Yu. V. Matiyasevich, On metamathematical approach to proving theorems of discrete mathematics, *Zap. Nauchn. Sem. LOMI*, 1975, Volume 49, 31–50

З а п и с к и   н а у ч н ы х   с е м и н а р о в Л О М И, т.49

Ю.В.Матиясевич

О МЕТАМАТЕМАТИЧЕСКОМ ПОДХОДЕ К ДОКАЗАТЕЛЬСТВУ ТЕОРЕМ ДИСКРЕТНОЙ МАТЕМАТИКИ

(Результаты доложены в марте – апреле 1974г.)

1. В настоящей работе описывается некоторый новый подход к задачам дискретной математики. Начало этому подходу, названному метаматематическим, было положено в работах автора [1],[2].

1.1. Основная черта метаматематического подхода состоит в следующем. Пусть мы изучаем некоторое свойство $\mathcal{R}$ конечных дискретных объектов какого-либо типа. Первый этап метаматематического подхода состоит в формализации свойства $\mathcal{R}$: мы должны попытаться найти некоторую дедуктивную систему $\mathcal{R}$ и связать с каждым объектом X , обладающим свойством $\mathcal{R}$, новый конечный дискретный объект – формальное доказательство $\mathcal{P}_{\mathcal{R}}(X)$ того, что X обладает свойством $\mathcal{R}$, проведенное в рамках системы $\mathcal{R}$. Дальнейшее изучение свойства $\mathcal{R}$ включает в себя рассмотрение наряду с X также и $\mathcal{P}_{\mathcal{R}}(X)$ и анализ структур обоих объектов. Именно введение в рассмотрение формальных доказательств и является основной характеристической чертой метаматематического подхода.

1.2. Новый подход был выдвинут в надежде, что рассмотрение формальных доказательств расширит наши возможности доказывать теоремы дискретной математики. При этом предполагается, что всякое доказательство в рамках метаматематического подхода должно допускать переизложение в традиционных терминах и потому принятие этого подхода не расширяет множество теорем. Таким образом, метаматематический подход не есть какой-либо новый принцип математических рассуждений, который может быть принят одними математиками,но оказаться неприемлемым для других. В этом отношении он в корне отличен, скажем, от метода математической индукции в арифметике или аксиомы выбора в теории множеств. Метаматематический подход дает лишь схему возможного доказательства, нацеливает нас на поиски доказательства той или иной формы. В этом отношении метаматематический подход подобен, например, методу производящих функций.

2. Опишем, что мы понимаем под дедуктивной системой и приведем примеры.

2.1. Произвольная д е д у к т и в н а я   с и с т е м а –

это четверка вида $\langle \mathcal{F}, \mathcal{A}, \mathcal{D}, \mathcal{H} \rangle$; здесь $\mathcal{F}$ - некоторое множество, элементы которого называют ф о р м у л а м и ; $\mathcal{A}$ - некоторое подмножество множества $\mathcal{F}$, формулы из которого называются а к с и о м а м и ; $\mathcal{D}$ - 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 каком-либо n , не меньшем 2; $\mathcal{H}$ - подмножество множества $\mathcal{F}$, формулы из которого называются ф и н а л ь н ы м и . Под в ы в о д о м мы понимаем всякий список формул $F_1, \ldots, F_k$, в котором для каждой формулы F_i , не являющейся аксиомой, можно указать такие формулы $F_{j_1}, \ldots, F_{j_m}$ $(j_1, \ldots, j_m < i)$, что набор формул $\langle F_{j_1}, \ldots, F_{j_m}, F_i \rangle$ удовлетворяет одному из правил вывода. Формула называется в ы в о д и м о й , если существует вывод, в который она входит.

Легко видеть, что можно было упростить терминологию, исключив понятие аксиомы и допустить в качестве правил одноместные предикаты, однако такая унификация нецелесообразна с эвристической точки зрения.

2.2. Мы говорим, что данное свойство $\mathcal{R}$ формализовано, если каждому объекту X (из области определения $\mathcal{R}$) поставлена в соответствие некоторая дедуктивная система $\mathcal{R}(X)$ такая, что X обладает свойством $\mathcal{R}$ в том и только том случае, когда в $\mathcal{R}(X)$ выводима хотя бы одна из финальных формул.

Более традиционный подход к формализации состоял бы в рассмотрении лишь одной фиксированной (т.е. не зависящей от объектов) дедуктивной системы (из которой было бы исключено понятие финальной формулы). В случае традиционной формализации объект X обладает свойством $\mathcal{R}$ в том и только том случае, когда в рассматриваемой дедуктивной системе выводима некоторая формула $H(X)$ (играющая роль финальных формул при нашей формализации). Однако опыт разработки методов машинного доказательства теорем (см. например,[3], [4]) и небольшой опыт применения метаматематического подхода (см. [1] ,[2]) показывает, что имеет смысл для каждого объекта строить свою специфическую дедуктивную систему, тесно связанную с этим объектом. При этом обычно удается в качестве финальных формул брать формулы очень простой структуры, что невозможно при более традиционном подходе к формализации.

3. Приведем примеры дедуктивных систем, возникающих при формализации некоторых свойств графов. Под графом в настоящей работе понимается конечный неориентированный граф без петель и кратных ребер. Такой граф может быть задан посредством множества V его вершин и симметричного двуместного предиката J , задающего отношение "быть вершинами, соединенными ребром"; мы будем обозначать этот граф парой $\langle V, J \rangle$.

Будем называть n-р а с к р а с к о й графа $\langle V, J \rangle$ отображение множества V в множество $\{1,\ldots,n\}$, интерпретируемое как "множество цветов". Раскраску будем называть правильной, если концы каждого ребра оказываются окрашенными в разные цвета. Граф будем называть n-(не)раскрашиваемым, если он (не) имеет правильную n-раскраску. Мы начнем с указания нескольких формализаций свойства "быть n-нераскрашиваемым графом".

3.I. Каждая раскраска однозначно (с точностью до перенумерации цветов) восстанавливается по симметричному двуместному отношению "вершины x и y окрашены в один цвет", которое мы будем обозначать $\mathcal{E}xy$. Мы будем считать, что предикат $\mathcal{E}$ определен на неупорядоченных парах неравных вершин и не различать обозначения $\mathcal{E}xy$ и $\mathcal{E}yx$.

Очевидно, что если предикат $\mathcal{E}$ соответствует некоторой раскраске, то для любых трех вершин x, y, z из $\mathcal{E}xy$ и $\mathcal{E}yz$ следует $\mathcal{E}xz$, или, что то же самое, справедлива формула

$$\neg\mathcal{E}xy \vee \neg\mathcal{E}yz \vee \mathcal{E}xz. \tag{I}$$

Наоборот, если произвольно заданный предикат удовлетворяет всем формулам вида (I), то он соответствует некоторой раскраске.

Если раскраска правильна, то на любой паре из двух вершин x и y, соединенных ребром, предикат $\mathcal{E}$ должен быть ложным. Мы будем записывать это символически в виде

$$(\mathcal{J}xy \Rightarrow) \qquad \neg\mathcal{E}xy. \tag{2}$$

(Говоря в дальнейшем про "все формулы вида (2)" мы будем иметь в виду всевозможные формулы вида $\neg\mathcal{E}xy$, где x и y - произвольные вершины, удовлетворяющие выписанному слева условию $\mathcal{J}xy$. Аналогичное обозначение будет применяться и дальше.) С другой стороны, если предикат $\mathcal{E}$ удовлетворяет всем формулам вида (I) и (2), то раскраска, которой он соответствует, правильна.

