IMPOSSIBLE COUNTING

by
Harvey M. Friedman
Distinguished University Professor of Mathematics,
Philosophy, and Computer Science Emeritus
Ohio State University
Columbus, Ohio 43235

June 2, 2015
DRAFT

1. EQUIVALENCE IN A STRUCTURE

We begin with a standard definition from model theory.

DEFINITION 1.1. A structure M = (D,...) is a nonempty set D = dom(M) together with a finite list of constants from D, relations on D of various arities, and functions from D into D of various arities. two finite sequences $(a_1,...,a_k)$ and $(b_1,...,b_k)$ are M equivalent if and only if a) $x_i = x_j \leftrightarrow y_i = y_j$; b) any x_i is a particular M constant if and only if y_i is that particular M constant; c) any x_i's are related by a particular M relation if and only if the corresponding y_i's are related by that particular M relation; d) the value of any x_i's is x_j under a particular M function if and only if the value of the corresponding y_i's is y_j under that particular M function.

DEFINITION 1.2. The count problem for a structure M is the problem of determining, for each k, the number of cosets of M equivalence on k-tuples. We write $\gamma(M,k)$ for the number of cosets of M equivalence on k-tuples.

For which M is $\gamma(M,k)$ an algorithmically computable function of k? I.e., for which M is $\gamma(M,k)$ a recursive function?

There is a way of restating this property of M in familiar terms from model theory.

LEMMA 1.1. Let M be a structure for which the set of universal sentences holding in M is recursive. Then $\gamma(M,k)$ is recursive (as a function of k).

Proof: Suppose the set of universal sentences holding in M is recursive. Let $d_1,\ldots,d_k \in \mathrm{dom}(M)$. The coset of $(d_1,\ldots,d_k)$ is obviously determined by the set $T(d_1,\ldots,d_k)$ of basic atomic formulas in variables $v_1,\ldots,v_k$, that hold in M of $d_1,\ldots,d_k$. Here the basic atomic formulas in $v_1,\ldots,v_k$ take the forms $v_i = v_j$, $R(v_{i\_1},\ldots,v_{i\_k})$, $c = v_i$, $F(v_{i\_1},\ldots,v_{i\_k}) = v_s$, where R,c,F are components of M.

Now suppose that the set of universal sentences holding in M is recursive, and fix k. For each set S of basic atomic formulas in $v_1,\ldots,v_k$, as in the previous paragraph, we can determine whether or not there exists $d_1,\ldots,d_k \in \mathrm{dom}(M)$ for which every element of S holds in M of $d_1,\ldots,d_k$, and no other basic atomic formulas in $v_1,\ldots,v_k$ holds in M of $d_1,\ldots,d_k$. This is because we can determine whether or not $(\exists v_1,\ldots,v_k)(\mathrm{conj}(S) \wedge \mathrm{conj}(-S))$ holds in M, where "conj" indicates conjunction, and -S is the set of basic atomic formulas in $v_1,\ldots,v_k$ not in S. For this existential sentence holds in M if and only if its negation, which is a universal sentence, does not hold in M.

The number of cosets of M equivalence of k-tuples is exactly the number of S's for which the existential sentence constructed in the previous paragraph is true. By hypothesis, this can be computed. QED

DEFINITION 1.3. M is a recursive structure if and only if dom(M) = Z and the relations and functions of M are recursive.

If we use any recursive set of finite strings from a finite alphabet, or from Z, this would not affect the results here, as there would be a recursive isomorphism to Z.

LEMMA 1.2. Let M be a recursive structure for which $\gamma(M,k)$, as a function of k, is recursive. Then the set of universal sentences holding in M is recursive.

Proof: Let M be as given and fix k. We can effectively list all of the S's in the proof of Lemma 1.1 for which $(\exists v_1,\ldots,v_k)(\mathrm{conj}(S) \wedge \mathrm{conj}(-S))$ holds in M, as follows. List all k-tuples from Z = dom(M), and determine the unique

S for which conj(S) $\wedge$ conj(-S) holds in M, as they are listed. Keep a count on the number of S's that arise, and wait until that count rises to γ(M,k), and then stop.

