

# COMBINATORICS OF THE CHANGE-MAKING PROBLEM

ANNA NIEWIAROWSKA, MICHAŁ ADAMASZEK\*

**ABSTRACT.** We investigate the structure of the currencies (systems of coins) for which the greedy change-making algorithm always finds an optimal solution (that is, a one with minimum number of coins). We present a series of necessary conditions that must be satisfied by the values of coins in such systems. We also uncover some relations between such currencies and their sub-currencies.

## 1. INTRODUCTION

In the change-making problem we are given a set of coins and we wish to determine, for a given amount  $c$ , what is the minimal number of coins needed to pay  $c$ . For instance, given the coins 1, 2, 5, 10, 20, 50, the minimal representation of  $c = 19$  requires 4 coins ( $10 + 5 + 2 + 2$ ).

This problem is a special case of the general knapsack problem with all coins of unit weights. In some cases the solution may be found by a greedy strategy that uses as many of the largest coin as possible, then as many of the next one as possible and so on. This greedy solution is optimal for the set of coins given above, but fails to be optimal in general. For instance, if we have coins 1, 5, 9, 16, then the amount 18 will be paid greedily as  $16 + 1 + 1$ , while the optimal solution ( $9 + 9$ ) requires just two coins. In this paper we shall concentrate on the combinatorial properties of those sets of coins for which the greedy solution is always optimal.

The sequence  $A = (a_0, a_1, \dots, a_k)$ , where  $1 = a_0 < a_1 < \dots < a_k$  will be called a *currency* or *coinage system*. We always assume  $a_0 = 1$  is the smallest coin to avoid problems with non-representability of certain amounts. For any amount  $c$  by  $\text{opt}_A(c)$  and  $\text{grd}_A(c)$  we denote, respectively, the minimal number of coins needed to pay  $c$  and the number of coins used when paying  $c$  greedily (for example, if  $A = (1, 5, 9, 16)$  then  $\text{opt}_A(18) = 2$  and  $\text{grd}_A(18) = 3$ ). The currency  $A$  will be called *orderly*<sup>1</sup> if for all amounts  $c > 0$  we have  $\text{opt}_A(c) = \text{grd}_A(c)$ .

If a coinage system  $A$  is not orderly then any amount  $c$  for which  $\text{opt}_A(c) < \text{grd}_A(c)$  will be called a *counterexample*.

Let us briefly summarize related work. Magazine, Nemhauser and Trotter [1] gave a necessary and sufficient condition to decide whether  $A = (1, a_1, \dots, a_{k+1})$  is orderly provided we know in advance that  $A' = (1, a_1, \dots, a_k)$  is orderly, the so-called one-point theorem (see section 2 of the present paper). Kozen and Zaks [6] proved, among other things, that the smallest counterexample (if exists), does not exceed the sum of

1991 *Mathematics Subject Classification.* Primary 05D99, Secondary 68R05.

\* University of Warsaw, Dept. of Mathematics, Informatics and Mechanics, ul. Banacha 2, 02-097 Warsaw, Poland, email: {annan, aszek}@mimuw.edu.pl.

<sup>1</sup>Various authors have used the terms orderly [4, 5], canonical [6, 7], standard [3] or greedy [9].

the two highest coins. They also asked if there is a polynomial-time algorithm that tests if a coinage system is orderly. Such an algorithm was presented by Pearson [7]. It produces a set of  $O(k^2)$  “candidates for counterexamples”, which is guaranteed to contain the smallest counterexample if one exists. The rest of the algorithm is just testing these potential candidates, and the overall complexity is  $O(k^3)$ . A similar set of possible counterexamples (perhaps not containing the smallest one), but of size  $O(k^3)$ , was given by Tien and Hu in [3] (see formula (4.20) and Theorem 4.1 of that paper). It leads to an  $O(k^4)$  algorithm. The authors of [1] and [3] were concentrating mainly on the error analysis between the greedy and optimal solutions. Apparently Jones [4] was the only one who attempted to give a neat combinatorial condition characterizing orderly currencies, but his theorem suffered from a major error, soon pointed out by Maurer [5]. Our paper has been paralleled by an independent work of Cowen, Cowen and Steinberg [9] about currencies whose all prefixes are orderly and about non-orderly currencies which cannot be “fixed” by appending extra coins. The results contained in section 4 and a special case ( $l = 2$ ) of Theorem 3.5 of this paper have also been proved in [9].

The aim of this paper is to study some orderly coinage systems from a combinatorial viewpoint, motivated by the need to have some nice characterization. One of the motivations was the observation that *if  $A = (1, a_1, a_2, \dots, a_k)$  is an orderly currency, then the currency  $(1, a_1, a_2)$  is also orderly*, that will be generalized and proved in Theorem 3.5. Going further, one may start with an orderly currency, take out some of its coins and ask if the remaining coins again form an orderly currency. The precise answer to this question, given in section 7, will be a consequence of the results of sections 3 and 5, where we prove some properties of the distances  $a_j - a_i$  between the coins of an orderly currency. In section 4 these results will be used to give a complete description of orderly currencies with less than 6 coins. In section 6 we study the behaviour of the currencies obtained as prefixes of an orderly currency. Some closing remarks and open problems are included in section 8.

## 2. PRELIMINARY RESULTS

If  $A = (1, a_1, \dots, a_k)$  is a currency it will often be convenient to set  $a_{k+1} = \infty$ . This will be especially useful whenever we want to choose, say, the first interval  $[a_m, a_{m+1}]$  of length at least  $d$  for some  $d$ . The reader will see that in all applications the infinite interval will be as useful as proper intervals.

There are three standard arguments that will be used repeatedly throughout this paper, so we quote them now to avoid excessive repetitions in the future. All the time we assume  $A = (1, a_1, \dots, a_k)$  is orderly.

First, suppose we have  $a_m$ ,  $a_i$  and  $a_l$ , such that  $a_l < a_m + a_i < a_{l+1}$ . Then  $a_m + a_i$  has a representation that uses 2 coins. Since  $a_m + a_i$  is strictly between  $a_l$  and  $a_{l+1}$  its greedy representation must start with  $a_l$ , followed (since  $A$  is orderly) by just one other coin  $a_r$ . It follows that there exists  $r$  such that  $a_m + a_i = a_l + a_r$ .

The second argument is a slight modification of the first one; namely, if  $a_l < a_m + a_i$  and the number  $a_m + a_i - a_l$  is not one of the coins, then  $a_{l+1} \leq a_m + a_i$ .

The third argument is a bit more complicated. Suppose that for some  $j > i \geq 1$  we have  $a_j - a_i = d$ . Let us choose the largest  $m$  for which  $a_m - a_{m-1} < a_i$  (such  $m$ 's exist,

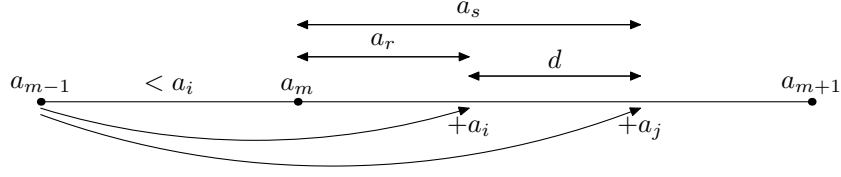


FIGURE 1. Illustration of a standard argument

for instance  $a_i - a_{i-1} < a_i$ ). Then  $a_{m+1} - a_m \geq a_i$  (here it is possible that  $a_{m+1} = \infty$ ), so we have  $a_m < a_{m-1} + a_i < a_{m+1}$ . If we also have  $a_m < a_{m-1} + a_j < a_{m+1}$  then, as before, there exist numbers  $r < i$  and  $s < j$  such that:

$$\begin{aligned} a_{m-1} + a_i &= a_m + a_r, \\ a_{m-1} + a_j &= a_m + a_s. \end{aligned}$$

Then  $a_s - a_r = a_j - a_i = d$ , so we decreased the coins' indices from  $(j, i)$  to  $(s, r)$ , keeping the difference  $d$  unchanged. Therefore, if additionally  $(j, i)$  was the *smallest* pair of indices for which  $a_j - a_i = d$ , we would have a contradiction, hence we may assume that in such case  $a_{m-1} + a_j \geq a_{m+1}$ .