Наконец, если мы имеем дело с n-раскраской, то в любом множестве из $(n+1)$-ой вершины $x_0,\ldots,x_n$ обязательно найдутся две, окрашенные одинаково, и, следовательно, все формулы вида

$$\bigvee_{i=0}^{n-1}\ \bigvee_{j=i+1}^{n} \mathcal{E}x_i x_j \tag{3}$$

должны быть истинны. С другой стороны, если предикат $\mathcal{E}$ удовлетворяет всем формулам вида (I) и (3), то он соответствует некоторой n-раскраске.

Таким образом

граф $\langle V, \mathfrak{I}\rangle$ является n-нераскрашиваемым тогда и только тогда, когда множество всех формул вида (I),(2) и (3) является противоречивым.

Известно много методов проверки множества формул на непротиворечивость. Здесь будет использован так называемый метод гиперрезолюций, введенный в [5]. Нам потребуется, по-существу, лишь его пропозициональный вариант и знакомство с работой [5] не обязательно для дальнейшего чтения.

Метод гиперрезолюций имеет две двойственные друг другу формы - можно строить выводы как из чисто положительных дизъюнкций, так и из чисто отрицательных. Первая форма дает следующую дедуктивную систему. Формулами являются всевозможные дизъюнкции элементарных формул вида $\mathcal{E}xy$; при этом здесь и в дальнейшем дизъюнкции, различающиеся лишь порядком или повторением членов, мы не различаем. Аксиомы - это формулы вида (3). Правила вывода соответствуют формулам (I) и (2) и, записанные в традиционной форме, выглядят так:

$$\frac{\mathfrak{A} \vee \mathcal{E}xy \qquad \mathfrak{B} \vee \mathcal{E}yz}{\mathfrak{A} \vee \mathfrak{B} \vee \mathcal{E}xz}, \qquad (4')$$

$$(\mathfrak{I}xy \Rightarrow) \qquad \frac{\mathfrak{A} \vee \mathcal{E}xy}{\mathfrak{A}}. \qquad (4'')$$

Единственной финальной формулой является тождественно ложная нульчленная дизъюнкция $\square$. Теорема о полноте метода гиперрезолюций (см.[5]) гарантирует, что пустая дизъюнкция $\square$ выводима, если (и, очевидно, только если) множество всех формул вида (I),(2) и (3) противоречиво. Таким образом мы действительно имеем дело с формализацией свойства "быть n-нераскрашенным графом".

Вторая форма метода гиперрезолюций дает такую дедуктивную систему. Формулами являются всевозможные дизъюнкции элементарных формул вида $\neg\mathcal{E}xy$, аксиомы - это формулы вида (2), а правила вывода таковы:

$$\frac{\mathfrak{A} \vee \neg\mathcal{E}xz}{\mathfrak{A} \vee \neg\mathcal{E}xy \vee \neg\mathcal{E}yz}, \qquad (5')$$

$$\frac{\mathfrak{A}_1 \vee \rceil\mathcal{E}x_0x_1 \ \ldots \ \mathfrak{A}_{n(n+1)/2} \vee \rceil\mathcal{E}x_{n-1}x_n}{\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_{n(n+1)/2}}. \qquad (5'')$$

Единственной финальной формулой также является □.

3.2. Укажем теперь две формализации того же свойства "быть n-нераскрашиваемым графом" в терминах отношения "вершина x окрашена в цвет с номером меньшим, чем вершина y". Мы будем записывать этот предикат в виде $x<y$, а вместо $\rceil(x<y)$ будем писать $x \geqslant y$; предполагается, что этот предикат определен на всех упорядоченных парах вершин, не обязательно различных.

Нетрудно проверить, что роль формул (I),(2) и (3) будут теперь играть формулы

$$x \geqslant x, \qquad (6)$$

$$x<y \vee y<z \vee x \geqslant z, \qquad (7)$$

$$(\mathcal{I}xy \Rightarrow) \qquad x<y \vee y<x, \qquad (8)$$

$$x_0 \geqslant x_1 \vee x_1 \geqslant x_2 \vee \ldots \vee x_{n-1} \geqslant x_n. \qquad (9)$$

Формулы вида (6) необходимы лишь для того, чтобы множество всех формул вида (I) имело своего полного аналога - множество всех формул вида (6) и (7) (предикат $<$ соответствует некоторой раскраске тогда и только тогда, когда он удовлетворяет всем формулам вида (6) и (7)). Если же мы интересуемся исключительно n-раскрасками, то формулы вида (6) можно исключить, поскольку они являются частным случаем формул вида (9).

Первая форма метода гиперрезолюций дает следующую дедуктивную систему. Формулами являются всевозможные дизъюнкции элементарных формул вида $x<y$, аксиомы - это формулы вида (8), а правила вывода таковы:

$$\frac{\mathfrak{A} \vee x<z}{\mathfrak{A} \vee x<y \vee y<z}, \qquad (10)$$

$$\frac{\mathfrak{A}_1 \vee x_1<x_0 \ \ldots \ \mathfrak{A}_n \vee x_{n+1}<x_n}{\mathfrak{A}_1 \vee \ldots \vee \mathfrak{A}_n}. \qquad (11)$$

Единственной финальной формулой является $\square$. Теорема о полноте метода гиперрезолюций вновь гарантирует нам, что мы действительно имеем дело с формализацией рассматриваемого нами свойства "быть n-нераскрашиваемым графом".

Вторая форма метода гиперрезолюций дает такую дедуктивную систему. Формулами являются всевозможные дизъюнкции элементарных формул вида $x \geqslant y$, аксиомы - это формулы вида (9), правила вывода таковы:

$$\frac{\mathfrak{A} \vee x \geqslant y \quad \mathfrak{B} \vee y \geqslant z}{\mathfrak{A} \vee \mathfrak{B} \vee x \geqslant z}, \tag{I2}$$

$$(\exists x y \Rightarrow) \qquad \frac{\mathfrak{A} \vee x \geqslant y \quad \mathfrak{B} \vee y \geqslant x}{\mathfrak{A} \vee \mathfrak{B}}. \tag{I3}$$

Единственной финальной формулой также является $\square$.

3.3. В качестве второго примера мы рассмотрим одно свойство графов, возникшее в работе Л.М.Витавера [6], а именно, свойство "быть графом, у которого при любой ориентации ребер возникает ориентированный маршрут длины не менее n". Мы будем задавать ориентацию посредством антисимметричного двуместного предиката $\prec$, который определен на парах вершин, соединенным ребром и указывает, в каком порядке идут вершины. Антисимметричность предиката $\prec$ соответствует истинности всех формул вида

$$(\exists x y \Rightarrow) \qquad x \prec y \ \vee \ y \prec x, \tag{I4}$$

$$(\exists x y \Rightarrow) \qquad x \succcurlyeq y \ \vee \ y \succcurlyeq x, \tag{I5}$$

где $x \succcurlyeq$ обозначает $\neg(x \prec y)$. Отсутствие ориентированных маршрутов длины не менее, чем n - это истинность всех формул вида

$$(\mathop{\&}_{i=1}^{n} \exists x_i x_{i+1} \Rightarrow) \ x_1 \succcurlyeq x_2 \vee x_2 \succcurlyeq x_3 \vee \ldots \vee x_n \succcurlyeq x_{n+1} \tag{I6}$$

По техническим причинам нам удобнее доопределить предикат $\prec$ на все пары вершин, считая его ложным на парах вершин, не соединенных ребром. Тогда истинными будут все формулы вида

$$x_1 \succcurlyeq x_2 \vee x_2 \succcurlyeq x_3 \vee \ldots \vee x_n \succcurlyeq x_{n+1} \tag{I7}$$

(и, тем более, все формулы вида (I5), являющиеся частным случаем уже формул (I5)).

