THE COIN-CHANGING PROBLEM

Year 2018-2019

Students: Luca Barisan (I); Gaia Barella, Marco Casagrande, Azzurra Sofia Pizzolotto, Simona Sota (III); Paolo Barisan, Tommaso Bernardi, Anna De Biasi, Silvia Giovani, Alessia Lot, Klara Metaliu (IV).
School: I.S.I.S.S. M.Casagrande, Pieve di Soligo, Treviso - Italy.
Teachers: Fabio Breda, Francesco Maria Cardano, Francesco Zampieri.
Researcher: Alberto Zanardo (University of Padova).

Abstract. *The aim of this article is to study a new operation $\oplus$ that given two finite sets yields a new finite set whose elements correspond to all the possible sums between the elements of the two separate sets. In this paper, we will focus on the case in which the operation is iterated k times for the same finite set in order to determine the cardinality of the set at each iteration. We will find a connection with the coin changing problem by considering the finite set as a coin system that can be used to express any natural value. Given a coin system, we will search for the minimum number of necessary coins to obtain any integer value. Eventually we will determine a series of conditions that must be satisfied by the coins of the system with which it will be possible to get any integer value with the greedy algorithm.*

1 The operation and the algebraic structure

We started our research with the study of a new binary operator called sum $\oplus$ defined on the set of finite families of integers.
The $A \oplus B$ set contains all the results of all the possible sums between the elements of the two sets.
Example. Let us consider two numerical sets $A = \{2, 5\}$ and $B = \{3, 6, 7\}$. We define

$$A \oplus B = \{5, 8, 9, 11, 12\}$$

It is possible to build an algebraic structure on the finite parts of the set of the natural numbers $Fin(\mathbb{N})$ and the operation sum $\oplus$.

It is easy to prove that the algebraic structure $(Fin(\mathbb{N}), \oplus)$ has the following properties:

- Commutative property.
- Associative property.
- Neutral element $N = \{0\}$.

Only the element $\{0\}$ has its own inverse element that is $\{0\}$. In fact $\{0\} \oplus \{0\} = \{0\}$. For any other element of $Fin(\mathbb{N})$ there is not an inverse element. So the algebraic structure $(Fin(\mathbb{N}), \oplus)$ is not a group but an abelian monoid.

2 The cardinality

One of first step of our work has been the analysis of the cardinality of the $A(n)_k$ set.
Let $A(n)_1 = \{a_1, a_2, a_3, ..., a_n\}$ be the starting set (with $a_i \neq 0 \quad \forall\, 1 \leq i \leq n$). Let us call $|A(n)_k|$ the cardinality of the set obtained by iterating k times (with $k \geq 2$) the sum of $A(n)_1$ with itself. For example:

$$A(3)_1 = \{1, 3, 7\} \quad \Rightarrow \quad A(3)_2 = \{2, 4, 6, 8, 10, 14\} \quad \Rightarrow \quad A(3)_3 = \{3, 5, 7, 9, 11, 13, 15, 17, 21\}$$

- For $n = 1$ (that is $A(1)_1 = \{a_1\}$) $A(1)_k$ will always consist just $ka_1 \Rightarrow |A(1)_k| = 1\,\forall k \geq 1$.
- For $n = 2$ then $|A(2)_k| = k + 1$, that is, for every starting set, the cardinality increases with arithmetic progression of common difference 1. For example:

$$A(2)_1 = \{1, 3\} \quad \Rightarrow \quad A(2)_2 = \{2, 4, 6\} \quad \Rightarrow \quad A(2)_3 = \{3, 5, 7, 9\}$$

- Such a result has been proved to be true for generic sets of n elements if these are in arithmetic progression, obtaining that the cardinality still increases with arithmetic progression of common difference $n - 1$: $|A(n)_k| = k(n - 1) + 1$.

Theorem 2.1. *If $A(n)_1 = \{a, a+d, ..., a+(n-1)d\}$ with n, d, k natural numbers, then $|A(n)|_k = k(n-1) + 1$*

Proof. We are going to prove that $A(n)_k = \{ka, ka + d, ..., ka + k(n - 1)d\}$. The proof proceeds by induction on k

For $k = 1$, $A(n)_1 = \{a, a + d, ..., a + (n - 1)d\}$ by definition.

Now we suppose that $A(n)_k = \{ka, ka + d, ..., ka + k(n - 1)d\}$. Then

$$\begin{aligned} A(n)_{k+1} &= \{ka + a, ka + d + a, ..., ka + k(n - 1)d + a + (n - 1)d\} \\ &= \{(k + 1)a, (k + 1)a + d, ..., (k + 1)a + (k + 1)(n - 1)d\}. \end{aligned}$$

Indeed, the lowest element of $A(n)_{k+1}$ is obtained from the sum of the first element of $A(n)_k$ plus a and the greatest one from the sum of the last element on $A(n)_k$ plus $a + (n - 1)d$ [1].

So $A(n)_k = \{ka, ka + d, ..., ka + k(n - 1)d\}$ and the elements of the set $A(n)_k$ are in arithmetic progression with common difference d and therefore $|A(n)_k| = k(n - 1) + 1$

□

- Finally, for $n \geq 3$ a numeric study has been implemented writing a C++ software that, given the starting set $A(n)_1$, generates the $A(n)_k$ set and calculates its cardinality.

2.1 $n = 3$ case

In the $n = 3$ case we studied various combinations of the starting values of the set through the C++ software and we were able to find some regularities in the possible cardinality progressions. By the observation of the generated sets, we tried to find analytical relations that describe the cardinality $|A(3)_k|$ as a function of k [2].
We immediately noticed that there exists a progression with the quickest increase of cardinality. In this case at every step the increase results to be greater of one unit with respect to the previous one:

$$|A(3)_k| = \sum_{i=0}^{k}(i+1) = \sum_{i=1}^{k+1} i = \frac{1}{2}(k+1)(k+2), \tag{1}$$

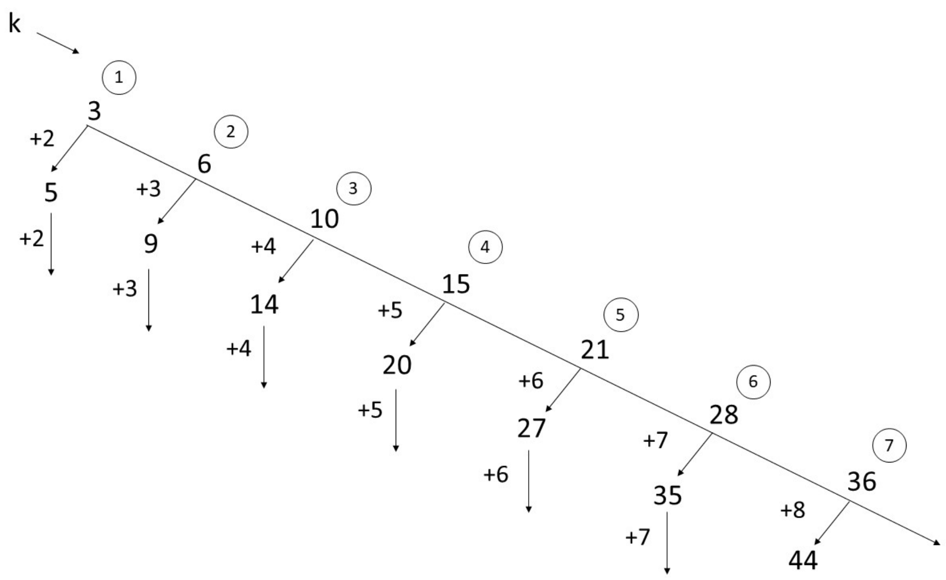
where the result of the sum can be easily obtained using the Gauss formula. These can be proved to be equal to the combinations $C'_{3;k}$ of 3 elements taken k at a time with repetitions. In fact, by multiplying and dividing for $k!$ one gets:

$$|A(3)_k| = \frac{k!(k+1)(k+2)}{2k!} = \frac{(k+2)!}{2k!} = \frac{(3+k-1)!}{k!(3+k-1-k)!} = \binom{3+k-1}{k} = C'_{3;k}$$

On the other hand we also noticed that if certain relation between the elements of the starting set $A(3)_1$ are verified, the cardinality will not increase with the quickest progression. We tried to guess the formulas that describe the cardinalities of $A(3)_k$ in this cases.
Given $A(3)_1 = \{a_1, a_2, a_3\}$, the most general condition for which the cardinality doesn't increases with the quickest progression has been identified as follows:
if there exist two natural numbers $(p, q) = 1$ with $q < p$ such that

$$pa_2 = qa_1 + (p-q)a_3, \tag{2}$$

the cardinality $|A(3)_k|$ exits from the quickest progression at the p^{th} step [3]. From there on it will always follow an arithmetic progression with common difference equal to the p^{th} increase.
These observations can be summarised in a tree diagram, where the possible values of $|A(3)_k|$ are represented as a function of k. From now on, this graph will be referred to as the cardinality tree.



