Threshold-gates, coin-weighing and indecomposable hypergraphs

(DRAFT)

Noga Alon *

Abstract

Let $m(n)$ denote the maximum possible number $m$ such that given a set of $m$ coins out of a collection of coins of two unknown distinct weights, one can decide if all the coins have the same weight or not using $n$ weighings in a regular balance beam. It is shown that $m(n) \geq n^{(1/2+o(1))n}$. This is tight up to the $o(1)$-term and settles a problem of Kozlov and Vu.

Let $D(n)$ denote the maximum possible degree of regularity of a regular multi-hypergraph on $n$ vertices that contains no proper regular nonempty subhypergraph. It is shown that for every $n$ which is a power of 2, $D(n) \geq n^{(1/2+o(1))n}$. This is tight up to the $o(1)$-term and improves estimates of Shapley, van Lint and Pollak.

Both results are proved by a similar technique whose main ingredient is a construction of Håstad of threshold gates that require large weights.

1 Introduction

In this paper we discuss two extremal problems that have been considered by various researchers. Although these problems are seemingly unrelated it turns out that both of them can be solved asymptotically by applying the same technique whose main ingredient is a construction of Håstad [5] of threshold gates that require large weights. We start with a formulation of the problems and the new results.

1.1 Coin-weighing

Coin-weighing problems deal with the determination or estimation of the minimum possible number of weighings in a regular balance beam that enable one to find the required information about the weights of the coins. These questions have been among the most popular puzzles during the last fifty years, see, e.g., [4] and its many references. Here we study the following variant of the old questions, considered in [6], [8].

*Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: noga@math.tau.ac.il. Research supported in part by a USA Israeli BSF grant and by the Fund for Basic Research administered by the Israel Academy of Sciences.
Given a set of \( m \) coins out of a collection of coins of two unknown distinct weights, we wish to decide if all the \( m \) given coins have the same weight or not using the minimum possible number of weighings in a regular balance beam. Let \( m(n) \) denote the maximum possible number of coins for which the above problem can be solved in \( n \) weighings. It is easy to check (see, e.g., [6], [8]) that \( m(n) \geq 2^n \). To see this, note that trivially \( m(1) = 2 \), and that if we already know some \( m \) coins that have the same weight, then we can, in one additional weighing, compare them to \( m \) new coins and either conclude that not all coins have the same weight, in case the weighing is not balanced, or conclude that all \( 2m \) coins have the same weight, in case the last weighing is balanced. Hence \( m(n+1) \geq 2m(n) \) for every \( n \), implying that \( m(n) \geq 2^n \).

Somewhat surprisingly, \( m(n) \) is in fact strictly larger than \( 2^n \) for all \( n > 2 \). This was proved by Kozlov and Vu [8] who proved that \( m(3) \geq 10 \) and that for every \( n \) divisible by 15,

\[
m(n) \geq 4.187^n.
\]

They also proved that
\[
m(n) \leq \frac{(3^n - 1)(n+1)(n+1)/2}{2},
\]
and conjectured that \( m(n) \geq n^{\Omega(n)} \). Here we prove this conjecture in the following sharp form.

**Theorem 1.1** For every \( n \) which is a power of 2

\[
m(n) \geq \frac{1}{2e^4n^2/2} n^{n/2},
\]
where here and throughout the paper \( \beta = \log(3/2) \), and all logarithms are in base 2.

We also slightly improve the upper bound in (1) as follows.

**Proposition 1.2** For every \( n \geq 2 \)

\[
m(n) \leq \frac{(3^n - 1)(n+1)n(n-1)/2}{2}.
\]

For large \( n \), this reduces the bound in (1) by roughly a factor of \( \sqrt{e} \).

Combining the assertion of Theorem 1.1 with some additional arguments we can determine the asymptotic behaviour of \( m(n) \) for every \( n \).

**Theorem 1.3** The function \( m(n) \) satisfies

\[
m(n) = n^{(\frac{1}{2}+o(1))n},
\]
where the \( o(1) \)-term tends to 0 as \( n \) tends to infinity.
1.2 Indecomposable hypergraphs

A (multi)-hypergraph $H$ on a set $N$ of $n$ vertices is a collection of (not necessarily distinct) subsets of $N$, called edges. The hypergraph is $d$-regular if every member $i \in N$ lies in precisely $d$-edges. A subhypergraph of $H$ is a sub (multi)-set of $H$. A regular hypergraph $H$ is indecomposable if it contains no proper nonempty regular subhypergraph. Let $D(n)$ denote the maximum possible degree $d$ so that there exists a $d$-regular indecomposable hypergraph on $n$ vertices. Huckeman and Jurkat (cf. [3]) proved that $D(n)$ is finite for every $n$ (see also [1] for another proof). The problem of determining or estimating the value of $D(n)$ received a considerable amount of attention (see [3] and its references). It is easy to see that $D(1) = D(2) = 1$ and $D(3) = 2$. Huckeman, Jurkat and Shapley proved that $D(n) \leq \frac{n+1}{2}$, for every $n$, Shapley showed that $D(n) \geq 2^{n-3} + 1$ for all $n > 2$. For more details, including the precise values of $D(n)$ for $n \leq 5$, see [3]. Here we improve the lower bound and show that it is not far from the above mentioned upper bound.

**Theorem 1.4** Let $n$ be a power of 2, then

$$D(n) \geq \frac{1}{4e^{4n/2}}n^{n/2}.$$ 

Note that since $D(n)$ is clearly a non-decreasing function of $n$ the above theorem shows that $D(n) \geq n^\Omega(n)$ for every $n$.

The proofs of both theorems above are based on a construction of H˚astad [5], described in the next section. In Section 3 we show how it implies Theorem 1.1 and in Section 4 we prove Theorem 1.4. Both proofs can be converted into constructive ones, as described in Section 5. Some of the properties of the constructive proof are applied in Section 6 to prove Proposition 1.2 and Theorem 1.3, together with some related results. The final Section 7 contains various concluding remarks and open problems.

2 Threshold gates

A threshold gate of $n$ inputs is a function $F : \{-1,1\}^n \mapsto \{-1,1\}$ defined by

$$F(x_1, \ldots, x_n) = \text{sign}\left(\sum_{i=1}^{n} w_i x_i - t\right),$$

where $w_1, \ldots, w_n, t$ are reals called weights, chosen in such a way that the sum $\sum_{i=1}^{n} w_i x_i - t$ is never zero for $(x_1, \ldots, x_n) \in \{-1,1\}^n$. Threshold gates are the basic building blocks of Neural Networks,
and have been studied extensively. See, e.g., [7] and its references. It is easy to see that every threshold gate can be realized with integer weights. Various researchers proved that there is always a realization with integer weights satisfying $|w_i| \leq 2^{-n(n+1)(n+1)/2}$. See, e.g., [9] for a proof.

