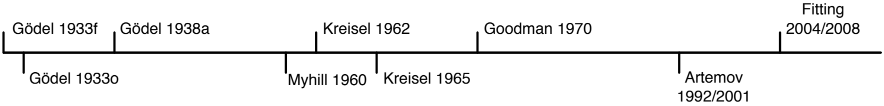
Gödel, Kreisel, and the origin of the Logic of Proofs

Explicit Paradigms in Logic and Computer Science
Bern
4-6 June 2012

Walter Dean
Department of Philosophy
University of Warwick

http://go.warwick.ac.uk/whdean

Outline



- Gödel 1933f: An interpretation of intuitionistic propositional calculus
- Gödel 1933o: The present situation in the foundations of maths.
- Gödel 1938a: Lecture at Zilsel's
- Myhill 1960: Remarks on the notion of proof
- Kreisel 1962: Foundations of intuitionistic logic
- Kreisel 1965: Mathematical logic
- Goodman 1970: A Theory of Constructions Equivalent to Arithmetic
- Artemov 1992/2001: The Logic of Proofs [LP]
- Fitting: 2004/2008: The Quantified Logic of Proofs [QLP]

Spoiler

1) Gödel and Kreisel both had systems similar to LP.
2) These systems contained quantifiers over proofs.
3) Kreisel's was inconsistent.
4) The structure of the derivation of an inconsistency is similar to that of the "Knower Paradox" (Myhill 1960, Montague 1963).
5) It relies on Constructive Necessitation (in addition to reflection and a self referential statement about provability).
6) Gödel foresaw reasons to reject Constructive Necessitation applied to *quantified* reasoning about constructive proofs.
7) LP gets it right: 1) perspicuous notation; 2) unrestricted Constructive Necessitation; 3) elimination of proof quantifiers in favor of free variables (although a little quantification is okay).

Godel 1933f ("An interpretation of intuitionistic propositional calculus")

- Idea: 1) introduce a propositional operator

$$\Box\varphi \quad \rightleftharpoons \quad \varphi \text{ is constructively provable}$$

  2) use this operator to express the clauses of the Heyting proof interpretation of IPC

- Define: $P^\circ = P$, $(\varphi \wedge \psi)^\circ = \varphi^\circ \wedge \psi^\circ$, $(\varphi \vee \psi)^\circ = \Box\varphi^\circ \vee \Box\psi^\circ$, $(\varphi \rightarrow \psi)^\circ = \Box\varphi^\circ \rightarrow \Box\psi^\circ$, $(\neg\varphi)^\circ = \neg\Box\varphi^\circ$
- S4 is the system

(T)	$\Box\varphi \rightarrow \varphi$	(K)	$\Box(\varphi \rightarrow \psi) \rightarrow (\Box\varphi \rightarrow \Box\psi)$
(4)	$\Box\varphi \rightarrow \Box\Box\varphi$	(Nec)	$\vdash \varphi \quad \therefore \quad \vdash \Box\varphi$

- Theorem:

$$\mathsf{IPC} \vdash \varphi \quad \Longleftrightarrow \quad \mathsf{S4} \vdash (\varphi)^\circ$$

- This provides a *classical* interpretation of intuitionistic validity.

Godel 1933f cont.

- Gödel observed:
  - $\mathsf{S4} \vdash \Box(\Box\varphi \rightarrow \varphi)$
  - $\mathrm{PA} \nvdash \mathsf{Prov}(\ulcorner \mathsf{Prov}(\ulcorner \bot \urcorner) \rightarrow \bot)\urcorner)$ (if it is consistent)
  - In fact, $\mathcal{N} \not\models \mathsf{Prov}(\ulcorner \mathsf{Prov}(\ulcorner \bot \urcorner) \rightarrow \bot)\urcorner)$
- So $\Box\varphi$ can't be interpreted as $\mathsf{Prov}(\ulcorner \varphi \urcorner)$ – i.e. as expressing provability "in a particular formal system."
- Rather it must represent provability "in an absolute sense" (i.e. "one can make it evident").
- On the "absolute" interpretation both

  (T) $\Box\varphi \rightarrow \varphi$
  (U) $\Box(\Box\varphi \rightarrow \varphi)$

  are valid.