The upper branch of the tree represents the progression with the quickest increase of cardinality given by formula (1), the circled numbers are the values of k while the others are the values of $|A(3)_k|$. For

each branch that starts from the main one the common difference of the arithmetic progression that yields $|A(3)_k|$ is specified. As previously explained, the exit from the main branch verifies at the p^{th} step if there exist two numbers p and q that satisfy the condition (2).
In the following, the cardinality that one obtains at the k^{th} iteration, exiting from the quickest progression at the p^{th} step will be referred to as $|A(3)_{k,p}|$.

- If $2a_2 = a_1 + a_3$ (that is the elements of the starting set are in arithmetic progression... [4]) then $p = 2$, so one exits from the main branch at the 2^{nd} step, obtaining

$$|A(3)_{k,2}| = \sum_{i=0}^{1}(i+1) + \sum_{i=2}^{k} 2 = 1 + 2 + (k-1)2 = 2k+1;$$

- else if $3a_2 = 2a_1 + a_3$ or $3a_2 = a_1 + 2a_3$ then $p = 3$, so one exits from the main branch at the 3^{rd} step, obtaining

$$|A(3)_{k,3}| = \sum_{i=0}^{2}(i+1) + \sum_{i=3}^{k} 3 = 1 + 2 + 3 + (k-2)3 = 3k;$$

- else if $4a_2 = a_1 + 3a_3$ or $4a_2 = 3a_1 + a_3$ then $p = 4$, so one exits from the main branch at the 4^{th} step, obtaining

$$|A(3)_{k,4}| = \sum_{i=0}^{3}(i+1) + \sum_{i=4}^{k} 4 = 1 + 2 + 3 + 4 + (k-3)4 = 4k-2;$$

- and so on...

Let us suppose that the exit condition is verified at the p^{th} step, where p satisfies the exit condition (2). In such a case, generalizing the previous results, one obtains:

$$|A(3)_{k,p}| = \sum_{i=0}^{p-1}(i+1) + \sum_{i=p}^{k} p = \sum_{i=1}^{p} i + \sum_{i=p}^{k} p = \frac{1}{2}p(p+1) + [k-(p-1)]p = \frac{1}{2}(2k-p+3)p.$$

On the other hand it can be noticed that the formula above only works if the iteration step is $k > p-3$ [5] . In the opposite case the formula can be simply corrected by substituting $p = k+2$, thus obtaining:

$$|A(3)_{k,p}| = |A(3)_{k,k+2}| = \sum_{i=0}^{k}(i+1) = \frac{1}{2}(k+1)(k+2)$$

that is once again the quickest progression.
To summarize:

- If $k > p-3$ then $|A(3)_{k,p}| = \sum_{i=1}^{p} i + \sum_{i=p}^{k} p = \frac{1}{2}(2k-p+3)p;$

- else if $k \leq p-3$ then $|A(3)_{k,p}| = |A(k+2)_k| = \sum_{i=0}^{n}(i+1) = \frac{1}{2}(k+1)(k+2);$

- for $p-3 < k < p$ both the relations return the same values for cardinality.

For example let us consider the starting set $A(3)_1 = \{1, 2, 5\}$. The two natural numbers $p = 4$, $q = 3$, with $(4, 3) = 1$ satisfy the previous relation (2):

$$4 \cdot 2 = 3 \cdot 1 + (4 - 3) \cdot 5$$

- if $k < 4$:

$$|A(3)_1| = \frac{1}{2}(1+1)(1+2) = 3, \ \ |A(3)_2| = \frac{1}{2}(2+1)(2+2) = 6, \ \ |A(3)_3| = \frac{1}{2}(3+1)(3+2) = 10$$

- else if $k \geq 4$:

$$|A(3)_4| = \frac{1}{2} \cdot (2 \cdot 4 - 4 + 3) \cdot 4 = 14, \quad |A(3)_5| = \frac{1}{2} \cdot (2 \cdot 5 - 4 + 3) \cdot 4 = 18, \quad ...$$

2.2 $n > 3$ case

In the $n = 3$ case it has been proved that the progression with the quickest increase of cardinality is given by the combinations with repetition of n elements of length k:

$$|A(n)_k| = C'_{n;k}.$$

Such a result can be proved to be still valid in the $n > 3$ cases. In fact the quickest increase in cardinality will always be given by the maximum number of combinations of n elements of length k, but when some of these are identical the cardinality will not increase with the quickest progression. The range of cardinality progressions that can occur in such cases, together with the conditions under which these will happen, can be very large and will not be further investigated in this work.
On the other hand, the slower increase has already been proved to be obtained if the elements of the starting set $A(n)_1$ are in arithmetic progression, and results to be still in arithmetic progression of common difference $n - 1$:

$$|A(n)_k| = k(n - 1) + 1$$

Ultimately we have that $|A(n)_k|$ will always be bounded by the slowest and the quickest progression:

$$(n - 1)k + 1 \leq A(n)_k \leq C'_{n;k}.$$

3 From the operation to the coin changing problem

The analysis of the $\oplus$ operation let us study the so-called *coin changing problem*, that consists in representing a given value V with the minimum number of coins that belong to a given finite set of coin denominations.
Starting with the $A(2)_1 = \{a_1, a_2\}$ set the iterations must assume the form

$$A(2)_2 = \{2a_1, a_1 + a_2, 2a_2\}$$

$$A(2)_3 = \{3a_1, 2a_1 + a_2, a_1 + 2a_2, 3a_2\}$$

$$...$$

$$A(2)_k = \{(ka_1, (k - 1)a_1 + a_2, ..., a_1 + (k - 1)a_2, ka_2\}$$

that is all the elements of $A(2)_k$ can be written as

$$(k - p)a_1 + pa_2, \quad p = 0, ..., k.$$

The problem of finding the minimum number of coins needed to decompose a given value V, can therefore be reduced to find the first $A(2)_k$ set in which the value itself appears: the number of coins

needed will then be equal to the corresponding iteration k.
For example, to write the value 12 with the coin system

$$A(2)_1 = \{2, 5\},$$

by iterating the operation one obtains

$$A(2)_2 = \{4, 7, 10\}$$

$$A(2)_3 = \{6, 9, 12, 15\}$$

$12 \in A(2)_3$ so the minimal number of coins needed to write 12 is 3 $(12 = 2 + 5 + 5)$.
On the other hand to build a coin system we need to know what kind of numbers do we have to use. Firstly we considered all the multiples of $0,01$ *euros*.

$$x \in \mathbb{Q}_0^+ \quad | \quad x = h \cdot \frac{1}{100} \quad h \in \mathbb{N}_0 \quad [6]$$

The coin system then becomes

$$A = \left\{ \frac{a_0}{100}, \frac{a_1}{100}, \frac{a_2}{100}, ..., \frac{a_n}{100} \right\}$$

with $a_0 < a_1 < ... < a_n$ non-zero natural numbers.
Then we noticed that operating with fractions like $a_n/100$ is equivalent to considering just the numerator of the fraction a_n which is by definition a natural number.
Let us consider an example. If we want to express 1 euro just with $0,02$ coins we will need 50 coins.

$$1 = \frac{2}{100} \cdot 50$$

That is equivalent to

$$100 = 2 \cdot 50$$

So we will consider only those coins whose value is a natural number.

$$A = \{a_0, a_1, a_2, ..., a_n\} \in \mathbb{N}_0$$

with $a_0 < a_1 < ... < a_n$ non-zero natural numbers.

