

THE LOGIC IN COMPUTER SCIENCE COLUMN

BY

ANUJ DAWAR

Department of Computer Science and Technology
University of Cambridge, Cambridge, CB3 0FD, UK
`anuj.dawar@cl.cam.ac.uk`

In this issue, I am delighted to present a contributed column by Harry Lewis. The author needs no introduction as his contributions to logic and the theory of computation over decades will be well known to readers. I myself studied his textbook on *Elements of the Theory of Computation*, written with Christos Papadimitriou, when I was an undergraduate student, as did a generation of computer scientists. In the present contribution, he revisits a combinatorial problem which was introduced by him and Stål Aanderaa in the context of studying the classical decision problem for prefix classes of first-order logic. The article gives a clean and modern exposition and the proof of undecidability. I trust the readers of this column will find it as much of a delight to read as I did.

LINEAR SAMPLING REVISITED

IN MEMORY OF STÅL AANDERAA (1931–2026)

Harry R. Lewis

Gordon McKay Professor of Computer Science, *emeritus*, Harvard University

1 Preface

When first Church [1936] and, soon after, Turing [1936] established the computational undecidability of the *Entscheidungsproblem*, the system to which they were referring was the first-order predicate calculus as formulated by Hilbert and Ackermann [1928]. Even before Church and Turing had formalized computability in order to resolve the main question, others had chipped away at it by identifying solvable subcases. Bernays and Schönfinkel [1928] established the decidability of satisfiability for the class of prenex formulas with quantifier prefixes of the form $\exists^*\forall^*$ —it was for a variation of this problem that Frank Ramsey [1930] then introduced the combinatorial theory that bears his name. The program of classifying prefix classes was completed when Kahr et al. [1962] established that satisfiability even of the $\forall\exists\forall$ class is undecidable: Except for the $\exists^*\forall^*$, $\exists^*\forall\exists^*$, and $\exists^*\forall\forall\exists^*$ classes, all the prefix classes are undecidable. (This is for first-order logic without function signs or the identity sign; the situation changes if either is allowed.) With the $\forall\exists\forall$ case settled, the search was on to classify subclasses of the $\forall\exists\forall$ class. Suppose the prefix is $\forall x\exists u\forall y$ and only monadic and dyadic (1- and 2-place) predicate letters are allowed. If the dyadic letters are allowed to appear only with certain arrangements of x , u , and y , which combinations result in solvable classes, and are the rest all reduction classes (of maximal r.e. degree)?

More than fifty years ago, in Aanderaa and Lewis [1974], Norwegian mathematician Stål Aanderaa and I completed this classification of $\forall\exists\forall$ subclasses. The bottom line is that any combination including both Pxy and Pyu (or the equivalent pair Pyx and Puy) yields a reduction class, and all the others are solvable. (In fact, monadic letters plus only a single dyadic predicate letter P suffice for the unsolvability result.) To establish this, we introduced a combinatorial problem we dubbed Linear Sampling, proved that it was undecidable, and reduced it to the logical problem of interest.

Aanderaa and Lewis [1974] was a collaboration between a combinatorial ge-

nus and a stumbling graduate student serving as scribe. The proofs are complex, incomplete, and poorly motivated. Stål died on January 26 of this year. In a spirit of humility prompted by memories of his stunning vision and of his warm generosity, I here offer a revised and fuller account of linear sampling. In 1974 we hoped that linear sampling might prove interesting independent of our logic proof. In that spirit, I hope the community will benefit from this improved exposition.

2 Introduction

Linear sampling systems classify two-way infinite tapes, that is, mappings from $\mathbb{Z}$ to a finite alphabet Σ . A linear sampling system *accepts* or *rejects* a particular tape τ depending on whether all specified “samples” from τ meet its constraints. A *sample* is a vector of symbols drawn from cells of τ whose coordinates satisfy numerical constraints specified as part of the system.

To be precise, a *Linear Sampling System* $X = \langle \Sigma, A, B, L \rangle$ is specified by

- a finite set Σ , the tape alphabet;
- a finite subset $A \subset \Sigma^k$ for some $k > 0$;
- a finite subset $B \subset \Sigma^\ell$ for some $\ell > 0$;
- a linear equation L in ℓ variables.

For X to accept a tape, the symbols in every block of k consecutive tape cells must be in A , and every ℓ -tuple of symbols at tape coordinates satisfying L must be in B . That is,

- $\langle \tau(n), \tau(n+1), \dots, \tau(n+k-1) \rangle \in A$ for all $n \in \mathbb{Z}$, and
- $\langle \tau(n_1), \dots, \tau(n_\ell) \rangle \in B$ for all $n_1, \dots, n_\ell \in \mathbb{Z}$ satisfying $L(n_1, \dots, n_\ell)$.

We’ll refer to a k -tuple satisfying the first condition as a *local sample* of the tape, and an ℓ -tuple satisfying the second condition as a *global sample*. We immediately narrow our focus to the linear equation in four variables

$$L(n_1, n_2, n_3, n_4) \quad \equiv \quad n_2 - n_1 = n_4 - n_3.$$

(We briefly consider other linear equations at the end of this paper, and there pose an open question.) So the decision problem can be stated thus: Suppose you are given the two finite sets $A \subset \Sigma^k$ and $B \subset \Sigma^\ell$. Is there a two-way infinite tape such that (a) the symbols in every block of k consecutive cells constitute a sequence in A and (b) the symbols in any four tape cells such that the distance between the

first two is the same as the distance between the last two comprise a sequence in B .

We refer to (a) as the *local condition* and to (b) as the *global condition*. The global condition relies on so little information about the relative positions of the cells that it may not be evident how to encode into it an undecidable word problem or automaton computation. Nonetheless, as we here show, there is no algorithm to determine from A and B whether a tape exists that satisfies both conditions.

3 The basic ideas

We're going to reduce the origin-constrained domino problem [Wang, 1961] to the linear sampling problem. A *domino system* includes a finite set of oriented, square tiles, that is quadruples whose components are drawn from a finite set of *colors*, plus a designated *origin domino*. The question is whether the first quadrant of the plane can be tiled by placing dominos at nonnegative integer coordinates in such a way that the domino at $\langle 0, 0 \rangle$ is the origin domino and the colors of all abutting edges match, that is, for all $i, j \in \mathbb{N}$,

- the color of the right edge of the domino at $\langle i, j \rangle$ is the color of the left edge of the domino at $\langle i + 1, j \rangle$, and
- the color of the top edge of the domino at $\langle i, j \rangle$ is the color of the bottom edge of the domino at $\langle i, j + 1 \rangle$.

It is not hard to construct from any Turing machine a set of dominoes that effectively represents in successive rows of any tiling the configuration of the Turing machine at successive instants of time. It follows that the origin-constrained domino problem is undecidable, as a tiling of the entire first quadrant would represent an unending computation by the Turing machine.

