ITT9132 Concrete Mathematics
Exercise session 2: 9 February 2023

Silvio Capobianco

Last modified: 10 February 2023

Exercise 1.2

Find the shortest sequence of moves that transfers a tower of n disks from the left peg A to the right peg B, if direct moves between A and B are disallowed.

Solution. For $n = 1$ the shortest sequence is $A \to C$, $C \to B$. For $n = 2$ it is:

1. $A \to C$.
2. $C \to B$.
3. $A \to C$.
4. $B \to C$. Note that the whole tower is on peg C now.
5. $C \to A$.
6. $C \to B$.
7. $A \to C$.
8. $C \to B$.

For the general case, observe that the strategy that solves the problem for n disks works as follows:

1. Move the upper tower of $n - 1$ disks on peg B.
2. Move the n-th disk to peg C.
3. Move the upper tower of $n - 1$ disks on peg A.

4. Move the n-th disk to peg B.

5. Move the upper tower of $n-1$ disks on peg B.

Then the number T_n of moves needed by the strategy to solve the problem with n disks satisfies $T_0 = 0$ and $T_n = 3T_{n-1} + 2$ for every $n > 0$. We will now prove by induction thet $T_n = 3^n - 1$ for every $n \geqslant 1$.

- **Base case:** $n = 1$. Then $T_1 = 2 = 3^1 - 1$.
- **Inductive step:** Assume that $T_{n-1} = 3^{n-1} - 1$ for a certain $n \geqslant 2$. Then, by our strategy,

$$\begin{aligned} T_n &= T_{n-1} + 1 + T_{n-1} + 1 + T_{n-1} \\ &= 3 \cdot (3^{n-1} - 1) + 2 \\ &= 3 \cdot 3^{n-1} - 3 + 2 = 3^n - 1 \,. \end{aligned}$$

  We conclude that, if $T_{n-1} = 3^{n-1} - 1$, then $T_n = 3^n - 1$. Our argument holds whatever the actual value of $n \geqslant 2$ is.

Another way to solve the recurrence is by putting $U_n = T_n + 1$. The new sequence satisfies:

$$\begin{aligned} U_1 &= 3 \,, \\ U_n &= 3(U_{n-1} - 1) + 2 + 1 \\ &= 3U_{n-1} \ \text{ for every } n \geqslant 2 \,. \end{aligned}$$

Then clearly $U_n = 3^n$, so $T_n = 3^n - 1$.

Exercise 1.3

Show that, in the previous exercise, each legal arrangement of n disks is encountered exactly once.

Solution. There is exactly one legal arrangement per subdivision of the n disks in three (possibly empty) sets. There are $3^n - 1$ moves between displacements, so there are 3^n displacements reached overall. If one of these was touched twice, then it would be possible to reduce the number of moves by performing, the first time we reach said displacement, the chain of steps we would have taken on the second of its occurrences: which contradicts the result we obtained in the previous exercise.

A note: The technique of minimum counterexample

Let $P(n)$ be a predicate whose truth or falsehood depends on a variable n, which takes values in the set $\mathbb{N}$ of natural numbers (nonnegative integers). If we want to prove that $P(n)$ is true for every value of n, we might use a technique which relies on the:

Theorem (Well Ordering Principle)**.** *Every nonempty subset of* $\mathbb{N}$ *has a minimum.*

The Well Ordering Principle is equivalent to the principle of mathematical induction, in the sense that, assuming either of the two, it is possible to prove the other. This is an interesting exercise.

Here's how the technique of minimum counterexample works:

1. By contradiction, assume that $P(n)$ is false for *some* n.
2. By the Well Ordering Principle, there is a *minimum* $m \in \mathbb{N}$ such that $P(m)$ is false.
3. Reach a contradiction. Possible ways:
   (a) Prove that m is *not minimum:*
   That is, there is some $n \in \mathbb{N}$, $n < m$ such that $P(n)$ is false.
   (b) Prove that m is *not a counterexample:*
   That is, $P(m)$ is actually true.
   (c) Obtain a contradiction with some other fact which you already know to be true.
4. Conclude that, since there is no minimum counterexample, there is no counterexample at all.

This technique, or variants of it, also works with other kinds of induction such as *structural induction.*

Exercise 1.4

Are there any starting and ending configurations of n disks on three pegs that are more than $2^n - 1$ moves apart, according to Lucas's original rules?