Вторая форма метода гиперрезолюций дает следующую дедуктивную систему: формулами являются всевозможные дизъюнкции элементарных формул вида $x \succcurlyeq y$, аксиомами - формулы вида (16), единственное правило вывода имеет вид

$$(\mathcal{I}xy \Rightarrow) \qquad \frac{\mathfrak{A} \vee x \succcurlyeq y \quad \mathfrak{B} \vee y \succcurlyeq x}{\mathfrak{A} \vee \mathfrak{B}}, \qquad (17)$$

единственной финальной формулой является $\square$.

3.4. В качестве третьего примера мы рассмотрим одно свойство графов, возникающее при изучении гипотезы о четырех красках. Напомним, что граф называется гамильтоновым, если он содержит замкнутый несамопересекающийся маршрут, проходящий через все вершины. Ради единообразия формулировок будем считать гамильтоновыми также полные графы с одной и двумя вершинами.

Из теоремы Уитни [7] (см. также [8]) следует, что для доказательства гипотезы о четырех красках достаточно показать, что можно раскрасить в четыре цвета все вершины произвольного плоского гамильтонова графа.

Будем называть плоский гамильтонов граф *многоугольным* (название подсказано естественным способом изображения таких графов на плоскости). Будем называть граф *почти многоугольным*, если к нему можно добавить, при необходимости, новые ребра так, чтобы получившийся граф стал многоугольным. Наконец, будем называть граф *антимногоугольным*, если ни он сам и ни один из графов (без петель!), получающихся из него склеиванием вершин (и соответствующим отождествлением ребер) не является почти многоугольным.

Гипотезу о четырех красках можно сформулировать в этих терминах следующим образом: каждый 4-нераскрашиваемый граф является антимногоугольным. Действительно, если бы это было не так, то нашелся бы 4-нераскрашиваемый граф, который после отождествления некоторых вершин (необязательного) и добавления некоторых ребер (также необязательного) становился бы плоским и, очевидно, по-прежнему 4-нераскрашиваемым. Кроме того, легко видеть, что никакой 4-раскрашиваемый граф не может быть антимногоугольным, ибо в нем можно склеить вершины, окрашенные в один цвет, а получившийся граф, имеющий не более четырех вершин, будет, очевидно, почти многоугольным.

Таким образом, гипотезу о четырех красках можно оформулировать так:

свойство "быть 4-нераскрашиваемым графом" эквивалентно свойству "быть антимногоугольным графом".

Ниже мы воспользуемся тем обстоятельством, что нам удалось сформулировать гипотезу о четырех красках в виде эквивалентности, а не в виде импликации, как обычно. Первое из свойств было формализовано выше, к формализации второго мы переходим.

Рассмотрим сначала произвольный плоский гамильтонов граф $\langle V, \mathfrak{I} \rangle$. Зафиксируем некоторый гамильтонов цикл. Выберем какую-либо вершину в качестве начальной и занумеруем все вершины в том порядке, в котором они встречаются при обходе цикла в одну из сторон. Этот порядок вершин описывается некоторым двуместным иррефлексивным антисимметричным транзитивным предикатом $\prec$:

$$x \succcurlyeq x, \tag{18}$$

$$(x \neq y \Rightarrow) \quad x \prec y \vee y \prec x, \tag{19}$$

$$x \succcurlyeq y \vee y \succcurlyeq x, \tag{20}$$

$$x \prec y \vee y \prec z \vee x \succcurlyeq z, \tag{21}$$

$x \succcurlyeq y$ обозначает $\neg(x \prec y)$.

Гамильтонов цикл делит все ребра, не лежащие на нем, на лежащие "внутри" и "вне". Ребра, лежащие на самом цикле, мы разделим на "внутренние" и "внешние" произвольным образом. Чтобы формализовать это деление, мы не будем вводить переменных для ребер, а воспользуемся тем, что мы рассматриваем лишь графы без кратных ребер и, таким образом, у нас каждое ребро однозначно определяется парой вершин. Будем обозначать через $\mathcal{G}uvxy$ предикат "ребро, соединяющее вершины u и v , лежит по ту же сторону от цикла, что и ребро, соединяющее вершины x и y ". Предикат $\mathcal{G}$ определен на четверках вершин $\langle u, v, x, y \rangle$ таких, что $\mathfrak{I}uv \,\&\, \mathfrak{I}xy$.

Из определения видно, что

$$\begin{aligned} \mathcal{G}uvxy &\Leftrightarrow \mathcal{G}vuxy \\ &\Leftrightarrow \mathcal{G}uvyx \\ &\Leftrightarrow \mathcal{G}xyuv. \end{aligned} \tag{22}$$

Аналогично тому, как это было сделано выше с предикатом $\mathcal{E}$, мы не будем переписывать это свойство предиката $\mathcal{G}$ в виде системы дизъюнкций, а просто будем не различать элементарные формулы, входящие в (22).

Предикат $\mathcal{G}$ транзитивен в следующем смысле:

$$\neg\mathcal{G}pquv \vee \neg\mathcal{G}uvxy \vee \mathcal{G}pqxy. \tag{23}$$

Кроме того, из любых трех ребер какие-то два лежат по одну сторону от цикла:

$$\varphi pquv \vee \varphi uvxy \vee \varphi pqxy. \qquad (24)$$

Предикат φ "согласован" с предикатом $\prec$ условием, что ребра не пересекаются:

$$(\mathcal{J}uv \,\&\, \mathcal{J}xy \Rightarrow) \qquad u \succcurlyeq x \vee x \succcurlyeq v \vee v \succcurlyeq y \vee \neg \varphi uvxy. \qquad (25)$$

Нетрудно проверить, что если на произвольном графе $\langle V, \mathcal{J} \rangle$ удалось определить предикаты $\succ$ и φ так, что условия (18)-(21), (23)-(25) оказались выполнены, то этот граф является почти многоугольным. Таким образом, граф $\langle V, \mathcal{J} \rangle$ не является почти многоугольным в том и только том случае, когда система (18)-(21),(23)-(25) противоречива. Осталось заметить, что граф $\langle V, \mathcal{J} \rangle$ является антимногоугольным в том и только том случае, когда противоречивой оказывается уже система получающаяся из системы (18)-(21) (23)-(25) заменой условия (19) на более слабое условие

$$(\mathcal{J}xy \Rightarrow) \qquad x \prec y \vee y \prec x. \qquad (26)$$

Дальнейшее построение дедуктивной системы проводится аналогично тому, как было сделано раньше. Формулами объявляются все - возможные дизъюнкции формул вида $x \prec y$ и $\varphi pquv$ (при условии $\mathcal{J}pq \,\&\, \mathcal{J}uv$, аксиомами - формулы вида (24) и (26), правила вывода имеют вид

$$\frac{\mathfrak{A} \vee x \prec x}{\mathfrak{A}}, \qquad (27)$$

$$\frac{\mathfrak{A} \vee x \prec z}{\mathfrak{A} \vee x \prec y \vee y \prec z}, \qquad (28)$$

$$(\mathcal{J}pq \,\&\, \mathcal{J}uv \,\&\, \mathcal{J}xy \Rightarrow) \frac{\mathfrak{A} \vee \varphi pquv \qquad \mathfrak{B} \vee \varphi uvxy}{\mathfrak{A} \vee \mathfrak{B} \vee \varphi pqxy} \qquad (29)$$

$$(\mathcal{J}pq \,\&\, \mathcal{J}xy \Rightarrow) \frac{\mathfrak{A} \vee u \prec x \quad \mathfrak{B} \vee x \prec v \quad \mathfrak{L} \vee v \prec y \quad \mathfrak{D} \vee \varphi uvxy}{\mathfrak{A} \vee \mathfrak{B} \vee \mathfrak{L} \vee \mathfrak{D}}, \qquad (30)$$

единственной финальной формулой является формула $\square$.

