Conference on Programming Language Design and Implementation (PLDI 2007). - 2007.

5. Newsome, J. Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software / J. Newsome, D. Song // In Proceedings of the 12th Annual Network and Distributed, System Security Symposium (NDSS 2005), -2005.

6. Тихонов, Д.И Введение в технологию taint analysis / Тихонов Д.И, Буканов Д.Ф // Актуальные проблемы информационной безопасности. Теория и практика использования программно-аппаратных средств: материалы VII всероссийской научно-технической конференции. -2014.

В.П. Цветов

ОБ ОДНОМ СИНТАКСИЧЕСКОМ АЛГОРИТМЕ НА ГРАФАХ

(Самарский государственный университет)

Алгоритмы на графах представляют интерес для различных прикладных направлений, в частности, они могут быть полезны при проектировании информационных систем или построении систем безопасности. Существующие алгоритмы используют различные подходы, опирающиеся на специальные представления и структуры данных, обширная библиография по которым представлена, например в [1].

В докладе рассматривается алгоритм нахождения оптимальных маршрутов на реберно-размеченных графах. Результат не претендует на практическую новизну, но демонстрирует возможный абстрактно алгебраический метод решения задач, связанных с построением степеней элементов ограниченной сверху структурно упорядоченной полугруппы [2] в матричном представлении.

Введем следующие обозначения.

$\mathbb{N}$-множество натуральных чисел;

$1..n := \{1,2,\dots,n\} \subset \mathbb{N}$;

$\mathcal{A} := \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ - алфавит мощности n;

$\mathbb{W}_{\mathcal{A}}^{k}$- множество слов длины k над алфавитом $\mathcal{A}$;

$\mathbb{W}_{\mathcal{A}} := \bigcup_{k=0}^{\infty} \mathbb{W}_{\mathcal{A}}^{k}$- множество слов над алфавитом $\mathcal{A}$;

$\langle \mathbb{W}_{\mathcal{A}}, (\bullet) \rangle$- моноид слов над алфавитом $\mathcal{A}$ с операцией сцепления;

$\mathbb{R}$- множество вещественных чисел;

$\mathbb{R}_{+}$- множество неотрицательных вещественных чисел;

$[0,1] \subset \mathbb{R}$ - замкнутый интервал вещественных чисел от 0 до 1;

$\langle \mathbb{R}, (\cdot, +) \rangle$ - поле вещественных чисел;

$\langle \mathbb{R}, (\wedge, \vee,) \rangle$ - решетка вещественных чисел, где $\xi_1 \wedge \xi_2 := \min(\xi_1, \xi_2)$, $\xi_1 \vee \xi_2 := \max(\xi_1, \xi_2)$;

$\mathbb{R}^{\infty} := \mathbb{R} \cup \{\iota\}$- расширенное множество вещественных чисел;
$\langle \mathbb{R}^{\infty}, (\wedge, \vee, \cdot, +) \rangle$- расширенная алгебра вещественных чисел, где $\xi \in \mathbb{R}$ и $\xi \wedge \iota = \iota \wedge \xi := \xi,\ \xi \vee \iota = \iota \vee \xi = \xi \cdot \iota = \iota \cdot \xi = \xi + \iota = \iota + \xi = \iota \cdot \iota = \iota + \iota := \iota$;
$\langle \mathbb{R}_{+}^{\infty}, (\wedge, \vee, \cdot, +) \rangle$- подалгебра $\langle \mathbb{R}^{\infty}, (\wedge, \vee, \cdot, +) \rangle$ с носителем $\mathbb{R}_{+}^{\infty}$; ;
2^{V}- булеан над множеством V;
$| V |$- мощность множества V;
$U \times V$- декартово произведение множеств U и V;
$2^{V \times V}$- множество бинарных отношений на V;
$\langle 2^{V \times V}, (\circ) \rangle$- моноид бинарных отношений на V с операцией произведения;
R^{k}- k-ая степень бинарного отношения $R \in 2^{V \times V}$, где $R^{k} := R^{k-1} \circ R$, $R^{1} := R$, $k > 1$.

Определим множества термов $T(\mathbb{R}, \mathbb{W}_{\mathcal{A}}) := \{\xi * w \mid \xi \in \mathbb{R}, w \in \mathbb{W}_{\mathcal{A}}\}$, $\mathbb{T}(\mathbb{R}^{\infty}, \mathbb{W}_{\mathcal{A}}) := \mathbb{R} \cup \mathbb{W}_{\mathcal{A}} \cup T(\mathbb{R}, \mathbb{W}_{\mathcal{A}}) \cup \{\iota\}$ и расширенную алгебру термов $\langle \mathbb{T}(\mathbb{R}^{\infty}, \mathbb{W}_{\mathcal{A}}), (\odot, \oplus) \rangle$, полагая для произвольных $\xi, \xi_1, \xi_2 \in \mathbb{R}$; $w, w_1, w_2 \in \mathbb{W}_{\mathcal{A}}$; $t = \xi * w, t_1 = \xi_1 * w_1, t_2 = \xi_2 * w_2 \in T(\mathbb{R}, \mathbb{W}_{\mathcal{A}})$; ι:

