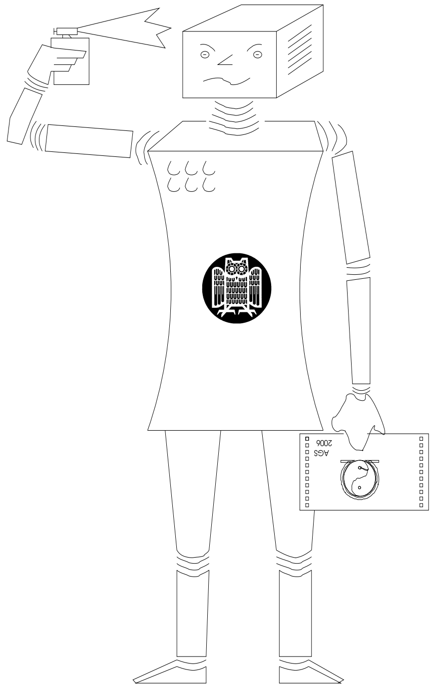
UNIVERSITÄT DES SAARLANDES
FACHRICHTUNG INFORMATIK
D–66123 SAARBRÜCKEN
GERMANY
WWW: http://www.ags.uni-sb.de/



SEKI-Report ISSN 1437-4447

The Method of *Descente Infinie* in History and Computer-Assisted Human-Oriented Theorem Proving

Paolo Bussotti
Via Paolo Lilla 66, 57122 Livorno, Italy
bussottipaolo@yahoo.com

Claus-Peter Wirth
Brandenburger Str. 42, D–65582 Diez, Germany
wirth@logic.at

SEKI-Report SR-2007-01

This SEKI-Report was internally reviewed by:

— *(Until now just under review!)* —

Editor of SEKI series:

Claus-Peter Wirth
Brandenburger Str. 42, D–65582 Diez, Germany
E-mail: `wirth@logic.at`
WWW: `http://www.ags.uni-sb.de/~cp`

The Method of *Descente Infinie* in History and Computer-Assisted Human-Oriented Theorem Proving

Paolo Bussotti
Via Paolo Lilla 66, 57122 Livorno, Italy
bussottipaolo@yahoo.com

Claus-Peter Wirth
Brandenburger Str. 42, D–65582 Diez, Germany
wirth@logic.at

Draft
January 8, 2007

Abstract

(The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end. The abstract remains to be written in the very end.)

1 Introduction

In this paper we contribute to the meta-level knowledge on the method of mathematical induction and its heuristics. Our interest is in the practical proof search of the working mathematician, but not in the well-known proof-theoretical peculiarities of mathematical induction that actually do not really have a practical effect; cf. Gödel (1931), Gödel (1986 ff.) for enumerability; Kreisel (1965) for cut elimination; Wirth (2006), Note 4 for practical irrelevance.

We are not interested in the induction methods for simple proofs at the level of freshmen or at the level of fully automated inductive theorem proving systems. To the contrary, we are interested in such proof tasks whose level of difficulty requires some ingenuity in proof search and an explicit presentation in an advanced mathematical publication. The order in a succinct presentation—say in a journal—more often than not differs from the way the proof was originally found. Most non-trivial proofs by induction are actually found by the *Method of Descente Infinie*. This the standard induction method for non-trivial proof tasks of the working mathematician from the ancient Greeks until today. It got lost in the Middle Ages and was reinvented and named by Fermat, cf. § 3.

Besides using the standard knowledge of working mathematicians, we approach the Method of *Descente Infinie* from two sides, namely from its history (cf. Bussotti (2006)) and from its logical description for human-oriented computer-assisted theorem proving (cf. Wirth (2004)).

As a first step we subdivide the Method of *Descente Infinie* into the sub-methods of *Nötherian induction*, indefinite descent, and reduction-descent, as classified in the following table.

Descente Infinie	**without Exceptions**	**with Special Cases**
affirmative	Nötherian induction	affirmative reduction-descent
apagogic	indefinite descent	apagogic reduction-descent

Note that this table does not refer to positive or negative propositions (which is a matter of choice of linguistic formulation) but to affirmative (positive) and apagogic ("that lead you away from", negative, refutational) methods of demonstration.

2 Motivation

(This may be too long here. But we may remove it in the completed paper, after it has been part of OUR motivation!)