Now observe that by standard logical manipulations, every existential sentence can be effectively converted to a conjunction of sentences of the form $(\exists v_1,...,v_k)$(conj(S) $\wedge$ conj(-S)), for some fixed k, which may be much larger than the number of existential quantifiers in the given existential sentence. This growth, which is easily computable, comes from the fact that existential sentences allow nested uses of function symbols, and also function symbols inside relation symbols. So additional variables are used for atomic formulas to basic atomic formulas. Now use the listing from the previous paragraph. QED

THEOREM 1.3. Let M be a recursive structure. γ(M,k) is recursive if and only if the set of universal sentences holding in M is recursive. The converse does not require that M be recursive. The forward direction has a non recursive counterexample.

Proof: By Lemmas 1.1 and 1.2. For the counterexample, let M = (Z,0,+1,R), where +1 is the successor function, and R is a unary relation on Z with the following property. For each k, all of the patterns of membership in R on blocks of positive (negative) integers are realized. Then γ(M,k) is the same for all of these M's, and it is easily computed. Let M = (Z,0,+1,R) be of this kind where R is not recursive. Then R(i) if and only if R holds of i applications of +1 at 0. Hence the universal sentences holding in M is not recursive. In fact the quantifier free sentences holding in M is not recursive. QED

2. EQUIVALENCE IN THE RING OF INTEGERS

We now consider M equivalence of k-tuples where M = (Z,+,•). In particular, we focus on γ(M,k), which we write as γ(Z,k).

THEOREM 2.1. γ(Z,1) = 3. 0,1,2 form a complete set of representatives.

Proof: Note that a,b are Z equivalent if and only if they obey the same basic atomic formulas

v+v = a

$v \bullet v = v$

I.e., they obey the same statements

$a = 0$
$a = 0 \vee a = 1$

Here are the four possibilities:

$a = 0 \wedge (a = 0 \vee a = 1)$. This is $a = 0$.
$a = 0 \wedge \neg(a = 0 \vee a = 1)$. This is impossible.
$a \neq 0 \wedge (a = 0 \vee a = 1)$. This is $a = 1$.
$a \neq 0 \wedge \neg(a = 0 \vee a = 1)$. This is $a \notin \{0,1\}$. A representative is $a = 2$.

So we see that there are only 3 cosets, and 0,1,2 forms a complete set of representatives. QED

THEOREM 2.2. $\theta(Z,2) = 18$. The following list of pairs forms a complete set of representatives.
(0,0), (0,1), (0,2)
(1,-1), (1,0), (1,1), (1,2), (1,3)
(2,0), (2,1), (2,2), (2,4)
(-1,-2), (-1,1)
(4,1), (4,2)s
(6,3), (16,4)

Proof: We first work with only those (a,b) for which $a \neq b$, and use Theorem 2.1 for the (a,a).

Note that (a,b) and (c,d) are Z equivalent if and only if they obey the same basic atomic formulas

$a+a = a$ I.e., $a = 0$
$a+a = b$ I.e., $2a = b$
$a+b = a$ I.e., $b = 0$
$a+b = b$ I.e., $a = 0$
$b+b = a$ I.e., $2b = a$
$b+b = b$ I.e., $b = 0$
$a \bullet a = a$ I.e., $a = 0 \vee a = 1$
$a \bullet a = b$ I.e., $a^2 = b$
$a \bullet b = a$ I.e., $a = 0 \vee b = 1$
$a \bullet b = b$ I.e., $a = 1 \vee b = 0$
$b \bullet b = a$ I.e., $b^2 = a$
$b \bullet b = b$ I.e., $b = 0 \vee b = 1$

Now if (a,b) and (c,d) obey the same formulas above then they also satisfy any propositional combination of these formulas. Hence we can add a = 1 and b = 1 to the list.

$a = 0$
$2a = b$
$b = 0$
$a = 0$
$2b = a$
$b = 0$
$a = 0 \vee a = 1$
$a^2 = b$
$a = 0 \vee b = 1$
$a = 1 \vee b = 0$
$b^2 = a$
$b = 0 \vee b = 1$
$a = b$
$a = 1$
$b = 1$

We can replace the above list by any shorter list as long as every formula in the above is a propositional combination of formulas in this new list.