4 The geometric method

We searched for a method to find the decomposition of a given value V by using an initial set of coins $A(n)_1 = \{a_1, a_2, a_3, ..., a_n\}$, according to the coin changing problem.
We tried a geometric approach to determine the set $S = \{x_1, x_2, ...x_n\}t$ of integer coefficients such that

$$V = x_1 a_1 + x_2 a_2 + ... + x_n a_n$$

4.1 $n = 2$ case

In this case, we have a starting set $A(2)_1 = \{a_1, a_2\}$ with $a_1 < a_2$.
We have to look for x_1 and x_2, two integer coefficients such that a given V is

$$V = x_1 a_1 + x_2 a_2$$

There must exist a value of k such that $V \in A(2)_k$, and all the elements of this set can be written as:

$$(k - p)a_1 + p a_2, \quad p = 0, 1, ..., k$$

From the tree (section 2) we can see that k is the sum of the coefficients:

$$x_1 + x_2 = k, \tag{3}$$

so $k \geq x_1$ e $k \geq x_2$.
So we build a (k, x_2) cartesian plane. Solving $V = a_1x_1 + a_2x_2$ with respect to x_1 one obtains:

$$x_1 = \frac{V - a_2x_2}{a_1} \tag{4}$$

Substituting it in (3), we got the final equation

$$x_2 = \frac{ka_1 - V}{a_1 - a_2} = \frac{a_1}{a_1 - a_2} \cdot k - \frac{V}{a_1 - a_2} \tag{5}$$

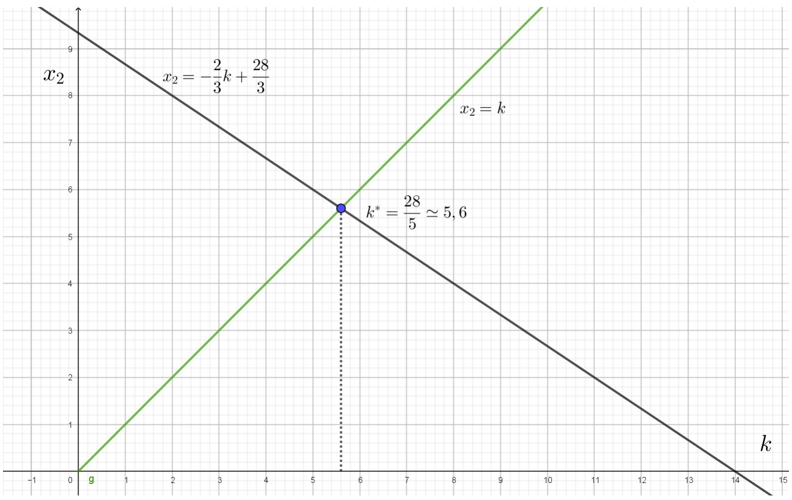
that represents a straight line in the (k, x_2) plane.
By intersecting this straight line with the bisector $k = x_2$, we get:

$$k^* = \frac{V}{a_2}$$

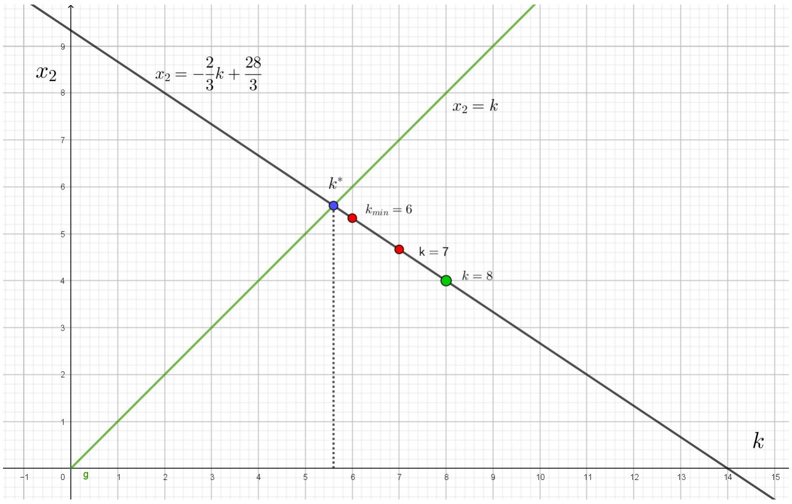
Let k_{min} be the minimum integer value such that $k_{min} \geq k^*$.
One can now calculate x_2 from (5), by substituting $k = k_{min}$. If x_2 is an integer, we can calculate x_1 from (3) and the decomposition is given.
In case x_2 is not an integer number, we have to increase k_{min} by one unit and repeat the search until x_2 is an integer number.

An example: Starting from $A(2)_1 = \{2, 5\}$, we try to express, for example, $V = 28$ as a combination of the elements of the starting set. Let us calculate k^*. According to (3) and to (5)

$$\begin{cases} x_2 &= -\frac{2}{3}k + \frac{28}{3} \\ x_2 &= k \end{cases} \quad \Rightarrow \quad k^* = \frac{28}{5} = 5,6$$



Moreover, taking $k_{min} = 6$ gives the non-integer value $x_2 = 16/3$. So we have to try with another integer value, $k = k_{min} + 1 = 7$ but it gives back the non-integer value $x_2 = 14/3$. If, finally, $k = 7 + 1 = 8$, it results $x_2 = 12/3 = 4$ which is integer, so the solution is acceptable. According (3), we find $x_1 = k - x_2 = 8 - 4 = 4$.
This means that $28 = 4 \cdot 2 + 4 \cdot 5$, so this value can be obtained with a minimum of $4 + 4 = 8$ coins.



4.2 $n = 3$ case

We tried to extend the method from dimension 2 to 3. Let $A(3)_1 = \{1, a_2, a_3\}$ be the starting set, with $a_1 = 1$ and $1 < a_2 < a_3$. Such a choice, which is needed in order to obtain all the possible values, gives us the advantage to greatly simplify the problem.
So now we have to find 3 integer coefficient x_1, x_2 and x_3 to write V as a linear combination:

$$V = x_1 + a_2x_2 + a_3x_3. \tag{6}$$

Similarly to the previous case, we know that it must exist a value k for which $V \in A(3)_k$, that provides the constraint:

$$x_1 + x_2 + x_3 = k. \tag{7}$$

Solving (6) with respect to x_1 one obtains:

$$x_1 = V - a_2x_2 - a_3x_3.$$

Substituting it in (7), we got the final equation

$$V - a_2x_2 - a_3x_3 + x_2 + x_3 = k, \tag{8}$$

that represents a plane in the (k, x_2, x_3) space.
By intersecting this plane with the two planes $x_2 = k, x_3 = k$ we get:

$$k^* = \frac{V}{a_2 + a_3 - 1}.$$

Let k_{min} be the minimum integer value such that $k_{min} \geq k^*$.
One can now calculate x_2 from (8) obtaining:

$$x_2 = \frac{V - k + (1 - a_3)x_3}{a_2 - 1}.$$

The algorithm proceeds now as follows:

- starting from $k = k_{min}$, and decreasing x_3 from k to 0, search for the first value that yields a non negative integer x_2;
- if no legit x_3 can be found, increase $k := k + 1$ and restart;

- else if a couple (x_3, x_2) of non negative integers can be found calculate the corresponding x_1 from (7);
- if x_1 is also a non negative integer, the decomposition for V has been obtained;
- else if no legit set (x_3, x_2, x_1) of non negative integers can be found, increase $k := k + 1$ and restart.

