THE BULLETIN OF SYMBOLIC LOGIC
Volume 11, Number 2, June 2005

GÖDEL'S REFORMULATION OF GENTZEN'S FIRST CONSISTENCY PROOF FOR ARITHMETIC: THE NO-COUNTEREXAMPLE INTERPRETATION

W. W. TAIT

Abstract. The last section of "Lecture at Zilsel's" [9, §4] contains an interesting but quite condensed discussion of Gentzen's first version of his consistency proof for *PA* [8], reformulating it as what has come to be called the *no-counterexample interpretation*. I will describe Gentzen's result (in game-theoretic terms), fill in the details (with some corrections) of Gödel's reformulation, and discuss the relation between the two proofs.

1. Let me begin with a description of Gentzen's consistency proof. As had already been noted in [5], we may express it in terms of a game.[1] To simplify things, we can assume that the logical constants of the classical system of number theory, *PA*, are $\wedge$, $\vee$, $\forall$ and $\exists$ and that negations are applied only to atomic formulas. $\neg\phi$ in general is represented by the *complement* $\overline{\phi}$ of ϕ, obtained by interchanging $\wedge$ with $\vee$, $\forall$ with $\exists$, and atomic sentences with their negations. The *components* of the sentences $\phi \vee \psi$ and $\phi \wedge \psi$ are ϕ and ψ. The components of the sentences $\exists x\phi(x)$ and $\forall x\phi(x)$ are the sentences $\phi(\bar{n})$ for each numeral $\bar{n}$. A $\wedge$- or $\forall$-sentence, called a $\bigwedge$-*sentence*, is thus expressed by the conjunction of its components and a $\vee$- or $\exists$-sentence, called a $\bigvee$-*sentence*, is expressed by the disjunction of them; and so it follows that every sentence can be represented as an infinitary propositional formula built up from *prime* sentences—atomic or negated atomic sentences. Disjunctive and conjunctive sentences with the components ϕ_n (where the range of n is $1, 2$ or ω) will be denoted respectively by

$$\bigvee_n \phi_n \qquad\qquad \bigwedge_n \phi_n$$

Submitted November 29, 2004; accepted November 30, 2004.
I am grateful to Jeremy Avigad, John W. Dawson Jr., and Solomon Feferman for valuable comments on earlier drafts of this paper.

[1]This paper is an expansion of §4 of [19]. I regret that I did not know Thierry Coquand's paper when I wrote [19] and so failed to cite it.

1079-8986/05/1102-0009/$2.40

2. There is of course one well-known game $\mathcal{T}(\phi)$ associated with sentences ϕ of *PA*, played by $\bigvee$ and $\bigwedge$. Each stage of the game consists of exactly one sentence on the board, with ϕ on the board at the first stage. Let ψ be on the board at a given stage. If ψ is a prime sentence, then the game is over and is won by $\bigvee$ if the sentence is true and by $\bigwedge$ otherwise. If ψ is a $\bigwedge$-sentence, then $\bigwedge$ replaces it on the board by one of its components at the next stage; and if it is a $\bigvee$-sentence, then $\bigvee$ replaces it on the board by one of its components at the next stage. The play is over in $\leq n+1$ steps, if n is the logical complexity of ϕ. The truth of ϕ is obviously equivalent to the existence of a winning strategy for $\bigvee$ in $\mathcal{T}(\phi)$. But, as is also well-known, there may be no *effective* such winning strategy. The most elementary example of this is

$$\forall x \exists y \forall z \left[\phi(x, y) \vee \overline{\phi(x, z)}\right]$$

where $\phi(x, y)$ is decidable and $\exists y \phi(x, y)$ is not.

3. Gentzen's game $\mathcal{G}(\Gamma)$, unlike $\mathcal{T}(\phi)$, is played with nonempty finite *sets* Γ of sentences, rather than with single sentences, and the plays are infinite. The game starts with Γ on the board. Let Δ be on the board at a given stage n. If Δ consists only of prime sentences, then the set on the board at stage $n+1$ is again Δ. Assume that Δ contains some composite sentences. Then $\bigvee$ designates one of them, say ϕ. If ϕ is a $\bigwedge$ sentence, then at stage $n+1$ $\bigwedge$ moves by adding to Δ a component of ϕ and possibly dropping ϕ from the set. If ϕ is a $\bigvee$-sentence, then $\bigvee$ moves by adding to Δ a component of ϕ and possibly dropping ϕ from the set. $\bigvee$ wins the play in $\mathcal{G}(\Gamma)$ iff at some stage, the set on the board contains a true prime sentence; otherwise, $\bigwedge$ wins. A winning strategy for $\bigvee$ in $\mathcal{G}(\Gamma)$ was called by Gentzen a *reduction of* Γ.[2]

It is not hard to see that the disjunction of the sentences in Γ is true if and only if there is an *effective* reduction of Γ. The essential difference between $\mathcal{G}(\{\phi\})$ and $\mathcal{T}(\phi)$, accounting for the effectiveness of the winning strategy in the former case, is that $\bigvee$ is allowed to *keep* the designated sentence $\bigvee_n \psi_n$ on the board as well as some component of it, so that if he makes a bad choice of a component the first time, he has a chance later on to choose a different one. In fact, a winning strategy (not a very efficient one!) consists in going back infinitely often to designate each $\bigvee_n \psi_n$ that appears on the board, so that eventually all of the ψ_n are chosen.