We shall frequently make use of the following famous result:

**Theorem 2.1 (One-point theorem, [1, 2, 9]).** *Suppose  $A' = (1, a_1, \dots, a_k)$  is orderly and  $a_{k+1} > a_k$ . Let  $m = \lceil a_{k+1}/a_k \rceil$ . Then  $A = (1, a_1, \dots, a_k, a_{k+1})$  is orderly if and only if  $\text{opt}_A(ma_k) = \text{grd}_A(ma_k)$ .*

**Remark.** According to this theorem, if the shorter currency  $A'$  is orderly, then the optimality of the greedy solution for  $A$  needs to be checked only for the single value  $ma_k$ . This justifies the name *one-point theorem*. Note, that although in general it is NP-hard to compute  $\text{opt}_A(c)$  for arbitrary  $A$  and  $c$  (see [8] and [6] for a discussion), the one-point theorem test  $\text{opt}_A(ma_k) = \text{grd}_A(ma_k)$  runs in polynomial time, since it is equivalent to  $\text{grd}_{A'}(ma_k - a_{k+1}) \leq m - 1$ . For the sake of completeness we decided to include a short proof of the one-point theorem.

**Proof.** One of the implications is trivial. Now suppose that  $\text{opt}_A(ma_k) = \text{grd}_A(ma_k)$ . We have

$$(m - 1)a_k + 1 \leq a_{k+1} \leq ma_k.$$

For all values  $c < a_{k+1}$  all the payments  $\text{grd}_A(c)$ ,  $\text{grd}_{A'}(c)$ ,  $\text{opt}_A(c)$ ,  $\text{opt}_{A'}(c)$  coincide, so  $\text{grd}_A(c) = \text{opt}_A(c)$ . All other  $c$  will be split in two groups:  $c \in [a_{k+1}, ma_k)$  and  $c \geq ma_k$ .

**1.**  $a_{k+1} \leq c < ma_k$ . For every such  $c$  we have  $c < 2a_{k+1}$ , therefore any payment of  $c$  contains either 0 or 1 copies of  $a_{k+1}$ . Together with the orderliness of  $A'$  this implies

$$\text{opt}_A(c) = \min\{1 + \text{grd}_{A'}(c - a_{k+1}), \text{grd}_{A'}(c)\}.$$

At the same time  $1 + \text{grd}_{A'}(c - a_{k+1}) = \text{grd}_A(c)$ , so in order to prove  $\text{opt}_A(c) = \text{grd}_A(c)$  it suffices to show the inequality

$$\text{grd}_A(c) \leq \text{grd}_{A'}(c).$$

Observe that

$$\text{grd}_{A'}(c) = (m - 1) + \text{grd}_{A'}(c - (m - 1)a_k).$$

The function  $\text{grd}_{A'} = \text{opt}_{A'}$  satisfies the triangle inequality, so

$$\text{grd}_{A'}(ma_k - a_{k+1}) + \text{grd}_{A'}(c - (m-1)a_k) \geq \text{grd}_{A'}(c - a_{k+1} + a_k) = 1 + \text{grd}_{A'}(c - a_{k+1}).$$

Finally

$$\begin{aligned} \text{grd}_{A'}(c) - \text{grd}_A(c) &= (m-1) + \text{grd}_{A'}(c - (m-1)a_k) - (1 + \text{grd}_{A'}(c - a_{k+1})) \geq \\ &\geq m-2+1 - \text{grd}_{A'}(ma_k - a_{k+1}) = m-1 - \text{grd}_{A'}(ma_k - a_{k+1}). \end{aligned}$$

However

$$1 + \text{grd}_{A'}(ma_k - a_{k+1}) = \text{grd}_A(ma_k) = \text{opt}_A(ma_k) \leq m,$$

which eventually implies the desired inequality

$$\text{grd}_{A'}(c) - \text{grd}_A(c) \geq 0.$$

**2.**  $c \geq ma_k$ . Denote by  $\mathcal{OPT}(c)$  the set of optimal payments for  $c$ :

$$\mathcal{OPT}(c) = \{(x_0, \dots, x_{k+1}) : \sum_{i=0}^{k+1} x_i a_i = c \text{ and } \sum_{i=0}^{k+1} x_i \text{ is minimal}\}$$

It is sufficient to exhibit a payment  $(x_i) \in \mathcal{OPT}(c)$  with  $x_{k+1} > 0$ . Consider any optimal payment  $(x_i)$ . We may apply to it the following two operations:

- if  $x_k \geq m$  then replace  $m$  coins  $a_k$  with the greedy decomposition of  $ma_k$ . This way the number of coins in the payment does not increase (since  $\text{opt}_A(ma_k) = \text{grd}_A(ma_k)$ ), while the multiplicity of  $a_k$  in the payment decreases.
- if  $\sum_{i=0}^{k-1} x_i a_i \geq a_k$  then instead of the coins needed to pay  $\sum_{i=0}^{k-1} x_i a_i$  insert the greedy decomposition of this amount with respect to  $A'$ . This will not increase the overall number of coins (since  $A'$  was orderly), but it will decrease the amount paid with  $1, a_1, \dots, a_{k-1}$ .

It is clear that repeating these two steps sufficiently many times we will finally end up with an optimal payment  $(x_i)$  satisfying  $\sum_{i=0}^{k-1} x_i a_i < a_k$  and  $x_k < m$ . Then

$$\sum_{i=0}^k x_i a_i \leq a_k - 1 + (m-1)a_k = ma_k - 1 < c$$

hence  $x_{k+1} > 0$  in this payment.  $\square$

It is obvious that the one-coin currency  $A = (1)$  is orderly, as well as all the two-coin currencies  $A = (1, a_1)$ . The reader may now wish to solve the easy problem of when a three-coin currency  $A = (1, a_1, a_2)$  is orderly. For reasons which will become clear later we shall express the solution in terms of the following set:

**Definition 2.2.** For any  $a > 0$  we define:

$$\begin{aligned} \mathcal{A}(a) &= \bigcup_{m=1}^{\infty} \bigcup_{l=0}^m \{ma - l\} = \\ &= \{a-1, a\} \cup \{2a-2, 2a-1, 2a\} \cup \dots \cup \{ma-m, \dots, ma\} \cup \dots \end{aligned}$$

**Proposition 2.3.** The currency  $A = (1, a_1, a_2)$  is orderly if and only if  $a_2 - a_1 \in \mathcal{A}(a_1)$ .

**Proof.** Let  $m = \lceil a_2/a_1 \rceil$ . By the one-point theorem  $A$  is orderly if and only if the greedy algorithm is optimal for  $ma_1$ , which is equivalent to

$$\text{grd}_A(ma_1) \leq m$$

or

$$ma_1 - a_2 \leq m - 1$$

which means that  $a_2 - a_1 = (m - 1)a_1 - (ma_1 - a_2) \in \mathcal{A}(a_1)$  (more precisely,  $a_2 - a_1$  belongs to the  $(m - 1)$ -st summand of  $\mathcal{A}(a_1)$ ). On the other hand, if  $m$  is the least number for which  $a_2 - a_1$  belongs to the  $(m - 1)$ -th summand of  $\mathcal{A}(a_1)$ , then  $\lceil a_2/a_1 \rceil = m$  and  $a_2 - a_1 = (m - 1)a_1 - l$  for some  $l \leq m - 1$ . Then

$$\text{grd}_A(ma_1) = 1 + (ma_1 - a_2) = 1 + l \leq m$$

as required.  $\square$

### 3. INVESTIGATING DIFFERENCES, PART I

In this section we begin investigating distances between the coins of an orderly coinage system, followed by an application of these results.

**Proposition 3.1.** *If  $A = (1, a_1, \dots, a_k)$  is orderly and  $a_1 \geq 3$ , then*

$$a_i - a_{i-1} \neq 1$$

*for all  $i = 1, \dots, k$ .*

**Proof.** Suppose, on the contrary, that  $a_j - a_{j-1} = 1$  and let  $j$  be the least index with this property. Since  $a_1 \geq 3$ , we have  $j \geq 2$ .

Let us choose the largest index  $m$  for which  $a_m - a_{m-1} < a_{j-1}$ . Then  $a_{m+1} - a_m \geq a_{j-1}$ , and if  $a_{m-1} + a_j < a_{m+1}$  then we would have a contradiction by the third standard argument from section 2. Therefore  $a_{m+1} \leq a_{m-1} + a_j$ . Since  $a_{m+1} - a_m \geq a_{j-1}$ , we have

$$a_j = a_{j-1} + 1 \leq (a_{m+1} - a_m) + (a_m - a_{m-1}) = a_{m+1} - a_{m-1} \leq a_j$$

meaning that  $a_m - a_{m-1} = 1$  and  $a_{m+1} - a_m = a_{j-1}$ .

