The Geometry of Coin-Weighing Problems (Extended Abstract)

Noga Alon * Dmitry N. Kozlov † Van H. Vu ‡

Abstract

Given a set of m coins out of a collection of coins of k 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 $m(n,k)$ denote the maximum possible number of coins for which the above problem can be solved in n weighings. We show that $m(n,2) = n^{(\frac{1}{2}+o(1))n}$, whereas for all $3 \leq k \leq n+1$, $m(n,k)$ is much smaller than $m(n,2)$ and satisfies $m(n,k) = \Theta(n \log n / \log k)$. The proofs have an interesting geometric flavour, and combine Linear Algebra techniques with geometric, probabilistic and combinatorial arguments.

*Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email address: 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.

†Department of Mathematics, Royal Institute of Technology, S-100 44, Stockholm, Sweden. Email address: kozlov@math.kth.se

‡Department of Mathematics, Yale University, New Haven, CT-06511, USA. Email address: vu-ha-van@math.yale.edu

1 Introduction

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. There are numerous questions of this type, see, e.g., [9] and its many references. Here we study the following variant of the old problems, which we call *the all equal problem.* Given a set of m coins, we wish to decide if all of them have the same weight or not, when various conditions about the weights are known in advance. The case in which the coins are given out of a collection of coins of k unknown distinct weights is of special interest. Let $m(n,k)$ denote the maximum possible number of coins for which this problem can be solved in n weighings. The case $k = 2$ has been considered in [12], following related questions discussed in [5] and other places. The authors of [12] observed that $m(n,2) \geq 2^n$ for every n. (To see this, note that $m(n,1) = 2$ and that once we already have m coins which are known to have the same weights, we can compare them to another set of m new coins. Since there are only two possible weights, if the weighing is balanced all $2m$ coins have the same weights.) Somewhat surprisingly, this bound is not tight. Applying a geometric approach, we show here that in fact $m(n,2) > 2^n$ for all $n > 2$. Combining this approach with some simple results in Lattice geometry as well as a construction of Håstad [10] of *threshold gates* that require large weights we determine the asymptotic behaviour of $m(n,2)$ as follows.

Theorem 1.1 *The function $m(n,2)$ satisfies*

$$m(n,2) = n^{(\frac{1}{2}+o(1))n},$$

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

The proof, with some extra work, provides an explicit weighing algorithm for the corresponding problem.

As a byproduct, we improve results of Shapley, van Lint and Pollak on a problem in Extremal Combinatorics motivated by the study of cores in n-person games and settle an open problem of Graham and Sloane concerning the norms of inverses of nonsingular matrices with $\{-1,1\}$ entries.

Surprisingly, it turns out that for $k \geq 3$, $m(n,k)$ is much smaller than $m(n,2)$. Using probabilistic arguments we prove the following.

Theorem 1.2 *There are two absolute positive constants c and C such that for every $n+1 \geq k \geq 3$*

$$c\frac{n\log n}{\log k} \leq m(n,k) \leq C\frac{n\log n}{\log k}.$$

It is worth noting that for $k > n+1$, $m(n,k) = n+1$, as we observe in Section 3.

Unlike the proof of Theorem 1.1, that of Theorem 1.2 is probabilistic, and does not supply an explicit weighing algorithm. For the special case $k = 3$ in which the three potential distinct weights are known to form an arithmetic progression we can describe an explicit algorithm.

Our basic approach is geometric. The geometric point of view is motivated by the observation that if we let $(w_1, w_2, \ldots, w_m)$ denote the weight-vector of the coins, then any weighing is simply a linear test, and its result determines if this vector lies on the corresponding hyperplane, or lies in one of the corresponding half-spaces. Therefore, any weighing algorithm is a linear decision tree. This implies that several known results about the complexity of linear decision trees, including the results in [6], [3], [4] which are based on geometric and topological arguments, yield immediately results about certain coin-weighing problems. The geometric approach needed for studying the all equal problem is, however, somewhat different, and is briefly explained in Section 2. In Section 3 we make several simple observations about the problem, including the observation that if no information on the weights of the coins is given in advance, then $m-1$ weighings are both necessary and sufficient for solving the all equal problem for m coins. In Sections 4 and 5 we study the asymptotic behaviour of $m(n,2)$ and show how it is related to the existence of threshold gates that require large weights. A very brief sketch of the proof of Theorem 1.2 is given in Section 6 and the final Section 7 contains some concluding remarks about related results and open problems. Due to space limitations we omit most detailed proofs from this extended abstract. These will appear in the full version of the paper(s).
All logarithms throughout the paper are in base 2, unless otherwise specified.

