ISSN: 2446-6719



A Simple Theory Containing its Own Truth Predicate

Nicholas Shackel

Abstract

Tarski's indefinability theorem shows us that truth is not definable in arithmetic. The requirement to define truth for a language in a stronger language (if contradiction is to be avoided) lapses for particularly weak languages. A weaker language, however, is not necessary for that lapse. It also lapses for an adequately weak theory. It turns out that the set of Gödel numbers of sentences true in arithmetic modulo n is definable in arithmetic modulo n.

Keywords: Truth, Predicate, Definable, Arithmetic modulo n

Introduction

Tarski's indefinability theorem gives us that 'the set of Gödel numbers of sentences true in [arithmetic] is not definable in arithmetic' (Boolos and Jeffrey 1989: 176). The requirement to define truth for a language in a stronger language (if contradiction is to be avoided) lapses for particularly weak languages, for example, Myhill's system which lacks negation (Quine 1980:137 fn 10). But a weaker language is not a prerequisite for that lapse. It also lapses for an adequately weak theory. It turns out that the set of Gödel numbers of sentences true in arithmetic modulo n is definable in arithmetic modulo n.

Notation

- L is the first order language of arithmetic.
- Sent(L) is the set of closed sentences of L.
- $\underline{0}^M$, $+^M$, \times^M etc. is what is denoted in a model M by the respective members of L.

- ϕ and ψ are always closed sentences of L.
- \underline{n} is the symbol $ss...s(\underline{0})$: n repetitions of s.
- [m] is the equivalence class of natural numbers defined by the relation 'having the same remainder on division by n': alternatively, and equivalently, the element $m+n\mathbb{Z}$ in the quotient ring $\mathbb{Z}/n\mathbb{Z}$, (i.e. in \mathbb{Z}_n).
- # is a Gödel coding
- $\lceil \phi \rceil$ is the Gödel numeral for $\# \phi$
- *M* is a model. In speaking of models *M*, I use '*M*' to refer both to the model and its domain, unless the context requires them to be distinguished.

1 Q_n : Modulo n arithmetic

We meet modular arithmetic in number theory, where congruence modulo n aids the study of divisibility and in algebra as the quotient ring $\mathbb{Z}/n\mathbb{Z}$, whose elements defined in terms of cosets of the ideal $n\mathbb{Z}$ turn out to be the equivalence classes induced by the congruence relation. Modular arithmetic is the structure of the ring of integers \mathbb{Z}_n .

For the purposes of this paper, Q_n is modulo n arithmetic, for n>1, with the following 7 axioms and 1 axiom schema:

- 1. $\underline{n} = \underline{0}$
- 2. $\forall x : (x = \underline{0} \lor x = \underline{1} \lor \ldots \lor x = \underline{n-1})$
- 3. $s(\underline{0}) \neq \underline{0}$
- 4. $\forall x : x + 0 = x$
- 5. $\forall x \forall y : x + s(y) = s(x + y)$
- 6. $\forall x : x \times 0 = 0$
- 7. $\forall x \forall y : x \times s(y) = x \times y + x$
- 8. Axiom schema. For any m that is a factor of n, $\underline{m} \neq \underline{0}$.

¹Factors of n, or multiples of such factors, are divisors of zero modulo n, which fact prevents us proving the inequation $\underline{\mathbf{m}} \neq \underline{\mathbf{0}}$ from the axioms already given. We need the inequations to guarantee the isomorphism of all models of Q_n

Properties of Q_n

- (i) $Q_n \vdash \forall x \forall y (s(x) = s(y) \rightarrow x = y)$).
- (ii) $Q_n \vdash \forall x \exists y (x = s(y)).$
- (iii) $m \not\equiv k \pmod{n}$ iff $Q_n \vdash \underline{m} \neq \underline{k}$.
- (iv) If $j \equiv m + k \pmod{n}$ then $Q_n \vdash j = \underline{m} + \underline{k}$.
- (v) If $j \equiv m \times k \pmod{n}$ then $Q_n \vdash \underline{j} = \underline{m} \times \underline{k}$.

