# Making Explicit a Constant Appearing in an Impossible Equation of Carl and Moroz

Matthew Weidner Carnegie Mellon University

February 28, 2020

#### Abstract

Recently, Carl and Moroz [1] constructed a Diophantine (integer polynomial) equation for which it is impossible to decide whether the equation has any (integer) solutions. However, their presentation is not as explicit as it could be, instead involving implicitly defined polynomials spread out over many pages. In particular, they give a two page description of a crucial constant without bothering to explicitly compute it. We resolve this issue using a bit of Python, SageMath, and 878 MB of disk space.

## 1 Introduction

The Matiyasevich–Robinson–Davis–Putnam (MRDP) theorem [4] states that Diophantine equations (polynomial equations with integer coefficients) are "Turing complete", in the sense that for any recursively enumerably set of integers S, there is a polynomial f with integer coefficients such that  $S = \{n \mid \exists x_1, \ldots, x_k \in \mathbb{Z}. \ f(n, x_1, \ldots, x_k) = 0\}$ . This famously implies that is undecidable to determine whether a Diophantine equation has any (integer) solutions, giving a negative answer to Hilbert's Tenth Problem.

Another consequence is that it is in principle possible to take your favorite axiomatization of mathematics, such as ZFC set theory, and construct a Diophantine equation such that, within that axiomatization, one can neither prove nor disprove whether the equation has any solutions. Recently, Carl and Moroz [1] did exactly this for Gödel-Bernays set theory, which has the same set of provable statements about sets as ZFC [5]. That is, they describe how to write down an "impossible" Diophantine equation such that, within "mathematics as we know it", one cannot prove or disprove whether it has a solution. However, their presentation is not as explicit as it could be—the equations are spread out over many pages, and some of them are not written explicitly as polynomials, instead involving polynomial functions of other polynomials.

It would be aesthetically pleasing to write down their impossible equation in an explicit, easily interpreted form. Such forms are known for a separate consequence of the MRDP theorem: just as one can construct universal Turing machines, one can construct universal Diophantine equations, which can be made to emulate any Turing machine by fixing some variable values. For example, there is a computable encoding of Turing machines as triples of integers (z, u, y), and Turing machine inputs as integers x, such that the Turing machine corresponding to (z, u, y) accepts input x iff the following system of equations has a solution [3]:

$$\begin{split} elg^2 + \alpha &= (b - xy)q^2, \quad q = b^{560}, \quad \lambda + q^4 = 1 + \lambda b^5, \quad \theta + 2z = b^5, \quad l = u + t\theta, \\ e &= y + m\theta, \quad n = q^{16}, \quad r = [g + eq^3 + lq^5 + (2(e - z\lambda)(1 + xb^5 + g)^4 \\ &\quad + \lambda b^5 + \lambda b^5 q^4)q^4][n^2 - n] + [q^3 - bl + l + \theta\lambda q^3 + (b^5 - 2)q^5][n^2 - 1], \\ p &= 2ws^2r^2n^2, \quad p^2k^2 - k^2 + 1 = \tau^2, \quad 4(c - ksn^2)^2 + \eta = k^2, \\ k &= r + 1 + hp - h, \quad a = (wn^2 + 1)rsn^2, \quad c = 2r + 1 + \phi, \\ d &= bw + ca - 2c + 4a\gamma - 5\gamma, \quad d^2 = (a^2 - 1)c^2 + 1, \quad f^2 = (a^2 - 1)i^2c^4 + 1, \\ (d + of)^2 &= ((a + f^2(d^2 - a))^2 - 1)(2r + 1 + jc)^2 + 1. \end{split}$$

A related fun result is the statement that any provable mathematical statement has an alternative proof consisting of 100 additions and multiplications of integers [3, Theorem 5].

Our work is a first step towards putting Carl and Moroz's equation into an aesthetically pleasing form. Specifically, we compute a constant which is defined implicitly in their work using two pages of equations, many of which are not true polynomials but instead involve polynomial functions of other polynomials.

