Common notation

We will use set notation throughout power round. Here is a guide to set notation. The format used is:

(math symbol): (meaning in words)

Sets

- $\varnothing$: empty set
- $a \in A$: a is an element of A
- $|A|$: the size of A
  Example. If $A = \{1, 2, 3\}$, then $|A| = 3$.
- $A \subseteq B$: A is a subset of B (i.e. all elements of A are elements of B)
  Example. $\{1, 2\} \subseteq \{1, 2\}$, $\varnothing \subseteq \{1, 2\}$ but $\{1, 2\} \not\subseteq \{1, 3\}$.
- $A \subset B$: A is a proper subset of B (i.e. $A \subseteq B$ and $A \neq B$)
  Example. $\{1, 2\} \subset \{1, 2, 3\}$, but $\{1, 2\} \not\subset \{1, 2\}$.
- $A \cap B$: the intersection of sets A and B
  Example. $\{1, 2\} \cap \{2, 3\} = \{2\}$.
- $A \cup B$: the union of sets A and B
  Example. $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$.
- $A \setminus B$: the set of elements in A but not in B
  Example. $\{1, 2\} \setminus \{2, 3\} = \{1\}$
- $\mathbb{N}$: the set of natural numbers (i.e. $\{1, 2, 3, ...\}$)
- $\mathbb{Z}$: the set of integers
- $\mathbb{Z}_{\geq 0}$: the set of non-negative integers
- $\mathbb{Q}$: the set of rational numbers
- $\mathbb{R}$: the set of real numbers
- $\mathbb{Z}_m$: the set of integers mod m (further explained in Section 2)

Functions

- $f : X \to Y$: f is a function taking values from set X and outputting values from set Y.
- $f : X \to Y$ is an *injection* if $f(x_1) \neq f(x_2)$ whenever $x_1 \neq x_2$.
- $f : X \to Y$ is a *surjection* if for every $y \in Y$, there exists $x \in X$ such that $f(x) = y$.

1 Part I: Polynomial Sequences

1.1 Introduction

Given a polynomial $Q(x)$ with integer coefficients, let's consider the sequence

$$\{q_i\}_{i\geq 0} = \{0, Q(0), Q(Q(0)), ...\}$$

Unless Q happens to be exceptionally simple, there will be no exact closed-form formula for the n-th term in the sequence. Indeed, such sequences sometimes exhibit chaotic and varied behaviors. For instance, it could grow swiftly towards infinity (e.g. $Q(x) = x + 1$), or even exhibit periodic behaviour (e.g. $Q(x) = (1 - x)^2$).

A strange question to ask might be if your favorite number appears as the trailing (decimal) digits of some term in the sequence. This sounds like a hopeless question to answer (especially if your favorite number is $\lfloor e^{\pi\sqrt{163}}\rfloor$), but here is a miraculous fact:

Fact. If every positive integer from one to a billion appears as the trailing digits of some term of the sequence, then so must every positive integer (regardless of how big it is).

We will prove the most general version of this fact, phrased as the following theorem:

Theorem. Given any natural number n and a polynomial with integer coefficients Q, suppose the sequence

$$\{q_i\}_{i\geq 0} = \{0, Q(0), Q(Q(0)), ...\}$$

has the property that the sequence covers all residue classes mod n^8 (i.e. for any $r \in \mathbb{N}$, there exists an index i where $q_i \equiv r \pmod{n^8}$)[1]. Then, the sequence covers all residue classes mod n^k for any positive integer k (.e. for any $r \in \mathbb{N}$, there is some i such that $q_i \equiv r \pmod{n^k}$).

Linear functions

To understand this problem better, we will spend some time trying to understand the problem for linear functions $Q(x) = Ax + B$.

We'll start off with the familiar setting of base $n = 10$.

1. [**1**] Find a choice of linear function $Q(x) = Ax + B$ for which the sequence covers all residue classes mod 10^k for any positive integer k.

   Note: you are not allowed to use the statement of the theorem above or later problems to answer this problem.

   Solution to Problem 1: $Q(x) = x+1$ works, since the sequence lists all natural numbers.

2. (a) [**2**] Give a general closed-form formula for q_n if $Q(x) = Ax + B$ (where $A, B \in \mathbb{N}$).

   (b) [**1**] Show that for integers $j > i \geq 0$, $q_j - q_i = A^i q_{j-i}$.

   Solution to Problem 2:

[1] 8 can in fact be replaced by a smaller number, but is chosen on purpose so as to reduce the amount of technical details required.

(a) If $A = 1$, then clearly $q_n = Bn$. Otherwise, $q_n = \frac{(A^n-1)B}{A-1}$. This can be shown by induction: clearly this holds for $n = 1$. Then

$$\frac{A(A^n-1)B}{A-1} + B = \frac{A^{n+1}B - AB + AB - B}{A-1} = \frac{(A^{n+1}-1)B}{A-1}$$

Hence by induction, we have the closed formula above.

(b) We plug in the formula from (a):

$$q_j - q_i = \frac{B}{A-1}\left(A^j - A^i\right) = \frac{BA^i}{A-1}\left(A^{j-i} - 1\right) = A^i q_{j-1}$$

3. (a) **[4]** Show that unless $A \equiv 1 \pmod{10}$, the sequence $\{q_i\}$ does not cover all residue classes mod 10.

(b) **[2]** Show that for $A = 11$, the sequence $\{q_i\}$ does not cover all residue classes mod 100.

Hint: powers of 11 mod 100 goes 1, 11, 21, 31, ...

Solution to Problem 3:

(a) This can be essentially done by a case bash, but the following points can shorten it:

- We can reduce to the case $B = 1$. The sequence is then $q_n = 1 + A + ... + A^{n-1}$
- Clearly if A and 10 have a common factor $d > 1$, then $q_n \equiv 1 \pmod{d}$ and we cannot cover all residues.
- For the remaining cases, note firstly that $q_j - q_i = A^i q_{i-j}$ (for $j > i$).