The **intended model M** of Q_n is $(D, [0], \sigma, \oplus, \otimes)$, defined by:

- 1. $dom(\mathbf{M}) = \{[0], [1], \dots, [n-1]\}$
- 2. for all k < n 1, $(\sigma[k]) = [k + 1]$
- 3. $\sigma([n-1]) = [0]$
- 4. $[k] \oplus [l] = [k+l]$
- 5. $[k] \otimes [l] = [k \times l]$

Clearly, $\mathbf{M} \models Q_n$. \mathbf{M} is just the ring \mathbb{Z}_n (or isomorphic to \mathbb{Z}_n if you prefer) since for $0 \le m < n$, [m] is the equivalence class of $m \pmod{n}$, and so it is also the relevant coset of the ideal $n\mathbb{Z}$, and hence $\mathbf{M} =$ the quotient ring $\mathbb{Z}/n\mathbb{Z}$. It is obvious from arithmetic that \mathbf{M} satisfies R1 - 8. Straightforwardly we have identities, inverses, associativity of and closure under \oplus and \otimes , commutativity of \oplus and left and right distributivity of \otimes over \oplus .

Interpretations of Q_n will have to use $\underline{0}$ to name [0]. However, for some n the numerals naming the other members of \mathbf{M} will be permutable whilst preserving truth. We shall make use of interpretations of Q_n that use the numeral \underline{m} to name [m].

Proposition 1.1 If $M \models Q_n$, then the domain of M has n members.

Proof. By the domain axiom, M has the form $\{\underline{0}^M, \dots, (\underline{n-1})^M\}$ so the domain has $\leq n$ members. There are n distinct elements by the inequations (property (iii)) so the domain has $\geq n$ members.

Theorem 1.2 All models of Q_n are isomorphic to \mathbf{M} .

Proof.

Let $M^* \models Q_n$. Let ρ be the function $\rho : \mathbf{M} \mapsto M^*$ such that: $\rho : \underline{m}^{\mathbf{M}} \mapsto \underline{m}^{M^*}$. ρ is a surjection. Suppose $x \in M^*$. Then $x = \underline{m}^{M^*}$ for some \underline{m} in L. Hence $\underline{m}^{\mathbf{M}} \in \mathbf{M}$ and $\rho(\underline{m}^{\mathbf{M}}) = \underline{m}^{M^*}$

 ρ is an injection. Suppose for a contradiction that $\underline{m}^{\mathbf{M}} \neq \underline{k}^{\mathbf{M}}$ but $\rho(\underline{m}^{\mathbf{M}}) = \rho(\underline{k}^{\mathbf{M}})$. Then $Q_n \vdash \underline{m} \neq \underline{k}$ (property (iii)) and hence, since Q_n is sound, $\underline{m}^{M^*} \neq \underline{k}^{M^*}$. But if $\rho(\underline{m}^{\mathbf{M}}) = \rho(\underline{k}^{\mathbf{M}})$, then $\underline{m}^{M^*} = \underline{k}^{M^*}$, which is the contradiction we sought.

Preservation of successor. We need to show that $\rho(\sigma(\underline{m}^{\mathbf{M}})) = \sigma^*(\rho(\underline{m}^{\mathbf{M}}))$. LHS of equation.

$$\sigma(\underline{m}^{\mathbf{M}}) = \sigma([m]) = [m+1] = (\underline{m} + \underline{1})^{\mathbf{M}}$$

so

$$\rho(\sigma(\underline{m}^{\mathbf{M}})) = \rho((\underline{m} + \underline{1})^{\mathbf{M}}) = (\underline{m} + \underline{1})^{M^*}$$

RHS of equation. We have

$$\sigma^*(\rho(\underline{m}^{\mathbf{M}})) = \sigma^*(\underline{m}^{M^*})$$

and since

$$Q_n \vdash s(\underline{m}) = s(\underline{m} + \underline{0}) = \underline{m} + \underline{1}$$

then soundness gives

$$\sigma^*(m^{M^*}) = \sigma^*((m+0)^{M^*}) = (m+1)^{M^*}$$

whence LHS = RHS.

Preservation of addition.