Our objective is to embed domino systems in linear sampling systems. If a domino system can tile the first quadrant, then there will be a two-way infinite tape satisfying the constraints of the linear sampling system. Each tape cell will represent the domino in a particular position in the first quadrant of the plane. However, every such domino position will be replicated infinitely often.

We will be working with two specific relatively prime positive integers p and q . Any relatively prime pair would work as long as the numbers are greater than certain thresholds that will emerge in the course of the proof. That said, it will prove convenient for expository purposes to stipulate from the beginning that $p < q$ and in fact that $q = p + 1$.

Let r be any integer ≥ 2 ; we use r as a variable ranging over $\{p, q\}$. Let's call the number of times r divides $n \in \mathbb{Z}$ the *r-order* of n . That is, the *r-order* of n is

the largest number e such that r^e divides n evenly. Every integer other than 0 has an r -order, which can also be described as the number of trailing 0s in the base- r notation for n . The r -order of 0 is infinite. Taking $r = 10$ for familiarity, nine out of every ten consecutive positive integers have 10-order 0. Of the numbers between 1 and 100 inclusive, 90 have 10-order 0, 9 have 10-order 1, and one has 10-order 2.

Our plan—which we can’t carry through in the simple form we are stating here—is to represent the domino at position $\langle i, j \rangle$ of a putative tiling at all tape coordinates that have p -order i and q -order j . The local condition can be used to force the origin domino onto the tape cells that have order 0 with respect to both p and q . The hard part will be devise a global condition that can extract enough information about the relative orders of different cells to ensure that domino edge colors match up if their coordinates differ by 1 in one dimension and are equal in the other dimension.

One problem with our plan is apparent immediately. Any shift of an accepted tape (addition of a constant to all cell coordinates) will also be accepted, since if $n_2 - n_1 = n_4 - n_3$, then $(n_2 + t) - (n_1 + t) = (n_4 + t) - (n_3 + t)$ for any $t \in \mathbb{Z}$. But this is not the only problem with our plan. It’s time to go a level deeper.

4 Perfect and Admissible Tapes

Domino systems will be mapped to linear sampling systems whose tapes can be regarded as having three tracks. That is, the tape alphabet is the cross product of three finite sets of symbols. The first two tracks contain “address” information, which will help the linear sampling system infer information about the relative p - and q -orders of cells’ coordinates. The third track will represent the domino itself.

For the moment we’ll focus just on an address channel and pick $r = p$ or $r = q$. An r -tape is a tape with symbols that are numbers in the range $1, \dots, r^2 - 1$ incongruent to 0 (mod r). In other words, they are two-digit numerals in base r notation with the second digit nonzero. Ideally, in an address track, the two digits in the cell with coordinate n will be the rightmost nonzero digit of the base r notation for n and the immediately preceding digit. For example, taking $r = 10$ again for convenience, the address track would contain 07 if the coordinate were 60700, and would contain 89 if the coordinate were -110 , since in 10’s complement notation, $-110 = \dots 999890$.

We’ll need some notation for these ideas. If r is understood, we’ll write $\omega(n)$ for the r -order of n , adding a subscript for clarity when needed. Similarly, with r understood, $\delta(n) = nr^{-\omega(n)}$, which can be understood as the number represented by the base- r notation for n with trailing 0s dropped.

For $n \neq 0$, $\lambda(n)$ is the remainder ($0 < \lambda(n) < r^2$) when $\delta(n)$ is divided by r^2 ,

that is, the last two base- r digits of $\delta(n)$. A *perfect r -tape* is then a tape in which for every $n \neq 0$, cell n contains symbol $\lambda(n)$. There are exactly $r^2 - r$ perfect r -tapes, which differ only in the cell at coordinate $n = 0$, which can contain any of the tape symbols.

Unfortunately, no linear sampling system can recognize all and only perfect r -tapes. We will define a broader class of r -tapes, the *admissible r -tapes*. Every perfect tape is admissible. A three-channel tape will be said to be *admissibly addressed* if its first channel is an admissible p -tape and its second channel is an admissible q -tape; similarly, a tape whose address channels are both perfect will be said to be *perfectly addressed*.

We'll show that it is possible to construct a LSS that recognizes all perfect tapes and only admissible tapes. and that any LSS that recognizes an admissibly addressed tape also recognizes a closely related perfectly addressed tape. The information in the address channels of such tape will provide the scaffolding for checking that the domino adjacency conditions are met by the dominos in the data track.

To define admissibility, we need the notion of i -admissibility, where i is a nonnegative integer. An admissible tape is one that is i -admissible for every i . The i -admissible tapes, for increasing values of i , are approximations of perfect tapes of increasing degrees of fidelity. An i -admissible tape can be shifted so that it agrees with a perfect tape on all but one of every r^{i+1} consecutive tape cells, and on the remaining cells, some are guaranteed to be in partial agreement.

To be precise: an r -tape is *i -admissible*, where $i \geq 0$, if it agrees with a shift of a perfect tape on cells of order less than i , and also agrees with this shifted tape on the second digits of cells of order equal to i . That is, τ is i -admissible if there is an integer $t \in \mathbb{Z}$ such that

$$\begin{aligned} \tau(n+t) &= \lambda(n) \quad \text{if } \omega(n) < i, \text{ and} \\ \tau(n+t) &\equiv \lambda(n) \pmod{r} \quad \text{if } \omega(n) = i. \end{aligned} \tag{4.1}$$

Note that if t satisfies these conditions for τ , then so does t plus any multiple of r^{i+1} , since adding r^{i+1} to a number of r -order at most i does not change its r -order.

As stated earlier, an *admissible r -tape* is one that is i -admissible for every i .

We'll define an LSS that recognizes admissible tapes, using an induction to infer $(i+1)$ -admissibility from i -admissibility. First, though, let's make the leap from admissible to perfect tapes. A *central segment* of a tape is the finite sequence of symbols between coordinates $-n$ and $+n$ for some $n \geq 0$.

Theorem 1. *An LSS that accepts an admissibly addressed tape ϕ accepts a perfectly addressed tape π with the property that every central segment of π is a segment of ϕ .*

Proof. Suppose that LSS X accepts admissibly addressed tape τ . We'll define an infinite sequence of finite sequences $s_0, s_1, \dots$, where s_k is of length $2k + 1$. Each s_k is a central segment of a perfectly addressed tape, though not necessarily of the same perfectly addressed tape for different values of k . We'll then use König's lemma to construct from these segments a single perfectly addressed tape accepted by X .