  If $A \not\equiv 1 \pmod{10}$, we have $20 \mid A^4 - 1$ but $(10, A-1) = 2$, so $10 \mid \frac{(A^4-1)/2}{(A-1)/2} = q_4$, hence the residue mod 10 has period 4 and cannnot possibly cover all residues.

(b) Check inductively that $11^k \equiv 10k+1 \pmod{100}$ so $q_k = 1+...+A^{k-1} \equiv 10 + \frac{10(10-1)}{2} \equiv 1 \pmod{20}$.

This tells us that the first interesting case happens when $A = 21$.

4. Suppose that $Q(x) = 21x + 1$.

(a) **[4]** Complete the following table for $q_{10a+b} \pmod{10^2}$:

		a									
		1	2	3	4	5	6	7	8	9	10
b	1	01	11	21	31	41	51	61	71		
	2	22	32	42	52	62	72	82	92		
	3	63	73	83	93	03	13	23	33		
	4	24	34	44	54	64	74	84	94		
	5	05	15	25	35	45	55	65	75		
	6	06	16	26	36	46	56	66	76		
	7	27	37	47	57	67	77	87	97		
	8	68	78	88	98	08	18	28	38		
	9	29	39	49	59	69	79	89	99		
	10	10	20	30	40	50	60	70	80		

(b) **[1]** Show that $\{q_i\}$ covers all residue classes mod 10.

(c) **[3]** Find a polynomial f such that $q_n \equiv 10f(n) + n \pmod{100}$, and justify why it works.

(d) **[2]** Show that $\{q_i\}$ covers all residue classes mod 10^2.

(e) **[4]** Show that $\{q_i\}$ covers all residue classes mod 10^k for all positive integers k.

Hint: Consider $q_{10^k}/q_{10^{k-1}}$.

Solution to Problem 4:

(a) When you move right you +10.

(b) Because $Q(x) \equiv x + 1 \pmod{10}$.

(c) If you stare really hard you will realize $f(n) = n(n-1)$ fits. The reason comes from the expansion of $(1 + 20)^n$:

$$(1+20)^n = 1 + \binom{n}{1}20 + \binom{n}{2}20^2 + 20^3(...)$$

so $\frac{21^n-1}{20} \equiv n + \binom{n}{2} \cdot 20 \pmod{100}$.

Comments. You can also show this inductively, or make use of the fact that $q_n - q_{n-1} \equiv A^n \equiv n(A-1) + 1$.

(d) From the above, we have that $q_{n+10} - q_n \equiv 10 \pmod{100}$ (since $10 \mid f(n+10) - f(n)$.

(e) $k = 1, 2$ are implied by the previous parts.

It is sufficient to show that for $k \geq 3$ $q_{n+10^k} - q_n \equiv 10^k \pmod{10^{k+1}}$. We will prove this inductively.

Indeed, $q_{n+10^k} - q_n = A^n q_{10^k}$, so because $A \equiv 1 \pmod{10}$ the above statement is equivalent to $q_{10^k} \equiv 10^k \pmod{10^{k+1}}$.

To complete the induction, it is sufficient to show that $q_{10^{k+1}}/q_{10^k} \equiv 10 \pmod 1)00$ for $k \geq 2$. Using the formula:

$$\begin{aligned} q_{10^{k+1}}/q_{10^k} &= \frac{A^{10^{k+1}} - 1}{A^{10^k} - 1} \\ &= 1 + A^{10^k} + ... + (A^{10^k})^9 \\ &\equiv 10 \pmod{100} \end{aligned}$$

where in the last line we used that $100 \mid (10q_k) \mid A^{10^k} - 1$.

The last problem should provide an inkling of how the proof might go in general (for any linear function Q). Surprisingly, the proof for general Q proceeds rather similarly, so we will dive right into it.

1.2 The main proof

We will temporarily make the following assumptions:

- $n = p$ for some p prime
- the sequence $\{q_i\}$ contains all residues $\pmod{p^k}$ for some $k \geq 8$.

- no further assumptions on Q (in particular, it might not be linear).

We start off with some generic facts about the sequence:

5. (a) [**1**] Prove that $\{q_i\}$ is eventually periodic modulo p^{k+1} (i.e. for some fixed N and t, for all $n \geq N$ we have $q_{n+t} \equiv q_n \pmod{p^{k+1}}$).

   (b) [**1**] Prove that $\{q_i\}$ is periodic modulo p^j for $1 \leq j \leq k-1$ (i.e. for some fixed t, we have $q_{n+t} \equiv q_n \pmod{p^j}$ for all $n \geq 0$).

   (c) [**2**] Show that the minimal period of $\{q_i\}$ modulo p^j is p^j for $1 \leq j \leq k$.

   In other words, if $q_{n+t} \equiv q_t \pmod{p^j}$ for all $n \geq 0$, then $t \geq p^j$ and that the congruence holds for $t = p^j$.

   Solution to Problem 5:

   (a) By pigeonhole, exists $q_i \equiv q_j \pmod{p^{k+1}}$ for some $i < j$. Then, $q_{i+t} \equiv q_{j+t} \pmod{q^{k+1}}$ for all t.

   (b) Note $q_i \equiv 0 \pmod{p^j}$ at least p times. Let t be smallest positive integer such that $q_t \equiv 0 \pmod{p^j}$, then $q_{t+n} \equiv q_n \pmod{p^j}$ for all n.

   (c) Let t be a period of $\{q_i\} \pmod{p^j}$. If $t < p^j$ it won't cover all residues. Clearly by pigeonhole, there is two equal elements among $\{q_0, \cdots, q_{p^j}\}$, so the eventual period (which matches the actual period) is exactly p^j.