Suppose $[m] \oplus [k] = [j]$. Then $Q_n \vdash \underline{j} = \underline{m} + \underline{k}$ (property (iv)), when by soundness

$$\begin{split} \underline{m}^{M^*} + ^{M^*} \underline{k}^{M^*} &= \underline{j}^{M^*} \\ \text{i.e. } \rho(\underline{m}^{\mathbf{M}}) + ^{M^*} \rho(\underline{k}^{\mathbf{M}}) &= \rho(\underline{j}^{\mathbf{M}}) \\ \text{i.e. } \rho([m]) + ^{M^*} \rho([k]) &= \rho([m] \oplus [k]) \end{split}$$

Preservation of multiplication. Similar proof to addition with \otimes for \oplus , \times for + and the use of property (v) instead of property (iv).

Theorem 1.3 Q_n is not weaker than the theory of rings.

Proof. Since **M** is a ring and all models of Q_n are isomorphic, there cannot be non-standard models (in which, e.g. $\forall x \forall y : x+y=y+x$ is not true) which can be used to show Q_n is weaker.

Theorem 1.4 Q_n is complete.

Proof. Suppose Q_n is not complete. Then there is a sentence ϕ such that ϕ is true in at least one model and false in at least one model of Q_n . But this is impossible, since all models are isomorphic.

Corollary 1.5 For any model, $M, Q_n \vdash \phi$ iff $M \models \phi$.

Definition 1.6 The truth set $\mathbf{T}_n = \{ \phi \in Sent(L) : M \models \phi \}$

Corollary 1.7 All models of Q_n have the same truth set (which is just the set of theorems of Q_n)

2 Finite Models

Theorem 2.1 For any finite model M the truth set is decidable.

Proof. First of all, the truth value of any atomic formulae can be determined by a finite calculation, as can any finite Boolean combinations of such formulae.

Let ϕ be a formula of the form $\forall x : \chi(x)$, where χ has only x free. Then, $M \models \phi$ iff $M \models \chi(\underline{0}) \land \chi(\underline{1}) \land \cdots \land \chi(\underline{n-1})$. Likewise, an existentially quantified formula $\exists x : \chi(x)$ can be expressed as a finite disjunction and M satisfies it iff M satisfies the finite disjunction. Hence, any singly quantified formula can be re-expressed as a finitely long Boolean combination.

An example will illustrate the general proof. Let ϕ be a closed prenex formula $\forall x_1 \exists x_2 : t(x_1, x_2) = u(x_1, x_2)$. We now inflate by use of the facts just mention to get a formula satisfied by M iff $M \models \phi$. From the outside moving in we get

$$\exists x_2 : t(\underline{0}, x_2) = u(\underline{0}, x_2) \land \exists x_2 : t(\underline{1}, x_2) = u(\underline{1}, x_2) \land \dots$$
$$\dots \land \exists x_2 : t(\underline{n-1}, x_2) = u(\underline{n-1}, x_2)$$

and then

$$\begin{aligned} &(t(\underline{0},\underline{0}) = u(\underline{0},\underline{0}) \wedge t(\underline{1},\underline{0}) = u(\underline{1},\underline{0}) \wedge \dots \wedge t(\underline{n-1},\underline{0}) = u(\underline{n-1},\underline{0})) \\ &\vee \dots \dots \\ &\vee \dots \dots \\ &\vee (t(\underline{0},\underline{n-1}) = u(\underline{0},\underline{n-1}) \wedge t(\underline{1},\underline{n-1}) = u(\underline{1},\underline{n-1}) \wedge \dots \\ &\dots \wedge t(\underline{n-1},\underline{n-1}) = u(\underline{n-1},\underline{n-1})) \end{aligned}$$

This is a Boolean combination of a finite number of atomic formulae so its truth value can be worked out by a finite calculation.

Evidently, any closed prenex formula with m quantifiers at the front can be inflated in stages in this way to a Boolean combination of n^m atomic formulae

each of the form $t(x_1, \ldots, x_m) = u(x_1, \ldots, x_m)$ Once again, its truth value can be worked out by a finite calculation.

Therefore a Turing machine can determine whether a closed formula belongs to \mathbf{T}_n , and hence the characteristic function of \mathbf{T}_n is recursive.

Theorem 2.2 The truth set for models of Q_n is decidable.

Proof. Apply proposition 1.1, theorem 2.1 and corollary 1.7. Models of Q_n are finite so have decidable truth sets, which are all identical.

Theorem 2.3 Q_n is decidable.