4. Переходим к описанию возможных схем доказательств с помощью метаматематического подхода. Мы ограничимся рассмотрением од-

ной типичной формы теорем, а именно, будем рассматривать теоремы вида $\forall X\,(\mathcal{R}(X) \Rightarrow Q(X))$.

4.I. Одной из наиболее употребительных схем доказательств в дискретной математике является доказательство по индукции. Метод математической индукции можно, грубо говоря, охарактеризовать так мы сводим доказательство интересующего нас свойства некоторого объекта к доказательству того же свойства для одного или нескольких более простых объектов(некоторая мера сложности объектов используется в качестве индукционного параметра), а для простейших объектов даем прямое доказательство (база индукции).

Часто оказывается, что используемая мера сложности никак не связана ни со свойством $\mathcal{R}$, ни со свойством Q, и возможности выбора "естественных" индукционных параметров обычно ограничены. Метаматематический подход дает много возможностей выбирать индукционные параметры, тесно связанные со свойством $\mathcal{R}$. Действительно, если нам удалось формализовать свойство $\mathcal{R}$ в некоторой дедуктивной системе $\mathcal{R}$, то в качестве меры сложности объекта X мы можем брать любую меру сложности доказательства $\mathcal{P}_{\mathcal{R}}(X)$. Перечислим некоторые потенциально возможные индукционные параметры:

а) число ветвей в $\mathcal{P}_{\mathcal{R}}(X)$;

б) длина самой длинной ветви;

в) общее число применений правил вывод:

г) число применений того или иного фиксированного правила или правил из фиксированной группы без учета числа применений других правил; более общо,

д) взвешенное число применений (разным правилам присваивается разный вес);

е) число вхождений (использований) той или иной аксиомы;

ж) число вхождений той или иной аксиомы, стоящих выше применений определенного правила.

По существу, именно по этой схеме проведено (в несколько тных терминах) доказательство части теоремы Кенига в [I]. Свойством $\mathcal{R}$ там является свойство "быть 2-нераскрашиваемым графом", а свойством Q является свойство "содержать цикл нечетной длины". В качестве формализации свойства $\mathcal{R}$ взята первая из рассмотренных нами формализаций, но рассматриваются только выводы, в которых никакое применение правила ($4''$) не стоит выше по ветви какого-либо применения правила ($4'$) (легко показать, что всякий вывод можно перестроить в вывод с таким свойством). В качестве индукционного параметра использовалось число применений правила ($4'$).

По описанной выше схеме "спуск" от более сложных объектов к более простым проходит, примерно, следующим образом:

по объекту X, обладающему свойством $\mathcal{R}$, находим доказательство $\mathcal{P}_{\mathcal{R}}(X)$;

по доказательству $\mathcal{P}_{\mathcal{R}}(X)$ находим более простое формальное доказательство $\mathcal{P}^*_{\mathcal{R}}$;

доказательство $\mathcal{P}^*_{\mathcal{R}}$ должно являться доказательством свойства $\mathcal{R}$ для некоторого объекта Y, то есть должно быть доказательством вида $\mathcal{P}_{\mathcal{R}}(Y)$;

применяя индукционное предположение получаем,что объект Y обладает свойством Q;

доказываем импликацию $Q(Y) \Rightarrow Q(X)$. При этом доказательство $\mathcal{P}^*_{\mathcal{R}}$ тесно связано с исходным доказательством $\mathcal{P}_{\mathcal{R}}(X)$, оно обычно получается из $\mathcal{P}_{\mathcal{R}}(X)$ путем неких упрощающих перестроек. В результате самым трудным шагом в доказательстве может оказаться нахождение того объекта Y, для которого упрощенное доказательство $\mathcal{P}^*_{\mathcal{R}}$ являлось бы доказательством свойства $\mathcal{R}$. (Если мы захотим поступить наоборот, то есть сначала выбрать объект Y, обладающий свойством $\mathcal{R}$, а затем построить для него какое-то доказательство $\mathcal{P}_{\mathcal{R}}(Y)$, то перед нами встанут еще большие трудности при сравнении сложности доказательств $\mathcal{P}_{\mathcal{R}}(X)$ и $\mathcal{P}_{\mathcal{R}}(Y)$.) Описанная выше схема имеет, по-видимому, довольно ограниченную область применимости.

4.2. Более широкую область применения имеет,вероятно, следующая схема, также использующая индукцию по выводу $\mathcal{P}_{\mathcal{R}}(X)$. Предположим, что нам удалось обобщить свойство $\mathcal{R}$ до свойств $\mathcal{R}_F$ (здесь F - произвольная формула из формализации свойства)таким способом, что

(а) если F - аксиома, то $Q_F(X)$;

(б) если $F_1, \ldots, F_{n-1}, F_n$ - формулы, удовлетворяющие одному из правил вывода, то из $Q_{F_1}(X) \& \ldots \& Q_{F_{n-1}}(X)$ следует $Q_{F_n}(X)$;

(в) если F - финальная формула, то из $Q_F(X)$ следует $Q(X)$. Ясно, что в этом случае мы обосновали импликацию $\mathcal{R}(X) \Rightarrow Q(X)$. Формально индукция проводится по сложности вывода формулы F в $\mathcal{R}$ (которую можно определить, например, как число формул в самой длинной ветви, или как общее число применений правил вывода), причем индукцией по этому параметру доказывается следующее вспомогательное утверждение: "если формула F выводима в $\mathcal{R}$, то X обладает свойством Q_F". При этом пункт (а) соответствует базе индукции, пункт (б) - индукционному переходу, а пункт (в) обеспечивает переход от вспомогательного утверждения к импликации $\mathcal{R}(X) \Rightarrow Q(X)$.

Эта схема доказательства реализована в [2] на примере части теоремы Витавера. Эта теорема утверждает, что граф не имеет раскраски вершин в n цветов тогда и только тогда, когда при каждой ориантации его ребер возникает ориентированный маршрут длины не менее n. В [2]в качестве свойства $\mathcal{R}$ взято свойство "быть n-нераскрашиваемым графом", формализация основана также не системе формул вида (1) – (3), но в качестве правила вывода взято более простое правило резолюции (см.[4]). Свойство $\mathcal{Q}_F$ отличается от свойства $\mathcal{Q}$, грубо говоря, тем, что формула F "разрешает" некоторые разрывы в требуемом ориентированном маршруте, и некоторые из этих разрывов учитываются при вычислении длины такого разрывного маршрута. При этом свойстве $\mathcal{Q}_\Box$ совпадает со свойством $\mathcal{Q}$.

