Universitat de Barcelona
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

VERITATS ARITMÈTIQUES INDEMOSTRABLES EN L'ARITMÈTICA DE PEANO

Autora: Paula Pastó Pellicer

Director:	Dr. Joan Bagaria Pigrau
Realitzat a:	Departament de Matemàtiques i Informàtica

Barcelona,	13 de juny de 2022

Abstract

Peano's arithmetic is given by a set of axioms that express the basic properties and operations of natural numbers. This paper introduces the basics of this theory and studies the undecidability of certain results in it. To do so, it focuses on the Hydra and Hercules theorem, and on Goodstein's theorem.

Resum

L'aritmètica de Peano consisteix en un conjunt d'axiomes que expressen les propietats i operacions dels nombres naturals. Aquest article és una introducció a l'aritmètica de Peano i estudia la indecidibilitat de certs resultats en aquesta. Per fer-ho, se centra en el teorema d'Hèrcules i Hydra, i en el teorema de Goodstein.

2020 Mathematics Subject Classification. 03B25, 03E30, 03E35, 03F30, 03F40

Agraïments

Vull agrair la bona predisposició i comunicació que el doctor Joan Bagaria i Pigrau, tutor d'aquest treball de final de grau, m'ha brindat durant el semestre. Tant en el moment de decidir l'enfocament del treball, com en l'execució d'aquest la seva ajuda m'ha facilitat i alleugerit el camí.

Per altra banda, estic molt agraïda amb el suport que rebut per part de la meva família, dels amics amb els quals ens hem recolzat mútuament i d'aquells amb qui he compartit reflexions i dubtes sobre el treball. M'agradaria fer una menció especial al Guillem Quingles, el Iago Pueyo i l'Axel Gómez.

Índex

1 Introducció **1**

2 Sistemes formals. L'aritmètica de Peano **2**

2.1 Algunes nocions bàsiques sobre sistemes formals 2

2.2 Aritmètica de Peano 4

3 Consistència i incompletesa de PA **6**

3.1 El problema d'incompletesa 6

3.2 Consistència del sistema 7

3.3 El teorema d'Hèrcules i Hydra 8

3.3.1 Nombres ordinals transfinits i bons ordres 10

3.3.2 Seqüències febles de Goodstein i la seva convergència 11

3.3.3 El teorema de Goodstein 13

3.4 Indecidibilitat en PA del teorema d'Hèrcules i Hydra 17

3.4.1 Indecidibilitat en PA del teorema de Goodstein 18

4 Conclusions **21**

Capítol 1

Introducció

El treball que s'exposa a continuació tracta de l'aritmètica de Peano (PA) i les seves característiques. Primerament, introdueix un seguit de conceptes bàsics dels sistemes formals com la completesa, la consistència o la indecidibilitat. A continuació, es descriuen els trets més bàsics de PA.

Aquest projecte s'inspira en el treball de diversos matemàtics. Cronològicament, el primer és Kurt Gödel. Això és a causa de la seva demostració de la incompletesa de qualsevol sistema formal consistent que conté l'aritmètica elemental i de la impossibilitat que un sistema consistent d'aquest tipus pugui demostrar que ho és. Fent referència a la consistència, es menciona també a Gerhard Gentzen, qui prova la consistència de l'aritmètica de Peano fent servir inducció transfinita fins a l'ordinal ϵ_0.

Basant-se en els resultats de Kurt Gödel i de Gerhard Gentzen, el treball planteja el problema de la indecidibilitat de certs enunciats en l'aritmètica de Peano.

L'objectiu principal d'aquest projecte és entendre la noció d'indecibilitat en les matemàtiques. Per profunditzar en aquesta noció i facilitar-ne la comprensió, exposa el teorema d'Hèrcules i Hydra i el de Goodstein, que en són exemples. El treball fa ús dels resultats de Laurie Kirby i Jeff Paris, i de J. Ketonen i Robert M. Solovay. El treball demostra tots dos teoremes usant mètodes pertanyents a teories més fortes que l'aritmètica de Peano. Finalment, esbossa les indicacions de les proves que els teoremes mencionats no poden ser demostrats en aquesta teoria.

Capítol 2

Sistemes formals. L'aritmètica de Peano

2.1 Algunes nocions bàsiques sobre sistemes formals

Introduïm un seguit de conceptes, extrets de [4] i [1], a tall de descriure les bases de les matemàtiques que es treballen al llarg d'aquest projecte

Un **llenguatge formal** de primer orde està format pels següents elements formalment especificats:

- Un conjunt de símbols primitius que constitueixen l'**alfabet** del llenguatge. Aquest comprèn les variables, les connectives lògiques, els parèntesis, els quantificadors i els símbols de constant, predicats, relacions i funcions. Això pot o no incloure el símbol $=$.

- Un conjunt de **regles de formació de fórmules**. Aquestes indiquen quan una fórmula està ben formada en el llenguatge.

Afegint un conjunt de regles de transformació d'unes fórmules en altres s'obté un **càlcul lògic** que permet un procediment de deducció dins d'aquest llenguatge.

Per a cada llenguatge formal existeix una **semàntica formal** que pot interpretar i donar significat a les fórmules ben formades del llenguatge.

Un llenguatge formal permet doncs decidir si un símbol pertany al llenguatge, si una fórmula determinada n'és una expressió ben formada o si una seqüència sintàctica de fórmules constitueix una demostració o una deducció en aquest.

Definició 2.1.1. *Un **sistema formal** és una formalització rigorosa del concepte de sistema axiomàtic. Es construeix sobre un llenguatge formal i consta de:*

- Axiomes, que són les fórmules que serveixen com a punt de partida de la demostració.

*- Regles d'inferència, és a dir, regles de transformació de fórmules que permeten deduir-ne unes de les altres. Les regles indiquen com una fórmula anomenada conclusió s'obté a partir d'altres anomenades hipòtesis. El conjunt de les regles d'inferència s'anomena **càlcul deductiu**.*

*- **Teoremes**, que són els seus axiomes i totes les fórmules que se'n poden derivar amb el càlcul deductiu.*

Definició 2.1.2. *Una **teoria** d'un llenguatge de primer ordre és un conjunt d'enunciats del llenguatge tancat per la relació de conseqüència lògica.*

*Un enunciat φ és **conseqüència lògica** d'un conjunt d'enunciats T si tota interpretació de T que fa tots els enunciats de T vertaders també fa vertadera φ.*

L'aritmètica de Peano és un exemple de sistema formal. Es tracta de la teoria elemental dels nombres naturals. Es construeix sobre un llenguatge formal de primer ordre de l'aritmètica. Els símbols específics d'aquest són $\{\mathrm{S}, +, \cdot, 0\}$.