There are several simple constructions of threshold gates of $n$ inputs that require some weights of size $2^{\Omega(n)}$. Håstad [5] constructed threshold gates that require larger weights, thus showing that the above mentioned upper bound is nearly tight. The precise statement of his theorem is the following.

**Theorem 2.1 ([5], Theorem 2.10)** For every $n$ which is a power of 2 there exists a threshold gate $F$ of $n$ inputs (described explicitly) so that if $w_1, \ldots, w_n, t$ are integers and

$$F = \text{sign}(\sum_{i=1}^{n} w_i x_i - t)$$

for every $(x_1, \ldots, x_n) \in \{-1, 1\}^n$, then for every $j$

$$|w_j| \geq \frac{1}{2ne^n2^n}n^{n/2}.$$ 

In addition, the above $F$ can be realized by weights $w_1, \ldots, w_n, t$ with $t = 0$.

### 3 Coin-weighing

In this section we prove Theorem 1.1. Let $V_n$ denote the set of all vectors of length $n$ with $\{-1, 1, 0\}$ coordinates. A sequence $v_1, \ldots, v_m$ of not necessarily distinct members of $V_n$ is called admissible if the sum of its elements is the zero vector 0, and it contains no proper nonempty subsequence whose sum is the zero vector. Kozlov and Vu [8] proved the following statement.

**Fact:** For every $n, m(n)$ is precisely the maximum possible length $m$ of an admissible sequence $v_1, \ldots, v_m$ of members of $V_n$.

The proof of this fact is not difficult, and we describe it, for the sake of completeness. Given an admissible sequence as above, let $A = (a_{ij})$ be the $n$ by $m$ matrix whose columns are the vectors $v_1, \ldots, v_m$. Given $m$ coins $\{1, 2, \ldots, m\}$, perform $n$ weighings as follows. For each $i$, $1 \leq i \leq n$, compare the set of coins $L_i = \{j : a_{ij} = -1\}$ with the set of coins $R_i = \{j : a_{ij} = 1\}$. Note that since the sum of columns of $A$ is 0, $|L_i| = |R_i|$ for every $i$ and hence if some weighing is not balanced, not all the coins have the same weight. On the other hand, we claim that if all weighings are balanced then all the coins have the same weight. To see this, assume this is false, let $\{1, 2, \ldots, m\} = J_1 \cup J_2$ be a partition of the set of coins into two nonempty disjoint sets, and assume all the coins in $J_1$ are of weight $\alpha$ and all those in $J_2$ are of weight $\delta$, where $\alpha \neq \delta$. Define $v_\alpha = \sum_{j \in J_1} v_j$ and $v_\delta = \sum_{j \in J_2} v_j$. Then, as all weighings are balanced,

$$\alpha v_\alpha + \delta v_\delta = 0.$$ 

Since the sum of all vectors $v_j$ is 0,

$$v_\alpha + v_\delta = 0.$$ 

4
As \( \alpha \neq \delta \) this implies that \( v_{\alpha} = v_{\delta} = 0 \), contradicting the assumption that the sum of no proper subsequence of the given sequence is 0. Therefore, \( m(n) \) is at least the length of the above sequence.

The proof of the converse inequality is similar. As the two possible weights of the coins are not known in advance and may be arbitrarily close to each other, it is easy to see that we may assume that the algorithm always compares in each weighing sets of coins of equal cardinalities. For each subset \( l \subseteq n \), let \( L_i, R_i \) be the two subsets of coins the algorithm compares in weighing number \( i \), assuming all previous weighings are balanced. Define a matrix \( A = (a_{ij}) \) by letting \( a_{ij} = -1 \) iff \( j \in L_i, 1 \) iff \( j \in R_i \) and 0 otherwise. Since \( |L_i| = |R_i| \) for all \( i \), the sum of columns of \( A \) is 0. Moreover, if there is a proper nonempty subset of columns of \( A \) whose sum is 0 then even if all the weighings are balanced it may be that the weights of all coins in this subset are \( \alpha \) and those of all other coins are \( \delta \) (for any choice of \( \alpha, \delta \)). Therefore, from any valid weighing algorithm we get a matrix whose columns form a sequence of vectors in \( V_n \) with the desired properties. This completes the proof of the fact.

In order to prove Theorem 1.1 using the above fact we have to prove the existence of a long admissible sequence. To do so, we apply the following procedure for obtaining such a sequence. Let \( B = (b_{ij}) \) be an \( n \) by \( (n + 1) \) matrix whose columns are members of \( V_n \), and suppose the rank of \( B \) is \( n \). Then the system of \( n \) linear equations \( By = 0 \), where \( y = (y_1, \ldots, y_{n+1}) \) is a (column) vector of variables has a one dimensional solution, that is, all the solutions of the system are scalar multiples of any fixed given nontrivial solution. The system obviously has a nontrivial integral solution, by Cramer’s rule, for example. Among all integral solutions, let \( y = (y_1, \ldots, y_{n+1}) \) be one with the minimum possible \( l_1 \)–norm, that is, with the minimum possible value of the sum \( \sum_{j=1}^{n+1} |y_j| \). Define \( z_j = |y_j| \), and note that by the minimality in the choice of \( y \) the greatest common divisor of the numbers \( z_j \) is 1. Let \( u_j \) be the column number \( j \) of \( B \) if \( y_j \) is positive, and the additive inverse of that column otherwise. Note that \( \sum_{j=1}^{n+1} z_j u_j = 0 \) and that if \( \sum_{j=1}^{n+1} s_j u_j = 0 \) then the vector \( s = (s_1, \ldots, s_{n+1}) \) is a scalar multiple of \( z = (z_1, \ldots, z_{n+1}) \). Therefore, if the numbers \( s_j \) are integers then \( s \) is an integral multiple of \( z \). This is because it is obviously a rational multiple of \( z \), that is \( s = \frac{p}{q} z \), where \( p, q \) are relatively prime, implying that \( q \) divides each \( z_j \), which is possible only for \( |q| = 1 \), as the greatest common divisor of the numbers \( z_j \) is 1. In particular, it follows that if \( \sum_{j=1}^{n+1} s_j u_j = 0 \) for some integers \( s_j \), not all zeros, then

\[
\sum_{j=1}^{n+1} |s_j| \geq \sum_{j=1}^{n+1} z_j.
\]  

