DIGITAL DISPLAY EXPANSION

by
Harvey M. Friedman
Distinguished University Professor of Mathematics, Philosophy, and Computer Science, Emeritus
The Ohio State University
July 7, 2018
DRAFT

the conjectures are crucial and I am working on polishing them
but I want to get these ideas out right away now that the proofs are under good control
these rather standard proofs are not the main point, of course
also I want to handle not only full expandability but also progressive expandability
this corresponds to the difference between two way tapes and one way tapes
I just treat full expandability via two way tapes here
in the next draft I will add the treatment with progressive expandability via one way tapes

Abstract. We construct a digital display with 376 × 376 pixels and 382 colors, which is fully expandable, but where its full expandability is not provable from the usual ZFC axioms for mathematics (all assuming ZFC is consistent). Here full expandability means that the display can be indefinitely enlarged with new pixels without creating any new 2 × 2 contiguous parts (4 element cells). By comparison, the daily production of digital displays from computer screens, smartphones, televisions, movies, digital photographs, satellite images, digital audio and MIDI recordings, and the like, results in perhaps trillions of incomparably larger digital displays per day, worldwide. We achieve this by a reinterpretation of recent work of Aaronson, Yeddida, myself, and O'Rear on the halting problem for Turing machines, that closely relates it to digital displays. This simple but basic conceptual shift opens up immediately transparent profound and challenging new dramatic areas of research at the interface of at least mathematical logic, combinatorics, computer science, and art. Aside from the obvious goal of finding increasingly

small digital displays so representing ZFC Incompleteness, there are other even deeper issues. Specifically, is full expandability expected or not, in random displays, on various adjustments of the parameters (number of pixels and number of colors)? What are the thresholds? Cen these thresholds be determined in ZFC? Are there thresholds where we expect ZFC Incompleteness to arise? And what about the rich digital displays randomly drawn from daily life such as from typical movies and musical recordings (digital audio and MIDI)? How invisibly can we doctor existing digital displays so as to represent ZFC Incompleteness? Our method of generating digital displays of various sizes exhibiting such ZFC Incompleteness is very flexible, raising the prospect of creating beautiful digital displays of various sizes meeting various criteria. In fact, we envision a creative process of adjusting colors and rearranging patterns, transforming a digital display from an unsightly mess to a work of art of equal size. This should also be approached on the musical side with digital and MIDI recordings, in a joint effort of mathematical logicians, combinatorists, computer scientists, audio engineers, and musicians.

1. TURING MACHINES

A TM(↔) is a deterministic Turing machine with a two way infinite tape and two symbols. I.e, it consists of a set Q of states $q_0,...,q_n$, $n \geq 0$, the two tape symbols 0,1, and the transition function T, which is a partial function $T:Q \times \{0,1\} \to Q \times \{0,1\} \times \{L,R\}$. Computation starts with all 0's on the tape, indexed by Z, and in state q_0. Computation continues according to T. I.e., if at any time we are in state q_k and reading tape symbol i, and $T(q_k,i) = (qn,j,X)$, then we transition to state q_n, overwrite j at the square where we are reading, and move to the left or right one square according to whether X is L or R. Computation halts when and only when T is undefined.

We also consider the variant TM(→). This is a deterministic Turing machine with a two way infinite tape and two symbols. I.e, it consists of a set Q of states $q_0,...,q_n$, n

≥ 0, the two tape symbols 0,1, and the transition function T, which is a partial function T:Q x {0,1} → Q x {0,1} x {L,R}. Computation starts with all 0's on the tape, indexed by Z, and in state q_0. Computation continues according to T. I.e., if at any time we are in state qk and reading tape symbol i, and $T(q_k,i) = (q_n,j,X)$, then we transition to state q_n, write j at the location where we are reading, and move to the left or right one square according to whether X is L or R. Computation halts when and only when T is undefined or we are reading square 0 and T tells us to move left (L).

When we write TM we mean a TM(→) or a TM(↔).

If TM eventually halts then we say that TM converges. If TM never halts then we say that TM diverges.

The following classical result is due to Turing.

THEOREM 1.1. There is no algorithm for determining whether a given TM converges.

COROLLARY 1.2. Let T be any consistent recursively axiomatized formal system T extending a small amount of arithmetic. There exists a TM such that
i. TM diverges.
ii. T does not prove "TM diverges".

Proof: SEE NEXT DRAFT

Here is a stronger well known result.

THEOREM 1.3. Let T be any consistent recursively axiomatized formal system extending a small amount of arithmetic. There exists a TM such that T does not prove or refute "TM converges". It follows that TM diverges.

