Proof Procedures as Bases for Metamathematical Proofs in Discrete Mathematics

Yuri Matiyasevich
Steklov Institute of Mathematics at Saint-Petersburg
27 Fontanka, Saint-Petersburg, 191011, Russia
URL: `http://logic.pdmi.ras.ru/~yumat`

This is an extended abstract of two talks given during the working meeting of INTAS-RFBR project 95-0095 on October 22-26, 1997

We shall consider a rather standard form of a theorem about some kind of finite combinatorial objects, say, graphs,

$$\mathcal{P}(X) \Longrightarrow \mathcal{Q}(X) \tag{1}$$

where $\mathcal{P}$ and $\mathcal{Q}$ are two properties. Typically, such a theorem is proved by induction on X. The idea of an induction is to deduce $\mathcal{Q}(X)$ from $\mathcal{Q}(Y)$ (and, maybe, also from $\mathcal{Q}(Y')$, $\mathcal{Q}(Y'')$, ...) where the Y's are in some sense simpler than X. To be able to use induction, we need first to introduce some well-ordering on the set of X having property $\mathcal{P}$. The choice of such orderings is usually rather limited and seldom depends on the property $\mathcal{P}$.

Having a suitable *formal system* for establishing the property $\mathcal{P}$, we can bring to consideration another finite combinatorial object, namely, *formalized proof* $P(X)$ of the fact that X does have the property $\mathcal{P}$. Now we can order the X's according to any complexity measure of the proof $P(X)$. It could be, for example,

- the total number of applications of rules of deduction, possibly with some weights assigned to the rules;
- the number of branches in the deduction tree;

- the length of the longest branch in the deduction.

What is important is that we need not consider arbitrary proofs but can restrict ourself to proofs obtained according to some suitable search strategy.

An example of such induction based on complexity of formalized proofs is given below as Example 1.

There is another potential usage of formalized proof $P(X)$ for induction. Namely, instead of proving the property Q itself, we could try to generalize it to a relation $Q^*(X, F)$ between our object X and a logical formula F which could occur in the proof $P(X)$. We need the following relationship between Q and Q^*:

(1^*) $Q^*(X, A)$ should be true for every axiom A;

(2^*) for every deduction rule $A_1, \ldots, A_n \Longrightarrow B$, the validity of $Q^*(X, A_1)$, $\ldots$, $Q^*(X, A_n)$ should imply the validity of $Q^*(X, B)$;

(3^*) $Q(X)$ should follow from $Q^*(X, F)$ for every formula F, deduction of which implies the property $P(X)$.

As soon as we succeeded in finding such a relation Q^*, we obtain a proof of our theorem (1), virtually by induction along the formalized proof $P(X)$. Again a choice of suitable search strategy can be crucial for the existence of a relation Q^* with the above described properties. An example of such a proof is given below as Example 2.

The next step is to consider what we could gain if both properties $\mathcal{P}$ and $\mathcal{Q}$ were formalized. In such a case, in order to prove a theorem (1) we need to transform a formal proof $P(X)$ into a formal proof $Q(X)$, and numerous techniques developed for automatic theorem proving could be of help here.

The success in transforming $P(X)$ into $Q(X)$ depends on how different are the formal systems used for formalizing $\mathcal{P}$ and $\mathcal{Q}$. An interesting fact was discovered by analysis of theorems in graph theory: for some theorems properties $\mathcal{P}$ and $\mathcal{Q}$ can be formalized in such a way that corresponding formal system for $\mathcal{Q}$ is a proper part of the system for $\mathcal{P}$. That means that in order to prove theorem (1), we need to show that some axioms and deduction rules in the formalization of $\mathcal{P}$ are redundant and can be eliminated from any proof $P(X)$.

Such an elimination could, of course, results in considerable growth of the size of the proof. On the other hand, we need not eliminate all the redundant axioms and deduction rules at once, this could be done in several stages, one axiom/rule being eliminated each time.

In its turn, elimination of a particular axiom/rule could be done by induction, say, on the number of occurences of this axiom/rule in the proof. This is a natural measure of the partial progress on the way from $P(X)$ to $Q(X)$. Such a gradual progress cannot be described in terms of $\mathcal{P}$ and $\mathcal{Q}$, only the elimination of the last redundant axiom/rule corresponds to passing from $\mathcal{P}$ to $\mathcal{Q}$.

An example of a such a metamathematical proof based on a transformation of $P(x)$ into $Q(X)$ can be found in [3]. Below (in Example 3) we present a non-evident formalizations of some properties $\mathcal{P}$ and $\mathcal{Q}$ for which (1) is equivalent to the Four Colour Theorem and for which the set of axioms for $Q(X)$ is a proper subset of axioms for $P(X)$.