# 2 The Impossible Equation and its Constant

Briefly, Carl and Moroz construct their equation as follows. Let  $\mathcal{L}$  denote the language of first-order logic with a single binary predicate symbol. First, they construct a polynomial  $f(t, \vec{x})$  which is a Diophantine version of a computer program that checks whether  $\vec{x}$  encodes a proof of t in  $\mathcal{L}$ . Thus for any statement P of  $\mathcal{L}$ , letting  $t_P$  be their integer encoding of P, P is provable in  $\mathcal{L}$  iff there exist integers  $\vec{x} \in \mathbb{Z}^{14558112}$  such that  $f(t, \vec{x}) = 0$ .

Next, they explain how to write down the integer encoding of the statement "the axioms of Gödel-Bernays set theory imply a contradiction". Specifically, the authors encode the statement

$$A_1 \Rightarrow (A_2 \Rightarrow (\cdots (A_{15} \Rightarrow (\forall x.x \in x))\cdots)),$$
 (1)

where  $A_1, \ldots, A_{15}$  are the axioms of the theory, and  $\in$  is the binary predicate symbol of  $\mathcal{L}$ . The axioms are meant to model that  $\in$  denotes ordinary set inclusion, and in particular, they imply that  $\forall x.x \in x$  is false, so this statement is provable iff Gödel-Bernays set theory is inconsistent. Thus by Gödel's second incompleteness theorem [2], the statement can be neither proved nor disproved within Gödel-Bernays set theory, hence within all of ordinary mathematics.<sup>2</sup>

In the author's notation, the integer encoding of (1) is denoted  $f_{15}(\vec{a},3)$ , where  $f_{15}$  is defined in equation (5) on page 49, and  $\vec{a}$  is the vector of the values  $a_1, \ldots, a_{15}$  defined in Section 8.

Our computation computes this  $f_{15}(\vec{a},3)$ .

# 3 Computation

Our program<sup>3</sup> is a straightforward Python transcription of the equations defining  $f_{15}(\vec{a},3)$  in [1]. One exception is that we re-order the axioms in (1) by the magnitude of their integer encodings. This helps to keep the magnitude of the overall result small, since the magnitude of  $B \Rightarrow C$  is approximately the square of the sum of the magnitudes of B and C. With the original axiom ordering, the program ran out of memory before finishing despite having 16 GB of RAM.

While the program could be run in Python, we actually ran it using SageMath [6]. This is about  $100 \times$  faster due to SageMath's use of the GMP library for integer arithmetic. It takes 11 minutes to run on the author's CMU-issued laptop.

The resulting value is 877,757,576 decimal digits long.

### 4 Result

We now include as many digits of the result as the editor will allow. We hope the reader finds its aesthetics more pleasing than the original presentation in [1], perhaps even on-par with the universal Diophantine equation reproduced above. The full result is available on a flashdrive by request from Gates 5005.

<sup>&</sup>lt;sup>1</sup>They use Gödel-Bernays set theory instead of the better-known ZFC set theory because Gödel-Bernays has only finitely many axioms, whereas some of ZFC's "axioms" are actually axiom schemas which describe infinite sets of first-order statements.

<sup>&</sup>lt;sup>2</sup>Unless the axioms are inconsistent, in which case we have bigger problems to worry about!

