The Method of Indirect Descent (Part II)

Adib Hasan and Thanic Nur Samin

1 Introduction

In the previous article, we introduced a generalization of the method of Infinite Descent [4, 2], which we call indirect descent. To prove a proposition through indirect descent, first we construct a “score function” \( s : \mathcal{T} \to \mathbb{N} \) from the set of hypothetical counterexamples into the natural numbers. Next, we construct a transformation \( \chi : \mathcal{T} \to \mathcal{T} \), such that \( s(\chi(c)) < s(c) \) for all counterexamples \( c \in \mathcal{T} \). That is to say, given any counterexample we have a way to generate another one with a lower score. Our work is then done, since even a single counterexample would result in an infinite descending chain of scores \( s(c) > s(\chi(c)) > s(\chi^2(c)) > \cdots \), but no such sequence can exist within the natural numbers. We thus conclude that \( \mathcal{T} \) is empty, and the proposition true.

In practice, we determine the transformation first, and then define the score function to fit the transformation. That is because the former is often harder to find.

The first article showed the application of indirect descent in Functional Equations and Functional Inequalities. This article will demonstrate its use in Combinatorics and Number Theory.

2 Combinatorial Problems

Example 1 (APMO 2017/1) We call a 5-tuple of integers arrangeable if its elements can be labeled \( a, b, c, d, e \) in some order so that \( a - b + c - d + e = 29 \). Determine all 2017-tuples of integers \( n_1, n_2, \ldots, n_{2017} \) such that if we place them in a circle in clockwise order, then any 5-tuple of numbers in consecutive positions on the circle is arrangeable.

Solution. (By Thanic.) Replace each number \( x \) on the circle with \( x - 29 \), as it converts the condition \( a - b + c - d + e = 29 \) into more symmetric \( a - b + c - d + e = 0 \). Additionally, note that all the numbers on the circle become even after the conversion.

Step 1. Suppose \( \mathcal{T} \subseteq \mathbb{Z}^{2017} \) denotes the set of all ordered 2017-tuples of integers that satisfy the problem statement. Notice that

\[
a - b + c - d + e = 0 \implies \frac{a}{2} - \frac{b}{2} + \frac{c}{2} - \frac{d}{2} + \frac{e}{2} = 0
\]

Since all the numbers on the circle are even, we conclude that

\[
(x_1, x_2, \ldots, x_{2017}) \in \mathcal{T} \implies \left(\frac{x_1}{2}, \frac{x_2}{2}, \ldots, \frac{x_{2017}}{2}\right) \in \mathcal{T}
\]
Hence, there is a transformation \( \chi : (x_1, x_2, \ldots, x_{2017}) \to \left( \frac{x_1}{2}, \frac{x_2}{2}, \ldots, \frac{x_{2017}}{2} \right) \) for each element of \( T \).

Step 2. Define a score function \( s : T \to \mathbb{Z} \) as

\[
s(x_1, x_2, \ldots, x_{2017}) = \sum_{i=1}^{2017} |x_i|.
\]

Note that \( s \) is bounded below since \( \sum_{i=1}^{2017} |x_i| \geq 0 \).

Step 3. Suppose \( T \in T \) and \( T = (x_1, x_2, \ldots, x_{2017}) \). If there is at least one \( k \) so that \( x_k \neq 0 \), then

\[
s(T) = \sum_{i=1}^{2017} |x_i| > \sum_{i=1}^{2017} \frac{|x_i|}{2} = s(\chi(T))
\]

So, applying \( \chi \) recursively on \( T \) will indefinitely decrease \( s \) and breach its lower bound. Therefore, all the numbers on the circle has to be 0 after the first replacement. Hence, the only solution is \((29, 29, \ldots, 29)\).

Example 2 (IMO Shortlist 1994/C3) Peter has 3 accounts in a bank, each with an integral number of dollars. He is only allowed to transfer money from one account to another so that the amount of money in the latter is doubled.

a) Prove that Peter can always transfer all his money into two accounts.

b) Can he always transfer all his money into one account?

Solution. (By Pranav A. Sriram [3] (The original solution was adapted to fit the format of this article.)) The second part of the question is trivial - if the total number of dollars is odd, it is clearly not always possible to get all the money into one account. Now, we solve the first part.

Step 1. Suppose \( T \) is the set of all triples \((A, B, C)\) such that \( A \leq B \leq C \) are the number of dollars in the accounts at a particular point of time. We want to find a triple in \( T \) containing 0. So, we look for a transformation that reduces the number of dollars in a particular account. We try Euclidean algorithm, since it reduces an ordered pair of natural numbers. This leads us to the following solution.