Proof: A,B recursively inseparable r.e. sets, where T proves A,B are disjoint. Suppose T decides TM halts for any given TM. Make the TM which halts iff n ∈ A, provably so? {n: T proves n ∈ A} is recursive and contains A. It's disjoint from B. Contradiction. QED

The question natural arises as to how many states does a TM(→) or TM(↔) need to have in order that it diverge, yet ZFC does not prove that it diverges? Or has many states does a TM(↔) or TM(↔) need to have in order that ZFC does not prove or refute that it diverges? And what can we say about the relationship between these two questions? These questions are exactly the same, as long as we trust ZFC.

THEOREM 1.4. Let T be any 1-consistent recursively axiomatized formal system extending a small amount of arithmetic, and TM be given. The following are equivalent.
i. TM diverges, and TM does not prove "TM diverges".
ii. TM does not prove or refute "TM diverges".

Proof: SEE NEXT DRAFT QED

An approach to this question on the number of states was initiated in [AY16], where they used a Π^0_1 sentence φ of mine that I showed was unprovable in ZFC (even SRP), assuming as is almost universally believed, that ZFC (SRP) is consistent. They programmed a 7910 state TM(↔) to simulate it in the following sense. They proved, in a weak fragment of arithmetic, that φ is equivalent to "TM(↔) diverges". Thus "TM(↔) diverges" is unprovable in ZFC (even SRP). That TM(↔) actually diverges follows from the truth of φ, which I established under a fairly strong assumption that is widely believed. SRP is a certain extension of ZFC via large cardinal hypothesis.

Soon later, the matter was taken up by O'Rear who used a much more direct method. He directly attacked (an equivalent version of) ZFC, bypassing my work, and getting the number of states down to 1919. He directly programs a search for an inconsistency in ZF, thereby obtaining a TM(↔) such that, provably in a weak fragment of arithmetic, "TM(↔) diverges if and only if Con(ZFC)".

It follows that, under this O'Rear approach, Con(ZFC) is used to prove that ZFC does not prove "TM diverges", and only 1-Con(ZFC) is used to prove that the TM actually diverges. In fact, 1-Con(ZFC) is used to prove that "TM converges" is neither provable nor refutable in ZFC.

2. FUNCTION EXPANSION

Here we give a method for converting an n state TM(↔) to a function with domain $[1,m]^2 \times$ with at most r values, so that TM(↔) diverges if and only if f is fully expandable (in the sense defined below). We relate this to Digital Display Expansion in section 3. There is a weaker notion called progressively expandable which is also very natural, and an analogous result is proved for progressively expandable (in the sense defined below) by instead using TM(→).

NOTE: WE WILL ADD THIS IN THE NEXT DRAFT.

Henceforth we will write TM instead of TM(↔).

DEFINITION 2.1. Z is the set of integers and N is the set of nonnegative integers. All intervals used here are discrete intervals in Z, where intervals are allowed to be one or two sided infinite, and required to be nonempty. Let dom(f) = I × J, dom(g) = I' × J', where I,J,I',J' are intervals in Z. A cell in f is a quadruple, written x,y;z,w, such that there exists i,j for which x = f(i,j), y = f(i+1,j), z = f(i,j+1), w = f(i+1,j+1). g is an expansion of f if and only if f ⊆ g and f,g have the same cells.

Note that x,y;z,w is to be visualized as a 2 × 2 matrix with entries x,y,z,w, where x,y comprise the bottom row, and z,w comprise the top row. The reason for this convention (for which we take full responsibility) stems from the classical Wang tiling theory, where the evolution of Turing machines is represented by tilings of the upper half integer plane, and each clock tick corresponds to moving up a unit. So we think of x,y;z,w as moving from adjacent x,y up to adjacent z,w.

DEFINITION 2.2. Let dom(f) = I × J. f is fully expandable if and only if f has an expansion with domain Z^2. f is progressively expandable if and only if f has an expansion with domain I' × J', where inf(I') = inf(I), inf(J') = inf(J), and sup(I') = sup(J') = ∞.

These notions are actually more concrete than they look.

THEOREM 2.1. Let dom(f) = [n,m] × [r,s] be finite. f is fully expandable if and only if for all t ≥ n,m,r,s, f has an expansion with domain [-t,t]2. f is progressively expandable if and only if for all m' ≥ m and s' ≥ s, f has an expansion with domain [n,m'] × [r,s']. Thus for finite such f, "f is fully expandable" and "f is progressively expandable" are (provably equivalent in WKL_0 to) Π^0_1 sentences.

Proof: This has a well known proof using the finitely branching tree lemma. A routine topologization of this situation replaces the use of the finitely branching tree lemma by the compactness of an infinite product of finite discrete topologies. QED

We fix TM(↔) with states $q_0,...,q_{n-1}$, tape symbols 0,1, and partial transition function $T:Q \times \{0,1\} \to Q \times \{0,1\} \times \{L,R\}$, where $Q = \{q_0,...,q_{n-1}\}$.

We assume that the reader is familiar with how computation runs in TM(↔). We initialize at time t = 0 where the state is q0 and the tape symbols are all 0's.