Solution. By contradiction, let m be the smallest number of tiles such that there are two configurations X and Y of m tiles which are at least 2^m moves apart. Then the largest tile in X and Y must be on two different pegs,

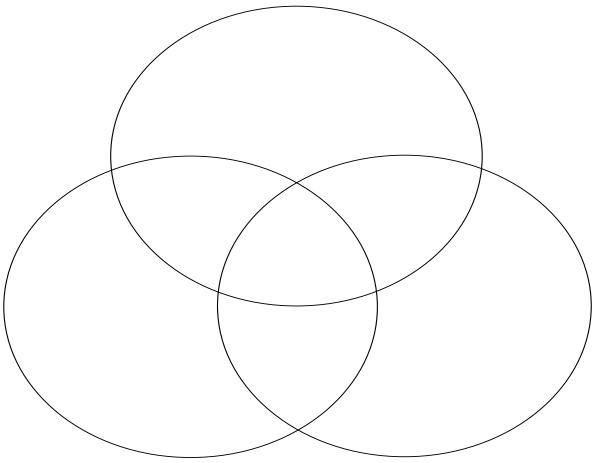

Figure 1: Venn diagram for three sets.

otherwise X could be turned into Y by only moving the $m-1$ smaller tiles, which requires less than 2^{m-1} moves by our hypothesis on m. But then, the problem can be solved by first transforming X into some other configuration Z where only the $m-1$ smaller tiles are moved, then moving the larger tile, and finally transforming Z into Y by only moving the $m-1$ smaller pegs: by our hypothesis on m, this requires at most $(2^{m-1}-1)+1+(2^{m-1}-1) = 2^m-1$ moves. This is a contradiction.

Exercise 1.5

A *Venn diagram* with three overlapping circles is often used to illustrate the eight possible subsets associated with three given sets (see Figure 1). Can the sixteen possibilities that arise with four given sets be illustratd by four overlapping circles?

Solution. Contrary to intuition coming from school years, the answer is: *no*. The reason is that two different circles have at most two points in common: consequently, an eventual fourth circle would add at most six regions, instead of the eight needed to fully represent a fourth set.

Surprisingly enough, four sets can be represented by four *ovals*. Even more surprisingly, and against a conjecture by John Venn himself, *five* sets can be represented by five *ellipses*.

Exercise 1.9 (tweaked)

In this exercise we will prove the famous:

Theorem (Arithmetic-geometric inequality)**.** *Let n be a positive integer. However chosen n positive reals $x_1, \ldots, x_n$,*

$$\sqrt[n]{x_1 \cdots x_n} \leqslant \frac{x_1 + \cdots + x_n}{n}\,. \tag{1}$$

That is: the *arithmetic mean* of a nonempty list of positive reals is an upper bound for the *geometric mean* of the same list.

To do this, let $P(n)$ be the proposition:

$$P(n) ::= \forall x_1, \ldots, x_n \in \mathbb{R}^+ \,.\, x_1 \cdots x_n \leqslant \left(\frac{x_1 + \cdots + x_n}{n}\right)^n \tag{2}$$

Observe that the inequality in (2) is equivalent to that in (1), and that $P(1)$ is trivially true.

1. Prove that $P(2)$ is true.
2. Prove that if $n \geqslant 2$ and $P(n)$ is true, then $P(n-1)$ is true. *Hint:* choose x_n well.
3. Prove that if $P(n)$ and $P(2)$ are both true, then $P(2n)$ is true.
4. Explain why it follows from the three points above that the arithmetic-geometric inequality is true for every positive integer n and positive reals $x_1, \ldots, x_n$.

Solution. 1. For $n = 2$ the proposition $P(2)$ is:

$$x_1 x_2 \leqslant \left(\frac{x_1 + x_2}{2}\right)^2 .$$

But the following manipulations turn each inequality into an equivalent inequality:

$$\begin{aligned} x_1 x_2 &\leqslant \left(\frac{x_1 + x_2}{2}\right)^2 \\ 4x_1 x_2 &\leqslant x_1^2 + 2x_1 x_2 + x_2^2 \\ 0 &\leqslant x_1^2 - 2x_1 x_2 + x_2^2 \end{aligned}$$

and the last inequality is true, because $x_1^2 - 2x_1 x_2 + x_2^2 = (x_1 - x_2)^2$, and the square of a real number is always nonnegative.