Mathematical methods are still taught only by paradigmatic examples. This has the advantages that lecturers do not have to provide meta-level descriptions of the methods and that students can proceed by a stepwise understanding of concrete examples and then use their highly-developed inductive-learning abilities. (Note that inductive learning is learning by examples and has nothing to do with mathematical induction in general.) The disadvantage of this procedure of teaching and learning, however, is that nobody really knows what a certain method exactly is and what the heuristics for its application are. While the whole process of mathematical theory development and theorem proving might never be grasped by the human intellect on the meta level, we are convinced that meta-level descriptions of standard proof methods are indeed possible. Such meta-level descriptions could be beneficial

1. to improve the clarity of mathematical discussion,
2. to ensure the success of inductive learning by providing a meta-level description in the conclusion,
3. to refine the understanding of the history of the methods,
4. to apply methods in software systems that assist the working mathematician in his daily work (Mathematics Assistance Systems, cf. Siekmann &al. (2002), Autexier &al. (2006)), and

This is not conceptually opposed to the wide-spread belief that a scientific *paradigm* does not need any concrete meta-level rules and that such rules would destroy scientific creativity, cf. Kuhn (1962), Feyerabend (1975). Indeed, the history of mathematics shows that concrete meta-level rules are not essential. As paradigm changes in mathematics are rarer than in natural sciences, we think that it is time to approach such meta-level descriptions for the classical methods in mathematics. And, if the enterprise of formulating these rules is successful, we still do not have to teach them if they are then found out to destroy creativity. Mathematical induction is an excellent candidate for starting this very difficult enterprise, because it is that area of mathematical theorem proving where our heuristic knowledge is best. This is the case both for human and for machine-oriented heuristics, cf. Wirth (2006).

We are quite aware of the difficulty of our enterprise and that the most advanced meta-level descriptions of mathematical methods in computer-assisted theorem proving and proof planning have not yet reached the level of difficulty we intend for our proofs, cf. Bundy (1988), Meier (2004), Meier & Melis (2004), Wirth (2004), Schmidt-Samoa (2006c). Nevertheless, we are confident to do a first practically relevant step toward the meta-level description of the Method of *Descente Infinie* and its application heuristics on the level of difficulty described in § 1.

Besides clearly describing the Method of *Descente Infinie* on a refined level and besides providing the paradigmatic historical examples, we want to develop some deeper knowledge on the area of application of certain sub-methods.

3 Historical Problems

(To be written by Paolo!)

3.1 Introduction and Prehistory

> (We need the whole French text here. CP only added that part he had already in ASCII.) S'il y avoit aucun triangle rectangle en nombres entiers qui eût son aire égale a un quarré, il y auroit un autre triangle moindre que celui-là, qui auroit la même propriété. S'il y en avoit un second, moindre que le premier, qui eût la même propriété, il y en auroit, par un pareil raisonnement, un troisième, moindre que le second, qui auroit la même propriété, et enfin un quatrième, un cinquième, &c. à l'infini en descendant. Or est-il qu'étant donné un nombre, il n'y en a point infinis en descendant moindres que celui-là (j'entends parler toujours des nombres entiers). D'où on conclut qu'il est done impossible qu'il y ait aucun triangle rectangle dont l'aire soit quarrée.[1]
>
> And since the normal methods, which are explained in the books, were not sufficient to prove such difficult propositions, finally I found an absolutely particular procedure for overcoming these difficulties. I called this way of demonstrating *descente infinie* or *indéfinie* [infinite or indefinite descent]. At the beginning I used this method for demonstrating negative propositions, like, for example: "there is no number of the form $3n{-}1$ which is equal to a square plus the triple of a square"; "there is no Pythagorean triangle of which the area is the square of an integer". The proof runs by *apagoghè eis adunaton* in this manner: If there were any right-angled triangle in whole numbers that had its area equal to a square, there would be another [right-angled] triangle smaller than that one, which would have the same property. If there were a second, smaller than the first, which had the same property, there would be, by a similar reasoning, a third, smaller than the second, which would have the same property, and finally a fourth, a fifth, &c., descending to infinity. But, given a number, there is not an infinite number of numbers less than it (I am speaking about integer numbers). Hence, one deduces the impossibility that a Pythagorean triangle has the area equal to the square of an integer.