However, there is a small change that we make in the usual setup. At this point, an n state machine has states $q_0,...,q_{n-1}$, and proceeds with the idea that it may stop computation - i.e., halt. This is considered to happen when there is a call to the transition function T that is not returned (undefinedness).

What it very convenient for our fully (unusually) rigorous treatment is to view an n state machine as having states $Q = \{q_0,...,q_n\}$, where there is no halting in the sense of stopping. I.e., all computation goes on forever. But the notion of halting is then taken to mean that the state q_n is reached at some time t. It is more convenient to work with the opposite notion, that of divergence. TM(↔) diverges if and only if it never reaches the state q_n.

DEFINITION 2.3. We define functions $SYS:Z \times N \to \{0,1\}$ and $H:Z \times N \to Q \cup \{0,1\}$ are defined as follows. SYS(k,t) is the tape symbol at location k and time t. H(k,t) is the state at time t if the reading head is at location k at time t; SYS(k,t) if the reading head is > k at time t; SYS(k-1,t) if the reading head is < k at time t. For the n state machine TM(↔) with states $Q = \{q_0,...,q_n\}$, we say that TM(↔) diverges if and only if there is no time t when the state of TM(↔) is q_n.

Note here that SYS is the "system function", and H is an auxiliary function connected with standard ways of encoding "instantaneous tape descriptions".

We want to analyze which cells in H arise, which take the form H(k,t'),H(k+1,t');H(k,t'+1),H(k+1,t'+1). We describe a set K based on the transition function T of TM, large enough so that K at least includes all of the cells in H.

LEMMA 2.2. Assume that for TM, the state at time t is qr ∈ Q, the location of the reading head at time t is p ∈ Z, the tape symbol at location p is i ∈ {0,1}, and $T(q_r,i) = (q_s,j,X)$, where X ∈ {L,R}. For all k ∈ Z,
i. H(k,t) = SYS(k,t) if k < p; qr if k = p; SYS(k-1,t) if k > p.
ii. If p ≤ k-2 then H(k,t) = H(k,t+1) ∈ {0,1}, H(k+1,t) = H(k+1,t+1) ∈ {0,1}, all four in {0,1}.
iii. If p ≥ k+3 then H(k,t) = H(k,t+1) ∈ {0,1}, H(k+1,t) = H(k+1,t+1) ∈ {0,1}, all four in {0,1}.
iv. If p = k-1 and X = L then H(k,t) = i, H(k+1,t) = H(k+1,t+1), H(k,t+1) = j, all four in {0,1}.
v. If p = k-1 and X = R then H(k,t) ∈ {0,1}, H(k+1,t) = H(k+1,t+1) ∈ {0,1}, H(k,t+1) = q_s,
vi. If p = k and X = L then H(k,t) = q_r, H(k+1,t) = i, H(k,t+1) ∈ {0,1}, H(k+1,t+1) = j.
vii. If p = k and X = R then H(k,t) = q_r, H(k+1,t) = i, H(k,t+1) = j, H(k+1,t+1) = q_s.
viii. If p = k+1 and X = L then H(k,t) = H(k+1,t+1) ∈ {0,1}, H(k+1,t) = q_r, H(k,t+1) = q_s.
ix. If p = k+1 and X = R then H(k,t) = H(k,t+1) ∈ {0,1}, H(k+1,t) = q_r, H(k+1,t+1) = j.
x. If p = k+2 and X = L then H(k,t) = H(k,t+1) ∈ {0,1}, H(k+1,t) ∈ {0,1}, H(k+1,t+1) = qs.
xi. If p = k+2 and X = R then H(k,t) = H(k,t+1) ∈ {0,1}, H(k+1,t) = H(k+1,t+1) ∈ {0,1}, all four in {0,1}.

Proof: I WILL FILL IN ALL OF THESE COMPUTATIONS IN THE NEXT DRAFT. THESE COMPUTATIONS ARE COMPLETELY STRAITFORWARD BUT MUST TO BE DONE WITH PAINSTAKING ACCURACY. QED

Let K[α] be the following set of cells, based entirely on a single transition statement α, of the form $T(q_r,i) = (q_s,j,X)$, X ∈ {L,R}.

GENERIC

a,b;a,b, a,b ∈ {0,1}. Count 4.

LEFT
assume $T(q_r,i) = (q_s,j,L)$

i,a;j,a, a ∈ {0,1}. Count 2.
qr,i;a,j, a ∈ {0,1}. Count 2.
a,qr;qs,a, a ∈ {0,1}. Count 2.
a,a;b,qs, a,b ∈ {0,1}. Count 4.

RIGHT
assume $T(q_r,i) = (q_s,j,R)$

a,b;q_s,b, a,b ∈ {0,1}. Count 4.
q_r,i;j,q_s. Count 1.
a,q_r;a,j, a ∈ {0,1}. Count 2.