In the linear case, we spent a lot of effort wrangling with the largest power of 10 that divided q_n. Here we introduce some notation to streamline this:

Definition. The **p-adic valuation** of an integer is the function $v_p(n) : \mathbb{Z} \to \mathbb{N}$ that describes the exponent of the largest power of p that divides it:

$$v_p(n) = \begin{cases} \max\{v \in \mathbb{N} : p^v \mid n\} & \text{if } n \neq 0 \\ \infty & \text{if } n = 0 \end{cases}$$

6. Here is a quick warmup on valuations:

   (a) [**1**] For each prime p dividing 2020, state the value of $v_p(2020)$.

   (b) [**1**] List the first 20 terms of the sequence $\{v_2(n)\}_{n \geq 1}$.

   Solution to Problem 6:

   (a) *Answer.* $v_2(2020) = 2, v_5(2020) = 1, v_{101}(2020) = 1$.

   (b) *Answer.* $0, 1, 0, 2, 0, 1, 0, 3, 0, 1, 0, 2, 0, 1, 0, 4, 0, 1, 0, 2$.

7. [**3**] Show that if $v_p(n) \leq k-1$, then $v_p(q_n) = v_p(n)$.

   Solution to Problem 7: The problem about minimal period means that for $1 \leq j \leq k$, $p^j \mid q_n$ iff $p^j \mid n$.

8. In this problem we recreate a "formula" for q_n (modulo some power of p).

(a) **[2]** Given any polynomial $P(x) \in \mathbb{Z}[x]$, show that there exists $R(x) \in \mathbb{Z}[x]$ such that for all integers x, z, and positive integer n,

$$P(x + zp^n) \equiv P(x) + zp^n R(x) \pmod{p^{2n}}$$

(b) **[4]** Show that exists an integer $\alpha \neq 1$ such that for all positive integers n and $k \geq 6$,

$$q_{np^{k-2}} \equiv q_{p^{k-2}} + \alpha q_{(n-1)p^{k-2}} \pmod{p^{k+2}}$$

(c) **[2]** Hence, show that

$$q_{np^{k-2}} \equiv \frac{\alpha^n - 1}{\alpha - 1} q_{p^{k-2}} \pmod{p^{k+2}}$$

Solution to Problem 8:

(a) Let $P(x) = \sum_i a_i x^i$. Then, expanding, $P(x + zp^n) \equiv \sum_i a_i (x + zp^n)^i \equiv \sum_i a_i (x^i + zp^n i x^{i-1}) \pmod{p^{2n}}$ So $R(x) = \sum_i a_i i x^{i-1}$ works.

Comment. One can think of this as the "Taylor expansion" with $\varepsilon = zp^n$, so $R(x)$ is in fact $P'(x)$.

(b) First note that $p^{k-2} \mid q_{p^{k-2}}$. Take $P(x) = Q^{p^{k-2}}(x)$, and the corresponding R from the previous part. Then $q_{np^k} = P(0 + q_{(n-1)p^k}) \equiv q_{p^{k-2}} + R(0) q_{(n-1)p^{k-2}} \pmod{p^{2k-4}}$ by letting $zp^{k-2} = q_{(n-1)p^{k-2}}$. Since $2k - 4 \geq k + 2$ we are done.

Of course, one of $R(0), R(0) + p^{k+2}$ will not be 1, so let α be that one.

(c) Inductively apply the previous part.

Because we don't have a closed-form general formula for q_n, we have to be more careful with our control over the exponents (i.e. the values of $v_p(q_n)$). The following theorem will allow us to do that (which you can subsequently use without proof):

Theorem. (Lifting the Exponent Lemma) If n is a positive integer and p is a prime, then

- for $p \neq 2$ and $p | x - 1$, then $v_p(x^n - 1) = v_p(n) + v_p(x - 1)$.
- for $p = 2$ and $4 | x - 1$, then $v_2(x^n - 1) = v_2(n) + v_2(x - 1)$.

This lemma tells us how to figure out the largest prime power that divides a number of the form $a^b - 1$.

9. (a) Find the largest power of 5 that divides the following numbers and justify your answers: (i) **[1]** $101^{100} - 1$ and (ii) **[1]** $99^{100} - 1$.

(b) **[5]** Show that if $v_p(n) \leq k + 1$, then $v_p(q_n) = v_p(n)$. (Compare this to problem 7.)

(c) **[1]** Prove that $\{q_i\} \pmod{p^{k+1}}$ has minimal period p^{k+1}.

Solution to Problem 9:

(a) The answer to both is 5^4. For the latter, $99^{100} - 1 = 9801^{50} - 1$.

(b) $v_p(q_{p^{k-2}}) = k - 2$ and $v_p(q_{p^{k-1}}) = k - 1$, so from problem 8b for $n = p$ we get that $v_p\left(\frac{\alpha^p - 1}{\alpha - 1}\right) = 1$.

If we can show that $v_p\left(\frac{\alpha^{mp}-1}{\alpha-1}\right) = 1 + v_p(m)$, then $v_p(q_{mp^{k-1}}) = (k-1) + v_p(m)$ as long as $v_p(m) \leq 2$, as desired.

(c) By the above, the smallest index n for which $q_n \equiv 0 \pmod{p^{k+1}}$ is $n = p^{k+1}$, so by earlier arguments this follows.

We can thus conclude that the sequence contains all residues modulo p^{k+1}. By induction, the sequence contains all residues modulo p^m where $m \geq 8$.

With just a little more work, we can generalize this for general composite n:

10. **[4]** Given a natural number n and $k \geq 8$, if $\{q_i\}$ contains all residues modulo n^k, then the sequence contains all residues modulo n^l for all positive integers l.

Solution to Problem 10: Fix any $r \in \mathbb{N}$. We want to show that there exists some m such that $q_m \equiv r \pmod{n^\ell}$.

