УДК 519.1

А.Н. Исаченко, А.М. Ревякин

О сводимости матроидных оракулов

Приведены полученные авторами за последнее время результаты теоретического исследования сводимости оракулов, соответствующих основным понятиям матроида. Важнейшим итогом являются теорема и иллюстрирующий ее граф.

Ключевые слова: матроид, оракул, сводимость.

Матроид можно определить, используя следующие понятия: независимое множество, база (базис), цикл, функция ранга, остовное множество, оператор замыкания, плоскость, гиперплоскость, функция периметра, циклическое множество, функция окружения. Учитывая двойственные соотношения, матроид можно определить также в терминах конезависимых множеств, кобаз (кобазисов), коциклов и т. д. Свойства указанных понятий матроида приведены в работах [1–7].

Основное определение матроида дается в терминах независимых множеств.

Пару (S, F), где S — конечное множество, $F \subseteq 2^S$, будем называть *системой независимости,* если выполняются следующие два свойства (аксиомы независимости):

($F1$) $\varnothing \in F$;

($F2$) если $A \in F$ и $B \subset A$, то $B \in F$.

Система независимости называется *матроидом* при выполнении условия (аксиома пополнения):

($F3$) если $A, B \in F$ и $|B| = |A| + 1$, то существует $s \in B \setminus A$ такое, что $A \cup s \in F$.

Подмножества из F называются *независимыми,* подмножества из $2^S \setminus F$ — *зависимыми* множествами матроида (S, F).

Максимальное по включению независимое множество называется *базой* матроида, а минимальное по включению зависимое множество — *циклом* матроида.

Остовное множество матроида — это любое множество, содержащее какую-либо его базу.

Циклическое множество матроида — любое множество, содержащее какой-либо его цикл.

Ранговая функция матроида определяется как функция $\rho : 2^S \to N$ со значениями $\rho(A) = \max\{|X| : X \subseteq A, X \in F\}$. $\rho(A)$ называется также *рангом* множества A, а $\rho(S)$ — рангом матроида (S, F).

Пусть (S, F) — матроид, A — некоторое подмножество S, x — некоторый элемент S. Тогда говорим, что x *зависит* от A в матроиде (S, F), если $\rho(A) = \rho(A \cup x)$. Отношение зависимости обозначаем символом «~».

Оператор замыкания определяется как отображение $\sigma:2^S \to 2^S$, при котором $\sigma(A) = \{x \mid x \sim A\}$. Множество, совпадающее со своим замыканием ($A = \sigma(A)$), называется *замкнутым* множеством или *плоскостью* матроида. Плоскость, ранг которой равен $\rho(S)-1$, называют *гиперплоскостью*.

Функция периметра матроида (S,F) есть функция $\gamma : 2^S \to N$ со значениями $\gamma(A) = \min\{|C| : C \subseteq A,\ C$ — цикл$\}$, если A — зависимое множество, и $\gamma(A) = 0$, если $A \in F$.

Окружением матроида называют функцию $\varphi : 2^S \to N \cup \{\infty\}$, задаваемую равенствами $\varphi(A) = \max\{|H| : A \subseteq H,\ H$ — гиперплоскость$\}$, если ранг A меньше ранга S, и $\varphi(A) = \infty$, в противном случае.

Матроид можно определить, используя каждое из приведенных выше понятий, с учетом следующих утверждений.

Утверждение 1. (Аксиома баз). Семейство β подмножеств непустого конечного множества S образует совокупность баз некоторого матроида (S, F) тогда и только тогда, когда оно удовлетворяет условию

($B1$) если $B_1, B_2 \in \beta$ и $x \in B_1 \setminus B_2$, то существует $y \in B_2 \setminus B_1$, для которого $(B_1 \cup y) \setminus x \in \beta$.

Утверждение 2. (Аксиомы циклов.) Семейство ϑ подмножеств непустого конечного множества S образует совокупность циклов некоторого матроида (S,F) тогда и только тогда, когда для него выполняются условия:

($C1$) если C_1, C_2 — различные подмножества из ϑ, то $C_1 \not\subset C_2$;
($C2$) если $C_1, C_2 \in \vartheta$ и $z \in C_1 \cap C_2$, то существует $C_3 \in \vartheta$ такое, что $C_3 \subseteq (C_1 \cup C_2) \setminus z$.

