Ю. В. Матиясевич, Одна схема доказательств в дискретной математике, *Зап. научн. сем. ЛОМИ*, 1974, том 40, 94–100

Ю.В.Матиясевич

ОДНА СХЕМА ДОКАЗАТЕЛЬСТВ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

(Результат доложен 24 мая 1973 г.)

Цель настоящей работы – описать одну возможную схему использования средств математической теории логического вывода для доказательства теорем дискретной математики.

Предлагаемая схема относится к теоремам вида "если объект X обладает свойством $\mathcal{P}$, то объект X обладает свойством Q", где X – переменная для конечных комбинаторных объектов какого-либо типа. При этом от свойства $\mathcal{P}$ требуется, чтобы оно допускало формализацию в рамках некоторой дедуктивной системы в смысле, разъясняемом ниже.

Под дедуктивной системой мы понимаем установление в соответствие каждому объекту X четверки вида $<Я, A, T, F>$; здесь $Я$ – некоторое множество, элементы которого будем называть ф о р м у л а м и; A – некоторое подмножество множества $Я$, формулы из которого будем называть а к с и о м а м и; T – некоторое множество предикатов (называемых п р а в и л а м и в ы в о д а), областью определения каждого из которых является множество всех n-ок формул при некотором n, не меньшем 2; F – некоторое подмножество множества $Я$, формулы из которого будем называть ф и н а л ь н ы м и. В ы в о д о м будем называть всякий список формул $P_1, \ldots, P_k$, в котором для каждой формулы P_j, не являющейся аксиомой, можно указать формулы $P_{i_1}, \ldots, P_{i_m}$ $(i_1, \ldots, i_m < j)$ такие, что набор формул $P_{i_1}, \ldots, P_{i_m}, P_j$ удовлетворяет одному из правил вывода. Как обычно, формула называется в ы в о д и м о й, если существует вывод, в который она входит. Мы говорим, что данная дедуктивная система ф о р м а л и з у е т свойство $\mathcal{P}$, если объект X обладает этим свойством в том и только в том случае, когда выводима хотя бы одна из финальных формул, соответствующих объекту X.

(Легко видеть, что мы могли бы упростить терминологию, исключив понятие аксиомы и разрешив вместо этого иметь одноместные правила вывода, однако такая унификация представляется нецелесообразной с эвристической точки зрения).

Доказательство импликации $\mathcal{P}(X) \Longrightarrow Q(X)$ может a priori быть проведено по следующей схеме:

1) указывается формализация свойства $\mathcal{P}$;

2) указывается свойство Q^*, определенное на парах вида $<X, P>$, где P – формула;

3) доказывается, что для любой аксиомы P имеет место $Q^*(X, P)$;

4) доказывается, что для любых формул $P_1, \ldots, P_n$, удовлетворяющих какому-либо правилу вывода, из $Q^*(X, P_1) \& \ldots$ $\ldots \& Q^*(X, P_{n-1})$ следует $Q^*(X, P_n)$;

5) доказывается, что для любой финальной формулы P из $Q^*(X,P)$ следует $Q(X)$.

Таким образом, по этой схеме доказательство теоремы "если X обладает свойством $\mathcal{P}$, то X обладает свойством Q" проводится индукцией по длине формального доказательства того, что X обладает свойством $\mathcal{P}$.

В оставшейся части статьи мы продемонстрируем "работоспособность" описанной выше абстрактной схемы, дав новое доказательство достаточности в следующей теореме.

ТЕОРЕМА (Л.М.Витавер). Для того, чтобы обыкновенный граф L допускал раскраску вершин не более, чем в γ цветов, необходимо и достаточно, чтобы существовала такая ориентация всех ребер графа L, при которой в получающемся ориентированном графе $\vec{L}$ нет ориентированных маршрутов длины γ.

Эта теорема доказана в [I]; доказательство ее приведено также в монографии [2], из которой мы заимствуем терминологию, относящуюся к теории графов.

Переформулируем интересующую нас часть теоремы в требуемом нам виде.