Let K[TM] be the union of the K[α] such that α is an element of the transition function T of TM.

LEMMA 2.3. Each K[α] has either 8 or 7 elements in addition to the four Generic elements and the special elements i,a;j,a, which total at most 8 elements across all α. K[TM] has at most 8n+12 elements. Every cell in H lies in K[TM].

Proof: For the count, note that the four generic elements are in common to all K[α], so the count is justified. Let C be a cell in H, say H(k,t),H(k+1,t);H(k,t+1),H(k+1,t+1). Let p,q_r,i be the parameters for Lemma 2.2 that are correct for TM. Let $T(q_r,i) = (q_s,j,X)$, X ∈ {L,R}. Apply Lemma 2.2. Compile the results into the above table for K[α], where α is the transition clause $T(q_r,i) = (q_s,j,X)$ from the T of TM. Then this cell lies in K[α]. Obviously K[TM] covers all transition clauses from T. QED

We now fix a function H':Z × N → Q ∪ {0,1} and t ∈ N, where H' = H on Z × {t}. We also assume that all cells in H' lie in K[TM]. Then we show that H' = H on Z × {t+1}. This will serve as the induction step we need. Let q_r be the state of TM at time t, i be the tape symbol being read at time t, p be the location of the reading head at time t, and $T(q_r,i) = (q_s,j,X)$, X ∈ {L,R}.

LEMMA 2.4. Assume X = L. Then the reading head at time t is at p, and at time t+1 is at p-1.
i. H(p,t+1) = H(p-1,t).

ii. H'(p,t+1) = H(p,t+1). H'(p+1,t+1) = j. H'(p-1,t+1) = q_s.
iii. For all k ≥ p, H'(k,t+1) = H(k,t).
iv. For all k ≥ p, H'(k,t+1) = H(k,t+1).
v. H'(p-1,t+1) = H(p-1,t+1) = q_s.
vi. For all k ≤ p-2, H'(k,t+1) ∈ {0,1}.
vii. For all k ≤ p-2, H'(k,t+1) = H(k,t).
viii. For all k ≤ p-1, H'(k,t+1) = H(k,t+1).
ix. H = H' on Z × {t+1}.

Proof: For i, H(p,t+1) = SYS(p-1,t+1) = SYS(p-1,t). H(p-1,t) = SYS(p-1,t).

For ii, first look at the cell H(p,t),H(p+1,t);H'(p,t+1),H'(p+1,t+1) = qr,i;H'(p,t+1),H'(p+1,t+1). By the Left list, line 2, H'(p+1,t+1) = j. Now look at the cell H(p-1,t),H(p,t);H'(p-1,t+1),H'(p,t+1) = H(p-1,t),qr;H'(p-1,t+1),H'(p,t+1). By the Left list, line 3, we see that H(p-1,t) = H'(p,t+1) = H(p,t+1), using i. Also by Left list, line 3, H'(p-1,t+1) = qs.

For iii, we prove by induction on k ≥ p that H'(k,t+1) = H(k,t) ∈ {0,1}. The basis case, k = p, is by ii. Now suppose H'(k,t+1) = H(k,t) ∈ {0,1}, k ≥ p, and derive H'(k+1,t+1) = H(k+1,t) ∈ {0,1}. Look at the cell H(k,t),H(k+1,t);H'(k,t+1),H'(k+1,t+1) = H(k,t),H(k+1,t);H(k,t),H'(k+1,t+1), where the first three terms are bits. This is because H(k+1,t) = SYS(k,t) ∈ {0,1}.

By the Generic and Left lists, the only possibilities for this cell are a,b;a,b, the first line of the Left list, and the fourth line of the Left list. The first two possibilities yield H(k+1,t) = H'(k+1,t+1) ∈ {0,1}, and so we use the fourth line of the Left list. Then H'(k+1,t+1) = q_s. Now look at the cell H(k+1,t),H(k+2,t);H'(k+1,t+1),H'(k+2,t+1), where the first two terms are bits and the third term is q_s. According to the Generic and Left lists, this is impossible.

For iv, let k ≥ p. The case k = p is from ii. Assume k ≥ p+1. Then H'(k,t+1) = H(k,t) = SYS(k-1,t). But H(k,t+1) = SYS(k-1,t+1) = SYS(k-1,t). Hence H'(k,t+1) = H(k,t+1).

For v, we have $H'(p-1,t+1) = q_s$ by ii. Now $H(p-1,t+1) = q_s$ since the reading head is at p-1 at time t+1.