Given $k \geq 0$, let i be any integer such that p^i and q^i both exceed k . Let's denote by τ and σ the two address tracks of ϕ . Because both address tracks are i -admissible, there are numbers t and u such that for every $n \in \mathbb{Z}$,

$$\tau(n + t) = \lambda_p(n) \quad \text{if } \omega_p(n) < i \quad (4.2)$$

$$\tau(n + t) \equiv \lambda_p(n) \pmod{p} \quad \text{if } \omega_p(n) = i \quad (4.3)$$

$$\sigma(n + u) = \lambda_q(n) \quad \text{if } \omega_q(n) < i \quad (4.4)$$

$$\sigma(n + u) \equiv \lambda_q(n) \pmod{q} \quad \text{if } \omega_q(n) = i. \quad (4.5)$$

Since p and q are relatively prime, so are p^{i+1} and q^{i+1} , and by the Chinese Remainder Theorem there is an integer v congruent to $t \pmod{p^{i+1}}$ and to $u \pmod{q^{i+1}}$. Equations (4.2)–(4.5) remain true when v is substituted for t and u , since (for $r = p$ or q) an i -admissible r -tape remains i -admissible when it is translated by a multiple of r^{i+1} . Now the sequence $s_k = \langle \phi(v - k), \dots, \phi(v + k) \rangle$ is a central segment of a perfectly addressed tape, since τ and σ are i -admissible and numbers less than or equal to k have p - and q -order less than i .

For each $k \geq 0$, infinitely many of the s_j ($j \geq k$) must agree on a central substring from position $-k$ to $+k$. By König's Lemma there is an infinite string of which every central substring is one of these perfectly addressed substrings, and which therefore is itself perfectly addressed and is accepted by X . $\square$

Theorem 2. *It is possible to construct an LSS that accepts all perfect tapes and only admissible tapes.*

Proof. The value of r is fixed for the remainder of this argument. The construction of the required LSS X_r is straightforward. The local and global conditions are simply the sets of local and global samples of perfect tapes. That is, $X_r = \langle \Sigma, A, B, L \rangle$, where $\Sigma = \{n : 0 < n < r^2 \text{ and } n \not\equiv 0 \pmod{r}\}$, L is, as always, the equation $n_2 - n_1 = n_4 - n_3$, and

$$A = \{ \langle \pi(n), \dots, \pi(n + r - 1) \rangle : n \in \mathbb{Z} \text{ and } \pi \text{ is a perfect } r\text{-tape} \}$$

$$B = \{ \langle \pi(n_1), \pi(n_2), \pi(n_3), \pi(n_4) \rangle : \pi \text{ is a perfect } r\text{-tape and } n_2 - n_1 = n_4 - n_3 \}.$$

It follows immediately that X_r accepts all perfect r -tapes. The challenge will be to show that the construction of X_r from samples of perfect r -tapes can, to a

useful extent, be inverted, so that a perfect tape can be constructed from any tape accepted by X_r .

So let τ be any tape accepted by X_r . We show that τ is i -admissible by induction on i . This is a lengthy proof; the base case is Lemma 1 and the induction step is Lemma 2.

Lemma 1. τ is 0-admissible.

Proof. When $i = 0$, condition (4.1). that $\tau(n + t) = \lambda(n)$ if $\omega(n) < i$, is vacuously satisfied, so proving 0-admissibility amounts to showing that there is a shift of τ by some number t , $0 \leq t < r$, such that

$$\tau(n + t) \equiv n \pmod{r} \text{ for every } n \in \mathbb{Z} \text{ such that } n \not\equiv 0 \pmod{r}. \quad (4.6)$$

Start by looking at $\langle \tau(0), \dots, \tau(r - 1) \rangle$; since τ is accepted, this vector must be in A , and for it to be in A there must be a perfect r -tape π and a displacement u such that $\tau(n) = \pi(n + u)$ for $0 \leq n < r$. Since π is perfect, $\pi(n) \equiv n \pmod{r}$ when $0 < n < r$, so $\tau(n - u) = \pi(n) \equiv n \pmod{r}$ when $0 < n < r$. Therefore (4.6) is satisfied with $t = -u$ when $0 \leq n < r$.

With (4.6) established for $0 \leq n < r$, it suffices to show that if (4.6) holds for any block of r symbols on an accepted tape, then it also holds for the blocks that begin one cell earlier and one cell later. The two cases being symmetrical, we'll consider just the case of a block and the block beginning one cell later.

Consider the second digit (the remainder when divided by r) of the contents of a cell of a perfect r -tape. For any three successive cells, these digits must fit one of these patterns:

- (a) $x, x + 1, x + 2$ for some x such that $1 \leq x \leq r - 3$
- (b) $r - 2, r - 1, x$, where $1 \leq x \leq r - 1$
- (c) $r - 1, x, 1$, where $1 \leq x \leq r - 1$
- (d) $x, 1, 2$, where $1 \leq x \leq r - 1$

The r cases listed here (option (a) covers $r - 3$ different cases) are unambiguous—no triple satisfies more than one of them. For example, if the first component is $r - 1$, the triple might be one of type (c) or of type (d), but since the third component must be 1 or 2, those two cases can be distinguished by looking at the third component. This means that if a local sample from a tape matches an element of A , any three consecutive members of that sequence suffice to determine uniquely $\pmod{r}$ the amount by which that section of the tape is shifted from a perfect tape.

Now as long as $r > 3$, the last three symbols of a local sample of a tape occur one position earlier in the local sample that begins one cell later. So the shift of both from a perfect tape must be the same $(\text{mod } r)$. That is, if $\tau(n+t) \equiv \lambda(n) \equiv n \pmod{r}$ for all n in the first block such that $n \not\equiv 0 \pmod{r}$, then the same holds for all $n \not\equiv 0 \pmod{r}$ in the second block, including the final position as was to be shown. This completes the proof of Lemma 1, the base case. $\square$

We note a further consequence of this argument that will prove useful later on. There is a mapping $\mu : A \rightarrow \{0, 1\}^r$ from the local condition to bit vectors of length r that identifies, for any local sample of a perfect tape, which elements have coordinates of order 0. That is, if π is a perfect tape and

$$\mathbf{g} = \langle \pi(n), \dots, \pi(n+r-1) \rangle \in A,$$

then element j ($0 \leq j \leq r-1$) of $\mu(\mathbf{g})$ is 0 if and only if $\omega(n+j) = 0$, and that element is 1 if $\omega(n+j) > 0$.

Now for the induction step in the proof that X_r accepts only admissible tapes.

Lemma 2. *For each $i \geq 0$, every i -admissible tape accepted by X_r is $(i+1)$ -admissible.*

Proof. We will define two kinds of global samples from a perfect tape, flat and incremental. We would like it to be the case that a flat sample indicates that the four cells have the same order and that an incremental sample indicates that the order of fourth is one greater than the order of the other three, but that is too much to ask. We can guarantee only that these properties hold under further conditions on the sample. We will then need a separate argument to guarantee that cells whose coordinates have the same p - and q -orders always have the same third track.

Flat samples first.

Let $\mathbf{g} = \langle g_1, g_2, g_3, g_4 \rangle$ be any quadruple of r -tape symbols. Then $\mathbf{g}$ is said to be *flat* provided that

- (a) $g_2 - g_1 \equiv g_4 - g_3 \not\equiv 0 \pmod{r}$;
- (b) $g_3 - g_1 \not\equiv 0 \pmod{r}$; and
- (c) $g_1 + g_4 \not\equiv 0 \pmod{r}$.