Gentzen's first version of his consistency proof consisted in effectively constructing, from each formal deduction of a set Γ of sentences of *PA*, a reduction of Γ.[3] Such a reduction determines a well-founded tree, whose paths are precisely the plays (up to the stage at which there is a true prime

[2]Gentzen considered, not sets of sentences, but *sequents*, of the form $\phi_1, \ldots, \phi_n \Rightarrow \psi$ ($n \geq 0$). We have simplified his treatment by coding this sequent by the set $\{\overline{\phi_1}, \ldots, \overline{\phi_n}, \psi\}$.

[3]In fact, Gentzen considered a 'semi-formal' system which, on the face of it, is stronger than *PA*: he admitted as axioms finitistically verifiable equations. This seems to be the system Hilbert describes in [10]. There would be no difficulty in extending the present treatment

sentence on the board) in accordance with the winning strategy for $\bigvee$ in $\mathcal{G}(\Gamma)$. In the published version of his first proof, Gentzen assigned an ordinal $< \epsilon_0$ to each formal deduction, which turns out to be a bound on the height of the associated tree. The construction of the reduction proceeds by recursion on the ordinal. [15], at the cost of slightly obscuring (if you don't read it thoughtfully) the constructive content of Gentzen's result, recasts the construction as a cut-elimination theorem for *PA* with the ω-rule, in which the cut-free deduction obtained from the given deduction is the tree determined by Gentzen's winning strategy.[4] An original version of Gentzen's proof, which he did not publish but is now published in [3], did not assign ordinals to deductions: in place of recursion on ordinals, it uses recursion on well-founded trees (essentially the principle of bar recursion).[5]

4. Gödel describes Gentzen's proof in [9] in a way that avoids a calculus of sequents (which, as I mentioned, we have replaced by finite sets). He considers deductions of single formulas in an ordinary Hilbert-style formalization of *PA*. Assume that with each formula ϕ in the deduction we associate a certain one of its prenex normal forms

$$\exists x_1 \forall y_1 \dots \exists x_n \forall y_n A(x_i, y_j)$$

with $A(x_i, y_j) = A(x_1, y_1, \dots, x_n, y_n)$ quantifier-free and so a decidable formula. (For example, in $\neg\phi \vee \psi$, bring out all the quantifiers in ϕ first.) Then we may as well—and, in what follows, will—regard sentences of the form $A(\bar{k}_i, \bar{m}_j)$ as prime in playing the game $\mathcal{G}(\{\phi\})$.

Note that a winning strategy for $\bigwedge$ in $\mathcal{T}(\phi)$ (again, taking quantifier-free sentences as prime) is uniquely determined by n functions

$$f'_k(x_1, \dots, x_k) = y_k$$

of the preceding existentially quantified variables such that

$$\forall x_1 \dots x_n \neg A\left[x_1, f'_1(x_1), \dots, x_n, f'_n(x_1, \dots, x_n)\right]$$

so that the system $f' = \langle f'_1, \dots, f'_n \rangle$ could be regarded as a counterexample to ϕ. Gödel considers systems f', but it will be simpler for us to consider instead systems $f = \langle f_1, \dots, f_n \rangle$, where

$$f_k(x_1, y_1, \dots, x_k) = y_k$$

to this 'system.' But if we assume that any such equation is derivable in primitive recursive arithmetic, then the greater scope of his theorem is only apparent.

[4][4] contains a detailed discussion of the relation between Gentzen's proof and Schütte's cut-elimination theorem.

[5]For a discussion of the criticism of the original version of Gentzen's proof, leading to the published version, see [14, pp. 52–54].

is a function of all the preceding quantified variables and so could be a Skolem function for

$$\exists y_j \forall x_{j+1} \exists y_{j+1} \dots \exists y_n \neg A(x_i, y_j)$$

so that, if ϕ is false, then

$$\forall x_1 \dots x_n \neg A\big[x_1, f_1(x_1), \dots, x_n, f_n(x_1, f_1(x_1), \dots, x_n)\big].$$

Clearly, systems f and f' are obtainable from one another: to obtain f from f', define

$$f_k(x_1, y_1, \dots, x_k) = f'_k(x_1, \dots, x_k)$$

and to obtain f' from f, define by induction on k

$$f'_k(x_1, \dots, x_k) = f_k(x_1, f_1(x_1), \dots, x_k).$$

Whichever we start with, f and f' determine the same strategy for $\bigwedge$ in $\mathcal{T}(\phi)$.

5. If in the game $\mathcal{G}(\{\phi\})$, we restrict $\bigwedge$'s moves to those given by f, a winning strategy for $\bigvee$ effectively yields a system $F = \langle F_1, \dots, F_m\rangle$ of computable functionals such that

$$\forall f A\big[F_i(f), f_j(F_1(f), \dots, F_j(f))\big].$$

On the branch of the strategy tree determined by f, find the true sentence $A(\overline{k}_i, \overline{m}_j)$ in the top node and set $F_i(f) = k_i$. Gentzen's proof amounts to a definition of this path as a functional of f by recursion on the height α of the tree, and so the F_i are obtainable directly from this proof as α-recursive functionals. Gödel's idea is to construct F directly from the Hilbert-style deduction of ϕ.