For vi, we prove $H'(k,t+1) \in \{0,1\}$ by induction on $k \leq p-2$ going backwards. The basis case is p-2. Look at the cell $H(p-2,t),H(p-1,t);H'(p-2,t+1),H'(p-1,t+1) = SYS(p-2,t),SYS(p-1,t);H'(p-2,t+1),q_s$, where the q_s is from v. This cell begins with two bits and ends with q_s. By the Left list, $H'(p-2,t+1) \in \{0,1\}$, completing the basis case. Now assume $H'(k,t+1) \in \{0,1\}$, $k \leq p-2$. Look at the chain $H(k-1,t),H(k,t);H'(k-1,t+1),H'(k,t+1) = SYS(k-1,t),SYS(k,t);H'(k-1,t+1),SYS(k,t+1) = SYS(k,t)$. Since the first, second, and fourth terms are bits, by the Left list we see that $H'(k-1,t+1) \in \{0,1\}$.

For vii, let $k \leq p-2$. Look at the chain $H(k-1,t),H(k,t);H'(k-1,t+1),H'(k,t+1)$. $H(k-1,t) = SYS(k,t)$, $H(k,t) = SYS(k,t)$. By vi, all terms in this cell are bits. By the Generic and Left list, the second and fourth terms must be equal.

For viii, let $k \leq p-1$. The case $k = p-1$ is $H'(p-1,t+1) = H(p-1,t+1)$, given by v. Now let $k \leq p-2$. By vii, $H'(k,t+1) = H(k,t) = SYS(k,t) = SYS(k,t+1) = H(k,t+1)$.

Finally, ix follows immediately from iv,viii. QED

LEMMA 2.5. Assume X = R. Then the reading head at time t is at p, and at time t+1 is at p+1.
i. For all $k \geq p+2$, $H(k,t),H(k,t+1) \in \{0,1\}$. For all $k \leq p-1$, $H(k,t),H(k,t+1) \in \{0,1\}$.
ii. For all $k \geq p+3$, $H'(k,t+1) = H(k,t)$.
iii. For all $k \geq p+3$, $H'(k,t+1) = H(k,t+1) = H(k,t)$.
iv. For all $k \leq p-1$, $H'(k,t+1) = H(k,t)$.
v. For all $k \leq p-1$, $H'(k,t+1) = H'(k,t+1) = H(k,t)$.
vi. $H(p,t) = q_r$. Every $H(p',t)$, $p' \neq p$, is a bit. $H(p,t+1) = SYS(p,t+1) = j$. $H(p+1,t+1) = qs$. $H(p+2,t+1) = SYS(p+1,t+1) = SYS(p+1,t)$.
vii. $H'(p,t+1) = j \wedge H'(p+1,t+1) = q_s \wedge H'(p+2,t+1) = H(p+2,t+1)$.
viii. $H = H'$ on $Z \times \{t+1\}$.

For i, let $k \geq p+2$. $H(k,t) = SYS(k-1,t) \in \{0,1\}$. $H(k,t+1) = SYS(k-1,t+1) \in \{0,1\}$. Let $k \leq p-1$. $H(k,t) = SYS(k,t) \in \{0,1\}$. $H(k,t+1) = SYS(k,t+1) \in \{0,1\}$.

For ii, first let $k \geq p+3$, and look at the cell $H(k,t),H(k+1,t);H'(k,t+1),H'(k+1,t+1)$. By i, the first two terms are bits. Hence this cell is either on the Generic list or the Right list, line 1. If it is on the Generic list then $H(k,t) = H'(k,t+1)$. So we assume it is on the Right list, line 1, and so $H'(k,t+1) = q_s$. Now look at the cell $H(k-1,t),H(k,t);H'(k-1,t+1),H(k,t+1)$. By i, the first two terms are bits, and the fourth term is cs. Hence this cell does not appear on the Generic and Right lists, and we have arrived at a contradiction.

For iii, let $k \geq p+3$. Then $H(k,t+1) = SYS(k-1,t+1) = SYS(k-1,t) = H(k,t) = H'(k,t+1)$, using ii.

For iv, Let $k \leq p-1$, and look at the cell $H(k-1,t),H(k,t);H'(k-1,t+1),H'(k,t+1)$. By i, the first two terms are bits. Hence this cell is either on the Generic list or the Right list, line 1. If it is on the Generic list then $H(k,t) = H'(k,t+1)$. Hence assume is on the Right list, line 1, with $H'(k-1,t+1) = q_s$. Now look at the cell $H(k-2,t),H(k-1,t);H'(k-2,t+1),H'(k-1,t+1)$. By i, the first two terms are bits, and the fourth term is c_s. Hence this cell does not appear on the Generic and Right lists, and we have arrived at a contradiction.

For v, let $k \leq p-1$. Then $H(k,t+1) = SYS(k,t+1) = SYS(k,t) = H(k,t) = H'(k,t+1)$, using iv.

For vi, $H(p,t) = q_r$ since the reading head is on p at time t. $H(p',t)$ is $SYS(p',t)$ or $SYS(p'-1,t)$. for the next two equations equation, use that the reading head is on p+1 at time t+1. For the final equation, the reading is not on p+2 at time t+1. For $SYS(p+1,t+1) = SYS(p+1,t)$ use that at time t, the reading head was not on p+1.