Example $A(3)_1 = \{1, 2, 5\}$ and $V = 37$.

Using this algorithm, we have found:

$$k^* = \frac{37}{2+5-1} = \frac{37}{6} \simeq 6,17 \Rightarrow k_{min} = 7$$

In the following table are shown the computed values (k, x_2, x_3) and the condition for x_1.

k	x_3	x_2	x_1
7	7	2	< 0
7	6	6	< 0
7	5	10	< 0
7	4	14	< 0
7	3	18	< 0
7	2	22	< 0
7	1	26	< 0
7	0	30	< 0
8	8	< 0	—
8	7	1	0

$$\Rightarrow 37 = 7 \cdot 5 + 1 \cdot 2 + 0 \cdot 1, \quad k = 7 + 1 = 8$$

5 The research for the coin system

We first tried to build a coin system S such that it is possible to express any natural We begin with some definitions.

Definition 5.1. *A coin system S is a finite set of natural numbers $0 < a_1 < a_2 < a_3 < ... < a_n$.*

Definition 5.2. *Given a coin system S and a natural number x, we call representation of x under S, indicated with $R_S(x)$, a possible sum of elements of S that yields x.*

Definition 5.3. *Given a representation $R_S(x)$, the size $\mid R_S(x) \mid$ of the representation is the number of coins used in it.*

The first idea could be to choose a set with infinite coin denominations: in this case the set S with which it is possible to write every $x \in \mathbb{N}_0$ using the least number of coins is

$$S_\infty = \mathbb{N}_0 \quad | \quad \forall\, x \in \mathbb{N}_0, \quad x = n \quad |S_\infty| = \infty$$

Obviously it is not possible to build this first set. Another possibility could be to choose a coin system with only one coin denomination which is the set

$$S_1 = \{1\} \quad | \quad \forall\, x \in \mathbb{N}_0, \quad x = 1 \cdot x \qquad |S_1| = 1$$

Both the coin system are not feasible and so we have to find another way to define the best coin system.

A possible representation of x under S can be obtained using the **greedy method**, which consists in summing the greater coin less than x and the greater coin less than the difference between x and the first coin and then repeating this procedure until we reach exactly x.

Definition 5.4. *Given a coin system S and a natural number x, we call greedy representation of x under S, indicated with $G_S(x)$, the representation obtained with the greedy method.*

Example 5.1. *Let $S = \{1, 5, 10, 20, 50\}$ be a coin system and $x = 35$ the number we have to represent.*

$$G_S(35) = 20 + 10 + 5 \qquad | G_S(35) |= 3$$

The disadvantage of the greedy method is that it does not always use the minimum number of coins.

Example 5.2. *Let us consider the coin system $S = \{1, 6, 10\}$ and let x be 12. Applying the greedy method we obtain the following representation:*

$$G_S(12) = 10 + 1 + 1 \qquad | G_S(12) |= 3$$

In this case it is possible to represent the number 12 with a smaller number of coins:

$$R_S(12) = 6 + 6 \qquad | R_S(12) |= 2$$

The coin system S_∞ minimizes the number of coins needed but its cardinality is infinite. On the other hand the coin system S_1 has the minimum cardinality but the number of coins needed to represent x increases significantly as x increases.
So we choose to consider as best coin system the one for which the greedy method uses the minimum number of coins. Even if it does not always yield the representation with the smallest size, we still choose this definition of best because in this way we have a clear algorithm to follow in order to get the representations of a certain x under different coin systems and compare them.
Therefore we call this coin system *canonical*.

Definition 5.5. *A coin system S is canonical if the number of coins used in the representation of every number x under S calculated with the greedy method is less than the number of coins used in any other representation of x under S.*

$$| G_S(x) |<| R_S(x) | \qquad \forall x \in \mathbb{N}_0, \forall R_S(x) \neq G_S(x)$$

That is the size of $G_S(x)$, for all x, is less than the size of $R_S(x)$ for all the representations $R_S(x)$ different from the greedy representation.

In order to decide if a coin system is *canonical* we have to consider all the representations of all numbers but this is not easy.
For this reason we introduce another definition of *canonical* that will be used to build the optimal coin system.

Definition 5.6. *A coin system S is "canonical2" by induction:*

- *$S = \{c\}$ is canonical2 for all $c \in \mathbb{N}_0$;*
- *$S = S' \cup \{c\}$ is canonical2 iff* $\begin{cases} S' \text{ is canonical2} \\ \forall\ x > c\ .\ |\ G_S(x)\ |<|\ G_{S'}(x)\ | \end{cases}$

With the second definition of *canonical* it is easier to compare different coin systems because we always use the same kind of representation that is the greedy representation.

Now our goal is to build a *canonical*2 coin system and from now on we will use the word *canonical* instead of canonical2.
Let us begin by the simplest case: a set with only one element.

Theorem 5.1. *The unitary coin* 1 *must belong to the canonical coin system* S *in order to represent any natural number.*

Proof. Let us assume that $1 \notin S$. If $1 \notin S$ then the natural number $n = 1$ cannot be represented with the coin system S, so 1 must belong to S. $\square$

Then $S_1 = \{1\}$ and by definition is canonical.

Now we have to increase the set S by adding another element a. There is no condition on how to chose a except it must be a natural number greater than one.
In fact we can substitute $a-$unitary coins with one-a coin. Hence

$$\forall a \in \mathbb{N}_0 \mid a > 1, \quad \forall x > a \qquad \mid G_{S_2}(x) \mid < \mid G_{S_1}(x) \mid$$

which means that S_2 is canonical.

Theorem 5.2. *The coin system* $S_2 = \{1, a\}$ *is canonical for any natural number* $a > 1$.

Let us proceed by adding another element b, with $b > a$, to the set of coins S in a such way that the coin system is canonical.
We would like to find a test to check if the addition of a natural number b to S_2 makes the coin system canonical. A first result is the following theorem.

Theorem 5.3. *Given* $S_3 = \{1, a, b\}$ *with* $1 < a < b$ *natural numbers. If* S_3 *is canonical then* $b \geq 2a$.

Proof. We assume that $a < b < 2a$ then we can write $x = 2a$ with 2 coins $(a + a)$.
By hypothesis $a < b < 2a$ so we can use only one b- coin and $2a - b$ unitary coins and $2a - b$ is less then b. Therefore

$$G_{S_3}(2a) = b + (2a - b) \qquad \Longrightarrow \qquad \mid G_{S_3}(2a) \mid = 2a - b + 1$$

Moreover $2a - b + 1 > b - b + 1 = 1$ then $\mid G_{S_3}(x) \mid = 2a - b + 1 \geq 2 = \mid R_{S_3}(x) \mid$. Therefore there exists a representation of $x = 2a$ different from the greedy representation which size is greater than or equal to the size of the greedy one of $x = 2a$. Then S_3 is not canonical. $\square$

Lemma 5.1. *Let* $S_2 = \{1, a\}$ *and* $S_3 = \{1, a, b\}$ *with* $1 < a < b$. *Let* x *be a natural number such that* $b + 2 \leq x \leq a + b - 1$. *If* $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ *then* $\mid G_{S_3}(x - 1) \mid < \mid G_{S_2}(x - 1) \mid$.