It follows that

$$a_m < a_{m-1} + a_{j-1} < a_{m+1}$$

which means that  $a_{m-1} + a_{j-1} - a_m = a_{j-1} - 1$  must be one of the coins, contradicting the minimality of  $j$ . This ends the proof.  $\square$

The previous proposition can be sharpened as follows:

**Proposition 3.2.** *If  $A = (1, a_1, \dots, a_k)$  is orderly then*

$$a_i - a_{i-1} \geq a_1 - 1$$

*for all  $i = 1, \dots, k$ .*

**Proof.** This is obviously true if  $a_1 = 2$ , so let  $a_1 \geq 3$ . Let  $j$  be the largest index for which  $a_j - a_{j-1} \leq a_1 - 2$ . By Proposition 3.1 we have  $a_j - a_{j-1} \geq 2$ . From the maximality of  $j$  we have  $a_{j+1} - a_j \geq a_1 - 1$  (it is possible that  $a_{j+1} = \infty$ ). Now consider the amount

$$c = a_{j-1} + a_1.$$

It satisfies  $a_j + 2 \leq c \leq a_j + a_1 - 2 < a_{j+1}$ , hence  $\text{opt}_A(c) = 2$ . When paid greedily,

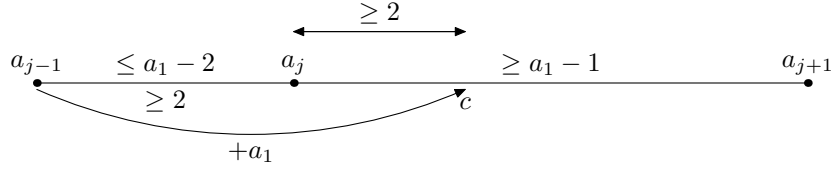


FIGURE 2. Illustration of the proof of Prop. 3.2

the amount  $c$  is decomposed to  $a_j$  and  $c - a_j$  copies of the coin 1, which makes

$$1 + (c - a_j) \geq 1 + 2 = 3$$

coins altogether. This contradicts the fact  $A$  is orderly, thus completing the proof of this proposition.  $\square$

Proposition 3.2 imposes certain restrictions on the possible differences  $a_i - a_{i-1}$ . In the next theorem we shall generalize this restriction, but first let us state without proof some obvious properties of the sets  $\mathcal{A}(a)$  that will be useful in the proof:

**Fact 3.3.** *Let  $a \geq 2$  be an integer. Then:*

- (1) *if  $x, y \in \mathcal{A}(a)$  then  $x + y \in \mathcal{A}(a)$ .*
- (2) *an integer  $x \geq 2$  does not belong to  $\mathcal{A}(a)$  if and only if there exists an integer  $p \geq 0$  such that*

$$pa + 1 \leq x \leq (p + 1)a - (p + 2).$$

- (3) *if  $p_1 < p_2 < \dots < p_m$  and  $p_m - p_1 \notin \mathcal{A}(a)$  then  $p_j - p_{j-1} \notin \mathcal{A}(a)$  for some  $2 \leq j \leq m$  (this follows from (1)).*
- (4) *if  $pa < x$  and  $x = (p + 1)a - c$  for some  $c$  (possibly negative), then  $x \in \mathcal{A}(a)$  implies  $c \leq p + 1$ .*

Now we can state the main theorem of this section:

**Theorem 3.4.** *If  $A = (1, a_1, \dots, a_k)$  is orderly then*

$$a_j - a_i \in \mathcal{A}(a_1)$$

*for all  $0 \leq i < j \leq k$ .*

**Proof.** If not then by property (3) above there exists a number  $j$  for which  $a_j - a_{j-1} \notin \mathcal{A}(a_1)$ , which is equivalent to

$$pa_1 + 1 \leq a_j - a_{j-1} \leq (p + 1)a_1 - (p + 2)$$

for some  $p$ . Among all pairs  $(p, j)$  for which these inequalities hold let us choose the lexicographically smallest one. Comparing the leftmost and rightmost expressions in this double inequality yields  $a_1 \geq p + 3$ , hence  $a_1 \geq 4$  and  $1 \leq p \leq a_1 - 3$ .

We have  $\text{opt}_A(a_{j-1} + (p + 1)a_1) \leq p + 2$  and

$$a_j + (p + 2) \leq a_{j-1} + (p + 1)a_1 \leq a_j + a_1 - 1$$

hence  $\text{grd}_{(1, \dots, a_j)}(a_{j-1} + (p + 1)a_1) \geq p + 3$ . It follows that  $a_{j+1} \leq a_{j-1} + (p + 1)a_1$ . Then

$$a_{j+1} - a_j \leq a_{j-1} + (p + 1)a_1 - a_j \leq a_1 - 1.$$

By Proposition 3.2 all these inequalities must in fact be equalities. In other words:

$$\begin{aligned} a_{j+1} &= a_{j-1} + (p+1)a_1, \\ a_j &= a_{j-1} + pa_1 + 1. \end{aligned}$$

Choose the largest  $l$  for which  $a_{l+1} - a_l \leq a_{j-1} + (p-1)a_1 + 2$  (such  $l$ 's exist, for instance  $a_{j+1} - a_j = a_1 - 1$  is sufficiently small). By maximality of  $l$  we have  $a_{l+2} - a_{l+1} \geq a_{j-1} + (p-1)a_1 + 3$  (it is possible that  $a_{l+2} = \infty$ ). Observe that

$$a_{l+2} - a_l = (a_{l+2} - a_{l+1}) + (a_{l+1} - a_l) \geq a_{j-1} + (p-1)a_1 + 3 + a_1 - 1 = a_{j-1} + pa_1 + 2 = a_j + 1$$

and

$$a_{l+1} - a_l \leq a_{j-1} + (p-1)a_1 + 3 = a_j - a_1 + 2$$

which means that

$$a_{l+1} + a_1 - 2 \leq a_l + a_j < a_{l+2}.$$

This eventually implies that  $a_l + a_j = a_{l+1} + a_r$  for some  $1 \leq r < j$ . The rest of the proof depends on the possible locations of  $a_l + a_{j-1}$ .

If  $a_l + a_{j-1} > a_{l+1}$  then the same argument yields an index  $s < j-1$  for which  $a_l + a_{j-1} = a_{l+1} + a_s$ . In that case  $a_r - a_s = a_j - a_{j-1} \notin \mathcal{A}(a_1)$ . By properties (3) and (2) of  $\mathcal{A}(a_1)$  there exist numbers  $s < r' \leq r$  and  $p'$  for which

$$p'a_1 + 1 \leq a_{r'} - a_{r'-1} \leq (p'+1)a_1 - (p'+2).$$

The inequality  $a_{r'} - a_{r'-1} \leq a_j - a_{j-1}$  implies  $p' \leq p$ . The pair  $(p', r')$  is lexicographically smaller than  $(p, j)$ , which is a contradiction since the latter was chosen to be minimal.

If, on the other hand,  $a_l + a_{j-1} = a_{l+1}$ , then  $a_l + a_j = a_l + a_{j-1} + pa_1 + 1 = a_{l+1} + pa_1 + 1$ , which means that  $a_r = pa_1 + 1$ . Then  $a_r - a_1 = (p-1)a_1 + 1 \notin \mathcal{A}(a_1)$ , contradicting the minimality of  $(p, j)$  by the same argument as above.

Therefore we are left with the case  $a_l + a_{j-1} < a_{l+1}$ . The number  $a_r$  satisfies

$$a_r = a_l + a_j - a_{l+1} < a_l + a_j - (a_l + a_{j-1}) = a_j - a_{j-1} = pa_1 + 1.$$

Since  $a_r - a_1 < (p-1)a_1 + 1$ , the minimality of  $p$  implies that  $a_r - a_1 \in \mathcal{A}(a_1)$ . It means that  $a_r = qa_1 - q'$  for some  $q \leq p$  and  $0 \leq q' < q$ .

Next we are going to show that  $a_{l+1} - (a_l + a_{j-1}) \notin \mathcal{A}(a_1)$ . Observe that

$$a_{l+1} - (a_l + a_{j-1}) = (a_l + a_j - a_r) - a_l - a_{j-1} = pa_1 + 1 - a_r = (p-q)a_1 + (1+q').$$

which is more than  $(p-q)a_1$ , while at the same time it equals:

$$(p-q+1)a_1 - (a_1 - 1 - q')$$

with  $a_1 - 1 - q' > (p+2) - 1 - q' = p+1 - q' > p-q+1$ . By property (2) the number  $a_{l+1} - (a_l + a_{j-1})$  does not belong to  $\mathcal{A}(a_1)$ .

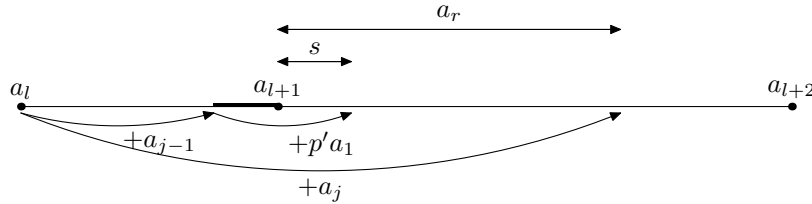


FIGURE 3. The last case of the proof. The length of the bold interval is not in  $\mathcal{A}(a_1)$ .

