 2 и соответствующей мощностью $|L(b_2)|$), который должен покрывать не другой элемент B^* , а элемент, не входящий в рассмотренный массив. Для него $L(b_2) = \{O, b_1\}$ при некотором $b_1 \in S$. Множество $L(b_2)$ имеет верхнюю грань $b_1 > O$, и тогда, как доказано выше, $b_2 \succ b_1$. При этом $b_1 \succ O$, так как в противном случае найдётся такой $r \in S$,

что $b_1 > r > O$, и тогда $O, b_1, r \in L(b_2)$, что противоречит условию $|L(b_2)| = 2$. Таким образом, недостающий фрагмент $O \prec b_1 \prec b_2$ цепочки $O \prec b_1 \prec \dots \prec b_{m-1}$ построен.

Как видно из доказательства, для проверки изоморфизма требуется совершить два прохода по матрице инцидентности решётки S и некоторое количество существенно меньших по трудоёмкости операций. ■

3. Алгоритмы восстановления решётки

В терминологии теории графов определение 3 формулируется следующим образом: вершина v_1 решёточного графа G покрывает вершину v_2 этого же орграфа, если в транзитивном замыкании графа G существует дуга (v_1, v_2) и не существует ориентированного пути $p(v_1, v_2)$, такого, что $|p(v_1, v_2)| > 1$. Атомарная вершина (определение 4) имеет одну и только одну исходящую дугу, причём эта дуга должна вести в сток (вершину без исходящих дуг) орграфа. Будем говорить, что решёточный граф соответствует решётке S , если он порождает решётку, изоморфную решётке S . Переформулируем теорему 2 в терминах теории графов. При этом заметим, что так как исследуемый орграф решёточный, то сток t в нём существует и единственен.

Теорема 4. Решёточный граф соответствует MLS -решётке $S = SX(n_1) \times SL(n_2)$ тогда и только тогда, когда:

- 1) число вершин орграфа $n = 2^{n_1} n_2$;
- 2) все вершины орграфа покрывают по крайней мере две других, кроме вершин $x_1, \dots, x_{n_1}, t, t_1, \dots, t_{n_2-1}$. Если $n_2 = 1$, вершины t_j ($j = 1, \dots, n_2 - 1$) отсутствуют. При этом:
 - t — сток орграфа;
 - вершины $x_1, \dots, x_{n_1}, t_1, \dots, t_{n_2-1}$ покрывают ровно одну вершину;
 - вершины $x_1, \dots, x_{n_1}, t_1$ атомарные;
 - вершины $t_{n_2-1} \succ \dots \succ t_1 \succ t$ образуют цепь последовательно покрывающих друг друга вершин.

Для проверки соответствия решёточного графа решётке подмножеств теорема 4 может быть переформулирована следующим образом.

Теорема 5. Решёточный граф соответствует решётке подмножеств $SX(n_1)$ тогда и только тогда, когда он удовлетворяет следующим трём условиям:

- 1) число вершин орграфа $n = 2^{n_1}$;
- 2) число атомарных вершин равно $\log_2 n = n_1$;
- 3) все вершины, кроме атомарных и стока, покрывают не менее двух других.

Представим алгоритм 1 проверки указанных в теореме 4 условий для определения структуры заданного решёточного графа.

Пусть решёточный граф G задан матрицей достижимости $\mathbf{M}^+$ размерности $n \times n$. Требуется получить ответ на вопрос, соответствует ли орграф G некоторой MLS -решётке $S = SX(n_1) \times SL(n_2)$. Для этого необходимо найти вершины орграфа G , покрывающие ровно одну вершину. Пусть эти вершины образуют множество P , $|P| = p$. Среди вершин множества P необходимо найти атомарные. Обозначим множество этих вершин A , $|A| = a$. Очевидно, что должны выполняться следующие равенства:

$$p = n_1 + n_2 - 1, \quad a = \begin{cases} n_1, & n_2 = 1, \\ n_1 + 1, & n_2 > 1. \end{cases}$$

Пусть $C = P \setminus A$ — множество вершин, покрывающих ровно один элемент, но не являющихся атомарными.

Алгоритм 1. Определение структуры решёточного графа

Вход: решёточный граф G задан матрицей достижимости $\mathbf{M}^+$ размерности $n \times n$; вспомогательный массив $\mathbf{V}$ размерности n .

Выход: соответствует ли орграф G некоторой MLS -решётке $S = SX(n_1) \times SL(n_2)$?