Proof. By hypothesis $x > b$ so $x = b + (x - b)$.
By hypothesis $V - b \leqslant a - 1$ so if we want to represent it we can only use unitary coins so $\mid G_{S_3}(x - b) \mid = x - b$. Hence, we obtain that $\mid G_{S_3}(x) \mid = 1 + x - b$. Now we write x (using the Euclidean division) as a sum of $a-$coins and $1-$coins.

$$x = q \cdot a + r \qquad \Longrightarrow \qquad \mid G_{S_2}(x) \mid = q + r$$

Therefore the inequality $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ can be written as

$$x - b + 1 < q + r \tag{9}$$

We can proceed in a similar way and express $x-1$ with elements of S_3.

$$x-1 = b + (x-1-b)$$

By hypothesis $x-1-b \leqslant a-1$ so $x-1-b$ can be represented only with unitary coins so $\mid G_{S_3}(x-b-1) \mid = x-b-1$.

$$\mid G_{S_3}(x-1) \mid = 1 + V - 1 - b = x - b$$

Again we write $x-1$ as a sum of $a-$coins and $1-$coins.

$$x-1 = q_1 \cdot a + r_1 \qquad \Longrightarrow \qquad \mid G_{S_2}(x-1) \mid = q_1 + r_1$$

$$x - b < q_1 + r_1 \tag{10}$$

From (9) we have that $x-b < q+r-1$; from (10) we have that $x-b < q_1 + r_1$. Now we have to check if $q+r-1 \leqslant q_1 + r_1$ or not.

$$q + r - 1 \leqslant q_1 + r_1 \qquad \Leftrightarrow \qquad aq + ar \leqslant a + aq_1 + ar_1$$

$$\Leftrightarrow aq + r + (a-1)r \leqslant a + aq_1 + r_1 + (a-1)r_1$$

From the previous Euclidean division we know that $x = aq + r$ and $x-1 = aq_1 + r_1$. By substitution we obtain that:

$$x + (a-1)r \leqslant a + x - 1 + (a-1)r_1$$

$$(a-1)r - (a-1) - (a-1)r_1 \leqslant 0 \qquad \Longrightarrow \qquad (a-1)(r - r_1 - 1) \leqslant 0 \tag{11}$$

By hypothesis $a > 1$ hence $r - r_1 - 1$ must be less than or equal to 0 to satisfy the inequality (11). Let us consider again the two Euclidean divisions:

$$x = qa + r \qquad \Longrightarrow \qquad V - 1 = qa + r - 1$$

$$x - 1 = q_1 a + r_1$$

By transitive property it follows that $qa + r - 1 = q_1 a + r_1$. That is equivalent to

$$qa - q_1 a = r_1 - r + 1 \qquad \Leftrightarrow \qquad a(q - q_1) = r_1 + 1 - r \tag{12}$$

We know that $q \geq q_1$, it follows that $a(q-q_1) \geqslant 0$. We then substitute in (12), leading to

$$r_1 + 1 - r \geqslant 0 \Longrightarrow r - r_1 - 1 \leqslant 0$$

So (11) is true, thus if $\mid G_{S_3}(V) \mid < \mid G_{S_2}(V) \mid$ then $\mid G_{S_3}(V-1) \mid < \mid G_{S_2}(V-1) \mid$. □

Theorem 5.4. *Given* $S_2 = \{1, a\}$ *and* $S_3 = \{1, a, b\}$ *with* $1 < a < b$, $\mid G_{S_3}(a+b-1) \mid < \mid G_{S_2}(a+b-1) \mid$ *iff* $b > a^2 - a + 1 - (a-1)r$ *where* r *is the remainder of the Euclidean division between* $(a+b-1)$ *and* a.

Proof. The necessary coins to express $a+b-1$ with the system S_3 are $1b-$coin and $a-1$ unitary coins, so $\mid G_{S_3}(a+b-1) \mid = a$. Let us now consider $\mid G_{S_2}(a+b-1) \mid$. We divide $a+b-1$ by a in order to see how many a-coins we need to use.

$$a + b - 1 = q \cdot a + r$$

The remainder r is the number of unitary coins needed. It follows that $\mid G_{S_2}(a+b-1) \mid = q+r$ and so the inequality $\mid G_{S_3}(a+b-1) \mid < \mid G_{S_2}(a+b-1) \mid$ is equivalent to $a < q+r$. From this last inequality we can get to the condition on b.

$$a < q + r \qquad \Longrightarrow \qquad a^2 < aq + ar \Longrightarrow a^2 < aq + r + (a-1)r$$

We can notice that $aq + r$ is equal to $a + b - 1$ so we can substitute it in the inequality and obtain the final condition

$$b > a^2 - a + 1 - (a-1)r$$

□

Theorem 5.5. *Given a system of coins $S_3 = \{1, a, b\}$ with $1 < a < b$ and $S_2 = \{1, a\}$ if $\mid G_{S_3}(a+b-1) \mid < \mid G_{S_2}(a+b-1) \mid$ then S_3 is canonical.*

Proof. We have already seen that S_2 is canonical. Now we have to prove that $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ for all $x > b$. We are going to consider tree different cases:
Let x denote an integer greater than b.

1. if x is such that $b+2 \leq x \leq a+b-1$ and $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ then $\mid G_{S_3}(x-1) \mid < \mid G_{S_2}(x-1) \mid$

   This first case has been proven by lemma 5.1. Then, from the hypothesis $\mid G_{S_3}(a+b-1) \mid < \mid G_{S_2}(a+b-1) \mid$ we can state that $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ for all the natural numbers x such that $b+2 \leq x \leq a+b-1$. Moreover is obvious that $\mid G_{S_3}(a+b) \mid < \mid G_{S_2}(a+b) \mid$ and $\mid G_{S_3}(b+1) \mid < \mid G_{S_2}(b+1) \mid$ therefore $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ for all x such that $b+1 \leq x \leq a+b$.

2. if x is such that $b+1 \leq x \leq a+b-1$ and $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ then $\mid G_{S_3}(x+\lambda a) \mid < \mid G_{S_2}(x+\lambda a) \mid$ for all the natural numbers λ such that $x + \lambda a \leq 2b - 1$

   Let x be such that $b \leq x \leq a+b-1$ and λ a natural number such that $x + \lambda a \leq 2b-1$, we can state that $\mid G_{S_3}(x+\lambda a) \mid = \lambda + \mid G_{S_3}(x) \mid$. In fact in order to represent $x + \lambda a$ we can use only one b-coin, as well as for x, because $x + \lambda a \leq 2b - 1$.

   In an analogous way $\mid G_{S_2}(x+\lambda a) \mid = \lambda + \mid G_{S_2}(x) \mid$ If $x = qa + r$ with q and r the quotient and the remainder of the division x by a then $x + \lambda a = a(q+\lambda) + r$.

   So the representations of the natural numbers between $a+b$ and $2b-1$ are based on the representations of the natural numbers less than $a+b-1$.

   Hence the relation $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ holds for all the natural numbers x such that $b+1 \leq x \leq 2b-1$.

3. if x is such that $(k+1)b+1 \leq x+kb \leq (k+2)b-1$ and $\mid G_{S_3}(x+kb) \mid < \mid G_{S_2}(x+kb) \mid$ then $\mid G_{S_3}(x+(k+1)b) \mid < \mid G_{S_2}(x+(k+1)b) \mid$ for all the natural numbers k.

   The proof proceeds by inductions on k.

   If $k = 0$ we have to prove $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ for $b+1 \leq x \leq 2b-1$, but we have already done it in the second case.

   Now we assume that $\mid G_{S_3}(x+kb) \mid < \mid G_{S_2}(x+kb) \mid$. It is clear that $\mid G_{S_3}(x+(k+1)b) \mid = 1 + \mid G_{S_3}(x+kb) \mid$.

   There exist q_1, q_2, r_1, r_2 such that $x + kb = q_1 a + r_1$ and $b = q_2 a + r_2$ with $r_1 < a$ and $r_2 < a$.

   - If $r_1 + r_2 < a$ then $x + (k+1)b = (q_1+q_2)a + (r_1+r_2)$ and so $\mid G_{S_2}(x+(k+1)b) \mid = q_1+q_2+r_1+r_2$ and $\mid G_{S_2}(x+kb) \mid = q_1 + r_1$.