Vegem la definició de certes propietats dels sistemes formals.

Definició 2.1.3. *Un sistema és **consistent** si no conté un teorema i la seva negació alhora.*

Definició 2.1.4. *Un sistema T és **complet** si per a tot enunciat φ del llenguatge de T, o bé φ o bé $\neg\varphi$ pertany a T.*

Definició 2.1.5. *Un sistema és **decidible** si tots els enunciats del llenguatge del sistema són demostrables o refutables en aquest.*

Definició 2.1.6. *Un enunciat és **independent** d'un conjunt d'enunciats si no és conseqüència lògica d'aquests. Un conjunt d'enunciats és independent si cada enunciat és independent dels altres.*

Definició 2.1.7. *Un enunciat φ és* ***indecidible*** *en un sistema formal si tant φ com $\neg\varphi$ són independents del sistema. En altres paraules, φ no es pot demostrar ni refutar en aquesta sistema.*

2.2 Aritmètica de Peano

El 1889, amb la intenció de reduir diversos elements de les matemàtiques a la lògica, Giuseppe Peano publica el llibre *"Arithmetices Principia"* que inclou una axiomatització dels nombres naturals. Amb això es dóna el que es coneixerà com l'aritmètica de Peano. Es tracta d'un conjunt d'axiomes que expressen les propietats i operacions bàsiques dels nombres naturals. A continuació s'exposen els trets més bàsics d'aquesta teoria.

A partir d'ara, al llenguatge de primer ordre, que té com a símbols no lògics, a més a més de $=$, símbols d'operacions binàries $+$ i $\cdot$, un símbol d'operació unària S i un símbol de constant 0, li diem el llenguatge de l'aritmètica. L'aritmètica de Peano (PA) és la teoria axiomàtica generada pels axiomes de primer ordre que s'enuncien a continuació.

La formulació original de PA assumeix les següents tres nocions: nombre enter positiu n, unitat, 1, i successor d'un nombre n, $S(n)$. En formulacions més modernes, es fa servir el 0 com a primer nombre natural, en comptes de l'1.

Axioma 2.2.1. $\nexists n \ (S(n) = 0)$

Axioma 2.2.2. $\forall n, m \ (S(m) = S(n) \Longrightarrow n = m)$

Axioma 2.2.3. $\forall n \ \ 0 + n = n$

Axioma 2.2.4. $\forall n, \forall m \ \ n + S(m) = S(n + m)$

Axioma 2.2.5. $\forall n \ \ n \cdot 0 = 0$

Axioma 2.2.6. $\forall n, \forall m \ \ n \cdot S(m) = n \cdot m + n$

Axioma 2.2.7. *Sigui P una propietat qualsevol, expressable en el llenguatge de l'aritmètica. Aleshores, $P(0) \wedge \forall n \ ((P(n) \Longrightarrow P(S(n))) \Longrightarrow \forall n \ P(n))$*

Observacions 2.2.8. Podem interpretar els axiomes de la següent manera:

Axioma 1. Afirma que el 0 és el primer nombre dels nombres naturals.

Axioma 2. Afirma que la operació S és injectiva.

Axioma 7. És el principi d'inducció, un esquema axiomàtic. Aquest, en realitat, és un llistat infinit d'axiomes; existeix un axioma per a cada propietat P.

Observació 2.2.9. Com que el llenguatge de l'aritmètica de Peano és un llenguatge de primer ordre, les variables sobre les quals quantifiquen els quantificadors són els nombres naturals i no pas conjunts de nombres naturals.

Definició 2.2.10. *Les successions de nombres naturals poden ser definides de diverses maneres diferents. Una* ***definició recursiva*** *és aquella que indica quin és el primer membre de la successió i com obtenir un terme a partir del seu o seus termes anteriors.*

Definició 2.2.11. *Una* ***funció recursiva*** *és una funció* $f : \mathbb{N} \longrightarrow \mathbb{N}$ *computable que es "crida a si mateixa", el que significa per calcular* $f(n)$ *s'utilitzen els seus propis termes anteriors* $\{f(m) \mid m < n\}$.

La teoria PA defineix els nombres naturals recursivament. Peano fa ús d'una estratègia recursiva per representar-los definint la funció successor de la següent manera.

Definició 2.2.12. *La* ***funció successor*** *és una aplicació* $S : \mathbb{N} \longrightarrow \mathbb{N}$ *tal que* $\forall n \in \mathbb{N}$

$S(n) = n \cup \{n\}$

D'aquesta definició s'extreu que $S(0) = 1$, $S(S(0)) = S(1) = 2$, i així successivament. En general doncs, $S(n) = n + 1$. A més a més, pel que afirma l'axioma 4, es tracta d'una funció injectiva. Segons l'axioma 3, el zero no té predecessor, però, tal com està definida la funció, per a la resta de nombres naturals sempre n'existirà un.

Capítol 3

Consistència i incompletesa de PA

3.1 El problema d'incompletesa

L'any 1931, Kurt Gödel publica els teoremes d'incompletesa. Ara se'n parla en base a [8].

Teorema 3.1.1. *(Primer teorema d'incompletesa de Gödel). Qualsevol sistema consistent que contingui PA és necessàriament incomplet.*

Amb aquest teorema demostra que cap sistema axiomàtic de l'aritmètica dels nombres naturals pot ser consistent i complet alhora. Interpretat semànticament, això ens diu que no existeix un conjunt recursiu, computable, d'axiomes complet pel conjunt d'enunciats aritmètics vertaders.

En altres paraules, sentencia que en qualsevol formalització consistent de les matemàtiques que contingui l'aritmètica, o un petit fragment d'aquesta, es pot construir una afirmació que ni es pot demostrar ni es pot refutar dins d'aquest sistema.

Teorema 3.1.2. *(Segon teorema d'incompletesa de Gödel). Cap sistema consistent que contingui PA pot demostrar la seva pròpia consistència.*

Gödel prova amb aquest teorema que la consistència de qualsevol sistema formal consistent capaç de formalitzar l'aritmètica, o un petit fragment d'aquesta, és inderivable en el sistema.

3.2 Consistència del sistema

El 1936, Gerhard Gentzen presenta un resultat arrel d'aquest descobriment.