2 The basic approach

There is a simple correspondence between coin weighing algorithms for the all equal problem and matrices with $\{0,-1,1\}$-entries.

To see this correspondence, consider weighing algorithms for the all equal problem for coins chosen out of a collection of k distinct (unknown) weights. Let $W_{m,k}$ denote the set of all real vectors of length m with positive coordinates and with at most k distinct coordinates. The set $W_{m,k}$ represents the set of all possible weight-vectors of our given m coins. Let $\mathcal{A}_{n,m}$ denote the set of all n by m matrices with $\{0,-1,1\}$-entries whose sum of columns is the zero vector. We can associate each matrix $A=(a_{ij}) \in \mathcal{A}_{n,m}$ with a weighing algorithm as follows. Put $[m]=\{1,\ldots,m\}$ and define, for each i, $1 \leq i \leq n$, two disjoint subsets L_i and R_i of $[m]$ by $L_i=\{j:\ a_{ij}=-1\}$ and $R_i=\{j:\ a_{ij}=1\}$. Note that since the sum of each row of A is 0, $|L_i|=|R_i|$. Trying to solve the all equal problem for a given set of m coins denoted $\{1,2,\ldots,m\}$, the weighing algorithm determined by A consists of n weighings. For $1 \leq i \leq n$ the algorithm compares, in step number i, the coins in L_i with those in R_i. If all weighings are balanced the algorithm declares that all coins have the same weight, otherwise, it states that not all weights are equal. It is not difficult to see that a necessary and sufficient condition for the algorithm to solve correctly the all equal problem for coins with up to k distinct weights is that the only solutions of the system $Ax=0$ which lie in $W_{m,k}$ are constant vectors. To see this, observe that since $|L_i|=|R_i|$ for every i, if not all the weighings are balanced, then certainly not all the coins have the same weight. If, on the other hand, all weighings

are balanced, and it is known that the vector of weights of the coins lies in $W_{m,k}$, then the vector of correct weights must lie in $ker(A) \cap W_{m,k}$, showing that the algorithm is correct iff there are no nonconstant vectors in $ker(A) \cap W_{m,k}$.

We have thus seen that any matrix $A \in \mathcal{A}_{n,m}$ defines a weighing algorithm. The converse is also true. Given an optimal weighing algorithm that solves the all equal problem for m coins with up to k weights note, first, that we may assume that the algorithm always compares sets of coins of equal cardinalities. (This is the case because all weights may well be close enough to each other so that the result of any weighing of sets of nonequal cardinalities will be known in advance. We omit the detailed explanation.) We can now define a matrix $A = (a_{ij}) \in \mathcal{A}_{n,m}$ from the algorithm as follows. For each $1 \leq i \leq n$, let $L_i \subset [m]$ and $R_i \subset [m]$ be the two sets of coins the algorithm compares in step number i assuming all previous weighings are balanced. Define $a_{ij} = -1$ if $j \in L_i$, $a_{i,j} = 1$ if $j \in R_i$ and $a_{ij} = 0$ otherwise. Clearly $A \in \mathcal{A}_{n,m}$. The algorithm reports that all coins are of the same weight iff all weighings are balanced, and it is correct for coins with up to k distinct weights iff $ker(A) \cap W_{m,k}$ consists only of constant vectors.

3 Two simple observations

Let us first observe that even if there are no conditions on the weights of the coins at all, one simple algorithm for solving the all equal problem always exists. Namely, one can compare all the coins to a fixed coin, one by one. This will certainly decide whether all the m coins have the same weight or not in $m-1$ weighings. In the next proposition we observe that if there are no conditions on the weights this number of weighings cannot be improved.