Now let us choose the least  $p'$  for which  $a_l + a_{j-1} + p'a_1 \geq a_{l+1}$ . In this case

$$a_l + a_{j-1} + p'a_1 < a_{l+1} + a_1 \leq a_{l+1} + a_r = a_l + a_j.$$

Obviously  $\text{opt}_A(a_l + a_{j-1} + p'a_1) \leq p' + 2$ . On the other hand, the greedy decomposition of  $a_l + a_{j-1} + p'a_1$  is  $a_{l+1} + s \cdot 1$ , where  $s = a_l + a_{j-1} + p'a_1 - a_{l+1}$ . By optimality

$$s + 1 \leq p' + 2$$

so  $s \leq p' + 1$ . On the other hand, we have already proved that  $p'a_1 - s = a_{l+1} - (a_l + a_{j-1}) \notin \mathcal{A}(a_1)$ , so  $s \geq p' + 1$ . Finally we have  $s = p' + 1$ .

To end the proof we compute  $a_r - a_1$  in terms of  $p, p'$  and  $a_1$ :

$$\begin{aligned} a_r - a_1 &= a_l + a_j - a_{l+1} - a_1 = a_l + (a_{j-1} + pa_1 + 1) - (a_l + a_{j-1} + p'a_1 - s) - a_1 = \\ &= (p - p' - 1)a_1 + (s + 1) = (p - p' - 1)a_1 + (p' + 2) = \\ &= (p - p')a_1 - (a_1 - p' - 2) \end{aligned}$$

Since  $a_r - a_1 \in \mathcal{A}(a_1)$ , by property (4) we obtain

$$\begin{aligned} a_1 - p' - 2 &\leq p - p', \\ a_1 &< p + 3. \end{aligned}$$

This contradiction ends the proof.  $\square$

As an immediate corollary we obtain the theorem announced in the introduction:

**Theorem 3.5.** *If  $A = (1, a_1, \dots, a_k)$  is orderly then for any  $2 \leq l \leq k$  the currency  $(1, a_1, a_l)$  is also orderly. In particular the currency  $(1, a_1, a_2)$  is orderly.*

**Proof.** If  $A$  is orderly then by Theorem 3.4 we have  $a_l - a_1 \in \mathcal{A}(a_1)$ . By Proposition 2.3 this is sufficient for  $(1, a_1, a_l)$  to be orderly.  $\square$

#### 4. SHORT CURRENCIES

Theorems 3.5 and 2.1 allow us to give a complete characterization of all orderly currencies with at most 5 coins. The currencies with 1, 2 and 3 coins have already been discussed. Here we concentrate on the cases of 4 and 5 coins. Following [9] call a currency  $A = (1, a_1, \dots, a_k)$  *totally orderly*<sup>2</sup> if every prefix sub-currency of the form  $(1, a_1, \dots, a_l)$  is orderly for  $l = 0, \dots, k$ .

**Proposition 4.1.** *The currency  $A = (1, a_1, a_2, a_3)$  is orderly if and only if it is totally orderly.*

**Proposition 4.2.** *The currency  $A = (1, a_1, a_2, a_3, a_4)$  is orderly if and only if*

- (1) *either  $(1, a_1, a_2, a_3, a_4) = (1, 2, a, a + 1, 2a)$  for some  $a \geq 4$ , in which case  $(1, a_1, a_2, a_3)$  is not orderly,*
- (2) *or  $A$  is totally orderly.*

**Remark.** The conditions given in the above propositions are efficiently computable, since it can be quickly checked if a currency is totally orderly (as opposed to checking whether it is just orderly). One simply repeats the one-point theorem test with for longer and longer prefixes; see also [9].

**Proof of Propositions 4.1 and 4.2.** The one-point theorem, together with Theorem 3.5 covers Proposition 4.1 and case (2) of Proposition 4.2.

---

<sup>2</sup>Also called normal in [3].



It remains to show that all orderly currencies  $(1, a_1, a_2, a_3, a_4)$  in which the sub-currency  $(1, a_1, a_2, a_3)$  is disorderly are of the form (1) from Proposition 4.2. Let  $m = \lceil a_3/a_2 \rceil$ .

The triple  $(1, a_1, a_2)$  is orderly by Theorem 3.5. By the one-point theorem  $ma_2$  is a counterexample for  $(1, a_1, a_2, a_3)$ , hence  $a_4 \leq ma_2$ . Both values  $a_3 + a_3$  and  $a_3 + a_2$  exceed  $ma_2$ , so they exceed  $a_4$ , so by optimality there must exist  $i < j \leq 2$  for which:

$$\begin{aligned} a_3 + a_2 &= a_4 + a_i, \\ a_3 + a_3 &= a_4 + a_j. \end{aligned}$$

Subtracting these equations we get

$$a_3 - a_2 = a_j - a_i < a_j \leq a_2$$

which in turn gives  $a_3 < 2a_2$ . That means  $m = 2$ .

There are two cases to consider:

$j = 2$ . Then  $a_3 - a_2 = a_2 - a_i$ , so  $2a_2 = a_3 + a_i$ , which contradicts the fact that  $(1, a_1, a_2, a_3)$  is disorderly.

$j = 1$ . Then  $i = 0$  and previous equations take the form:

$$\begin{aligned} a_3 + a_2 &= a_4 + 1, \\ a_3 + a_3 &= a_4 + a_1. \end{aligned}$$

The following computation

$$a_4 + 1 = a_3 + a_2 > 2a_2 = ma_2 \geq a_4$$

implies

$$a_4 + 1 = a_3 + a_2 = 2a_2 + 1.$$

Setting  $a_2 = a$  we get  $a_3 = a + 1$ ,  $a_4 = 2a$  and  $a_1 = 2a_3 - a_4 = 2$ .

The routine check that  $(1, 2, a, a + 1, 2a)$  is orderly resembles the technique used in the proof of case 2 of Theorem 2.1 and is left to the reader. For  $a \geq 4$  the sub-currency  $(1, 2, a, a + 1)$  is disorderly.  $\square$

Attempts to continue similar reasoning with longer coinage systems encounter a serious problem, because the applicability of the one-point theorem is limited. More precisely, the “intermediate” currencies may not be orderly even if  $A$  is orderly as we see from part (1) of Proposition 4.2. We shall return to these matters in section 6.

## 5. INVESTIGATING DIFFERENCES, PART II

In the previous sections we were discussing relation of the distances  $a_j - a_i$  and the value of  $a_1$ . Here we shall extend some of this to further coins. Note that Proposition 3.2 may be interpreted as follows: if some difference  $a_j - a_i$  belongs to the interval  $(1, a_1)$ , then it must be necessarily equal  $a_1 - 1$ . We are interested in the possible values of  $a_j - a_i$  in the cases when this difference belongs to  $(a_{m-1}, a_m)$ . **Throughout this section we always assume that  $A = (1, a_1, \dots, a_k)$  is orderly.** The key results of this sections are Corollary 5.5 and Theorem 5.6.

**Lemma 5.1.** *If*

$$a_m - a_{l+1} < a_j - a_i < a_m - a_l$$

*for some  $i < j, l < m$ , then*

$$a_{j+1} \leq a_i + a_m.$$

**Proof.** We have  $a_j + a_l < a_i + a_m < a_j + a_{l+1}$ . If there was no new coin between  $a_j$  and  $a_i + a_m$  then there would be no greedy decomposition of  $a_i + a_m$  in two steps.  $\square$

**Lemma 5.2.** *There are no numbers  $0 \leq i < j \leq k$  and  $1 \leq m \leq k$  that satisfy  $a_{m-1} \leq a_j - a_i < a_m - a_{m-1}$ .*

**Proof.** Suppose the contrary and let  $(j, i, m)$  be some triple satisfying the above inequalities, such that  $j$  is the least possible. If  $i = 0$  then  $a_{m-1} \leq a_j - 1 < a_m - a_{m-1} < a_m$ , hence  $j = m$ , which in turn implies  $a_{m-1} < 1$ , but this is not possible.