4.3. До сих пор мы рассматривали, что дает формализация свойства $\mathcal{R}$. Допустим теперь, что и свойство $\mathcal{Q}$ формализовано в некоторой дедуктивной системе $\mathcal{G}$. В такой ситуации мы можем следующим образом детализировать предыдущую схему. Пусть каждой формуле F из формализации свойства $\mathcal{R}$ поставлено в соответствие некоторое множество $\mathcal{N}_F$ формул из формализации свойства $\mathcal{Q}$, причем для каждой финальной формулы F множество $\mathcal{N}_F$ также содержит финальную формулу. Мы можем пытаться реализовать описанную выше схему, взяв в качестве $\mathcal{Q}_F$ свойство "все формулы из $\mathcal{N}_F$ выводимы в $\mathcal{G}(X)$". Свойство (в) будет выполнено благодаря выбору множеств $\mathcal{N}_F$, а свойства (а) и (б) будут доказаны, если удастся найти соответствующие "вставки".("Вставка" – непосредственно вывод в $\mathcal{G}$ формул $\mathcal{N}_F$, если F есть аксиома, и вывод формул, входящих в $\mathcal{N}_{F_n}$, из формул, входящих в $\mathcal{N}_{F_1} \cup \ldots \cup \mathcal{N}_{F_{n-1}}$, при условии, что F_n выводима из $F_1, \ldots, F_{n-1}$ в $\mathcal{R}$.) Таким образом, доказательство свойства $\mathcal{Q}$ будет получено в результате "пошагового моделирования" доказательства $\mathcal{R}$.

Формализация свойства $\mathcal{Q}$ может оказаться полезной также ввиду так называемого "парадокса изобретателя". Он состоит в следующем. Пусть мы хотим доказать некоторое свойство $\mathcal{A}(n)$ (для простоты n – натуральное число). Может оказаться, (см. например,[9]), что это нельзя сделать непосредственно, так как индукционный переход $\mathcal{A}(n) \Longrightarrow \mathcal{A}(n+1)$ недоказуем без индукции. В то же время может найтись свойство $\mathcal{B}(n)$, более сильное, чем $\mathcal{A}(n)$, причем импликация $\mathcal{B}(n) \Longrightarrow \mathcal{A}(n)$, база индукции $\mathcal{B}(0)$ и индукционный переход $\mathcal{B}(n) \Longrightarrow \mathcal{B}(n+1)$ доказуемы без индукции. Таким образом, чтобы доказать свойство $\mathcal{A}$, надо сперва "изобрести" более сильное свойство $\mathcal{B}$.

Иллюстрацией "парадокса изобретателя" может служить формула

$$\frac{1 \cdot 3 \cdot 5 \ldots (2n-1)}{2 \cdot 4 \cdot 6 \ldots (2n)} < \frac{1}{\sqrt{n}} . \qquad (31)$$

Прямая попытка доказать это неравенство индукцией проваливается, так как неравенство

$$\frac{1}{\sqrt{n}} \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{n+1}} \qquad (32)$$

неверно. В то же время более сильное неравенство

$$\frac{1\cdot 3\cdot 5\ldots(2n-1)}{2\cdot 4\cdot 6\ldots(2n)} < \frac{1}{\sqrt{n+1}} \qquad (33)$$

легко доказывается по индукции, ибо

$$\frac{1}{\sqrt{n+1}} \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{n+2}}. \qquad (34)$$

На выбор свойства $\mathcal{B}$ накладывается два противоречащих друг другу требования. С одной стороны, оно должно быть сильнее свойства $\mathcal{A}$, но, с другой стороны, оно не должно быть слишком сильным, иначе не все объекты будут им обладать.

В такой ситуации может оказаться полезным искать усиление свойства в терминах ограничений на выводы (имеются в виду сильные ограничения, нарушающие, в общем случае, полноту системы). Усиленное свойство $\mathcal{Q}^{\sim}$ может состоять в том, что имеется вывод одной из финальных формул, удовлетворяющий дополнительным требованиям, например, такого вида:

а) нигде в выводе выше применения данного правила не встречается такая-то аксиома или такое-то правило вывода;

б) одна из посылок данного правила всегда является аксиомой (такого-то типа):

в) ниже каждого применения данного правила обязательно есть применение такого-то правила.

Усиления такого типа могут оказаться как раз "золотой серединой" - не слишком сильными, так что импликация $\mathcal{R}(X) \Longrightarrow \mathcal{Q}^{\sim}(X)$ будет верна, и достаточно сильными, чтобы индукционный переход был доказуем непосредственно. Понятно, что использовать такие усиления естественней всего, когда индукция идет по какому-либо метаматематическому параметру. Например, можно сочетать эти усиления с предыдущей схемой, беря в качестве $\mathcal{Q}^{\sim}_F$ такое свойство: "Каждая формула из $\mathcal{N}_F$ имеет вывод, удовлетворяющий таким-то и таким-то дополнительным требованиям". Здесь парадокс изобретателя может проявиться следующим образом: перестройка произвольных выводов формул из $\mathcal{N}_{F_1}, \ldots, \mathcal{N}_{F_{n-1}}$ в какие-то выводы формул из $\mathcal{N}_{F_n}$ будет невозможна, а перестройка выводов (тех же формул), удовлетворяющих некоторым дополнительным требованиям в удовлетворяющие тем же требованиям выводы формул из $\mathcal{N}_{F_n}$ будет осуществима.

4.4. До сих пор мы рассматривали раздельно формализации свойств $\mathcal{R}$ и $\mathcal{Q}$. Теперь мы рассмотрим, что может дать изучение "совместных формализаций".

Мы говорим, что свойства $\mathcal{R}$ и Q формализованы совместно, если каждому объекту X из (общей) области определения $\mathcal{R}$ и Q поставлена в соответствие некоторая дедуктивная система $\langle \mathcal{F}, \mathcal{A}, \mathcal{D}, \mathcal{H} \rangle$, оснащенная следующей дополнительной информацией. В множествах $\mathcal{A}$, $\mathcal{D}$, $\mathcal{H}$ указаны такие подмножества $\mathcal{A}_{\mathcal{R}}$ и $\mathcal{A}_Q$, $\mathcal{D}_{\mathcal{R}}$ и $\mathcal{D}_Q$, $\mathcal{H}_{\mathcal{R}}$ и $\mathcal{H}_Q$ соответственно, что X обладает свойством $\mathcal{R}$ (свойством Q) в том и только том случае, когда одна из формул из $\mathcal{H}_{\mathcal{R}}$ (соответственно, из $\mathcal{H}_Q$) выводима из $\mathcal{A}_{\mathcal{R}}$ (соответственно, из $\mathcal{A}_Q$) посредством лишь правил из $\mathcal{D}_{\mathcal{R}}$ (соответственно, $\mathcal{D}_Q$).

Имея совместную формализацию свойств $\mathcal{R}$ и Q мы можем пытаться доказывать импликацию $\mathcal{R}(X) \Longrightarrow Q(X)$ посредством многошаговой перестройки вывода, соответствующего свойству $\mathcal{R}$, в вывод, соответствующий свойству Q.