Proof. For any model M of Q_n , the truth set \mathbf{T}_n of M is decidable. $Q_n \vdash \phi$ iff $M \models \phi$ so any decision procedure for \mathbf{T}_n will yield a decision procedure for Q_n

3 The Truth Predicate for Q_n

A truth predicate for Q_n , satisfying Tarski's material adequacy condition would be a predicate $T_n(x)$ such that for all $\phi, Q_n \vdash T_n(\lceil \phi \rceil) \leftrightarrow \phi$

Lemma 3.1
$$\lceil \phi \rceil^{M} = [\# \phi]$$

Proof. $\lceil \phi \rceil$ is the Gödel numeral for $\# \phi$ so the object in \mathbf{M} named by it is $\llbracket \# \phi \rrbracket$

Definition 3.2 Let Θ be any theory in the language L, M be any model of Θ . An **acceptable** M **coding for a theory** Θ is a Gödel coding # such that for any closed formulas ϕ, ψ , if $\lceil \phi \rceil^M = \lceil \psi \rceil^M$ then for any model M^* of $\Theta, M^* \models \phi$ iff $M^* \models \psi$

We are interested only in acceptable \mathbf{M} codings for Q_n , which from hereon we call acceptable codings. Not all codings are acceptable for Q_n . The simplest unacceptable coding can be got by an injection from expressions into the set of multiples of n (see proposition 4.1 below).

Lemma 3.3 For acceptable codings #, for any closed formulas ϕ, ψ , any of the following equivalent propositions:

1. (a)
$$\lceil \phi \rceil^{\mathbf{M}} = \lceil \psi \rceil^{\mathbf{M}}$$

(b)
$$\#\phi \equiv \#\psi \pmod{n}$$

(c)
$$[\#\phi] = [\#\psi]$$

implies any of the following equivalent propositions:

- 2. (a) $\mathbf{M} \models \phi \text{ iff } \mathbf{M} \models \psi$
 - (b) $\phi \in \mathbf{T}_n$ iff $\psi \in \mathbf{T}_n$
 - (c) $\mathbf{M} \models \phi \leftrightarrow \psi$
 - (d) $Q_n \vdash \phi \leftrightarrow \psi$

Proof. The definition gives us that if 1(a) then 2(a) and so equivalents to 1(a) imply equivalents to 2(a).

Lemma 3.4 Let # be an acceptable coding and ϕ, ψ closed formulae. If $\#\phi \equiv \#\psi \pmod{n}$ then $\phi \in T_n$ iff $\psi \in T_n$.

Proof. Using the aforementioned equivalences

Remarks 3.5 Essentially, this lemma is telling us that an acceptable coding is a Gödel coding such that if the Gödel numbers of two closed sentences in L are in the same equivalence class modulo n, then they have the same truth value.

Lemma 3.6 For any Q_n an acceptable Gödel coding exists.

Proof. Let P be the set of primes and R the set of primes in the prime factorisation of n. Use P\R as the basis for a powers of primes Gödel coding g. Then define the following function $\#: L \mapsto \mathbb{N}$

$$\#\phi = \begin{cases} n \times g(\phi) \text{ if } \phi \in \mathbf{T}_n \\ g(\phi) \text{ if } \phi \notin \mathbf{T}_n \end{cases}$$

By the unique prime factorisation theorem # is an injection and

$$\#\phi \in \mathbf{T}_n$$
 iff $[\#\phi] = [0]$ (since for all ϕ, n is a factor of $n \times g(\phi)$)

$$\#\phi \notin \mathbf{T}_n$$
 iff $[\#\phi] \neq [0]$ (since for all ϕ, n is a not factor of $n \times g(\phi)$)

If the characteristic functions of the conditions for a function defined by cases from recursive functions are themselves recursive then the function defined by cases is also recursive. Since \mathbf{T}_n is decidable the characteristic function for membership of \mathbf{T}_n is recursive. Both g and multiplication by n are recursive functions. Hence # is recursive. Therefore # is a Gödel coding. For any ϕ, ψ, ϕ and ψ will have Gödel numbers congruent modulo n only if they have the same truth value. Therefore # is an acceptable coding.