Sublemma 1. *If π is a perfect tape, $n_2 - n_1 = n_4 - n_3$, and the global sample $\langle \pi(n_1), \dots, \pi(n_4) \rangle$ is flat, then n_1, n_2, n_3, n_4 , and $n_2 - n_1 = n_4 - n_3$ all have equal, finite order.*

Proof. Since r is fixed, in what follows all congruences and incongruences will be understood to be $(\text{mod } r)$. Let $g_i = \pi(n_i)$ for each $i = 1, \dots, 4$. First note that in addition to the four quantities stipulated in (a)–(c) to be incongruent to 0, two more incongruences are implied:

(d) $g_4 - g_2 \not\equiv 0$, because

$$\begin{aligned} g_3 &\equiv g_1 - g_2 + g_4 \text{ by (a), so} \\ g_3 - g_1 &\equiv g_1 - g_2 + g_4 - g_1 = g_4 - g_2 \not\equiv 0 \text{ by (b).} \end{aligned}$$

(e) $g_2 + g_3 \not\equiv 0$, because

$$\begin{aligned} g_4 &\equiv g_2 + g_3 - g_1 \text{ by (a), so} \\ g_1 + g_4 &\equiv g_1 + g_2 + g_3 - g_1 = g_2 + g_3 \not\equiv 0 \text{ by (c).} \end{aligned}$$

Let ℓ , be an index $1 \leq \ell \leq 4$ such that n_ℓ has lowest order among $n_1, \dots, n_4$. (The incongruences imply that the g_i are not all equal to each other, so at least one of the n_i must be nonzero and hence of finite order.) Let $e_i = \omega(n_i) - \omega(n_\ell)$ for $i = 1, \dots, 4$, so that $e_\ell = 0$ and all of the e_i are nonnegative. We need to show that $e_i = 0$ for each i .

Recall that for any $n \neq 0$, $n = r^{\omega(n)}\delta(n)$. Dividing the equation $n_2 - n_1 = n_4 - n_3$ by $r^{\omega(n_\ell)}$, it follows that

$$\begin{aligned} r^{e_2}\delta(n_2) - r^{e_1}\delta(n_1) &= r^{e_4}\delta(n_4) - r^{e_3}\delta(n_3), \text{ so} \\ r^{e_2}g_2 - r^{e_1}g_1 &\equiv r^{e_4}g_4 - r^{e_3}g_3 \pmod{r}, \end{aligned} \tag{4.7}$$

since for each i , $g_i = \pi(n_i) = \lambda(n_i)$, the last two digits of $\delta(n_i)$. Now if $e_i > 0$ for three different i , then the fourth would also have to be > 0 for (4.7) to hold, but that would contradict the fact that $e_\ell = 0$. Nor can $e_i > 0$ for only one i , for then (4.7) would require that $g_i \equiv 0$ for that value of i , contradicting the fact that all $g_i \not\equiv 0$. Finally, each of the six cases in which two of the e_i are 0 and two are nonzero contradicts one of the six incongruences in (a)–(e):

- If $e_1 = e_2 = 0$ while $e_3 > 0$ and $e_4 > 0$, then (4.7) would imply that $g_2 - g_1 \equiv 0$, contradicting (a).
- If $e_1 = e_3 = 0$ while $e_2 > 0$ and $e_4 > 0$, then (4.7) would imply that $-g_1 \equiv -g_3$, contradicting (b).
- If $e_1 = e_4 = 0$ while $e_2 > 0$ and $e_3 > 0$, then (4.7) would imply that $-g_1 \equiv g_4$, contradicting (c).

- If $e_2 = e_3 = 0$ while $e_1 > 0$ and $e_4 > 0$, then (4.7) would imply that $g_2 \equiv -g_3$, contradicting (e).
- If $e_2 = e_4 = 0$ while $e_1 > 0$ and $e_3 > 0$, then (4.7) would imply that $g_2 \equiv g_4$, contradicting (d).
- If $e_3 = e_4 = 0$ while $e_1 > 0$ and $e_2 > 0$, then (4.7) would imply that $g_4 - g_3 \equiv 0$, contradicting (a).

This completes the proof of Sublemma 1. □

Next we define samples which will, under certain conditions, be sufficient to establish that the first three cells have order one less than the fourth.

Let $\mathbf{g} = \langle g_1, g_2, g_3, g_4 \rangle$ be a quadruple of r -tape symbols. Then $\mathbf{g}$ is said to be *incremental* provided that all of the following hold:

- (A) $g_1 + g_4 \not\equiv 0 \pmod{r}$
- (B) $g_1 - g_4 \not\equiv 0 \pmod{r}$
- (C) $g_2 + g_4 \not\equiv 0 \pmod{r}$
- (D) $g_2 - g_4 \not\equiv 0 \pmod{r}$
- (E) $g_3 + g_4 \not\equiv 0 \pmod{r}$
- (F) $g_3 - g_4 \not\equiv 0 \pmod{r}$
- (G) $g_1 - g_2 - g_3 \equiv 0 \pmod{r}$ but $g_1 - g_2 - g_3 \not\equiv 0 \pmod{r^2}$

Sublemma 2. *If π is a perfect tape, $n_2 - n_1 = n_4 - n_3$, and the global sample $\langle \pi(n_1), \dots, \pi(n_4) \rangle$ is incremental, then n_1, n_2 , and n_3 have equal order, which is 1 less than the order of n_4 , and $r\lambda(n_4) \equiv \lambda(n_2) + \lambda(n_3) - \lambda(n_1) \pmod{r^2}$.*

Proof. We first note that (G) implies certain additional incongruences when taken together with the fact that all tape symbols are incongruent to 0 $\pmod{r}$:

- (H) $g_3 - g_1 \not\equiv 0 \pmod{r}$, because $g_2 \not\equiv 0 \pmod{r}$
- (I) $g_2 + g_3 \not\equiv 0 \pmod{r}$, because $g_1 \not\equiv 0 \pmod{r}$
- (J) $g_2 - g_1 \not\equiv 0 \pmod{r}$, because $g_3 \not\equiv 0 \pmod{r}$.

As in the proof of Sublemma 1, let ℓ , $1 \leq \ell \leq 4$, be an index such that n_ℓ has lowest order among $n_1, \dots, n_4$, and let $e_i = \omega(n_i) - \omega(n_\ell)$. We aim to show that $e_1 = e_2 = e_3 = 0$ and $e_4 = 1$. Equation (4.7) holds for the same reasons as in the proof of Sublemma 1.