Example 1.

König's theorem states that *if a graph G has no colorings of vertices in two colours* (property $\mathcal{P}$) *then it contains a circle of odd length* (property $\mathcal{Q}$).

Let $\mathcal{S}(i,j)$ mean that *the vertices i and j are coloured in the same colour*. This relation is transitive, i.e. for all i, j, and k

$$\neg\mathcal{S}(i,j) \vee \neg\mathcal{S}(j,k) \vee \mathcal{S}(i,k). \tag{2}$$

We will not write down the symmetry of $\mathcal{S}$ by corresponding formulas. Instead of this we shall not distinguish $\mathcal{S}(i,j)$ and $\mathcal{S}(j,i)$.

Since there are only two colours, for all i, j, and k

$$\mathcal{S}(i,j) \vee \mathcal{S}(j,k) \vee \mathcal{S}(i,k). \tag{3}$$

As soon as i and k are connected by an edge, they are coloured differently:

$$\neg\mathcal{S}(i,k). \tag{4}$$

Now the property P is equivalent to the statement that the system of axioms (2)–(4) is contradictory. For a formal proof $P(G)$ we take a deduction of the false empty disjunction $\square$ from axioms (3) by hyperresolution rules

$$\frac{A \vee \mathcal{S}(i,j) \qquad B \vee \mathcal{S}(j,k)}{A \vee B \vee \mathcal{S}(i,k)} \tag{5}$$

and

$$\frac{C \vee \mathcal{S}(i,k)}{C} \tag{6}$$

corresponding to axioms (2) and (4). Moreover, without loss of generality we assume that rules (6) are applied only below rules (5). As our complexity measure for $P(G)$ we take the number of applications of rules (5).

The basis of the induction is trivial: if there is no application of rules (5) then our graph is nothing else but the triangle K_3.

The induction transition is done as follows. Consider the last application

$$\dfrac{\dfrac{\dfrac{\begin{matrix}\vdots \\ A \vee \mathcal{S}(i,j)\end{matrix} \qquad \begin{matrix}\vdots \\ B \vee \mathcal{S}(j,k)\end{matrix}}{A \vee B \vee \mathcal{S}(i,k)}}{\begin{matrix}\vdots \\ C \vee \mathcal{S}(i,k)\end{matrix}}}{\begin{matrix} C \\ \vdots \\ \Box\end{matrix}}$$

in $P(G)$ of a rule of type (5). This proof can be transformed into two proofs $P(G_1)$ and $P(G_2)$, namely,

$$\begin{matrix}\vdots \\ \dfrac{A \vee \mathcal{S}(i,j)}{A} \\ \vdots \\ \Box\end{matrix} \qquad\qquad \begin{matrix}\vdots \\ \dfrac{B \vee \mathcal{S}(j,k)}{B} \\ \vdots \\ \Box\end{matrix}$$

corresponding to graphs G_1 and G_2 which are obtained from graph G by adding edges between vertices i and j or, respectively, between vertices j and k.

Each of the two new proofs contains smaller number of applications of rules (5), so we can assume that both graphs G_1 and G_2 contain circles of odd length. Moreover, without loss of generality we can assume that these circles are simple, i.e., do not contain repeated edges. If one of these circles does not contain the new edge (between vertices i and j or, respectively, between vertices j and k), then it is the required odd length circle in the graph G.

Otherwise, the graph G contains simple paths of even length between i and j, and between j and k. Together with the edge between i and k these two paths form the required odd length circle in the graph G.

Example 2.

L.M.Vitaver's theorem [4] states that *if a (non-oriented) graph G has no colourings of vertices in γ colours* (property $\mathcal{P}$) *then for every orientation of its edges there is an oriented path of length γ* (property $\mathcal{Q}$).

Now instead of (3) we have weaker axioms

$$\bigvee_{k=0}^{\gamma-1} \bigvee_{l=k+1}^{\gamma} \mathcal{S}(i_k, i_l) \tag{7}$$

for every $\gamma + 1$ vertices $i_0, \ldots, i_\gamma$.

Let us now distinguish $\mathcal{S}(i,j)$ and $\mathcal{S}(j,i)$ and respectively add axioms

$$\mathcal{S}(i,j) \vee \neg\mathcal{S}(j,i). \tag{8}$$

We say that two formulas are *parallel* if one of them can be obtained from the other by several replacements of positive literal $\mathcal{S}(i,j)$ by $\mathcal{S}(j,i)$; we need not allow replacements of negative literal $\neg\mathcal{S}(i,j)$ by $\neg\mathcal{S}(j,i)$.