Teorema 3.2.1. *La teoria T que estén PA amb el principi d'inducció aritmètica fins a l'ordinal ϵ_0 demostra que PA és consistent.*

La demostració de Gentzen destaca un aspecte del segon teorema d'incompletesa: la consistència d'una teoria només pot demostrar-se en una teoria més forta.

Definició 3.2.2. *La **inducció transfinita** és una generalització de la inducció matemàtica a conjunts ben ordenats. És a dir, a conjunts tals que qualsevol subconjunt no buit té un primer element. S'enuncia de la manera següent.*

Sigui X un conjunt ben ordenat i $x \in X$, si algun teorema és cert pel primer $x_0 \in X$, i també ho és per un element $x_i \in X$ si és cert per cada element precedent a ell, aleshores el teorema és cert per a tot $x \in X$.

Amb els resultats de Gödel i Gentzen es descobreixen doncs enunciats naturals en el llenguatge de PA que no poden ser demostrats ni refutats en PA. Es tracta de veritats sobre allò finit que necessiten l'existència de conjunts infinits per poder ser demostrats. La demostració d'aquests enunciats requereix intrínsecament l'ús de conjunts infinits.

Els exemples donats per Gödel d'enunciats que fan que PA sigui una teoria incompleta, són exemples fets a mida per a les demostracions d'incompletesa, però són anti-naturals en sentit estrictament matemàtic.

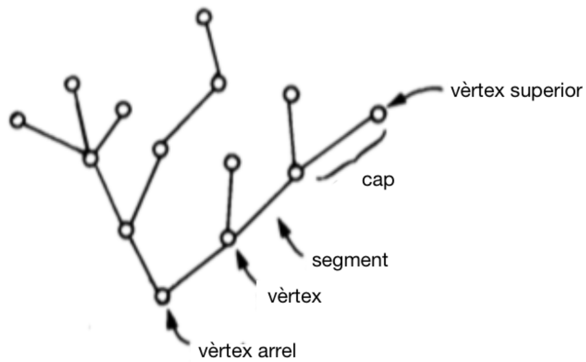
Seguidament s'exposa un exemple que sí que és natural en sentit matemàtic d'enunciat indecidible en PA.

3.3 El teorema d'Hèrcules i Hydra

Primerament, es dóna un breu context mitològic extret de [10]. El mite de l'Hydra de Lerna parla sobre un monstre aquàtic que formava part de l'inframon grec. Aquesta bèstia habitava en el llac de Lerna, prop de Nauplia. En la cultura antiga, hi havia déus celestes i també deïtats de la foscor. Aquest ser pertanyia a la segona categoria. Diu el mite que aquesta criatura tenia molts caps. Un dels seus poders era precisament el de regenerar els seus caps quan aquests li eren amputats. Per cadascun que perdia, li'n creixien dos de nous. Li encomanaren a Hèrcules una missió que semblava impossible d'aconseguir; matar a l'Hydra.

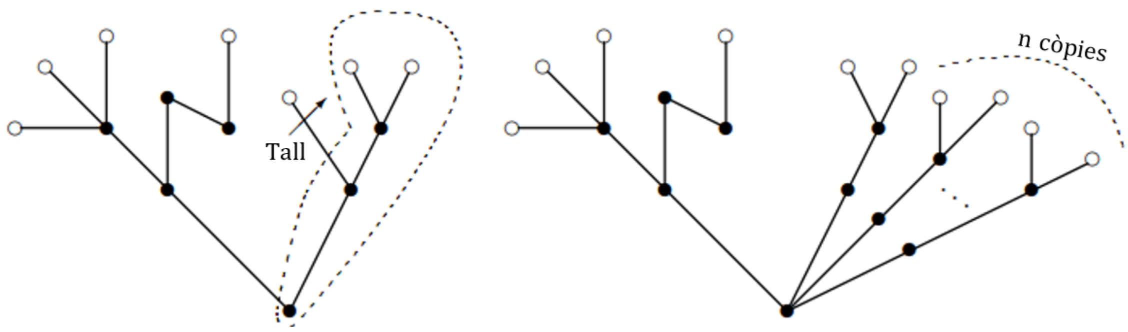
Definició 3.3.1. *Una* ***Hydra*** *és un arbre finit, que pot ser considerat una col·lecció finita de segments que uneixen vèrtexs tals que cada vèrtex està connectat per un únic camí al vèrtex arrel.*

El vèrtex arrel és aquell des del qual s'origina l'arbre. El vèrtex superior és aquell que està unit a un sol segment i que no és l'arrel. Juntament amb aquest segment, representen el cap de l'Hydra.



Per entrar en el context del teorema que s'enunciarà, cal entendre que el combat entre Hèrcules i Hydra fa referència a com s'ho farà Hèrcules per matar Hydra. És a dir, quina estratègia seguirà per aconseguir deixar-la sense caps.

El combat entre Hèrcules i la bèstia, Hydra, es desenvolupa de la manera detallada a continuació. Si Hèrcules talla un cap en el pas n, Hydra genera n nous caps. Ho fa des del vèrtex que estava unit al cap que Hèrcules acaba de tallar, seguint un segment cap a l'arrel fins arribar al següent vèrtex. A partir d'aquest últim vèrtex, broten n rèpliques de la part de l'Hydra que queda per sobre d'aquest (sense el cap amputat). Si el cap que acaba de tallar-se tenia l'arrel com un dels seus vèrtexs, no es generen caps nous. A continuació hi ha un exemple gràfic del que s'acaba de descriure.



Definició 3.3.2. *Una **estratègia** és una funció que determina, per a qualsevol batalla, quin cap ha de tallar Hèrcules a cada pas.*

*Una **estratègia recursiva** és una estratègia en la qual Hèrcules va escollint els caps que talla en funció d'algun mètode o algoritme precís.*

Teorema 3.3.3. *(Hèrcules i Hydra). Tota estratègia recursiva és guanyadora.*

En altres paraules, sigui quina sigui la combinació de caps de l'Hydra inicial, Hèrcules acaba vencent el combat tallant-li tots els caps a l'Hydra. Aquest és un exemple de resultat indecidible en PA.

Abans de poder provar aquest teorema, a tall de facilitar-ne la comprensió, n'exposarem un altre que es demostra de manera molt similar, el teorema de Goodstein.

