Canonical coin systems

Jakub Cisło

Jagiellonian University

jakub@cislo.net.pl

April 14, 2016

Overview

1. Brief description of the problem
   - Definitions
   - Properties of greedy decomposition
2. Smallest counterexample characterization
   - Properties of subvectors
   - $M(w)$ vs $G(c_{i-1} - 1)$
3. Polynomial algorithm for checking canonicity

Brief description of the problem

Brief description of the problem

Denominations

Brief description of the problem

Denominations

14

Brief description of the problem

Denominations

14

Greedy

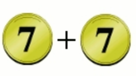
Brief description of the problem

Denominations

14

Greedy

Optimal



Definitions

$C = (c_1, c_2, ..., c_n)$

where $c_1 > c_2 > ... > c_n$ are denominations

Decomposition of w

vector V satisfying $V \cdot C = w$ (where $\cdot$ is scalar product)

$G(w)$

greedy decomposition of w

$M(w)$

optimal decomposition of w (minimalize $|M(w)| = M(w) \cdot (1, ..., 1)$)

Properties of greedy decomposition

$G(\cdot)$ is monotonic

$x \le y \implies G(x) \le G(y)$

$G(w)$ is the greatest lexicographical representation of w

$\forall_{U : U \cdot C = w} U \le G(w)$

Properties of subvectors

Definition

V *is greedy* if and only if $V = G(V \cdot C)$

Definition

V *is minimal* if and only if $V = M(V \cdot C)$

Lemma

a) If $U \subseteq V$ and V is greedy, then U is greedy.
b) If $U \subseteq V$ and V is minimal, then U is minimal.

$M(w)$ vs $G(c_{i-1} - 1)$

Theorem

Let w be the smallest counter example, i - the first index of nonzero value in $M(w)$, j - the last one. Then $M(w)$ is identical with $G(c_{i-1} - 1)$ on positions from 1 to $j - 1$-th. It's one greater on j-th position. The remaining entries are all zeros.

$O(n^2)$ candidates

$O(n^2)$ candidates
every checked in $O(n)$

$O(n^2)$ candidates

every checked in $O(n)$

$$=$$

$$O(n^3)$$

Thank you