- 1: Сформируем множества P , A и C . Для этого
- 2: **Для всех** вершин v_i орграфа G
- 3: По строке i матрицы достижимости совершим проход и найдём максимальный элемент среди тех, которые формируют множество $L(v_i)$; обозначим его v_* (напомним, что $v_j \geq v_k \Leftrightarrow [\mathbf{M}^+]_{jk} = 1$).
- 4: Ещё за один проход по i -й строке матрицы проверим, что v_* является верхней гранью для $L(v_i)$ ($[\mathbf{M}^+]_{*j} = 1$ для всех $v_j \in L(v_i)$).
- 5: **Если** в i -й строке матрицы единичный элемент один (он же является верхней гранью), **то**
- 6: $v_i \in P$ и $v_i \in A$.
- 7: **Если** единичных элементов более одного и верхняя грань найдена, **то**
- 8: $v_i \in P$ и $v_i \in C$. Пополним элемент массива $[\mathbf{V}]_q$ вершиной v_i , где индекс q — это мощность множества $L(v_i)$.
- 9: Проанализируем множества P и A . Возможны два случая.
- 10: **Если** $A = P$, **то**
все вершины множества P атомарны. Тогда $n_1 = p$, $n_2 = 1$.
- 11: **Если** $n \neq 2^p$ (условие 1 теоремы 4), **то**
- 12: требуемого соответствия нет,
- 13: **иначе**
- 14: орграф G соответствует решётке подмножеств $S = XS(p)$ (или эквивалентной MLS -решётке $S = XS(p-1) \times LS(2)$ (следствие 1)).
- 15: **Если** $A \subset P$, **то**
- 16: не все вершины множества P атомарны. Тогда $n_1 = a - 1$, $n_2 = p - a + 2$.
- 17: **Если** $n \neq 2^{a-1}(p - a + 2)$ (условие 1 теоремы 4), **то**
- 18: требуемого соответствия нет,
- 19: **иначе**
- 20: **Если** все элементы массива $\mathbf{V}$ в диапазоне индексов от 2 до $n_2 - 1$ содержат ровно одну вершину, каждая следующая вершина этого массива в заданном диапазоне покрывает предыдущую, вершина $[\mathbf{V}]_2$ покрывает некоторую атомарную вершину из множества A , **то**
- 21: орграф G соответствует MLS -решётке $S = XS(a-1) \times LS(p-a+2)$,
- 22: **иначе**
- 23: требуемого соответствия нет.

Прокомментируем шаги 2–10 алгоритма 1. В них $L(v_i) = \{v_j : v_i > v_j\}$ — множество вершин, до которых существует ориентированный путь из вершины v_i . Для этих вершин $[\mathbf{M}^+]_{ij} = 1$, то есть множество $L(v_i)$ определяется единичными недиагональными элементами строки i матрицы достижимости. При доказательстве теоремы 3 показано, что для проверки принадлежности вершины v_i множеству P достаточно выяснить, содержит ли множество $L(v_i)$ свою верхнюю грань. Если $|L(v_i)| = 1$, то v_i — атомарная вершина.

После того как множества P , A и C сформированы, необходимо проанализировать их структуру (шаги 11–25 алгоритма 1). Пояснений требует случай, когда $A \subset P$ и

$n = 2^{a-1}(p - a + 2)$ (шаг 22). В этой ситуации остаётся проверить, что все вершины из множества C образуют указанную в условии 2 теоремы 4 цепь, последовательно покрывая друг друга. Это означает, что число вершин, в которые существует ориентированный путь из вершины v_i , для всех вершин множества C уникально. Более того, эти величины образуют полный набор чисел в диапазоне от 2 до $n_2 - 1$ (см. доказательство теоремы 3). Для проверки этого факта на этапе построения множества C каждую его вершину v_i необходимо продублировать в массив, индексированный числом вершин, в которые существует ориентированный путь из v_i (это число единиц в строке i матрицы достижимости, или мощность множества $L(v_i)$). Индексы k этого массива меняются от 2 до $n_2 - 1$. Каждый элемент массива должен содержать ровно одну вершину. Если указанное условие не выполнено, то искомого соответствия нет. Иначе осталось проверить, что каждая следующая вершина массива покрывает предыдущую: $v_{i_{k+1}} \succ v_{i_k}$. Для этого достаточно, чтобы $[M^+]_{i_{k+1}i_k} = 1$. Отдельно необходимо рассмотреть вершину v_{i_2} , которая должна покрывать не другую вершину множества C , а некоторую атомарную вершину из множества A (что также проверяется по матрице достижимости: $[M^+]_{i_2j} = 1$ для некоторой вершины $v_j \in A$).

Замечание 1. Алгоритм 1 очевидным образом можно адаптировать для проверки соответствия решёточного графа решётке подмножеств.