But contrary to Gödel's assertion (p. 108) that such a system F of functionals is a reduction of ϕ, playing in accordance with the functions f (or f') constitutes a *restriction* on the play for $\bigwedge$ in $\mathcal{G}(\{\phi\})$, since it could happen that the sets $\Delta \cup \{\forall x \psi(x)\}$ and $\Delta' \cup \{\forall x \psi(x)\}$ are, respectively, an earlier and a later stage in a play, in each case with $\forall x \psi(x)$ designated. According to the strategy determined by f, the same component $\psi(\overline{n})$ must be chosen in both cases, whereas this is not required in the game $\mathcal{G}(\{\phi\})$ in general. However, it is not hard to see that $\bigvee$ can always modify his winning strategy in the restricted game by never designating $\forall x \psi(x)$ more than once, so that the apparent restriction on $\bigwedge$ never comes into play. In any case, we will briefly indicate in §13 how a winning strategy in the form of a system of functionals F for $\bigvee$, with $\bigwedge$ restricted to strategies of the form f, effectively determines a winning strategy even when $\bigwedge$ is allowed to exercise all of its options.

C. Parsons and W. Sieg observe in their introductory note [7, p. 82] that the winning strategy F for $\bigvee$ (in the restricted game) is precisely a witness for the so-called *no-counterexample interpretation*, *NCI*

$$\exists F \forall f A\big[F_i(f), f_j(F_1(f), \ldots, F_j(f))\big]$$

of ϕ, first introduced in print in [13]. Kreisel showed that, from any deduction of ϕ, one could extract a witness. His proof is not based on the game-theoretic idea behind Gentzen's consistency proof for *PA*, but rather is a corollary of Ackermann's proof, using the ϵ-substitution method [1]: Assume given a deduction of ϕ. From ϕ logically follows

$$\exists x_1 \ldots x_n A\big[x_1, f'_1(x_1), \ldots, x_n, f'_n(x_1, \ldots, x_n)\big].$$

In the ϵ-calculus, this has the form

$$A\big[t_1, f'_1(t_1), \ldots, t_n, f'_n(t_1, \ldots, t_n)\big]$$

where the t_k are ϵ-terms. Applying Ackermann's result, the ϵ-terms are eliminated from the deduction, so that t_k is replaced by some $F_k(f')$, and the resulting deduction is in primitive recursive arithmetic together with a principle of definition by transfinite recursion on the segment of ordinals up to some $\alpha < \epsilon_0$ (where α depends on the given deduction of ϕ). We shall see that the key lemma is the same in the two cases, Gödel's direct derivation of the *NCI* using Gentzen's idea and Ackermann's elimination of ϵ-terms, leading to Kreisel's derivation of the *NCI*. (See §14.)[6]

6. It is easy to see that, if there is a witness $G = \langle G_1, \ldots, G_n \rangle$ for the *NCI* of ϕ, then there is one F in *standard form*, i.e., such that for each $k \leq n$, if

$$\bigwedge_{i<k} f_i(F_1(f), f_1(F_1(f)), \ldots, F_i(f)) = g_i(F_1(g), g_1(F_1(g)), \ldots, F_i(g))$$

and

$$\bigwedge_{i<k} F_i(f) = F_i(g)$$

then

$$F_k(f) = F_k(g).$$

Namely, setting $B(x_1, \ldots, x_n) = A(x_i, f_j(x_1, f_1(x_1), \ldots, x_j))$, we have

$$\exists x_1 \leq G_1(f) \ldots \exists x_n \leq G_n(f) B(x_1, \ldots, x_n).$$

Successively define $F_i(f)$ to be the least $x_i \leq G_i(f)$ such that

$$\exists x_{i+1} \leq G_{i+1}(f) \ldots \exists x_n \leq G_n(f) B(F_1(f), \ldots, F_{i-1}(f), x_i, \ldots, x_n).$$

[6]A direct proof of the *NCI* for *PA* based on that lemma is given in the unpublished manuscript [20] dating from the early 1960's and listed among the references in [18] as "To Appear."

7. To obtain the no-counterexample interpretation directly, we need to obtain the witness of the *NCI* of the conclusion of each inference in the given deduction from witnesses of the *NCI*'s of its premises. Since a Hilbert-style deduction of a sentence may contain steps which are open formulas $\psi(\vec{x})$, we must understand by a witness for the *NCI* of this formula a sequence of functionals that also depend upon the parameters $\vec{x}$. Gödel states that the only non-trivial case is modus ponens: from ϕ and $\phi \longrightarrow \psi$ (i.e., $\overline{\phi} \vee \psi$), infer ψ.