It is impossible for all four e_i to be 0, as (4.7) would then imply that

$$g_1 - g_2 - g_3 \equiv -g_4 \not\equiv 0 \pmod{r},$$

contradicting (G). Nor can exactly three of the e_i be nonzero, since as in the proof of Sublemma 1, (4.7) would then require that the fourth be nonzero as well. Ruling out the possibility that exactly two of the e_i are 0 requires a case analysis similar to that in the proof of Sublemma 1 (all congruences being $\pmod{r}$):

- If $e_1 = e_2 = 0$ while $e_3 > 0$ and $e_4 > 0$, then (4.7) would imply that $g_2 - g_1 \equiv 0$, contradicting (J).
- If $e_1 = e_3 = 0$ while $e_2 > 0$ and $e_4 > 0$, then (4.7) would imply that $-g_1 \equiv -g_3$, contradicting (H).
- If $e_1 = e_4 = 0$ while $e_2 > 0$ and $e_3 > 0$, then (4.7) would imply that $-g_1 \equiv g_4$, contradicting (B).
- If $e_2 = e_3 = 0$ while $e_1 > 0$ and $e_4 > 0$, then (4.7) would imply that $g_2 \equiv -g_3$, contradicting (I).
- If $e_2 = e_4 = 0$ while $e_1 > 0$ and $e_3 > 0$, then (4.7) would imply that $g_2 \equiv g_4$, contradicting (D).
- If $e_3 = e_4 = 0$ while $e_1 > 0$ and $e_2 > 0$, then (4.7) would imply that $g_4 - g_3 \equiv 0$, contradicting (F).

That leaves the four cases in which exactly one of the e_i is nonzero and the others are 0.

- If $e_1 > 0$ while $e_2 = e_3 = e_4 = 0$, then (4.7) would imply that $g_2 - g_4 + g_3 \equiv 0 \pmod{r}$, which together with (G) implies that $g_1 - g_4 \equiv 0 \pmod{r}$, contradicting (B).
- If $e_2 > 0$ while $e_1 = e_3 = e_4 = 0$, then $-g_1 - g_4 + g_3 \equiv 0 \pmod{r}$, which implies $g_2 + g_4 \equiv 0 \pmod{r}$, contradicting (A).
- If $e_3 > 0$ while $e_1 = e_2 = e_4 = 0$, then $g_2 - g_1 - g_4 \equiv 0 \pmod{r}$, which implies that $g_3 + g_4 \equiv 0 \pmod{r}$, contradicting (E).

So $e_1 = e_2 = e_3 = 0$ and $e_4 > 0$. It remains to show that $e_4 \not\geq 1$. But if $e_4 \geq 2$, then (4.7) would imply that $g_1 - g_2 - g_3 \equiv 0 \pmod{r^2}$, contradicting the second clause of (G).

Now substituting $e_1 = e_2 = e_3 = 0$ and $e_4 = 1$ into $r^{e_2}g_2 - r^{e_1}q_1 = r^{e_4}g_4 - r^{e_3}g_3$ yields $g_2 - g_1 = r \cdot g_4 - g_3$, which implies that $r \cdot g_4 \equiv g_2 + g_3 - g_1 \pmod{r^2}$. This completes the proof of Sublemma 2. $\square$

We can now complete the proof of Lemma 2, that every i -admissible tape accepted by X is $(i + 1)$ -admissible.

Let τ be an i -admissible tape accepted by X_r , and let t an integer such that

$$\begin{aligned} \tau(n + t) &= \lambda(n) \quad \text{if } \omega(n) < i, \text{ and} \\ \tau(n + t) &\equiv \lambda(n) \pmod{r} \quad \text{if } \omega(n) = i. \end{aligned}$$

We will show that there is an integer u such that

$$\tau(N + u) = \lambda(N) \quad \text{if } \omega(N) \leq i, \text{ and} \tag{4.8}$$

$$\tau(N + u) \equiv \lambda(N) \pmod{r} \quad \text{if } \omega(N) = i + 1, \tag{4.9}$$

thus establishing that τ is $(i + 1)$ -admissible.

We first show that if M, N , and their difference are all of order $i < \infty$, then $\tau(N + t) - \tau(M + t) \pmod{r^2}$ depends only on $N - M$, and is in fact equal to $\lambda(N - M)$.

Let k_1 and k_2 be distinct numbers of order 0 and let d be a number of order 0 such that $k_1 + d$ and $k_2 + d$ are also of order 0. Thus multiplying any of these numbers by r^i yields a number of order i . Let $N_j = k_j r^i$ for $j = 1, 2$. We plan to show that moving down the tape distance dr^i starting from either $N_1 + t$ or $N_2 + t$ results in the same change in the values in the tape cells, namely by $\lambda(d)$. To be precise, we aim to show that

$$\begin{aligned} \tau(N_1 + dr^i + t) - \tau(N_1 + t) &\equiv \tau(N_2 + dr^i + t) - \tau(N_2 + t) \\ &\equiv \lambda(d) \pmod{r^2}. \end{aligned}$$

It may not be possible to show this using Sublemma 1 directly because these tape coordinates may not satisfy the conditions of that proposition, so instead we will have to find a suitable third coordinate and compare both to that third position.

Let k be an integer in the range $0 \leq k < r$ such that each of the following is incongruent to 0 $\pmod{r}$:

(i) k

(ii) $k + d$

$$(iii) \ k - k_1$$

$$(iv) \ k - k_2$$

$$(v) \ k + k_1 + d$$

$$(vi) \ k + k_2 + d$$

It is possible to find a suitable k as long as $r > 6$. Let $N = kr^i$. Then for $j = 1$ and $j = 2$, the quadruple

$$\mathbf{g}_j = \langle \tau(N_j + t), \tau(N_j + dr^i + t), \tau(N + t), \tau(N + dr^i + t) \rangle$$

is flat: condition (a) holds because τ is i -admissible and all coordinates have the same order, as does the distance separating the two members of each pair, condition (b) holds by (i) and (ii), and condition (c) holds by (iii) and (iv).

Note that the quadruples $\mathbf{g}_1$ and $\mathbf{g}_2$ have the same third and fourth components and possibly different first and second components.

Since τ is accepted by X_r , $\mathbf{g}_j \in B$, the global condition of X_r . So there are, for $j = 1$ and 2 , perfect tapes π_j and nonzero integers m_j , n_j , and d_j , such that

$$\mathbf{g}_j = \langle \pi_j(m_j), \pi_j(m_j + d_j), \pi_j(n_j), \pi_j(n_j + d_j) \rangle.$$

By Sublemma 1, for $j = 1$ and 2 , m_j , $m_j + d_j$, n_j , $n_j + d_j$, and d_j all have the same order. These orders being finite, we can replace π_1 and π_2 by λ throughout. So for $j = 1$ and 2 ,

$$\lambda(m_j + d_j) - \lambda(m_j) \equiv \lambda(n_j + d_j) - \lambda(n_j) \equiv \lambda(d_j) \pmod{r^2}$$

But

$$\langle \lambda(n_1), \lambda(n_1 + d_1) \rangle = \langle \lambda(n_2), \lambda(n_2 + d_2) \rangle,$$

since the left and right sides are equal to the last two components of $\mathbf{g}_1$ and $\mathbf{g}_2$, respectively, which are equal to each other. Because $\mathbf{g}_1$ and $\mathbf{g}_2$ are flat, it follows that

$$\begin{aligned} \tau(N_1 + dr^i + t) - \tau(N_1 + t) &\equiv \lambda(n_1 + d_1) - \lambda(n_1), \\ &= \lambda(n_2 + d_2) - \lambda(n_2) \\ &\equiv \tau(N_2 + dr^i + t) - \tau(N_2 + t) \\ &\equiv \lambda(d) \pmod{r^2}, \end{aligned}$$

as was to be shown.