Hence, considering that $q_2 \geq 1$ and $r_2 \geq 0$,

$$\mid G_{S_3}(x+(k+1)b) \mid = 1 + \mid G_{S_3}(x+kb) \mid < 1 + \mid G_{S_2}(x+kb) \mid$$

$$= 1 + q_1 + r_1 < q_1 + q_2 + r_1 + r_2 = \mid G_{S_2}(x+(k+1)b) \mid$$

- If $r_1 + r_2 \geq a$ then $\mid G_{S_2}(x+(k+1)b) \mid = (q_1+q_2+1)a + (r_1+r_2-a)$.
  First of all we can prove that $q_2 + r_2 - a \geq 0$ in fact it is equivalent to $a^2 \geq aq_2 + r_2 + (a-1)r_2 = b + (a-1)r_2$ such as $b > a^2 - (a-1)r_2$. By hypothesis and by the theorem 5.4, $b > a^2 - (a-1)(1+r_3)$ with r_3 the remainder of the division of $(b-1)$ by a. Then $b \geq a^2 - (a-1)(1+r_3)$.
  The number b can not be a multiple of a because otherwise $r_2 = 0$, and so $r_1 + r_2 < a$ leading to $r_2 = 1 + r_3$. Then $b \geq a^2 - (a-1)(r_2)$ hence $q_2 + r_2 - a \geq 0$. Therefore

$$\mid G_{S_3}(x+(k+1)b) \mid = 1 + \mid G_{S_3}(x+kb) \mid < 1 + \mid G_{S_2}(x+kb) \mid$$
$$= 1 + q_1 + r_1 \leq q_1 + q_2 + 1 + r_1 + r_2 - a = \mid G_{S_2}(x+(k+1)b) \mid$$

Therefore $\mid G_{S_3}(x) \mid < \mid G_{S_2}(x) \mid$ for all x greater than b. □

So we obtain this theorem:

Theorem 5.6. *Given a coin system $S_3 = \{1, a, b\}$ with $1 < a < b$ is canonical iff $b > a^2 - a + 1 - (a-1)r$ where r is the remainder of the Euclidean division between $(a+b-1)$ and a.*

Example 5.3. *Let $C = \{1, 3, 8\}$ be a coin system. The first condition that we have to check is $b \geq 2a$ and $8 \geq 6$ so it is ok. Then we verify the second condition on b that is $b > a^2 - a + 1 - (a-1)r$.*

$$8 > 9 - 3 + 1 - 2 \cdot 1 = 5$$

$$\mid G_{S_3}(10) \mid = 3 < 4 = \mid G_{S_2}(10) \mid$$

Consequently, the coin system C is canonical.

We tried to extend this theorem to four-coin systems and to look for a condition to check in order to state if the coin system is canonical or not. But we found this counterexample.

Counterexample 5.1 *Given $S_4 = \{1, 5, 14, 38\}$ and $S_3 = \{1, 5, 14\}$ we can see that $\mid G_{S_4}(c+b-1) \mid < \mid G_{S_3}(c+b-1) \mid$:*

$$c + b - 1 = 38 + 14 - 1 = 51$$

$$G_{S_4}(51) = 1 \cdot 38 + 2 \cdot 5 + 3 \cdot 1 \implies \mid G_{S_4}(51) \mid = 6$$
$$G_{S_3}(51) = 3 \cdot 14 + 1 \cdot 5 + 4 \cdot 1 \implies \mid G_{S_3}(51) \mid = 8$$

However S_4 is not canonical, in fact $\mid G_{S_4}(47) \mid > \mid G_{S_3}(47) \mid$:

$$G_{S_4}(47) = 1 \cdot 38 + 1 \cdot 5 + 4 \cdot 1 \implies \mid G_{S_4}(47) \mid = 6$$
$$G_{S_3}(47) = 3 \cdot 14 + 1 \cdot 5 \implies \mid G_{S_3}(47) \mid = 4$$

We have not been able to find a method to verify if a four-coin system is canonical but we proved some other theorems about particular coins systems.

5.1 Particular results

We studied some sets of coins and we achieved the following results.

Theorem 5.7. *The coin system $S = \{1, a, b\}$ with $1 < a < b$ is canonical for every $b > a^2 - a + 1$.*

Proof. By theorem (5.6) we know that the coin system $S = \{1, a, b\}$ is canonical iff $b > a^2 - a + 1 - (a-1)r$, with r the remainder of the euclidean division between $b-1$ and a. Given that $(a-1)r \geq 0$ we can say that

$$a^2 - a + 1 - (a-1)r \leq a^2 - a + 1$$

So if $b > a^2 - a + 1$ then the coin system $S = \{1, a, b\}$ is canonical.

□

From this theorem we can understand that for any $a > 1$ there are infinitely many b that form canonical coin systems $\{1, a, b\}$ and so there are infinitely many canonical three-coin systems.

Theorem 5.8. *The coin system $S = \{1, 2, b\}$ is canonical for every $b \geq 4$.*

Proof. In this case $a = 2$, so

$$b > 4 - 2 + 1 - r \qquad \Longrightarrow \qquad b > 3 - r$$

The smaller value for r is 0 so the biggest value for $3-r$ is 3. The condition $b > 3-r$ is always verified because b must be bigger than 4. Then by theorem (6.3) the coin system $S = \{1, 2, b\}$ is canonical. □

Theorem 5.9. *The coin system $C = \{1, a, ka\}$ with $a \in \mathbb{N}_0$, $a > 1$, $k \in \mathbb{N}_0$, $k > 1$, is canonical.*

Proof. From the theorem (6.3) we obtained that if b is greater than $a^2 - a + 1 - (a-1)r$ with r the remainder of the division between $a + ka - 1$ and a then the coin system considered is canonical. In this case the remainder r is equal to $a - 1$ and $b = ka$ so

$$ka > a^2 - a + 1 - (a-1)(a-1)$$
$$ka > a^2 - a + 1 - a^2 + 2a - 1$$
$$ka > a$$

which holds for $k > 1$ and $a > 1$. □

Theorem 5.10. *Given $S_4 = \{1, a, b, c\}$ with $1 < a < b < c$ natural numbers. If S_4 is canonical then $c \geq 2b$.*

Proof. We suppose by contradiction that $b < c < 2b$ then we can write the number $x = 2b$ with 2 coins $(b+b)$. The greedy representation uses the coin c and at least another coin. So, as we have seen in the theorem (5.3), there exists a representation R such that $\mid R_{S_4}(x) \mid \leq \mid G_{S_4}(x) \mid$. □

Theorem 5.11. *Given a system of coins $S_4 = \{1, a, b, c\}$, $S_3 = \{1, a, b\}$ and $m = LCM(b, c)$, for all $x > c$ if $\mid G_{S_4}(x) \mid < \mid G_{S_3}(x) \mid$ then $\mid G_{S_4}(x+m) \mid < \mid G_{S_3}(x+m) \mid$.*

Proof. Let us consider the first inequality. If we want to represent x under S_4 we got that

$$x = q_1 c + q_2 b + q_3 a + r_3 \qquad \Longrightarrow \qquad \mid G_{S_4}(x) \mid = q_1 + q_2 + q_3 + r_3$$

Given that m is by definition a multiple of c the remainder of the division between m and c is zero.

$$\mid G_{S_4}(m) \mid = \frac{m}{c}$$

This means that if we add m to x in the representation of $x+m$ the number of $c-$coins used will increase.

$$x + m = q_4 c + q_2 b + q_3 a + r_3$$

$$\mid G_{S_4}(x+m) \mid = q_4 + q_2 + q_3 + r_3$$

with $q_4 = q_1 + \mid G_{S_4}(m) \mid = q_1 + \frac{m}{c}$.
Then we consider the representations of x and $x+m$ under S_3.

$$x = q_5 b + q_6 a + r_6 \qquad \Longrightarrow \qquad \mid G_{S_3}(x) \mid = q_5 + q_6 + r_6$$

As in the previous case, given that m is by definition a multiple of b the remainder of the division between m and b is zero and so we got to the following representation.

$$x + m = q_7 b + q_6 a + r_6$$

$$\mid G_{S_3}(x+m) \mid = q_7 + q_6 + r_6$$

with $q_7 = q_5 + \mid G_{S_3}(m) \mid = q_5 + \frac{m}{b}$.
Finally we substitute in the inequality and we find

$$\begin{aligned} \mid G_{S_4}(x+m) \mid &= q_4 - q_1 + \mid G_{S_4}(x) \mid = \frac{m}{c} + \mid G_{S_4}(x) \mid \\ &< \frac{m}{c} + \mid G_{S_3}(x) \mid < \frac{m}{b} + \mid G_{S_3}(x) \mid = \mid G_{S_3}(x+m) \mid \end{aligned}$$

□

The coin system $S_{n+1} = \{1, a, 2a, 3a, ...na\}$ is not canonical. In fact we can see it in the following example.