We can now define an admissible sequence consisting of \( \sum_{j=1}^{n+1} z_j \) members of \( V_n \) by taking \( z_j \) copies of \( u_j \), for every \( j \). The sum of the members of this sequence is clearly the zero vector. Moreover, any proper nonempty subsequence of it contains \( s_j \) copies of \( u_j \) for some \( 0 \leq s_j \leq z_j \), where \( 0 < \sum_{j=1}^{n+1} s_j < \sum_{j=1}^{n+1} z_j \), and hence the sum of its members cannot be 0, by (2). We have thus proved the following.

\[
\sum_{j=1}^{n+1} |s_j| \geq \sum_{j=1}^{n+1} z_j.
\]
Proposition 3.1 Let $B$ be an $n$ by $(n+1)$ matrix of rank $n$ whose columns are members of $V_n$, and suppose that every nontrivial integral solution $y = (y_1, \ldots, y_{n+1})$ of the system $By = 0$ satisfies
\[
\sum_{j=1}^{n+1} |y_j| \geq M.
\]
Then $m(n) \geq M$.

The main part of the proof of Theorem 1.1 is the following.

Proposition 3.2 For every $n$ which is a power of 2 there exists an $n$ by $(n+1)$ matrix $B$ of rank $n$ with $\{-1,1\}$-entries so that every nontrivial integral solution $y = (y_1, \ldots, y_{n+1})$ of the system $By = 0$ satisfies
\[
\sum_{j=1}^{n+1} |y_j| \geq \frac{1}{2e^{4n^2}}n^{n/2}.
\]

Proof. Let
\[
F(x_1, \ldots, x_n) : \{-1,1\}^n \mapsto \{-1,1\}
\]
be a threshold gate satisfying the assertion of Theorem 2.1. Define
\[
P = \{(\epsilon_1, \ldots, \epsilon_n) \in \{-1,1\}^n, \quad F(\epsilon_1, \ldots, \epsilon_n) = 1\}
\]
and
\[
Q = \{(\epsilon_1, \ldots, \epsilon_n) \in \{-1,1\}^n, \quad F(\epsilon_1, \ldots, \epsilon_n) = -1\}.
\]
Consider the following system of $2^n$ inequalities with the $n$ variables $w_1, \ldots, w_n$
\[
\sum_{j=1}^{n} \epsilon_j w_j \geq 1 \quad \text{for all} \quad (\epsilon_1, \ldots, \epsilon_n) \in P;
\]
\[
\sum_{j=1}^{n} \epsilon_j w_j \leq -1 \quad \text{for all} \quad (\epsilon_1, \ldots, \epsilon_n) \in Q.
\]
Since $F$ can be realized with weights $w_1, \ldots, w_n, t$ where $t = 0$ there is a solution of the above system of inequalities. We claim that there is a solution in which $n$ inequalities are tight, where the linear forms of these inequalities have full rank. This is in fact a standard result from the theory of Linear Programming, but since the proof is short we include it. Among all solutions of the above system of inequalities choose one, say $w' = (w'_1, \ldots, w'_n)$ with the maximum number of equalities. Let $L_i(w) = L_i(w_1, \ldots, w_n) = \delta_i$, $(i \in I)$ be the set of all these equalities. If the linear forms $L_i, i \in I$ span $R^n$, there is nothing to prove. Else, there is a nontrivial solution $w'' = (w''_1, \ldots, w''_n)$ of the system $L_i(w) = 0$ for all $i \in I$. Each point $w$ on the line $\{w' + tw'' : t \in R\}$ satisfies all the equalities $L_i(w) = \delta_i$ for $i \in I$, and the point corresponding to $t = 0$ satisfies our original system of inequalities as well. By choosing either the maximum or the minimum $t$ for which this is still true
we obtain a solution of the system with more equalities. (To see that there is such a \( t \), note that since \( w' \) is nontrivial, there is some \((\epsilon_1, \ldots, \epsilon_n) \in \{-1, 1\}^n\) whose inner product with \( w' \) is nonzero, and hence it is impossible that all points on the line satisfy all inequalities.) This contradicts the maximality in the choice of \( w' \) and completes the proof of the claim.

Let \( C \) denote the \( n \times n \) matrix whose rows are \( n \) tight independent linear forms \( L_i \) as above and let \( \delta \) be the corresponding vector of values of \( L_i(w') \). Note that \( C \) is an \( n \times n \) matrix of full rank with \( \{-1, 1\} \) entries and \( \delta \) is a vector with \( \{-1, 1\} \) coordinates. By the discussion above, our system of inequalities has a solution \( w' = (w'_1, \ldots, w'_n) \) which is the unique solution of the system of \( n \) equations \( Cw = \delta \). Let \( B \) be the \( n \times (n+1) \) matrix obtained from \( C \) by adding to it the column \( \delta \). Then \( y' = (w'_1, \ldots, w'_n, -1) \) is a nontrivial solution of the system \( By = 0 \) and any integral solution of it must be an integral multiple of \( y' \) (since the last coordinate has to be integral). Hence, any integral solution \( y \) of the system \( By = 0 \) is of the form \( y = py' = (pw'_1, \ldots, pw'_n, -p) \), where \( p \) is an integer, and it thus follows that either the vector of first \( n \) coordinates of any such solution or its additive inverse satisfies all inequalities in the system above. This shows that for any such \( y = (y_1, \ldots, y_{n+1}) \) either \( w_i = y_i \) or \( w_i = -y_i \) satisfy

\[
F(x_1, \ldots, x_n) = \text{sign} \left( \sum_{i=1}^{n} w_i x_i \right)
\]

for all \((x_1, \ldots, x_n) \in \{-1, 1\}^n\).

By Theorem 2.1 this implies that the absolute value of each of the first \( n \) coordinates of \( y \) is at least

\[
\frac{1}{2n e^{n^{4/3}2n n^{n/2}}},
\]

completing the proof of the proposition, and implying, in view of Proposition 3.1, the assertion of Theorem 1.1 as well. \( \Box \)

**Remark.** Note that since the matrix \( B \) in the last proposition has no zeros, in the weighing algorithm it provides every coin participates in every weighing.

### 4 Indecomposable hypergraphs

This short section contains the proof of Theorem 1.4. The proof is based on Proposition 3.2.