Если обыкновенный граф L не допускает раскраски вершин не более, чем в γ цветов (свойство $\mathcal{P}$), то *при любой ориентации всех ребер графа* L *в получающемся* ориентированном графе $\vec{L}$ есть ориентированный маршрут длины γ (свойство Q).

Для формализации свойства $\mathcal{P}$ мы введем в рассмотрение $\nu(\nu-1)/2$ булевых переменных, где ν – число вершин графа L. Каждой булевой переменной поставим во взаимно однозначное соответствие неупорядоченную пару вершин графа L. Будем считать, что вершины пронумерованы числами $1, \ldots, \nu$ и обозначать через $E_{i,j}$ и $E_{j,i}$ $(i \neq j)$ одну и ту же булеву переменную, которой ставится в соответствие пара, состоящая из i-ой и j-ой вершин графа.

Формулами будут всевозможные дизъюнкции переменных $E_{i,j}$ и их отрицаний. При этом мы не будем различать дизъюнкции, отличающиеся лишь перестановкой или повторением членов.

Аксиомами будут всевозможные формулы следующих трех типов:

$$\neg E_{i,j} \quad (\widetilde{ij} \in U), \tag{I}$$

где U – множество ребер графа L,

$$\neg E_{i,j} \vee \neg E_{j,k} \vee E_{i,k} \quad (1 \le i,j,k \le \nu,\ i \ne j,\ j \ne k,\ i \ne k), \tag{2}$$

$$\bigvee_{1 \le k < \ell \le \gamma+1} E_{i_k, i_\ell} \quad (1 \le i_1 < i_2 < \ldots < i_{\gamma+1} \le \nu). \tag{3}$$

Семантика этих формул такова. Допустим, что граф L каким-то образом раскрашен не более, чем в γ цветов. Присвоим переменной $E_{i,j}$ значение ИСТИНА, если i-я и j-я вершины раскрашены в один цвет, и ЛОЖЬ в противном случае. По определению раскраски все формулы вида (I) примут значение ИСТИНА. Это же значение примут и все формулы вида (2) ввиду транзитивности отношения "быть вершинами, раскрашенными в один цвет". А поскольку раскраска использует не более γ цветов, то все формулы вида (3) также примут значение ИСТИНА. С другой стороны, нетрудно проверить, что если переменным $E_{i,j}$ каким-либо способом присвоены истиностные значения так, что при этом все формулы (I)–(3) приняли значение ИСТИНА, то граф L допускает раскраску вершин не более чем в γ цветов.

В качестве единственного правила вывода мы возьмем правило, восходящее (в пропозициональном случае) к работам П.С.Порецкого и названное в [3] правилом резолюции. Согласно этому правилу из взятых в произвольном порядке формул $G \vee B$ и $\neg B \vee H$, где B – булева переменная, а G и H – произвольные дизъюнкции, можно вывести формулу $G \vee H$. Как показано выше, если граф L обладает свойством $\mathcal{P}$ (то есть не допускает раскраски не более, чем в γ цветов), то нельзя присвоить переменным $E_{i,j}$ такие значения, при которых все аксиомы примут значение ИСТИНА. В этом случае согласно теореме о полноте правила резолюции (см., например, [3]) из аксиом посредством, вообще говоря, неоднократного применения правила резолюции выводима тождественно ложная пустая дизъюнкция, которую мы будем обозначать через $\square$ и которая будет являться единственной финальной формулой.

Для того, чтобы сформулировать свойство Q^*, нам надо обобщить понятие ориентированного маршрута. Ориентацию ребер графа можно описывать посредством антисимметричного предиката $\mathcal{R}_L$, определенного на парах вершин, соединенных ребром. Свойство Q можно сформулировать следующим образом: каков бы ни был антисимметричный предикат $\mathcal{R}_L$, существует список троек вида

$$\langle i_1, 1, i_2 \rangle, \langle i_2, 1, i_3 \rangle, \ldots, \langle i_\gamma, 1, i_{\gamma+1} \rangle,$$