For vii, look at the cell $H(p,t),H(p+1,t);H'(p,t+1),H'(p+1,t+1) = qr,H(p+1,t);H'(p,t+1),H'(p+1,t+1)$, and this cell must be on the Right list, line 2. Hence $H(p+1,t) = i \wedge H'(p,t+1) = j \wedge H'(p+1,t+1) = qs$. Now look at the cell $H(p+1,t),H(p+2,t);H'(p+1,t+1),H'(p+2,t+1) = i,H(p+2,t);qs,H'(p+2,t+1)$. This cell must be on the Right list, line 1, and so H(p+2,t) = H'(p+2,t+1) = SYS(p+1,t) = SYS(p+1,t+1) = H(p+2,t+1).

For viii, by by iii,iv, H = H' on [3,∞) ∪ [-∞,p-1] × {t+1}. By vi,vii, H(p,t+1) = H'(p,t+1) = j ∧ H(p+1,t+1) = H'(p+1,t+1) = q_s ∧ H(p+2,t+1) = H'(p+2,t+1). QED

DEFINITION. We say that a function H':Z × N → Q ∪ {0,1} initializes for TM(↔) if and only if H'(k,0) = q_0 if k = 0; 0 otherwise. For a general n state TM(↔), Q = {q_0,...,q_n} and TM(↔) diverges if and only if it never reaches state q_n in the course of computation.

LEMMA 2.6. An n state TM(↔) diverges if and only if q_n ∉ rng(H). H initializes for TM(↔). Here H is the associated auxiliary function.

Proof: The first claim follows from the fact that every state is the value of H at the location of the reading head at a time that the TM is in that state, and also that all state values of H are actual states at the time present in the arguments given rise to such values. For the second claim, note that H(0,0) is the state at time 0, which is q_0, because the reading head is on 0 at time t = 0. QED

THEOREM 2.7. An n state TM(↔) diverges if and only if there exists H':Z × N → Q ∪ {0,1} which initializes for TM, has all of its cells lying in K[TM], and omits the value qn. If TM(↔) diverges then its auxiliary function H is the unique H':Z × N → Q ∪ {0,1} which initializes for TM, has all cells lying in K[TM]. If n state TM(↔) diverges then its auxiliary function omits the value qn.

Proof: Let TM(↔) have n states q_0,...,q_n, and diverge. By Lemma 2.7 and Lemma 2.2 along with its resulting compilation, the auxiliary function H:Z × N → Q ∪ {0,1} has the required properties, including omitting the value q_n, with the help of Lemma 2.6. Conversely, let H':Z × N → Q ∪ {0,1} have those properties. We show by induction on t that H' = H on Z × {t}. This is clear for t = 0 since H,H' initialize for TM(↔). Suppose H' = H on Z × {t}, t ∈ N. Suppose H' = H on Z × {t}, t ∈ N. For TM(↔), let q_r be the state at time t, i the tape symbol being read at time t, p the location of the reading head at time t, and T(q_r,i) =

(q_s,j,X), $X \in \{L,R\}$. Now invoke Lemma 2.4 or 2.5, according to whether X = L or X = R, to establish that H' = H on {t+1}. We now conclude that H' = H, and so H omits the value qn. Therefore TM(↔) diverges.

For the second claim, let TM(↔) diverge. For the required uniqueness, we note that the induction proof in the previous paragraph relies only on the initialization and cell conditions. The final claim has already been used, but is worth highlighting and comes from Lemma 2.6. QED

Now fix TM(↔) with its states $Q = \{q_0,...,q_n\}$. Recall that q_n is the special state whereby if it ever gets used, we no longer have divergence. So we want to use $Q' = \{q_0,...,q_{n-1}\}$ in this construction.

We now construct the associated $g:[-2,m-3] \times [-m+1,0] \rightarrow Q' \cup [0,5]$ so that TM diverges if and only if g is fully expandable. We will specify m later, but in order to avoid any nuisance trivialities, we will assume in the construction that $m \geq 5$. We later normalize g, putting it into the form $f:[1,m]^2 \rightarrow [1,n+5]$. Clearly dom(f) is an m x m square.

1. On the top row of dom(g), g takes on the m values 0,0,q0,0..,0 from left to right. On the first two columns of dom(f), g takes on the same m values 0,2,...,2 top/down. On the last two columns of dom(g), g takes on the same m values 0,3,...,3,2 top/down. We are now left with a blank $m-1 \times m-4$ rectangle R with m-1 rows and m-4 columns.

2. Now we partition R into 3×3 regions each with 9 points (no gaps), starting at the lower left corner. Each row of 3×3 regions, one region after the another, will consist of at least (m-6)/3 disjoint touching 3×3 regions, and each column of these 3×3 parts will consist of at least (m-3)/3 touching disjoint 3×3 regions. This will result in a total of at least (m-6)(m-3)/9 3×3 regions.