Gödel 1933o: ("The present situation ...")

- Question: Is it possible to prove consistency by "unobjectionable means" – i.e. avoiding "non-constructive existence proofs, non-predicative definitions ... for it is exactly a justification for the doubtful methods we are seeking." p. 51
- Set down criteria on an "unobjectable" formal system A:
  - R1) Primitive operations must be computable, primitive relations decidable.
  - R2) Logical principles do not allow for non-constructive existence proofs.
  - R3) The application of $(\forall x)$ "is to be restricted to those infinite totalities for which we can give a finite procedure for generating all their elements" [1933o]
- Question: Does intuitionistic logic satisfy these criteria?

Gödel's 1933o: "The presentation situation ..."

Heyting's axioms ... violate the principle which I stated before, that the word "any" can be applied only to those totalities for which we have a finite procedure for generating all their elements ... For the totality of all possible proofs certainly does not possess this character, and nevertheless the word "any" is applied to this totality in Heyting's axioms as [can be seen from] "Given *any* proof for a proposition p, you can construct a reductio ad absurdum from the proposition $\neg p$". Totalities whose elements cannot be generated by a well-defined procedure are in some sense vague and indefinite as to their borders. And this objection applies particularly to the totality of intuitionistic proofs because of the vagueness of the notion of constructivity. p. 53

Gödel 1938a: "Lecture at Zilsel's"

- Different "constructive" methods of proving consistency:
  - i) Functionals of higher-type (anticipation of *Dialectica*)
  - ii) **The "modal-logical route" (refinement of 1933f)**
  - iii) Transfinite induction (Gentzen consistency proof)

Heyting's system violates all essential requirements on constructivity, but perhaps it is still to be made somehow constructive. For [by] what reason do the intuitionists recognize it [as constructive]? They are thinking of a constructive interpretation

$$p \supset q \text{ means "} q \text{ is derivable from } p \text{"}$$

[where] "derivable" . . . is understood in the constructive sense . . . that is, one has a derivation. p. 101

- Idea: axiomatize the relation

$$zBp, q \;\; \leftrightharpoons \;\; z \text{ is a derivation of } q \text{ from } p$$

Gödel 1938a: axiomatic system

Axioms: for example transitivity of implication: $zBp, q \,\&\, uBq, r \rightarrow f(z,u)Bp, r$.

Other axioms: $zB\varphi(x,y) \rightarrow \varphi(x,y), uBv \rightarrow u'B(uBv)$; furthermore, if q has been proved and a is the proof, so that "aBq" is to be written down, then as above $aB[(u){\sim}uB(0=1)]$ would be provable.

- $u, v, \ldots$ are intended as variables over constructive proofs.
- $\varphi, \psi, \ldots$ are formulas constructed from $zB(\varphi, \psi)$, connectives and quantifiers over proofs.
- Notational abuse: $zB(\varphi) =_{df} zB(\top, \varphi)$
- Axioms:
  - G1: $(zB(\varphi, \psi) \wedge uB(\psi, \chi)) \rightarrow f(z,u)B(\varphi, \chi)$
  - G1′: $(zB(\varphi \rightarrow \psi) \wedge uB(\varphi)) \rightarrow f(z,u)B(\psi)$
  - G2: $zB(\varphi) \rightarrow \varphi$
  - G3: $uB(\varphi) \rightarrow u'B(uB(\varphi))$
  - rG4: $\vdash \varphi \quad \therefore \quad \vdash aB\varphi$ (where a is a derivation of φ)

Gödel 1938a: consistency proof

- Let $\bot =_{df} (0 = 1)$, $\neg\varphi =_{df} \varphi \to \bot$.
- We can reason in Gödel's system as follows:
  1) $xB(\bot) \to \bot$ G2
  2) $aB(xB(\bot) \to \bot)$ G4
  3) $a'B((\forall x)(xB(\bot) \to \bot)$ **???**
     $\equiv a'B((\forall x)(\neg xB(\bot))$
- Question: What justifies the step from 2) to 3)?
- Issues about the proof/system:
  1) Gödel doesn't state UG as a rule.
  2) $(\forall x)$ isn't introduced at the beginning of the fmla.
  3) Per R3), UG wouldn't be licensed **unless the class of (constructive, absolute) proofs was finitely generable**.
  4) Where does a' come from? (Gödel doesn't make clear that that Constructive Necessitation is a *derived* principle.)