It follows that there is some k_0 such that $\tau(k_0r^i + dr^i + t) = \lambda(d)$ whenever $d \not\equiv 0 \pmod{r}$. Taking $u = k_0r^i + t$ establishes (4.8).

It remains to establish (4.9), that $\tau(N + u) \equiv \lambda(N) \pmod{r}$ if $\omega(N) = i + 1$. So let N be a number of order $i + 1$ and let $n = \tau(N + u)$. To find an incremental sample, we choose two order-0 numbers, m and d , from the set $\{j : 1 \leq j \leq r - 1\}$, subject to the following incongruences $\pmod{r}$:

1. $m + d \not\equiv 0$
2. $n + m \not\equiv 0$
3. $n - m \not\equiv 0$
4. $n + m + d \not\equiv 0$
5. $n - d \not\equiv 0$
6. $n + d \not\equiv 0$
7. $n - m + d \not\equiv 0$

Given n , each condition rules out at most $r - 1$ possible choices for the pair $\langle m, d \rangle$, so—estimating conservatively, since some pairs are ruled out by more than one incongruence—there will be at least one left provided that

$$(r - 1)^2 - 7 \cdot (r - 1) = (r - 8) \cdot (r - 1) > 0,$$

which is true provided that $r \geq 9$.

We claim that the sample

$$\mathbf{g} = \langle g_1, g_2, g_3, g_4 \rangle = \langle \tau(mr^i + u), \tau(mr^i + dr^i + u), \tau(N - dr^i + u), \tau(N + u) \rangle$$

is incremental. The seven conditions are satisfied:

(A)

$$\begin{aligned} \tau(mr^i + u) + \tau(N + u) &\equiv \lambda(m) + n \text{ by (4.8) and the definition of } n \\ &\equiv m + n \\ &\not\equiv 0 \pmod{r} \text{ by (2).} \end{aligned}$$

(B) $\tau(mr^i + u) - \tau(N + u) \equiv \lambda(m) - n \equiv m - n \not\equiv 0 \pmod{r}$ by (3).

(C) $\tau(mr^i + dr^i + u) + \tau(N + u) \equiv m + d + n \not\equiv 0 \pmod{r}$ by (1) and (4).

(D) $\tau(mr^i + dr^i + u) - \tau(N + u) \equiv m + d - n \not\equiv 0 \pmod{r}$ by (1) and (7).

(E) $\tau(N - dr^i + u) + \tau(N + u) \equiv -d + n \not\equiv 0 \pmod{r}$ by (5)

(F) $\tau(N - dr^i + u) - \tau(N + u) \equiv -d - n \not\equiv 0 \pmod{r}$ by (6)

(G)

$$\begin{aligned} & \tau(mr^i + u) - \tau(mr^i + dp^i + u) - \tau(N - rr^i + u) \\ \equiv & m - (m - d) - d = 0 \pmod{r} \end{aligned}$$

because all three terms have order i . And because N has order exactly $i + 1$, $0 < m < r$, and $0 < d < r$,

$$\begin{aligned} & \tau(mr^i + u) - \tau(mr^i + dr^i + u) - \tau(N - dr^i + u) \\ \equiv & m - (m + d) - (r - d) \equiv r \not\equiv 0 \pmod{r^2}. \end{aligned}$$

Equation (4.7), with $e_1 = e_2 = e_3 = 0$ and $e_4 = 1$, then implies that

$$\begin{aligned} p \cdot \tau(N + u) & \equiv \tau(N - dr^i + u) + \tau(mr^i + dr^i + u) - \tau(mr^i + u) \\ & \equiv \lambda(N - dr^i) + \lambda(mr^i + dp^i) - \lambda(mr^i) \\ & \equiv \lambda(rn - d) + \lambda(m + d) - \lambda(m) \\ & \equiv r \cdot \lambda(n) \pmod{r^2}, \text{ by Sublemma 2,} \end{aligned}$$

and therefore $\tau(nr^{i+1} + u) \equiv n \pmod{r}$, as was to be shown. This completes the proof of Lemma 2 (the induction step in the proof that tapes accepted by X_r are admissible). $\square$

Completing the proof of Lemma 2 finishes the proof of Theorem 2, establishing that X_r accepts all perfect and only admissible r -tapes. $\square$

5 Reducing domino systems to linear sampling systems

Theorem 3 (Main Theorem). *Given a domino system, it is possible to construct a linear sampling system that accepts a tape if and only if there is a tiling of the first quadrant of the plane consistent with the constraints of the domino system.*

Proof. First we need to combine the linear sampling systems guaranteed by Theorem 2 to accept all perfect and only admissible p - and q -tapes to accept all perfectly addressed and only admissibly addressed three-channel tapes. The method is basically a cross-product construction, with a small technical twist.

Suppose that for $r = p, q$, X_r is an LSS accepting all perfect r -tapes and only admissible r -tapes. Then from X_p and X_q we can construct an LSS X accepting all perfectly addressed tapes and only admissibly addressed tapes.

We construct X by taking for its global condition the cross product of the global conditions of X_p and of X_q (and all possible symbols in the data channel), but it is not immediately possible to do the same for the local conditions, which have different dimensions. So the local condition for X_p must first be extended to be of dimension q (recall that $p < q$) by including all strings of length q whose first p and last p symbols are in the local condition for X_p . It is evident that X is as required.

We'll say that the tape cell with coordinate n is of *type* $\langle i, j \rangle$ ($i, j \geq 0$) just in case n has p -order i and q -order j .

Suppose D is the set of dominoes, $d_0 \in D$ is the domino that must be placed at the origin, and $H, V \subseteq D \times D$ are the sets of pairs of dominoes that may abut horizontally and vertically, respectively. Let $X = \langle \Sigma, A, B, L \rangle$ be an LSS that accepts all perfectly addressed tapes and only admissibly addressed tapes with members of D in the data track. The dimension of A is q . The required system X' will be $\langle \Sigma, A', B', L \rangle$, where $A' \subseteq A$ and $B' \subseteq B$. From the discussion following the proof of Lemma 1 we can find a mapping μ from A to $\{\{0, 1\} \times \{0, 1\}\}^q$ that identifies whether the cells of a sample of a perfectly addressed tape have type $\langle 0, 0 \rangle$: If π is perfectly addressed tape, then component j of $\mu(\langle \pi(n), \dots, \pi(n+q-1) \rangle)$ is $\langle 0, 0 \rangle$ just in case $n+j$ is of type $\langle 0, 0 \rangle$. Then A' is formed from A by removing any member of A mapped to a bit vector for which some component j equal to $\langle 0, 0 \rangle$ but d_0 is not component j of the data channel. That is, if $\mathbf{g} \in A$ and $\mu(\mathbf{g}) = \langle x_0, \dots, x_{q-1} \rangle$, then $\mathbf{g}$ is excluded from A' unless component j the data track of $\mathbf{g}$ contains d_0 whenever $x_j = \langle 0, 0 \rangle$. The effect will be that in any perfect tape accepted by X' , cells of type $\langle 0, 0 \rangle$ will all have d_0 in the data track.