Замечание 2. Трудоёмкость проверки соответствия решёточного графа, заданного матрицей смежности, некоторой MLS -решётке $S = XS(n_1) \times LS(n_2)$ при неизвестных заранее n_1 и n_2 в общем случае не превосходит $O(n^3)$, где n — число вершин орграфа. Действительно, в теореме 3 доказано, что сложность проверки не превосходит $O(n^2)$ для матрицы инцидентности исследуемой решётки. При теоретико-графовой интерпретации эта матрица совпадает с матрицей достижимости M^+ орграфа. Если исследуемый решёточный граф задан матрицей смежности, то трудоёмкость повышается до $O(n^3)$, так как «узким» местом проверки будет алгоритм Уоршелла, позволяющий построить матрицу достижимости.

Следует заметить, что при оценке трудоёмкости алгоритмов операции по формированию множеств считались линейными, тогда как трудоёмкость подобных операций существенно зависит от реализации структур данных.

Теоремы 2 и 3 позволили построить алгоритм проверки соответствия решёточного графа MLS -решётке (в частном случае, решётке подмножеств). Исследуем случай линейной решётки.

Теорема 6. Трудоёмкость проверки соответствия решёточного графа некоторой линейной решётке не превосходит $O(n^3)$.

Доказательство. Для проверки соответствия решёточного графа линейной решётке достаточно показать, что любая пара вершин сравнима, то есть для любой пары вершин существует ориентированный путь, их соединяющий. Очевидно, трудоёмкость алгоритма определяется алгоритмом Уоршелла построения матрицы достижимости. ■

Заключение

Доказано, что задача восстановления решётки ценностей по орграфу разрешима за полиномиальное время. Этот факт существенен при построении систем разграничения доступа, основанных на мандатной модели безопасности [8], так как гарантирует получение результата за приемлемое время.

Авторы выражают благодарность Ю. С. Ракицкому за полезные замечания и предложения в процессе подготовки статьи.

ЛИТЕРАТУРА

1. *Belim S., Bogachenko N., and Ilushechkin E.* An analysis of graphs that represent a role-based security policy hierarchy // J. Computer Security. 2015. V. 23. No. 5. P. 641–657.
2. *Birkhoff G.* Lattice Theory. N.Y.: Amer. Math. Soc. Colloquium Publ., 1967.
3. *Jakubik J.* On isomorphisms of graphs of lattices // Czechoslovak Math. J. 1985. V. 35. No. 2. P. 188–200.
4. *Mainetti M.* Arguesian identities in linear lattices // Adv. Math. 1999. No. 144. P. 50–93.
5. *Mainetti M. and Yan C. H.* Geometric identities in lattice theory // J. Combinatorial Theory. Ser. A. 2000. No. 91. P. 411–450.
6. *Felsner S. and Knauer K. B.* Distributive lattices from graphs // Proc. VI Jornadas de Matematica Discreta y Algoritmica. Lleida, 2008. P. 11–23.
7. *Bertet K.* The dependence graph of a lattice // Proc. CLA, Malaga, Spain, 2012. P. 223–231.
8. *Belim S. V., Bogachenko N. F., Kabanov A. N., and Rakitskiy Yu. S.* Using the Decision Support Algorithms Combining Different Security Policies // Dynamics of Systems, Mechanisms and Machines (Dynamics). 15–17 Nov. 2016. IEEE Xplore. <http://ieeexplore.ieee.org/document/7818976/>.

REFERENCES

1. *Belim S., Bogachenko N., and Ilushechkin E.* An analysis of graphs that represent a role-based security policy hierarchy. J. Computer Security, 2015, vol. 23, no. 5, pp. 641–657.
2. *Birkhoff G.* Lattice Theory. N.Y., Amer. Math. Soc. Colloquium Publ., 1967.
3. *Jakubik J.* On isomorphisms of graphs of lattices. Czechoslovak Math. J., 1985, vol. 35, no. 2, pp. 188–200.
4. *Mainetti M.* Arguesian identities in linear lattices. Adv. Math., 1999, no. 144, pp. 50–93.
5. *Mainetti M. and Yan C. H.* Geometric identities in lattice theory. J. Combinatorial Theory, Ser. A, 2000, no. 91, pp. 411–450.
6. *Felsner S. and Knauer K. B.* Distributive lattices from graphs. Proc. VI Jornadas de Matematica Discreta y Algoritmica, Lleida, 2008, pp. 11–23.
7. *Bertet K.* The dependence graph of a lattice. Proc. CLA, Malaga, Spain, 2012, pp. 223–231.
8. *Belim S. V., Bogachenko N. F., Kabanov A. N., and Rakitskiy Yu. S.* Using the Decision Support Algorithms Combining Different Security Policies. Dynamics of Systems, Mechanisms and Machines (Dynamics), 15–17 Nov. 2016, IEEE Xplore. <http://ieeexplore.ieee.org/document/7818976/>.