Утверждение 3. (Аксиомы ранга.) Функция $\rho : 2^S \to Z^+$ является ранговой функцией некоторого матроида (S, F) тогда и только тогда, когда для нее выполняются условия:

($R1$) $\rho(\varnothing) = 0$;
($R2$) $\rho(X) \le \rho(X \cup y) \le \rho(X) + 1,\ X \subseteq S,\ y \in S$;
($R3$) если $\rho(X \cup y) = \rho(X \cup x) = \rho(X)$, то $\rho(X \cup x \cup y) = \rho(X)$.

Утверждение 4. (Аксиомы замыкания.) Отображение $\sigma : 2^S \to 2^S$ является оператором замыкания матроида, определенного на множестве S, тогда и только тогда, когда она удовлетворяет условиям:

($S1$) $A \subseteq \sigma(A)$;
($S2$) если $A, B \in 2^S$ и $A \subseteq B$, то $\sigma(A) \subseteq \sigma(B)$;
($S3$) для любого $X \in 2^S$, $\sigma(X) = \sigma(\sigma(X))$;
($S4$) если $y \notin \sigma(X)$, $y \in \sigma(X \cup x)$, то $x \in \sigma(X \cup y)$.

Утверждение 5. (Аксиомы плоскостей.) Семейство P подмножеств непустого конечного множества S образует совокупность плоскостей некоторого матроида (S,F) тогда и только тогда, когда для него выполняются условия:

($P1$) $S \in P$;
($P2$) если $P_1, P_2 \in P$, то $P_1 \cap P_2 \in P$;
($P3$) для каждого $P_1 \in P$, и $x, y \in S \setminus P_1$, $x \ne y$; если существует $P_2 \in P$ такое, что $P_2 \supseteq P_1 \cup x$, $y \notin P_2$, то существует $P_3 \in P$ такое, что $P_3 \supseteq P_1 \cup y$.

Утверждение 6. (Аксиомы гиперплоскостей.) Семейство H подмножеств непустого конечного множества S образует совокупность циклов некоторого матроида (S, F) тогда и только тогда, когда для него выполняются условия:

($H1$) если $H_1, H_2 \in H, H_1 \neq H_2$, то $H_1 \not\subset H_2$;

($H2$) если $H_1, H_2 \in H$ и $x \notin H_1 \cup H_2$, то существует $H_3 \in H$ такое, что $H_3 \supseteq (H_1 \cap H_2) \cup x$.

Утверждение 7. (Аксиомы периметра.) Функция $\gamma : 2^S \to N$ является функцией периметра некоторого матроида (S, F) тогда и только тогда, когда для нее выполняются условия:

($G1$) если $\gamma(X) > 0$, то существует множество $Y \subseteq X$, для которого $\gamma(X) = \gamma(Y) = |Y|$;

($G2$) если $X \supseteq Y$, то $\gamma(X) \geq \gamma(Y)$;

($G3$) если $\gamma(X) = |X|$, $\gamma(Y) = |Y|$, $X \neq Y$, $x \in X \cap Y$, то $\gamma((X \cap Y) \setminus x) > 0$.

Утверждение 8. (Аксиомы окружения.) Функция $\varphi: 2^S \to N \cup \{\infty\}$ является окружением некоторого матроида (S, F) тогда и только тогда, когда для нее выполняются условия:

($\Psi1$) если $\varphi(X) < \infty$, то существует множество $Y \supseteq X$, для которого $\varphi(X) = \varphi(Y) = |Y|$;

($\Psi2$) если $X \supseteq Y$, то $\varphi(X) \leq \varphi(Y)$;

($\Psi3$) если $\varphi(X) = |X|$, $\varphi(Y) = |Y|$, $X \neq Y$, $x \in X \cup Y$, то $\varphi((X \cap Y) \cup x) < \infty$.

Утверждение 9. (Аксиомы циклических множеств.) Семейство ϑ подмножеств непустого конечного множества S образует совокупность циклических множеств некоторого матроида (S, F) тогда и только тогда, когда для него выполняются условия:

($\vartheta1$) если $X, Y \in \vartheta$, то $X \cup Y \in \vartheta$;

($\vartheta2$) для каждого $X \in \vartheta$ и любых $x, y \in X$, $x \neq y$, если существует $Y \in \vartheta$ такое, что $Y \subseteq X \setminus x$, $y \in Y$, то существует $Z \subseteq X \setminus y$, принадлежащее ϑ.

