Detailed Proof on Multiplicities of Differences in a Sequence

Theorem 1. *For a strictly increasing sequence $x_1 < x_2 < \cdots < x_n$ of real numbers, let $S = \{x_j - x_i \mid 1 \leq i < j \leq n\}$ be the multiset of differences. If each element of S has multiplicity at most 2, then there exist at least $\lfloor n/2 \rfloor$ elements of S with multiplicity exactly 1.*

Proof. Let $k_0 = \lfloor n/2 \rfloor$. We construct a set of k_0 distinct differences, each with multiplicity 1 in S.

1. Construction of Diagonal Differences

For $1 \leq m \leq k_0$, define the *diagonal difference*:

$$D_m := x_{n-m+1} - x_m$$

Lemma 1. *The differences $D_1, \ldots, D_{k_0}$ are strictly decreasing:*

$$D_1 > D_2 > \cdots > D_{k_0} > 0$$

Thus they are all distinct.

Proof. For $m < p$, observe:

$$\begin{aligned} m &< p \\ \Rightarrow n - m + 1 &> n - p + 1 \quad (\text{since } -m > -p) \\ \Rightarrow x_{n-m+1} &> x_{n-p+1} \quad (\text{strictly increasing sequence}) \end{aligned}$$

and

$$\begin{aligned} m &< p \\ \Rightarrow x_m &< x_p \quad (\text{strictly increasing sequence}) \end{aligned}$$

Therefore:

$$D_m - D_p = (x_{n-m+1} - x_m) - (x_{n-p+1} - x_p) = \underbrace{(x_{n-m+1} - x_{n-p+1})}_{>0} + \underbrace{(x_p - x_m)}_{>0} > 0$$

Thus $D_m > D_p$ for $m < p$, proving strict decrease. Positivity follows from $x_{n-m+1} > x_m$. □

2. Multiplicity Analysis of D_m

For each D_m, consider its multiplicity in S. The multiplicity cannot exceed 2 by hypothesis. We analyze two cases:

Case 1: Multiplicity 1

If D_m appears only as the difference between x_m and x_{n-m+1}, it directly contributes to our set.

Case 2: Multiplicity 2

Suppose D_m has multiplicity 2. Then there exists another pair $(i, j) \neq (m, n-m+1)$ with $i < j$ such that:

$$x_j - x_i = D_m = x_{n-m+1} - x_m$$

Rearranging gives:

$$x_{n-m+1} + x_i = x_j + x_m \quad (*)$$

We analyze possible index configurations:

Lemma 2. *If D_m has multiplicity 2, then exactly one of these holds:*

1. ***Left 3-AP:*** *$i < m < n-m+1$ and x_i, x_m, x_{n-m+1} form an arithmetic progression with common difference D_m*
2. ***Right 3-AP:*** *$m < n-m+1 < j$ and x_m, x_{n-m+1}, x_j form an arithmetic progression with common difference D_m*

Moreover, the indices $\{i, j, m, n-m+1\}$ have exactly 3 distinct elements.

Proof. From equation (*), we systematically eliminate cases:

Subcase 1: $i = m$

Then $x_{n-m+1} + x_m = x_j + x_m \Rightarrow x_j = x_{n-m+1} \Rightarrow j = n-m+1$, contradicting $(i, j) \neq (m, n-m+1)$.

Subcase 2: $j = n-m+1$

Then $x_{n-m+1} + x_i = x_{n-m+1} + x_m \Rightarrow x_i = x_m \Rightarrow i = m$, again a contradiction.

Subcase 3: $i = n-m+1$

Then $x_{n-m+1} + x_i = 2x_{n-m+1} = x_j + x_m$. Since $i = n-m+1 < j$ (as $i < j$), we have $j > n-m+1$. Then:

$$x_j - x_{n-m+1} = x_{n-m+1} - x_m = D_m$$

Thus x_m, x_{n-m+1}, x_j form a right 3-AP with common difference D_m. The distinct indices are $m, n-m+1, j$.

Subcase 4: $j = m$

Then $x_{n-m+1} + x_i = x_m + x_m \Rightarrow x_{n-m+1} - x_m = x_m - x_i$. Since $i < j = m$, we have $i < m$. Thus:

$$x_m - x_i = x_{n-m+1} - x_m = D_m$$

So x_i, x_m, x_{n-m+1} form a left 3-AP. The distinct indices are $i, m, n-m+1$.