Proposition 3.1 *The most efficient algorithm solving the all equal problem for m coins with arbitrary weights uses $m-1$ weighings.*

Proof. An algorithm using $m-1$ weighings is the obvious one described above. Simply pick a fixed coin and compare it to every other coin, each one in its turn. Clearly all the coins have the same weight iff all weighings are balanced.

To prove that one cannot do better, assume $n < m-1$ weighings suffice and let $A \in \mathcal{A}_{n,m}$ be the matrix corresponding to an optimal algorithm. Then, if all the weighings are balanced, any vector $w = (w_1, \ldots, w_m) \in ker(A)$ may be the vector of weights of the m given coins. However, the dimension of $ker(A)$ is at least $m - n > 1$, showing that it must contain a nonconstant vector, and completing the proof. □

Note that by the above proposition and its proof it follows that for the function $m(n,k)$ defined in the introduction, $m(n,k) = n+1$ for all $k > n+1$.

One may be interested in determining how many different weights the coins have. Formulated as a decision problem, this corresponds to the following question: Given m coins of arbitrary weights,

decide whether they have at least k distinct weights or not. Let $T(m,k)$ denote the minimum number of weighings required to answer this problem.

Proposition 3.2 *For every $m > k > 1$,*

$$max\{m-1, m\log_3(k-1)-k+1\} \leq T(m,k) \leq m\log_2(2k).$$

Proof: Björner and Lovász observed in [4] that the above problem can be solved using at most $m\log_2(2k)$ steps, where in each step we compare two coins to each other. On the other hand, they proved in the same paper, using a topological approach, that any algorithm that performs in each step an arbitrary linear test on the weights of the coins (that is, in each step the algorithm may check if a specified linear form in the weights is positive, negative or zero), and decides in the end if there are at least k distinct weights, must perform, in the worst case, at least $max\{m-1, m\log_3(k-1)-k+1\}$ tests. Note that the fact that the authors of [4] allow arbitrary linear tests and not only comparisons between two weights, which might seem a bit artificial in the original context, is essential here. Since every weighing is a special case of a linear test, the desired result follows. □

4 Threshold gates

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

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

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., [11] 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., [13] for a proof.

There are several simple constructions of threshold gates of n inputs that require some weights of size $2^{\Omega(n)}$. Håstad [10] 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 4.1 ([10], 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*

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

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

$$|w_j| \geq \frac{1}{2ne^{n^{4\beta}}2^n} n^{n/2},$$

where here and from now on $\beta = \log(3/2)$.
In addition, the above F can be realized by weights $w_1,\ldots,w_n,t$ with $t = 0$.

5 Coin-weighing

In this section we sketch the proof of 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, and it contains no proper nonempty subsequence whose sum is the zero vector.

Fact: For every n, $m(n, 2)$ 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. Here is a sketch. Given an admissible sequence as above, let $A = (a_{ij})$ be the n by m matrix whose columns are the vectors $v_1, \ldots, v_m$. Clearly $A \in \mathcal{A}_{n,m}$ and it is not too difficult to check that since the sequence is admissible, there is no solution w of the system $Aw = 0$ in which w is a nonconstant vector whose coordinates attain only two distinct values. Conversely, any correct weighing algorithm corresponds, by the discussion in Section 2, to a matrix in $\mathcal{A}_{n,m}$ with no nonconstant vectors in $ker(A) \cap W_{m,2}$ and it is easy to check that the columns of such a matrix form an admissible sequence.

In order to prove the upper bound in Theorem 1.1 we have to bound the maximum possible length of an admissible sequence of elements of V_n. A geometric argument based on Steinitz's Lemma, following the ideas in [1], can be given, but it only yields a weaker estimate. The best upper bound we can prove is that for $n > 1$

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

This is proved by considering the cone consisting of all integer nonnegative vectors of length 3^n that describe dependencies between the members of V_n. Using some standard results about Hilbert bases of polyhedral cones (see, e.g., [14]), it can be shown that any member of this cone is an integral nonnegative linear combination of certain members of the cone, each of which is a nonnegative linear combination of at most $(3^n - 1)/2$ integral vectors whose l_1-norms can be bounded by applying Cramer's rule and Hadamard's Inequality. The details are not complicated, but are somewhat lengthy, and will appear in the full version.