For a proof $P(G)$ we take any deduction of the false empty disjunction $\Box$ from axioms (2), (4), (7) and (8) by the resolution principle.

To define required property Q^*, we consider *generalized oriented paths* in couple $\langle\vec{G}, H\rangle$ where $\vec{G}$ is an orientation of G and H is a disjunction of positive and negative literals. Such a path is a sequence $i_0, \ldots, i_m$ of vertices such that for every k from 1 to m at least one of the following holds:

(I) G contains an edge oriented from i_{k-1} to i_k;

(II) H contains $\mathcal{S}(i_{k-1}, i_k)$;

(III) H contains either $\neg\mathcal{S}(i_{k-1}, i_k)$ or $\neg\mathcal{S}(i_k, i_{k-1})$.

By the *length of a generalized path* we shall understand the number of k for which options (I) or (II) hold.

Let $Q^*(G,F)$ mean that *for every orientation $\vec{G}$ and for every formula H parallel to F there is a generalized oriented path of length γ in $\langle\vec{G}, H\rangle$.*

Now we need to verify properties (1*)–(3*).

Axiom (2) has two parallel formulas: itself and

$$\neg\mathcal{S}(i,j) \vee \neg\mathcal{S}(j,k) \vee \mathcal{S}(k,i). \tag{9}$$

The required generalized paths are

$$i,k,j,i,k,j,\ldots,i,k,j \tag{10}$$

and

$$i,j,k,i,j,k,\ldots,i,j,k \tag{11}$$

respectively.

For an axiom (4) the required generalized path is

$$i,k,i,k,\ldots,i,k. \tag{12}$$

For an axiom (8) and the other formula parallel to it the required generalized path is

$$i,j,i,j,\ldots,i,j. \tag{13}$$

Let H be a formula parallel to an axiom (7). The required generalized path can be constructed by induction on γ. The case $\gamma = 1$ is trivial. For $\gamma > 1$ there are two possibilities:

- there is an index m such that i_m never occurs as the first argument of $\mathcal{S}$ in H;
- for every index m there is another index n such that H contains $\mathcal{S}(i_m, i_n)$; such an n will be denoted by $\nu(m)$.

In the former case, find a generalized path of length $\gamma - 1$ for formula H' resulting from H by deleting all literals containing i_m and then extend the path by i_m. In the latter case, take the following generalized path:

$$i_0, i_{\nu(0)}, i_{\nu(\nu(0))}, \ldots, i_{\nu(\ldots\nu(0)\ldots)}. \tag{14}$$

Now consider an application

$$\frac{A \vee \mathcal{S}(i,j) \qquad B \vee \neg\mathcal{S}(j,i)}{A \vee B} \tag{15}$$

of the resolution principle. Let us fix an orientation of edges $\vec{G}$ and let $A' \vee B'$ be a formula parallel to the conclusion in (15). Let

$$q_0, q_1, \ldots, q_w \tag{16}$$

be a generalized path of length γ in $\langle \vec{G}, B' \vee \neg\mathcal{S}(i,j) \rangle$ with the least possible value of w. We need to distinguish two main cases:

(Q0) all vertices in (16) are different;

(Q1) there are indices m_1 and m_2 such that $m_1 < m_2$, $q_{m_1} = q_{m_2}$ but there no other equal vertices in the generalized path

$$q_{m_1}, \dots, q_{m_2}. \tag{17}$$

In the latter case the length of the path (17) is positive because otherwise we would be able to delete vertices $q_{m_1+1}, \dots, q_{m_2}$ and still have the path

$$q_0, \dots, q_{m_1} = q_{m_2}, \dots, q_w \tag{18}$$

of the length γ, which contradicts the minimality of w.

If path (16) contains neither $\dots, i, j, \dots$ no $\dots, j, i, \dots$ then it is the required generalized path in $\langle \vec{G}, A' \vee B' \rangle$. Analogously, if the circle path (17) contains neither $\dots, i, j, \dots$ no $\dots, j, i, \dots$ then its power

$$q_{m_1}, \dots, q_{m_2} = q_{m_1}, \dots, q_{m_2}, \dots q_{m_1}, \dots, q_{m_2} \tag{19}$$

is a generalized path in $\langle \vec{G}, A' \vee B' \rangle$ the length of which can be made arbitrary large.