Мы уделим соновное внимание рассмотрению того частного случая, когда $\mathcal{A}_{\mathcal{R}} \supseteq \mathcal{A}_Q$, $\mathcal{D}_{\mathcal{R}} \supseteq \mathcal{D}_Q$ и $\mathcal{H}_{\mathcal{R}} = \mathcal{H}_Q$. Ясно, что в этом случае справедлива импликация $\mathcal{R}(X) \Longleftarrow Q(X)^{Q}$ и, таким образом, речь идет о доказательстве эквивалентности $\mathcal{R}(X) \Longleftrightarrow Q(X)$. Такая совместная формализация свойств $\mathcal{R}$ и Q часто действительно часто существует и является естественной при условии, что импликация $\mathcal{R}(X) \Longleftarrow Q(X)$ доказуема тривиально.

Допустим сначала, что имеет место не просто включение $\mathcal{A}_{\mathcal{R}} \supseteq \mathcal{A}_Q$, а даже равенство $\mathcal{A}_{\mathcal{R}} = \mathcal{A}_Q$. В этом случае доказательство импликации $\mathcal{R}(X) \Rightarrow Q(X)$ сводится к доказательству допустимости правил из $\mathcal{D}_{\mathcal{R}} \setminus \mathcal{D}_Q$ в $\langle \mathcal{F}, \mathcal{A}_Q, \mathcal{D}_Q, \mathcal{H}_Q \rangle$. При этом надо отметить следующее.

При принятом нами понятии дедуктивной системы мы интересуемся лишь выводами некоторых формул, а именно, финальных. Для таких систем допустимыми, естественно, называют те правила, применения которых могут быть устранены из любого вывода, оканчивающейся финальной формулой(обычно допустимыми в некоторой системе называют те правила, применения которых могут быть устранены из любого вывода). Ясно также, что нас интересует совместная допустимость правил, поскольку из допустимости в некоторой системе каждого из какой-то группы правил не обязательно следует, что все применения правил этой группы могут быть устранены из вывода, в котором они встречаются одновременно.

Рассмотрим теперь случай, когда имеет место просто включение $\mathcal{A}_{\mathcal{R}} \supseteq \mathcal{A}_Q$, но зато выполнено равенство $\mathcal{D}_{\mathcal{R}} = \mathcal{D}_Q$. В этом случае для доказательства импликации $\mathcal{R}(X) \Longrightarrow Q(X)^{Q}$ достаточно доказать, что любая формула из $\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}_Q$ выводима из $\mathcal{A}_Q$ посредством правил из $\mathcal{D}_Q$. Однако это может оказаться слишком сильным требованием. Поскольку нас интересуют только выводы финальных формул, то достаточно доказать, что аксиомы из $\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}_Q$

могут быть устранены из любого вывода (с аксиомами из $\mathcal{A}_{\mathcal{R}}$)любой финальной формулы, проведенного посредством правил из $\mathcal{D}_{Q}$. В такой ситуации также будем говорить, что эти аксиомы совместно допустимы.

Наконец, рассмотрим общий случай, когда имеют место просто включения $\mathcal{A}_{\mathcal{R}} \supseteq \mathcal{A}_{Q}$ и $\mathcal{D}_{\mathcal{R}} \supseteq \mathcal{D}_{Q}$. Понятно, что в этом случае для доказательства импликации $\mathcal{R}(X) \Rightarrow Q(X)$ достаточно установить совместную допустимость формул из $\mathcal{A}_{\mathcal{R}} \setminus \mathcal{A}_{Q}$ и правил из $\mathcal{D}_{\mathcal{R}} \setminus \mathcal{D}_{Q}$ в системе $\langle \mathcal{F}, \mathcal{A}_{Q}, \mathcal{D}_{Q}, \mathcal{H}_{Q} \rangle$ (это понятие определяется естественным образом).

Приведем пример теоремы, которая могла быть доказана по описанной выше схеме. Сравнение второй формализации свойства "не иметь раскраски вершин не более чем в n цветов" и формализации выше свойства графов, возникшего в работе Витавера, показывает,что если мы отождествим предикаты $<$ и $\prec$ (а теперь мы можем это сделать, ибо после формализации оба предиката стали лишь формальными символами), то формализация первого свойства отличается от формализации второго лишь на одно дополнительное правило

$$\frac{\mathfrak{A} \vee x \succcurlyeq y \quad \mathfrak{B} \vee y \succcurlyeq z}{\mathfrak{A} \vee \mathfrak{B} \vee x \succcurlyeq z} \tag{35}$$

Таким образом, теорема Витавера - это теорема о том, что в дедуктивной системе, имеющей аксиомами формулы вида (16), правило (17)и единственной финальной формулой формулу $\square$, допустимо правило (35).

Доказать допустимость правила (35) можно следующим образом Пусть $\mathcal{P}$ - некоторый вывод, из которого надо устранить применения правила (35). Поскольку правило (17) не содержит в заключении каких-либо элементарных формул, которые не входили бы в посылки, то вывод $\mathcal{P}$ легко может быть перестроен в вывод $\mathcal{P}'$, в котором любое применение правила (17) находится ниже любого применения правила (35). Основной шаг состоит в доказательстве того, что любое применение правила (35) к аксиомам дает формулу, содержащую некоторую аксиому как подформулу. Пусть

$$p_1 \succcurlyeq p_2 \vee \ldots \vee p_n \succcurlyeq p_{n+1}$$

и

$$q_1 \succcurlyeq p_2 \vee \ldots \vee q_n \succcurlyeq q_{n+1}$$

- две аксиомы, к которым применяется правило (31), где $x = p_i$,

$$p_{i+1} = y = q_j, \quad q_{j+1} = z \quad (1 \leqslant i \leqslant n, \ 1 \leqslant j \leqslant n).$$

Мы рассмотрим случай,когда вершины $p_1, \ldots, p_{n+1}$ (и, аналогично, вершины $q_1, \dots, q_{n+1}$) попарно различны. В таком случае заключение применения правила (35) содержит две подформулы

$$p_1 \succcurlyeq p_2 \vee \dots \vee p_{i-1} \succcurlyeq x \vee x \succcurlyeq z \vee z \succcurlyeq q_{j+1} \vee \dots \vee q_n \succcurlyeq q_{n+1} \quad (36)$$

и

$$q_1 \succcurlyeq q_2 \vee \dots \vee q_{j-1} \succcurlyeq y \vee y \succcurlyeq p_{i+1} \vee \dots \vee p_n \succcurlyeq p_{n+1}. \quad (37)$$

Эти формулы содержат вместе $2n-1$ элементарную подформулу, и потому одна из них содержит аксиому вида (16).

Случаи, когда среди вершин $p_1, \dots, p_{n+1}$ или среди вершин $q_1, \dots, q_{n+1}$ есть одинаковые, рассматриваются лишь немногим сложнее (ср. с доказательством из [2]) и мы не будем здесь этого делать.

Так как применение правила (35) к аксиомам дает формулы, содержащие аксиомы, то в выводе $\mathcal{P}'$ можно удалить какое-либо самое верхнее применение правила (35) (если их нет вообще, то $\mathcal{P}'$ уже есть искомый вывод), заменить его заключение на содержащуюся в нем аксиому и затем "прополоть" вывод. Получившийся вывод содержит меньше применений правила (35), и все они расположены выше любого применения правила (17). Повторив описанный выше процесс достаточное число раз, мы получим в конце концов искомый вывод, вовсе не содержащий применений правила (35).