Example 5.4. *Let $S_4 = \{1, 3, 6, 9\}$ and $n \in \mathbb{N}_0$ such that $n > 3a$, for example $n = 14$.*

$$14 = 9 + 3 + 1 + 1 \qquad |G_{S_4}(n)| = 4$$

$$14 = 6 + 6 + 1 + 1 \qquad |R_{S_4}(n)| = 4$$

The coin system made of 1 and a multiples is not canonical because the number of coins used to express n with the greedy method ($G_{S_4}(n)$) is not less than the number of coins used by another method ($R_{S_4}(n)$).

It is interesting to notice that even if, as shown before $\{1, a, ka\}$ is canonical, the set $\{1, a, 2a, 3a, ..., na\}$ with $a \in \mathbb{N}_0$, $a > 1$, $n \in \mathbb{N}_0$, $n \geq 3$ is not canonical.
However we proved that:

Theorem 5.12. *Let $S_4 = \{1, a, b, kb\}$ with $S_3 = \{1, a, b\}$ canonical and $k \in \mathbb{N}$, $k > 1$. Then S_4 is canonical.*

Proof. Let $x \in \mathbb{N}$ such that $x > kb$,

$$G_{S_4}(x) = q_1 \cdot kb + q_2 b + (x - q_1 \cdot kb - q_2 b) \qquad \Longrightarrow \qquad \mid G_{S_4}(x) \mid = q_1 + q_2 + \mid G_{S_4}(x - q_1 \cdot kb - q_2 b) \mid$$

$$G_{S_3}(x) = (q_1 k + q_2) \cdot b + (x - (q_1 k + q_2) \cdot b) \Longrightarrow \mid G_{S_3}(x) \mid = q_1 k + q_2 + (x - (q_1 k + q_2) \cdot b) + \mid G_{S_3}(x - q_1 k \cdot b - q_2 b) \mid$$

Given that $\mid G_{S_4}(x - q_1 \cdot kb - q_2 b) \mid = \mid G_{S_3}(x - q_1 k \cdot b - q_2 b) \mid$ and $k > 1$, $|G_{S_4}(x)| < |G_{S_3}(x)|$ so the coin system S_4 is canonical. □

We give another result:

Theorem 5.13. *The coin system $S_{n+1} = \{1, a, a^2, ..., a^n\}$ is canonical for all $a > 1$.*

Proof. Let $x \in \mathbb{N}_0$ such that $x > a^n$,

$$G_{S_{n+1}}(x) = q \cdot a^n + (x - q \cdot a^n) \qquad \Longrightarrow \qquad | G_{S_{n+1}}(x) |= q+ | G_{S_{n+1}}(x - q \cdot a^n) |$$

$$G_{S_n}(x) = qa \cdot (a^{n-1}) + (x - q \cdot a(a^{n-1})) \qquad \Longrightarrow \qquad | G_{S_n}(x) |= qa+ | G_{S_n}(x - q \cdot a(a^{n-1})) |$$

Given that $| G_{S_{n+1}}(x - q \cdot a^n) |=| G_{S_n}(x - q \cdot a(a^{n-1})) |$ and $a > 1$, $|G_{S_{n+1}}(x)| < |G_{S_n}(x)|$ so the coin system S_{n+1} is canonical. □

6 Comparing different coin systems

We proved that there are infinite canonical coin systems made of three or four elements.
In order to compare them with each other and to define which coin system is the best, we used the C++ language to create a function, which we have called **cost function**. The reason is given an initial set of coins it returns two values: the first one is the mean of coins enabling us to express all the values from 1 to 100 with the Greedy Method and the second one is the greater number of coins used during this process.
Through these results we could create a relation between different coin systems and define which is the best. In particular we tried to compare a coin system made of the first three elements of the Euro system with a coin system made of the first three elements of the american one.
As shown in the following table these coin systems are not the best if we look at the values coming from the cost function and also that exists another coin system which has the mean of coins used and the maximum number of coins used less than the other two coin systems.

	S	$Mean$	Max
	$\{1, 5, 22\}$	5.26	7
European	$\{1, 2, 5\}$	10.7	21
American	$\{1, 5, 10\}$	7	14

We compared also different coin systems with cardinality equal to four and we found out that there is an S better than the coin systems made of the first four elements of the Euro and the american coin system.

	S	$Mean$	Max
	$\{1, 3, 11, 38\}$	4.1	5
European	$\{1, 2, 5, 10\}$	6.2	12
American	$\{1, 5, 10, 25\}$	4.7	9

This is only the first part of a deeper research: we could continue our study by analysing sets of bigger cardinality or sets of different cardinality between them. However we recognised that the use of a coin of 22 or 38 is more laborious and it would make the daily calculations too difficult.

7 Open problems

7.1 Cardinality of $n > 3$ sets

In the case $n = 3$ we obtained the formulas for the progression with the quickest increase in cardinality of the set A_n and all the other ones that describe the slower progressions one gets exiting from the main branch of the tree at p-step.
On the other hand for $n > 3$ only formulas for the quickest and the slowest progressions have been guessed but we don't know what happens in between these two cases.

7.2 Extension of the geometric method

The geometric method can be extended to $n > 3$ following an analogous reasoning.
For example, it can be easily guessed that for $n > 3$ it is necessary to intersect $n - 1$ hyperplanes in an hyperspace of n dimension and so on.

7.3 Equivalence of the definitions of *canonical*

In the fifth chapter we considered two different ways to define a canonical coin system.

Definition 7.1. *The set of coins S is **canonical1** iff for every $x \in \mathbb{N}_0$ and for every $P_S(x) \neq G_S(x)$ it is* $\mid G_S(x) \mid < \mid P_S(x) \mid$

Definition 7.2. *The set of denomination S is defined* canonical2 *by induction:*

- $S = \{c\}$ *is canonical2 for every* $c \in \mathbb{N}_0$.
- $S = S' \cup \{c\}$ *is canonical2 iff* $\begin{cases} S' \text{ is canonical2} \\ \forall\ x > c\ .\ \mid G_S(x) \mid < \mid G_{S'}(x) \mid \end{cases}$

We tried to prove that the two definitions are equivalent. We proved that:

Theorem 7.1. *The following recurrences characterize the partitions P_S and G_S:*

$$P_{\{c\}}(x) = G_{\{c\}}(x) \qquad |P_{\{c\}}(x)| = |G_{\{c\}}(x)| = \frac{x}{c} \qquad \textit{whenever} \quad x \,\%\, c = 0$$

$$G_S(x) = (\ G_{S'}(x \,\%\, c)\ ,\ \left\lfloor \frac{x}{c} \right\rfloor\ ) \qquad |G_S(x)| = |G_{S'}(x \,\%\, c)| + \left\lfloor \frac{x}{c} \right\rfloor$$

$$P_S(x) = (\ P_{S'}(x - a \cdot c)\ ,\ a\ ) \qquad |P_S(x)| = |P_{S'}(x - a \cdot c)| + a \qquad \textit{where} \quad a \in \{0 \ldots \left\lfloor \frac{x}{c} \right\rfloor\}$$