Therefore  $i \geq 1$  and we are free to choose the largest index  $l$  for which  $a_l - a_{l-1} < a_i$ . If  $a_{l-1} + a_j < a_{l+1}$  then by the standard argument we obtain a contradiction with the minimality of  $j$ . Hence  $a_{l-1} + a_j \geq a_{l+1}$ . It follows that

$$a_l - a_{l-1} = (a_{l+1} - a_{l-1}) - (a_{l+1} - a_l) \leq a_j - a_i < a_m - a_{m-1}.$$

By Lemma 5.1 it follows that  $a_{l+1} - a_{l-1} \leq a_m$ , so  $a_i < a_{l+1} - a_{l-1} \leq a_m$ . In effect  $i \leq m - 1$ . At the same time we also have  $a_j > a_{m-1}$ , so  $j \geq m$ . All this implies

$$a_j - a_i \geq a_m - a_{m-1}.$$

This contradiction ends the proof.  $\square$

**Lemma 5.3.** *Let  $m \geq 2$ . If the difference  $a_j - a_i$  belongs to the interval  $[a_m - a_1, a_m - 1]$  then it can only be one of the numbers  $a_m - a_1$ ,  $a_m - a_1 + 1$  and  $a_m - 1$ .*

**Proof.** Suppose that

$$a_m - a_1 < a_j - a_i < a_m - 1.$$

From Lemma 5.1 we get  $a_{j+1} \leq a_i + a_m < a_j + a_1$ . In this case Proposition 3.2 implies  $a_{j+1} = a_j + a_1 - 1$ . Moreover, we have

$$a_j + 2 \leq a_i + a_m \leq a_j + a_1 - 1 = a_{j+1}.$$

Hence  $a_i + a_m = a_{j+1}$  (otherwise the amount  $a_i + a_m$  would not have a greedy decomposition in two steps). Eventually we get

$$a_j - a_i = (a_{j+1} - a_1 + 1) - (a_{j+1} - a_m) = a_m - a_1 + 1.$$

$\square$

**Lemma 5.4.** *If  $a_1 < a_2 - a_1 + 1 < a_2 - 1$  then the value  $a_2 - a_1 + 1$  cannot be attained by any of the differences  $a_j - a_i$ .*

**Proof.** First note that the given inequalities imply  $a_1 \geq 3$ . Suppose that  $j$  is the minimal number for which there exists an  $i$  such that  $a_j - a_i = a_2 - a_1 + 1$ . Clearly  $i \geq 2$ . From the proof of Lemma 5.3 we know that

$$a_{j+1} = a_i + a_2 = a_j + a_1 - 1.$$

Let  $m$  be the maximal index for which  $a_m - a_{m-1} < a_i$ . Then  $a_{m+1} - a_m \geq a_i$ .

If  $a_{m-1} + a_j < a_{m+1}$  then considering the amounts  $a_{m-1} + a_i$  and  $a_{m-1} + a_j$  and their greedy decompositions we obtain a contradiction with the minimality of  $j$  in the usual way. Hence we may assume that

$$a_{m-1} + a_j \geq a_{m+1}.$$

If  $a_{m-1} + a_j = a_{m+1}$  then consider the amount  $a_{m-1} + a_{j+1}$ . It satisfies

$$a_{m-1} + a_{j+1} = a_{m+1} + a_1 - 1 < a_{m+1} + a_2 \leq a_{m+1} + a_i \leq a_{m+2}.$$

Since  $a_1 - 1 \geq 2$  this amount cannot be greedily decomposed in two steps, so we have a contradiction, which means that

$$a_{m-1} + a_j \geq a_{m+1} + 1$$

which in turn implies

$$a_m - a_{m-1} = (a_{m+1} - a_{m-1}) - (a_{m+1} - a_m) \leq a_j - 1 - a_i = a_2 - a_1.$$

We know from the previous lemmas that in this case the only possible values of the difference  $a_m - a_{m-1}$  are  $a_2 - a_1$ ,  $a_1$  and  $a_1 - 1$ . Let us investigate these cases separately.

**Case 1.**  $a_m - a_{m-1} = a_2 - a_1$ . Then  $a_{m+1} \geq a_m + a_i$  and

$$a_{m+1} \leq a_{m-1} + a_j - 1 = a_m - a_2 + a_1 + a_j - 1 = a_m + a_i$$

hence  $a_{m+1} = a_m + a_i = a_{m-1} + a_j - 1$ . Now consider the amount  $a_m + a_j$ . It satisfies  $a_m + a_j = a_m + a_i + a_2 - a_1 + 1 = a_{m+1} + a_2 - a_1 + 1 < a_{m+1} + a_2 \leq a_{m+1} + a_i \leq a_{m+2}$  so it could be decomposed greedily in two steps only if  $a_2 - a_1 + 1$  was one of the coins, which is not true by the assumptions of the lemma.

**Case 2.**  $a_m - a_{m-1} = a_1$ . Now consider the amount  $a_{m-1} + a_2$ :

$$a_m < a_{m-1} + a_2 = a_m + (a_2 - a_1) < a_m + a_i \leq a_{m+1}.$$

This amount can only be decomposed optimally if  $a_2 - a_1$  is a coin. Since  $a_1 \geq 3$ , by Proposition 3.1 we have  $a_2 - a_1 \neq 1$ . Therefore  $a_2 - a_1 = a_1$  and we have

$$a_m - a_{m-1} = a_1 = a_2 - a_1$$

and the argument from case 1 can be repeated.

**Case 3.**  $a_m - a_{m-1} = a_1 - 1$ . An exact repetition of case 2 shows that in this case  $a_2 - a_1 + 1$  would have to be one of the coins. However, this possibility is excluded by the assumptions of our lemma.  $\square$

The results from this section, together with Proposition 3.2 can be used to characterize the set of possible values of  $a_j - a_i$  which fit in the interval  $(1, a_2)$ . For a currency  $A$  let  $S(A) = \{a_j - a_i : 0 \leq i < j \leq k\}$ .

**Corollary 5.5.** *For an orderly currency  $A = (1, a_1, a_2, \dots, a_k)$*

(a) *we always have*

$$S(A) \cap (1, a_1) \subset \{a_1 - 1\}$$

$$S(A) \cap (a_1, a_2) \subset \{a_2 - a_1, a_2 - 1\}$$

(b) *if  $a_2 = 2a_1 - 1$  or  $a_2 = 2a_1$  then  $S(A) \cap (1, a_2) \subset \{a_1 - 1, a_1, a_2 - 1\}$*

(c) *if  $a_2 > 2a_1$  then  $S(A) \cap (1, a_2) = \{a_1 - 1, a_2 - a_1, a_2 - 1\}$*

**Proof.** Property (a) is just a restatement of Proposition 3.2 and Lemmas 5.2, 5.3 and 5.4.

By Theorem 3.4 there are no other possible values of  $a_2$  except of those in (b) and (c). In both cases, if  $a_j - a_i < a_1$ , then Proposition 3.2 applies.

In case (c)  $a_1 < a_2 - a_1 < a_2 - a_1 + 1 \leq a_2 - 1$  and an application of Lemmas 5.3 and 5.4 proves that our theorem enumerates all possible elements of  $S(A) \cap (1, a_2)$ .

Of course all the given values are attained, so in (c) we are free to use equality rather than inclusion.

In case (b) the difference  $a_1$  may or may not be attained (consult the currencies  $(1, 3, 5)$  and  $(1, 3, 5, 8, 10, 15)$ ). Once again one needs to combine the before-mentioned lemmas; we omit the details.  $\square$

**Remark.** Corollary 5.5 and Theorem 3.4 give two independent conditions that must be satisfied by orderly currencies. For instance every three-coin currency satisfies Corollary 5.5, but not necessarily Theorem 3.4 (it is also easy to imagine more complicated examples of this kind). On the other hand, the currency  $(1, 3, 7, 12)$  satisfies Theorem 3.4, but  $12 - 7 = 5 \notin \{7 - 3, 7 - 1\}$ , so part (a) of Corollary 5.5 is violated.

Our last theorem in this section will be important in section 7. It can roughly be stated as “if some two consecutive differences are large, then the subsequent differences must also be large”.

**Theorem 5.6.** *Suppose  $(1, a_1, \dots, a_k)$  is orderly,  $m \geq 2$  and*

$$a_{m-1} > 2a_{m-2}, \quad a_m > 2a_{m-1}.$$

*Then for every  $t \geq m$  we have  $a_{t+1} - a_t \geq a_m - a_{m-1}$ .*

**Proof.** Suppose, on the contrary, that  $a_{t+1} - a_t < a_m - a_{m-1}$  for some  $t \geq m$ , and let  $t$  be the smallest index with these properties. Choose  $s$  as the largest index for which

$$a_{s+1} - a_s < a_t - a_{m-2}$$

(such numbers  $s$  exist; for instance  $s = t - 1$  satisfies this inequality). Note that by maximality of  $s$  we have  $a_{s+2} - a_{s+1} \geq a_t - a_{m-2}$  (possibly  $a_{s+2} = \infty$ ) and  $a_{s+3} - a_{s+2} \geq a_t - a_{m-2}$  (if  $a_{s+2} < \infty$ ). The proof is split into two cases.

