Hypercube problems

Lecture 21

December 19, 2019

Lecturer: Petr Gregor Scribe by: Tung Anh Vu Updated: February 17, 2020

1 Coin weighing

We are given n coins, some of them are genuine and the rest are counterfeit. We know genuine coins have weight a and counterfeit coins have different weight b. We have a spring scale at our disposal, which we can use to determine the total weight of any subset of coins. The question is how many weighings are needed to identify all counterfeit coins?

To formalize the problem denote $X \subseteq [n]$ the set of counterfeit coins. Each weighing can be viewed as selecting a subset $Y \subseteq [n]$ and determining $|Y \cap X|$. Then the results of k weighings is a sequence $(|X \cap Y_1|, \ldots, |X \cap Y_k|)$. Let $f(n)$ be the minimal number k of sets $Y_1, \ldots, Y_k \subseteq [n]$ such that the sequence $|X \cap Y_i|$ for $i = 1, \ldots, k$ determines X for any subset of counterfeit coins $X \subseteq [n]$. We emphasize that sets $Y_1, \ldots, Y_k$ are fixed for all possible inputs.

Example 1 *Given four coins any subset of counterfeit coins can be distinguished using three subsets* $Y_1 = \{1,2,3\}, Y_2 = \{1,3,4\}, Y_3 = \{1,2,4\}$. *As an example* $|X \cap Y_1| = |X \cap Y_2| = |X \cap Y_3| = 1 \implies X = \{1\}$ *or* $|X \cap Y_1| = |X \cap Y_3| = 2 \wedge |X \cap Y_2| = 1 \implies X = \{1,2\}$.

We can also view the coin weighing problem in the language of matrices. Note that arithmetics in the following definition are done over real numbers.

Definition 2 *A binary* $k \times n$ *matrix* M *is a* detecting matrix *if* $Mu \neq Mv$ *for every distinct* $u, v \in \mathbb{Z}_2^n$.

Rows of the detecting matrix correspond to characteristic vectors Y_i and determining $|Y_i \cap X|$ is achieved by the multiplication $M_{i:} \cdot x$ where x is the characteristic vector of X. Then we can define $f(n)$ as the minimum number of rows of a detecting matrix.

This concept has numerous application, such as in detection problems, distinguishing family problems, network discovery and verification, robot navigation and many more.

1.1 A simple lower bound

Let M be a $k \times n$ detecting matrix with minimum k. For any vector $u \in \mathbb{Z}_2^n$ it holds that $(Mu)_i \in \{0, 1, \ldots, n\}$ for every $i \in [k]$. Since we need to distinguish 2^n distinct vectors, we have $(n+1)^k \geq 2^n$ and therefore

$$f(n) \geq \frac{n}{\log_2(n+1)}. \qquad (1)$$

So far we have always announced the sequence Y_i in advance, what if we can adapt Y_i depending on the result of previous weighings $|X \cap Y_1|, \ldots, |X \cap Y_{i-1}|$? Surprisingly the same lower bound holds. For $X \subseteq [n]$ let $r(X) = (a_1, \ldots, a_r)$, where $a_i \in \{0, 1, \ldots, n\}$, be the sequence of weighing results in an optimal adaptive scheme with k steps, where $r \in \{1, \ldots, k\}$ is the step when X was determined. Thus $\{r(X) \mid X \subseteq [n]\}$ must be a prefix-free code and by Kraft–McMillan inequality we have $2^n \leq (n+1)^k$ which implies the same lower bound.

2 Metric dimension

In the following section, the set $[n]$ in context of hypercubes means the vertex $11 \ldots 1$.

Definition 3 *A subset S of vertices* resolves *a graph G if every vertex is uniquely determined by its vector of distances to vertices of S. The* metric dimension *of G is the minimum cardinality $m(G)$ of a resolving set of G.*

Example 4

- *An example of a resolving set for Q_5 is $S = \{00000, 00011, 00101, 01001\}$.*
- *The metric dimension of a graph G on n vertices is $n-1$ if and only if G is a clique on n vertices.*
- *The metric dimension of a graph G is 1 if and only if G is a path.*
- *The metric dimensions of some hypercubes of small dimensions are known, see Table 1.*

n	2	3	4	5	6	7	8	10	15
$m(Q_n)$	2	3	4	4	5	6	6	≤ 7	≤ 10

Table 1: Some known metric dimensions of hypercubes.

How are coin weighing problems and metric dimension of hypercubes related?

Proposition 5 *$|m(Q_n) - f(n)| \leq 1$ for every $n \geq 1$. Furthermore $f(n) \leq m(Q_n) \leq f(n) + 1$ since w.l.o.g. $[n]$ is in a resolving set.*

Proof Let X, X' be two distinct subsets of counterfeit coins. If $|X| \neq |X'|$, then we can detect/resolve them using the set $[n]$. Assume $|X| = |X'|$, observe that $|X| + |Y_i| = |X \triangle Y_i| + 2|X \cap Y_i|$ implies $|X \triangle Y_i| = |X' \triangle Y_i| \iff |X \cap Y_i| = |X' \cap Y_i|$. Combining these two observations we can conclude that if $\{Y_1, \ldots, Y_k\}$ is resolving, then $\{Y_1, \ldots, Y_k\} \cup \{[n]\}$ is detecting, and if $\{Y_1, \ldots, Y_k\}$ is detecting, then $\{Y_1, \ldots, Y_k\} \cup \{[n]\}$ is resolving. ■

In terms of metric dimension, the previous lower bound (1) can be significantly improved as follows.