Now let n be the unique index such that either

$$q_{n-1} = i, \qquad q_n = j \tag{20}$$

or

$$q_{n-1} = j, \qquad q_n = i. \tag{21}$$

In case (20) let $i' = j$, $j' = i$, in case (21) let $i' = i$, $j' = j$. Now in case (Q0) we have in $\langle \vec{G}, A' \vee B' \rangle$ two generalized paths

$$q_0, \dots, q_{n-1} = j' \tag{22}$$

and

$$i' = q_n, \dots, q_w, \tag{23}$$

the sum of lengths of which is equal to γ. In case (Q1) we have in $\langle \vec{G}, A' \vee B' \rangle$ generalized path of positive length

$$i' = q_n, \dots, q_{m_2} = q_{m_1}, \dots, q_{n-1} = j'. \tag{24}$$

Now let

$$p_0, p_1, \ldots, p_v \tag{25}$$

be a generalized paths of length γ in $\langle \vec{G}, A' \vee \mathcal{S}(i', j')\rangle$ with the least possible value of v. We repeat for it a case inspection analogous to the one done for path (16) with proper modification.

Again there are two main cases:

(P0) all vertices in (25) are different;

(P1) there are indices k_1 and k_2 such that $k_1 < k_2$, $p_{k_1} = p_{k_2}$ but there no other equal vertices in the generalized path

$$p_{k_1}, \ldots, p_{k_2}. \tag{26}$$

In the latter case the length of the path (26) is positive because otherwise we would be able to delete vertices $p_{k_1+1}, \ldots, p_{k_2}$ and still have the path

$$p_0, \ldots, p_{k_1} = p_{k_2}, \ldots, p_v \tag{27}$$

of the length γ, which contradicts the minimality of v.

If path (25) does not contain $\ldots, i', j', \ldots$ then it is the required generalized path in $\langle \vec{G}, A' \vee B'\rangle$. Analogously, if the circle path (26) does not contain $\ldots, i', j', \ldots$ then its power

$$p_{k_1}, \ldots, p_{k_2} = p_{k_1}, \ldots, p_{k_2}, \ldots p_{k_1}, \ldots, p_{k_2} \tag{28}$$

is a generalized path in $\langle \vec{G}, A' \vee B'\rangle$ the length of which can be made arbitrary large.

Now let l be the unique index such that $p_{l-1} = i'$, $p_l = j'$. In case (P0) we have in $\langle \vec{G}, A' \vee B'\rangle$ two generalized paths

$$p_0, \ldots, p_{l-1} = i' \tag{29}$$

and

$$j' = p_l, \ldots, p_v, \tag{30}$$

the sum of the lengths of these two paths is equal to $\gamma - 1$. In case (P1) we have in $\langle \vec{G}, A' \vee B'\rangle$ generalized path

$$j' = p_l, \ldots, p_{k_2} = p_{k_1}, \ldots, p_{l-1} = i'. \tag{31}$$

If both cases (P0) and (Q0) hold, we have in $\langle \vec{G}, A' \vee B' \rangle$ two generalized paths

$$p_0, \dots, p_{l-1} = i' = q_n, \dots, q_w \tag{32}$$

and

$$q_0, \dots, q_{n-1} = j' = p_l, \dots, p_v. \tag{33}$$

The sum of the length of these two paths is equal to $2\gamma - 1$, so one of them has the lengths at least γ.

If both cases (P0) and (Q1) hold, we have in $\langle \vec{G}, A' \vee B' \rangle$ generalized path

$$p_0, \dots, p_{l-1} = i' = q_n, \dots, q_{m_2} = q_{m_1}, \dots, q_{n-1} = j' = p_l, \dots, p_v \tag{34}$$

of length at least γ.

Analogously, if both cases (P1) and (Q0) hold, we have in $\langle \vec{G}, A' \vee B' \rangle$ generalized path

$$q_0, \dots, q_{n-1} = j' = p_l, \dots, p_{k_2} = p_{k_1}, \dots, p_{l-1} = i' = q_n, \dots, q_w \tag{35}$$

of length at least γ.

At last, if both cases (P1) and (Q1) hold, we have in $\langle \vec{G}, A' \vee B' \rangle$ generalized circle path

$$i' = q_n, \dots, q_{m_2} = q_{m_1}, \dots, q_{n-1} = j' = p_l, \dots, p_{k_2} = p_{k_1}, \dots, p_{l-1} = i' \tag{36}$$

of positive length. Respectively, taking a power of this path, we can obtain a path of arbitrary length.

Finally, we need to show that $Q^*(G, \square)$ implies $Q(G)$. But this is evident because for the empty disjuction generalized paths coincides with regular oriented paths in the graph.

Example 3.

The Four Colour Theorem (FCT) states ([1, 2]) that *every planar graph has a colouring of vertices in four colours.* It follows from an old result of H. Whitney [5] that it sufficient to prove the FCT for Hamiltonian planar graphs.