**Case 1.**  $a_s + a_{t+1} < a_{s+2}$ . With this assumption we have

$$a_{s+1} < a_s + a_t < a_s + a_{t+1} < a_{s+2}$$

so there exist indices  $r, l$  such that

$$\begin{aligned} a_s + a_t &= a_{s+1} + a_r, \\ a_s + a_{t+1} &= a_{s+1} + a_l, \end{aligned}$$

with  $r < l \leq t$ . This implies

$$a_l - a_{l-1} \leq a_l - a_r = a_{t+1} - a_t < a_m - a_{m-1}.$$

Since  $l - 1 < t$  and  $t$  was chosen to be minimal with respect to the condition  $t \geq m$  and the above inequality, we obtain  $l - 1 < m$ . Since  $l = m$  does not satisfy the above inequality, we have  $l \leq m - 1$  and  $r \leq m - 2$ , but then

$$a_{s+1} - a_s = a_t - a_r \geq a_t - a_{m-2}$$

contradicting the choice of  $s$ . This completes the first case of the proof.

**Case 2.** Now suppose  $a_s + a_{t+1} \geq a_{s+2}$ . We are going to prove the following sequence of inequalities:

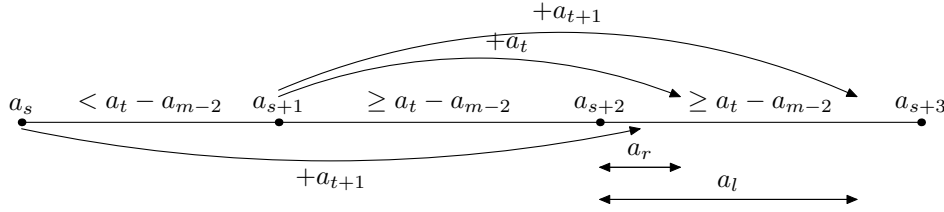


FIGURE 4. The situation in case 2. in Theorem 5.6.

- (1)  $a_{s+1} - a_s > a_{m-2}$
- (2)  $a_{s+2} - a_s > a_m$
- (3)  $a_{s+1} - a_s < a_m$
- (4)  $a_{s+1} - a_s \geq a_m - a_{m-1}$
- (5)  $a_{s+2} < a_{s+1} + a_t < a_{s+1} + a_{t+1} < a_{s+3}$

(1): We always have

$$a_{s+2} - a_s > a_{s+2} - a_{s+1} \geq a_t - a_{m-2} \geq a_m - a_{m-2} > a_{m-1}.$$

If we also had  $a_{s+1} - a_s \leq a_{m-2}$  then

$$a_{s+1} \leq a_s + a_{m-2} < a_s + a_{m-1} < a_{s+2}.$$

As usually, it means that  $a_{m-1} - a_{m-2} = a_l - a_r$  for some  $r < l \leq m-2$  or  $a_{m-1} - a_{m-2} = a_l$  for  $l \leq m-2$ . In either case  $a_{m-1} - a_{m-2} \leq a_{m-2}$ , contradicting the assumptions of the theorem. Therefore  $a_{s+1} - a_s > a_{m-2}$ .

(2): This follows straight from (1) and the maximality of  $s$ :

$$a_{s+2} - a_s = (a_{s+2} - a_{s+1}) + (a_{s+1} - a_s) > a_t - a_{m-2} + a_{m-2} = a_t \geq a_m.$$

(3): Since we assumed  $a_{s+2} - a_s \leq a_{t+1}$  for this case, we obtain, using the properties of  $s$  and  $t$ , that

$$a_{s+1} - a_s = (a_{s+2} - a_s) - (a_{s+2} - a_{s+1}) \leq a_{t+1} - (a_t - a_{m-2}) < a_m - a_{m-1} + a_{m-2} < a_m.$$

(4): By (2) and (3) we have  $a_{s+1} < a_s + a_m < a_{s+2}$ , therefore  $a_s + a_m = a_{s+1} + a_r$  for some  $r \leq m-1$ . Finally

$$a_{s+1} - a_s = a_m - a_r \geq a_m - a_{m-1}.$$

(5): First note that by  $a_t \geq a_m$  and  $2a_{m-2} < a_{m-1}$  we obtain

$$a_{s+3} - a_{s+1} \geq 2(a_t - a_{m-2}) = a_t + a_t - 2a_{m-2} > a_t + a_m - a_{m-1} > a_{t+1}.$$

Moreover, by (4) and the assumption  $a_{s+2} - a_s \leq a_{t+1}$  we get

$$a_{s+2} - a_{s+1} = (a_{s+2} - a_s) - (a_{s+1} - a_s) \leq a_{t+1} - (a_m - a_{m-1}) < a_t.$$

This ends the proof of (1)–(5). Now (5) implies the existence of  $r < l \leq t$  such that

$$\begin{aligned} a_{s+1} + a_t &= a_{s+2} + a_r, \\ a_{s+1} + a_{t+1} &= a_{s+2} + a_l. \end{aligned}$$

As a consequence of these formulae we obtain the inequality

$$a_r = a_t - (a_{s+2} - a_{s+1}) \leq a_t - (a_t - a_{m-2}) = a_{m-2}, \text{ hence } r \leq m-2,$$

which in turn implies

$$a_l = (a_{t+1} - a_t) + a_r < a_m - a_{m-1} + a_{m-2} < a_m, \text{ hence } l \leq m - 1.$$

Combining this, we get

$$a_{s+1} - a_s = a_{s+2} - a_s + a_l - a_{t+1} \leq a_{t+1} + a_l - a_{t+1} = a_l \leq a_{m-1}.$$

However, by (4)  $a_{s+1} - a_s \geq a_m - a_{m-1} > a_{m-1}$ , so we have a contradiction which ends the proof of case 2, and the whole theorem.  $\square$

## 6. $+/-$ -CLASSES

If  $A = (1, a_1, \dots, a_k)$  is orderly then some prefix sub-currency, i.e. a currency of the form  $A' = (1, a_1, \dots, a_l)$  with  $l < k$  might not be orderly (for instance,  $(1, 2, a, a+1, 2a)$  is orderly, but  $(1, 2, a, a+1)$  is not for  $a \geq 4$ , as in Proposition 4.2). This situation was still quite manageable in the case of 5 coins, but it gets more and more complicated as the number of coin increases, thus making inductive analysis (possibly using the one-point theorem) impossible.

To describe the prefix currencies we introduce the notion of  $+/-$ -classes. To every currency  $A = (1, a_1, \dots, a_k)$  we may assign a pattern of  $k+1$  signs  $+$  and  $-$ , defined as follows: the  $l$ -th symbol of the pattern ( $l = 0, \dots, k$ ) is  $+$  if the prefix currency  $(1, a_1, \dots, a_l)$  is orderly and  $-$  in the opposite case. A  $+/-$ -class is the set of all currencies corresponding to a given  $+/-$ -pattern. For instance, the pattern  $++++ \dots +++$  corresponds to totally orderly currencies. Another well-described example is the  $+/-$ -class given by the pattern  $++++-$  — it consists precisely of the currencies  $(1, 2, a, a+1, 2a)$  with  $a \geq 4$  (this is the consequence of Proposition 4.2, since an orderly 5-coin currency which is not totally orderly satisfies part (1) of that proposition).

The  $+/-$ -patterns that correspond to non-empty classes cannot be completely arbitrary, for instance, if a pattern ends with a  $+$  then it must begin with  $+++$  — this is a consequence of Theorem 3.5. The patterns beginning with  $+++$  and ending with  $+$  will be called *proper*. Mysteriously, some proper patterns describe empty classes. Here is a sample proposition of this sort:

**Proposition 6.1.** *The  $+/-$ -class described by the pattern  $++++--$  is empty.*

**Proof.** Suppose that  $A = (1, a_1, a_2, a_3, a_4, a_5, a_6)$  is a coinage system in the class  $++++--$ . By case (1) of Proposition 4.2 we know that in fact  $A$  is of the form

$$(1, 2, a, a+1, 2a, a_5, a_6)$$

for some  $4 \leq a$ ,  $2a < a_5 < a_6$ . By the one-point theorem some multiple of  $2a$  is a counterexample for  $(1, 2, a, a+1, 2a, a_5)$ . Extending this by  $a_6$  must fix this problem, hence

$$a_6 - a_5 < 2a.$$

Since  $A$  is orderly, there exist numbers  $r, s$  such that:

$$\begin{aligned} a_5 + a_5 &= a_6 + a_r, \\ a_5 + 2a &= a_6 + a_s, \end{aligned}$$

with  $a_r \leq 2a$ ,  $a_s \leq a + 1$ ,  $1 \leq a_s < a_r$ . Subtracting the two equations yields  $a_5 - 2a = a_r - a_s$ . Possible differences  $a_r - a_s$  ( $0 \leq s < r \leq 4$ ) form the set

$$\{1, a - 2, a - 1, a, 2a - 2, 2a - 1, 2a\}$$

so the possible values of  $a_5$  are  $2a + 1, 3a - 2, 3a - 1, 3a, 4a - 2, 4a - 1, 4a$ .