Kriesel 1962/65: The theory of constructions

- Language (slightly simplified):
  - $t, u, v, \ldots$ variables over "constructions"
  - these are applicable and abstractable: $t(u_1, \ldots, u_n)$, $\lambda u.t$
  - operations on constructions: e.g. $t \cdot u, t_0, t_1, \ldots$
  - 0 true, 1 falsity
  - $\boldsymbol{\pi(t, u, v) = 0} \quad \leftrightharpoons \quad$ **t a proof that $u = v$**
- Interpretation of HPC (e.g.):
  - $\Pi(t; \langle F \rangle)$ is defined inductively in terms of F

    $$\Pi(t; \langle F \to G \rangle) =_{df} \pi(t_1, \lambda x.\Pi(x; F) \supset \Pi(t_2(x); G), \lambda x.0) = 0$$
- Derived principles:
  - $\Pi(t; \langle \Pi(u; \langle F \rangle) \rangle) \supset \Pi(\psi_F(t; u); \langle F \rangle)$
  - $\Pi(t; \langle F \rangle) \supset (\Pi(s; \langle F \to G \rangle) \supset \Pi(s \cdot t; \langle G \rangle))$
- Results (*sketched*):
  - ≈ Embed. + Lifting: If HPC $\vdash F$, then C $\vdash \Pi(t; \langle F \rangle)$ for some t.
  - ≈ Arithmetical soundness: If we replace $\Pi(t; \langle F \rangle)$ with Prov$(t^*, \ulcorner F \urcorner)$, then the axioms of C are true in $\mathcal{N}$.

Myhill 1960 "Some Remarks on the Notion of Proof"

- In light of 1933f, Myhill considers whether "absolute provability" should be treated as an operator or as a predicate.

Proposition

Let $T \supseteq$ Q be a $\mathcal{L}_a \cup \{B(x)\}$-theory satisfying

$$\text{(T)} \quad B(\ulcorner\varphi\urcorner) \rightarrow \varphi \qquad \text{(Nec)} \quad T \vdash \varphi \quad \therefore \quad T \vdash B(\ulcorner\varphi\urcorner).$$

Then T is **inconsistent**.

1) $T \vdash \delta \leftrightarrow \neg B(\ulcorner\delta\urcorner)$ for some δ via the Diagonal Lemma
2) $T \vdash B(\ulcorner\delta\urcorner) \rightarrow \delta$ T
3) $T \vdash \neg B(\ulcorner\delta\urcorner)$
4) $T \vdash \delta$
5) $T \vdash B(\ulcorner\delta\urcorner)$ Nec 4)
6) $T \vdash \bot$

Goodman 1970: "A theory of constructions equivalent to arithmetic"

"A theory of constructions is a type-free and logic-free theory directly about the rules and proofs which underlie constructive mathematics. The idea of such a theory as a basis for mathematics is implicit in many of the intuitionistic writings. For example, in Heyting (1930), an informal theory of this sort is tacitly used for the interpretation of the logical connectives." p. 101

- The basis of Goodman's system is combinatory logic (or untyped lambda-calculus) plus a primitive proof predicate:

$$\pi(u, v) = \top \quad \rightleftharpoons \quad v \text{ is a proof that for } \underline{\text{all}}\ z,\ uz = \top$$

- Goodman eliminates type restrictions implicit in Kreisel's treatment and adopts an unrestricted reflection principle.