**Proof of Theorem 1.4.** Let \( B = (b_{ij}) \) be an \( n \times (n+1) \) matrix satisfying the assertion of Proposition 3.2. By replacing some columns of \( B \) by their inverses, if needed, we may and will assume that the only nontrivial relation between the columns of \( B \) is with all coefficients of the same sign. By replacing some of the rows of \( B \) by their inverses, if needed, we may and will assume that each entry in the last column of \( B \) is \(-1\). Let \( v_1, \ldots, v_n, v_{n+1} \) denote the columns of the resulting \( B \), then \( v_{n+1} = -J \), where \( J \) denotes the all 1 (column) vector. Let \( x = (x_1, \ldots, x_{n+1}) \) denote the nontrivial integral solution of \( Bx = 0 \) for which \( x_j \geq 0 \) for all \( j \) and \( \sum x_j \) is minimal. Then, by
Proposition 3.2

\[
\sum_{j=1}^{n+1} x_j \geq \frac{1}{2e4^{n^2/2}} n^{n/2}. \tag{3}
\]

Clearly,

\[
\sum_{j=1}^{n} x_j v_j = x_{n+1} J.
\]

Adding \( \sum_{j=1}^{n} x_j J \) to both sides and defining \( s = \sum_{j=1}^{n+1} x_j \) we conclude that

\[
\sum_{j=1}^{n} x_j (v_j + J) = sJ.
\]

Note that the number \( s \) is even (since each equation in the system \( Bx = 0 \) shows that some linear combination of the numbers \( x_j \) with \( \{-1, 1\} \)-coefficients is zero.) For each \( j, 1 \leq j \leq n \), define \( u_j = (v_j + J)/2 \). Note that each \( u_j \) is a \((0, 1)\)-vector, and that

\[
\sum_{j=1}^{n} x_j u_j = \frac{s}{2} J. \tag{4}
\]

Claim: There are no integers \( z_1, \ldots, z_n \geq 0 \) satisfying

\[
0 < \sum_{j=1}^{n} z_j < \sum_{j=1}^{n} x_j \tag{5}
\]

for which

\[
\sum_{j=1}^{n} z_j u_j = tJ
\]

for some integer \( t \).

Proof. Assuming there are such integers \( z_j \), double the last equality and subtract \( \sum_{j=1}^{n} z_j J \) from it to conclude that

\[
\sum_{i=1}^{n} z_j v_j = (2t - \sum_{j=1}^{n} z_j) J.
\]

This shows that the vector \((z_1, z_2, \ldots, z_n, 2t - \sum_{j=1}^{n} z_j)\) is an integral solution of the system \( By = 0 \), and it therefore must be an integral multiple of the vector \((x_1, \ldots, x_n, x_{n+1})\). This is impossible by (5), completing the proof of the claim.

Let \( H \) be the (multi)-hypergraph on the set of vertices \( N = \{1, 2, \ldots, n\} \) obtained by taking \( x_j \) copies of the edge \( \{i : b_{ij} = 1\} \) for each \( i \). By (4), \( H \) is \( s/2 \)-regular, and by the above claim it is decomposable. Hence

\[
D(n) \geq s/2 = \frac{1}{2} \sum_{j=1}^{n+1} x_j \geq \frac{1}{2e4^{n^2/2}} n^{n/2}
\]

where the last inequality follows from (3). This completes the proof of the theorem.  \( \square \)
5 Explicit constructions

The proofs of Theorems 1.1 and 1.4 described in the last two sections are existence proofs. It is desirable to find constructive versions of them, especially in the case of Theorem 1.1, since it is better to actually describe an explicit algorithm for solving our coin-weighing problem than to merely prove that one exists. By slightly modifying the proof of Theorem 2.1 given in [5] one can obtain a constructive proof for Proposition 3.2 (and hence for Theorems 1.1 and 1.4). In this section we present such an explicit construction. In the next section we apply some of the properties of this explicit construction in order to prove Theorem 1.3 and some related results.

Let \( n = 2^l \) be a power of 2. Our main task in this section is to define an \( n \times n \) matrix \( C \) with \( \{-1, 1\}\)-entries and show that the unique solution of the system \( Cz = J \), where \( z \) is a vector of \( n \) variables and \( J \) is the all 1 vector, has large coordinates.

To this end, define \( L = \{1, 2, \ldots, l\} \). By an easy inductive argument given in [5] the family of all \( n = 2^l \) subsets of \( L \) can be ordered in a sequence \( \alpha_1, \alpha_2, \ldots, \alpha_n \) such that for every \( 1 \leq i < n \), \( |\alpha_i| \leq |\alpha_{i+1}| \) and such that the symmetric difference of any two consecutive subsets \( \alpha_i \) and \( \alpha_{i+1} \) in the ordering is of size 1 or 2. Fix such an ordering, and let us index the rows of \( C \) by the subsets of \( L \) according to this ordering. The columns of \( C \) are indexed by the set \( V \) of all vectors \((x_1, \ldots, x_l)\) in \( \{-1,1\}^l \). Therefore, for each \( \alpha \subset L \), the row of \( C \) indexed by \( \alpha \) can be viewed as a function \( g_\alpha \) of \( x_1, \ldots, x_l \).

To define \( C \), we specify the function representing each of its rows. This is done as follows.

- The first \( l + 1 \) rows are simple; \( g_\emptyset \equiv 1 \) and \( g_{\{i\}} = x_i \) for each \( 1 \leq i \leq l \).
- Let \( \{a, b\} \) be the index of the first row (according to our fixed ordering) indexed by a set of cardinality 2, and let \( \{a\} \) be the index of the preceding row. Then
  \[
  g_{\{a, b\}}(x_1, \ldots, x_l) = x_a \quad \text{if} \quad (x_a, x_b) = (-1, 1),
  \]
  and
  \[
  g_{\{a, b\}}(x_1, \ldots, x_l) = -x_a \quad \text{otherwise}.
  \]
- For any row indexed by a set \( \{a, c\} \) of cardinality 2, for which the preceding row is indexed by another set of cardinality 2, \( \{a, b\} \), define
  \[
  g_{\{a, c\}}(x_1, \ldots, x_l) = x_a x_b \quad \text{if} \quad (x_a, x_b, x_c) \in \{(-1, 1, 1), (-1, -1, -1)\}
  \]
  and
  \[
  g_{\{a, c\}}(x_1, \ldots, x_l) = -x_a x_b \quad \text{otherwise}.
  \]
- Let \( \{a, b, c\} \) be the index of the first row indexed by a set of cardinality 3, and let \( \{a, b\} \) be the index of the preceding row. Then
  \[
  g_{\{a, b, c\}}(x_1, \ldots, x_l) = x_a x_b \quad \text{if} \quad (x_a, x_b, x_c) = (-1, -1, 1),
  \]
and
\[ g_{\{a,b,c\}}(x_1, \ldots, x_l) = -x_a x_b \text{ otherwise.} \]