The values  $3a - 1, 3a, 4a - 2, 4a - 1, 4a$  can be excluded from this set, since then  $(1, 2, a, a + 1, 2a, a_5)$  would be orderly, which can be checked easily by the one-point theorem (the “suspected” amount to be tested for optimality is  $4a$ ).

Therefore we are left with  $a_5 \in \{2a + 1, 3a - 2\}$ .

If  $a_5 = 2a + 1$  then the greedy algorithm for  $(1, \dots, a_5)$  fails to be optimal already for  $3a = 2a + a$ , hence  $a_6 \leq 3a$ . On the other hand, all three numbers  $2a + 2a$ ,  $2a + (2a + 1)$  and  $(2a + 1) + (2a + 1)$  can be obtained with two coins, hence  $4a - a_6$ ,  $4a + 1 - a_6$  and  $4a + 2 - a_6$  must be three consecutive integers which are coins, all less than  $a_6$ . This is only possible if  $a_6 = 4a$ , contradiction.

Now suppose that  $a_5 = 3a - 2$ . Then for the number  $2a + (a + 1) = 3a + 1$  not to be a counterexample we must have  $3a - 1 \leq a_6 \leq 3a + 1$ . If  $a_6 = 3a - 1$  then  $4a - 2 = (3a - 2) + a = (3a - 1) + (a - 1)$  is a counterexample ( $a - 1$  is not a coin). If  $a_6 = 3a$  then the counterexample is  $4a - 1 = (3a - 2) + (a + 1) = 3a + (a - 1)$  (reason as before). Finally, if  $a_6 = 3a + 1$  then  $4a = 2a + 2a = (3a + 1) + (a - 1)$  is the counterexample.  $\square$

Of course, given a currency, we may recover its  $+/-$ -class in  $O(k^4)$  time simply by repeating Pearson’s algorithm [7] for each prefix sub-currency. The reverse problem, to determine whether a given proper  $+/-$ -pattern describes a non-empty  $+/-$ -class is actually much harder and we have not been able to find any algorithm solving it.

From this point of view the most “messy” orderly currencies are those which belong to the class determined by  $+++-----\dots--+$ . These classes are indeed non-empty for  $k = 0, 2 \pmod{3}$ . Their representatives for  $k = 3l$  and  $k = 3l - 1$ , respectively, are

$$\begin{aligned} &(1, 2, 4, 5, 7, 8, \dots, 3l - 2, 3l - 1, 3l + 1, 3l + 4, \dots, 6l - 2), \\ &(1, 2, 4, 5, 7, 8, \dots, 3l - 2, 3l - 1, 3l + 2, 3l + 5, \dots, 6l - 4). \end{aligned}$$

On the other hand, there seem to be no coinage systems of type  $+++-----\dots--+$  for  $k = 1 \pmod{3}$ , but we have not been able to prove this.

## 7. CLASSIFICATION OF ORDERLY SUB-CURRENCIES

Every set  $P = \{i_0, i_1, \dots, i_l\} \subset \{0, 1, \dots, k\}$ , where  $0 = i_0 < i_1 < \dots < i_l$  determines a sub-currency  $(a_{i_0}, a_{i_1}, \dots, a_{i_l})$  of any currency  $A = (1, a_1, \dots, a_k)$ . From Theorem 3.5 we know that if  $A$  is orderly then the sub-currency determined by  $P = \{0, 1, l\}$  ( $2 \leq l \leq k$ ) is also orderly. Is this just a lonely phenomenon, or could a similar theorem be proved for some other sets  $P$ ?

**Definition 7.1.** *The set  $P$  of the form given above will be called hereditary if the following is true:*

*for every orderly currency  $A = (1, a_1, \dots, a_k)$   
the sub-currency determined by  $P$  is also orderly*

Let us enumerate some interesting classes of subsets of  $\{0, 1, \dots, k\}$ :  
type 1: the singleton set  $\{0\}$

type 2: the sets  $\{0, l\}$  for  $1 \leq l \leq k$   
 type 3: the sets  $\{0, 1, l\}$  for  $2 \leq l \leq k$   
 type 4: the sets  $\{0, 1, 2, l\}$  for  $4 \leq l \leq k$   
 type 5: the full set  $\{0, 1, \dots, k\}$

Note that  $\{0, 1, 2, 3\}$  is a peculiar exception: it is *not* of type 4 (an immediate example is  $(1, 2, a, a+1, 2a)$  for  $a \geq 4$  and its non-orderly sub-currency  $(1, 2, a, a+1)$  determined by  $\{0, 1, 2, 3\}$ ).

We already know that sets  $P$  of type 1, 2, 3 or 5 are hereditary. In this section we shall prove that sets that are not specified in types 1–5 are not hereditary.<sup>3</sup> We also conjecture that all sets  $P$  of type 4 are hereditary, and we prove this conjecture under some mild additional assumptions. The general case remains open.

Before proceeding with the elimination of non-hereditary subsets  $P$  let us make a few observations.

**Lemma 7.2.** *For any  $l \geq 3$  let  $B_l$  denote the currency*

$$B_l = (1, 2, 3, \dots, l-1, 2l-2, 2l-1, 4l-4)$$

*where  $a_l = 2l-1$ . Then  $B_l$  is orderly of type  $+++ \dots +-+$ .*

**Proof.** The prefix currency  $(1, 2, 3, \dots, l-1)$  is clearly of type  $+++ \dots +-+$ . Extending this by  $2(l-1)$  we get an orderly currency by the one-point theorem. The next prefix, ending in  $2l-1$  is not orderly since  $2 \cdot 2(l-1) = 4l-4$  is the smallest counterexample. The complete currency is orderly which can be proved easily by the techniques from the proof of Theorem 2.1.  $\square$

**Lemma 7.3.** *For any  $m > l \geq 2$  and  $p \geq 1$  let  $A_{l,m}(p)$  denote the currency:*

$$A_{l,m}(p) = (a_0, a_1, a_2, \dots, a_{l-1}, a_l, a_{l+1}, a_{l+2}, \dots, a_m) = \\ (1, 2, 3, \dots, l, pl, (2p-1)l, (3p-2)l, \dots, ((m-l+1)p - (m-l))l)$$

*where  $a_l = pl$ . This currency is orderly. Moreover, if  $p > m-l$  then  $\lceil a_m/a_l \rceil = m-l+1$ .*

**Proof.** The given currency is in fact of type  $++++ \dots +++$ , which can be verified inductively by the one-point theorem: to check that  $(1, a_1, \dots, a_{l+i})$  is orderly for  $i \geq 1$  it suffices to observe that

$$2a_{l+i-1} = 2(pi - (i-1))l = (p(i+1) - i)l + (p(i-1) - (i-2))l = a_{l+i} + a_{l+i-2}.$$

To prove the last statement note that

$$a_m = ((m-l+1)p - (m-l))l < (m-l+1)pl = (m-l+1)a_l$$

and, if  $p > m-l$ :

$$a_m = ((m-l+1)p - (m-l))l = (m-l)pl + l(p - (m-l)) > (m-l)a_l.$$

$\square$

---

<sup>3</sup>To be precise, every set  $P$  should always be thought of as a subset of  $\{0, 1, \dots, k\}$  for a certain  $k$ . In most cases  $k$  will be implicit, but to improve clarity we shall sometimes stress this connection by writing  $P \subset \{0, 1, \dots, k\}$ .



**Lemma 7.4.** *An orderly currency may be extended by any multiple of its highest coin and the resulting currency will be orderly.*

**Proof.** A trivial consequence of the one-point theorem.  $\square$

The last observation will be used in the following way: suppose we want to prove that some set  $P = \{i_0, i_1, \dots, i_l\} \subset \{0, 1, \dots, k\}$  is not hereditary. First we find a shorter orderly currency  $A' = (1, a_1, \dots, a_r)$ , such that the sub-currency determined by  $P' = \{i_0, i_1, \dots, i_{r'}\} \subset \{0, 1, \dots, r\}$  is not orderly (here  $r' < r \leq k$ ) and  $i_{r'+1} > r$  or  $r' = l$ . Let  $c$  be any counterexample for this sub-currency and let  $m$  be any number for which  $ma_r > c$ . Then the currency

$$A = (1, a_1, \dots, a_r, ma_r, 2ma_r, \dots, (k-r)ma_r)$$

is orderly (Lemma 7.4) and its sub-currency determined by  $P$  is not, since all the added coins are too large to fix the problem with  $c$  (the exact form of  $P \setminus P'$  is actually immaterial, it is important that its smallest element is at least  $r+1$ ).