Definition 3.7 We make use of an acceptable coding, #. Let $K_n = \{k_1, \ldots, k_i\}$ be the set such that

```
k \in K_n iff 0 \le k < n and there exists a \phi such that \phi \in \mathbf{T}_n and k \equiv \#\phi \pmod{n}
```

So K_n is the set of numbers between 0 and n-1 which are congruent to the Gödel numbers of the true sentences of Q_n .

Lemma 3.8 If # is acceptable then for any $\phi, \phi \in \mathbf{T}_n$ iff for some $k \in K_n, [\#\phi] = [k]$.

Proof. Suppose that $\phi \in \mathbf{T}_n$. By the division algorithm for some r such that $0 \le r < n$, $\#\phi \equiv r \pmod{n}$ and hence $r \in K_n$. Suppose that for some $k \in K_n$, $k \equiv \#\phi \pmod{n}$. Then for some $\psi \in \mathbf{T}_n$, $k \equiv \#\psi \pmod{n}$, so $\#\phi \equiv \#\psi \pmod{n}$, hence $\phi \in \mathbf{T}_n$ iff $\psi \in \mathbf{T}_n$ (because # is acceptable), whence $\phi \in \mathbf{T}_n$

Theorem 3.9 Let the open L-formula $T_n(x)$ be the open formula $(x = \underline{k_1} \lor x = \underline{k_2} \lor \cdots \lor x = \underline{k_i})$. $T_n(x)$ defines truth in Q_n (and hence in \mathbf{M}).

Proof. We make use of an acceptable coding, #. For any $\phi \in Sent(L), Q_n \vdash T_n(\ulcorner \phi \urcorner)$

```
iff \mathbf{M} \models T_n(\lceil \phi \rceil) (soundness and completeness) iff \mathbf{M} \models [(\lceil \phi \rceil = \underline{k_1}) \lor (\lceil \phi \rceil = \underline{k_2}) \lor \cdots \lor (\lceil \phi \rceil = \underline{k_i}) iff either [\#\phi] = [k_1] or [\#\phi] = [k_2] or ... or [\#\phi] = [k_i] iff, for some k, [\#\phi] = [k] and k \in K_n iff \phi \in \mathbf{T}_n (by lemma 3.8)
```

Theorem 3.10 $T_n(x)$ is a truth predicate satisfying Tarski's material adequacy condition, i.e. for all $\phi \in Sent(L), Q_n \vdash T_n(\lceil \phi \rceil) \leftrightarrow \phi$

Proof. Given any ϕ , $\mathbf{M} \models T_n(\lceil \phi \rceil)$ iff $\phi \in \mathbf{T}_n$ iff $\mathbf{M} \models \phi$, hence $\mathbf{M} \models T_n(\lceil \phi \rceil) \leftrightarrow \phi$, whence by completeness we have $Q_n \vdash T_n(\lceil \phi \rceil) \leftrightarrow \phi$

We have now proved our main result. The set of Gödel numbers of sentences true in arithmetic modulo n is definable in arithmetic modulo n, Q_n , by the predicate $T_n(x)$. Hence for all n, arithmetic modulo n is a theory containing its own truth predicate.

4 Coding, representability and acceptability.

Clearly, the set of Gödel numbers for a set of expressions, and representability in general, is relative to coding: but in Q (Robinson arithmetic) and extensions of Q all codings can be shown to be $\mathbb N$ acceptable, simply because Gödel codings must be injections into $\mathbb N$. For the same reason, for all the non-standard models $\mathbb N \mathbb S$ of Q of which I am aware, in which the domain is got by adding extra elements to $\mathbb N$, all codings are $\mathbb N \mathbb S$ acceptable. So in general, relativity to coding is irrelevant and not discussed for that reason.

However, when using L for a theory of a finite model then the syntax may no longer be properly represented in the theory. Although any coding will still be injective into \mathbb{N} , and although there will still be an injection from \mathbb{N} to the numerals of L, any theory which induces a partition on the numerals is in danger of proving that for distinct $\phi, \psi, \lceil \phi \rceil = \lceil \psi \rceil$. Of course, it is only in danger of doing this if at least one equivalence class has more than one member. In Q_n the relation inducing the partition can be defined by $x \sim y$ iff $Q_n \vdash x = y$, and since there are infinite numerals and only n equivalence classes of numerals, Q_n is in that danger. Indeed, there is a coding for Q_n which ensures that for all $\phi, \psi, Q_n \vdash \lceil \phi \rceil = \lceil \psi \rceil$.