3. Next we place the elements of K into these 3×3 regions. For this purpose, we use only the bottom left 2×2 cells in these 3×3 regions so that there is no touching between these entered elements of K. The only restraint on this placement is that every element of K gets placed. Duplicate

placements are even allowed, and also we can leave some 3 × 3 regions empty.

4. In each of the 3 × 3 regions that have been used in 3, put 4 at the top left and 5 at the remaining four points.

5. Finally, put 5 at all points that still remain.

This completes the construction of g:[-2,m-3] × [-m+1,0] → Q' ∪ [0,5].

LEMMA 2.8. If g is fully expandable then TM diverges.

Proof: Assume h:Z × Z → Q' ∪ [0,5] is an expansion of g. We claim that the cells in g are of the following kinds.

i. The critical cells 2,2;0,0, 2,2;2,2, 3,3;0,0, 3,3;3,3, 2,2;3,3.
ii. The cells in K.
iii. Various cells, none of which have second column 0,2, top down, and none of which have a 3 in the first column.

To see that this list is exhaustive, if the left edge of a cell in dom(g) is on the left boundary of dom(g), or the right edge is on the right boundary, then the cell is a critical cell. All other cells have their right corner in Q' ∪ {0,1,4}, with the exception of the single cell whose right column is 3,2, top down. Also all other cells have their left corner in Q' ∪ {0,1,3}.

We claim that h initializes for TM(↔). We have already arranged that h initializes for TM(↔) across the top row of dom(f) by h ⊇ g. The cell g(-3,-1),2;g(-3,0),0 has second column, 0,2 top down, and so must be critical. Therefore it is 2,2;0.0. The same argument works inductively, successively to the left, showing that h on (-∞,-3] × {0} is constantly 0. On the other side, the cell 3,g(-m-2,-1);0,g(-m-2,0) has first column 0,3, top down, and so must be critical. Therefore it is 3,3;0,0. The same argument works inductively, successively to the right, showing that h on [m-2,∞) × {0} is constantly 0. This establishes the claim.

We claim that any cell a,b;x,y in g with a,b ∈ Q ∪ {0,1}, is either in K or is a,b;4,5.

We claim that if a,b;x,y and b,c;y,z are cells in g with a,b,c ∈ Q ∪ {0,1}, then both cells are in K. To see this, first suppose a,b;x,y is not in K. Then by the previous claim, a,b,x,y is a,b,4,5. Therefore b,c,5,z is either in K, or b,c;5,z is b,c,4,5. Both of these are impossible.

We now claim that all cells in h that live within Z × N lie in K. We prove this by induction on the rows in Z × N going up. We show that every cell in g whose left corner lies in Z × {i}, i ≥ 0, lies in K. The basis case is obvious by the previous claim, since we see only elements of Q ∪ {0,1] on Z × {0}. For the induction step, suppose every cell in g whose left corner lies in Z × {i}, i ≥ 0, lies in K. Then clearly we see only elements of Q ∪ {0,1} on Z × {i,i+1}, and hence we can repeat this argument to easily see that every cell in h whose left corner lies in Z × {i+1} lies in K.

We have now established that h restricted to Z × N not only initializes for TM(↔), but also has all of its cells lying in K. Furthermore, K[TM] and h use ony Q' and not qn. Hence by Lemma 2.7, TM must diverge. QED

LEMMA 2.9. If TM diverges then g is fully expandable.

Proof: Let TM diverge, and by Lemma 2.7, let H:Z × N → Q ∪ {0,1} initialize for TM(↔) and have all cells lying in K[TM]. Since q_n is not present in K[TM], q_n is not present in H. We now extend H to a full expansion h of g.

Since dom(H) = Z × N, we need to extend H on Z × $(-\infty,-1]^2$. Of course, extend on dom(g) by g. Extend H on the rest of Z × N to be all 2's, except on [m-2,∞) × {-m+2,-2}, where it is all 3's. We have only to check that every cell in this extension h:Z^2 → Q ∪ [0,5] of H is an expansion of g.

Clearly every cell in h whose left corner lies in Z × N lies in K since this is the case for H. It is also clear that every cell in h whose left corner lies on Z × {-1} is obviously either 2,2;0,0 or 3,3;0,0 or wholly resides within dom(g).

Every cell in h whose left corner lies on Z × {-m+2,-2} is clearly 2,2;2,2 or 3,3;3,3 or wholly resides within dom(h). Also every cell in g whose left corner lies on Z × {-m+1} is either 2,2;2,2 or 2,2;3,3 or wholly resides within dom(h).

Recall that we constructed f so that these critical cells 2,2;0,0, 2,2;2.2., 3,3;0,0, 3,3;3,3, 2,2;3,3 are all cells in g. QED

LEMMA 2.10. TM diverges if and only if g:[-2,m-3] × [-m+1,0] → Q' ∪ [0,5] is fully expandable. We can set m ≥ (72n + 110.25)1/2 + 4.5, and use a function f:[1,m]2 → [1,n+6].