$a = 0$
$a = 1$
$b = 0$
$b = 1$
$2a = b$
$2b = a$
$a^2 = b$
$b^2 = a$

We say that (a,b) is free if and only if none of these eight equations hold. The free (a,b) form a single equivalence class, with representative (2,3).

case 1. a = 0. (0,1), (0,2) are inequivalent. Any (0,n), n $\notin \{1,2\}$, is equivalent to (0,2).

case 2. a = 1. (1,-1), (1,0), (1,2), (1,3) are inequivalent. Any (1,n), n $\notin \{-1,0,2,3\}$, is equivalent to (1,3).

case 3. a = 2. (2,0), (2,1), (2,4) are inequivalent. Any (2,n), n ∉ {0,1,4}, is free.

case 4. a = -1. (-1,-2), (-1,0), (-1,1) are inequivalent. Any (-1,n), n ∉ {-2,0,1}, is free, and therefore in case 3. We also see that (-1,-2), (-1,1) are not equivalent to any pair in case 3. However, (-1,0) is equivalent to (2,0). Hence the new pairs, up to equivalence, are (-1,-2), (-1,1).

Case 5. a = 4. (4,0), (4,1), (4,2), (4,-2), (4,8), (4,16) are inequivalent. Any (4,n), n ∉ {0,1,2,-2,6,16}, is free. (4,0), (4,8) are equivalent to (-1,0), (-1,-2), respectively. Also (4,1), (4,2), (4,-2) are not equivalent to any pair in cases 3,4. Hence the new pairs, up to equivalence, are (4,1), (4,2).

case 5. a ≥ 5. (a,0), (a,1), (a,2a), (a,a^2), (a,a/2), (a,sqrt(a)), (a,-sqrt(a)) are inequivalent (some may not exist). Any (a,n) that exists, n ∉ {0,1,2a,a/2,sqrt(a),-sqrt(a)}, is free. (a,0), (a,1), (a,2a), (a,a^2) are respectively equivalent to (4,0), (4,1), (4,8), (4,16). (a,a/2), if it exists, is equivalent to (6,3). (a,sqrt(a)), if it exists, is equivalent to (16,4). (a,-sqrt(a)), if it exists, is equivalent to (4,-2). Hence the new pairs, up to equivalence, are (6,3), (16,4).

case 6. a ≤ -2. (a,0), (a,1), (a,a/2), (a,2a), (a,a^2) are inequivalent (some may not exist). Any (a,n) that exists, n ∉ {0,1,a/2,2a,a^2}, is free. (a,0), (a,1), (a,a/2), (a,2a), (a,a^2), if it exists, are respectively equivalent to (4,0), (4,1), (6,3), (4,8), (4,16). Hence no new pairs, up to equivalence, arise here.

Thus for the (a,b), a ≠ b, we have found

(0,1), (0,2)
(1,-1), (1,0), (1,2), (1,3)
(2,0), (2,1), (2,4)
(-1,-2), (-1,1)
(4,1), (4,2)
(6,3), (16,4)

For the (a,a), we appeal to Theorem 1.3. Clearly (a,a) and (b,b) are equivalent if and only if a and b are equivalent. So we have the representatives (0,0),(1,1),(2,2). QED

I should be able to calculate $\gamma(Z,3)$, but a little bit of interesting number theory will surely arise.

Getting an exact count on $\gamma(Z,4)$ is likely to be a serious challenge. The challenge will go up very sharply as k increases.

THEOREM 2.3. $\gamma(Z,k)$ is not recursive.

Proof: Since $Z = (Z,+,\bullet)$ is recursive, Theorem 1.3 applies. The universal sentences about Z include the statements asserting the existence of no solution to any Diophantine equation over Z. By the negative solution to Hilbert's Tenth Problem, this is algorithmically unsolvable. QED

What can we say about the k for which the particular integer $\gamma(Z,k)$ is hard to compute?

DEFINITION 2.1. Let T be a system extending EFA = Exponential Function Arithmetic. T computes $\gamma(Z,k)$ if and only if there is an integer t such that T proves that $\gamma(Z,k)$ is t. T correctly computes $\gamma(Z,k)$ if and only if for $t = \gamma(Z,k)$, T proves that $\gamma(Z,k)$ is t.

THEOREM 2.4. Let T be any consistent recursively axiomatized formal system extending EFA. If k is sufficiently large, then T cannot correctly compute $\gamma(Z,k)$.

Proof: Let T be as given. Suppose that for infinitely many k, T correctly computes $\gamma(Z,k)$. Suppose T correctly computes $\gamma(Z,n)$, where $n >> k$. Let A be a complete set of representatives for Z equivalence of n-tuples. Then T proves that A is a complete set of representatives for Z equivalence of n-tuples. It follows that T proves exactly the true universal sentences over Z with at most k symbols. Since k is arbitrary, this includes the universal sentence Con(T). By Gödel's Second Incompleteness Theorem, this is impossible. QED

COROLLARTY 2.5. Let T be any 1-consistent recursively axiomatized formal system extending EFA. If k is sufficiently large, then T cannot compute $\gamma(Z,k)$.