Let us say that a graph G is *almost Hamiltonian planar* if it becomes Hamiltonian planar after the following two operation:

- identification (gluing) of some vertices;
- addition of new edges.

The FCT is equivalent to the statement that *if graph G has no colouring of vertices in four colours* (property $\mathcal{P}$) *then it is not almost Hamiltonian planar* (property $\mathcal{Q}$).

We fix one vertex and a direction, say, clock-wise, on a Hamiltonian graph G. This would introduce a linear order on the vertices which will be denoted by $\prec$. It satisfies standard axioms of linear order:

$$\neg(i \prec i), \tag{37}$$

$$\neg i \prec j \vee \neg j \prec i, \tag{38}$$

$$\neg i \prec j \vee \neg j \prec k \vee k \prec i. \tag{39}$$

In case when vertices i and j are connected by an edge, we also have

$$i \prec j \vee j \prec i \tag{40}$$

(we do not demand this condition for an arbitrary i and j because we allow gluing vertices).

The edges of a Hamiltonian planar graph can be classifies as *internal* and *external* (classification of the edges on the Hamiltonian circle can be arbitrary). This defines relation $\mathcal{T}(i, j, k, l)$ saying that *the edge between vertices i and j is of the same type as the edge between vertices k and l* (if there is no corresponding edge then the relation $\mathcal{T}$ should be defined as if the missing edge were, say, internal). This relation satisfies the following axioms:

$$\mathcal{T}(i, j, i, j), \tag{41}$$

$$\neg\mathcal{T}(i, j, k, l) \vee \neg\mathcal{T}(k, l, m, n) \vee \mathcal{T}(i, j, m, n), \tag{42}$$

$$\mathcal{T}(i,j,k,l) \vee \mathcal{T}(k,l,m,n) \vee \mathcal{T}(i,j,m,n) \tag{43}$$

(we do not distinguish $\mathcal{T}(i,j,k,l)$, $\mathcal{T}(j,i,k,l)$ and $\mathcal{T}(k,l,i,j)$).

The planarity of graph G is expressed by the validity of all disjunctions of the form

$$\neg(i \prec k) \vee \neg(k \prec j) \vee \neg(j \prec l) \vee \neg\mathcal{T}(i,j,k,l) \tag{44}$$

where vertices i and j, as well as vertices k and l, are connected by edges.

For a proof $Q(G)$ we can take any deduction of the false empty disjunction $\square$ from axioms (37)–(44).

To formalize $\mathcal{P}$, we *reinterpret* $i \prec j$ as the statement that *the colour of vertex i is less than the colour of vertex j* (we take numbers 1,2,3,4 as the colours). Under this interpretation all formulas (37)–(40) remain valid. Besides them, we have in addition the axiom

$$\neg(i_0 \prec i_1) \vee \neg(i_1 \prec i_2) \vee \neg(i_2 \prec i_3) \vee \neg(i_3 \prec i_4) \tag{45}$$

saying that we have only four colours.

We could take for $P(G)$ any deduction of the false empty disjunction $\square$ from axioms (37)–(40) and (45). To achieve the desired relationship with our formalization of property $\mathcal{Q}$, we take for $P(G)$ any deduction of $\square$ from all axioms (37)–(45). To justify inclusion of axioms (41)–(44) we reinterpret $\mathcal{T}(i,j,k,l)$ as being false if and only if

$$\{\{\sigma(i),\sigma(j)\},\{\sigma(k),\sigma(l)\}\} = \{\{1,3\},\{2,4\}\} \tag{46}$$

where $\sigma(n)$ denotes the colour of vertex n.

References

[1] K. Appel, W. Haken. Every planar map is four colorable. Part I. Discharging. *Illinois J. of Mathematics*, **21**(3):429–490 (1977).

[2] K. Appel, W. Haken, J. Koch. Every planar map is four colorable. Part II. Reducibility. *Illinois J. of Mathematics*, **21**(3):491–567 (1977).

[3] Yu.V.Matiyasevich. A metamathematical approach to proving theorems of discrete mathematics (in Russian). *Zapiski nauchnykh seminarov LOMI AN SSSR*, 49:31–50, 1975. English translation in *Journal of Soviet Mathematics*, 10(4):517–533, 1978.

[4] L.M.Vitaver. Finding minimal colourings of the vertices of a graph via Boolean powers of the incidence matrix (in Russian). *Doklady AN SSSR*, 147(4):758-759, 1962.

[5] H.Whitney. A theorem on graphs. *Ann. Math.*, 32(2):378-390, 1931.