Certainly he is right that the axioms and rules of inference other than modus ponens and mathematical induction are quite trivial. In the case of a deduction of ϕ involving neither modus ponens or mathematical induction, witnesses for the *NCI* of ϕ can be built by means of definition by (decidable) cases from functionals of the form $L(h) = t$, where t is a term of *PA* extended by numerical function variables. To see the necessity of definition by cases, consider a deduction of $\forall x A(x) \vee \forall y B(y) \longrightarrow \forall z C(z)$ from $\forall x A(x) \longrightarrow \forall z C(z)$ and $\forall y B(y) \longrightarrow \forall z C(z)$. So we assume that we have witnesses F and G for the *NCI* of the premises:

$$A(a) \longrightarrow C(F(a)) \qquad B(b) \longrightarrow C(G(b))$$

from which we get the witness H for the conclusion

$$A(a) \vee B(b) \longrightarrow C(H(a,b))$$

by

$$H(a,b) = \begin{cases} F(a) & \text{if } A(a), \\ G(b) & \text{otherwise.} \end{cases}$$

It is shown in [18, §6] that, in fact, the functionals built up in this way suffice for the *NCI* of sentences proved without use of mathematical induction. This follows from the fact that they suffice for the elimination of ϵ-terms in this case.[7] Notice that the elimination of definition by cases from the definition of the witness for the *NCI* of ϕ yields the familiar form

$$\bigvee_{h_1<k_1} \cdots \bigvee_{h_n<k_n} A\left[t_{i,h_i}, f_j(t_{1,h_1}, \ldots, t_{j,h_j})\right]$$

where the t_{i,h_i} are terms of *PA* supplemented by the function symbols f_j.

[7]In terms of our present direct treatment of modus ponens, the ordinals α_L considered in the treatment of modus ponens in section 10 are finite for such functionals L, and so 2^{α_L} is also finite. But recursion on a finite ordinal is obviously reducible to definition by cases. Our reduction in the last section of a witness $G = \langle G_1, \ldots, G_n\rangle$ to one, F, in standard form involved the use of the least number operator; but when the G_i are all defined from terms by definition by cases, it is easy to see that we can choose F with the F_i also so definable.

8. Concerning the construction of a witness for the *NCI* of ψ from witnesses for the *NCI*'s of ϕ and $\phi \longrightarrow \psi$, there seems to be only one natural way to go. I will illustrate it with the case in which ϕ and ψ have the prenex forms $\exists x \forall y \exists z \forall u A(x, y, z, u)$ and $\exists v \forall w B(v, w)$, respectively, so that $\neg\phi \vee \psi$ has the form $\forall x \exists y \forall z \exists u \exists v \forall w[\neg A(x, y, z, u) \vee B(v, w)]$. Thus the *NCI*'s of ϕ and $\neg\phi \vee \psi$ are of the form

$$A\big[F_1(f), f_1(F_1(f)), F_2(f), f_2(F_1(f), F_2(f))\big]$$
$$\neg A\big[g_1, G_1(g), g_2(G_1(g)), G_2(g)\big] \vee B\big[G_3(g), g_3(G_1(g), G_2(g), G_3(g))\big]$$

where we may assume these are in standard form. We may restrict g_3 to functions that depend only on the last argument, so that the second formula can be rewritten as

$$\neg A\big[g_1, G_1(g), g_2(G_1(g)), G_2(g)\big] \vee B\big[G_3(g), g_3(G_3(g))\big].$$

We can solve the equations

$$g_1 = F_1(f),\ \ f_1(g_1) = G_1(g),\ \ g_2(f_1(F_1(f))) = F_2(f)$$
$$f_2(g_1, g_2(G_1(g))) = G_2(g)$$

one-by-one from the left, substituting the solution in the subsequent equations, obtaining g_1 as a function of f_1, g_2, f_2, g_3, then f_1 as a function of g_2, f_2, g_3, then g_2 as a function of f_2, g_3 and, finally, f_2 as a function $G(g_3)$ of g_3. Then $B[G(g_3), g_3(G(g_3))]$, a witness for the *NCI* of ψ, is obtained by modus ponens.[8]

The first equation is an explicit definition. The remaining ones, ignoring parameters, have the form

$$h(L(h)) = K(h)$$

where, because the *NCI*'s are in standard form,

$$L(h) = L(h') \longrightarrow K(h) = K(h').$$

h is being represented here as a numerical function of one variable, whereas in fact the f_i and g_i are in general functions of more than one variable; but such functions can of course be coded primitive recursively as functions of one variable. Similarly, numerical-valued functionals of an argument $(f_1, \ldots, f_m, k_1, \ldots, k_n)$ consisting of numerical functions and numbers, can be primitive recursively coded as numerical-valued functionals of one numerical function of a single argument.

[8][12, Remark 3.9] notes that the solution of the corresponding system of equations for ϕ a Π^0_3 sentence $\forall x \exists y \forall z A(x, y, z)$ is the same system that is solved by bar recursion in [16] to obtain the *Dialectica* interpretation of

$$\forall x \neg\neg\exists y \forall z A(x, y, z) \longrightarrow \neg\neg\phi.$$

Kohlenbach uses the same construction to obtain the *NCI* for ψ from witnesses of the *NCI*s of ϕ and $\phi \longrightarrow \psi$ in this case.