Consider the prime factorization $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j}$. By assumption, the sequence contains all residues mod $p_i^{k\beta_i}$, so by the previous problem the sequence mod $p_j^{\ell\beta_j}$ has minimal period $p_j^{\ell\beta_j}$. Hence, there exists m_j such that any $m \equiv m_j \pmod{p_j^{\ell\beta_j}}$ satisfies $q_m \equiv r \pmod{p_j^{\ell\beta_j}}$.

By the Chinese remainder theorem, there exists a single m for which $m \equiv m_j \pmod{p_j^{\ell\beta_j}}$, so $q_m \equiv r \pmod{p_j^{\ell\beta_j}}$. Since $\{p_j^{\ell\beta_j}\}$ are coprime across j, it follows that $q_m \equiv r \pmod{n^\ell}$.

2 Part II: van der Waerden's theorem

2.1 Introduction

"Complete disorder is impossible." - T. Motzkin

In this section, we will prove van der Waerden's theorem:

Theorem. (van der Waerden) Let $\mathbb{N} = C_1 \cup C_2 \cup ... \cup C_r$ be a finite partition of the natural numbers (i.e. C_i and C_j are disjoint subsets of $\mathbb{N}$ for any $i \neq j$). Then some $C_j, j \in \{1, ..., r\}$ contains arbitrarily long[2] arithmetic progressions[3].

Here are some reasons why this might be surprising:

11. (a) **[1]** In the "finite partition" interpretation, perhaps you might figure out that one of the sets C_i are infinite. However, this is not a good reason why it might contain long arithmetic progressions.

In particular, construct an infinite subset $S \subset \mathbb{N}$ such that S does not contain any length 3 arithmetic progression.

(b) **[10]** Partitions can conspire (somewhat effectively) to avoid arithmetic progressions.

Suppose $r = 100$, $k = 101$. Show that $\{1, 2, ..., 10^{100}\}$ can be partitioned into r disjoint subsets, each of which does not contain a length k arithmetic progression.

(Partial credit if you manage to partition $\{1, 2, ..., N\}$ for $N \geq 10^5$ or $N \geq 10^{10}$.)

[2] for all $n_0 \in \mathbb{N}$, C_j contains an arithmetic progression of length $n \geq n_0$.

[3] by convention, arithmetic progressions must have a positive common difference. In particular, constant sequences are not arithmetic progressions.

Solution to Problem 11:

(a) $1, 2, 2^2, ...$ works.

(b) (2 pts) $N \geq 10^5$: Let

$$C_i = \{a + i \cdot 10^2 + b \cdot 10^4 \mid a, b \in \{1, 2, ..., 100\}\}$$

(7 pts) $N \geq 10^{10}$: Let

$$C_i = \left\{ \sum_{j=0}^{5} (100b_j + a_j)(200)^i \mid a_j = \{1, 2, ..., 100\}, (\overline{b_5 b_4 ... b_0})_2 = i - 1 \right\}$$

and in fact we'll just use 64 out of the 100 sets. Each set alternates between "gaps" of size $100 \cdot 200^i$ and a self-similar region of size $100 \cdot 200^i$. However, there are only 9 such gaps (in some region), so if you cross one such gap you have to cross 10 gaps of this size, a contradiction.

(10 pts) $N \geq 10^{100}$: We use a non-constructive method. There are 100^N partitions, and there are at most N^2 arithmetic progressions (N choices for first index, N choices for common differences), so there are at most $100^{N-100} \cdot N^2$ partitions that contain some arithmetic progression. In fact, this is strict because some partitions contain more than one arithmetic progression. This gives that $N = 100^{50}$ works.

We can interpret this as a statement about letters and words. Here an **infinite word** on three **letters** $\{a, b, c\}$ (also called a **ternary** word) is:

$$W = abcb\ abcb\ abcb\ abcb\ ...$$

where the pattern repeats (and the spaces are purely decorative). We might say that:

- *abcb* is a **finite word** of length 4 that appears in W (and synonymously *abcb* is a **subword** of W).
- The letter a **appears at indices** $0, 4, 8, 12$ and so on, and we will also say that the word *abcba* appears at index 4 because its first letter appears at index 4.
- The word *abcba* is also a **prefix** (of W) since it also appears at index 0.
- The letter a appears (in W) at 4 indices which form an arithmetic progression.

In the language of words and letters, we can phrase van der Waerden's theorem as follows:

Theorem. (van der Waerden, letters on words) Let W be an infinite word with r distinct letters. Then, for any k, there exists some letter that appears at k indices which form an arithmetic progression.

Generalizing from letters to words

Note: this subsection was missing from the contest version.

You might be tempted to attempt a proof by induction on the length of the arithmetic progression k, but the statement of the theorem for $k = m$ is much, much weaker than the statement for

$k = m+1$. We must somehow do a *double induction* on r, k, but this is tricky because having more (or less) letters creates an incompatibility that is hard to resolve.

Can we retain the full general power of the theorem while fixing the number of letters? A suggestion could be to consider the point of view of a robot, which fundamentally understands only two letters.

12. Fix $k \in \mathbb{N}$ and consider the following two statements:

    - For any natural r, given an infinite word W on r-distinct letters, there exists some **letter** that appears at k indices which form an arithmetic progression.
    - For any natural m, given an infinite **binary** word W, there exists some **word of length** m that appears at k indices which form an arithmetic progression.

    (a) **[1]** Show that the former implies the latter.

    (b) **[3]** Show that the latter implies the former.

    Solution to Problem 12:

    (a) Treat each possible m-letter block of (binary) letters as an individual letter. Then this follows from the first statement for $r = 2^m$.

    (b) We simulate the r-distinct letters using binary: let

    $$w_i = \underbrace{11...1}_{i\ 1\text{'s}} \ \underbrace{00...0}_{(m+1-i)\ 1\text{'s}} \qquad \text{for } i = 1, 2, ..., m$$

    then encode the i-th letter using w_i Using the second statement for $m = (r+1)(k+1)$, we get matching words of length $(r+1)(k+1)$ lying in an arithmetric progression. However, these can be uniquely decoded into the original r-letters (possibly including a suffix and a prefix, since an r-letter ends whenever we have the word '01').