$$\xi_1 \odot \xi_2 := \xi_1 + \xi_2;$$
$$\xi_1 \oplus \xi_2 := \xi_1 \wedge \xi_2;$$
$$\xi \odot w = w \odot \xi = \xi \oplus w = w \oplus \xi := \xi * w;$$
$$\xi \odot t_1 = t_1 \odot \xi := (\xi + \xi_1) * w_1;$$
$$\xi \oplus t_1 = t_1 \oplus \xi := \begin{cases} \xi * w_1, \xi \wedge \xi_1 = \xi \\ t_1, \quad \xi \wedge \xi_1 = \xi_1 \end{cases};$$
$$\xi \odot \iota = \iota \odot \xi := \iota;$$
$$\xi \oplus \iota = \iota \oplus \xi := \xi;$$
$$w_1 \odot w_2 = w_1 \oplus w_2 := w_1 \bullet w_2;$$
$$w_2 \odot w_1 = w_2 \oplus w_1 := w_2 \bullet w_1;$$
$$w \odot t_1 := \xi_1 * (w \bullet w_1);$$
$$t_1 \odot w := \xi_1 * (w_1 \bullet w);$$
$$w \oplus t_1 = t_1 \oplus w := t_1;$$
$$w \odot \iota = \iota \odot w := \iota;$$
$$w \oplus \iota = \iota \oplus w := w;$$
$$t_1 \odot t_2 := (\xi_1 + \xi_2) * (w_1 \bullet w_2);$$
$$t_1 \oplus t_2 := \begin{cases} t_1, \ \xi_1 = \xi_2 \text{ или } \xi_1 \wedge \xi_2 = \xi_1 \\ t_2, \ \xi_1 \neq \xi_2 \ \text{ и } \ \xi_1 \wedge \xi_2 = \xi_2 \end{cases};$$
$$t_1 \odot \iota = \iota \odot t_1 = \iota \odot \iota = \iota \oplus \iota := \iota;$$
$$t_1 \oplus \iota = \iota \oplus t_1 := t_1.$$

Введем обозначение $\sum_{k=1}^{n} \tau_k := \tau_1 \oplus \tau_2 \oplus \ldots \oplus \tau_n$, где $\tau_k \in \mathbb{T}(\mathbb{R}^{\infty}, \mathbb{W}_{\mathcal{A}})$, $k \in 1..n$.

Рассмотрим множество квадратных матриц порядка n над множеством термов $\mathbb{M}(\mathbb{T}(\mathbb{R}^{\infty},\mathbb{W}_{\mathcal{A}}),n) := \{(\tau_{ij})|\tau_{ij} \in \mathbb{T}(\mathbb{R}^{\infty},\mathbb{W}_{\mathcal{A}})\}$. Определим матричные операции полагая для произвольных $M_1 = (\tau_{ij}^1)$, $M_2 = (\tau_{ij}^2) \in \mathbb{M}(\mathbb{T}(\mathbb{R}^{\infty},\mathbb{W}_{\mathcal{A}}),n)$:

$M_1 \boxdot M_2 := (\sum_{k-1}^{n} \tau_{ik}^1 \odot \tau_{kj}^2)$;

$M_1 \boxplus M_2 := (\tau_{ij}^1 \oplus \tau_{ij}^2)$;

$M_1 \boxtimes M_2 :- (\tau_{ij}^1 \odot \tau_{ij}^2)$.

Введем обозначение $\sum_{k=1}^{n} M_k :- M_1 \boxplus M_2 \boxplus \ldots \boxplus M_n$, где $M_k \in \mathbb{M}(\mathbb{T}(\mathbb{R}^{\infty},\mathbb{W}_{\mathcal{A}}),n)$, $k \in 1..n$.

Рассмотрим матричную алгебру $\langle \mathbb{M}(\mathbb{T}(\mathbb{R}^{\infty},\mathbb{W}_{\mathcal{A}}),n),(\boxdot,\boxplus,\boxtimes)\rangle$.

Естественным образом определяются подалгебры $\langle \mathbb{T}(\mathbb{R}_{+}^{\infty},\mathbb{W}_{\mathcal{A}}),(\odot,\oplus)\rangle$, $\langle \mathbb{M}(\mathbb{T}(\mathbb{R}_{+}^{\infty},\mathbb{W}_{\mathcal{A}}),n),(\boxdot,\boxplus,\boxtimes)\rangle$.

