(F20, må 17 maj 2004)

Lite om oändliga mängder, forts.

Med transfinit rekursion definieras också:
Multiplikation av ordinaltal:
För alla $\alpha \in \mathcal{O}$: $\alpha \cdot 0 = 0$
$\alpha \cdot \beta = \alpha \cdot \gamma + \alpha \qquad \beta = S(\gamma)$
$\alpha \cdot \beta = \sup\{\alpha \cdot \gamma \mid \gamma \in \beta\}, \quad \beta$ ett gränsordinaltal
Multiplikation är liksom addition **inte kommutativ**, men **associativ**. Dessutom gäller en **distributiv lag**: $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$, men för en del $\alpha, \beta, \gamma \in \mathcal{O}$ gäller $(\alpha + \beta) \cdot \gamma \neq \alpha \cdot \gamma + \beta \cdot \gamma$
Division från vänster i $\mathcal{O}$:
Om $\alpha, \gamma \in \mathcal{O}, \alpha \neq 0$: Det finns **unika** $\beta, \rho \in \mathcal{O}, \rho < \alpha$ med $\gamma = \alpha \cdot \beta + \rho$.

Potenser av ordinaltal:
För alla $\alpha \in \mathcal{O}$: $\alpha^0 = 1$
$\alpha^\beta = \alpha^\gamma \cdot \alpha \qquad \beta = S(\gamma)$
$\alpha^\beta = \sup\{\alpha^\gamma \mid \gamma \in \beta\}, \quad \beta$ ett gränsordinaltal

Sats: Varje ordinaltal $\alpha > 0$ kan entydigt skrivas (**normalform**)

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$$

med $\beta_1, \ldots, \beta_n \in \mathcal{O}$, $\beta_1 > \cdots > \beta_n$, och $n, k_1, \ldots, k_n \in \omega, > 0$.
Ex. (**Goodsteinföljder**)
Välj ett naturligt tal $m \neq 0$ och bilda en talföljd $a_2, a_3, a_4, \ldots$ enligt
$a_2 = m$,
$a_{i+1} = a_i[i \to i+1] - 1$, dvs med a_i i **ren bas** i, byt i mot $i+1$, dra bort 1.
t.ex. $m = 21$ ger $a_2 = 21 = 2^{2^2} + 2^2 + 1, a_3 = 3^{3^3} + 3^3 + 1 - 1 = 3^{3^3} + 3^3, a_4 = 4^{4^4} + 4^4 - 1 = 4^{4^4} + 4^3 \cdot 3 + 4^2 \cdot 3 + 4 \cdot 3 + 3, \ldots$
Sats: $a_n = 0$ för något $n \geq 3$.
(Visas elegant med hjälp av oändliga ordinaltal.)

Kardinalitet

Definition: Mängderna M, N har samma **kardinalitet**, är lika stora, skrivet $|M| = |N|$, om det finns en **bijektion** $f : M \to N$ (dvs en funktion så att för varje $n \in N$ finns precis ett $m \in M$ med $f(m) = n$).

Ordinaltal som inte har samma kardinalitet som något tidigare kallas **kardinaltal**. Varje naturligt tal är ett kardinaltal. Det första oändliga kardinaltalet ω kallas $\aleph_0$ (läses "alef-noll"), nästa kallas $\aleph_1$ etc. Det finns $\aleph_\alpha$ för varje $\alpha \in \mathcal{O}$ och $\aleph_\alpha < \aleph_\beta \Leftrightarrow \alpha < \beta$

Sats: (Cantor) För varje mängd M gäller $|M| < |\mathcal{P}(M)|$.
$\mathcal{P}(M)$ betecknar här **potensmängden** $\{A \mid A \subseteq M\}$ till M, dvs mängden av delmängder till M.

Om $\mathcal{M}$ är en mängd ordinaltal gäller $\sup\{\aleph_\alpha \mid \alpha \in \mathcal{M}\} = \aleph_{\sup \mathcal{M}}$
Med detta visas det förbluffande: Det finns ett kardinaltal κ så att $\kappa = \aleph_\kappa$.

Gödels första ofullständighetssats: Det finns ingen **fullständig, konsistent, axiomatiserbar** utvidgning till Q-axiomen.

Speciellt är inte $\mathcal{T}_{AR}$ axiomatiserbar (den är ju en fullständig och konsistent utvidgning till Q-axiomen). För varje konsistent axiomsystem finns det sentenser som är sanna (i $\mathbb{N}$) men inte bevisbara med det systemet.

Idén i beviset är enkel:
Betrakta ett konsistent axiomsystem och finn en sentens p som "säger" att p själv inte är bevisbar (i det aktuella systemet),

- p kan inte bevisas (då vore den sann och därmed obevisbar)
- $\sim p$ kan inte bevisas ($\sim p$ säger att p kan bevisas)

Eftersom varken p eller $\sim p$ kan bevisas är systemet inte fullständigt.