El que s'explica a continuació està extret de [7] i [2]. Amb l'estudi de l'evolució de certs fenòmens naturals apareixen les seqüències numèriques i la curiositat per esbrinar més sobre el seu comportament a llarg termini i sobre la seva convergència. El 1944, el lògic britànic Reuben Louis Goodstein publica "On the Restricted Ordinal Theorem, Journal of Symbolic Logic". Utilitza aquest treball per introduir unes seqüències que, tal com veurem més endavant, descriuen un comportament inusual. Es tracta de seqüències els valors inicials de les quals incrementen tan ràpidament que fan pensar que creixeran infinitament, però, sorprenentment, totes acaben tendint a zero. Amb això presenta també el següent resultat, que és un exemple natural d'enunciat indecidible en PA.

El teorema de Goodstein afirma que tota seqüència de Goodstein convergeix cap a zero. La demostració requereix l'ús de mètodes infinitaris. Aquesta és la causa que no pugui ser demostrat en PA i calgui una teoria més forta. A continuació, s'exposa una introducció als nombres ordinals transfinits per tenir totes les eines necessàries per demostrar-ho.

3.3.1 Nombres ordinals transfinits i bons ordres

El concepte d'ordinal transfinit és introduït l'any 1895 per Georg Cantor amb l'objectiu d'aclarir algunes implicacions de la noció d'infinit, que s'associava a nombres majors que tots els nombres finits, però no necessàriament absolutament infinits. El concepte de nombre ordinal transfinit representa una extensió del concepte de nombre ordinal a conjunts infinits.

Els nombres ordinals transfinits són nombres ordinals usats per a ordenar conjunts infinits, de manera que la seva definició es basa en el concepte del bon ordre. El que es troba definit en aquest subapartat s'ha extret de [3].

A continuació, exposem propietats dels nombres ordinals transfinits a tall de poder treballar amb ells més endavant, en la demostració que farem.

Propietat 3.3.4. *Les operacions suma i producte dels nombres enters poden ser esteses als ordinals transfinits, tot i que la seva commutativitat no.*

Ja coneixem com s'ordenen els nombres naturals, parlem doncs dels ordinals majors que ells. L'ordinal w és el primer nombre major que qualsevol enter i ϵ_0 és el menor ordinal major que totes les sumes de potències iterades de w. Vegem quin ordre segueixen els ordinals amb els quals treballarem:

$0 < 1 < 2 < ... < n < ... < w < w + 1 < ... < w + n < ...$

$w \cdot 2 < w \cdot 2 + 1 < ... < w \cdot 2 + n < ... < w \cdot 3 < w \cdot 3 + 1 < ... < w \cdot n < ...$

$w^2 < w^2 + 1 < ... < w^3 < ... < w^n < ...$

$w^w < w^w + 1 < ... < w^{2 \cdot w} < w^{2 \cdot w} + 1 < ... < w^{2 \cdot w} + w < ... < w^{3 \cdot w} < ...$

$w^{w^w} < ... < \epsilon_0$

Tots els ordinals mencionats fins ara formen un conjunt numerable. Són només el principi de la cadena d'ordinals. No tots tenen predecessor immediat, tot i això, el conjunt de nombres ordinals està ben ordenat (qualsevol conjunt d'ordinals no buit té element mínim). Aquesta propietat és la raó per la qual sabem que no existeix una seqüència estrictament decreixent infinitament llarga de nombres ordinals.

Amb això, ja podem fer les operacions amb els nombres ordinals transfinits que es requereixen per entendre la demostració de la convergència a zero de les seqüències de Goodstein.

3.3.2 Seqüències febles de Goodstein i la seva convergència

Les seqüències febles de Goodstein són més simples que les seqüències de Goodstein, però hi estan estretament relacionades, per això les introduïm ara. Aquestes treballen amb el concepte de descomposició única en potències d'una certa base.

Definició 3.3.5. *Una* ***seqüència feble de Goodstein*** $\{u_k\}$ *que pren com a valor inicial* u_0*, és aquella seqüència de nombres naturals que parteix de l'única descomposició en potències de base* $b = 2$ *d'*u_0 *i que, per obtenir* u_{k+1} *a partir d'*u_k *on* $k \in \mathbb{N}$ *tal que* $k = b-2$*, ho fa de la següent manera:*

- *Escriu la representació d'*u_k *canviant totes les* b *per* $b+1$*.*

- *Resta* 1 *al resultat.*

- *El reescriu en base* $b+1$*.*

- *Finalment, si* $u_{k+1} \neq 0$*, segueix iterant aquest procés. Si* $u_{k+1} = 0$*, s'acaba el procés.*

Exemple 3.3.6. A tall de fer-ne la definició més visual, exemplifiquem la seqüència feble de Goodstein que té per valor inicial $u_0 = 266$.

La seva única descomposició en potències de base 2: $266 = 2^8+2^3+2^1$. Un cop tenim això, detallem el procés que cal seguir per anar trobant els següents membres de la seqüència.

Tenim que $u_0 = 266$, per obtenir u_1, cal:

- Agafar la representació d'u_0 en base 2 i canviar totes les bases 2 per bases 3.

- Restar-li 1 a aquest resultat i reescriure-ho en base 3.

Operant aquests passos iterativament obtenim:

$u_0 = 2^8 + 2^3 + 2^1 = 266$

$u_1 = 3^8 + 3^3 + 3^1 - 1 = 3^8 + 3^3 + 2 = 6590$

$u_2 = 4^8 + 4^3 + 2 - 1 = 4^8 + 4^3 + 1 = 65601$

$u_3 = 5^8 + 5^3 + 1 - 1 = 5^8 + 5^3 = 390750$

$u_4 = 6^8 + 6^3 - 1 = 6^8 + 5 \cdot 6^2 + 6^2 - 1 = 6^8 + 5 \cdot 6^2 + 5 \cdot 6^1 + 5 = 1679831$

$u_5 = 7^8 + 5 \cdot 7^2 + 5 \cdot 7^1 + 5 - 1 = 7^8 + 5 \cdot 7^2 + 5 \cdot 7^1 + 4 = 5765085$

L'exemple ens fa més gràfic el fet que els termes de la seqüència ràpidament es tornen molt elevats, però si prenem un valor inicial més petit, veiem més fàcilment com realment la seqüència va decreixent i acaba valent zero.