This shows that the latter is equivalent to the original van der Waerden's theorem. As we shall see, this turns out to be the right generalization to consider (though we will replace binary with r-ary so that we have clearer examples).

Theorem. (van der Waerden, varying length) Let W be an infinite word with r distinct letters. Then, for any k, m, there exists k instances of the same length m word such that their respective indices form an arithmetic progression.

For subsequent problems in the rest of this section, assume that all (finite or infinite) words are on an alphabet of size r.

2.2 Reducing to easier cases

Consider the following infinite word:

$$W = c\ ab\ c\ ab\ c\ aaabbbababbaaab...$$

where W continues with just the letters a and b (but with no obvious pattern).

If we want to find k of the same letter (in W) appearing at indices that form an arithmetic progression, it appears that we require van der Waerden's theorem for infinite word on $r = 3$ letters. But here's a trick: consider

$$T^7(W) = aaabbbababbaaab...$$

where $T^7(W)$ is W but with the first seven letters **truncated**. This is now an infinite word on $r = 2$ letters, which is an easier case of the problem!

Now suppose that maybe we do manage to find k of the same letter appearing in $T^7(W)$ at indices $a, a+d, ..., a+(k-1)d$. This letter must appear in the original W at indices $a+7, (a+7)+d, ..., (a+7)+(k-1)d$, which is an arithmetic progression.

Here is a definition that captures the essence of the relationship between W and $T^7(W)$:

Definition. Given two infinite words, we say that W' is **included** in W (equivalently, we write $W' \prec W$) if any finite subword of W' appears in W. We will sometimes say that W' is a **reduction** of W.

For example, $T^7(W) \prec W$, and equivalently $T^7(W)$ is a reduction of W.

Informally, this means if $W' \prec W$, then whatever we find in W' will be in W, so the statement of the theorem for W can be reduced to that of W'.

13. (a) **[2]** Show that for every infinite word W, there exists an infinite word $W^* \prec W$ such that any letter that appears in W^* will appear at infinitely many indices.

    (b) **[2]** Show that for every infinite word W and a fixed $m \in \mathbb{N}$, there exists an infinite word $W^* \prec W$ such that any word of up to length m that appears in W will appear at infinitely many indices.

    (c) **[2]** Construct a binary word W such that for any positive integer $\ell \in \mathbb{N}$, there is some finite word w_ℓ that appears in $T^\ell(W)$ finitely many times.

Solution to Problem 13:

(a) Suppose a letter last appears at index m. Then we can just truncate W before index $m+1$. There are only finitely many letters, so we can just do this once for every letter.

(b) Similar to above.

(c) Something like this should work:

$$W = a\ b\ aa\ bb\ aaa\ bbb\ ...$$

Then we have $aa...ab$ only ever appears once.

The conclusion is that we may assume (in the context of the theorem) without loss of generality, every finite word w (up to some fixed length m) either appears infinitely often or not at all in W.

How might we extend this for all (infinitely many) finite words?

2.3 Limits

Here's another example: consider the infinite (ternary) string

$$W = c\ a\ c\ ab\ c\ aba\ c\ abab\ c\ ababa\ c\ ababab\ c...$$

where between every two c's we have a sequence of alternating a's and b's that increase in length.

Despite there being infinitely many c's, we claim that remove them all without losing generality!

14. **[1]** Indeed, show that $W' = ab\ ab\ ab...$ satisfies $W' \prec W$.

    Solution to Problem 14: The length n prefix of W' appears at index $\frac{n(n+1)}{2}$, and every subword of W' appears in some prefix of W', so we conclude that every subword of W' appears in W.

One perspective to understand this is to consider a sequence of truncations:

$$\begin{aligned}
T^1(W) &= a\ c\ ab\ c\ aba\ c\ abab\ c\ ababa\ c\ ababab\ c...\\
T^3(W) &= ab\ c\ aba\ c\ abab\ c\ ababa\ c\ ababab\ c...\\
T^6(W) &= aba\ c\ abab\ c\ ababa\ c\ ababab\ c...\\
T^{10}(W) &= abab\ c\ ababa\ c\ ababab\ c\ abababa\ c...\\
T^{15}(W) &= ababa\ c\ ababab\ c\ abababa\ c...\\
T^{21}(W) &= ababab\ c\ abababa\ c...
\end{aligned}$$

These words appear to **converge** to $W' = ab\ ab\ ab\ ab....$

Definition. A sequence of infinite words $W_1, W_2, ...$ **converges** (to W^*) if for each $j \in \mathbb{N}$, the j-th letter of W_i is eventually constant[4] for large enough i (and equal to the j-th letter of W^*). In the example above, we say that W' converges to W.

Definition. We call X a T**-limit** of W if there exists indices $n_1 \le n_2 \le ...$ where the sequence

$$T^{n_1}(W), T^{n_2}(W), T^{n_3}(W), ...$$

converges to X. In the example above, we would say that W' is a T-limit of W.

15. (a) **[2]** An infinite word can have more than one T-limit! (So we always want to say *a* T-limit rather than *the* T-limit).

    In fact, construct an infinite word X such that any infinite word W is a T-limit of X.

    (b) **[4]** Here we make the connection between T-limits and reductions:

    Show that W^* is a T-limit of W if and only if $W^* \prec W$.

    (c) **[5]** (Closure property) Let $X_1, X_2, ...$ be a sequence of T-limits of W that converge to X^*. Show that X^* is also a T-limit of W.

    Solution to Problem 15:

    (a) Just concatenate all natural numbers in r-ary.

    (b) ($\Rightarrow$): This is clear since every finite subword of W^* lies in a truncation of W, and truncations are reductions.

    ($\Leftarrow$): Note that the length m prefix of W^* is somewhere in W, so it is the prefix of some truncation $T^{k_m}(W)$. Then we simply take an non-decreasing subsequence of $(k_1, k_2, ...)$, and the resulting subsequence of truncations will converge to W^*.