2. Suppose $P(n)$ is true. Then it remains true with the special choice of x_n:

$$\begin{aligned}
&x_1 \cdots x_{n-1} \cdot \frac{x_1 + \ldots + x_{n-1}}{n-1} \\
&\leqslant \left(\frac{x_1 + \ldots + x_{n-1} + \frac{x_1 + \ldots + x_{n-1}}{n-1}}{n} \right)^n \\
&= \left(\frac{\frac{(n-1)(x_1 + \ldots + x_{n-1}) + (x_1 + \ldots + x_{n-1})}{n-1}}{n} \right)^n \\
&= \left(\frac{x_1 + \ldots + x_{n-1}}{n-1} \right)^n \\
&= \left(\frac{x_1 + \ldots + x_{n-1}}{n-1} \right)^{n-1} \cdot \frac{x_1 + \ldots + x_{n-1}}{n-1} .
\end{aligned}$$

As $x_1, \ldots, x_{n-1}$ are arbitrary and $(x_1 + \ldots + x_{n-1})/(n-1) > 0$, $P(n-1)$ is true.

3. Suppose $P(n)$ and $P(2)$ are both true. Then:

$$\begin{aligned}
&x_1 \cdots x_n \cdot x_{n+1} \cdots x_{2n} \\
&\leqslant \left(\frac{x_1 + \ldots + x_n}{n} \right)^n \cdot \left(\frac{x_{n+1} + \ldots + x_{2n}}{n} \right)^n \\
&= \left(\left(\frac{x_1 + \ldots + x_n}{n} \right) \cdot \left(\frac{x_{n+1} + \ldots + x_{2n}}{n} \right) \right)^n \\
&\leqslant \left(\left(\frac{\frac{x_1 + \ldots + x_n}{n} + \frac{x_{n+1} + \ldots + x_{2n}}{n}}{2} \right)^2 \right)^n \\
&= \left(\frac{x_1 + \ldots + x_n + x_{n+1} + \ldots + x_{2n}}{2n} \right)^{2n} .
\end{aligned}$$

As $x_1, \ldots, x_{2n}$ are arbitrary, $P(2n)$ is true.

4. We could conclude that $P(n)$ is true for every positive integer n if we could know that every positive integer n falls under at least one of the following cases:

   (a) $n = 1$;

   (b) $n = 2$;

   (c) $n = m - 1$ for some integer $m \geqslant 2$;

(d) $n = 2m$ for some positive integer m.

But that it is so, we can prove in the following way. Consider the following algorithm:

- Initialize the variable m with the value 1.
- While $m \leqslant n$: update m to $2m$.
- While $m > n$: update m to $m - 1$.

Then, when the algorithm terminates, the value of m is exactly n.

The last point deserves some consideration, as it shows that the set $\mathbb{Z}^+$ of positive integers can be obtained with the following choice of base cases and constructors:

- **Base case 1:** $1 \in \mathbb{Z}^+$.
- **Base case 2:** $2 \in \mathbb{Z}^+$.
- **Constructor case 1:** if $n \in \mathbb{Z}^+$ and $n \geqslant 2$ then $n - 1 \in \mathbb{Z}^+$.
- **Constructor case 1:** if $n \in \mathbb{Z}^+$ then $2n \in \mathbb{Z}^+$.

This definition, however, is *ambiguous* in the sense that a positive integer can be obtained in more than one way. For example,

$$2 \to 4 \to 8 \to 7 \to 6$$

produces 6, but so does:

$$1 \to 2 \to 4 \to 8 \to 16 \to 15 \to 14 \to 13 \to 12 \to 11 \to 10 \to 9 \to 8 \to 7 \to 6$$

Instead, the definition given in Lecture 2 is *unambiguous*, because every positive integer can be obtained in a *unique* way from the base case 1 with the operations of doubling and doubling increased.

A note on the repertoire method

Consider a family of recurrences of the form:

$$\begin{aligned} g(0) &= \alpha\ , \\ g(n+1) &= \Phi(g(n)) + \Psi(n; \beta, \gamma, \ldots) \quad \text{for every} \quad n \geqslant 0 \end{aligned} \tag{3}$$

where $\alpha, \beta, \gamma, \ldots$ are m parameters. Assume that the following happens:

1. Φ is *linear in* g: that is, if $g(n) = \lambda_1 g_1(n) + \lambda_2 g_2(n)$, then $\Phi(g(n)) = \lambda_1 \Phi(g_1(n)) + \lambda_2 \Phi(g_2(n))$.

2. Ψ is linear in each of the $m-1$ parameters $\beta, \gamma, \ldots$ No hypothesis is made on the dependence of Ψ on n.

Then the whole system is linear in the parameters $\alpha, \beta, \gamma, \ldots$, and we can think of a general solution of the form:

$$g(n) = \alpha A(n) + \beta B(n) + \gamma C(n) + \ldots$$

where $A(n), B(n), C(n), \ldots$ are *uniquely determined* functions.