Exemple 3.3.7. Sigui $u_0 = 3$,

$u_0 = 2^1 + 2^0 = 2^1 + 1 = 3$

$u_1 = 3^1 + 1 - 1 = 3^1 = 3$

$u_2 = 4^1 - 1 = 3 \cdot 4^0 = 3$

$u_3 = 3 \cdot 5^0 - 1 = 2 \cdot 5^0 = 2$

$u_4 = 2 \cdot 6^0 - 1 = 6^0 = 1$

$u_5 = 7^0 - 1 = 0$

Dels exemples s'observa que el fet que a cada iteració se sumi 1 al valor de la base provoca un gran increment del terme. Com s'explica que el simple pas de restar 1 al resultat acabi fent convergir la seqüència a 0?

Si ens hi fixem, tot i que a mesura que busquem termes de la seqüència, van incrementant-se les bases, els exponents en la nova representació decreixen. Visualment, en l'exemple 3.3.6, del pas u_3 al pas u_4. O en l'exemple 3.3.7, de l'u_1 a l'u_2.

Definició 3.3.8. *Un nombre m en base b és de la forma: $m = \lambda_r \cdot b^r + ... + \lambda_1 \cdot b^1 + \lambda_0$. Diem que el **terme unitat** de m és λ_0 i l'escrivim $\overline{m}$.*

Proposició 3.3.9. *Tota seqüència feble de Goodstein convergeix cap a zero.*

Demostració. A cada seqüència feble de Goodstein $\{u_k\}$ se n'associa una d'ordinals estrictament decreixent $\{\alpha_k\}$. Aquesta es construeix substituint la base de cada terme d'$\{u_k\}$ per w.

n	u_n	α_n
0	$2^8 + 2^3 + 2^1$	$\omega^8 + \omega^3 + \omega^1$
1	$3^8 + 3^3 + 3 - 1 = 3^8 + 3^3 + 2$	$\omega^8 + \omega^3 + 2$
2	$4^8 + 4^3 + 1$	$\omega^8 + \omega^3 + 1$
3	$5^8 + 5^3$	$\omega^8 + \omega^3$
4	$6^8 + 6^3 - 1 = 6^8 + 5.6^2 + 5.6^1 + 5$	$\omega^8 + \omega^2.5 + \omega^1.5 + 5$
5	$7^8 + 5.7^2 + 5.7^1 + 4$	$\omega^8 + \omega^2.5 + \omega^1.5 + 4$
6	$8^8 + 5.8^2 + 5.8^1 + 3$	$\omega^8 + \omega^2.5 + \omega^1.5 + 3$
...	...	...
9	$11^8 + 5.11^2 + 5.11^1$	$\omega^8 + \omega^2.5 + \omega^1.5$
10	$12^8 + 5.12^2 + 4.12^1 + 11$	$\omega^8 + \omega^2.5 + \omega^1.4 + 11$
...	...	...

Així doncs, cada terme d'$\{\alpha_k\}$ és major que el respectiu terme d'$\{u_k\}$, ja que w és major que qualsevol nombre natural. Però, es pot observar que, al contrari que la seqüència $\{u_k\}$, $\{\alpha_k\}$ decreix estrictament, vegem-ho.

Sigui $\overline{u_k}$ el terme unitat d'$\{u_k\}$,

- Si $\overline{u_k} \neq 0$, aleshores $\overline{u_{k+1}} = \overline{u_k} - 1$.

- Si $\overline{u_k} = 0$, aleshores en reescriure la descomposició en la nova base, cal separar el terme d'exponent menor (d'aquesta manera va decreixent l'exponent).

En la seqüència $\{\alpha_k\}$ tots els termes tenen base ω. Aleshores, tant si es redueix $\overline{\alpha}_k$ com si ho fa el menor exponent d'α_k, $\alpha_{k+1} < \alpha_k$.

Hem provat que $\{\alpha_k\}$ és estrictament decreixent. Com que els ordinals segueixen un bon ordre, no pot existir una seqüència estrictament decreixent infinita. És a dir, $\exists n \in \mathbb{Z} \mid \alpha_n = 0$. Com que $u_k \leq \alpha_k \; \forall k$, aleshores $u_n = 0$. Això es tradueix en els termes d'$\{u_k\}$ assolint zero en un nombre finit de passos.

$\square$

Observació 3.3.10. $\forall u_k \in \{u_k\}, u_k < w^w$

3.3.3 El teorema de Goodstein

En aquest apartat es troba la demostració del teorema de Goodstein feta en la teoria de conjunts, que és més forta que PA.

Definició 3.3.11. *Una* ***seqüència de Goodstein*** $\{g_k\}$*, que pren com a valor inicial* g_0*, és aquella seqüència de nombres naturals que parteix de l'única descomposició en potències de base* $b = 2$ *de* g_0 *escrivint també els exponents en base* b *i que, per obtenir* g_{k+1} *a partir de* g_k *on* $k \in \mathbb{N} \mid k = b - 2$*, ho fa de la següent manera:*

- Escriu la representació de g_k *canviant totes les* b *per* $b + 1$*.*

- Resta 1 *al resultat.*

- El reescriu en base $b + 1$ *i amb els exponents en aquesta base també.*

- Finalment, si $g_{k+1} \neq 0$*, segueix iterant aquest procés. Si* $g_{k+1} = 0$*, s'acaba el procés.*

Exemple 3.3.12. Visualitzem-ho construint la seqüència de Goodstein que té per valor inicial $g_0 = 266$.

La seva única descomposició en potències de base 2: $266 = 2^8 + 2^3 + 2^1$. La reescrivim expressant les potències en base 2: $266 = 2^{2^{2^1+1}} + 2^{2^1+1} + 2^1$. Un cop tenim això, detallem el procés que cal seguir per anar trobant els següents membres de la seqüència.

Tenim que $g_0 = 266$, per obtenir g_1, cal:

- Agafar l'expressió obtinguda de g_0 en base $b = 2$ i substituir tots els $b = 2$ per $b + 1 = 3$.

- Restar-li 1 a aquest resultat.

- Reescriure-ho en base $b = 3$ i expressar també els exponents en base $b = 3$.