In the same way, B' is formed by omitting certain quadruples from B . First we need to ensure that in an accepted perfectly addressed tape, all cells of the same type have the same domino in the data track. This is achieved by omitting from B' any flat quadruple in B in which the contents of the data track of the four components are not all the same.

Next we use incremental samples from the global condition to impose the adjacency constraints of the domino system. Omit any quadruple that is incremental in its first components and flat in its second components unless the data track of third and fourth components form a pair in H , and also omit any quadruple that is incremental in its second components and flat in its first components unless the data track of the third and fourth components form a pair in V .

We claim first that if there is a tiling of the first quadrant satisfying the domino constraints, then a tape is accepted by X' , namely any of the perfectly addressed tapes in which the domino at position $\langle i, j \rangle$ is in the third track of all cells of type $\langle i, j \rangle$. The proof is straightforward.

The converse requires more work. Suppose that X' accepts a tape τ . That tape must be admissibly addressed, so some perfectly addressed tape π is also accepted

by X' , with the further property that every central segment of π is a segment of τ . We first show that all cells of π of the same type must contain the same domino in the data track. It will suffice to show a more restricted result:

Lemma 3. *If m and n are of the same type, $\lambda_p(m) \not\equiv \lambda_p(n) \pmod{p}$, and $\lambda_q(m) \not\equiv \lambda_q(n) \pmod{q}$, then the data tracks of $\pi(m)$ and $\pi(n)$ contain the same domino.*

Given this Lemma, cells of the same type that fail the second or third premise of the lemma can be compared to any cell that satisfies all three premises (given that $p, q > 2$), so all cells of the same type will contain the same domino.

Proof. Suppose n and m are of the same type but are not equal and that $\lambda_p(m) \not\equiv \lambda_p(n) \pmod{p}$ and $\lambda_q(m) \not\equiv \lambda_q(n) \pmod{q}$. We will show that there exist N and M so that $N - M = n - m$ and both address channels of the global sample $\langle \lambda(M), \lambda(N), \lambda(m), \lambda(n) \rangle$ are flat. It will follow from Sublemma 1 that n and m (as well as N and M) have the same type.

We need to choose M and N so that $M - N = m - n$ and the flatness conditions for p and q are satisfied:

1. $\lambda_p(N) - \lambda_p(M) \equiv \lambda_p(n) - \lambda_p(m) \not\equiv 0 \pmod{p}$
2. $\lambda_p(m) - \lambda_p(M) \not\equiv 0 \pmod{p}$
3. $\lambda_p(M) + \lambda_p(n) \not\equiv 0 \pmod{p}$
4. $\lambda_q(N) - \lambda_q(M) \equiv \lambda_q(n) - \lambda_q(m) \not\equiv 0 \pmod{q}$
5. $\lambda_q(m) - \lambda_q(M) \not\equiv 0 \pmod{q}$
6. $\lambda_q(M) + \lambda_q(n) \not\equiv 0 \pmod{q}$

Since m and n are stipulated and $N = M - m + n$, we need to choose a value for M that will result in all of (1)–(6) being satisfied. Choose M so that $1 \leq M \leq p-1$ and conditions (2), (3), (5), and (6) are met; each of these 6 conditions rules out one possible value for M in this range. We also require that

$$\begin{aligned}\lambda_p(M) &\equiv \lambda_p(m) - \lambda_p(n) + \lambda_p(M + n - m) \pmod{p} \\ \lambda_q(M) &\equiv \lambda_q(m) - \lambda_q(n) + \lambda_q(M + n - m) \pmod{q}\end{aligned}$$

which will be true unless $M + n - m \equiv 0 \pmod{p}$ or $M + n - m \equiv 0 \pmod{q}$, ruling out two more possible values for M . With 8 of the $p-1$ values ruled out, we can choose M to satisfy all conditions provided that $p > 9$, concluding the proof of Lemma 3. $\square$

It remains only to show that the horizontal and vertical adjacency conditions are satisfied. Since all cells of the same type contain the same domino, it suffices to find *any* m of type $\langle i, j \rangle$ and n of type $\langle i + 1, j \rangle$ (checking vertical adjacencies is analogous), and M and N such that $N - M = n - m$ and the global sample $\langle \pi(M), \pi(N), \pi(m), \pi(n) \rangle$ is incremental on the first track and flat on the second. So we want all of the following to hold ((1)–(6) are the conditions for incrementality on the first track and (9)–(11) are the conditions for flatness on the second).

1. $\lambda_p(M) + \lambda_p(n) \not\equiv 0 \pmod{p}$
2. $\lambda_p(M) - \lambda_p(n) \not\equiv 0 \pmod{p}$
3. $\lambda_p(N) + \lambda_p(n) \not\equiv 0 \pmod{p}$
4. $\lambda_p(N) - \lambda_p(n) \not\equiv 0 \pmod{p}$
5. $\lambda_p(m) + \lambda_p(n) \not\equiv 0 \pmod{p}$
6. $\lambda_p(m) - \lambda_p(n) \not\equiv 0 \pmod{p}$
7. $\lambda_p(M) - \lambda_p(N) - \lambda_p(m) \equiv 0 \pmod{p}$
8. $\lambda_p(M) - \lambda_p(N) - \lambda_p(m) \not\equiv 0 \pmod{p^2}$
9. $\lambda_q(N) - \lambda_q(M) \equiv \lambda_q(n) - \lambda_q(m) \not\equiv 0 \pmod{q}$
10. $\lambda_q(m) - \lambda_q(M) \not\equiv 0 \pmod{q}$
11. $\lambda_q(M) + \lambda_q(n) \not\equiv 0 \pmod{q}$

We have assumed already that $p > 7$ and that $q > p$. To complete the argument it will be convenient to set $q = p + 1$, so, for example, 8 and 9 would be suitable values for p and q .