Subcase 5: Four distinct indices

Assume all indices distinct. By equation (*), we have two possibilities:

Subsubcase 5a: $i < m$

Then from (*), $x_j = x_{n-m+1} + x_i - x_m$. Since $x_i < x_m$ and $x_{n-m+1} > x_m$, we need $x_j > x_{n-m+1}$ to maintain equality, so $j > n-m+1$. Thus indices satisfy $i < m < n-m+1 < j$. Now:

$$x_j - x_i = (x_j - x_{n-m+1}) + (x_{n-m+1} - x_m) + (x_m - x_i) > D_m$$

since both $(x_j - x_{n-m+1}) > 0$ and $(x_m - x_i) > 0$, contradiction.

Subsubcase 5b: $i > m$

Then $x_j = x_{n-m+1} + x_i - x_m < x_{n-m+1}$ (since $x_i < x_{n-m+1}$ but the combination decreases), so $j < n-m+1$. Thus $m < i < j < n-m+1$. Then:

$$D_m = x_{n-m+1} - x_m = (x_{n-m+1} - x_j) + (x_j - x_i) + (x_i - x_m) > x_j - x_i = D_m$$

again a contradiction.

Thus only Subcases 3 and 4 are possible, corresponding to right and left 3-APs. ☐

3. Double Differences and Their Uniqueness

When D_m has multiplicity 2 (i.e., 3-AP case), define the *double difference*:

$$\delta_m := \begin{cases} x_{n-m+1} - x_i & \text{(left 3-AP, } i < m) \\ x_j - x_m & \text{(right 3-AP, } j > n-m+1) \end{cases}$$

In both cases, $\delta_m = 2D_m$.

Lemma 3. *Each δ_m has multiplicity exactly 1 in S.*

Proof. We prove for left 3-AP (right case analogous). Let $\delta_m = x_{n-m+1} - x_i$. By construction, this difference appears at least once. Suppose it appears again via another pair $(p,q) \neq (i, n-m+1)$:

$$x_q - x_p = \delta_m = x_{n-m+1} - x_i \ (**)$$

Case 1: Four distinct indices
Assume $\{p, q, i, n-m+1\}$ distinct. By (**), we have $x_q + x_i = x_p + x_{n-m+1}$. The same index analysis as Lemma 2 shows contradiction in all subcases (similar to Subcase 5).
Case 2: Three distinct indices
Must involve arithmetic progression. But any 3-AP containing x_i and x_{n-m+1} would require a middle term y such that:

$$y - x_i = x_{n-m+1} - y \Rightarrow 2y = x_i + x_{n-m+1}$$

By the left 3-AP property, $x_m = \frac{x_i + x_{n-m+1}}{2}$, so $y = x_m$. Thus the only 3-AP is the original one, giving pairs (i, m) and $(m, n-m+1)$, but these produce differences D_m, not $\delta_m = 2D_m$. No new pairs yield δ_m.
Thus no other representation exists, so δ_m has multiplicity 1. □

Lemma 4. *The set $\{\delta_m \mid D_m$ has mult. $2\}$ is disjoint from $\{D_p \mid p = 1, \ldots, k_0\}$ and all δ_m are distinct.*

Proof. **Distinctness:** Since $\delta_m = 2D_m$ and D_m are distinct positive reals, all δ_m are distinct.
Disjointness: Suppose $\delta_m = D_p$ for some m, p. Then:

$$2(x_{n-m+1} - x_m) = x_{n-p+1} - x_p$$

Consider index relationships. For left 3-AP (right analogous):

$$x_{n-m+1} - x_i = x_{n-p+1} - x_p$$

Since $x_i = 2x_m - x_{n-m+1}$ (from 3-AP), substitute:

$$x_{n-m+1} - (2x_m - x_{n-m+1}) = x_{n-p+1} - x_p \Rightarrow 2(x_{n-m+1} - x_m) = x_{n-p+1} - x_p$$

Thus $2D_m = D_p$. But Lemma 1 implies $D_p < D_1$ while:

$$2D_m \geq 2 \min D_k > \max_{k \neq 1} D_k \quad \text{and} \quad 2D_m \leq 2D_1$$