где $i_1, \ldots, i_{\gamma+1}$ – вершины графа L и при $k = 1, \ldots, \gamma$ i_k-я и i_{k+1}-я вершины соединены ребром и имеет место $\mathcal{R}_L(i_k, i_{k+1})$. Для формулировки свойства Q^* мы для каждой формулы H будем рассмат-

ривать всевозможные антисимметричные предикаты $\mathcal{R}_H$, определенные на тех парах вершин, для которых поставленные им в соответствие булевы переменные входят в H не под знаком отрицания. Будем называть $(\mathcal{R}_L, \mathcal{R}_H)$ -м а р ш р у т о м всякий список троек вида

$$<i_1, N_1, i_2>, <i_2, N_2, i_3>, \ldots, <i_m, N_m, i_{m+1}>, \qquad (4)$$

где $i_1, \ldots, i_m$ - вершины графа L, и при $k = 1, \ldots, m$ выполнено одно из следующих условий:

а) $N_k = 1$, i_k -я и i_{k+1} -я вершины соединены ребром и имеет место $\mathcal{R}_L(i_k, i_{k+1})$;

б) $N_k = 2$, переменная $E_{i_k, i_{k+1}}$ входит в H не под знаком отрицания и имеет место $\mathcal{R}_H(i_k, i_{k+1})$;

в) $N_k = 3$ и переменная $E_{i_k, i_{k+1}}$ входит в H под знаком отрицания.

Д л и н о й $(\mathcal{R}_L, \mathcal{R}_H)$ -маршрута (4) будем называть количество тех троек, средний член которых не равен 3. Если $\mathcal{A}$ - некоторый $(\mathcal{R}_L, \mathcal{R}_H)$ -маршрут вида (4), в котором $i_1 = i_m$, а k - натуральное число, то через $(\mathcal{A})^k$ будем, как обычно, обозначать маршрут, получающийся k -кратным повторением $\mathcal{A}$.

Будем говорить, что имеет место $Q^*(L, H)$, если каковы бы ни были антисимметричные предикаты $\mathcal{R}_L$ и $\mathcal{R}_H$, существует $(\mathcal{R}_L, \mathcal{R}_H)$ -маршрут длины не менее, чем γ.

Проверим, что для любой аксиомы P имеет место $Q(L, P)$. Пусть P - аксиома вида (I). Не ограничивая общности, мы можем считать, что имеет место $\mathcal{R}_L(i, j)$. $(\mathcal{R}_L, \mathcal{R}_H)$ -маршрут

$$(<i, 1, j>, <j, 3, i>)^\gamma$$

имеет длину γ.

Пусть теперь P - аксиома вида (2). Не ограничивая общности, мы можем считать, что имеет место $\mathcal{R}_P(k, i)$. $(\mathcal{R}_L, \mathcal{R}_P)$ -маршрут

$$(<i, 3, j>, <j, 3, k>, <k, 2, i>)^\gamma$$

имеет длину γ.

Рассмотрим теперь случай, когда P - аксиома вида (3). Будем искать требуемый $(\mathcal{R}_L, \mathcal{R}_P)$ -маршрут среди маршрутов вида

$$<j_1, 2, j_2>, \ldots, <j_m, 2, j_{m+1}>, \qquad (5)$$

где $j_1, \ldots, j_m$ - вершины из множества $\{i_1, \ldots, i_{\gamma+1}\}$. Допустим, что все такие маршруты имеют длину менее γ и пусть (5) - самый длинный из них. Так как $m < \gamma$, то среди вершин $i_1, \ldots, i_{\gamma+1}$ есть вершина (обозначаемая ниже через i), которая не встречается в (5). Список

$$<i, 2, j_1>, <j_1, 2, j_2>, \ldots, <j_m, 2, j_{m+1}>$$

не является $(\mathcal{R}_L, \mathcal{R}_H)$ -маршрутом ввиду максимальности маршрута (5), поэтому имеет место $\neg\mathcal{R}_P(i, j_1)$ и по антисимметричности предиката $\mathcal{R}_P$ выполнено $\mathcal{R}_P(j_1, i)$. Пусть k - наибольшее число, не превосходящее $m+1$, такое, что имеет место $\mathcal{R}_P(j_k, i)$. Так как список