Proposition 4.1 For any n > 1 there exists a Gödel coding of a language L which makes the code of every formula and its negation congruent to zero modulo n.

Proof. Take any Gödel coding #. # maps L into N (is an injection). Let g be a function $g: \mathbb{N} \to \mathbb{N}, g: x \mapsto nx$. Then let $f: L \mapsto \mathbb{N}, f: x \mapsto g(\#x)$.

Both g and # are injections and hence f is an injection from L into \mathbb{N} and as such is a Gödel coding. Under f all formulas of L are congruent to 0 modulo n, a fortior i, so is each formula and its negation.

Hence the need for an acceptable coding if anything of significance is to be got out of a coding. But even with an acceptable coding, coding of the syntax of L into any model of Q_n will be many-one and consequently the capacity for representation of relations of the models must be fairly crude. The proof above shows that being the code of a true sentence is definable. Adapting the Q_n acceptable coding given above in a fairly obvious manner would create what Ketland calls a Frege coding.

Definition 4.2 A **Frege Coding** Fc. Given a model M, pick any two elements of the domain, say a and b. Then define the coding as follows, for any ϕ

$$Fc(\phi) = \begin{cases} a \text{ if } M \models \phi \\ b \text{ if } M \models \neg \phi \end{cases}$$

Intuitively, a and b are just the two truth values, 'The True' and 'The False'.

Definition 4.3 A Frege Coding for Q_n . In our case we can define Fc, using the acceptable coding of lemma 3.6.

$$Fc(\phi) = \begin{cases} [1] & \text{if } \#\phi \equiv 0 \pmod{n} \\ [0] & \text{if } \#\phi \not\equiv 0 \pmod{n} \end{cases}$$

It might be that the capacity for representation in Q_n is so crude that very little else is representable or definable. I don't know. I haven't investigated representability or definability in general for Q_n . The following results may be relevant to the problems of definability and representability in Q_n :

Corollary 4.4 Given an acceptable coding, the diagonal function is not representable in Q_n relative to that coding.

Proof. If the diagonal function were representable, we could derive a contradiction in the standard way. But Q_n is consistent (it has a model).

Corollary 4.5 Introduce a new predicate $T^*(x)$ and let DT^* be the set of all axioms $T^*(\lceil \phi \rceil \leftrightarrow \phi)$, with $\phi \in Sent(L)$. Then $Q_n \cup DT^*$ is a conservative extension of Qn.

Proof. Take any model M. Define an expansion (M, E) by interpreting the new predicate $T^*(x)$ as the set E, where E is got from the set K_n defined above as follows

$$\underline{m}^M \in E$$
 iff for some $k \in K_n, m \equiv k \pmod{n}$.

Then
$$(M, E) \models Q_n \cup DT^*$$
. (Plainly E is definable in Q_n).

5 Final remarks

First we note some further questions worth asking. 1) Are there codings by which we can show M to be an acceptable structure? 2) Could it be that acceptability is not a problem in free logic?

A reservation that might be raised is whether $T_n(x)$ is properly called a truth predicate? Certainly we have seen that it satisfies Tarksi's material adequacy condition. Nevertheless, you might reject it because you deny the coding we used being a Gödel coding. However, since such coding can never be one-one into a finite model, it is the best coding we can get, and it is sufficient for truth. So this reservation appears pedantic and we set it aside.

In theorem 3.10 we proved our main result. Since for all n, the set of Gödel numbers of sentences true in arithmetic modulo n is definable by the

predicate $T_n(x)$, arithmetic modulo n is a simple theory containing its own truth predicate. ²

References

- [1] Boolos, G. and Jeffrey, R. C. Computability and Logic. 3rd ed. Cambridge University Press, 1989.
- [2] Quine, W. V. From a Logical Point of View: 9 Logico-Philosophical Essays. 2nd ed. Harvard University Press, 1980.

Nicholas Shackel Philosophy Cardiff University Great Britain

Oxford Uehiro Centre for Practical Ethics University of Oxford Great Britain

E-mail: shackeln@cardiff.ac.uk

²This paper has benefited from extensive discussion with Jeffrey Ketland.