• For any row indexed by a set \(\{a, b, d\}\) of cardinality 3, for which the preceding row is indexed by another set \(\{a, b, c\}\) of cardinality 3, define
\[ g_{\{a,b,d\}}(x_1, \ldots, x_l) = x_a x_b x_c \text{ if } (x_a, x_b, x_c, x_d) \in \{(−1, −1, 1, 1), (−1, −1, −1, −1)\} \]
and
\[ g_{\{a,b,d\}}(x_1, \ldots, x_l) = -x_a x_b \text{ otherwise.} \]

• Let \(\{a_1, a_2, \ldots, a_k\}\) be the first row indexed by a set of cardinality \(k \geq 4\), and let \(\{a_1, \ldots, a_k−1\}\) be the index of the preceding row. Let \(a\) be the last set in the ordering which is a proper subset of \(\{a_1, \ldots, a_k\}\) and is not \(\{a_1, \ldots, a_{k−1}\}\). Fix values \(b_1, \ldots, b_{k−1} \in \{-1, 1\}\) so that \(b_k = 1\) and \(\prod_{j=1}^{k−1} b_j \neq \prod_{j=1}^{k−1} b_j\). Then
\[ g_{\{a_1, \ldots, a_k\}}(x_1, \ldots, x_l) = x_{a_1} \cdots x_{a_{k−1}} \text{ if } (x_{a_1}, \ldots, x_{a_k}) = (b_1, \ldots, b_k), \]
and
\[ g_{\{a_1, \ldots, a_k\}}(x_1, \ldots, x_l) = -x_{a_1} \cdots x_{a_{k−1}} \text{ otherwise.} \]

• For any row indexed by a set \(\{a_1, \ldots, a_k−1, a_{k+1}\}\) of cardinality \(k \geq 4\), for which the preceding row is indexed by another set \(\{a_1, \ldots, a_k\}\) of cardinality \(k\), let \(\alpha\) denote the last set that differs from those two, and is a subset of \(\{a_1, \ldots, a_{k+1}\}\) containing precisely one of the two elements \(a_k, a_{k+1}\). Fix values \(b_1, \ldots, b_{k+1} \in \{-1, 1\}\) so that \(b_k = b_{k+1} = 1\) and \(\prod_{j \in \alpha} b_j \neq \prod_{j=1}^{k} b_j\). Then
\[ g_{\{a_1, \ldots, a_{k−1}, a_{k+1}\}}(x_1, \ldots, x_l) = x_{a_1} \cdots x_{a_k} \text{ if } (x_{a_1}, x_{a_2}, \ldots, x_{a_{k+1}}) \in \{(b_1, \ldots, b_{k+1}), (b_1, \ldots, b_{k−1}, −b_k, −b_{k+1})\}, \]
and
\[ g_{\{a_1, \ldots, a_{k+1}\}}(x_1, \ldots, x_l) = -x_{a_1} \cdots x_{a_k} \text{ otherwise.} \]

**Proposition 5.1** Let \(n\) and \(C\) be as above, let \(z\) be a vector of \(n\) variables indexed by the vectors in \(\{-1, 1\}^l\) and let \(J\) be the all 1 vector of length \(n\). Then in the unique solution of the system \(Cz = J\) each coordinate of \(z\) is an integral multiple of \(1/n\), and the absolute value of each such coordinate is at least
\[
\frac{n^{n/2}}{2ne^{4n^3/2n}}.
\]
The proof of the above proposition is very similar to the proof of the main result in [5]. We therefore only sketch it, pointing to the relevant lemmas in [5] where the precise details can be found.
Proof of Proposition 5.1 (Sketch). The main idea is to consider the Fourier transform of \( z \) instead of considering \( z \) itself. Let \( W \) be the \( n \) by \( n \) matrix whose rows are indexed by all subsets of \( L \) and whose columns are indexed by all vectors \( (x_1, \ldots, x_l) \in \{-1,1\}^l \), where the row indexed by \( \alpha \) is simply the function \( \prod_{i \in \alpha} x_i \). Let \( w \) be the (column) vector of length \( n \) indexed by the vectors in \( \{-1,1\}^l \) and defined by \( w = Wz \). Since \( W \) is a Hadamard matrix, \( z = \frac{1}{n} W^t w \), where \( W^t \) denotes the matrix \( W \) transposed. Substituting the expression of \( z \) in our system, we conclude that

\[
\frac{1}{n} C W^t w = J.
\]

The above system consists of all equations of the form

\[
(Wg_\alpha, w) = n = 2^l, \quad (\alpha \subset L),
\]

where here \( g_\alpha \) is considered as a column vector, and \((h,f)\) denotes the inner product of the two vectors \( h \) and \( f \).

The functions \( g_\alpha \) have been chosen so that each vector \( Wg_\alpha \) has a convenient form. Note that the coordinates of each such vector are indexed by the subsets of \( L \). It turns out that for each \( \beta \) that follows \( \alpha \) in our ordering, the coordinate indexed by \( \beta \) of \( Wg_\alpha \) is zero. The coordinate indexed by \( \alpha \) itself is \( 2^{l+1-|\alpha|} \), that indexed by the preceding subset of \( L \) is \(-2^{l-1-|\alpha|} \), and the rest of the coordinates lie in \( \{0,-2^{l+1-|\alpha|},2^{l+1-|\alpha|}\} \). Substituting the precise value of each such product \( Wg_\alpha \) in (6) we obtain a system of equations that shows that the coordinates of the vector \( w \) are all positive integers, and grow rapidly. This will enable us to deduce the assertion of the proposition.

More precisely, one can apply the (simple) computation in the proofs of lemmas 2.7, 2.8 and 2.9 in [5], which contain the expressions for \( Wg_\alpha \) for each \( \alpha \). Substituting these in (6) we get the following equations in the coordinates \( w_\alpha \) of the vector \( w \).