    (c) Suppose $\{Y_i\} \to Y^*$. If $W_{n,k} \to Y_n$, then let $f(n)$ be such that $W_{n,f(n)}$ shares the first n letters of Y^*. Then we easily check that $W_{n,f(n)} \to Y^*$.

[4] i.e. for each j, there exists a positive integer N_j where the j-th letter of W_i are all the same for any $i > N_j$

2.4 Compactness

In general however, the given word will not be as well-behaved. Consider instead the following word:

$$W = c\ a\ c\ ab\ c\ ba\ c\ bba\ c\ ababbb\ c\ baabba\ c\ b\ c\ abababbaa\ c...$$

This time there isn't a clear pattern of which words are between adjacent c's. However, you could imagine that if we were clever about picking the right subsequence, we could still obtain a T-limit of W which might get rid of all the c's (perhaps:

$$T^3(W) = ab...$$
$$T^{13}(W) = abab...$$
$$T^{29}(W) = ababab...$$

and hopefully we can keep going).

Is this always possible? To answer this question, it might be helpful to consider the notion of a **strict limit**, which somewhat generalizes T-limits:

Definition. W is a **strict limit** of the sequence of infinite words $W_1, W_2, W_3, ...$ if there is is an infinite sequence of indices $n_1 < n_2 < n_3 < ...$ such that $W_{n_1}, W_{n_2}, ...$ converges to W.

For example, any T-limit of W will be either a term or strict limit of the sequence $W, T^1(W), T^2(W), ...$

16. Fix a sequence of infinite words $W_1, W_2, ...$ We will show that at least one strict limit exists.

    (a) **[1]** Show that the sequence $\{W_i\}$ has a subsequence $W_1^{(1)}, W_2^{(1)}, ...$ whose first letters are all equal to some letter a_0.

    Note: a subsequence of $\{W_i\}$ *must be of the form* $\{W_{i_1}, W_{i_2}, ...\}$*, where* $i_1 < i_2 < ....$

    (b) **[1]** Show that the sequence $\{W_i\}$ has a subsequence $W_1^{(2)}, W_2^{(2)}, ...$ whose first two letters are (a_0, a_1) for some letter a_1 (and a_0 is the same as above).

    (c) **[3]** Show that every infinite sequence of infinite words has a strict limit.

    Solution to Problem 16:

    (a) Infinite pigeonhole: some letter appears infinitely often as the first letter.

    (b) Infinite pigeonhole again: in $\{W_i^{(1)}\}$, some letter appears infinitely often as the second letter.

    (c) We continue the construction above to get a_n and $\{W_k^{(n)}\}$. But $\{W_k^{(k)}\}$ will converge to $A = (a_0, a_1, ...)$, and the indices are strictly increasing.

17. **[3]** Let us revisit the last thing we wanted to prove in the "Reducing to an easier case" section:

    Show that for every infinite word W, there exists an infinite word $W^* \prec W$ such that every finite word in W^* that appears in W will do so at infinitely many indices.

    Solution to Problem 17:

18. (Finitary van der Waerden) Here is a visible consequence of compactness. Consider the following two versions of van der Waerden's theorem:

- (Original) For every r, k, given an infinite word W formed from r-distinct letters, there are k of the same letters whose indices form an arithmetic progression.
- (Finitary) For every r, k, there exists $N = N(r, k)$ where for any infinite word W with r-letters, some letter appears at k indices forming an arithmetic progressions **within the first N letters of W.**

(a) **[2]** Construct and justify a value of $N(r, 2)$ that satisfies the conditions in the finitary formulation.

(b) **[4]** Show that the latter statement is implied by the former statement above.

(Take note: you should prove that the same N works for any infinite word W.)

Solution to Problem 18:

(a) $N(r, 2) = r + 1$ works by pigeonhole.

(b) Suppose that the finitary version was false, so it is false for any N. Let W_N be the counterexample, then take W^* to be a ω-limit point of $\{W_N\}$. Then W^* does not contain any arithmetic progressions, since any prefix of W^* is contained in some W_N. This contradicts the original vdW.

2.5 Syndeticity

Armed with compactness, we will now show that we can discard any letter (and also any finite word), possibly appearing infinitely often, for which there are increasing gaps between occurences of that letter.

Definition. An increasing sequence of natural numbers $\{n_1 < n_2 < ....\}$ is **syndetic** if it is both infinite and has bounded gaps, i.e. there exists a constant $C > 0$ such that $n_{i+1} - n_i < C$ for all $i \in \mathbb{N}$.

Definition. If W is an infinite words and f is a finite word, we say that f **densely populates** W if the set of indices at which f appears in W is syndetic. Otherwise, we say that f **sparsely populates** W. For example, c sparsely populates W for

$$W = c\ a\ c\ ab\ c\ aba\ c\ abab\ c\ ababa\ c\ ababab\ c...$$

but a, b densely populates it.

19. **[2]** If w sparsely populates W, show that there exists a T-limit W^* of W which does not contain w.

Solution to Problem 19: Write

$$W = w_0\ f\ w_1\ f\ w_2\ f\ ...$$

where each w_i does not contain w. If some w_i is infinite just use that. Otherwise just use a ω-limit point of $\{w_i\}$.

The above construction will prove to be very useful, so we give it a shorthand:

Definition. Write

$$[W]_f = \begin{cases} W^* & \text{a } T\text{-limit of } W \text{ which does not contain } f, \text{ if } f \text{ sparsely populates } W \\ W & \text{otherwise.} \end{cases}$$

20. Enumerate all finite words $\{f_1, f_2, ...\}$, and define a sequence of words as follows:

$$W_i = \begin{cases} W & \text{for } i = 0 \\ [W_{i-1}]_{f_i} & \text{otherwise} \end{cases}$$

   (a) **[3]** Show that f_i does not sparsely populate W_j for all $j \geq i$.

