Invariants

Munir Uz Zaman

January 30, 2022

An *invariant* is a quality or quantity that never changes. For example, the net energy of a closed system is invariant (This is known as *the law of conservation of energy*). A *monovariant* or *semi-invariant* is a quantity that either always increases or always decreases.
Finding an invariant is a common idea in problems asking to prove that something cannot be achieved or some state cannot be reached (by applying some algorithm). Monovariants are also very efficient in showing that the corresponding process must stop after finitely many moves.

§1 Examples

Problem 1.1

You are given the set of integers $1, 2, \cdots, n$. In each step you can pick any two numbers a and b, remove those two numbers and add $ab+a+b$ to the set. Show that after $n-1$ steps the number that will remain will always be $(n+1)!-1$.

Solution: Let $x_1, x_2, \cdots, x_k$ be the numbers currently in the set. Now let us consider the value, $X = (x_1+1)(x_2+1)\cdots(x_k+1)$. After removing any two numbers x_i and x_j, and adding $x_ix_j + x_i + x_j$ to the set, the value X will still be the same.

$$X = (x_1+1)\cdots(1+x_i+x_j+x_ix_j)\cdots(x_k+1) = (x_1+1)\cdots(x_i+1)(x_j+1)\cdots(x_k+1)$$

Therefore X is an invariant. Initially $X = (n+1)!$. If A is the integer that will remain after $n-1$ steps then,

$$X = A+1 \implies A = (n+1)!-1$$

We are done!

♣

Problem 1.2

The integers $x_1, x_2, \cdots, x_n$ are all written around a circle. You can pick any 4 successive integers $x_k, x_{k+1}, x_{k+2}, x_{k+3}$. If $(x_k - x_{k+3})(x_{k+1} - x_{k+2}) < 0$ then you can replace x_{k+1} with x_{k+2} and x_{k+2} with x_{k+1} (swap x_{k+1}, x_{k+2}). Show that you cannot do this indefinitely.

Solution: It makes sense to try to find a monovariant as the problem wants us to show that a certain process cannot go on indefinitely. Let us consider the sum, (assume that if $k > n$ then $x_k = x_r$ where $r = k - \left\lfloor \frac{k}{n} \right\rfloor n$)

$$S = x_1x_2 + x_2x_3 + \cdots + x_{n-1}x_n + x_nx_1$$

Now if $(x_k - x_{k+3})(x_{k+1} - x_{k+2}) < 0$ then we can replace x_{k+1} with x_{k+2} and x_{k+2} with x_{k+1}. Suppose S_1 is the new value of the sum after swapping x_{k+1} and x_{k+2}, and S_0 is the old value of the sum.

$$S_0 = x_1x_2 + \cdots + x_kx_{k+1} + x_{k+1}x_{k+2} + x_{k+2}x_{k+3} + \cdots + x_nx_1$$

$$S_1 = x_1x_2 + \cdots + x_kx_{k+2} + x_{k+2}x_{k+1} + x_{k+1}x_{k+3} + \cdots + x_nx_1$$

The difference between the two values will be

$$S_1 - S_0 = x_kx_{k+2} - x_kx_{k+1} + x_{k+1}x_{k+3} - x_{k+2}x_{k+3} \implies S_1 - S_0 = (x_k - x_{k+3})(x_{k+2} - x_{k+1})$$

Since $(x_k - x_{k+3})(x_{k+1} - x_{k+2}) < 0 \implies (x_k - x_{k+3})(x_{k+2} - x_{k+1}) > 0$, $S_1 > S_0$. Therefore the value of the sum S is strictly increasing in each step. Now we just need to show that S is bounded above, that is, we need to find an upper bound for the sum. Let us assume $X = \max(x_1, \cdots, x_n)$. For any i, $x_ix_{i+1} \leq X^2 \implies x_ix_{i+1} < X^2 + 1$. Thus,

$$S = x_1x_2 + \cdots + x_nx_1 < n \times (X^2 + 1)$$

And so the value of S cannot increase forever which implies that the process cannot go on indefinitely.

♣

Proposition 1.3

Let a_n be a sequence recursively defined as,

$$a_n = \sum_{i=1}^{k} n_ia_{n-i} = n_1a_{n-1} + \cdots + n_ka_{n-k}$$

If N is an integer such that, $\sum_{i=1}^{k} n_i \equiv 1 \pmod N$ and X_n is a sequence such that,

$$X_n = \sum_{i=1}^{k} x_ia_{n+i-1} = x_1a_n + \cdots + x_ka_{n+k-1}$$

where, $x_i \equiv \sum_{j=1}^{i} n_{k-j+1} \pmod N$ then the sequence X_n is invariant modulo N, that is, $X_n \equiv X_{n-1} \pmod N$ for all n.

Proof: We first prove that, $x_{i+1} \equiv x_i + n_{k-i} \pmod N$.

$$x_{i+1} \equiv \sum_{j=1}^{i+1} n_{k-j+1} \equiv \sum_{j=1}^{i} n_{k-j+1} + n_{k-i} \equiv x_i + n_{k-i} \pmod N$$

Since $\sum_{i=1}^{k} n_i \equiv 1 \pmod N \implies x_k \equiv 1 \pmod N$,

$$X_n \equiv \sum_{i=1}^{k} x_ia_{n+i-1} \pmod N$$

$$\implies X_n \equiv \sum_{i=1}^{k-1} x_ia_{n+i-1} + x_ka_{n+k-1} \pmod N$$

$$\implies X_n \equiv \sum_{i=1}^{k-1} x_ia_{n+i-1} + a_{n+k-1} \pmod N$$

Now since $a_{n+k-1} \equiv \sum_{i=1}^{k} n_i a_{n+k-i-1}$,

$$\implies X_n \equiv \sum_{i=1}^{k-1} x_i a_{n+i-1} + a_{n+k-1} \pmod{N}$$
$$\implies X_n \equiv \sum_{i=1}^{k-1} x_i a_{n+i-1} + \sum_{i=1}^{k} n_i a_{n+k-i-1} \pmod{N}$$

Since $\sum_{i=1}^{k} n_i a_{n+k-i-1} = \sum_{i=0}^{k-1} n_{k-i} a_{n+i-1}$,

$$\implies X_n \equiv \sum_{i=1}^{k-1} x_i a_{n+i-1} + \sum_{i=1}^{k} n_i a_{n+k-i-1} \pmod{N}$$
$$\implies X_n \equiv \sum_{i=1}^{k-1} x_i a_{n+i-1} + \sum_{i=0}^{k-1} n_{k-i} a_{n+i-1} \pmod{N}$$
$$\implies X_n \equiv n_k a_{n-1} + \sum_{i=1}^{k-1} (x_i + n_{k-i})\, a_{n+i-1} \pmod{N}$$
$$\implies X_n \equiv x_1 a_{n-1} + \sum_{i=1}^{k-1} x_{i+1} a_{n+i-1} \pmod{N}$$
$$\implies X_n \equiv x_1 a_{n-1} + \sum_{i=2}^{k} x_i a_{n+i-2} \pmod{N}$$
$$\implies X_n \equiv \sum_{i=1}^{k} x_i a_{n-1+i-1} \pmod{N}$$
$$\implies X_n \equiv X_{n-1} \pmod{N}$$

And we are done!

♣