Goodman 1970 (2)

- It is possible to construct a sentence (construction) d which "says of itself" that it is not provable.
  1) $(\pi(yz, w) \supset \bot)$ "w is not a proof of yz"
  2) $\pi(\pi(yz, w) \supset \bot), z)$ "z is a proof that 1) is unprovable"
  3) $h(yz) = \lambda y.\lambda z.(\pi(\pi(yz, w), z) \supset \bot)$
  4) Find d such that $dz \equiv h(dz)$ by taking

$$d = \lambda z.(\lambda y.(h(yy)z)(\lambda y.(h(yy)z))$$

- This leads to a *contradiction* (assuming reflection – i.e. $\pi(u, v) = \top \vdash uv = \top$).
- Claim: Goodman's proof of this fact is essentially the same as Myhill's except that
  - Self reference is achieved by the Paradoxical Combinator instead of the Diagonal Lemma.
  - Constructive Necessitation is used instead of the rule Nec (or Σ^0_1-completeness).

Fitting 2004/2008: The Quantified Logic of Proofs (QLP)

- The class of QLP *proof terms* is given by

$$t := x_i \mid a_i(x_{i_1}, \ldots, x_{i_n}) \mid !t \mid t_1 \cdot t_2 \mid t_1 + t_2 \mid \langle t \forall x \rangle$$

  - $x_1, x_2, x_3, \ldots$ are *proof variables*
  - $a_1(\vec{x}), a_2(\vec{x}), a_3(\vec{x}), \ldots$ are *primitive proof terms*
  - $!$, $\cdot$, $+$ and $\langle \cdot \forall \cdot \rangle$ are *proof operations*

- The class of QLP formulas is given by

$$\varphi := P_i \mid F \wedge G \mid F \vee G \mid F \rightarrow G \mid \neg F \mid t : F \mid (\forall x)F \mid (\exists x)F$$

- Some characteristic validities:
  - $(\forall x)(x : F \rightarrow !x : x : F)$
  - $(\forall x)(\forall y)(\exists z)[x : (F \rightarrow G) \rightarrow (y : F \rightarrow z : G)]$
  - $(\forall x)(x : F \rightarrow F) \equiv (\exists x)x : F \rightarrow F$

(Q)LP (axioms)

LP0	all tautologies of classical propositional logic
LP1	$t : (F \to G) \to (s : F \to t \cdot s : G)$
LP2	$t : F \to F$
LP3	$t : F \to !t : t : F$
LP5	$t : F \to t + s : F$ and $s : F \to t + s : F$
QLP1	$(\forall x)F(x) \to F(t)$
QLP2	$(\forall x)(F \to G(x)) \to (F \to (\forall x)G(x))$
QLP3	$F(t) \to (\exists x)F(x)$
QLP4	$(\forall x)(F(x) \to G) \to ((\exists x)F(x) \to G)$

- Usual definition of FV(F).
- Usual free-variable restrictions for QLP1-QLP4.
- Compare Yavorsky 2001/2002.

QLP (rules)

- A *primitive term specification* is a mapping $\mathcal{P}$ s.t. $\mathcal{P}(a(\vec{x}))$ is a set of QLP axioms with free variables among $\vec{x}$.
- QLP rules:
  - Modus Ponens
  - Axiom Necessitation: if $F(\vec{x}) \in \mathcal{P}(a(\vec{x}))$,
    then $\Gamma \vdash a(\vec{x}) : F(\vec{x})$
  - Universal Generalization [UG]:

$$\frac{\Gamma \vdash F(x)}{\Gamma \vdash (\forall x) F(x)} \quad x \notin \mathsf{FV}(\Gamma)$$

  - Justified Universal Generalization [JUG]:

$$\frac{\vec{s} : \vec{\Gamma} \vdash t(x) : F(x)}{\vec{s} : \vec{\Gamma} \vdash \langle t(x) \forall x \rangle : (\forall x) F(x)} \quad x \notin \mathsf{FV}(\vec{s} : \vec{\Gamma})$$

where $\vec{s} : \vec{\Gamma} = s_1 : \psi_1, \ldots, s_n : \psi_n$.