Assume \( B = qA + r \) with \( r < A \). Enumerate the account with money \( A, B, C \) as 1, 2, 3, respectively. If \( A = 0 \), we are done. So, assume \( A > 0 \). \((m_1m_2 \ldots m_k)_2\) is the binary representation of \( q \). Transfer money \( k \) times to account 1 from accounts 2 or 3. The \( i^{th} \) transfer will be from account 2 if \( m_i = 1 \) and from account 3 otherwise. The number of dollars in the first account starts with \( A \) and keeps doubling in each step. Thus we end up transferring

\[
A(m_0 + 2m_1 + \ldots + 2^k m_k) = Aq
\]
dollars from account 2, and \((2^k - 1 - q)A\) dollars from account 3. So we are left with \(B - Aq = r\) dollars in account 2, which now becomes the account with smallest money. Hence,

\[
\chi : (A, B, C) \rightarrow \begin{cases} (r, 2^k A - A, C + (1 + q)A - 2^k A), & \text{or,} \\ (r, C + (1 + q)A - 2^k A, 2^k A - A) \end{cases}
\]

Step 2. But in both cases \(\min(\chi(T)) \leq r\). So we define \(s(T) = \min(A, B, C)\) for each \(T \in \mathcal{T}\), so \(s\) is indeed bounded below.

Step 3. \(\chi\) reduces \(s\) from \(A\) to \(r < A\) or even less. Therefore, applying \(\chi\) on a fixed \(T \in \mathcal{T}\) repeatedly, we can reduce \(s\) to 0. At that point, all the money will get transferred to two accounts.

\[\square\]

**Remark.** In combinatorics, such score functions are called monovariants since they only change in one direction.

### 3 Number Theoretic Problems

**Example 3 (Bulgaria NMO 2005/6 [1])** Let \(a, b, c \in \mathbb{N}\) such that \(ab\) divides \(c(c^2 - c + 1)\) and \(c^2 + 1\) divides \(a + b\). Prove that the sets \(\{a, b\}\) and \(\{c, c^2 - c + 1\}\) must coincide.

**Solution.** WLOG assume \(a \geq b\). Suppose \(c(c^2 - c + 1) = rab\). We want to prove \(r = 1\). Assume the contrary, and proceed like this: At first, show that

\[
rb^2 + 1 \equiv 0 \pmod{c^2 + 1} \quad (1)
\]

\[
c \geq 2b \quad (2)
\]

\[
a > c^2 - c + 1 \quad (3)
\]

Set \(d = c - b\). Thus \(d \geq b\).

After a little investigation, it becomes apparent that \(\frac{d}{b}\) will be very large. This makes us wonder how large it can possibly be.

Step 1. Assume

\[
\mathcal{T} = \left\{ n \mid \frac{d}{b} \geq n, n \in \mathbb{N} \right\}
\]

For any \(n \in \mathcal{T}\),

\[
c = b + d \geq (n + 1)b \implies c^2 + 1 \geq (n + 1)^2 b^2 + 1.
\]

From 1,

\[
rb^2 + 1 \geq c^2 + 1 \geq (n + 1)^2 b^2 + 1 \implies r \geq (n + 1)^2
\]
Hence

\[
\frac{c(c^2 - c + 1)}{ab} = \frac{c^2 - c + 1}{a} + \frac{d(c^2 - c + 1)}{ab} = r \geq (n + 1)^2 \quad (4)
\]

From 3, we know \( \frac{c^2 - c + 1}{a} < 1 \). Therefore,

\[
\frac{d}{b} > \frac{d(c^2 - c + 1)}{ab} = r - \frac{c^2 - c + 1}{a} > (n + 1)^2 - 1 = n^2 + 2n
\]

implying \( n^2 + 2n \in T \). Therefore, there is a transformation

\[
\chi : n \to n^2 + 2n \quad \forall n \in T
\]

Step 2. Set \( s(n) = \frac{1}{n} \quad \forall n \in T \). For a fixed triple \((a, b, c)\), \( s \) has a lower bound.

Step 3. Applying \( \chi \) recursively on any \( n \in T \), it is possible to decrease \( s \) below any positive real number. This raises a contradiction. Hence the \( r \geq 2 \) case is impossible; implying \( r = 1 \).