Operant aquests passos iterativament obtenim:

$g_0 = 2^8 + 2^3 + 2^1 = 2^{2^{2^1+1}} + 2^{2^1+1} + 2^1$

$g_1 = 3^{3^{3^1+1}} + 3^{3^1+1} + 3^1 - 1 = 3^{3^{3^1+1}} + 3^{3^1+1} + 2 \simeq 10^{38}$

$g_2 = 4^{4^{4^1+1}} + 4^{4^1+1} + 1 \simeq 10^{616}$

$g_3 = 5^{5^{5^1+1}} + 5^{5^1+1} \simeq 10^{10921}$

$g_4 = 6^{6^{6^1+1}} + 6^{6^1+1} - 1 = 6^{6^{6^1+1}} + 5 \cdot 6^6 + 5 \cdot 6^5 + 5 \cdot 6^4 + 5 \cdot 6^3 + 5 \cdot 6^2 + 5 \cdot 6^1 + 5 \simeq 10^{217832}$

$g_5 = 7^{7^{7^1+1}} + 5 \cdot 7^7 + 5 \cdot 7^5 + 5 \cdot 7^4 + 5 \cdot 7^3 + 5 \cdot 7^2 + 5 \cdot 7^1 + 4 \simeq 10^{4871822}$

L'exemple ens fa més gràfic el fet que els termes de la seqüència ràpidament es tornen molt elevats. Però, tot i així, provarem que la seqüència convergeix a zero. La demostració es desenvolupa de manera similar a la de les seqüències febles de Goodstein.

Teorema 3.3.13. *(Goodstein). Tota seqüència de Goodstein convergeix a zero.*

Demostració. A cada seqüència de Goodstein $\{g_k\}$ se n'associa una d'ordinals estrictament decreixent $\{\beta_k\}$. Aquesta es construeix substituint la base de cada terme de $\{g_k\}$ per w. Així doncs, cada terme d'$\{\beta_k\}$ és major que el respectiu terme de $\{g_k\}$. Però, es pot observar que, al contrari que la seqüència $\{g_k\}$, $\{\beta_k\}$ decreix estrictament. Provem-ho.

Sigui $\overline{g_k}$ el terme unitat de $\{g_k\}$,

- Si $\overline{g_k} \neq 0$, aleshores $\overline{g_{k+1}} = \overline{g_k} - 1$.

- Si $\overline{g_k} = 0$, aleshores en reescriure la descomposició en la nova base, cal separar el terme d'exponent menor.

Com que en la seqüència $\{\beta_k\}$ totes les bases i bases d'exponents són ω i cada terme β_k de la seqüència està definit a partir de g_k, veiem que en qualsevol cas $\beta_{k+1} < \beta_k$.

Hem provat doncs que $\{\beta_k\}$ és estrictament decreixent. Com ja hem dit abans, no existeix cap seqüència d'ordinals estrictament decreixent infinita. Per tant, té un element mínim. És a dir, $\exists n$ tal que $\beta_n = 0$.

Com que $g_k \leq \beta_k \ \forall k$, aleshores $g_n = 0$. Això es tradueix en els termes de $\{g_k\}$ assolint zero en un nombre finit de passos.

□

Observació 3.3.14. El fet que en aquesta demostració es treballa amb ordinals majors que w^w, és el causant de la indecidibilitat en PA del teorema de Goodstein.

Com que les seqüències de Goodstein treballen només amb nombres naturals i eines per operar amb aquests, es tracta d'un teorema que s'enuncia en PA, però no pot ser demostrat usant només els recursos de PA. S'observa en la prova del teorema l'ús de la teoria de conjunts que inclou els nombres ordinals transfinits.

Demostració del teorema d'Hèrcules i Hydra

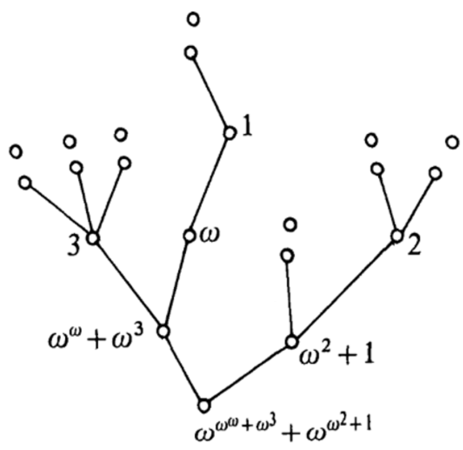
Demostració. Està basada en els articles [11] i [6]. Sigui H l'Hydra del combat.

Primerament, cal assignar un ordinal $\alpha < \epsilon_0$ a cada vèrtex d'H. Fem-ho:

- Als vèrtexs superiors els assignem 0.

- A la resta de vèrtexs els assignem $\omega^{\alpha_1} + ... + \omega^{\alpha_n}$ on $\alpha_1 \geq ... \geq \alpha_n$ són els ordinals assignats als vèrtexs que es troben immediatament per sobre.

Vegem com quedaria en l'exemple d'Hydra que hem donat abans:



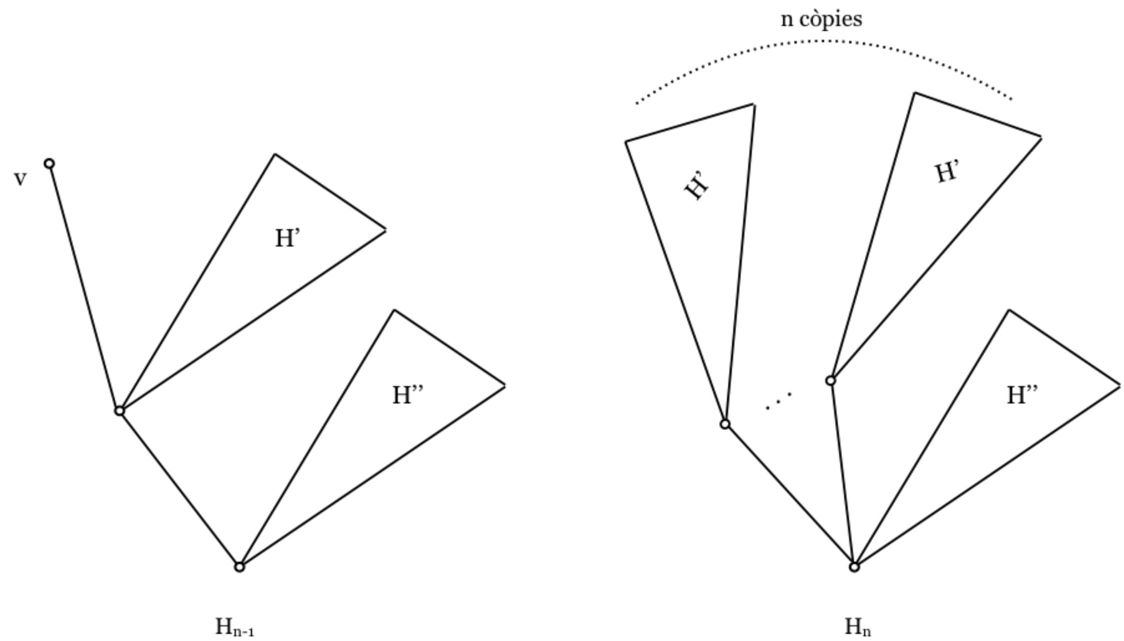
L'ordinal associat a H és l'ordinal que assignem al vèrtex arrel. És a dir, en aquest cas, l'ordinal d'H és $w^{w^w+w^3}+w^{w^2+1}$. El denotarem per $ord(H)$.