- The first \( l + 1 \) equations are simple; \( w_\emptyset = 1 \) and \( w_{\{i\}} = 1 \) for each \( 1 \leq i \leq l \).
- Let \( \{a,b\} \) be the index of the first row indexed by a set of cardinality 2, and let \( \{a\} \) be the index of the preceding row. Then
  \[
  w_{\{a,b\}} = w_{\{a\}} + w_{\{b\}} + w_\emptyset + 2.
  \]
- For any row indexed by a set \( \{a,c\} \) of cardinality 2, for which the preceding row is indexed by another set of cardinality 2, \( \{a,b\} \),
  \[
  w_{\{a,c\}} = w_{\{a,b\}} + w_{\{a\}} + w_{\{b\}} + 2.
  \]
- Let \( \{a,b,c\} \) be the index of the first row indexed by a set of cardinality 3, and let \( \{a,b\} \) be the index of the preceding row. Then
  \[
  w_{\{a,b,c\}} = 3w_{\{a,b\}} + w_{\{a,c\}} + w_{\{b,c\}} + w_{\{a\}} + w_{\{b\}} - w_{\{c\}} - w_\emptyset + 4.
  \]
• For any row indexed by a set \( \{a, b, d\} \) of cardinality 3, for which the preceding row is indexed by another set \( \{a, b, c\} \) of cardinality 3,

\[
w_{\{a,b,d\}} = 3w_{\{a,b,c\}} + w_{\{a,c\}} + w_{\{b,c\}} + w_{\{a,d\}} + w_{\{b,d\}} - w_{\{c\}} - w_{\{d\}} + 4.
\]

• Let \( \alpha \) be the first row indexed by a set of cardinality \( k (\geq 4) \), let \( \alpha' \) be the index of the preceding row and let \( \alpha'' \) be the last subset of \( \alpha \) that differs from \( \alpha \) and \( \alpha' \). Define \( B = \{ \beta \subset \alpha, \beta \neq \alpha, \alpha' \} \). Then there are numbers \( \epsilon_\beta \in \{-1, 1\} \) (that can be computed from the function \( g_\alpha \), but are not needed here) such that

\[
w_\alpha = (2^{k-1} - 1)w_{\alpha'} + w_{\alpha''} + \sum_{\beta \in B} \epsilon_\beta w_\beta + 2^{k-1}.
\]

For any row indexed by a set \( \alpha \) of cardinality \( k (\geq 4) \), for which the preceding row is indexed by another set \( \alpha' \) of cardinality \( k \), let \( \alpha'' \) denote the last set that differs from those two, is contained in \( \alpha \cup \alpha' \), and contains exactly one member of their symmetric difference. Let \( B \) denote the set of all subsets of \( \alpha \cup \alpha' \) other than \( \alpha, \alpha' \), that contain exactly one member of their symmetric difference. Then

\[
w_\alpha = (2^{k-1} - 1)w_{\alpha'} + w_{\alpha''} + \sum_{\beta \in B} \epsilon_\beta w_\beta + 2^{k-1},
\]

for some \( \epsilon_\beta \in \{-1, 1\} \).

The above equations enable us to determine the numbers \( w_\alpha \) one by one, as each of them is expressed in terms of the preceding ones. It is obvious that all of them are integers, and by the argument in Lemma 2.9 of [5], if \( |\alpha| = k \geq 2 \) and \( \alpha' \) is the preceding set, then

\[
w_\alpha > (2^{k-1} - 1)w_{\alpha'}.
\]

By the computation in [5] that follows the proof of Lemma 2.9, this implies that for the last coordinate \( w_L \) of \( w \),

\[
w_L \geq \frac{n^{n/2}}{e^{4n^{3/2}}2^{n}},
\]

and that it exceeds half the sum of all previous coordinates of \( w \). Since \( z = \frac{1}{n}W^tw \), it follows that each coordinate of \( z \) is an integral multiple of \( 1/n \) and that its absolute value is at least

\[
\frac{n^{n/2}}{2ne^{4n^{3/2}}2^{n}},
\]

completing the proof of the proposition. \( \square \)

Proposition 5.1 supplies a constructive solution of Proposition 3.2, as follows.
Proposition 5.2 Let $n = 2^l$ be a power of 2, let $C$ be the $n$ by $n$ matrix described in the beginning of this section, and let $B$ be the $n$ by $(n+1)$ matrix obtained from $C$ by adding to it the all 1 column. Then $B$ is a rank $n$ matrix with $\{-1,1\}$ entries, and every integral solution $y = (y_1,\ldots,y_{n+1})$ of the system $B y = 0$ satisfies

$$\sum_{j=1}^{n+1} |y_j| \geq \frac{1}{2e4^{n^2}2^n} n^{n/2}.$$ 

Moreover, if $y$ is a solution with the minimum possible $l_1$–norm then $|y_{n+1}| \leq n$.

Proof. If $z = (z_1,\ldots,z_n)$ is the unique solution of the system $C z = J$, then $y' = (z_1,\ldots,z_n, -1)$ is a solution of $B y = 0$. Since any other solution of this system is a multiple of $y'$ it follows that any integral solution must be an integral multiple of $y'$ (as the last coordinate must be integral). The desired lower estimate for the $l_1$–norm of any such solution follows from Proposition 5.1. Since each entry of $y'$ above is an integral multiple of $1/n$, $n y'$ is integral and the last claim of the proposition follows. □

Since the matrix $C$ is explicit, the above proof supplies constructive proofs of Theorems 1.1 and 1.4. The fact that $y_{n+1} \leq n$ will be useful in the proof of Theorem 1.3 presented in the next section.

6 More on coin-weighing

In this section we prove Proposition 1.2 and Theorem 1.3.

Proof of Proposition 1.2. For an $r$ by $(r + 1)$ matrix $B$, let $B_j$ denote the matrix obtained from $B$ by deleting its $j^{th}$ column, let $b$ denote the greatest common divisor of the $r + 1$ numbers $\{|\det(B_j)| : 1 \leq j \leq r + 1\}$, and define

$$g(B) = \frac{\sum_{j=1}^{r+1}|\det(B_j)|}{b}.$$ 

Let $\gamma(r)$ denote the maximum possible value of $g(B)$, as $B$ ranges over all $r$ by $(r + 1)$ matrices of $\{0, -1, 1\}$ entries. Kozlov and Vu proved in [8] that

$$m(n) \leq \frac{3^n - 1}{2} \max\{\gamma(r) : r \leq n\}.$$ 

They also showed that $\gamma(r) \leq (r + 1)^{(r+1)/2}$ and hence deduced that (1) holds. Here we slightly improve this estimate and prove that for every $r \geq 2$

$$\gamma(r) \leq (r + 1)^{(r-1)/2}. \quad (7)$$ 

Together with the above mentioned inequality this implies the assertion of Proposition 1.2.