9. To solve these equations, define the sequence $\langle h_n \mid n < \omega\rangle$ of approximations to a solution for this equation by $h_0(m) = 0$ for all m and

$$h_{n+1}(m) = \begin{cases} K(h_n) & \text{if } m = L(h_n), \\ h_n(m) & \text{otherwise.} \end{cases}$$

It is easy to show that $h_n(m) \neq 0$ implies that $h_n(m) = h_{n+k}(m)$ for all k. We need to infer from this property that, for some n,

$$L(h_n) = L(h_{n+1}).$$

For then $h = h_{n+1}$ is the desired solution for the equation. n itself is a functional $n = N(b)$ of the remaining parameters b (which I have been hiding).

10. Classically, the continuity of L on Baire space, which just follows from the assumption that it is computable, yields an n such that $L(h_{n+m}) = L(\lim_{k\to\infty} h_k)$ for all m. But we want more information about N and we have more about L than its continuity. It is in this context that Gödel appeals to "Souslin's schema" (a.k.a. Brouwer's Bar Theorem). I quote [9, §19]:

> The proof for [$\phi \longrightarrow \psi$] goes as follows: We can assign ordinals of the second number class to the functionals that are defined in a finitary way (that is, computable for every concretely presented f) (Souslin's schema). The reducing function for ψ is defined by transfinite induction on the ordinal of the reducing function for ϕ, and if we compute the ordinal that is assigned to the reducing function for ψ, then that for ϕ occurs in the exponent. It is therefore exactly the inference of introducing a certain new ordinal by recursion on an ordinal already recognized as such and then again applying recursive definition on this new [ordinal].

He is right that, for his proposed proof of the *NCI* of every prenex formula ϕ which is a theorem of *PA*, it suffices to restrict the witnesses F of *NCI*s to those such that each F_i has an ordinal, i.e., its associated tree of unsecured sequences is well-founded. But his equation of functionals "defined in a finitary way" with functionals that are computable for every concretely presented [argument] f is misleading, since there are partial computable functionals, defined for all computable f (which presumably includes all the concretely presented ones) for which no ordinal can be assigned—the tree of unsecured sequences is not well-founded. Souslin's schema applies to total continuous functionals (on Baire space) in the classical sense. It was because this schema is *not* valid in general for constructive functionals defined on computable arguments that Brouwer stated it for functionals defined on free choice sequences (although I can understand Brouwer's argument for the well-foundedness of the tree of unsecured sequences only as a partial statement of what the notation for free choice sequences really means).

Also, Gödel's statement that the reducing function for ψ (i.e., in his reformulation, the witness of the *NCI* of ψ) is obtained by recursion on the ordinal of the reducing function for ϕ is incorrect in two respects. First, only in the case that ϕ is Π^0_2 or Σ^0_2 is it the case that the reducing function for ψ depends only on the reducing function for ϕ. For example, with ϕ and ψ as above, the third of the equations we need to solve has the form $g_2(G_1(g)) = F_2(f)$, where G_1 is part of the witness for the *NCI* of $\phi \longrightarrow \psi$, i.e., $\neg\phi \vee \psi$, not of ϕ. Second, the equation is solved (as we shall see) not by recursion on the ordinal α of $\lambda g_2 G_1(g)$, but by recursion in 2^α.

In the first published treatment of the *NCI* for modus ponens, in [12], the functional N is defined directly by the principle of bar recursion. As noted in [20] and by Kohlenbach, this yields the witness H of ψ as a function of the witnesses F and G of the *NCI*s of ϕ and $\phi \longrightarrow \psi$—the construction of H is *uniform in* F and G. But it does not directly yield the ordinals of the functionals H_i as a function of the ordinals of the F_i and G_i (nor, one should add, was it the purpose of Kohlenbach's paper to do so). This method of constructing N parallels the unpublished version of Gentzen's first consistency proof for *PA*, at least as this is presented in [3]. In this version, a reduction of Γ is obtained from a deduction of Γ by recursion on the reductions (as well-founded trees) of the premises from which Γ is obtained.

The method of constructing H in [20], drawing on the machinery set up in [17], is not uniform in F and G; but it does yield the ordinal of the functionals in H from those of the functionals in F and G, and so more parallels the *published* version of Gentzen's proof. Moreover, in this proof, reference to functionals may be regarded as a shorthand for speaking about numerical functions, so that speaking of "functionals that are defined in a finitary way" makes some sense. Namely, the functionals L from which we need to construct the corresponding functional N have this property: we can associate with such an L a numerical function Φ_L, an ordinal $\alpha_L < \epsilon_0$, and function Ψ_L from the natural numbers into the segment of ordinals $< \alpha_L$ such that, writing $\overline{f}(n)$ for the code of the sequence $\langle f(0), \ldots, f(n-1)\rangle$,

$$\Phi_L(\bar{f}(n)) = 0 \longrightarrow \Psi_L(\bar{f}(n+1)) < \Psi_L(\bar{f}(n))$$
$$\Phi_L(\bar{f}(n)) \neq 0 \longrightarrow L(f) = \Phi_L(\bar{f}(n+m)) - 1, \text{ for all } m.$$