Утверждение 10. (Аксиомы остовных множеств.) Семейство O подмножеств непустого конечного множества S образует совокупность остовных множеств некоторого матроида (S, F) тогда и только тогда, когда для него выполняются условия:

($O1$) $S \in O$;

($O2$) если $A \in O$ и $B \supset A$, то $B \in O$;

($O3$) если $A, B \in O$ и $|B| = |A| + 1$, то существует $s \in B \setminus A$ такое, что $A \cup s \in O$.

Из приведенных утверждений следует эквивалентность определений матроида в терминах любого из указанных выше понятий. Задав, например, матроид семейством его циклов, мы однозначно определим семейство его независимых множеств, баз, циклов, циклических и остовных множеств, плоскостей и гиперплоскостей, функции ранга, периметра, окружения и оператор замыкания.

Одно из главных понятий теории матроидов — двойственность — основано на следующем утверждении.

Утверждение 11. Пусть β — семейство баз матроида (S, F). Тогда множество $\beta^* = \{S \setminus B, B \in \beta\}$ является семейством баз некоторого матроида (S, F^*).

Матроид (S, F^*) называется двойственным по отношению к матроиду (S, F). Множество $X \in F^*$ по отношению к исходному матроиду (S, F) называют конезависимым, $B \in \beta^*$ — кобазой, $C \in \Im^*$ семейству циклов (S, F^*) — коциклом матроида (S, F). Аналогично определяем понятие коциклических и коостовных множеств, коплоскостей и когиперплоскостей, функции коранга, копериметра, коокружения и оператор козамыкания. Тем самым к имеющимся определениям матроида добавляются еще одиннадцать эквивалентных определений.

Предположим теперь, что рассматривается некоторая задача на матроиде (S, F). С точки зрения вычислительной сложности [5] размер задачи следует определить через количество элементов множества S. Но при этом количество входных данных будет зависеть от способа задания матроида и выражаться либо через число подмножеств, определяющих то или иное семейство матроида, либо через число значения той или иной функций на всех подмножествах из 2^S. То есть количество входных данных асимптотически экспоненциально, что приводит к экспоненциальной временной сложности от $|S|$ построения входных данных для задачи и тем самым бессмысленности определения временной сложности алгоритма решения задачи как функции от длины входа задачи. Для устранения данной трудности вводится понятие оракула матроида. Пусть $M = (S, F)$ — матроид, а u — некоторое понятие матроида. Если понятие определяет характер каждого множества $A \subseteq S$, то через $u(M)$ обозначим соответствующее семейство подмножеств матроида. Если u определяет функцию, то через $u(A, M)$ обозначим ее значение для подмножества A на матроиде M. Оракулом $O(u)$ назовем инъективное отображение $W_u : (2^S, \mu) \to E(u)$, где $\mu(S)$ — совокупность всех матроидов на множестве S, $E(u)$ — множество, конкретное для каждого понятия. Так для понятий независимое, конезависимое, база (базис), кобаза (кобазис), цикл, коцикл, остов, коостов, поверхность, коповерхность, циклическое, коциклическое, гиперплоскость, когиперплоскость $E(u) = \{$ДА, НЕТ$\}$ и $W_u(A, M) = \{$ДА, если $A \in u(M)$; НЕТ, если $A \notin u(M)\}$. Для понятий замыкание, козамыкание $E(u) = 2^S$, для понятий ранг, коранг, периметр, копериметр $E(u) = \{0, \ldots, |S|\}$, для понятий окружение, коокружение $E(u) = \{1, \ldots, |S|, \infty\}$. Для всех этих понятий $W_u(A, M) = u(A, M)$.

Если имеется задача Ω на матроиде $M = (S, F)$, заданном понятием u, то сложность ее решения алгоритмом Λ относительно оракула $O(u)$ определяется как число элементарных операций, выполняемых алгоритмом. Обозначим это число через $m_u(\Omega, \Lambda, M)$. При этом одно обращение к оракулу $O(u)$, то есть получение значения $W_u(A, M)$, также считается элементарной операцией. Сложность алгоритма Λ для задачи Ω относительно оракула $O(u)$ определяется как $\max\limits_{M \in \mu(S)} (m_u(\Omega, \Lambda, M))$.