Necessitation versus Constructive Necessitation

- In S4 we have the <u>Necessitation Rule</u>

$$\frac{\Box\Gamma \vdash \varphi}{\Box\Gamma \vdash \Box\varphi}$$

- In LP & QLP we have <u>Constructive Necessitation *Theorem*</u>

$$\frac{\vec{s} : \vec{\Gamma}, \vec{y} : \Delta \vdash \varphi}{\vec{s} : \vec{\Gamma}, \vec{y} : \vec{\Delta} \vdash t(\vec{s}, \vec{y}) : \varphi}$$

  for some term $t(\vec{s}, \vec{y})$ constructed inductively from the derivation $\vec{s} : \vec{\Gamma}, \vec{y} : \Delta \vdash \varphi$.

- As a corollary, in QLP we have

$$\frac{\vec{s} : \vec{\Gamma}, \vec{y} : \Delta \vdash \varphi}{\vec{s} : \vec{\Gamma}, \vec{y} : \vec{\Delta} \vdash (\exists x)x : \varphi}$$

Reconstructing Gödel's consistency proof in QLP

1)	$x : \bot \to \bot$	LP2
2)	$r(x) : (x : \bot \to \bot)$	Axiom Necessitation
3)	$r(x) : (\forall x)(x : \bot \to \bot)$	UG???
4)	$r(x) : (\forall x)(x : \bot \to \bot)$	**NO** – this is a misapplication
5)	$(\forall x)r(x) : (x : \bot \to \bot)$	UG
6)	$\langle r(x)\forall x\rangle : (\forall x)(x : \bot \to \bot)$	JUG, **3** -**NO**)
7)	$\langle r(x)\forall x\rangle : (\forall x)(x : \bot \to \bot)$ $\equiv \langle r(x)\forall x\rangle : (\forall x)\neg(x : \bot)$	JUG, **2**)

- Uniform Barcan Formula:

$$(\forall x)t(x) : F(x) \to \langle t\forall x\rangle : (\forall x)F(x)$$

- JUG is weaker than UBF.
- But one of JUG or UBF is **required** to derive 4).

Reconstructing Myhill's proof in QLP (1)

Prop: S4 + $\Box(D \leftrightarrow \neg\Box D)$ is inconsistent for any D.

1)	$\Box(D \leftrightarrow \neg\Box D)$	$\vdash D \leftrightarrow \neg\Box D$	T
2)	"	$\vdash \Box D \rightarrow D$	T
3)	"	$\vdash \neg\Box D$	
4)	"	$\vdash D$	
5)	"	$\vdash \Box D$	Nec
6)	"	$\vdash \bot$	
7)		$\vdash \neg\Box(D \leftrightarrow \neg\Box D)$	

- Two possible reactions:
  1) The existence of *provably* "absolutely unprovable" statements (i.e. Gödel fixed points) is inconsistent with S4.
  2) The use of $\Box$ and modal Necessitation are obscuring something.

Reconstructing Myhill's proof in QLP (2)

- Consider the mapping $(\cdot)^{\exists}$ such that $(\Box\varphi)^{\exists} = (\exists x)x : \varphi$
- Fitting (2008): S4 $\vdash F \iff$ QLP $\vdash F^{\exists}$
- Proceeding in this manner ...

0)	$y : (D \leftrightarrow \neg(\exists x)x : D)$	$\vdash D \leftrightarrow \neg(\exists x)x : D$	
1)	"	$\vdash (\exists x)x : D \to \neg D$	
2)	"	$\vdash (\exists x)x : D \to D$	
3)	"	$\vdash \neg(\exists x)x : D$	
4)	"	$\vdash D$	
5)	"	$\vdash t(y) : D$	**for some $t(y)$ (via Con. Nec.)**
5')	"	$\vdash (\exists x)x : D$	
6)	"	$\vdash \bot$	
7)		$\vdash \neg(\exists y)y : [D \leftrightarrow \neg(\exists x)x : D]$	

Reconstructing Myhill's proof in QLP (3)

- In order to construct $t(y)$, we need to internalize the proof of $(\exists x) : D \rightarrow D$:

  1) $\vdash x : D \rightarrow D$
  2) $\vdash r(x) : (x : D \rightarrow D)$
  3) $\vdash \langle r(x) \forall x \rangle : (\forall x)(x : D \rightarrow D)$ JUG, 2)
  4) $\vdash q : (\forall x)(x : D \rightarrow D) \rightarrow ((\exists x)x : D \rightarrow D)$
  5) $\vdash q \cdot \langle r(x) \forall x \rangle : ((\exists x)x : D \rightarrow D)$
  6) $\vdash (\exists y)y : ((\exists x)x : D \rightarrow D)$

- 1) - 3) mirror Gödel's consistency proof.
- Again JUG (or UBF) is required to show

  (U$_q$) $\quad (\exists y)y : ((\exists x)x : D \rightarrow D) = (\Box(\Box\varphi \rightarrow \varphi))^{\exists}$

Arithmetical interpretation of QLP^- (Dean & Kurokawa 2009)

- $\mathsf{QLP}^- = \mathsf{QLP}$ - JUG, $\mathcal{L}_{\mathsf{QLP}^-} = \mathcal{L}_{\mathsf{QLP}} - \langle\cdot\forall\cdot\rangle$
- Define $(\cdot)^*$ from the $\mathcal{L}_{\mathsf{QLP}^-}$ to $\mathcal{L}_a$ s.t.
  - $(x_i)^* = p(y_i)$ where p enumerates the gns of PA proofs
  - $(P_i)^*$ is some fixed closed sentence of $\mathcal{L}_a$
  - $(t : F)^* = \mathsf{Proof}(\ulcorner t^* \urcorner, \ulcorner F^* \urcorner)$
- **Soundness Thm**: If $\mathsf{QLP}^- \vdash \varphi$, then $\mathcal{N} \models (\varphi)^*$ for all $(\cdot)^*$.
  - So, e.g., $\mathcal{N} \models ((\exists x)x : \varphi \rightarrow \varphi)^* = \mathsf{Prov}(\ulcorner \varphi \urcorner) \rightarrow \varphi$
  - But $\mathcal{N} \not\models ((\exists y)y : ((\exists x)x : \bot \rightarrow \bot))^* = \mathsf{Prov}(\ulcorner \mathsf{Prov}(\ulcorner \varphi \urcorner) \rightarrow \varphi \urcorner)$
  - So this result cannot be extended to QLP.
  - In particular, the rule JUG is not arithmetically sound.
- But without JUG, QLP lacks Constructive Necessitation:

$$\mathsf{QLP} \vdash (\exists y)y : ((\exists x)x : P \rightarrow P) \text{ but}$$
$$\mathsf{QLP}^- \nvdash (\exists y)y : ((\exists x)x : P \rightarrow P)$$

Tentative morals

- Resolutions proposed by philosophers to the Myhill/Montague paradox: weakening reflection, rejecting epistemic closure, typing.
- But a characteristic feature of this derivation (and those of Goodman and Gödel) is the **use of Necessitation**.
- Explicit modal logics allow us to see the "fine structure" of Nec:

(Nec) $\Box\Gamma \vdash \varphi \quad \therefore \quad \Box\Gamma \vdash \Box\varphi$

(Con. Nec.) If $\vec{s} : \vec{\Gamma}, \Delta \vdash F$, then exists $t(\vec{s}, \vec{y})$ s.t. $\vec{s} : \vec{\Gamma}, \vec{y} : \vec{\Delta} \vdash t(\vec{s}, \vec{y}) : F$.

- Sometimes $\vec{s} : \vec{\Gamma}, \Delta \vdash F$ involves quantified reasoning about proofs – e.g. $\vdash x : F \rightarrow !x : x : F \quad \therefore \quad \vdash (\forall x)(\exists y)(x : F \rightarrow y : x : F)$.
- Gödel 1933o/38a: Such reasoning should be forbidden because we don't have a determinate conception of "all proofs".
- Less severe diagnosis: such reasoning may be sound, but can't always be consistently internalized.