In fact, representing the ordinals $< \epsilon_0$ in the usual way by natural numbers, Φ_L and Ψ_L are definable in the extension of primitive recursive arithmetic *PRA* obtained by adding definition by recursion on α_L. For the witnesses L of the *NCI* of formulas deducible in *PA* without using modus ponens or mathematical induction, it is easy to see that $\alpha_L < \omega$. For functionals L definable by transfinite recursion on an ordinal $\beta \geq \omega$, α_L will be $< \beta^\omega$ and Φ_L and Ψ_L are definable in *PRA* with recursion on ordinals $< \beta^\omega$. (For details, see Theorem 1 of [17].) For example, if L is defined by the primitive recursion

$$L(h, 0) = K(h) \qquad L(h, n+1) = M(h, n, L(h, n))$$

then α_L is bounded by $\alpha_K + (\alpha_M \times \omega)$.

When L is so represented in terms of Φ_L, α_L, and Ψ_L, it is easy to define r_n (as a function of n and the other parameters) as the least number k such that $\Phi_L(\bar{h}_n(k)) = 0$ by recursion on α_L. Let $m_{n,1}, \dots, m_{n,s_n}$ be the increasing sequence of numbers $m < r_n$ such that $h_n(m) = 0$, and let $\gamma_{n,i} = \Psi_L(\bar{h}_n(m_{n,i}))$. Set

$$\gamma_n = 2^{\gamma_{n,1}} + \dots + 2^{\gamma_{n,m_{n,s_n}}} < 2^{\alpha_L}.$$

If $L(h_n) \neq L(h_{n+1})$, then $\gamma_{n+1} < \gamma_n$. So we may define by induction on 2^{α_L} the function N_k such that $N_k(b)$ is the least number x such that $L(h_{k+x}) = L(h_{k+x+1})$. The required function N then is just N_0.[9]

11. Returning to the above quote from [9, §19], notice that Gödel reverses the true situation: He asserts that the ordinal α_L of a β-recursive functional L is in general exponential in β and, as we have already noted, that the solution of the equation $h(L(h)) = K(h)$ is obtained by recursion on α_L.[10] One should recall that the quoted passage is from notes that he wrote *for himself* as a basis for a lecture and therefore not expect the same level of care as in a published paper. However, another possibility in the case of the first inaccuracy is that he confused two notions of recursive definition of functionals on $\beta \geq \omega$, one predicative and the other impredicative. In the predicative sense, a functional F is defined by giving its numerical value $F(h, x)$ in terms of its numerical value $F(h, k(h, x))$, where $k(h, x) \prec x$ and $\prec$ is the standard well-ordering of the natural numbers with order type β. For functionals L defined using only elementary operations and predicative recursion on β, $\alpha_L < \beta^\omega$. On the other hand, if we admit impredicative recursion, allowing $F(h, x, y)$ to be defined in terms of $\lambda u F(h, k(h, x), u)$, then, indeed, we may have $\alpha_L = \omega^\beta$. But notice that, in our construction of witnesses for the *NCI* of theorems of *PA*, we have used only predicative recursions.

With respect to uniformity, note that, in contrast with [12], we obtain the witness H for the conclusion of modus ponens, not as a function of the witnesses F and G of the premises, but in terms of the representations $\langle \Phi_L, \alpha_L, \Psi_L \rangle$ of functionals L successively derived from them.

[9] [2] solves the equation $L(h_n) = L(h_{n+1})$ in essentially the same way as [17], as an instance of constructing a finite fixed point of an *update procedure*. The update procedure in this case is $F(h) = \langle L(h), K(h) \rangle$.

[10] Of course Gödel asserts this when L is the reducing function for ϕ and, as we have noted, this makes sense only if ϕ is of at most two-quantifier form. But even in this case, the assertion is in general false.

12. Writing on p. 110 that the whole difficulty of the proof of the *NCI* of theorems of *PA* lies with modus ponens, Gödel dismisses the case of mathematical induction by noting that, if we have witnesses for the *NCI* of the premises

$$\phi(0) \qquad \phi(x) \longrightarrow \phi(x+1)$$

then, by applying modus ponens n times, we have a witness for the *NCI* of $\phi(\overline{n})$ and so, by induction, one for $\phi(x)$. But this argument won't do. As we have seen, passing from $\phi(\overline{n})$ to $\phi(\overline{n+1})$ can involve ascending from an ordinal α to 2^{α}_{k}, where $\phi(x) \in \Sigma^0_{2k}$, $2^{\alpha}_{0} = \alpha$ and $2^{\alpha}_{m+1} = 2^{2^{\alpha}_{m}}$. So just two applications of mathematical induction, on this analysis, could get us already to ϵ_0.[11]