$$<j_1, 2, j_2>, \ldots, <j_m, 2, j_{m+1}>, <j_k, 2, i>$$

также не может быть $(\mathcal{R}_L, \mathcal{R}_P)$ -маршрутом, то $k < m+1$. По выбору k имеет место $\neg\mathcal{R}_P(j_{k+1}, i)$ и, значит, $\mathcal{R}_P(i, j_{k+1})$. Мы получаем следующий $(\mathcal{R}_L, \mathcal{R}_P)$ -маршрут, более длинный, чем маршрут (5):

$$<j_1, 2, j_2>, \ldots, <j_{k-1}, 2, j_k>, <j_k, 2, i>, <i, 2, j_{k+1}>,$$
$$<j_{k+1}, 2, j_{k+2}>, \ldots, <j_m, 2, j_{m+1}>.$$

Искомое противоречие получено.

Покажем теперь, что правило резолюции сохраняет истинность предиката Q^*. Пусть $A = A' \vee E_{i,j}$, $B = \neg E_{i,j} \vee B'$, $C = A' \vee B'$ и пусть имеет место $Q^*(L, A)$ & $Q^*(L, B)$. Чтобы установить истинность $Q^*(L, C)$ мы должны для любых двух антисимметричных предикатов $\mathcal{R}_L$ и $\mathcal{R}_C$ указать $(\mathcal{R}_L, \mathcal{R}_C)$-маршрут длины не менее γ.

Обозначим через $\mathcal{R}_B$ предикат, совпадающий с $\mathcal{R}_C$ в области своего определения (которая, очевидно, не шире области определения $\mathcal{R}_C$). Обозначим через

$$<b_1, N_1, b_2>, \ldots, <b_s, N_s, b_{s+1}> \qquad (6)$$

какой-либо $(\mathcal{R}_L, \mathcal{R}_B)$ -маршрут длины не менее γ. Маршрут (6) может, вообще говоря, содержать тройки

$$<i, 3, j>, \quad <j, 3, i>. \qquad (7)$$

Не ограничивая общности будем предполагать в дальнейшем, что маршрут (6) содержит наименьшее возможное суммарное число троек (7).

Если ни одна из троек (7) не входит в (6), то это и есть искомый $(\mathcal{R}_L, \mathcal{R}_C)$ -маршрут. Допустим теперь, что в (6) входят обе тройки $<i, 3, j>$ и $<j, 3, i>$, скажем, на k -ом и ℓ -ом местах соответственно $(1 \le k < \ell \le s)$, а на местах от $(k+1)$-го до $(\ell+1)$ -го стоят тройки других видов. Если $N_{k+1} = \ldots = N_{\ell-1} = 3$, то список

$$<b_1, N_1, b_2>, \ldots, <b_{k-1}, N_{k-1}, b_k>, <b_{\ell+1}, N_{\ell+1}, b_{\ell+2}>, \ldots,$$
$$<b_s, N_s, b_{s+1}>$$

также является $(\mathcal{R}_L, \mathcal{R}_B)$ -маршрутом длины не менее γ , но содержит меньше троек вида (7), что противоречит минимальности маршрута (6). Таким образом, среди чисел $N_{k+1}, \ldots, N_{e-1}$ есть число, отличное от 3, и искомым $(\mathcal{R}_L, \mathcal{R}_c)$ -маршрутом является маршрут

$$(<b_{k+1}, N_{k+1}, b_{k+2}>, \ldots, <b_{e-1}, N_{e-1}, b_e>)^{\gamma}.$$

В дальнейшем, не ограничивая общности, мы будем считать, что в маршрут (6) не входит тройка $<j, 3, i>$.