To prove (7), let $B$ be an $r$ by $(r + 1)$ matrix with $\{0, -1, 1\}$-entries. We have to bound $g(B)$. If there are at least two rows of $B$ that contain no zeros, then each submatrix $B_j$ contains at least two rows with $\{-1,1\}$ entries. Adding one of them to the other, we get a matrix with a row all of whose
entries are \( \{0, -2, 2\} \) and hence its determinant is divisible by 2. Since this is also the determinant of \( B_j \) itself we conclude that in this case all numbers \( |\det(B_j)| \) are divisible by 2. Thus, in this case, 
\[
g(B) \leq \sum_{j=1}^{r+1} |\det(B_j)|/2.
\]
By adding to \( B \) a row \((b_1, \ldots, b_{r+1})\) of \( \{-1, 1\}\) entries, where \( b_j = \text{sign}(B_j) \) we obtain a matrix \( B' \) satisfying 
\[
|\det(B')| = \sum_{j=1}^{r+1} |\det(B_j)|.
\]
By Hadamard Inequality, 
\[
|\det(B')| \leq (r + 1)^{(r+1)/2}
\]
and hence in this case 
\[
g(B) \leq \frac{(r + 1)^{(r+1)/2}}{2} < (r + 1)^{(r-1)/2},
\]
as needed.

It remains to bound \( g(B) \) in case each of its rows, but possibly one, contains at least one zero. In this case, by Hadamard Inequality and with \( B' \) as above,
\[
g(B) \leq \sum_{j=1}^{r+1} |\det(B_j)| = |\det(B')| \leq (r + 1)^{(r-1)/2}.
\]
Since \( B \) was arbitrary, the desired result follows.

In order to prove Theorem 1.3 we consider a slightly more general coin-weighing problem. Let \( M(n) \) denote the maximum possible number \( m \) such that given a set of \( m \) coins out of a collection of coins of an arbitrary number of unknown distinct weights, and given a distinguished coin which is known to be either the heaviest or the lightest one among the given \( m \) coins, one can decide if all the coins have the same weight or not using \( n \) weighings in a regular balance beam. Note that the distinguished coin may be either the heaviest or the lightest, and it is not known in advance which of the two it is. If there are only two possible weights, then any coin is distinguished, and hence \( m(n) \geq M(n) \). The reason for defining the function \( M(n) \) is that it is easily shown to be super-multiplicative, as follows.

**Lemma 6.1** For every positive integers \( n_1 \) and \( n_2 \),
\[
M(n_1 + n_2) \geq M(n_1)M(n_2).
\]

**Proof.** Put \( m_1 = M(n_1) \), \( m_2 = M(n_2) \). Given a collection of \( m_1m_2 \) coins together with a distinguished one, we first apply the algorithm to the first \( m_1 \) coins (including the distinguished one), and use \( n_1 \) weighings to decide if all these coins have the same weight. If not, the algorithm ends. Otherwise, we split all coins into groups of size \( m_1 \), where the first group is the one consisting of the \( m_1 \) coins we already know to be equal. Viewing the groups as new coins, note that the first one must be either the heaviest or the lightest group. We can thus apply the algorithm and check the \( m_2 \) groups in \( n_2 \) weighings. If all the groups have the same weight, so do all the coins, and otherwise, not all coins are identical.

To obtain a lower bound for \( M(n) \) we prove the following.
Proposition 6.2 Let \( n = 2^l \) be a power of 2. Then
\[
M(n + l) \geq \frac{1}{2e^n n^{n/2}}.
\]

Proof. Let \( B \) be the \( n \times n+1 \) matrix described in Proposition 5.2. Let \( y = (y_1, \ldots, y_{n+1}) \) be an integral solution of minimum \( l_1 \)-norm of the system \( By = 0 \). Let \( u_j \) be the column number \( j \) of \( B \) if \( y_j \) is positive, and its additive inverse if \( y_j \) is negative, and define \( z_j = |y_j| \). Note that \( z_{n+1} \leq n \). We need the following simple lemma.

Lemma 6.3 There is a vector \( w \in \mathbb{R}^n \) whose inner products with the vectors \( u_j \) satisfy
\[ (w, u_j) < 0 \text{ for all } 1 \leq j \leq n \text{ and } (w, u_{n+1}) > 0. \]

Proof (of Lemma). Since the rank of \( B \) is \( n \), the only nontrivial linear dependence between the vectors \( u_j \) is
\[
\sum_{j=1}^{n+1} z_j u_j = 0
\]
(its scalar multiples), in which \( z_{n+1} \) is strictly positive. It follows that 0 is not in the convex hull of the vectors \( u_1, \ldots, u_n \), implying that there is a hyperplane through the origin so that all the vectors \( u_j \) lie in its negative side. The vector \( u_{n+1} \) must lie on the positive side, since 0 is a nonnegative linear combination of the vectors \( u_j \). If \( \sum_{j=1}^{n+1} w_i x_i = 0 \) is the equation of this hyperplane, then \( (w, u_j) < 0 \) for all \( 1 \leq j \leq n \), and \( (w, u_{n+1}) > 0 \), where \( w = (w_1, \ldots, w_n) \). \( \square \)

Returning to the proof of the proposition, define \( m = \sum_{j=1}^{n+1} z_j \) and let \( A = (a_{i,r}) \) be the \( n \times m \) matrix whose columns consist of \( z_j \) copies of \( u_j \), for \( 1 \leq j \leq n+1 \). Given a collection of \( m \) coins together with a distinguished one, our weighing algorithm proceeds as follows. In the first \( l = \log_2 n \) weighings we apply the trivial doubling algorithm for checking if the first \( n \) coins (including the special one) have equal weights. If this is the case, we associate each column of \( A \) with a coin, where all the coins associated to the \( z_{n+1} \) columns which are duplicates of \( u_{n+1} \) are among the coins whose weights are already known to be equal to the weight of the distinguished coin. We claim that if all weighings are balanced, then all the coins have the same weight. To see this, let \( \alpha_r \) denote the weight of the coin associated with the \( r^{th} \) column, and let \( \delta_r \) denote the inner product of this column with the vector \( w \) of Lemma 6.3. Since the sum of columns of \( A \) is 0 it follows that
\[
\sum_{r=1}^{m} \delta_r = 0. \tag{8}
\]
Since all weighings are balanced \( A\alpha = 0 \), where \( \alpha \) is the column vector whose coordinates are the weights \( \alpha_r \). Taking the inner product with \( w \) we conclude that
\[
\sum_{r=1}^{m} \delta_r \alpha_r = 0. \tag{9}
\]
Let \( \{1, 2, \ldots, m\} = S \cup R \) be a partition of the set of indices of the columns of \( A \) into two disjoint sets, where \( S \) is the set of all columns corresponding to copies of \( u_{n+1} \), and \( R \) is the set of all other columns. Note that by Lemma 6.3, \( \delta_r < 0 \) for all \( r \in R \) whereas \( \delta_r = (w, u_{n+1}) > 0 \) for all \( r \in S \).
Denote \((w, u_{n+1}) = \delta\), and let \(\alpha\) denote the weight of the distinguished coin (which is also the weight of each of the coins associated with a column in \(S\)). Then, by (8)

\[
\sum_{r \in R} (-\delta_r) = z_{n+1} \delta,
\]

that is,

\[
\sum_{r \in R} -\delta_r z_{n+1} \delta = 1.
\]

Similarly, by (9),

\[
\sum_{r \in R} -\delta_r z_{n+1} \delta \alpha_r = \alpha.
\]

By the last two equations, \(\alpha\) is a weighted average of the weights \(\alpha_r\), and since \(\alpha\) is either the smallest or the biggest \(\alpha_r\), by assumption, it follows that \(\alpha = \alpha_r\) for all \(r \in R\), showing that indeed all coins have the same weight.