För att förklara hur en sentens i aritmetikens språk kan "säga" något om bevisbarhet och att en sådan sentens p finns, visas tre saker:

(1) (vissa) funktioner $\mathbb{N}^k \to \mathbb{N}$ kan **representeras** av aritmetiska formler
(2) syntaxen (inklusive bevisbarhet) kan formuleras som funktioner i $\mathbb{N}$
(3) en sådan sentens p finns ("diagonallemmat")

1. Låt $\mathcal{T}$ vara en axiomatiserbar utvidgning till $\mathcal{T}_Q$, Q-axiomens teori.
Funktionen $f : \mathbb{N}^k \to \mathbb{N}$ sägs vara **representerbar i** $\mathcal{T}$ om det finns en formel $A(x_1, x_2, \ldots, x_k, x_{k+1})$ så att för alla $m_1, \ldots, m_k, n \in \mathbb{N}$:

$$f(m_1, \ldots, m_k) = n \;\Leftrightarrow\; \vdash_{\mathcal{T}} \forall x\, (A(\underline{m_1}, \ldots, \underline{m_k}, x) \leftrightarrow x = \underline{n})$$

($\vdash_{\mathcal{T}}$ står för härledning från $\mathcal{T}$:s axiom och om $m \in \mathbb{N}$ betecknar $\underline{m}$ termen $S(S(\ldots S(0)\ldots))$ (med m st S).)
De representerbara funktionerna är precis de **rekursiva funktionerna**, dvs (troligen, detta är den obevisade (och obevisbara) "Churchs tes") alla de funktioner som kan beskrivas med algoritmer.
Relationen $Rm_1 \ldots m_k$ på $\mathbb{N}^k$ sägs vara representerbar i $\mathcal{T}$ om det finns en formel $B(x_1, x_2, \ldots, x_k)$ så att

$$Rm_1 \ldots m_k \text{ sann} \;\Rightarrow\; \vdash_{\mathcal{T}} B(\underline{m_1}, \ldots, \underline{m_k}),$$

$$Rm_1 \ldots m_k \text{ falsk} \;\Rightarrow\; \vdash_{\mathcal{T}} \sim B(\underline{m_1}, \ldots, \underline{m_k}).$$

2. **Gödelnumrering**: en enentydig funktion

$$\text{gn} : \{ \text{ alla strängar i språket } \} \to \mathbb{N},$$

dess exakta form är inte viktig (här).
Låt $\ulcorner\phi\urcorner$ vara $\underline{\text{gn}(\phi)}$, dvs termen $S(S(\ldots S(0)\ldots))$ (gn(ϕ) stycken S).
Syntaxen svarar då mot rekursiva funktioner på $\mathbb{N}$, t.ex. con : $\mathbb{N}^2 \to \mathbb{N}$ som uppfyller $\text{con}(\text{gn}(\phi), \text{gn}(\psi)) = \text{gn}(\phi \,\&\, \psi)$. Man säger att syntaxen har **aritmetiserats**.
Relationen Bev mn på $\mathbb{N}^2$, som är sann precis om $m = \text{gn}(p_1 \ldots p)$ och $n = \text{gn}(p)$, där p är en sentens och $p_1 \ldots p$ är ett bevis för p (i $\mathcal{T}$), representeras av formeln $\text{Prov}(x, y)$.
Då "säger" formeln $\text{Pr}(y)$: $\exists x\, \text{Prov}(x, y)$ att **sentensen med gödeltal** y **kan bevisas**.
Med beteckningen $\Box p$ för $\text{Pr}(\ulcorner p\urcorner)$ gäller

$$\vdash_{\mathcal{T}} \Box p \;\Rightarrow\; \vdash_{\mathcal{T}} p$$

och de tre viktiga (som uttrycker att $\Box$ är ett "bevisbarhetspredikat")

D1 $\quad \vdash_{\mathcal{T}} p \;\Rightarrow\; \vdash_{\mathcal{T}} \Box p$
D2 $\quad \vdash_{\mathcal{T}} \Box(p \to q) \to (\Box p \to \Box q)$
D3 $\quad \vdash_{\mathcal{T}} \Box p \to \Box\Box p$

(D2 och D3 ger också D4 $\vdash_{\mathcal{T}} p \to q \;\Rightarrow\; \vdash_{\mathcal{T}} \Box p \to \Box q$.)

3. **Diagonaliseringslemmat**:
Om ϕx är en formel utan andra fria variabler än x, finns en sentens p så att

$$\vdash_{\mathcal{T}} p \leftrightarrow \phi\ulcorner p \urcorner.$$

Detta lemma är den kritiska observationen. Låt nämligen sentensen p vara sådan att $\vdash_{\mathcal{T}} p \leftrightarrow \sim\Box p$ (lemmat tillämpat med $\sim$Pr som ϕ). p "säger" alltså just att p inte kan bevisas.
Då fås dels
$\vdash_{\mathcal{T}} p \overset{\text{D1}}{\Rightarrow} \vdash_{\mathcal{T}} \Box p \overset{\text{def av } p}{\Rightarrow} \vdash_{\mathcal{T}} \sim p$, så $\vdash_{\mathcal{T}} p \Rightarrow \vdash_{\mathcal{T}} \lightning$
och dels
$\vdash_{\mathcal{T}} \sim p \overset{\text{def av } p}{\Rightarrow} \vdash_{\mathcal{T}} \Box p \overset{\Box\text{:s betydelse}}{\Rightarrow} \vdash_{\mathcal{T}} p$, så $\vdash_{\mathcal{T}} \sim p \Rightarrow \vdash_{\mathcal{T}} \lightning$

Det innebär att varken p eller $\sim p$ kan bevisas i en konsistent, axiomatiserbar utvidgning av $\mathcal{T}_Q$!

I slutet av den utdelade stencilen från Boolos bok visas också att

$$\nvdash_{\mathcal{T}} \lightning \Rightarrow \nvdash_{\mathcal{T}} \sim\Box\lightning,$$

dvs om $\mathcal{T}$ är konsistent kan detta inte bevisas i $\mathcal{T}$ (om $\mathcal{T}$ **inte** är konsistent kan dess konsistens (liksom allt annat) förstås bevisas i $\mathcal{T}$!). Detta är **Gödels andra ofullständighetssats**.