 $<sup>^3</sup>$ http://mattweidner.com/diophantine\_impossible/diophantine\_impossible.sage

```
695625203950800210600411251141612864337550179304017966106528945313026379073842199545157616068260096095799999297373390022609680578099743507386916378544\\127810195558352207068808792219590834862172328815682879321161938049540653107791138626960875999470472077995426505365709201076234444452428779172865531931
687380954460771395517965079737053303957103904583764921606505693215931816823669807454911524236297809084333734902634388557991182791004179213352767126051\\477649095567744930033917716600797014283201164867033119172443760968785631969314287940442111993198477651786650446091288313791981817005637553541988320594
608697169744128340094124417299190837362752285410022945985549659124712450620950285311042570224749400708758495977996167605824265797255111465901661650648\\304336316043722757688366000891240492112081990642824458976514642730043871902209625227886635099062978810711085882221144478148824287024729393476820104558
127775296178082051897808851040063447926413786454858791035648768240948655311729536714997407310972372822764231621632702924837481300222103761727230204687\\347084236329309606663111928059691340573889876254662894538095227907187612062983099663418965779116893658411896721674751292789607777604679128769634246846
453937205108782925225164970954535998023779518684741398764853506916066958081103724337375209388680081409084016384934820622273584084839545302501474070116\\421952997327163764266587061915585736708433359816950126961242887258809063959236161019337158575468986353417194272077303741382774134426223945721335425901
33291497531441531560911848444299479992766926025027793579342285124542249256453435237264457716366723155624269969032889399710928868156042853449889513961
435377613263552140356656961983346631871921392253969534297620797551025938432811374698718285262679036593214121882411029051893808439345906779692817495769
686643481019218601109532021734471555588252652342067586130520934865800849946806533922176870082007193186584516617448834866868158622161221137969886438435
\frac{646048875422555415521844250791994979414411344766714570541928910309108780588612880211863831446509446666614130179639517821083755664797375231477548799774342232860122624158026644531903752714213568574181133926026698254520191059371599501686296620916429290965952587467829398614548208547150159155332546245681
213758849892567160690125956477447778607779146072414827264965126475042661163916155061646545200376374531091955160263732747087778031000765395089803492508\\ 457106649722805558289800199202190265333463240737232263115834987784634023024231557986620347535933327956165335588279729818780896698969131292310331844582
208693138763945968935173256625137383425866488387277171597283863966024513646556673632898787586250319284735322624998275959922149972719257007612138492543
033269303161748052268676862642233076290780708002093805323926312318717632571277564547515011217516888044393491964498998960696251433578046978251009728084\\148305256608712117382899627618092932983357278773502930014723954015602752878532299451370294927456875033801390660546710951085898988817601703700283161443
937496703350060577816223389456981074628639798723722287901224336409989259419848861751676184941977402256871270092826081555541095930469121555372303139520
053723862339295313335928009335310551229240913443669352582716353882928066956871352826559508629284917242771959009100999142688999591605403387546359432538
936809414291527869318847639948920679605102892103714534565932583612839336859256183118957907129960682753702993093420668317355231987279651083849808234215
836698887545790173027181778241239544431292277473080904009106337091929759174832940573854568188733781400868197509674911219799139136921381891752594759418
024854315134387095479847880212889617302176003706934430000394646644874070810266940004170119127129090408093559320592962932525236715284752228754228091798\\405497228411026947001296897352114639725012631480020572902258413741709133684523696655525412483692552994093975020451854104483398813005174417681467583503
586772179856561973509245868552019721846333928752522184633461969272774958635722279510131803819032875031814301927864220309441141862126969339890090920045\\ 556917374782134333707761902203322272241484428879353217986053829692567812925791792208140878871602473587992031314371271471406099624588730090401138410692
808806916396581544375483762501301897862718396765991240330958001764522369485747560021173262517870120377053329425268114579028961252617502770513088802373\\377640931067730853366651677568449761170014852868878251762735090286834969290971910014080917532809508642770768882845524494789008481841829143057112808094
302938201818253578486740819680307299996492138141073855132090828610056271175109739150576611256387097559273493034942152103727416827578407266009560108864\\738985641625548063957628744151994206217409025346442911482831451664392082926544951057444731428927438894566768906981871052552022180520336111974031509855
143555666902178561755866718369850234255717734904423183962144309366502879297750315770639530769027557173294979525519749373446870761208527765134477248320\\246121567992015855518586906140516317918216426479621543126147053725126395064001931468841516969724159936596923203322262110328950068120523655462996631295
761078423005143374141239850576411760938164322127600610431770594422596597686599729573836873394184198758426110199728955077008195432379143516590629696066\\845604490505626285726004607291914053582512930335571354949784689867766130463984559168468859209955524601174296926214665575920006308555982369232238748823
124473427433270661089837065907347455659619741502341777888243485237262097528884743540489299510138521014172890470072414636825880709789064318959126563902\\297580768981617190173584203387754779456742769870684128496229372580591554899079646605894644178861467893689405972501210611279915364268249170779537167743
848868492538409262050352515573541636195568304290333607446922969040781388818718589415953592701940164503440795273714025053498630055542022446997939035641
719263907872844442553614709923551858333116282892743979685996525858835888340707518123939457797547959645912735143558571752480741636858140702859131818835
407730730883327403870908280965842821351623553674011337111108485999672417940483859372876865089986131323581100662663728598726368220345155385764141591025
724988120283006467860632573194930616200207495351425084623518415702760799118599461637320123241501775559548739034224711371289061291472994875576720834483\\426874601930333875757105249272267274910263996174055495362100521197234653677367675414278055928005024603142816535025787676675782794891854063119248827592
```