With these words by Fermat, it is clear (even if not properly defined) what the infinite or indefinite descent are, and that the history of this method begins exactly with Fermat. The method is conceived as follows: Let us suppose that we have to prove a theorem $\forall x.\, T(x)$ and let us reason *ad absurdum*, posing, for some natural number m, that $T(m)$ is false and $\neg T(m)$ true. If this position implies that, given another natural number n with $n \prec m$, an infinite number of whole numbers would exist between n and m, this is absurd, hence $\neg T(m)$ must be false, and therefore $\forall x.\, T(x)$ is true. Fermat judged himself the inventor

[1]Fermat wrote these words in a letter sent to Huygens through Carcavi in August 1659. The letter is titled *Relation des nouvelles dcouvertes en la science des nombres*. It can be consulted in Fermat (1891ff.), Vol. II, pp. 431–436. The discovery of this letter has an interesting history that is summarized in Bussotti (2006), p. 5, Note 4.

of this method because for the first time he clearly separated this procedure from other methods and because he applied the descent to difficult theorems. By other words: he fully understood the potential of this method and thought to make it one of the most important—if not even *the* most important—in number theory. However, a prehistory of this method exists.[2] In this period only some isolated and (at least for us) most simple theorems were demonstrated by indefinite descent. We remind the reader of the first among the theorems surely proved through this procedure: Euclid in Elements, VII, 31 wants to prove that every composite number has a prime number as a divisor. He reasons in the following way:

> Let p be a composite number, then p has at least two divisors p_1 and p_2 that are different from p and from 1. If one of the two divisors is a prime number, the theorem is true. So both p_1 and p_2 are composite numbers. Let us consider p_1. This number will have two divisors p_1' and p_1'' and, obviously both p_1' and p_1'' are smaller than p. If one of these two numbers is a prime number, then the theorem is true. If we suppose that neither p_1' nor p_1'' are prime, then, considering for example p_1', we will have two other numbers, for example p_1''' and p_1'''', that are divisors of p_1', and $p_1''' \prec p_1' \prec p$. But if we deny that p has a prime number as a divisor, this reduction can be continued infinitely and we would be obliged to admit the existence of an infinite number of integers between 1 and p. This is clearly absurd, therefore, the theorem is true.

Fermat claimed that "the standard form" of the indefinite descent works when the method is applied to "negative propositions", namely propositions posed in the form of a negated existential quantification, in modern notation $\neg\exists x.\,T(x)$; but the application to "positive propositions" needs "the addition of some new principles".[3] From a modern point of view Fermat's distinction appears to be a little bit strange because it is obvious that every negative assertion can be posed in an affirmative one (such as $\forall x.\,\neg T(x)$) which is logically equivalent and vice versa. However, we will see what Fermat wrote makes mathematical sense. First of all, let us see what these "new principles" are. In the letter to Huygens, Fermat asserted that one of the most important "affirmative" theorems he demonstrated by descent is the famous proposition that every prime number of the form $4n{+}1$ is the sum of two squares. He wrote:

> (We should add the French original here!)

> If an arbitrary prime number of the form $4n{+}1$ were not composed of two squares, there would exist a less prime of the same nature and a third one, descending infinitely (à l'infini) to 5, which is the smallest prime of this type and that should not be composed of two squares. But 5 is the sum of two squares. Hence we deduce through the reductio ad absurdum that every number of this type is composed of two squares.[4]

[2]A good bibliography on the history of the infinite or indefinite descent can be consulted in Goldstein (1995) and in Bussotti (2006). With regard to the descent before Fermat the reader can consult for example Cassinet, 1980; Genocchi, 1855; Vacca, 1927-28.

[3]Fermat (1891ff.), Vol. II, p. 432.

[4]Ibidem, p. 432.

Literally interpreted the assertion by Fermat makes no sense because within the natural numbers it is impossible to descent infinitely starting from a given natural number and to reach 5. But in this case, it is not difficult to provide a meaningful interpretation: If we suppose that a prime p of the form $4n{+}1$ would exist which is not the sum of two squares, then this would imply the existence of another number p', less than p and not the sum of two squares, after that a number p'', less than p' and not the sum of two squares and so on, until reaching 5, a number that, according to the construction, should not be the sum of two squares. But, as 5 is the sum of two squares, this implies an absurdity that arises from supposing p not to be sum of two squares, hence p is the sum of two squares.

More general: Let us suppose that we must prove the theorem $\forall x.\ T(x)$. Suppose that $T(x)$ is true for x among some initial values. It is possible to use the expression "$T(x)$ is true for x being a small number". For S being the predicate that holds exactly for these small numbers, we then have $\forall x.\ (S(x) \Rightarrow T(x))$. Now let us suppose that $T(n)$ is false for an arbitrary natural number n, and that we are able to construct an algorithm such that, if $T(n)$ is false, then $T(m)$ is false for a natural number m smaller than n. (This description lacks generality: "algorithm" means computability. But we do not even need constructiveness, not even describability or ontological existence, we just need logical existence.)