Veiem doncs, com a cada pas n, l'arbre que representa l'Hydra té un ordinal associat. Amb això podem construir una seqüència d'ordinals.

Tot i que, intuïtivament sembla que l'arbre creixerà infinitament, en realitat aquest creixerà en amplitud, però cada vegada tindrà menys nivells en alçada. Això farà que Hèrcules acabi tallant caps directament connectats al vèrtex arrel i que, per tant, venci a Hydra.

Com hem vist amb les seqüències de Goodstein, n'hi ha prou amb provar que la seqüència d'ordinals és estrictament decreixent, per veure que acaba tendint a zero en un nombre finit de passos. Això és equivalent a vèncer l'Hydra sigui quina sigui l'estratègia.

Considerem la següent Hydra H en el pas $n-1$, és a dir, H_{n-1}.



Vegem que si tallem el cap v, en el pas n l'ordinal associat a l'Hydra disminueix.

En el pas $n-1$, $ord(H_{n-1}) = \omega^{1\ +\ ord(H')} + ord(H'')$.

Si tallem el cap v, l'ordinal de la nova Hydra és $ord(H_n) = \omega^{ord(H')} \cdot n + ord(H'')$.

Com que $\forall n,\ n < \omega$, tenim que $\omega^{ord(H')} \cdot n < \omega^{ord(H')} \cdot \omega = \omega^{1\ +\ ord(H')}$.

Per tant és clar que $ord(H_n) < ord(H_{n-1})$.

En l'argument anterior hem utilitzat que el vèrtex v està a una distància de dos del vèrtex arrel. Si aquest no és el cas, agafem la subHydra formada per tot el que queda per sobre del vèrtex que està a distància 2 del cap que estem tallant. Aquesta subHydra té la mateixa forma que l'Hydra H_{n-1} de l'argument i ja hem vist que el seu ordinal associat disminueix en fer el pas n. Com que en fer el pas n, el tall només varia la subHydra, és clar que l'ordinal associat a l'Hydra disminuirà.

No estem considerant el cas que el vèrtex v estigui a una distància inferior a dos del vèrtex arrel, ja que en aquest cas, tal com hem definit el combat, l'Hydra no genera caps nous.

En conclusió, hem vist que la seqüència d'ordinals associats a les Hydres de cada pas és estrictament decreixent. Aleshores, qualsevol estratègia és vencedora.

□

3.4 Indecidibilitat en PA del teorema d'Hèrcules i Hydra

En aquest apartat es tracta el perquè no existeix la manera de provar-lo ni refutar-lo sense necessitar una teoria més potent, que inclogui els ordinals transfinits. El que es presenta a continuació està basat en els articles [5], [6] i [9], que presenten resultats de Kirby i Paris. Aquests fan ús, entre d'altres, de mecanismes de Ketonen i Solovay.

Teorema 3.4.1. *Almenys existeix una estratègia recursiva que, tot i ser guanyadora, no es pot demostrar que ho sigui en PA.*

Simplificant, podem afirmar que la impossibilitat de provar el teorema d'Hèrcules i Hydra (3.3.3) en PA radica en el fet que existeixen estratègies recursives en les quals el nombre d'etapes necessàries per vèncer a l'Hydra és immens. Aquesta serà doncs, la manera de demostrar que el teorema 3.3.3 és indecidible en PA.

Es donaran uns indicacions de la demostració d'aquest teorema. Com que el patró de creixement de les seqüències de Goodstein està estretament lligat al creixement dels caps de l'Hydra, ho exemplificarem amb l'esbós de la prova que el teorema de Goodstein (3.3.13) també és indecidible en PA.

3.4.1 Indecidibilitat en PA del teorema de Goodstein

Teorema 3.4.2. *El teorema de Goodstein és indemostrable en PA.*

La raó per la qual el teorema de Goodstein no pot ser provat en PA és l'immens temps que triga la seqüència $\{g_k\}$ a arribar a zero. La causa d'aquest fet és que les seqüències de Goodstein descriuen el mateix comportament que una funció recursiva de creixement ràpid. Exposem unes indicacions de la demostració de que el teorema de Goodstein no pot ser demostrat en PA.

Indicacions de la demostració.

Sigui $\{g_k\}$ una seqüència de Goodstein, la funció de Goodstein $G : \mathbb{N} \longrightarrow \mathbb{N}$ val $k+1$ on k és el menor nombre tal que $g_k = 0$.

Suposo que el teorema de Goodstein és demostrable en PA.

Del teorema de Goodstein es pot deduir que la funció de Goodstein és recursiva i, en particular, està ben definida de $\mathbb{N}$ a $\mathbb{N}$, és a dir, en PA.

Malauradament, això implica pel teorem de Kreisel que, com que la funció $f : \mathbb{N} \longrightarrow \mathbb{N}$ està ben definida en PA, f_α domina f per a algun $\alpha < \epsilon_0$. Però aquest fet contradiu el resultat de Kirby i Paris que afirma que la funció de Goodstein creix amb l'ordre de f_{ϵ_0}.

Aleshores veiem que el teorema de Goodstein no pot ser demostrat en PA.

□

Demostració de la indecidibilitat en PA del teorema d'Hèrcules i Hydra

Amb la finalitat de donar unes indicacions de la prova de la indecidibilitat del teorema d'Hèrcules i Hydra (3.3.3) cal definir una nova operació prèviament.

Definició 3.4.3. $\forall n \in \mathbb{N}$, $\{\alpha\}(n)$ *és una operació dels ordinals* $\alpha < \epsilon_0$ *per inducció sobre* α *que satisfà:*

$\{0\}(n) = 0$

$\{\beta + 1\}(n) = \beta$

$\{\omega^{\gamma+1}(\beta + 1)\}(n) = \omega^{\gamma+1} \cdot \beta + \omega^{\gamma} \cdot n$

i $\forall \delta$ *límit,* $\quad \{\omega^{\delta}(\beta + 1)\}(n) = \omega^{\delta} \cdot \beta + \omega^{\{\delta\}(n)}$

Indicacions de la demostració.