In order to prove the lower bound in 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. 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

$$\sum_{j=1}^{n+1} |s_j| \geq \sum_{j=1}^{n+1} z_j. \tag{1}$$

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 (1). We have thus proved the following.

Proposition 5.1 *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 $m(n) \geq M$.

Before procceeding with the proof of the asymptotic result note that the 3 by 4 matrix

$$B = \begin{bmatrix} -1 & 1 & 1 & -1 \\ 0 & -1 & 1 & -1 \\ 1 & 0 & -1 & -1 \end{bmatrix}$$

whose kernel is spanned by the vector $(4, 2, 3, 1)$ already shows that $m(3, 2) \geq 4+2+3+1 = 10$ (> 8). Similarly, by a computer search, we have found matrices providing explicit algorithms that show that, for example, $m(4, 2) \geq 30$, $m(10, 2) \geq 259606$ and $m(15, 2) \geq 2132870658$.

The main part of the proof of the lower bound in Theorem 1.1 is its proof when n is a power of 2, using Theorem 4.1. The result can then be deduced for all n by some additional tricks. The additional tricks require a detailed constructive description for the proof for powers of two and are thus omitted, due to space limitations. Here is the proof for powers of two.

Proposition 5.2 *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*

$$\sum_{j=1}^{n+1} |y_j| \geq \frac{1}{2e^{4n^\beta} 2^n} n^{n/2}.$$

Proof. Let

$$F(x_1, \ldots, x_n) : \{-1, 1\}^n \mapsto \{-1, 1\}$$

be a threshold gate satisfying the assertion of Theorem 4.1. Consider the following system of 2^n inequalities with the n variables $w_1, \ldots, w_n$

$$\sum_{j=1}^{n} \epsilon_j w_j \geq 1 \quad \text{if} \quad (\epsilon_1, \ldots, \epsilon_n) \in \{-1, 1\}^n, \quad F(\epsilon_1, \ldots, \epsilon_n) = 1,$$

$$\sum_{j=1}^{n} \epsilon_j w_j \leq -1 \quad \text{if} \quad (\epsilon_1, \ldots, \epsilon_n) \in \{-1, 1\}^n, \quad F(\epsilon_1, \ldots, \epsilon_n) = -1.$$

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. By a standard result from the theory of Linear Programming, which we omit, there is a solution in which n inequalities are tight, where the linear forms of these inequalities have full rank.

Let C denote the n by n matrix whose rows are n tight independent linear forms L_i as above and let δ be the corresponding vector of values of $L_i(w')$. Note that C is an n by n matrix of full rank with $\{-1, 1\}$ entries and δ 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 by $(n + 1)$ matrix obtained from C by adding to it the column δ. 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

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

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

By Theorem 4.1 this implies that the absolute value of each of the first n coordinates of y is at least

$$\frac{1}{2ne^{n^{4\beta}}2^n} n^{n/2},$$

completing the proof of the proposition, and implying, in view of Proposition 5.1, the assertion of Theorem 1.1 as well. □

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. We note also that the proof here can be converted into a constructive one by some additional work, thus yielding an explicit algorithm for the corresponding problem.

6 Three weights or more

In this section we sketch the proof of Theorem 1.2. Note, first that by the discussion in Section 2, $m(n,k)$ is simply the maximum integer m such that there exists an n by m matrix $A \in \mathcal{A}_{n,m}$ for which $ker(A) \cap W_{m,k}$ contains only constant vectors, where $W_{m,k}$ is the set of all vectors of length m with positive coordinates in which the number of distinct coordinates is at most k. The upper bound in Theorem 1.2 is rather simple, and is proved in the following lemma.

Lemma 6.1 *Suppose $k \geq 3$, put $m = m(n,k)$ and define $r = \lfloor (k-1)/2 \rfloor$. Then*

$$(r+1)^{m-1} \leq (2r(m-1)+1)^n. \tag{2}$$

Therefore,

$$m(n,k) \leq C \frac{n \log n}{\log k}$$

for some absolute constant C.