If $p = 1$, $2D_m = D_1 \Rightarrow 2(x_{n-m+1} - x_m) = x_n - x_1$. But:

$$x_n - x_1 \geq x_{n-m+1} - x_m \quad \text{and} \quad 2(x_{n-m+1} - x_m) > x_{n-m+1} - x_m$$

with equality only if $x_{n-m+1} = x_n$ and $x_m = x_1$, but then $2(x_n - x_1) = x_n - x_1 \Rightarrow x_n = x_1$, contradiction. For $p \neq 1$, $D_p < D_1 < 2D_m$ since $D_1 \geq D_m$ and $2D_m \geq D_1$ only if $D_m \geq D_1/2 > D_2 \geq D_p$ (as $D_1 > D_2 > \cdots$), contradiction. Thus no overlap. □

4. Constructing the Set T

Define the set of differences:

$$T = \{t_m \mid 1 \leq m \leq k_0\}, \quad \text{where} \quad t_m = \begin{cases} D_m & \text{if } \operatorname{mult}(D_m) = 1 \\ \delta_m & \text{if } \operatorname{mult}(D_m) = 2 \end{cases}$$

Lemma 5. *The set T has exactly k_0 distinct elements, each with multiplicity 1 in S.*

Proof. **Size:** One element per m, so $|T| = k_0$.

Distinctness:

- If $t_m = D_m$ and $t_p = D_p$, then $t_m \neq t_p$ by Lemma 1
- If $t_m = \delta_m$ and $t_p = \delta_p$, then $t_m \neq t_p$ by Lemma 4
- If $t_m = D_m$ and $t_p = \delta_p$, then $t_m \neq t_p$ by Lemma 4

Multiplicity 1:

- If $t_m = D_m$, then $\operatorname{mult}(D_m) = 1$ by case choice
- If $t_m = \delta_m$, then $\operatorname{mult}(\delta_m) = 1$ by Lemma 3

□

Thus T contains exactly $\lfloor n/2 \rfloor$ distinct elements of S with multiplicity exactly 1. □

Problem 2

Finiteness of Indecomposable Uniform Coverings

May 28, 2025

Problem Statement

For a given positive integer n, a set $S = \{1, 2, \ldots, n\}$ is considered. A **uniform covering** $\mathcal{C}$ is a nonempty, finite multiset of subsets of S, where each element of S is contained in the same number of sets in the covering. Let this common number be $k \geq 0$. A uniform covering $\mathcal{C}$ is said to be **indecomposable** if it cannot be partitioned into two nonempty uniform coverings $\mathcal{C}_1$ and $\mathcal{C}_2$ such that $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ (as multisets).

For example, if $n = 4$, $(\{1\}, \{1\}, \{2, 3\}, \{2, 4\}, \{3, 4\})$ is a 2-uniform covering (each element from $\{1, 2, 3, 4\}$ is in exactly two sets). Also, $(\emptyset)$ is a 0-uniform covering. Both of these examples are given as uniform coverings.

The goal is to prove that *there exist only finitely many uniform coverings that are indecomposable.*

Proof

1. **Representing Coverings as Vectors**: Let $\mathcal{P}(S)$ be the power set of S. There are 2^n distinct subsets of S. Let these subsets be $X_1, X_2, \ldots, X_{2^n}$. Any multiset of subsets $\mathcal{C}$ can be represented by a vector of multiplicities $c = (c_j)_{j=1}^{2^n}$, where $c_j \in \mathbb{Z}_{\geq 0}$ is an integer indicating how many times the subset X_j appears in $\mathcal{C}$. Since $\mathcal{C}$ is nonempty, at least one $c_j > 0$, so $\sum_{j=1}^{2^n} c_j > 0$.

2. **Condition for Uniform Covering**: Let $v_j \in \{0, 1\}^n$ be the characteristic vector of the subset X_j. The i-th component of v_j, denoted $(v_j)_i$, is 1 if $i \in X_j$ and 0 otherwise. The condition that each element $i \in S$ is contained in exactly k sets in $\mathcal{C}$ translates to the following system of n linear equations:

$$\sum_{j=1}^{2^n} c_j (v_j)_i = k \quad \text{for each } i \in \{1, 2, \ldots, n\}$$

   This can be written more compactly as $\sum_{j=1}^{2^n} c_j v_j = k \cdot \mathbf{1}$, where $\mathbf{1}$ is the vector in $\mathbb{R}^n$ with all components equal to 1. The value k must be a non-negative integer.