(The following question is most serious in my humble opinion: The question for the *inner* gestalt of the mathematician's thinking will not lead us too far. This seems to be especially fruitless in history of mathematics, because we cannot communicate with dead mathematicians and because—without any chance to confirm our theses on the inner gestalt—the role of such an insight into the history of mathematics can only be a most questionable one. Therefore, I think that the only way to judge on the gestalt of mathematics in former times is to look what the mathematicians have actually done, i.e. what their proofs are. Their additional rhetorical remarks may guide us, but we should not rely on them, and we should not give too much on their metaphors unless they have an effect on the tasks of their proofs. This is somehow a behavioristic point of view, but I hardly see another chance to come to serious results, different from Unguru's sophisticated speculations that escape mathematical practice.

Regarding the actual theorem proving activity of the mathematician, this method of reduction descent differs from the method of indefinite descent only if he may additionally assume that n is not a small number. So, please, Poalo, answer the following question to me: Does $\left(\begin{array}{ll} & \neg S(n) \wedge \neg T(n) \\ \Rightarrow & \exists m \prec n.\ \neg T(m) \end{array}\right)$ suffice or is the mathematician required to show $\left(\begin{array}{ll} & \neg T(n) \\ \Rightarrow & \exists m \prec n.\ \neg T(m) \end{array}\right)$ for the method of reduction descent actually? In the later case I would be very unhappy for two reasons:

1. I did not understand you and your book properly up to now and what I wrote about you in SWP–2006–02 is wrong although you counter-checked it. It is just now in the printing factory, and I would like to stop it if possible and if to prove the former would not suffice for the method of reduction descent.

2. I do not think the distinguishing of the two concepts "indefinite descent" and "reduction descent" to be appropriate *in any mathematical sense, even not in the historical one*, but judge this as a sophistication which is "over the top" similar to what I wrote in § 2.4.1 on Unguru and Acerbi in SWP–2006–02. Sorry for being so horribly explicit, but I am a German, after all, even if I do not like the Germans.

Even if you think that the latter is actually required, maybe Fermat thought differently? What do the many reconstructions of Sergio Paolini say about this? Is there any example of a reduction descent where $\neg S(n)$ is used in the proof, i.e. the reduction assumes that then n is not a small number? A single example would show that the former alternative is right and that we all could be happy!) Let us suppose that the process can be iterated and that the "small numbers" are reached. Obviously T might be false in particular exactly for the "small numbers". However, for the small numbers T is true, so we have a contradiction and such a contradiction arises because we have supposed $\neg T(n)$ to be true. Therefore T is true for every number. We will call this method *reduction-descent*. Thus, in the set of methods which can be called descent, it is possible to distinguish, following Fermat's implicit indications:

1. the indefinite descent in a proper sense where if we suppose false the theorem to prove we have:
   (a) a number m, less than n;
   (b) a reduction that starts from n and that, from a formal point of view, can be continued infinitely, but that cannot reach m for particular mathematical reasons which are specified in every single theorem;
   (c) the absurdity which derives from this situation: an infinite number of integers should subsist between m and n;
2. the reduction-descent:
   (a) the theorem to prove is true for some initial values;
   (b) if we suppose the theorem false for a value we have a reduction that (and this is the main difference with the standard indefinite descent) reaches the initial values;
   (c) for these values the theorem should be at the same time true and false, this is absurd, hence the supposition 2b has to be removed.

Now we can try to answer the question why Fermat deemed the reduction-descent more suitable for the affirmative theses. The answer is exactly that in this case there is a set of initial values for which the theorem is true, therefore a mathematician can be induced to exploit this fact in some way and Fermat did this in the manner we have described. Therefore even if there is no difference from a logical point of view between "negative" and "affirmative propositions" and even if, of course, the standard descent can be applied to affirmative theses and the reduction-descent to negative theses, nevertheless the form of the two methods justifies the assertions by Fermat. The logical equivalence is only an aspect of the problem; there are other aspects which are even more important to understand the way in which a mathematician proved a certain proposition or in which he applied a method. These aspects depend on the historical background, on the habits which are typical of mathematics in a certain period, on the linguistic form one prefers to give to a problem or to a set of problems and on the general state of the mathematical language in the period. On the basis of these considerations one is perhaps able to understand and to appreciate the plurality of methods (even logically equivalent methods) the mathematicians developed in the course of the time. By the way, this can enrich our conceptual horizon and be useful to the logical research itself. After having described the two variants of Fermat's method, it is necessary to see the application to nontrivial problems because it is possible to appreciate a method only if we realize how it really works. With regard to Fermat, he claimed to have demonstrated the following significant propositions through descent:

1. there is no Pythagorean triangle of which the area is equal to the square of an integer;
2. every prime of the form $4n+1$ is the sum of two squares;
3. every prime of the form $8n+1$ or $8n+3$ is the sum of a square and the double of another square;
4. every prime of the form $3n+1$ is the sum of a square and the triple of another square;
5. Pell's equation: the equation $x^2 = Ny^2 + 1$ (N integer different from a square) has always whole solutions;
6. every integer is the sum of four squares (this assertion is part of the famous polygonal numbers theorem by Fermat);
7. the equations $x^3 + y^3 = z^3$ and $x^4 + y^4 = z^4$ have no integer solutions, apart from those trivial;
8. the equation $x^2 + 2 = y^3$ has the only solution $(5, 3)$;
9. the equation $x^2 + 4 = y^3$ has the only solutions $(2, 2)$ and $(11, 5)$.