Proof. 1. Of course, when c is the only currency available, there is at most one partition possible (i.e. when c covers the amount x).
2. The greedy method uses all the $\lfloor \frac{x}{c} \rfloor$ possible coins c in order to pay the amount x; the remainder $x \,\%\, c$ is paid using the other currencies in S', again with the greedy method.
3. In general, any partition P_S can use the currency c any number of times a ranging from 0 to $\lfloor \frac{x}{c} \rfloor$; the remainder $x - a \cdot c$ is paid using the other currencies, recursively.
The computation of the respective cardinality is straightforward. □

Theorem 7.2. *Let $S = S' \cup \{c\}$. If S is canonical1 then S' is canonical1.*

Proof. Suppose S canonical1. Then by definition for every amount x and every partition $P_S(x)$ different from the greedy one, we have $|G_S(x)| < |P_S(x)|$.
By the previous theorem, we can rewrite the last inequality as:

$$\mid G_{S'}(x \,\%\, c) \mid + \left\lfloor \frac{x}{c} \right\rfloor < \mid P_{S'}(x - a \cdot c) \mid + a \quad \text{for every } 0 \leq a \leq \left\lfloor \frac{x}{c} \right\rfloor$$

When $a = \lfloor \frac{x}{c} \rfloor$, it must be $P_{S'}(x) \neq G_{S'}(x)$ (otherwise $P_S(x) = G_S(x)$), and:

$$\mid G_{S'}(x \,\%\, c) \mid + \left\lfloor \frac{x}{c} \right\rfloor < \mid P_{S'}(x - \left\lfloor \frac{x}{c} \right\rfloor \cdot c) \mid + \left\lfloor \frac{x}{c} \right\rfloor$$

that is $\mid G_{S'}(x \,\%\, c) \mid < \mid P_{S'}(x \,\%\, c) \mid$.

□

Theorem 7.3. *S is canonical1 iff S is canonical2.*

Proof. The proof proceeds by induction on $|S|$:

1. When $S = \{c\}$ both S canonical1 and S canonical2 hold true.

2. As usual, call $S = S' \cup \{c\}$. By inductive hypothesis it is S' canonical1 iff S' canonical2. We prove the two directions separately:

$\Rightarrow$) If S is canonical1 then S' is canonical1 (by the previous theorem) and hence S' canonical2, by inductive hypothesis. Moreover, for every $x > c$ take $P_S(x) := G_{S'}(x)$ which is surely different form $G_S(x)$ (as it uses c while $P_S(x)$ does not).
By definition of canonical1 it is $|G_S(x)| < |G_{S'}(x)|$, and hence S is canonical2.

$\Leftarrow$) Suppose S is not canonical1, and prove it is not canonical2.
In the case S' is not canonical1 then by inductive hypothesis it is not canonical2, and therefore neither S can be canonical2.

Otherwise we are in the case S' is canonical1, while S is not; then there exists a value x and some partition $P_S(x) \neq G_S(x)$ such that $|G_S(x)| \geq |P_S(x)|$. This means that using coins smaller than c in order to pay x results in a optimal partition. Suppose wlog[1] c is used only once by G_S (and hence not used by P_S). Then we can rephrase the inequality as:
$\mid G_S(x) \mid \geq \mid P_{S'}(x - 0 \cdot c) \mid + 0$, and composing with $\mid P_{S'}(x) \mid > G_{S'}(x) \mid$ (by hypothesis S canonical1), we get the desired result.

$\square$

To complete the proof it is necessary to prove that the two definitions are equivalent for all $x \in \mathbb{N}$.

7.4 Four-coins systems

Given a system of coins $S_4 = \{1, a, b, c\}$ with $1 < a < b < c$ we already saw that the check on the number $c + b - 1$ is not enough to prove that S_4 is canonical. In fact the greedy method might give the best representation for $c + b - 1$ but not for a value less than $c + b - 1$ as we saw in the previous counterexample (5.1).
We suppose that the check should be done only on $c+b-1$, $c+b-a$, $c+b-2a$, ... , $c+b-ka$ with $k < \dfrac{b-1}{a}$.

Example 7.1. *Given $S_4 = \{1, 5, 14, 38\}$ and $S_3 = \{1, 5, 14\}$, we have that $c + b - 1 = 51$.*

$$\mid G_{S_4}(51) \mid = 6 < 8 = \mid G_{S_3}(51) \mid$$

In this case $k < \dfrac{13}{5}$ so we need to check just for $k = 1$ and $k = 2$.

$$c + b - a = 47 \qquad \Longrightarrow \qquad \mid G_{S_4}(47) \mid = 6 > 4 = \mid G_{S_3}(47) \mid$$

$$c + b - 2a = 42 \qquad \Longrightarrow \qquad \mid G_{S_4}(42) \mid = 5 > 3 = \mid G_{S_3}(42) \mid$$

So the coin system $S_4 = \{1, 5, 14, 38\}$ is not canonical.

Acknowledgement

We thank Alberto Meneghello for sharing his computer program and for his valuable and numerous suggestions that greatly improved the quality of the article.

[1]Otherwise we could find another $x' = x - hc$ for some h for which the assumption holds.

Bibliography

- Kozen, D. and Zaks, S., Optimal bounds dor the change-making problems, Theoretical Computer Science 123 (1994), 377-388.
- Niewiarowska, A. and Adamamaszek, M., Combinatorics of the change-making problem, University of Warsaw, Department of Mathematics, Informatics and Mechanics, Banacha 2, 2-97, Warsaw, Poland.
- Xuan, C., Canonical coin systems for change-making problems, Shangai Jiao Tong University, Department of Computer Science and Engineering, China.
- Cowen, L.J., Cowen, Robert and Steinberg, Arthur, Totally greedy coin sets and greedy obstructions (2008), Queens College, Department of Mathematics, CUNY.
- Pearson, David, A polynomial-time algorithm for the change-making problem (1994), Cornell University, Department of Computer Science, Ithaca, New York, USA.
- Shallit, Jeffrey, What this country needs in an 18 piece (2003), University of Waterloo, Department of Computer Science, Waterloo, Ontario, Canada.

Editing Notes

[1] And given any element of $A(n)_{k+1}$ other then the greatest one, expressed as a sum of a term from $A(n)_1$ and a term from $A(n)_k$, the next element is obtained by adding d to either one of these terms, so $A(n)_{k+1}$ is still an arithmetic progression with common difference d.
[2] The results in this paragraph are presented as observations. The reader may try to prove them.
[3] In fact for every set $A(3)_1$ with 3 elements there exist natural integers p and q satisfying the requirements of the exit condition, and thus the cardinalities leaves the quickest progression. Indeed, since $(a_3-a_2)a_1+(a_2-a_1)a_3 = a_3a_1-a_2a_1+a_2a_3-a_1a_3 = (a_3-a_1)a_2$ and $a_2-a_1 = (a_3-a_1)-(a_3-a_2)$, if we let $p = a_3-a_1$ and $q = a_3-a_2$ we obtain two natural integers satisfying (2); we can then divide p and q by their greatest common divisor to get $(p,q) = 1$.
[4] So, the result below, $|A(3)_{k,2}| = 2k+1$, is the same as that of Theorem 2.1 in the case $n = 3$.
[5] Of course, the formula cannot hold for all k. The computation above is done for k starting at the exit step p, but the result still holds for $k = p-1$ since the second sum is null, and also for $k = p-2$ since the second sum takes the value $-p$ which cancels the last term of the first sum.
[6] $\mathbb{N}_0$ denotes the set $\mathbb{N} \setminus \{0\}$ of positive integers.