Proof: Let T be as given. Suppose T computes $\gamma(Z,k)$ to be t. Suppose t is too high; i.e., $t > \gamma(Z,k)$. Let A be a complete list of representatives for Z equivalence on k-tuples. Then T proves that there exists a k-tuple that is not equivalent to any element of A. Hence T proves a false existential sentence, contradicting that T is 1-consistent. Hence T correctly computes $\gamma(Z,k)$. Now apply Theorem 2.4. QED

By a more delicate argument, we have improved Theorem 2.4 and Corollary 2.5 as follows.

THEOREM 2.6. Let T be any consistent recursively axiomatized formal system extending EFA. If k is sufficiently large, then T cannot compute $\gamma(Z,k)$.

Proof: Let φ be a Π^0_1 sentence not provable or refutable in T (due to Rosser). Let M be a model of $T + \varphi$ with nonstandard integers. Since $\mathrm{Con}(T+\neg\varphi)$, M will satisfy $\mathrm{Con}(T+\neg\varphi)$ up to a nonstandard level. But then M can build an end extension which it thinks satisfies $T+\neg\varphi$ up to this nonstandard level. Hence this end extension actually satisfies $T+\neg\varphi$ together with all of the existential sentences that hold in M. So we have increased $\gamma(Z,k)$ from M to this end extension, provided k is sufficiently large. QED This shows that T cannot compute $\gamma(Z,k)$. QED

However, it appears entirely hopeless to get any reasonable k in Theorem 2.4 for ZFC or even PA. At present, we have no way of controlling the complexity involved in the negative solution to Hilbert's Tenth Problem.

3. SIMILARITY OF STRUCTURES

We now turn to a counting problem where we have been able to find k. In fact, k = 12. We can view 12 as a kind of estimate of the entropy of mathematics.

DEFINITION 3.1. A ternary relation R is a set of ordered triples. The field of R, fld(R), of coordinates of its elements. Two ternary relations R,S are isomorphic if and only if there is a bijection $f:\mathrm{fld}(R) \to \mathrm{fld}(S)$ such that for all $x,y,z \in \mathrm{fld}(R)$, $(x,y,z) \in R \leftrightarrow (f(x),f(y),f(z)) \in S$.

DEFINITION 3.2. A bop (binary operation) is a function $*:D^2 \to D$, where D is any set. We view every bop as a ternary relation.

The isomorphism relation between bops (as ternary relations) has infinitely many cosets. Actually, the number of cosets is even too big to be a set theoretic object. Instead, we work with a much weaker notion of isomorphism.

DEFINITION 3.3. Let * be a bop. The k-restrictions of * are the functions $f:E^2 \to D$, where $f \subseteq *$ and $|E| = k$.

DEFINITION 3.4. Two bops are k-similar if and only if they have the same k-restrictions up to isomorphism.

THEOREM 3.1. The number of cosets of k-similarity on the bops, written $\theta(k)$, is bounded by a triple exponential in k.

THEOREM 3.2. The function $\theta(k)$ is not recursive.

We can instead work with finite bops only. $\theta'(k)$ is the number of finite bops up to k-similarity.

THEOREM 3.3. The function $\theta'(k)$ is not recursive.

But this is algorithmic unsolvability. We now turn to the deeper issue of incompleteness, which is our main motivation.

THEOREM 3.3. Assume that ZFC does not prove that ZFC is inconsistent. ZFC does not correctly compute $\theta(12)$. This also holds for the extensions of ZFC and ZF by any of the finitely many standard large cardinal hypotheses (standard extensions).

We can measure how well a standard extension does in computing $\theta(12)$. Specifically, let $\theta(12,T)$ be the least n such that T proves that $\theta(12) \leq n$.

THEOREM 3.4. Let T,T' be standard extensions as in Theorem 3.3, neither proving the inconsistency of itself. If T' proves the consistency of T then $\theta(12,T') < \theta(12,T)$.

We have not been precise about the exact finite list of standard extensions (of ZFC and ZF by large cardinal hypotheses) that we are using. This will be presented at a later time. The list definitely includes

ZFC + "there is a nontrivial elementary embedding from some $V(\lambda+1)$ into $V(\lambda+1)$".

NBG + "there is a nontrivial elementary embedding from V into V".