Обозначим через $\mathcal{R}_A$ предикат, истинный на паре $<j, i>$ и совпадающий на остальных парах из области своего определения с предикатом $\mathcal{R}_c$. Обозначим через

$$<a_1, M_1, a_2>, \ldots, <a_t, M_t, a_{t+1}> \qquad (8)$$

какой-либо $(\mathcal{R}_L, \mathcal{R}_A)$ -маршрут длины не менее γ. Если тройка $<j, 2, i>$ не входит в (8), то это и есть искомый $(\mathcal{R}_L, \mathcal{R}_B)$-маршрут. Оставшаяся часть доказательства распадается на два случая.

Случай I. Тройка $<j, 2, i>$ входит в (8) не менее, чем дважды. Пусть тройка $<j, 2, i>$ входит в (8) на m -ом и n-ом местах, $1 \le m < n \le t$, а на местах от $(m+1)$-го до $(n-1)$-го стоят другие тройки. В этом случае, заменив в (6) каждое вхождение тройки $<i, 3, j>$ на список

$$<a_{m+1}, M_{m+1}, a_{m+2}>, \ldots, <a_{n-1}, M_{n-1}, a_n>,$$

мы получим искомый $(\mathcal{R}_L, \mathcal{R}_c)$ -маршрут.

Случай 2. Тройка $<j, 2, i>$ входит в (8) ровно один раз. Пусть тройка $<j, 2, i>$ входит в (8) на m -ом месте. Возможны два подслучая.

Подслучай 2.I. Тройка $<i, 3, j>$ входит в (6) не менее, чем дважды. Пусть тройка $<i, 3, j>$ входит в (6) на k -ом и ℓ -ом местах, $1 \le k < \ell \le s$, а на местах от $(k+1)$-го до $(\ell-1)$-го стоят другие тройки. Если $N_{k+1} = \ldots = N_{\ell-1} = 3$, то список

$$<b_1, N_1, b_2>, \ldots, <b_k, N_k, b_{k+1}>,$$

$$<b_{\ell+1}, N_{\ell+1}, b_{\ell+2}>, \ldots, <b_s, N_s, b_{s+1}>$$

также является $(\mathcal{R}_L, \mathcal{R}_B)$ -маршрутом длины не менее γ , но содержит меньше троек вида (7), что противоречит минимальности маршрута (6). Таким образом, среди чисел $N_{k+1}, \ldots, N_{\ell-1}$ есть число, отличное от 3. Заменив m-ю тройку в (8) на список

$$<b_{k+1}, N_{k+1}, b_{k+2}>, \ldots, <b_{\ell-1}, N_{\ell-1}, b_\ell>,$$

мы получим искомый $(\mathcal{R}_L, \mathcal{R}_c)$ -маршрут.

Подслучай 2.2. Тройка $<i, 3, j>$ входит в (6) ровно один раз. Пусть тройка $<i, 3, j>$ входит в (6) на k -ом месте. Сум-

ма длин двух $(\mathcal{R}_1, \mathcal{R}_2)$ -маршрутов

$$<a_1, M_1, a_2>, \ldots, <a_{m-1}, M_{m-1}, a_m>,$$

$$<b_{k+1}, N_{k+1}, b_{k+2}>, \ldots, <b_s, N_s, b_{s+1}>$$

и

$$<b_1, N_1, b_2>, \ldots, <b_{k-1}, N_{k-1}, b_k>,$$

$$<a_{m+1}, M_{m+1}, a_{m+2}>, \ldots, <a_t, M_t, a_{t+1}>$$

не меньше, чем $2\gamma - 1$, следовательно, хоть один из них имеет длину не менее γ .

Нам осталось проверить, что из $Q^*(L, \square)$ следует $Q(L)$, но это очевидно.

Литература

I. Витавер Л.М. Нахождение минимальных раскрасок вершин графа с помощью булевых степеней матрицы смежности. "Докл. АН СССР", I962, I47, № 4, 758–759.

2. Зыков А.А. Теория конечных графов. Новосибирск, I969.

3. Robinson J.A. A machine-oriented logic based on the resolution principle. "J.Assoc.Comp.Mach.", 1965, 12, № 1, 23–41 (русск.перев. в "Киберн.сб.", I970, 7, I94–2I8).