Proof. Given a matrix $A \in \mathcal{A}_{n,m}$ corresponding to an optimal algorithm, let $v_1, \ldots, v_m$ denote the columns of A. Define

$$S = \{\sum_{j=2}^{m} r_j v_j, \ r_j \in \mathbb{Z}, 0 \leq r_j \leq r\},$$

where $\mathbb{Z}$ denotes the set of all integers. Then $|S| = (r+1)^{m-1}$. We claim that no two vectors in S are equal. To see this, assume this is false and suppose

$$\sum_{j=2}^{m} r_j v_j = \sum_{j=2}^{m} t_j v_j,$$

where r_j, t_j are integers and there is at least one j for which r_j and t_j differ. Then the vector $y = (0, r_1 - t_1, r_2 - t_2, \ldots, r_m - t_m)$ lies in $ker(A)$ and is not a constant vector. Since the vector J consisting of m ones is also in $ker(A)$, so is $(r+1)J + y$, which is in $W_{m,k}$ as each of its coordinates is an integer between 1 and $2r+1 \leq k$. Therefore, A does not correspond to a valid algorithm, showing that indeed all members of S are distinct.

Since each coordinate of any vector in S is an integer whose absolute value cannot exceed $r(m-1)$ the inequality (2) follows, completing the proof. □

Remark. One can apply the second moment method (see, e.g., [2]) to improve the best estimate obtained for C by the above argument, but since we are not trying to optimize the constants here we omit the details.

The lower bound in Theorem 1.2 is proved by a probabilistic argument.

Lemma 6.2 *There exists an absolute positive constant c such that for every n and k satisfying $n+1 \geq k \geq 3$,*

$$m(n,k) \geq c \frac{n \log n}{\log k}.$$

Proof (brief sketch). Since $m(n,k) \geq n+1$ for every k the result is trivial for, say, $k \geq n^{1/3}$ (for all $c < 1/3$), and we thus may assume that $k \leq n^{1/3}$. Given a large n, let m be an even integer satisfying $m = (1+o(1))cn \log n / \log k$, where $c < 1/3$ is an absolute positive constant to be chosen later. Let $A \in \mathcal{A}_{n,m}$ be a random matrix obtained by choosing each row or A, randomly and independently, among all row-vectors of length m containing precisely $m/2$ -1-coordinates and $m/2$ 1-coordinates. To complete the proof it suffices to show that almost surely (that is, with probability that tends to 1 and n tends to infinity) the weighing algorithm corresponding to A solves the all equal problem for coins with up to k distinct weights. To do so, we must show that there is no nonconstant vector in $W_{m,k}$ that lies in $ker(A)$. Note that there are infinitely many vectors in $W_{m,k}$ and hence the proof requires some ideas besides standard probabilistic arguments. This, however, can be done by considering certain minimal possible linear relations and by combining them with appropriate estimates for hypergeometric distributions. The details are rather complicated and will appear in the final version. □

7 Concluding remarks

Our techniques here enable us to improve the known results for several additional seemingly unrelated questions. Three examples are the following.

- 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. The problem of determining or estimating the value of $D(n)$, which is motivated by questions in game theory, received a considerable amount of attention (see [8] and its references). Huckeman, Jurkat and Shapley proved that

  $$D(n) \leq (n+1)^{(n+1)/2},$$

  for every n, Shapley showed that $D(n) \geq \frac{2^{n-1}}{n-1}$ for all $n > 2$, and van Lint and Pollak improved this lower bound and showed that $D(n) \geq 2^{n-3} + 1$ for all $n > 2$. Our techniques here enable us to improve the lower bound and show that it is not far from the above mentioned upper bound, that is, that the asymptotic behaviour of $D(n)$ is given by $D(n) = n^{(\frac{1}{2}+o(1))n}$.

- Answering a question of Graham and Sloane [7], which was motivated by questions in Numerical Algebra, we can show that the maximum possible entry in an inverse of an n by n invertible matrix with $\{-1,1\}$ entries is $n^{(\frac{1}{2}+o(1))n}$. A similar estimate holds for $\{0,1\}$-matrices.