3. **Homogeneous Linear Diophantine System**: We are looking for non-negative integer solutions $(c_1, \ldots, c_{2^n}, k)$ to this system. This can be rewritten as a system of n homogeneous linear Diophantine equations by treating k as a variable:

$$\left(\sum_{j=1}^{2^n} c_j (v_j)_i \right) - k = 0 \quad \text{for each } i \in \{1, 2, \ldots, n\}$$

   Let x be a vector $(k, c_1, \ldots, c_{2^n})$ of length $2^n + 1$. The set of all non-negative integer solutions x to this system forms a commutative monoid $\mathcal{M}$ under component-wise addition. The zero vector $\mathbf{0} = (0, 0, \ldots, 0)$ is the identity element of this monoid.

4. **Finitely Generated Monoid**: By Gordan's Lemma (or more generally, by theorems on Hilbert bases for integer cones, or the finite generation of monoids of non-negative integer solutions to homogeneous linear Diophantine systems), the monoid $\mathcal{M}$ is finitely generated. This means there exists a finite set

of non-zero solutions $G = \{g_1, g_2, \dots, g_N\}$, called generators, such that any non-zero solution $x \in \mathcal{M}$ can be expressed as a sum $x = \sum_{l=1}^{N} a_l g_l$ for some non-negative integers $a_l \in \mathbb{Z}_{\geq 0}$, where at least one $a_l > 0$. These generators are precisely the non-zero elements $g \in \mathcal{M}$ that cannot be written as a sum of two other non-zero elements in $\mathcal{M}$. That is, if $g = x_a + x_b$ with $x_a, x_b \in \mathcal{M}$, then either $x_a = \mathbf{0}$ or $x_b = \mathbf{0}$.

5. **Indecomposable Coverings and Generators**: A uniform covering $\mathcal{C}$, represented by multiplicities (c_j) and uniformity k, corresponds to a solution vector $x = (k, c_1, \dots, c_{2^n}) \in \mathcal{M}$. Since $\mathcal{C}$ must be nonempty, $\sum c_j > 0$, which implies that x is not the zero vector $\mathbf{0}$. The covering $\mathcal{C}$ is decomposable if it can be partitioned into two *nonempty* uniform coverings $\mathcal{C}_1$ and $\mathcal{C}_2$. Let $x_1 = (k_1, (c_{1,j}))$ and $x_2 = (k_2, (c_{2,j}))$ be the solution vectors corresponding to $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. If $\mathcal{C}$ is decomposable, then $x = x_1 + x_2$. The condition that $\mathcal{C}_1$ is nonempty means $\sum c_{1,j} > 0$. If all $c_{1,j} = 0$, then k_1 must also be 0 (as elements of S would be covered 0 times). Thus, $x_1 \neq \mathbf{0}$. Similarly, the condition that $\mathcal{C}_2$ is nonempty means $\sum c_{2,j} > 0$, so $x_2 \neq \mathbf{0}$. Therefore, $\mathcal{C}$ is indecomposable if its corresponding solution vector x cannot be written as the sum of two non-zero solution vectors $x_1, x_2 \in \mathcal{M}$. This is precisely the definition of a non-zero generator of the monoid $\mathcal{M}$.

6. **Conclusion**: Since the indecomposable uniform coverings correspond exactly to the non-zero generators of the monoid $\mathcal{M}$ of solutions, and this monoid is finitely generated (i.e., has a finite number of generators), there are only a finite number of such generators. Therefore, there exist only finitely many indecomposable uniform coverings.

Problem 3

Geometric Reflection and Circumcircle Proof

Problem

In $\triangle ABC$, points D, E, and F lie on sides BC, CA, and AB, respectively, such that $AEDF$ is a parallelogram. A point P satisfies $AP \perp BC$ and $DP \parallel AO$. Lines EP and FP intersect the perpendicular bisectors of CD and BD at K and L, respectively. Prove that the reflection of D over KL lies on the circumcircle of $\triangle ABC$.

Proof

Let D' be the reflection of D across the line KL. We will show that

$$\angle BD'C = \angle BAC,$$

which implies that A, B, C, D' lie on a common circle.

Step 1: Perpendicular Bisectors

Since K lies on the perpendicular bisector of CD, we have:

$$KC = KD.$$

By symmetry, $KD' = KD = KC$, so K also lies on the perpendicular bisector of CD'. Similarly, since L lies on the perpendicular bisector of BD, and D' is the reflection of D, we have:

$$LB = LD = LD',$$

so L lies on the perpendicular bisector of BD'. Therefore, the perpendicular bisectors of BD' and CD' intersect at some point $O_{D'}$, which is the center of the circle through B, C, and D'.