Now, suppose that we have a *repertoire* of m pairs of the form $((\alpha_i, \beta_i, \gamma_i, \ldots), g_i(n))$ satisfying the following conditions:

1. For every $i = 1, 2, \ldots, m$, $g_i(n)$ is the solution of the system corresponding to the values

$$\alpha = \alpha_i, \beta = \beta_i, \gamma = \gamma_i, \ldots .$$

2. The m m-tuples

$$(\alpha_i, \beta_i, \gamma_i, \ldots)$$

are *linearly independent*.

Then the functions $A(n), B(n), C(n), \ldots$ are uniquely determined.

The reason is that, for every fixed n,

$$\begin{array}{lllll} \alpha_1 A(n) & +\beta_1 B(n) & +\gamma_1 C(n) & +\ldots & = g_1(n) \\ \vdots & & & & \vdots \\ \alpha_m A(n) & +\beta_m B(n) & +\gamma_m C(n) & +\ldots & = g_m(n) \end{array}$$

is a system of m linear equations in the m unknowns $A(n), B(n), C(n), \ldots$ whose coefficients matrix is invertible.

Exercise A.1

Use the repertoire method to solve the following general recurrence:

$$\begin{array}{rcl} g(0) & = & \alpha \, , \\ g(n+1) & = & 2g(n) + \beta n + \gamma \ \text{ for every } n \geqslant 0 \, . \end{array} \tag{4}$$

Solution. The recurrence (4) has the form (3) with $\Phi(g) = 2g$ and $\Psi(n; \beta, \gamma) = \beta n + \gamma$, which are linear in g and in β and γ, respectively: therefore we can apply the repertoire method. The right-hand side of the recurrence suggests that the solution might have an exponential component, a linear component, and a constant component: we use this intuition to construct our test functions.

1. The choice $g(n) = 2^n$ for every $n \geqslant 0$ gives the recurrence:

$$\begin{aligned} 1 &= \alpha \,, \\ 2^{n+1} &= 2 \cdot 2^n + \beta n + \gamma \text{ for every } n \geqslant 0 \,. \end{aligned}$$

   Then $\alpha = 1$. For $n = 0$ we get $2 = 2 \cdot 1 + \gamma$, so $\gamma = 0$; for $n = 1$ we get $4 = 2 \cdot 2 + \beta$, so $\beta = 0$. Our first tuple-function pair is thus:

$$((1, 0, 0), 2^n) \,.$$

2. The choice $g(n) = n$ for every $n \geqslant 0$ gives the recurrence:

$$\begin{aligned} 0 &= \alpha \,, \\ n + 1 &= 2n + \beta n + \gamma \text{ for every } n \geqslant 0 \,. \end{aligned}$$

   Then $\alpha = 0$. For $n = 0$ we get $1 = 2 \cdot 0 + \gamma$, so $\gamma = 1$; for $n = 1$ we get $2 = 2 \cdot 1 + \beta + \gamma$, so $\beta = 1$. Our second tuple-function pair is thus:

$$((0, -1, 1), n) \,.$$

3. The choice $g(n) = 1$ for every $n \geqslant 0$ gives the recurrence:

$$\begin{aligned} 1 &= \alpha \,, \\ 1 &= 2 \cdot 1 + \beta n + \gamma \text{ for every } n \geqslant 0 \,. \end{aligned}$$

   Then $\alpha = 1$. For $n = 0$ we get $1 = 2 \cdot 1 + \gamma$, so $\gamma = -1$; for $n = 1$ we get $1 = 2 \cdot 1 + \beta - 1$, so $\beta = 0$. Our third tuple-function pair is thus:

$$((1, 0, -1), 1) \,.$$

Putting everything together, we obtain the system:

$$\begin{array}{rrrcl} A(n) & & & = & 2^n \\ & -B(n) & +C(n) & = & n \\ A(n) & & -C(n) & = & 1 \end{array}$$

whose solution is:

$$A(n) = 2^n\,;\;\; B(n) = 2^n - n - 1\,;\;\; C(n) = 2^n - 1\,.$$

The general solution of the recurrence is thus:

$$\begin{aligned} g(n) &= \alpha A(n) + \beta B(n) + \gamma C(n) \\ &= \alpha \cdot 2^n + \beta \cdot (2^n - 1 - n) + \gamma \cdot (2^n - 1) \\ &= (\alpha + \beta + \gamma) \cdot 2^n - \beta n - (\beta + \gamma)\,. \end{aligned}$$