The problem with Fermat is that he only left us with the explicit demonstration of the sole assertion (1). For all the rest, he left only some more or less vague indications.[5] The proof of assertion (1) is not difficult, but rather complicated, therefore we prefer to present the demonstration by Euler of the impossibility to solve in integers the equation $x^4 + y^4 = z^4$. This provides a clear, even if not too trivial, example of a proposition demonstrated by standard indefinite descent. By the way 1) implies the assertion on the equation $x^4 + y^4 = z^4$. Like an example of demonstration provided by reduction-descent, we will supply Euler's proof that every number of the form $x^2 + y^2$ with $\gcd(x, y) = 1$ is divided only by numbers of its same form. Euler exploited this proposition to demonstrate that every prime of the form $4n+1$ is the sum of two squares.

[5]Fermat demonstrated n. 1) in his Observations sur Diophante (observation 45), see, Fermat, Oeuvres 1, p. 340; n. 2) is quoted in many letters and in the Observations. What Fermat wrote in the letter to Huygens is the most âĂIJcompleteâĂİ reference to reconstruct his possible demonstration; n. 3) and 4) are quoted in a letter to Pascal in 1654, see Fermat, Oeuvres, 2, pp. 310-314. The so called Pell's equation (better FermatâĂŹs equation) was proposed by Fermat as a challange to Frenicle and the English mathematicians in the period 1657-1658. It is quoted in many letters by Fermat and in the letter to Huygens in 1659, too; with regard to n. 6), Fermat deemed the polygonal numbers theorem like his most signficant. It is quoted many times, even in the Observations (number 18), and in the letter to Pascal in 1654. In the letter to Huygens, Fermat claimed he proved the proposition for the four squares by descent; n. 7) are two particular cases of FermatâĂŹs last theorem, to which Fermat reffered more than once, see letter to Huygens, too. The general proposition is quoted only once in the Observations (number 2); n. 8) and 9) are mentioned in the letter to Huygens like examples of difficult problems solved by descent.

3.2 Euclid

3.3 Fermat's Pythagorean Triangle

3.4 One of Euler's Demonstrations by Reduction-Descent

Leonhard Euler (1707–1783)

3.5 Where these Methods are Used

4 Logical Considerations

4.1 Logical Equivalence

At Fermat's time, natural language was still the predominant tool for expressing terms and equations in mathematical writing, and it was too early for a formal axiomatization. Moreover, carefully notice that an axiomatization captures only validity, but in general does neither induce a method of proof search nor provide the data structures required to admit both a formal treatment and a human-oriented proof search. The formalizable logic part, however, of *descente infinie* can be expressed in what is called the (second-order) *Theorem of Nötherian Induction* (N), after A. Emmy Nöther (1882–1935). This is not to be confused with the *Axiom of Structural Induction*, which is generically given for any inductively defined data structure, such as the *Axiom of Structural Induction* (S) *for the natural numbers inductively defined by the constructors zero* $\mathsf{0}$ *and successor* s. Moreover, we need the definition $(\mathsf{Wellf}(<))$ of wellfoundedness of a relation $<$.

$$
\begin{array}{lll}
(\mathsf{Wellf}(<)) & \forall Q. & \Big(\exists x.\ Q(x) \quad \Rightarrow \quad \exists m.\ \big(\ Q(m) \wedge \neg\exists w{<}m.\ Q(w)\ \big) \Big) \\
(\mathsf{N}) & \forall P. & \left(\forall x.\ P(x) \quad \Leftarrow \quad \exists{<}.\ \left(\begin{array}{l} \quad \forall v.\ \big(\ P(v) \quad \Leftarrow \quad \forall u{<}v.\ P(u)\ \big) \\ \wedge \ \ \mathsf{Wellf}(<) \end{array} \right) \right) \\
(\mathsf{S}) & \forall P. & \Big(\forall x.\ P(x) \quad \Leftarrow \quad P(\mathsf{0}) \ \wedge \ \forall y.\ \big(\ P(\mathsf{s}(y)) \Leftarrow P(y)\ \big) \Big) \\
(\mathsf{nat1}) & \forall x. & \big(\ x{=}\mathsf{0} \vee \exists y.\ x{=}\mathsf{s}(y)\ \big) \\
(\mathsf{nat2}) & \forall x. & \mathsf{s}(x){\neq}\mathsf{0} \\
(\mathsf{nat3}) & \forall x,y. & (\mathsf{s}(x){=}\mathsf{s}(y) \Rightarrow x{=}y)
\end{array}
$$

