# How to find counterfeit coins on a precision scale if the weights of coins are a priori unknown


Grigory Kabatiansky & Elena Egorova

Skolkovo Institute of Science and Technology


**Combinatorics and Geometry Days II at MIPT**

April 16, 2020

# Problem statement

There are $n$ coins. Let us enumerate them and let $x_1, \ldots, x_n$ be their weights with at least $n - t$ of them being of equal weight, say $a$. Denote $I = \{i : \ x_i = a\}$ and $J = [n] \setminus I$, with $|J| \leq t$.

There is a precision scale that allows to know the exact weight of any subset of coins.

*What is the minimal number $Q(n, t)$ of non-adaptive weighings which allows to find weights for all coins?*

# Non-adaptive strategy: search matrix

A non-adaptive search with $r$ weighings is uniquely defined by its $r \times n$ binary *search matrix* $H$ which $i$-th row is the characteristic vector of the $i$-th weighted subset of coins.

The property that a given non-adaptive search defined by $H$ can find all weights is equivalent to the property that if $H\mathbf{x}^T = H\mathbf{y}^T$ then $\mathbf{x} = \mathbf{y}$.

# Search matrix

Denote by $r_{\mathbb{R}}(n,t)$ and by $r_2(r,t)$ the minimal $r$ such that there exist $n$ *binary* $r$-dimensional vectors with the property that any $2t$ of them are linear independent over the field $\mathbb{R}$ and over the field $\mathbb{F}_2$ correspondingly.

**Proposition [1]**

$r_{\mathbb{R}}(n,t) \leq Q(n,t) \leq 2t+1+r_{\mathbb{R}}(n,t)$

[1] Nader H. Bshouty, Hanna Mazzawi. "On parity check (0,1)-matrix over Zp", SODA '11, Proceedings 22nd ACM-SIAM symposium on Discrete algorithms, pp. 1383–1394, 2011

Let us prove that any $2t$ columns of $H$ are linear independent over $\mathbb{R}$ and hence $Q(n,t) \geq r_{\mathbb{R}}(n,t)$.
Indeed, let assume the inverse. Consider $2t$ columns which are linear dependent, i.e.,

$$\sum_{k=1}^{2t} \lambda_k \mathbf{h}_{i_k} = 0,$$

where $\mathbf{h}_j$ is the $j$-th column of $H$. Then $H\mathbf{x}^T = H\mathbf{y}^T$, where $x_{i_k} = \lambda_k$ for $k = 1, \ldots, t$ and the rest $x_i = 0$, versus $y_{i_k} = \lambda_k$ for $k = t+1, \ldots, 2t$ and the rest $y_i = 0$.

Now let us show that $Q(n,t) \leq 2t + 1 + r_{\mathbb{R}}(n,t)$.
Let $H_0$ be $r_{\mathbb{R}}(n,t) \times n$ matrix, in which any $2t$ columns are linear independent, and let $I_m$ be $m \times m$ unit matrix. Construct matrix $H$

$$H = \left( \begin{array}{c|c} I_{2t+1} & \mathbf{0} \\ \hline \multicolumn{2}{c}{H_0} \end{array} \right)$$

Let $\mathbf{s} = (s_1, \ldots, s_r) = H\mathbf{x}^T$. The following algorithm finds $\mathbf{x}$.
First of all $a := maj\{s_1, \ldots, s_{2t+1}\} = maj\{x_1, \ldots, x_{2t+1}\}$.
Then choose a subset $L \subset [n]$ s.t. $|L| = t$ and solve (if possible) the following system of linear equations $H_0\mathbf{x}^T = \mathbf{s}_0$, where $\mathbf{s}_0 = (s_{2t+2}, \ldots, s_r)$, $x_j : j \in L$ are unknown variables and $x_i = a$ for all $i \notin L$. For $L = J$ this system has the solution and any two solutions will give a linear dependence between at most $2t$ columns of $H_0$ what contradicts to the choice of $H_0$.

**Proposition**

$r_{\mathbb{R}}(n,t) \leq r_2(n,t) \leq t \log_2 n$

Left inequality follows from the fact that if the determinant of a binary matrix is non-zero over mod 2 then it is non-zero over $\mathbb{R}$. Right inequality follows if one takes as the corresponding vectors all columns of a parity-check matrix of an irreducible binary Goppa code of length $n = 2^m$, correcting $t$ errors.Hence

$$Q(n,t) \leq t \log_2 n(1 + o(1))$$

It was previously known that $Q(n,t) = O(t \ln n)$ [1]
The best known lower bound

$$Q(n,t) \geq 2 \frac{t}{\log_2 t} \log_2 n(1 + o(1))$$

follows from the known upper bound on the cardinality of $t$-signature codes for the binary adder channel.

## Open questions

There are at least three open questions:

1. what is $Q(n, t)$ or $r_{\mathbb{R}}(n, t)$ for $t = \mathit{fixed}$ and $n \to \infty$?
2. what is $Q(n, t)$ for $t = \lambda n$ and $n \to \infty$?
3. to develop "decoding" algorithm which finds weights for all coins with low polynomial complexity for $t = \mathit{fixed}$.