I shall illustrate the treatment of mathematical induction with the case of $\phi(x) = \exists y \forall z A(x, y, z)$. We can assume that, corresponding to the premises of mathematical induction, we have

$$A\big[0, F'(f), f(0, F'(f))\big]$$
$$A\big[x, g(x), G(x, f, g)\big] \longrightarrow A\big[x+1, F''(x, f, g), f(x, F''(x, f, g))\big]$$

where the witnesses are in standard form and we have restricted f to depend only on x and $F''(x, f)$. If we define $F(0, f, g) = F'(f)$ and $F(x+1, f, g) = F''(x, f, g)$, then

$$A\big[0, F(0, f, g), f(0, F(0, f, g))\big]$$
$$A\big[x, g(x), G(x, f, g)\big] \longrightarrow A\big[x+1, F(x+1, f, g), f(x, F(x+1, f, g))\big].$$

Explicitly define g in terms of the unkown functions f_1 and g_1 by

$$g(x) = F(x, f_1, g_1)$$

and, using the fact that the witness $\langle G, F''\rangle$ is in standard form, solve the equation

$$f_1(x, F(x, f_1, g_1)) = G(f, g).$$

This has again the form $h(L(h)) = K(h)$ with $L(h) = L(h') \longrightarrow K(h) = K(h')$ and so the method of sections 9 and 10 can be applied and we can define $f_1 = \Psi(f, g_1)$ using recursion on 2^{α_F}. Define the function $\theta^x(f)$ by the impredicative primitive recursion

$$\theta^0(f)(y) = 0 \qquad \theta^{x+1}(f)(y) = F\big[y, \Psi(f, \theta^x(f)), \theta^x(f)\big]$$

(which can be reduced to predicative recursion on ω^ω). Setting $g_1 = \theta^x(f)$, $\Phi^x(f) = \Psi(f, \theta^x(f))$ and $K(x, f) = F(x, f, \theta^x(f))$, we have $g = \theta^{x+1}(f)$ and

$$A\big[0, K(0, f), f(0, K(0, f))\big]$$

[11] Alas, in [19] I accepted Gödel's treatment of mathematical induction, although I knew the correct treatment over forty years ago.

$$A\big[x, K(x, \Phi^x(f)), \Phi^x(f)(x, K(x, \Phi^x(f)))\big]$$
$$\longrightarrow A\big[x+1, K(x+1, f), f(x+1, K(x+1, f))\big].$$

Then $A[x, K(x, f), f(x, K(x, f))]$ follows by mathematical induction with substitution in parameters, which is reducible to the rule of mathematical induction [17, VI].[12]

13. To see how a witness for the the *NCI* of ϕ yields a winning strategy for $\bigvee$ in $\mathcal{G}(\{\phi\})$, consider the simple case

$$\phi = \exists x \forall y \exists u \forall v A(x, y, u, v)$$

and let $F = \langle G, H\rangle$ be a witness for its *NCI*. $J(m, n) = 1/2[(m+n)(m+n+1)]+m$ is the position of $\langle m, n\rangle$ in the ordering of pairs of natural numbers according to least sum $m+n$ and, within that, according to least first member m. We can assume that functionals K of two function variables are coded by functionals K' of one argument, where $K(f, g) = K'[\lambda n J(f(n), g(n))]$.

A winning strategy for $\bigvee$ in $\mathcal{G}(\{\phi\})$ determined by F is as follows. Let $m = J(i, j)$. At stage $4m$ $\bigvee$ designates ϕ and adds $\forall y \exists u \forall v A(\bar{\imath}, y, u, v)$. At stage $4m+1$, he designates this sentence. After $\bigwedge$'s response $\exists u \forall v A(\bar{\imath}, \bar{b}_i, u, v)$, $\bigvee$ designates this sentence at stage $4m+2$ and adds $\forall v A(\bar{\imath}, \bar{b}_i, \bar{\jmath}, v)$. At stage $4m+3$, he designates this sentence so that $\bigwedge$'s must choose some $A(\bar{\imath}, \bar{b}_i, \bar{\jmath}, \bar{c}_j)$. At stage $h(m) = 8m(2m-1)$, sentences $A[\bar{\imath}, \bar{b}_i, \bar{\jmath}, \bar{c}_j]$ are on the board for all $i, j < m$. If $\Phi_{G'}(\langle J(b_0, c_0), \ldots, J(b_{m-1}l, c_{m_1})\rangle) > 0$ and $\Phi_{H'}(\langle J(b_0, c_0), \ldots, J(b_{m-1}l, c_{m_1})\rangle) > 0$, then choose f and g such that $f(i) = b_1$ and $g(j) = c_j$ for all $i, j < m$. Then at stage $J(G(f, g), H(f, g)) + 3$, if not before, the game is won for $\bigvee$. So, by induction on $\alpha_{G'} + \alpha_{H'}$, $\bigvee$ wins.

14. As I indicated at the end of section 5, the solution of the equation $L(h_n)) = L(h_{n+1})$ using recursion on 2^{α_L} arises also in connection with the ϵ-substitution method for *PA*.[13]

The essence of the substitution method is defining functions h satisfying a finite set of conditions

$$A(x, L_i(h)) \longrightarrow A(x, h(x))$$

[12] Assume $B(0, f)$ and $B(x, \xi^x(f)) \longrightarrow B(x+1, f)$. Define $\eta^0(f) = f$ and $\eta^{x+1}(f) = \xi^x(\eta^x(f))$. Then $B(0, \eta^{n-0}(f))$ and

$$x < n \longrightarrow \big[B(x, \eta^{n-x}(f)) \longrightarrow B(x+1, \eta^{n-x-1}(f))\big]$$

by substitution. So by mathematical induction, $x \leq n \longrightarrow B(x, \eta^{n-x}(f))$. Apply this now to $x = n$.