Возникает вопрос: отличается ли сложность алгоритма относительно разных оракулов? Будем говорить, что оракул $O(u_1)$ полиномиально сводим к оракулу $O(u_2)$, если значение $W u_1(A, M)$ может быть получено за полиномиальное число обращений к оракулу $O(u_2)$. Относительно полиномиальной сводимости оракулов справедлива следующая теорема [5].

Теорема. В ориентированном графе, вершинами которого являются матроидные оракулы, путь от вершины a к вершине b существует тогда и только тогда, когда оракул a полиномиально сводим к оракулу b.

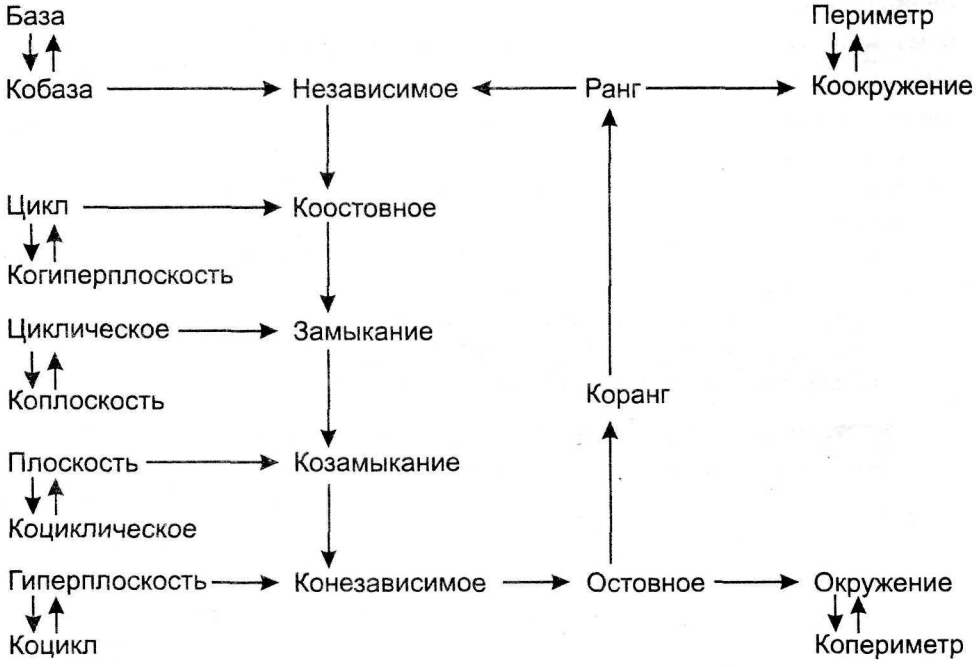

Рис. 1. Граф, иллюстрирующий полиномиальную сводимость оракула

На графе представлены практически все полученные ранее результаты по полиномиальной сводимости матроидных оракулов. Сформулированная теорема является главным результатом работы и практически закрывает это интересное направление исследований.

Литература

1. *Welsh D.J.A.* Matroid theory. London: Acad. Press, 1976.
2. *Инглтон Э.У.* Трансверсальные матроиды и родственные им структуры // Проблемы комбинаторного анализа. М.: Мир, 1980. С. 64–81.
3. *Robinson G.C., Welsh D.J.A.* The computational complexity of matroid algorithms // Mathematical Proceedings of the Cambridge Philosophical Society. 1980. Vol. 87. P. 29–45.
4. *Исаченко А.Н.* Об одном критерии для матроидов // Вестник БГУ. Сер. 1. 1983. № 2. С. 59–60.
5. *Исаченко А.Н.* Полиномиальная сводимость матроидных оракулов // Известия АН БССР. Сер. физ.-мат. наук. 1984. № 6. С. 33–36.
6. *Ревякин А.М.* Матроиды: криптоморфные системы аксиом и жесткость ферм // Вестник МГАДА. Серия «Философские, социальные и естественные науки». 2010. № 5. С. 96–106.
7. *Revyakin A.M.* Matroids // J. Math. Sci. 2002. Vol. 108. № 1. P. 71–130.

Authors' recent results of reduction of matroid oracles are presented. The theorem and it's attached graph are the most important results of the long reseach.

Keywords: matroid, oracle, reduction.