Let $\mathsf{Wellf}(\mathsf{s})$ denote $\mathsf{Wellf}(\lambda x,y.\,(\mathsf{s}(x)=y))$, which implies the wellfoundedness of the ordering of the natural numbers. The natural numbers can be specified up to isomorphism either by (S), $(\mathsf{nat2})$, and $(\mathsf{nat3})$, or else by $\mathsf{Wellf}(\mathsf{s})$ and $(\mathsf{nat1})$. The first alternative is the traditional one, following Dedekind and named after Peano. As the instances for P and $<$ in (N) are often still easy to find when the instances for P in (S) are not, the second alternative together with (N) is to be preferred in theorem proving for its usefulness and elegance. Cf. Wirth (2004) for more on this.

The proposition to be proved by *descente infinie* is represented in (N) by $\forall x.\ P(x)$. Roughly speaking, a *counterexample* for Γ is an instance a for which $\neg P(a)$ holds, but we should be more careful here because this is actually a semantical notion and not a syntactical one; cf. Wirth (2004), § 2.3.2. To treat counterexamples properly, a logic that actually models the mathematical process of proof search by *descente infinie* itself and directly supports it with the data structures required for a formal treatment requires a semantical treatment of free variables. The only such logic can be found in Wirth (2004).

The level of abstraction of our previous discussion of *descente infinie* is well-suited for the description of the structure of mathematical proof search in two-valued logics, where the difference between a proof by contradiction and a positive proof of a given theorem is only a linguistic one and completely disappears when we formalize these proofs in a state-of-the-art modern logic calculus, such as the one of Wirth (2004). An investigation into the history of mathematics, however, also has to consider the linguistic representation and the exact logical form of the presentation.

We suggest the following classification scheme for proof by mathematical induction, which is unproblematic in the sense that it does not refer the working mathematician's consciousness, but only to the written documents. It suffices to speak of

1. quasi-general proofs (i.e. proofs by generalizable examples) (This has to be explained somewhere!),
2. general proofs (i.e. proofs we would accept from our students in an examination today),
3. proofs with an explicit statement of the related instance of an induction axiom or theorem, and
4. proofs with an explicit statement of an induction axiom or theorem itself.

There is evidence that such a linguistic and logic-historical refinement is necessary to understand the fine structure of historical reasoning in mathematics. For instance, in Euclid's Elements, Proposition VIII.7 is just the contrapositive of Proposition VIII.6, and this is just one of several cases that we find a proposition with a proof in the Elements, where today we just see a corollary. Moreover, even Fermat reported in his letter for Huygens (This has to be presented somewhere!) that he had had problems to apply the Method of *Descente Infinie* to positive mathematical statements.

> "Je fus longtemps sans pouvoir appliquer ma méthode aux questions affirmatives, parce que le tour et le biais pour y venir est beaucoup plus malaisé que celui dont je me sers aux négatives. De sorte que, lorsqu'il me fallut démontrer que *tout nombre premier, qui surpasse de l'unité un multiple de 4, est composé de deux quarrés*, je me trouvai en belle peine. Mais enfin une méditation diverses fois réitérée me donna les lumières qui me manquoient, et les questions affirmatives passèrent par ma méthode, à l'aide de quelques nouveaux principes qu'il y fallut joindre par nécessité." [Fermat (1891ff.), Vol. II, p. 432]

> "For a long time I was not able to apply my method to affirmative conjectures because the ways and means of achieving this are much more complicated than the ones I am used to for negative conjectures. So that, when I had to show that any prime number which exceeds 1 by a multiple of 4 is the sum of two squares, I found myself pretty much in trouble. But finally oft-repeated meditation gave me the insight I lacked, and affirmative questions yielded to my method with the aid of some new principles which had to be added to it." (our translation)

Due to the work of Frege and Peano, these logical differences may be considered trivial today. Nevertheless, they were not trivial before, and to understand the history of mathematics and the fine structure in which mathematicians reasoned, the distinction between affirmative and negative theorems and between direct and apagogic methods of demonstration is important.