Now suppose \( a + b > c^2 + 1 \). Then

\[
2a \geq a + b \geq 2(c^2 + 1) \implies \frac{c^2 - c + 1}{a} < 1
\]

1 implies \( c \leq b \). If \( c = b \), we have \( a = c^2 - c + 1 \), proving the problem statement. Else if \( c < b \), then

\[
1 = \frac{c(c^2 - c + 1)}{ab} < \frac{b(c^2 - c + 1)}{ab} < 1
\]

This is again a contradiction. So \( a + b = c^2 + 1 \). Now we have \( a + b = c + (c^2 - c + 1) \) and \( ab = c(c^2 - c + 1) \). So we must have \( \{a, b\} = \{c, c^2 - c + 1\} \) \( \square \)

### 4 Selected Problems

1. (China NMO 2013/2) Find all nonempty sets \( S \) of integers such that \( 3m - 2n \in S \) for all (not necessarily distinct) \( m, n \in S \).

2. (USAMO 2015/6) Consider \( 0 < \lambda < 1 \), and let \( A \) be a multiset of positive integers. Let \( A_n = \{a \in A : a \leq n\} \). Assume that for every \( n \in \mathbb{N} \), the set \( A_n \) contains at most \( \frac{n(n+1)}{2} \lambda \) numbers. Show that there are infinitely many \( n \in \mathbb{N} \) for which the sum of the elements in \( A_n \) is at most \( \frac{n(n+1)}{2} \lambda \). (A multiset is a set-like collection of elements in which order is ignored, but repetition of elements is allowed and multiplicity of elements is significant. For example, multisets \( \{1, 2, 3\} \) and \( \{2, 1, 3\} \) are equivalent, but \( \{1, 1, 2, 3\} \) and \( \{1, 2, 3\} \) differ.)
3. (USA Team Selection Test 2002/6) Find all ordered pairs of positive integers \((m, n)\) such that \(mn - 1\) divides \(m^2 + n^2\).

4. (IMO 2007/5) Let \(a\) and \(b\) be positive integers. Show that if \(4ab - 1\) divides \((4a^2 - 1)^2\), then \(a = b\).

5. (Thanic) Suppose you are given a bee hive in the shape of a regular hexagon with side length of \(n\) hexagons. Some configuration \(S\) of the hexagon shaped cells are infected. Then, the infection spreads as follows: a cell becomes infected if and only if at least 3 of its neighbors are infected (two cells are neighbours if they share an edge.) If the entire board eventually becomes infected, prove that \(|S| \geq 2n - 1\) (that is, at least \(2n - 1\) of the cells were infected initially).

6. (IMO Shortlist 2013/C3) A crazy physicist discovered a new kind of particle which he called an imon, after some of them mysteriously appeared in his lab. Some pairs of imons in the lab can be entangled, and each imon can participate in many entanglement relations. The physicist has found a way to perform the following two kinds of operations with these particles, one operation at a time.

i) If some imon is entangled with an odd number of other imons in the lab, then the physicist can destroy it.

ii) At any moment, he may double the whole family of imons in his lab by creating a copy \(I'\) of each imon \(I\). During this procedure, the two copies \(I'\) and \(J'\) become entangled if and only if the original imons \(I\) and \(J\) are entangled, and each copy \(I'\) becomes entangled with its original imon \(I\); no other entanglements occur or disappear at this moment.

Prove that the physicist may apply a sequence of such operations resulting in a family of imons, no two of which are entangled.

7. (IMO 2010/5) Each of the six boxes \(B_1, B_2, B_3, B_4, B_5, B_6\) initially contains one coin. The following operations are allowed:

i) Choose a non-empty box \(B_j, 1 \leq j \leq 5\), remove one coin from \(B_j\) and add two coins to \(B_{j+1}\);

ii) Choose a non-empty box \(B_k, 1 \leq k \leq 4\), remove one coin from \(B_k\) and swap the contents (maybe empty) of the boxes \(B_{k+1}\) and \(B_{k+2}\).

Determine if there exists a finite sequence of operations of the allowed types, such that the five boxes \(B_1, B_2, B_3, B_4, B_5\) become empty, while box \(B_6\) contains exactly \(2010^{2010^{2010}}\) coins.

Copyright © Canadian Mathematical Society, 2018
References


Adib Hasan
Massachusetts Institute of Technology
notadib@mit.edu

Thanic Nur Samin
Notre Dame College, Bangladesh
thanicsamin@gmail.com