[13] In fact, it is a special case of Theorem 3 of [17], which is called there the 'principal lemma of the substitution method,' and is applied in [18] to obtain (essentially) Ackermann's [1] proof of the consistency of *PA*.

$$A(x, L_i(h)) \longrightarrow h(x) \leq L_i(h)$$

for $i < k$, where A is quantifier-free and x does not occur in the $L_i(h)$ (although function parameters other than h in general do). These conditions are derived from the *critical formulas* associated with the ϵ-term $\epsilon y A(x, y)$ in a given deduction in the ϵ-calculus of a sentence, where $h(x)$ represents this ϵ-term. (In general, x is a finite sequence of variables.) Let

$$L(h) = max\{L_i(h) \colon i < k\}$$

and define $h_0(x) = 0$ and

$$h_{n+1}(x) = \begin{cases} \mu y_{\leq L(h_n)} A(x, y) & \text{if } \exists y_{\leq L(h_n)} A(x, y), \\ 0 & \text{otherwise.} \end{cases}$$

Again, $h_n(x) > 0$ implies that $h_n(x) = h_{n+k}(x)$ for all k, and so, as above, we obtain $n = N(b)$ such that $L(h_n) = L(h_{n+1})$ by recursion on 2^{α_L}. $h = h_{n+1}$ will then satisfy the set of conditions.

REFERENCES

[1] W. Ackermann, *Zur Widerspruchsfreiheit der Zahlentheorie*, ***Mathematische Annalen***, vol. 117 (1940), pp. 162–194.

[2] J. Avigad, *Update procedures and the 1-consistency of arithmetic*, ***Mathematical Logic Quarterly***, vol. 48 (2002), pp. 3–13.

[3] P. Bernays, *On the original Gentzen-Takeuti reduction steps*, ***Institutionism and proof theory*** (A. Kino, J. Myhill, and R. Vesley, editors), North-Holland, Amsterdam, 1970, pp. 409–418.

[4] W. Buchholz, *Explaining the Gentzen-Takeuti reduction steps*, ***Archive for Mathematical Logic***, vol. 40 (2001), pp. 255–272.

[5] T. Coquand, *A semantics of evidence for classical arithmetic*, ***The Journal of Symbolic Logic***, vol. 60 (1995), pp. 325–337.

[6] J. Dekker (editor), ***Recursive function theory***, Proceedings of Symposia in Pure Mathematics, vol. 5, American Mathematical Society, Providence, 1962.

[7] S. Feferman, J. W. Dawson, W. Goldfarb, C. Parsons, and R. M. Solovay (editors), ***Kurt Gödel: Collected works, Vol. III***, Oxford University Press, Oxford, 1995.

[8] G. Gentzen, *Die Widerspruchfreheit der reinen Zahlentheorie*, ***Mathematische Annalen***, vol. 112 (1936), pp. 493–565.

[9] K. Gödel, *Lecture at Zilsel's*, In Feferman et al. [7], pp. 87–133.

[10] D. Hilbert, *Die Grundlegung der elementaren Zahlenlehre*, ***Mathematische Annalen***, vol. 104 (1930), pp. 485–565, Reprinted in part in [11].

[11] ———, ***Gesammelte Abhandlungen***, vol. 3, Springer, Berlin, 1935.

[12] U. Kohlenbach, *On the no-counterexample interpretation*, ***The Journal of Symbolic Logic***, vol. 64 (1999), pp. 1491–1511.

[13] G. Kreisel, *On the interpretation of non-finitist proofs—Part I*, ***The Journal of Symbolic Logic***, vol. 16 (1951), pp. 241–267.

[14] E. Menzler-Trott, ***Gentzens Problem: Mathematische Logik im nationalsozialistischen Deutschland***, Birkhäuser Verlag, Basel, 2001.

[15] K. Schütte, *Beweisetheoretische Erfassung der unendlichen Induktion in der Zahlentheorie*, ***Mathematische Annalen***, vol. 122 (1951), pp. 369–389.

[16] C. Spector, *Provably recursive functionals of analysis: a consistency proof of analysis by an extension of the principles formulated in current intuitionistic mathematics*, In Dekker [6], pp. 1–27.

[17] W. W. Tait, *Functionals defined by transfinite recursion*, ***The Journal of Symbolic Logic***, vol. 30 (1965), pp. 155–174.

[18] ———, *The substitution method*, ***The Journal of Symbolic Logic***, vol. 30 (1965), pp. 175–192.

[19] ———, *Gödel's unpublished papers on foundations of mathematics*, ***Philosophia Mathematica***, vol. 9 (2001), pp. 87–126.

[20] ———, *The no counterexample interpretation for arithmetic*, unpublished manuscript.

5522 S. EVERETT AVE.
CHICAGO, IL 60637, USA
E-mail: wwtx@earthlink.net