To find values for m , n , M , and N , we will use parameters k and ℓ in the range $\{2, \dots, p - 2\}$ in such a way that conditions (1)–(11) are satisfied.

	m	n	M	N
Value	$p^i q^j$	$kp^{i+1} q^j$	$(p - \ell)p^i q^j$	$((k + 1)p - \ell - 1)p^i q^j$
ω_p	i	$i + 1$	i	i
$\lambda_p \pmod{p^2}$	q^j	kq^j	$(p - \ell)q^j$	$((k + 1)p - \ell - 1)q^j$
ω_q	j	j	j	j
$\lambda_q \pmod{q^2}$	p^i	kp^{i+1}	$(p - \ell)p^i$	$((k + 1)p - \ell - 1)p^i$

First note that $N - M = n - m$ as required, and that $p - \ell$ and $(k + 1)p - \ell - 1$ are both incongruent to 0 (mod p) because $2 \leq \ell \leq p - 2$. Also $\omega_p(n) = i + 1$ because $2 \leq k \leq p - 2$, and similarly $\omega_p(M) = \omega_p(N) = i$. The q -order of m, n, M , and N are equal to j because q is relatively prime to p and the coefficients $k, p - \ell$ and $(k + 1)p - \ell - 1$ are all incongruent to 0 (mod q).

Accordingly the λ_p and λ_q rows show in the column headed by variable x the quantity whose remainder (mod p^2 or q^2) is $\lambda(x)$.

We next enumerate the additional conditions on k and ℓ because of (1)–(11).

1. $\lambda_p(M) + \lambda_p(n) \equiv (p - \ell)q^j + kq^j \equiv (p + k - \ell)q^j \not\equiv 0 \pmod{p}$ provided that $k - \ell \not\equiv 0$ (since $2 \leq k, \ell \leq p - 2$).
2. $\lambda_p(M) - \lambda_p(n) \equiv (p - \ell)q^j - kq^j \equiv (p - k - \ell)q^j \not\equiv 0 \pmod{p}$ provided that $k + \ell \not\equiv p$.
3. $\lambda_p(N) + \lambda_p(n) \equiv ((k + 1)p - \ell - 1)q^j + kq^j \equiv ((k + 1)p + k - \ell - 1)q^j \not\equiv 0 \pmod{p}$ provided that $k - \ell - 1 \not\equiv 0$.
4. $\lambda_p(N) - \lambda_p(n) \equiv ((k + 1)p - \ell - 1)q^j - kq^j \equiv ((k + 1)p - k - \ell - 1)q^j \not\equiv 0 \pmod{p}$ provided that $k + \ell + 1 \not\equiv p$.
5. $\lambda_p(m) + \lambda_p(n) \equiv q^j + kq^j \equiv (k + 1)q^j \not\equiv 0 \pmod{p}$ since $k \leq p - 2$.
6. $\lambda_p(m) - \lambda_p(n) \equiv q^j - kq^j \equiv (1 - k)q^j \not\equiv 0 \pmod{p}$ since $k \geq 2$.
- 7.

$$\begin{aligned} \lambda_p(M) - \lambda_p(N) - \lambda_p(m) &\equiv (p - \ell)q^j - ((k + 1)p - \ell - 1)q^j - q^j \\ &\equiv (p - \ell - kp - p + \ell + 1 - 1)q^j \\ &\equiv -kp \equiv 0 \pmod{p}. \end{aligned}$$

8. The same calculation implies that $\lambda_p(M) - \lambda_p(N) - \lambda_p(m) \not\equiv 0 \pmod{p^2}$ since $2 \leq k \leq p - 2$.

9.

$$\begin{aligned} \lambda_q(N) - \lambda_q(M) &\equiv ((k + 1)p - \ell - 1)p^i - (p - \ell)p^i \\ &\equiv kp^{i+1} - p^i \\ &\equiv \lambda_q(n) - \lambda_q(m) \\ &\not\equiv 0 \pmod{q} \text{ since } q \text{ is relatively prime to } p. \end{aligned}$$

10. $\lambda_q(m) - \lambda_q(M) \equiv p^i - (p - \ell)p^i \equiv (\ell - p + 1)p^i \not\equiv 0 \pmod{q}$ provided that $\ell + 1 \not\equiv p \pmod{q}$. But $2 \leq \ell \leq p - 2 < q - 2$, so $3 \leq \ell + 1 \leq p - 1 < q - 1$, from which it follows that $\ell + 1 \not\equiv p \pmod{q}$.

11. $\lambda_q(M) + \lambda_q(n) \equiv (p - \ell)p^i + kp^{i+1} \equiv ((k + 1)p - \ell)p^i \not\equiv 0 \pmod{q}$, provided that $\ell \not\equiv p \pmod{q}$, which is guaranteed since $2 \leq \ell \leq p - 2 < q - 2$.

There are $(p - 3)^2$ possible pairs $\langle k, \ell \rangle$ such that $2 \leq k, \ell \leq p - 2$. Of these, $p - 3$ are ruled out by the requirement that $k - \ell \neq 0$; fewer than $p - 3$ by the requirement that $k + \ell \neq p$; fewer than $p - 3$ by the requirement that $k - \ell - 1 \neq 0$; and fewer than $p - 3$ by the requirement that $k + \ell + 1 \neq p$. So at least $(p - 3) \times (p - 7)$ possibilities remain, which is > 0 provided that $p \geq 8$. This completes the proof of the Main Theorem. $\square$

Readers who wish to experiment could try these values, which satisfy all constraints: $p = 10, q = 11, k = 4, \ell = 2$.

6 Other linear forms

At the beginning of this exposition, we narrowed our focus to the linear equation $n_2 - n_1 = n_4 - n_3$. In Aanderaa and Lewis [1974] we showed that the linear sampling problem is also undecidable for the equation $n_2 - n_1 = n_3$. A too-casual remark on page 521 of that paper states that linear sampling systems have a solvable decision problem if the linear equation has only two variables. I am today unable either to support or to refute that claim. I have no doubt that were Stål here to help, he would see that question right through to its resolution.

References

- Stål O. Aanderaa and Harry R. Lewis. Linear sampling and $\forall\exists\forall$ case of decision problem. *The Journal of Symbolic Logic*, 39(3):519–548, 1974. ISSN 0022-4812.
- Paul Bernays and Moses Schönfinkel. Zum entscheidungsproblem der mathematischen logik. *Mathematische Annalen*, 99:342–272, 1928.
- Alonzo Church. An unsolvable problem of elementary number theory. *American Journal of Mathematics*, 58(2):345–363, 1936. ISSN 00029327.
- David Hilbert and Wilhelm Ackermann. *Grundzüge der theoretischen Logik / [von] D. Hilbert und W. Ackermann*. J. Springer, 1928, Germany, 1928.
- A. S. Kahr, Edward F. Moore, and Hao Wang. Entscheidungsproblem reduced to the $\forall\exists\forall$ case. *Proceedings of the National Academy of Sciences*, 48:365–377, 1962.

Frank P. Ramsey. On a problem of formal logic. *Proceedings of the London Mathematical Society*, s2-30:264–286, 1930.

Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1): 230–265, 1936. URL <http://doi.org/10.1112/plms/s2-42.1.230>.

Hao Wang. Proving theorems by pattern recognition II. *Bell Systems Technical Journal*, 40:1–141, 1961.