Therefore, in Bussotti (2006), following the above statement of Fermat, the Method of *Descente Infinie* is subdivided into *indefinite descent* (ID) and *reduction-descent* (RD):

$$(\mathsf{ID}) \quad \forall P.\ \left(\forall x.\ P(x) \quad \Leftarrow \quad \exists{<}.\ \left(\begin{array}{l} \quad \forall v.\ (\ \neg P(v) \ \Rightarrow\ \exists u{<}v.\ \neg P(u)\ ) \\ \wedge\ \ \mathsf{Wellf}(<) \end{array} \right) \right)$$

$$(\mathsf{RD}) \quad \forall P.\ \left(\forall x.\ P(x) \quad \Leftarrow \quad \exists{<}.\ \exists S.\ \left(\begin{array}{l} \quad \forall u.\ (\ S(u) \ \Rightarrow\ P(u)\ ) \\ \wedge\ \ \forall v.\ \left(\begin{array}{l} \quad \neg S(v) \wedge \neg P(v) \\ \Rightarrow\ \exists u{<}v.\ \neg P(u) \end{array} \right) \\ \wedge\ \ \mathsf{Wellf}(<) \end{array} \right) \right)$$

Actually the $\mathsf{Wellf}(<)$ does not occur in Bussotti (2006) because for Fermat the Method of *Descente infinie* was actually restricted to the wellfounded ordering of the natural numbers.

Notice that, as already repeatedly expressed above, a logical formalization cannot capture a mathematical method. Moreover, as also already expressed above for Nötherian and structural induction, logical equivalence of formulas does not imply the equivalence of the formalized methods. For an interesting discussion of this difficult subject cf. Bussotti (2006), § 7.

Nevertheless, (N), (ID), and (RD) sketch methods of proof search equivalent for the working mathematician of today. Indeed: (ID)—roughly speaking—is the contrapositive of (N), which means that in two-valued logics the methods only differ in verbalization. Moreover, a proof by (ID) is a proof by (RD) when we set S to the empty predicate. Finally, a proof by (RD) can be transformed into a proof by (ID) as follows: Suppose we have proofs for the statements in the conjunction of the premise of (RD). The proofs of $\forall u.\ (\ S(u) \ \Rightarrow\ P(u)\ )$ and $\forall v.\ \left(\begin{array}{l} \quad \neg S(v) \wedge \neg P(v) \\ \Rightarrow\ \exists u{<}v.\ \neg P(u) \end{array} \right)$ give a proof of $\forall v.\ \left(\begin{array}{l} \quad \neg S(v) \wedge \neg P(v) \\ \Rightarrow\ \exists u{<}v.\ (\neg S(v) \wedge \neg P(u)) \end{array} \right)$. Instantiating the P in (ID) via $\{P \mapsto \lambda z.\ (S(z) \vee P(z))\}$, the latter proof can be schematically transformed into a proof of $\forall x.\ (S(x) \vee P(x))$ by (ID). And then from the proof of $\forall u.\ (\ S(u) \ \Rightarrow\ P(u)\ )$ again, we get a proof of $\forall x.\ P(x)$, as intended. Thus, in any case, the resulting proof does not significantly differ in the mathematical structure from the original one.

Notice that this is contrary to the case of Nötherian vs. structural induction, where the only transformation I see from the former to the latter (the other direction is trivial, cf. Wirth (2004), § 1.1.3) is to show that the *axiom* (S) implies $\mathsf{Wellf}(\mathsf{s})$, and then leave the application of (N) unchanged. This transformation, however, is not complete because it does not remove the application of (N), which is a *theorem* anyway.

All in all, this shows that—while structural and Nötherian induction vastly differ in practical applicability—for a working mathematician today it is not important for his proof search to be aware of the differences between Nötherian induction (N), indefinite descent (ID), and reduction-descent (RD).

4.2 Relevance for Mathematical Methods

5 Discussion

6 Conclusion

Acknowledgements

References

Serge Autexier, Christoph Benzmüller, Dominik Dietrich, Andreas Meier, Claus-Peter Wirth (2006). *A Generic Modular Data Structure for Proof Attempts Alternating on Ideas and Granularity.* 4th MKM 2005, LNAI 3863, pp. 126–142, Springer. `http://www.ags.uni-sb.de/~cp/p/pds/welcome.html (July 22, 2005).`

Jürgen Avenhaus, Ulrich Kühler, Tobias Schmidt-Samoa, Claus-Peter Wirth (2003). *How to Prove Inductive Theorems?* QUODLIBET*!*. 19th CADE 2003, LNAI 2741, pp. 328–333, Springer. `http://www.ags.uni-sb.de/~cp/p/quodlibet/welcome.html (July 23, 2003).`

Alan R. Bundy (1988). *The use of Explicit Plans to Guide Inductive Proofs.* DAI Research Paper No. 349, Dept. Artificial Intelligence, Univ. Edinburgh. Short version in: 9th CADE 1988, LNAI 310, pp. 111–120, Springer.