Step 2: Angle Chasing

We now use the fact that $DP \parallel AO$ and $AP \perp BC$. Since $AO \perp BC$, we conclude that $DP \perp BC$ as well. Thus, P is the foot of the perpendicular from both A and D to line BC, which implies that A and D are symmetric with respect to the line through P perpendicular to BC. This means the reflection of A over this line is D and vice versa.

Therefore, under this reflection, the circumcircle Γ of triangle ABC is sent to the circle through B, C, and D (and by symmetry, through D'). Thus, the center O of Γ maps to the center $O_{D'}$ of the circle $\odot BCD'$.

Because central angles are preserved under this symmetry, we have:

$$\angle BO_{D'}C = \angle BOC = 180^\circ - \angle BAC,$$

and therefore:

$$\angle BD'C = 180^\circ - \angle BO_{D'}C = \angle BAC.$$

Thus, A, B, C, D' lie on the same circle. ■

Problem 4

We call a positive integer orz if it is of the form n^2+n+1 for some positive integer n. Prove that there exists a set S of infinitely many orz integers that are not quadratfrei such that if a^2 and b^2 are respective divisors of two distinct elements of S then $\gcd(a,b)=1$

Let $P(n) = n^2+n+1$

First, note that we can choose an infinite sequence of distinct primes $(p_k)_{k=1}^{\infty}$ such that $p_k \equiv 1 \pmod 3$.

The condition $p_k \equiv 1 \pmod 3$ is necessary for $P(n) \equiv 0 \pmod{p_k^2}$ to have solutions.

$$n^2+n+1 \equiv 0 \pmod{p_k} \longleftrightarrow n \equiv \frac{-1 \pm \sqrt{-3}}{2}$$

$$\left(\frac{-3}{p_k}\right) = \left(\frac{-1}{p_k}\right)\left(\frac{3}{p_k}\right) = (-1)^{\frac{p_k-1}{2}} (-1)^{\frac{p_k-1}{2}} \left(\frac{p_k}{3}\right)$$

$$= \left(\frac{p_k}{3}\right).$$

$p'(x_k) = 2x_k+1$. If $p'(x_k) \equiv 0 \pmod{p_k}$ then $2x_k'+1 \equiv 0$, but in fact $(2x_k'+1)^2 \equiv -3 \pmod{p_k}$ so $p_k = 3$, but we chose $p_k \equiv 1 \pmod 3$.

Thus we can apply Hensel's lemma to see that there exists x_k such that
$P(x_k) \equiv 0 \pmod{p_k^2}$.

We inductively construct $S = \{s_1, s_2, \ldots\}$
$s_k = P(z_k)$

Base case: choose ~~x_0~~ $z_1 = x_1$. Then $s_1 = P(z_1)$
$p_1^2 \mid s$

<u>Inductive step</u> Assume $s_1, \ldots, s_{k-1}$ have been chosen:
$$S_F(x) = \{p \text{ prime} \mid p^2 \mid x\}$$
$$S_F(s_i) \cap S_F(s_j) = \emptyset \quad \text{for } 1 \leq i < j \leq k-1$$
Let $\mathcal{P}_{k-1} = \bigcup_{j=1}^{k-1} S_F(s_j)$
This is a finite set of primes.
Consider the following set of congruences:

$$z_k \equiv x_k \pmod{p_k^2}$$
$$z_k \equiv 0 \pmod{q^2} \text{ for all } q \in \mathcal{P}_{k-1}$$

[we pick p_k not in $\mathcal{P}_{k-1}$]
By the Chinese Remainder thm, there exists a solution z_k to this system.
We let $s_k = \mathcal{P}(z_k)$, $\quad s_k \equiv 0 \pmod{p_k^2}$

$$S_k \equiv 1 \pmod{q^2}$$

So $\quad S_F(S_k) \cap \mathcal{P}_{k-1} = \emptyset$

This construction generates an inf sequence $S_1, S_2, \ldots$ of odd integers

We can choose the z_k to be increasing so that the S_k are distinct.

By construction $S_F(S_i) \cap S_F(S_j) = \emptyset$. ∎