**Theorem 7.5.** *The sets  $P$  not of the form 1, 2, 3, 4 or 5 are not hereditary.*

**Proof.** Let  $P = \{i_0, \dots, i_s\} \subset \{0, \dots, k\}$ ,  $i_0 = 0$ , be such a set. Let  $r$  be the largest index for which  $i_r = r$  (i.e.  $\{0, \dots, r\} \subset P$ ,  $r+1 \notin P$ ). We shall consider a few cases:

**Case**  $3 \leq r < k$ . Here we employ the orderly currency  $B_r$ . Its sub-currency  $(1, a_1, \dots, a_r)$  is not orderly. If  $r = k-1$  then we are done, while for  $r < k-1$  we must expand  $B_r$  to an orderly currency with  $k+1$  coins in the standard way described earlier. The resulting currency will have a disorderly sub-currency determined by  $P$ .

**Case**  $r = 2$ . In this case  $|P| \geq 5$ , since otherwise  $P$  would be of the form  $\{0, 1, 2\}$  or  $\{0, 1, 2, l\}$  for some  $l \geq 4$  and these sets are of type 3 and 4, respectively. Denote  $l = i_3 \geq 4$ ,  $m = i_4$  and consider the currency  $A_{l,m}(p)$  with  $p > m-l$ . Its sub-currency

$$(1, 2, 3, a_l, a_m)$$

is not orderly since the amount

$$\lceil a_m/a_l \rceil a_l = (m-l+1)a_l$$

paid greedily splits into the coin  $a_m$  and some of the coins 1, 2, 3, thus requiring at least

$$1 + \frac{(m-l)l}{3} > 1 + (m-l)$$

coins, which is more than if it was paid with  $m-l+1$  copies of  $a_l$ . Now it suffices to expand this currency to a currency with  $k+1$  coins as previously.

**Case**  $r = 1$ . Then  $|P| \geq 4$ , since otherwise  $P$  would be of the form  $\{0, 1, l\}$ , which is of type 3. Let  $l = i_2 \geq 3$  and  $m = i_3$  and consider the currency  $A_{l,m}(p)$  with  $p > m-l$ . The sub-currency  $(1, 2, a_l, a_m)$  is not orderly for the same reason as previously: the amount  $\lceil a_m/a_l \rceil a_l = (m-l+1)a_l$  must be paid greedily with at least  $1 + \frac{(m-l)l}{2} > 1 + (m-l)$  coins and the proof follows.

**Case**  $r = 0$ . Clearly  $|P| \geq 3$ , since sets of the form  $\{0\}$  and  $\{0, l\}$  are of type 1 and 2. Let  $l = i_1 \geq 2$  and  $m = i_2$ . Repeat the same arguments with the currency  $A_{l,m}(p)$  ( $p > m-l$ ) and its sub-currency  $(1, a_l, a_m)$ : this time the amount  $\lceil a_m/a_l \rceil a_l = (m-l+1)a_l$  must be paid greedily with at least  $1 + \frac{(m-l)l}{1} > 1 + (m-l)$  coins.  $\square$

Sets  $P$  of type 4 are the most peculiar ones. We believe they are also hereditary; that is, we have the following:

**Conjecture 7.6.** *If  $A = (1, a_1, \dots, a_k)$  is orderly, then the currency  $(1, a_1, a_2, a_l)$  is also orderly for every  $4 \leq l \leq k$ .*

While this is not known to be true in general, we can prove this conjecture under some mild additional conditions.

**Theorem 7.7.** *Conjecture 7.6 is true if we additionally assume that  $a_2 > 2a_1$  and  $a_3 > 2a_2$ .*

**Proof.** We shall verify that  $(1, a_1, a_2, a_l)$  is orderly by Proposition 4.1. Let  $m = \lceil a_l/a_2 \rceil$ . By Theorem 5.6 for every  $l \geq 3$  we have the first of the following inequalities:

$$a_{l+1} - a_l \geq a_3 - a_2 > a_2 > ma_2 - a_l.$$

It means that  $a_{l+1} > ma_2$ , so there is no new coin between  $a_l$  and  $ma_2$ , and the greedy decomposition of  $ma_2$  with respect to  $A$  involves only the coins  $1, a_1, a_l$ . This justifies the first equality in the following comparison:

$$\text{grd}_{(1, a_1, a_2, a_l)}(ma_2) = \text{grd}_A(ma_2) = \text{opt}_A(ma_2) \leq \text{opt}_{(1, a_1, a_2, a_l)}(ma_2)$$

and by Proposition 4.1 the proof is complete.  $\square$

## 8. CLOSING REMARKS AND OPEN PROBLEMS

Throughout this paper we have proposed some possible approaches to the problem of describing orderly coinage systems and their interesting properties. Some of these techniques have enabled us to prove the most important results of this paper, namely the structural theorems, like Theorem 3.4 and Corollary 5.5, or to give concise descriptions of small systems. There is still quite a lot of work to be done in the following areas:

- **sub-currencies:** prove Conjecture 7.6, thus completing the classification of orderly sub-currencies.
- **prefix sub-currencies:** invent an algorithm to decide whether a given  $+/-$  pattern describes a non-empty class or devise some other properties of such  $+/-$  patterns. Another interesting conjecture, to which we have not found a counterexample, is:

**Conjecture 8.1.** *If a  $+/-$ -class is non-empty, then it has a representative  $A = (1, a_1, \dots, a_k)$  with  $a_1 = 2$ .*

- **differences:** can Corollary 5.5 be generalized? In other words, what can be said about the differences  $a_j - a_i$  that belong to  $(a_{m-1}, a_m)$  for some  $m$ ? Is it true that in general

$$S(A) \cap (a_{m-1}, a_m) \subset \{a_m - a_{m-1}, a_m - a_{m-2}, \dots, a_m - 1\},$$

where  $S(A) = \{a_j - a_i : 0 \leq i < j \leq k\}$  for an orderly currency  $A$ ? We already know this is true for  $m = 1, 2$ . The lemmas from section 6 provide some partial results in the general case as well.

- **extending:** Theorem 3.4, Corollary 5.5 and Conjecture 7.6 can be thought of as *obstructions* against extending: if a currency does not satisfy one of these conditions then it cannot be extended to an orderly currency by appending new coins of high denominations (higher than all the existing coins). What are the other invariants of this sort? Is there an algorithm that decides if a currency can be extended to an orderly one? Problems related to obstructions and extending can also be found in [9].

**Acknowledgements.** We are indebted to the referee, whose valuable suggestions improved both the presentation and some technical aspects of our paper. We also thank Lenore Cowen for pointing us to [9].

#### REFERENCES

- [1] M.J.Magazine, G.L.Nemhauser, L.E.Trotter Jr., When the Greedy Solution Solves a Class of Knapsack Problems, *Operations Research*, Vol.23, No.2. (Mar.-Apr., 1975), pp. 207-217
- [2] T.C.Hu, M.L.Lenard, Optimality of a Heuristic Solution for a Class of Knapsack Problems, *Operations Research*, Vol.24, No.1. (Jan.-Feb., 1976), pp. 193-196
- [3] B.N.Tien, T.C.Hu, Error Bounds and the Applicability of the Greedy Solution to the Coin-Changing Problem, *Operations Research*, Vol.25, No.3. (May-Jun., 1977), pp. 404-418
- [4] J.D.Jones, Orderly Currencies, *The American Math. Monthly*, Vol.101, No.1. (Jan., 1994), pp. 36-38
- [5] S.B.Maurer, Disorderly Currencies, *The American Math. Monthly*, Vol.101, No.5. (May, 1994), pp. 419
- [6] D.Kozen, S.Zaks, Optimal Bounds for the Change-Making Problem, *Theoret. Comput. Sci.* 123 (1994), 377-388
- [7] D.Pearson, A Polynomial-time Algorithm for the Change-Making Problem, Technical Report TR 94-1433, Department of Computer Science, Cornell University, June 1994; also in *Operations Research*, Vol.33, No.3. (May 2005), pp. 231-234
- [8] J.Shallit, What This Country Needs is an 18c Piece, *Math. Intelligencer* 25 (2) 2003, 20-23
- [9] L.J.Cowen, R.Cowen, A.Steinberg, Totally Greedy Coin Sets and Greedy Obstructions, *Electronic Journal of Combinatorics* 15 (2008), #R90