Alan R. Bundy (1999). *The Automation of Proof by Mathematical Induction.* Informatics Research Report No. 2, Division of Informatics, Univ. Edinburgh. Also in: Robinson & Voronkov (2001), Vol. 1, pp. 845–911.

Paolo Bussotti (2006). *From Fermat to Gauß: indefinite descent and methods of reduction in number theory.* Algorismus **55**, Dr. Erwin Rauner Verlag, Augsburg.

Pierre Fermat (1891ff.). *Œuvres de Fermat.* Paul Tannery, Charles Henry (eds.), Gauthier-Villars, Paris. `http://fr.wikisource.org/wiki/%C5%92uvres_de_Fermat (Aug. 15, 2006).`

Paul K. Feyerabend (1975). *Against Method.* New Left Books, London.

Dov M. Gabbay, Christopher John Hogger, J. Alan Robinson (eds.) (1994). *Handbook of Logic in Artificial Intelligence and Logic Programming. Vol. 2: Deduction Methodologies.* Clarendon Press.

Kurt Gödel (1931). *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.* Monatshefte für Mathematik und Physik **38**, pp. 173–198.

Kurt Gödel (1986 ff.). *Collected Works.* Solomon Feferman (ed.), Oxford Univ. Press.

Catherine Goldstein (1995). *Un Théorème de Fermat et ses Lecteurs.* Histoires de Science, Presses Universitaires de Vincennes, Saint-Denis.

Matt Kaufmann, Panagiotis Manolios, J S. Moore (2000). *Computer-Aided Reasoning: An Approach.* Kluwer.

Georg Kreisel (1965). *Mathematical Logic.* In: T. L. Saaty (ed.). Lectures on Modern Mathematics, Vol. III, pp. 95–195, John Wiley & Sons, New York.

Thomas S. Kuhn (1962). *The Structure of Scientific Revolutions.* Univ. Chicago Press.

Andreas Meier (2004). *The Proof Planners of* ΩMEGA*: A Technical Description.* SEKI-Report SR–2004–03, ISSN 1437-4447. http://www.ags.uni-sb.de/~veire/SEKI/2004/SR-2004-03/all.ps.gz (Oct. 24, 2006).

Andreas Meier, Erica Melis (2004). *Proof Planning Limit Problems with Multiple Strategies.* SEKI-Report SR–2004–04, ISSN 1437-4447. http://www.ags.uni-sb.de/~veire/SEKI/2004/SR-2004-04/all.ps.gz (Oct. 24, 2006).

J. Alan Robinson, Andrei Voronkov (eds.) (2001). *Handbook of Automated Reasoning.* Elsevier.

Tobias Schmidt-Samoa (2006c). *Flexible Heuristic Control for Combining Automation and User-Interaction in Inductive Theorem Proving.* Ph.D. thesis, Univ. Kaiserslautern. http://www.ags.uni-sb.de/~cp/p/samoadiss/welcome.html (July 30, 2006).

Jörg H. Siekmann, Christoph Benzmüller, Vladimir Brezhnev, Lassaad Cheikhrouhou, Armin Fiedler, Andreas Franke, Helmut Horacek, Michaël Kohlhase, Andreas Meier, Erica Melis, Markus Moschner, Immanuël Normann, Martin Pollet, Volker Sorge, Carsten Ullrich, Claus-Peter Wirth, Jürgen Zimmer (2002). *Proof Development with* ΩMEGA. 18th CADE 2002, LNAI 2392, pp. 144–149, Springer. http://www.ags.uni-sb.de/~cp/p/omega/welcome.html (July 23, 2003).

Christoph Walther (1994). *Mathematical Induction.* In: Gabbay &al. (1994), pp. 127–228.

Claus-Peter Wirth (2004). *Descente Infinie + Deduction.* Logic J. of the IGPL **12**, pp. 1–96, Oxford Univ. Press. http://www.ags.uni-sb.de/~cp/p/d/welcome.html (Sept. 12, 2003).

Claus-Peter Wirth (2006). *Progress in Computer-Assisted Inductive Theorem Proving by Human-Orientedness and Descente Infinie?.* SEKI-Working-Paper SWP–2006–01, ISSN 1860-5931. http://www.ags.uni-sb.de/~cp/p/swp200601/welcome.html (Aug. 16, 2006).