Покажем теперь, что известная гипотеза о четырех красках может быть сформулирована как утверждение о допустимости одного правила в некоторой дедуктивной системе.

Выше мы показали, что гипотеза о четырех красных эквивалентна импликации $\mathcal{R}(X) \Rightarrow Q(X)$, где $\mathcal{R}$ - свойство "быть нераскрашиваемым в четыре цвета", а Q - свойство "быть антимногоугольным".

В качестве формализации свойства $\mathcal{R}$ мы возьмем первую формализацию п.3.2I. В нашем случае $n = 4$ и правила (II) выглядят так:

$$\frac{\mathfrak{A}_1 \vee x_1 < x_0 \qquad \mathfrak{A}_2 \vee x_2 < x_1 \quad \mathfrak{A}_3 \vee x_3 < x_2 \quad \mathfrak{A}_4 \vee x_4 < x_3}{\mathfrak{A}_1 \vee \mathfrak{A}_2 \vee \mathfrak{A}_3 \vee \mathfrak{A}_4}. \quad (38)$$

Свойство Q было формализовано в п.3.4.

Сравнивая эти формализации свойств $\mathcal{R}$ и Q видим, что все аксиомы и правила вывода в формализации $\mathcal{R}$, за исключением правил (II), имеют своих аналогов в формализации Q (мы отождествляем теперь $<$ и $\prec$). В то же время аксиомы (24) и правила (29),(30) из формализации Q не имеют аналогов в формализации $\mathcal{R}$, так как там нет аналога предикату φ.

Чтобы получить совместную формализацию с $\mathcal{A}_{\mathcal{R}}=\mathcal{A}_{Q}, \mathcal{D}_{\mathcal{R}} \supseteq \mathcal{D}_{Q}$ и $\mathcal{H}_{\mathcal{R}}=\mathcal{H}_{Q}$,мы формально пополним рассматриваемую формализацию свойства $\mathcal{R}$ предикатом $\varphi uvxy$, аксиомами вида (24) и правилами (29) и (30). Нам надо лишь проверить, что расширенная система по-прежнему формализует свойство $\mathcal{R}$, а для этого достаточно убедиться в том, что если граф L имеет правильную 4-раскраску, то можно определить предикат $<(\prec)$ и предикат φ так,что истинными будут все формулы (7),(8),(9),(23,(24) и (26). Покажем, что это действительно имеет место.

Пусть L- граф, имеющий 4-раскраску. Склеим вершины, имеющие одинаковый цвет. Получившийся граф будет, очевидно, частью полного графа с четырьмя вершинами. Будем теперь интерпретировать предикаты $<$ и φ так же, как при формализации свойства Q , тогда все формулы (7), (8),(23),(24) и (26) окажутся истинными, поскольку полный граф с четырьмя вершинами является многоугольным, а формулы вида (9) будут истинными, поскольку у этого графа всего четыре вершины.

Итак, мы показали, что

> гипотеза четырех красок эквивалентна следующей: правило (38) допустимо в дедуктивной системе, имеющей аксиомами формулы вида (24) и (26), правилами вывода - правила (27) - (30), единственной финальной формулой - формулу $\square$.

Трудность доказательства гипотезы, по-видимому, объясняется тем, что правило (38) является очень мощным, требующим для своего устранения экспоненциального увеличения длины вывода.

Вернемся теперь к общему случаю, то есть откажемся от предположения $\mathcal{A}_{\mathcal{R}} \supseteq \mathcal{A}_{Q}$, $\mathcal{D}_{\mathcal{R}} \supseteq \mathcal{D}_{Q}$, $\mathcal{H}_{\mathcal{R}}=\mathcal{H}_{Q}$. Мы по-прежнему можем пытаться доказывать импликацию $\mathcal{R}(X) \Rightarrow Q(X)$посредством многошаговой перестройки вывода, соответствующего свойству $\mathcal{R}$, в вывод, соответствующий свойству Q . Однако в рассматриваемом общем случае промежуточные выводы будут, вообще говоря, малоосмысленными: они не будут давать ни формализации свойства $\mathcal{R}$, ни формализации свойства Q .

Многошаговая перестройка выводов может проводиться по различным схемам. Например, достаточно доказать следующие три леммы.

а) Если $H \in \mathcal{H}_{\mathcal{R}}$ и H выводима из $\mathcal{A}_{\mathcal{R}}$ посредством правил из $\mathcal{D}_{\mathcal{R}}$, то H выводима из $\mathcal{A}_{Q}$ посредством правил из $\mathcal{D}$.

б) Если $H \in \mathcal{H}_{\mathcal{R}}$, то любой вывод H из $\mathcal{A}_{Q}$ посредством правил из $\mathcal{D}$, содержащий применения правил из $\mathcal{D} \setminus \mathcal{D}_{Q}$, можно перестроить в новый вывод H из $\mathcal{A}_{Q}$ посредством правил $\mathcal{D}$, содержащий меньшее число применений правил из $\mathcal{D} \setminus \mathcal{D}_{Q}$.

в) Если $H \in \mathcal{H}_{\mathcal{R}}$ и H выводима из $\mathcal{A}_{Q}$ посредством правил из $\mathcal{D}_{Q}$, то некоторая формула из $\mathcal{H}_{Q}$ выводима из $\mathcal{A}_{Q}$ посредством правил из $\mathcal{D}_{Q}$.

Литература

1. Матиясевич Ю.В. Применение методов теории логического вывода в теории графов. - Матем. заметки, 1972, т.12, № 6, с.781-790.
2. Матиясевич Ю.В. Одна схема доказательств в дискретной математике. - Зап.научн.семинаров ЛОМИ, 1974, т.40, АН СССР, с.94-100.
3. Maslov S.Yu. Proof-search strategies for methods of the resolution type. - Machine Intelligence, 1971, v.6, Edinburg, p.77-90.
4. Robinson J.A. A machine-oriented logic based on the resolution principle. - J.Assoc.Comput. Mach., 1965, v.12, № 1, p.23-41(русск.пер.:Киберн.сб.,1970, т.7, с.194-218)
5. Robinson J.A. Automatic deduction with hyper-resolution. "Int. J.Comput.Math.", 1965, v.1, p.227-234.
6. Витавер Л.М. Нахождение минимальных раскрасок вершин графа с помощью булевых степеней матрицы смежности. - Докл. АН СССР, 1962, т.147, № 4, с.758-759.
7. Whitney H. A theorem on graphs. - Ann.Math., 1931, v.32, № 2, p.378-390.
8. Tutte W.T. A theorem on planar graphs. - Trans.Amer.Math.Soc., 1956, v.82, № 1, p.99-116 (русск.пер.: Киберн. сб., 1973, т.10, с.66-86).
9. Polya G. Now to solve it. Princeton, 1946 (русск.пер.:Пойа Д. Как решать задачу. М., 1961).

Matijasevic Yu.V. <u>On metamathematical approach to proving theorems of discrete mathematics</u>. I. The first investigations in the framework of the new approach, called metamathematical, were author's papers [1],[2].

1.1. The main distinguishing feature of the approach is as follows: investigating a property $\mathfrak{R}$ of finite discrete objects one gets information about an object X , having the property $\mathfrak{R}$, by analyzing the structure of a formal proof $\mathcal{P}_{\mathfrak{R}}(X)$ of the fact that X does have the property $\mathfrak{R}$. Here $\mathfrak{R}$ is a mitable deductive system.