 $908528140581247256442448819469116746180914283547092667022405513584305990148976245286722180296782115235610878545099794581971342410128294767562709645379\\252187218291128816485145059937304314523834519320108377289810959965158026663157275930080896247366106175684198730702916667593306386225407193464328968456$ 494831691650721161062465887631338222740503782999201561094184209421151652465897687788450778131221224054948161693341017450112877216811066161237608182304 33415496066063789929391635617654906893939392592064676651242420205464071456056393456463340250949719965235044416017733728934446604635143255137220282307 905486870181408220331895359593194263817678482890220304398212750621607335517634734806899842702058535075991594150086098126588782841663760129691270009228 079997518933180794927903249900281765520384461286595047993286003782887065747839211774790393809591922016373812913580878079873839289295014111430582126601 413127581349451214822661896390314434298867678151369702321626405116556211135428677974137404377401854118749714774560812001698820813736509933053568152354  $546546999858482437063639502119082235278554019913565931521205837465500886352764438056129449297463673449735744852703948483346099334956478284831900770381\\282372219683858182321802769633895972151971030608565087957862083782221923029240623684940815539187668940087835674290501761893762834913308003011945356302$  $914794676527524083023242487569717893259676477397623104027099956734623259553655444103083247401426229704461227289154503503424728226464804447325804951908\\186067371178587034501926716880411702037401240977123199852245975756694418977438212245599030478130680537533076572370516077259310384402267211417688962358$ 417231596598316068088408622857156843615738494265647252190880570748585511399534759096207737357363929828397597424971940576591111731332821826143339443603670583876728072627735068838432915199483374818199284820205902605622992430427847226160199204357600613234765599297228938063740551153447598960343804826253022976969747510943907372963018653704070843746450553021382313941802612398779491350440490737846605041945796417397311054338626608196543067688466750715097616076761607676160767616076761607676160767616076761607676160767616076761607676160767616076761607676160767616076761607676160761607676160767616076160767676160767616076761607676160767616076160761607616076160761607616076761607616076160761607616076160761607616076160761607616076160767616076076160760717036315110683879760954166966954702064243794134960601941719837308047950762569714336878345215764824171302726727100307444859044744194346323897767952949 955354467602251489634483990040534048977589511318289110180944127477465165839140034801757511085330773629138638535050716047408567029912002542754021832233 289434929967065961650481042249529946728506249025067146172598638587403031120194247131623871877307550565631699718195661836805325925271723912478438258693 507971666744746905056925988486734726598454560667472051572585401706864143647534894479089591524315751312892126687916408910395283568225372553858274907594  $206348565052459282391447068111270205455654600553295884506348917641102137327750390384420156663024849145758600847175899117674727213920386096228698377\dots$ 

### References

- [1] M. Carl and B. Z. Moroz. On a Diophantine representation of the predicate of provability. *Journal of Mathematical Sciences*, 199(1):36–52, 2014.
- [2] K. Gödel. Über Formal Unentscheidbare Sätze der Principia Mathematica und Verwandter Systeme, I. Monatshefte für Math. u. Physik, 38:173–198, 1931.
- [3] James P. Jones. Universal Diophantine equation. The Journal of Symbolic Logic, 47(3):549–571, 1982.
- [4] Yu. V. Matiyasevich. Enumerable sets are Diophantine (in Russian). *Doklady Akademii Nauk SSSR*, 191(2):279–282, 1970.
- [5] M. Szudzik. von Neumann-Bernays-Gödel Set Theory. MathWorld-A Wolfram Web Resource, created by Eric W. Weisstein. http://mathworld.wolfram.com/vonNeumann-Bernays-GoedelSetTheory.html.
- [6] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 9.0), 2020. https://www.sagemath.org.