   (b) **[4]** (Minimality condition) Deduce that there exists $W_{min} \prec W$ where no f_i sparsely populates W.

   Solution to Problem 20:

   (a) It suffices to show that for any two words f, f', if f' sparsely populates $[W]_f$ then f' sparsely populates W (then the problem follows immediately from the contrapositive).

   Note that $[W]_f$ contains arbitrarily long words of the form fxf (where x does not contain f), but it is included in W, so W also contains arbitrarily long words of the form fxf.

   (b) First note that inductively, W_i is a T-limit of W.

   Let W_{min} be a limit point of $\{W_i\}$. By closure, this is also a T-limit of W.

   Because $W_{\text{min}} \prec W_i$ for each i, by the same argument in the previous part we get that W_{min} cannot be sparsely populated by f_i.

This means that we can replace W with W_{min} where each of its subwords reappear such that the gap between adjacent occurences is bounded (depending on the subword).

This construction is optimal in the following sense:

21. **[2]** Show that W_{min} has the same set of (finite) subwords as any T-limit of itself. Furthermore, each T-limit satisfies the minimality condition (problem 20b).

   Solution to Problem 21: Let W' be a T-limit of $W = W_{min}$. Then the subwords in W' must appear in W. However, each subword w of W must appear in W' since w appears in any sufficiently long subword of W.

2.6 The main proof

We now have the fundamental ideas to prove van der Waerden's theorem without too much difficulty:

Without loss of generality, we may assume W satisfies the minimality condition (from the previous section). Suppose that for some fixed k and infinite string W, van der Waerden (varying length form) is true for any word length m.

22. Here is a surprising fact: syndeticity allows us to force the position of the arithmetic progression (i.e. we may assume without loss of generality that the arithmetic progression starts at index 0) for any m.

   (a) **[3]** Show that for any finite word w that appears in W will do so at k indices which form an arithmetic progression.

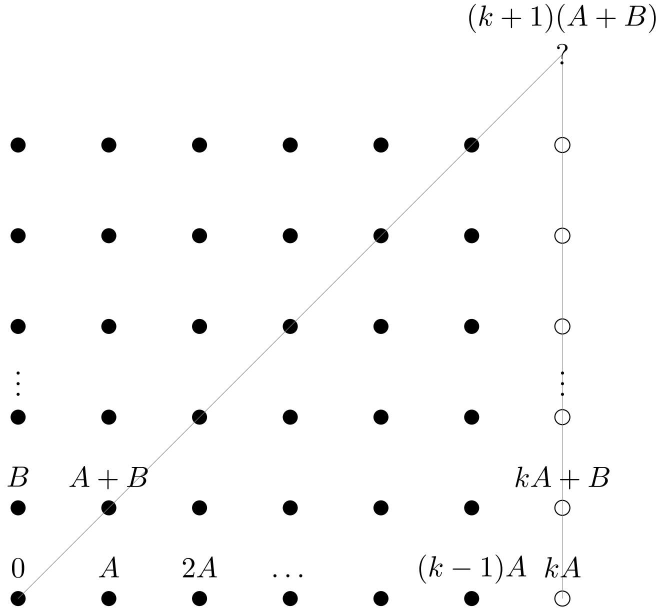
(b) **[3]** Show that there exists an infinite word $W^* \prec W$ such that for any prefix w of W^*, w appears in W^* at k indices forming an arithmetic progression starting with 0.

Solution to Problem 22:

(a) This follows by dense population + picking a large enough m' where there are k length-m' words in arithmetic progression.

(b) We inductively construct: let w_1 be the first letter of W. Then a_i is an index where $T^{a_i}(W)$ starts with k equally-spaced instances of w_i, and w_{i+1} is a prefix of $T^{a_i}(W)$ containing all k instances of w_i. Then, $\{T^{a_i}(W)\}_i$ converges, and the limit satisfies this property.

Now we give a hint of how we might be able to produce a longer arithmetic progression (of length $k+1$). Consider the case where $r = 2$ and $m = 1$, and suppose we've found a letter appearing at indices $0, A, ..., (k-1)A$ (represented by a black dot below). If the same letter was also at index kA, we have found an arithmetic progression of length $k+1$, but suppose otherwise. Then, using the fact above, we can "clone" this arithmetic progression k times with some equal spacing B. We represent this in the following diagram:



However, depending on which letter appears at index $(k+1)(A+B)$, we are forced to have an arithmetic progression of length $(k+1)$!

23. Set $W = W^*$ above and fix m. By assumption, for each $m' \in \mathbb{N}$, there should be a corresponding $n(m') > m'$ where the length m' prefix of W repeats another k times with spacing $n(m')$.

We will now show that there exists a length m word with $(k+1)$ instances in W which form an arithmetic progression.

Write $a \sim b$ for two indices $a, b \in \mathbb{N}$ if the first m letters of $T^a(W)$ and $T^b(W)$ match.

(a) **[2]** (Universe cloning lemma) Let $\Omega = \{(x, y) \mid x \sim y, x, y \in \mathbb{N}\}$, and let S be a finite subset of Ω. Show that there exists $d = d(S)$ such that $S \oplus d \subset \Omega$, where

$$S \oplus d = \{(x + k_1 d, y + k_2 d) \mid (x, y) \in S, k_1, k_2 \in \{0, 1, ..., k-1\}\}$$

(b) **[3]** (Cloned arithmetic progressions) Suppose $\{(a, a)\} \oplus d' \subset S$ (i.e. there is a length k arithmetic progression starting at index a). Show that for $d = d(S)$, the following both hold:

$$\{(a, a)\} \oplus d \subset S \oplus d$$
$$\{(a, a)\} \oplus (d + d') \subset S \oplus d$$

(c) **[3]** Let $S_0 = \varnothing$, $d_0 = k_0 = 0$. We inductively construct larger subsets of Ω as follows:

- $S_i^+ = S_i \cup \{(a_i, a_i)\})$ where $a_i = k(d_1 + ... + d_{i-1})$.
- $d_{i+1} = d(S_i^+)$
- $S_{i+1} = S_i \oplus d_i$

Show that for any $i < j$, $\{(a_i, a_i)\} + \frac{a_j - a_i}{k} \in \Omega$.