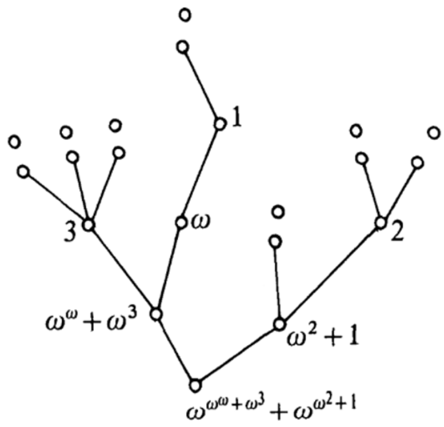
Sigui H l'Hydra del combat.

Primerament, cal assignar un ordinal $\alpha < \epsilon_0$ a cada vèrtex d'H. Ho fem de la següent manera:

- Als vèrtexs superiors els assignem 0.

- A la resta de vèrtexs els assignem $\omega^{\alpha_1} + ... + \omega^{\alpha_n}$ on $\alpha_1 \geq ... \geq \alpha_n$ són els ordinals assignats als vèrtexs que es troben immediatament per sobre.

Vegem com quedaria en l'exemple d'Hydra que hem donat abans:



L'ordinal associat a H és l'ordinal que assignem al vèrtex arrel. És a dir, en aquest cas, l'ordinal d'H és $w^{w^w+w^3} + w^{w^2+1}$.

Ara, per a qualsevol estratègia σ, definim l'operació $[\alpha]_\sigma(n)$. Aquesta envia l'ordinal d'H després del pas $n-1$ a l'ordinal d'H després del pas n.

Aleshores, sigui τ una estratègia recursiva tal que $[\alpha]_\tau(n) = \{\alpha\}(n+1)$, vegem que τ és una estratègia guanyadora.

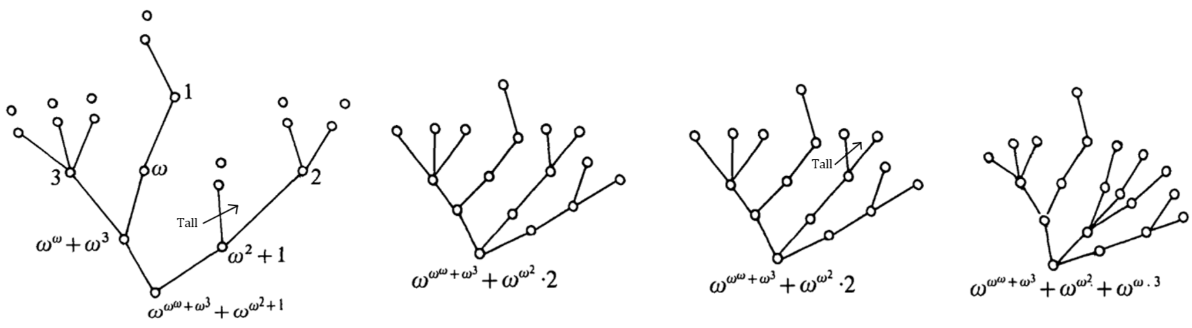
Definim l'algoritme que segueix τ:

- Començant pel vèrtex arrel, pugem per l'arbre H fins trobar un vèrtex.

- Llavors, escollim el vèrtex d'immediatament sobre d'aquest tal que tingui associat el menor ordinal.

- Si n'hi ha més d'un amb el mateix ordinal, triem el que estigui més a l'esquerra.

- Fem això fins que arribem a un vèrtex superior, aleshores tallem el cap que hi està unit.



Pas 1 Després del pas 1 Pas 2 Després del pas 2

Demostrar que l'estratègia τ és vencedora és equivalent a la prova de la ϵ_0-inducció respecte $\{\alpha\}(n)$. Usant resultats de Ketonen i Solovay, sabem que si això fos veritat, la funció $\lambda nx \cdot g_n(x)$ estaria ben definida i seria recursiva. Com que això és impossible en PA, obtenim que també és impossible demostrar que τ és guanyadora. I, per tant, queda vist el que volíem demostrar.

$\square$

Capítol 4

Conclusions

Aquesta memòria constitueix un repàs dels descobriments entorn a certes característiques dels sistemes formals. Se centra en l'estudi de la incompletesa, la consistència i sobretot la indecidibilitat de certs resultats en l'aritmètica de Peano. I, finalment, profunditza en els factors que provoquen la impossibilitat de provar amb eines de PA enunciats del llenguatge de l'aritmètica.

El fet que puguem enunciar quelcom en el marc d'una teoria, però no provar que allò és cert ni fals dins d'aquesta, sembla difícil de creure. Els teoremes de Goodstein i d'Hèrcules i Hydra són exemples naturals d'això que en faciliten la comprensió. No obstant, hi ha molts altres resultats als quals els ocorre el mateix.

Tot i que, només hem vist aquesta problemàtica en el context de l'aritmètica de Peano, no només té lloc en aquesta teoria. Però, he pres aquest enfocament perquè he trobat curiós que es pogués relacionar tan estretament un mite de l'antiga Grècia amb les matemàtiques.

Bibliografia

[1] https://plato.stanford.edu/.

[2] https://risingentropy.com/the-mindblowing-goodstein-sequences/. 2020.

[3] https://en.wikipedia.org/wiki/Transfinite_number/. 2022.

[4] Joan Bagaria. *Fundamentals of Mathematical Logic*. ICREA and Universitat de Barcelona, 2004-05.

[5] E Adam Cichon. A short proof of two recently discovered independence results using recursion theoretic methods. *Proceedings of the American Mathematical Society*, 87(4):704–706, 1983.

[6] Laurie Kirby and Jeff Paris. Accessible independence results for peano arithmetic. In *Bulletin of the London Mathematical Society*. Citeseer, 1982.

[7] Antoine Nectoux. http://blog.kleinproject.org/?p=674. 2015.

[8] Panu Raatikainen. Gödel's Incompleteness Theorems. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Spring 2022 edition, 2022.

[9] Will Sladek. The termite and the tower: Goodstein sequences and provability in pa, 2007.

[10] Edith Sánchez. https://lamenteesmaravillosa.com/mito-hidra-lerna//.

[11] Eduardo Piza Volio. hércules contra la hidra y la muerte del internet. *Revista de Matemática: Teoría y Aplicaciones*, 11(1):1–16, 2004.