Рассмотрим тотальную функцию $\rho: 1..n \times 1..n \to R_{+}^{\infty}$. Значения функции ρ будем интерпретировать как длину ребра размеченного графа G, соединяющего вершины с номерами i и j, если $\rho(i,j) \in \mathbb{R}_{+}$, и как отсутствие ребра в случае, если $\rho(i,j) = \iota$. Воспользуемся матричным представлением функции ρ, полагая $P := (\rho_{ij}) := (\rho(i,j))$.

Определим матрицы $M_1 = (\tau_{ij}^1)$, $M_2 = (\tau_{ij}^2) := (\tau_{ji}^1) = M_1^T$, полагая $\tau_{ij}^1 := \alpha_i$.

Хорошо известно [3] следующее свойство транзитивного замыкания бинарного отношения $R \in 2^{V \times V}$ на конечном множестве V:

$$\bigcup_{k=1}^{\infty} R^k = \bigcup_{k=1}^{|V|} R^k,$$

из которого, в силу определения алгебры $\langle \mathbb{M}(\mathbb{T}(\mathbb{R}^{\infty},\mathbb{W}_{\mathcal{A}}),n),(\boxdot,\boxplus,\boxtimes)\rangle$, следует, что элементы матрицы

$$M = (\tau_{ij}) := \left(\sum_{k=1}^{n} (P \boxtimes M_1)^k\right) \boxtimes M_2$$

будут иметь вид $\tau_{ij} = \xi_{ij} \star w_{ij} \in T(\mathbb{R},\mathbb{W}_{\mathcal{A}})$, если на графе G существует маршрут из вершины с номером i в вершину с номером j, и $\tau_{ij} = \iota$ в случае, если такого маршрута не существует. При этом $w_{ij} = \alpha_i \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_s} \alpha_j$ будет определять маршрут наименьшей длины из вершины с номером i в вершину с номером j в вершинной форме, а ξ_{ij} будет равно длине этого маршрута.

Предложенный метод допускает очевидную модификацию посредством переопределением операций

$\xi_1 \odot \xi_2 := \xi_1 \cdot \xi_2$,

$\xi_1 \oplus \xi_2 := \xi_1 \vee \xi_2$;

$w \odot 0 = 0 \odot w := 0$,

$t \odot 0 = 0 \odot t := 0$,

а также функции $\rho: 1..n \times 1..n \to [0,1]$. $\sum_{j=1}^{n} \rho(i,j) = 1$, и использования алгебр $\langle \mathbb{T}([0,1], \mathbb{W}_{\mathcal{A}}), (\odot, \oplus) \rangle$, $\langle \mathbb{M}(\mathbb{T}([0,1], \mathbb{W}_{\mathcal{A}}), n), (\boxdot, \boxplus, \boxtimes) \rangle$ для решения задач о блужданиях, порожденных стохастическими матрицами.

Алгоритм реализации вычисления всех элементов матрицы M имеет верхние оценки временной и емкостной сложности порядка $O(n^4)$ и $O(n^2)$, соответственно.

Литература

1. Кормен, Т. Алгоритмы: построение и анализ [Текст] / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн.– 2-е изд.– М.: Издательский дом «Вильямс», 2005.– 1296 с.

2. Биркгоф, Г. Теория структур [Текст] / Г. Биркгоф. – М.: Издательство иностранной литературы, 1952.– 407 с.

3. Свами, М. Графы, сети и алгоритмы [Текст] / М. Свами, М., К Тхуласираман.– М.: Мир, 1984. - 455 с.

А.Н. Цибуля, М.Н. Хо

О ФОРМАЛИЗАЦИИ ПОНЯТИЯ «АУТЕНТИЧНОСТЬ ЭЛЕКТРОННОГО ДОКУМЕНТА»

(Академия ФСО России, г. Орел)

Переход организаций на использование систем электронного документооборота (СЭД) в условиях необходимости обеспечения требуемых свойств документированной информации требует переосмысления понятийного аппарата, сложившегося при традиционном делопроизводстве. Государственный стандарт ГОСТ Р ИСО 15489-1–2007 определяет, что "организации должны создавать и сохранять аутентичные, надежные и пригодные для использования документы, а также защищать целостность этих документов в течение требуемого времени". Как показал проведенный анализ, в отношении термина "аутентичность документа" отечественные и зарубежные источники дают существенные различия в формулировках. Некоторые из них приведены в таблице 1.

Таблица 1. Определения термина "аутентичность документа"

Источник	Определение
ГОСТ Р ИСО/МЭК 13335-1-2006	1. Подлинность 2. Свойство, гарантирующее, что субъект или ресурс идентичны заявленным
ГОСТ Р 51141-98	**Подлинный документ**: документ, сведения об авторе, времени и месте создания которого, содержащиеся в самом документе или выявленные иным путем, подтверждают досто-