1.2. Formal proofs should admit on principle elimination from any argument although the result of eliminating may be more tedions than the initial argument.

2.1. A deductive system is quadruple $\langle \mathcal{F}, \mathcal{A}, \mathcal{D}, \mathcal{H} \rangle$ where $\mathcal{F}$ is a set of f o r m u l a s , $\mathcal{A}$ is a set of a x i o m s , $\mathcal{A} \subset \mathcal{F}$, $\mathcal{D}$ is a set of d e d u c t i o n r u l e s ,

$\mathcal{H}$ is a set of f i n a l f o r m u l a s , $\mathcal{H} \subset \mathcal{F}$. The notions of deduction and deducible formula are traditional.

2.2. We say that a property $\mathfrak{R}$ is formalized if a deductive system $\mathfrak{R}(X)$ is specified to every object X from the domain of $\mathfrak{R}$ and X has the property $\mathfrak{R}$ if and only if at least one final formula (i.e. one belonging to $\mathcal{H}(X)$) is deducible in $\mathfrak{R}(X)$.

3. Below we give some examples of deductive systems formalizing some properties of graphs. By a graph we mean a couple $\langle V, \mathfrak{I} \rangle$ where V is a finite set of vertices and $\mathfrak{I}$ is a symmetric binary predicate indicating the pairs of vertices bridged by an edge.

3.I. The first property considrred is "to have no proper vertex coloration in n colors". The first two deductive systems are formulated in terms of relation $\mathcal{E}xy$ meaning "vertices x and y have the same color". The logical background for all formalizations considered is a variant of classical propositional calculus based on hyperresolution principle [5].

The first formalization: the formulas are arbitrary disjunctions of elementary formulas of the form $\mathcal{E}xy$; the axioms are formulas (3); (4′) and (4″) are the rules of deduction; the only final formula is the empty disjunction $\Box$. Symbolically, the first formalization is $\langle \mathcal{E}xy$ (3); (4′), (4″); $\Box \rangle$ and the second one is $\langle \neg \mathcal{E}xy$; (2); (5′), (5″); $\Box \rangle$.

3.2. Two other formalizations of the same property are given in terms of the relation $x < y$ meaning "the color of x is less than the color of y" (here it is supposed that colors are numbered by integers $1, \ldots, n$) . The first formalization is $\langle x < y$; (8); (IO), (II); $\Box \rangle$, the second one is $\langle x \geqslant y$; (9);(I2), (I3); $\Box \rangle$.

3.3. The second property considered is "to contain an oriented route of length n for each orientation of the edges". $x \prec y$ means that the edge bridging x and y is directed from y to x ; $x \succcurlyeq y$ means $\neg(x \prec y)$. The formalization is $\langle x \succcurlyeq y$;(I6); (I7); $\Box \rangle$.

3.4. The third property considered is "to be antipolygonal graph". (A graph is antipolygonal if it cannot be transformed into Hamiltonian planar loopless graph by adding new edges and identifying some vertices). The formalization is $\langle x \prec y$, $\mathcal{G}uvx$; (24), (26); (27)-(30); $\Box \rangle$ wehere $\prec$ and $\mathcal{G}$ are some predicates connected in a natural way with the Hamiltonian structure of a planar graph.

4. Below we will deal only with theorems of the form
$\mathfrak{R}(X) \Rightarrow Q(X)$

4.I. It is possible to use some parameters of a formal proof

$\mathcal{P}_{\mathfrak{R}}(X)$ as the induction parameters closely conncected with the theorem to be proved; an example is given in [I].

4.2. The theorem is proved if one is able to specify properties $Q_F(X)$ where $F \in \mathcal{F}(X)$ such that

(a) if $F \in \mathcal{A}(X)$ then $Q_F(X)$;

(b) if F_n is directly deducible from $F_1, \dots, F_{n-1}$ in $\mathcal{R}(X)$ then $Q_{F_1}(X) \& \dots \& Q_{F_{n-1}}(X)$ implies $Q_{F_n}(X)$;

(c) if $F \in \mathcal{H}(X)$ then $Q_E(X)$ implies $Q(X)$.

An example is given in [2].

4.3. If $\mathfrak{Q}$ is a formalization of Q then Q_F may be taken to be the property "all formulas from $\mathfrak{M}_F$ are deducible in $\mathfrak{Q}(X)$ " where $\mathfrak{M}_F$ is a sutable set of formulas from $\mathfrak{Q}(X)$.

may also be found to be of value due to the so-called "inventor's paradox" (example: (3I) cannot be proved directly by induction because (32) is not valid while stronger inequality (33) can be easily proved since (34) is valid). Thus it may be easier to prove stronger theorem $\mathfrak{R}(X) \Rightarrow Q^{\sim}(X)$ where $Q^{\sim}(X)$ means "there is a deduction in $\mathfrak{Q}(X)$ of a final formula which satisfies certain additional restrictions."

4.4. A joint formalization of two properties $\mathfrak{R}$ and Q is a quadruple $\langle \mathcal{F}, \mathcal{A}, \mathcal{D}, \mathcal{H} \rangle$ in which subsets $\mathcal{A}_{\mathfrak{R}}, \mathcal{A}_Q, \mathcal{D}_{\mathfrak{R}}, \mathcal{D}_Q, \mathcal{H}_{\mathfrak{R}}, \mathcal{H}_Q$ are specified such that $\langle \mathcal{F}, \mathcal{A}_{\mathfrak{R}}, \mathcal{D}_{\mathfrak{R}}, \mathcal{H}_{\mathfrak{R}} \rangle$ and $\langle \mathcal{F}, \mathcal{A}_Q, \mathcal{D}_Q, \mathcal{H}_Q \rangle$ are formalizations of $\mathfrak{R}$ and Q respectively. The most interesting situation arrises when $\mathcal{A}_{\mathfrak{R}} \supseteq \mathcal{A}_Q$, $\mathcal{D}_{\mathfrak{R}} \supseteq \mathcal{D}_Q$, $\mathcal{H}_{\mathfrak{R}} = \mathcal{H}_Q$. (It is often the case when the inverse implication $\mathfrak{R}(X) \Leftarrow Q(X)$ is trivial). In such a situation to prove $\mathfrak{R}(X) \Rightarrow Q(X)$ it suffies to show that axioms from $\mathcal{A}_{\mathfrak{R}} \setminus \mathcal{A}_Q$ and rules from $\mathcal{D}_{\mathfrak{R}} \setminus \mathcal{D}_Q$ are admissible in $\langle \mathcal{F}, \mathcal{A}_Q, \mathcal{D}_Q, \mathcal{H}_Q \rangle$.

On can state a theorem from [6] in the form "the rule (35) is admissible in $\langle x \succcurlyeq y$; (I6); (I7); $\square \rangle$; a proof of admissibility is outlines.

Witney's theorem enables (cf.[7] or [8]) one to restate the famous four-color conjecture in the form "the rule (38) is admissible in $\langle x < y$; (24), (26), (27)-(30); $\square \rangle$ " (here we identify symbols $<$ and $\prec$). It is very plausible that the difficulty in proving the conjecture is caused by the fact that the rule (38) is very powerful, its elimination (if it is possible, i.e. if the conjecture is true) requiring exponential growth in the length of the deduction.