- As described in Section 4, Håstad proved that for every n which is a power of 2 there is a threshold gate $F(x_1,\ldots,x_n)$ such that in any realization of it with integral weights, some

weights are of absolute value at least $n^{(\frac{1}{2}+o(1))n}$. He further mentioned that it is not clear how to get a similar estimate for all values of n (although, as he remarked, this is not extremely intriguing, as his result clearly implies that for every n some threshold gates of n inputs require weights of size at least $n^{(\frac{1}{4}+o(1))n}$.) Combining his technique with some of our ideas here we can show that in fact for every n, some threshold gates of n inputs require weights of size $n^{(\frac{1}{2}+o(1))n}$.

The results in Section 5 apply to a slightly more general case which we may call *generic weights*. A set of weights $w_1, \ldots, w_t$ is called *generic* if any vector of integers $(\lambda_1, \ldots, \lambda_t)$ that satisfies $\sum_{i=1}^{t} \lambda_i = 0$ and $\sum_{i=1}^{t} \lambda_i w_i = 0$ is the zero vector. Note that any set of two numbers 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 can be shown that the results described in Section 5 apply to this case (without any essential change in the proofs) and show (constructively) that $m'(n) = n^{(\frac{1}{2}+o(1))n}$. Another variant of the all equal problem for two weights is the following. 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 $m(n) \geq M(n)$. We can extend our method here and show that the asymptotic behaviour of $M(n)$ also satisfies $M(n) = n^{(\frac{1}{2}+o(1))n}$.

The proof of the lower bound in Theorem 1.2 described in Section 6 is not constructive. It would be interesting to find a constructive proof yielding an explicit algorithm for the corresponding problem. We can describe a constructive algorithm for the case of three (unknown) weights, known to form an arithmetic progression. Even this seemingly simple case, where n weighings suffice to solve the problem for $\Theta(n \log n)$ coins, requires some nontrivial construction whose detailed description is omitted.

References

[1] N. Alon and K. Berman, *Regular hypergraphs, Gordon's lemma, Steinitz's lemma and Invariant Theory*, J. Combinatorial Theory, Ser. A 43(1986), 91–97.

[2] N. Alon and J. H. Spencer, *The Probabilistic Method*, Wiley, New York, 1992.

[3] A. Björner, L. Lovász and A. C.-C. Yao, *Linear decision trees: volume estimates and topological bounds,* Proc. 24^{th} ACM STOC, ACM Press, New York, 1992, 170–177.

[4] A. Björner and L. Lovász, *Linear decision trees, subspace arrangements and Möbius functions*, J. AMS 7 (1994), 677–706.

[5] P.D. Chen, X.D. Hu and F.K. Hwang, *A new competitive algorithm for the counterfeit coin problem,* Information Processing Letters 51 (1994), 213–218.

[6] D. Dobkin and R. Lipton, *On the complexity of computation under varying sets of primitives*, in: *Automata Theory and Formal Languages* (H. Bradhage, ed.), Lecture Notes in Computer Science 33, Springer Verlag 1975, 110-117.

[7] R. L. Graham and N. J. A. Sloane, *Anti-Hadamard matrices*, Linear Algebra and its Applications 62 (1984), 113-137.

[8] J. E. Graver, *A survey of the maximum depth problem for indecomposable exact covers*, in: *"Infinite and Finite Sets"*, Colloq. Math. Soc. Soc. János Bolyai 10, North Holland, Amsterdam (1973), pp. 731-743.

[9] R. K. Guy and R. J. Nowakowski, *Coin-weighing problems*, Amer. Math. Monthly 102 (1995), 164–167.

[10] J. Håstad, *On the size of weights for threshold gates,* SIAM J. Discrete Math. 7 (1994), 484–492.

[11] J. Hertz, R. Krogh and A. Palmer, *An Introduction to the Theory of Neural Computation*, Addison-Wesley, Reading, MA 1991.

[12] X.D. Hu and F.K. Hwang, *A competitive algorithm for the counterfeit coin problem*, to appear.

[13] S. Muroga, *Threshold Logic and its Applications*, Wiley-Interscience, New York, 1971.

[14] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, 1986.