(d) **[1]** Conclude that there are $(k + 1)$ instances of some length m word in arithmetic progression.

Solution to Problem 23:

(a) Let $m' = \max\{x, y : (x, y) \in \Omega\} + m$. Then take $d = n(m')$.

(b) By construction, it follows that if $T \subset S$ then $T \oplus d \subset S \oplus d$ (so the first claim immediately follows).

The second claim follows once we know that $T \oplus (d + d') \subset (T \oplus d') \oplus d$, but this is straightforward from the definitions.

(c) $\frac{a_j - a_i}{d} = d_i + ... + d_{j-1}$, and furthermore

$$(...((S_i \oplus d_i) \oplus d_{i+1})... \oplus d_{j-1}) \subset S_j \subset \Omega$$

(d) Among $a_0, a_1, ..., a_{r^m}$, there are two terms $a_i \sim a_j$, so by the above we have a length $(k + 1)$ arithmetic progression starting at index a_i (with common difference $\frac{a_j - a_i}{d}$.)

2.7 Applications

You are allowed to use any results from the previous sections without proof.

24. **[4]**Prove that every syndetic subset of $\mathbb{N}$ contains arbitrarily long arithmetic progressions.[5]

Solution to Problem 24: Let $S = \{n_1 < n_2 < ...\}$ be the syndetic set, then suppose $N = \max\{n_{i+1} - n_i\}$. Then define $S_0 = 0, S_i = S + i \setminus (\cup_{j \leq i-1} S_j)$. Notice that $S_0, S_1, ..., S_{n-1}$ are disjoint but cover $\mathbb{N}$, so by van der Waerden's theorem one of them contains arbitrarily long arithmetic progressions. However, since $S_i - i \subset S$, we conclude that S contains arbitrarily long arithmetic progressions.

[5] Obviously, you need to use van der Waerden's theorem somehow. But perhaps it's interesting to note that you could use this statement to prove van der Waerden's theorem too!)

25. **[4]**Let $\{a_1 < a_2 < ...\}$ be a sequence of natural numbers containing arbitrarily long arithmetic progressions. Suppose that there exists another sequence of natural numbers $\{b_1 < b_2 < ...\}$ such that the quantity $|a_i - b_i|$ is bounded. Show that $\{b_i\}$ also contains arbitrarily long arithmetic progressions.

    Solution to Problem 25: Use finitary vdW: Suppose $|a_i - b_i| \le C$. let A be an arithmetic progression of length $N(k, 2C+1)$ (as defined in the finitary vdW). Then A contains an arithmetic progression $A' \subset A$ where $(a_i - b_i)$ is constant for $a_i \in A'$.

26. (a) **[4]** Let $\langle x \rangle$ denote the minimum distance from x to the nearest integer (or equivalently, $\langle x \rangle = \min\{x - \lfloor x \rfloor, \lfloor x \rfloor + 1 - x\}$ where $\lfloor x \rfloor$ is the greatest integer below x).

    Show that for any irrational x and real number $\varepsilon > 0$, there exists positive integer n such that $\langle n^2 x \rangle < \varepsilon$.

    (Hint: notice the identity $(n+2k)^2 - 2(n+k)^2 + n^2 = (2k)^2$)

    (b) **[6]** Prove that there are infinitely many perfect squares expressible as $\lfloor n\pi^{2020} \rfloor$. You may use the fact that π^{2020} is irrational without proof.

    Solution to Problem 26:

    (a) Note firstly that $\langle x - y \rangle = \langle \{x\} - \{y\} \rangle$.

    Divide up $[0, 1)$ into $M > \frac{1}{2\varepsilon}$ intervals of the form $[\frac{k}{M}, \frac{k+1}{M})$. Each term $\{n^2\varepsilon\}$ falls into one of the M intervals, so applying vdW, some interval contains $\{n^2\varepsilon\}$, $\{(n+k)^2\varepsilon\}$ and $\{(n+2k)^2\varepsilon\}$ for some $n, k \in \mathbb{N}$. Hence applying the identity we can finish.

    (b) Let $x = \pi^{2020}$. From the previous section, we know that k^2/x is close to an integer infinitely often (across $k \in \mathbb{N}$), so there are infinitely many integers where nx is close to some perfect square k^2. If nx is slightly more than k^2 infinitely often, then $\lfloor nx \rfloor = k^2$ infinitely often. This translates to wanting k^2/x to be slightly less than n infinitely often (i.e. $\sup_{k \in \mathbb{N}}\{k^2/x - \lfloor k^2 x \rfloor\} = 1$).

    Let $\alpha = 1/x$. We start by picking $\langle k^2(1/x) \rangle = \varepsilon$. Assume that $k^2(1/x)$ is slightly more than an integer (i.e. $\{k^2(1/x)\} = \varepsilon$).

    Now we consider the above expression for $k, 2k, 3k, ...,$, so

    $$\{(ak)^2(1/x)\} \text{ where } a \ge 1 : \varepsilon, 4\varepsilon, 9\varepsilon, ..., m^2\varepsilon, (m+1)^2\varepsilon - 1$$

    where $m = \lceil \varepsilon^{-1/2} \rceil - 1$ (i.e. the maximal m such that $m^2 2\varepsilon < 1$). This means that $m^2\varepsilon > 1 - (2m+1)\varepsilon \ge 1 - 2\varepsilon^{1/2} - \varepsilon$.

    As $\varepsilon \to 0$, $1 - \{(mk)^2(1/x)\} \to 0$ which is what we wanted.