Since by Proposition 5.2

\[
m = \sum_{j=1}^{n+1} z_j \geq \frac{1}{2e^{4n^3}} n^{n/2}.
\]

this completes the proof. \(\square\)

**Corollary 6.4** The function \(M(n)\) satisfies

\[
M(n) = n^{(\frac{1}{2} + o(1))n},
\]

where the \(o(1)\)-term tends to 0 as \(n\) tends to infinity.

**Proof.** Since \(M(n) \leq m(n)\) the fact that

\[
M(n) \leq n^{(\frac{1}{2} + o(1))n}
\]

follows from the upper bound (1) mentioned in the introduction (or from Proposition 1.2.) To prove the lower bound we argue as follows. Given a large integer \(n\), let \(g\) be the biggest power of 2 which does not exceed \(n/p\), where \(p = p(n)\) is a large integer, to be chosen later. By Proposition 6.2

\[
M(g + \log g) \geq \frac{1}{2e^{4g^3/2g}} g^{g/2}.
\]

Let \(s(g + \log g)\) be the largest integral multiple of \((g + \log g)\) which does not exceed \(n\). Then, by the monotonicity of the function \(M(n)\) and by Lemma 6.1,

\[
M(n) \geq M(s(g + \log g)) \geq \left(\frac{g^{g/2}}{2e^{4g^3/2g}}\right)^n > \frac{g^{ng/2}}{2^{10g^2}}.
\]
Since $gs \leq n$, $g \geq \frac{n}{2p}$ and $gs > n - s \log g - g - \log g$ we conclude that

$$M(n) \geq \frac{(\frac{n}{2p})^{gs/2}}{2^{10n}} \geq \frac{n^{n/2}}{2^{\frac{1}{2} \log g + s + \log g}} \frac{n}{(2p)^{n/2} 2^{10n}}.$$

Choosing, for example, $p = \lceil \log n \rceil$ it follows that $\frac{n}{2^{\lceil \log g \rceil}} \leq g \leq \frac{n}{\log n} = o(n)$, $s \log g < n \log g/g = o(n)$, and hence the denominator in the last lower bound for $M(n)$ is at most $n^{o(n)}$, completing the proof of the corollary. $\Box$

Note that the last proof is constructive in the sense that it provides an explicit weighing algorithm for the corresponding problem.

**Proof of Theorem 1.3.** The upper bound follows from inequality (1) mentioned in the introduction (or from Proposition 1.2). The lower bound follows from the last corollary, and the fact that $m(n) \geq M(n)$. $\Box$

### 7 Concluding remarks

- The results about $m(n)$ described above apply to the slightly more general case of generic weights considered in [8]. A set of weights $w_1, \ldots, w_t$ is called generic if there are no integers $\lambda_1, \ldots, \lambda_t$, not all zeros, such that $\sum_{i=1}^{t} \lambda_i = 0$ and $\sum_{i=1}^{t} \lambda_i w_i = 0$. Note that any set of two weights is generic. Let $m'(n)$ denote the maximum possible number $m$ such that given a set of $m$ coins out of a collection of coins of unknown generic weights, one can decide if all the coins have the same weight or not using $n$ weighings in a regular balance beam. It is easy to see that the results described in Sections 3 and 5 apply to this case (without any essential change in the proofs) and show (constructively) that for every $n$ which is a power of 2

$$m'(n) \geq \frac{1}{2e^{4n^3} 2^n} n^{n/2}.$$

- Let $m(n, k)$ denote the maximum possible number $m$ such that given a set of $m$ coins out of a collection of coins of $k$ unknown distinct weights, one can decide if all the coins have the same weight or not using $n$ weighings in a regular balance beam. In particular, $m(n, 2)$ is the function $m(n)$ considered in the previous sections. Surprisingly, it turns out that $m(n, k)$ for $k \geq 3$ is much smaller than $m(n, 2) (= n^{O(n)})$. In a subsequent joint paper with Kozlov [2] we show that for every $3 \leq k \leq n + 1$, $m(n, k) = \Theta(n \log n / \log k)$.

- Although the asymptotic behaviour of the two functions $m(n)$ and $D(n)$ has been determined quite accurately in the previous sections, the problem of determining these two functions precisely remains open, and seems very difficult. Our best lower bound for $m(n)$, described in Section 5, is based on an algorithm in which every coin participates in every weighing, and it can be slightly improved by allowing matrices with zeros in the proof. This does not seem to imply any real progress in the study of the precise value of $m(n)$.
• Although the function $m(n)$ is monotone by definition, it is not clear that so is the following version of its inverse. For an integer $m$, let $n(m)$ denote the minimum integer $n$ such that given a set of $m$ coins out of a collection of coins of two unknown distinct weights, one can decide if all the coins have the same weight or not using $n$ weighings in a regular balance beam. It is not clear if for $m' < m$ the inequality $n(m') \leq n(m)$ holds, since the existence of an efficient weighing algorithm for $m$ does not seem to imply the existence of an efficient one for a smaller number of coins. Using our techniques here we can, however, determine the asymptotic behaviour of $n(m)$ and show that
\begin{equation}
    n(m) = (2 + o(1)) \frac{\log m}{\log \log m},
\end{equation}
where the $o(1)$-term tends to zero as $m$ tends to infinity.

**Acknowledgment** Part of this work was done during a Combinatorics workshop in Oberwolfach, Germany, organized by W. Deuber, D. Jackson and D. Jungnickel in January 1996. I would like to thank the organizers and the participants of the workshop, including, in particular, A. Bjorner and G. Ziegler, for helpful discussions. I would also like to thank D. Kozlov for sending me an early draft of [8] and for helpful comments.

**References**