Proof: The first claim is from Lemmas 2.8, 2.9. For the second claim, we refer to step 2 in the construction of g. We require that (m-6)(m-3)/9 ≥ |K| and m ≥ 5. By Lemma, |K| ≤ 16n+4, and (m-6)(m-3)/9 ≥ 8n+12 reduces to m^2 - 9m + 18 ≥ 72n + 108, $(m - 9/2)^2$ - 81/4 + 18 ≥ 72n + 108, |m - 9/2| ≥ (72n + 110.25)1/2, with m ≥ $(72n + 110.25)^{1/2}$ + 4.5 ∧ m ≥ 5 being sufficient. The m ≥ 5 is redundant, so we can use any m ≥ $(72n + 110.25)^{1/2}$ + 4.5.

For the second claim, let g be as given. Define f:$[1,m]^2$ → Q ∪ [0,5] by f(i,j) = g(i-3,j-m). We claim that g is fully expandable if and only if f is fully expandable. To see this, let g' be a full expansion of g. Then f' is a full expansion of f, where we set f'(i,j) = g'(i-3,j-m). Clearly f ⊆ f'. Note that every cell g'(i,j),g'(i+1,j);g'(i,j+1),g'(i+1,j+1) in g' is the cell f'(i+3,j+m),f'(i+3,j+m);f'(i+3,j+m+1),f'(i+3,j+m+1) in h'. The converse is proved the same way.

Thus we have constructed f:$[1,m]^2$ → Q ∪ [0,5] from TM such that TM diverges if and only if f is fully expandable. Obviously we can use range [1,m+6] since the contents of the range plays absolutely no role. QED

THEOREM 2.11. Assume ZFC is consistent and TM is a deterministic n state 2 symbol infinite two way Turing machine. There is an f:[1,m]2 → [1,n+6], m = ceiling((72n + 110.25)1/2 + 4.5), where a very weak fragment of ZFC proves that "TM diverges if and only if f is fully expandable". Furthermore, there is a highly efficient method of converting TM to f and generating the proof of this equivalence in the very weak fragment of ZFC.

LEMMA 2.12. Assume ZFC is consistent. There is a divergent TM with 1919 states such that "TM diverges" is not provable in ZFC. Assume ZFC is 1-consistent. There is a divergent TM with 1919 states such that "TM converges" is either provable nor refutable in ZFC. The TM is deterministic, with two tape symbols and a two way infinite tape.

Proof: O'Rear [SO16] has programmed such a 1919 state TM that searches for a contradiction in ZFC. So his "TM diverges" is equivalent to Con(ZFC). For the first claim, apply Gödel's Second Incompleteness Theorem. For the second claim, the additional claim that "TM diverges" is not refutable in ZFC comes from the 1-consistency of ZFC, since "TM diverges" is a $\Pi^0{}_1$ sentence. QED

Prior work of [YA16], using adapted work of mine from Emulation Theory, used 7910 states.

COROLLARY 2.13. Assume ZFC is consistent. There is a fully expandable function f:{1,...,376}2 → {1,...,382} such that "f is fully expandable" is not provable in ZFC. Assume ZFC is 1-consistent. There is a fully expandable function f:{1,...,376}2 → {1,...,382} such that "f is fully expandable" is independent of ZFC.

Proof: By Theorem 2.11 and Lemma 2.12 together with the calculation that the ceiling of (72n + 110.25)1/2 + 4.5 with n = 1919 is 376. QED

If we use the earlier version of [YA16] with 7910 states, we obtain the following.

COROLLARY 2.14. Assume SRP is consistent. There is a fully expandable function f:$\{1,...,755\}^2$ → {1,...,761} such that "f is fully expandable" is not provable in SRP. Assume SRP is 1-consistent. There is a fully expandable function f:$\{1,...,755\}^2$ → {1,...,761} such that "f is fully expandable" is independent of SRP.

Proof: [YA16] programs a Turing machine that corresponds to a $\Pi^0{}_1$ statement of mine that is provably equivalent to Con(SRP) over a weak fragment of ZFC. QED

However, we expect that using the approach of [SO16], Corollary 2.14 can be improved with a number fairly close to 376.

We now indicate the modifications that are needed to obtain these results for progressive expandability rather than full expandability.

TO BE CONTINUED.

REFERENCES

[SO16] S. O'Rear, NQL (Not Quite Laconic) code on github, and comments regarding 1919 states,
https://github.com/sorear/metamath-turing-machines/tree/99a8c95
http://www.scottaaronson.com/blog/?p=2741#comment-1100142df

[YA16] A. Yeddida and S. Aaronson. A Relatively Small Turing Machine Whose
Behavior Is Independent of Set Theory, Complex Systems 25(4), 2016.