Theorem 6

$$m(Q_n) \geq \frac{2n}{\log_2(n) + O(1)} \quad \textit{for any } n \geq 1.$$

Proof Let $u \in \mathbb{Z}_2^n$ be a vertex of Q_n, k be the minimum size of a resolving set $S = \{s_1, \ldots, s_k\}$ of Q_n. If we view u as a uniformly distributed random variable from the set of vertices to the set of binary vectors of length n, then the entropy of u is $H(u) = n$. Let $X_i = d_H(u, s_i)$ be the Hamming distance between u and s_i. The entropy of X_i is $H(X_i) = \frac{1}{2}\log(n) + O(1)$ as $X_i \sim B(n, \frac{1}{2})$. Let $X = (X_1, \ldots, X_k)$. Since S resolves u, the mutual information between u and X is $I(u : X) = H(u)$. Intuitively, once we know X we can determine u and there is no "surprise". On the other hand,

$$I(u : X) \leq H(X) \leq \sum_{i=1}^{k} H(X_i)$$

holds. Therefore $n \leq k(\frac{1}{2}\log_2(n) + O(1))$, which implies

$$k \geq \frac{2n}{\log_2(n) + O(1)}.$$

■

2.1 Explicit construction

We will inductively construct a detecting binary $(2^m - 1) \times 2^{m-1}$ matrix for any $m \geq 1$. We strengthen the notion of detecting matrices and require that they also distinguish vectors of length n whose first k coordinates are integers and the rest are binary.

Definition 7 *A matrix $A \in \mathbb{Z}^{k \times n}$ where $k \leq n$ is* strongly detecting *if $Ax \neq Ay$ for any distinct $x, y \in \mathbb{Z}^k \times \mathbb{Z}_2^{n-k}$.*

Let $f'(n)$ be the minimum number of rows of a binary strongly detecting matrix with n columns. Observe that $f(n) \leq f'(n) \leq n$, where the second inequality follows from the fact that the identity matrix is strongly detecting.

First we construct a strongly detecting $\{-1, 0, 1\}$-matrix, which we will later use to construct a strongly detecting binary matrix.

Lemma 8 *For every $m \geq 0$ there exists a strongly detecting matrix $B_m \in \{-1, 0, 1\}^{k \times n}$ where $k = 2^m, n = 2^{m-1}(m+2)$ such that its last row is binary.*

Proof It is simple to verify that $B_0 = (1)$ satisfies all requirements. For the inductive step consider the matrix

$$B'_{m+1} = \begin{pmatrix} B_m & -B_m & I \\ B_m & B_m & 0 \end{pmatrix}.$$

Clearly B'_{m+1} is a $2^{m+1} \times 2^m(m+3)$ matrix with $\{-1, 0, 1\}$ entries and the bottom row is binary. Let $x, y \in \mathbb{Z}^k \times \mathbb{Z}_2^{n-k}, z \in \mathbb{Z}_2^k$ and

$$B'_{m+1} \begin{pmatrix} x, & y, & z \end{pmatrix}^T = \begin{pmatrix} \lambda'_1, & \cdots, & \lambda'_k, & \lambda''_1, & \cdots, & \lambda''_k \end{pmatrix}^T.$$

Let $(b_{ij}) = B'_{m+1}$. For $i = 1, \ldots, k$ we have

$$\begin{aligned} \lambda'_i &= \sum_{j=1}^{n} b_{ij} x_j - \sum_{j=1}^{n} b_{ij} y_j + z_i \\ \lambda''_i &= \sum_{j=1}^{n} b_{ij} x_j + \sum_{j=1}^{n} b_{ij} y_j \end{aligned},$$

so $\lambda'_i + \lambda''_i \equiv z_i \pmod 2$, which means that λ'_i and λ''_i uniquely determine z_i. Since B_m is strongly detecting and $\lambda'_i + \lambda''_i = 2\sum_{j=1}^{n} b_{ij} x_j + z_i$ for every $i = 1, \ldots, k$, it follows that λ'_i and λ''_i determine x_j uniquely. In a similar fashion since $\lambda''_i - \lambda'_i = 2\sum_{j=1}^{n} b_{ij} y_j - z_i$ for every $i = 1, \ldots, k$ it follows that λ'_i and λ''_i also uniquely determine y_j. To obtain the strongly detecting matrix B_{m+1} we only need to permute columns of B'_{m+1} so that columns $n + 1, \ldots, n + k$ of B'_{m+1} appear as columns $k + 1, \ldots, 2k$ in B_{m+1}. The resulting matrix B_{m+1} is in form

$$B_{m+1} = \begin{pmatrix} b_{:1} & \cdots & b_{:k} & b_{:n+1} & \cdots & b_{:n+k} & b_{:k+1} & \cdots & b_{:n} & b_{:n+k+1} & \cdots & b_{:2n+k} \end{pmatrix}.$$

■

Theorem 9 *For any $m \geq 1$ there is a binary strongly detecting $k \times n$ matrix A_m where $k = 2^m - 1$ and $n = 2^{m-1}m$. Consequently,*

$$f'(2^{m-1}m) \leq 2^m - 1. \qquad (2)$$

Proof Again verify that $A_1 = (1)$ meets the requirements. Let A be the $(k+1) \times n$ matrix obtained from A_m by appending a bottom row of zeros, $r = 2^m$ and $s = 2^{m-1}(m + 2)$. The matrix B_m from Lemma 8 can be written as $B_m = V - W$ where $V = (v_{ij})$ and $W = (w_{ij})$ are $r \times s$ binary matrices. Consider the $2r \times (n + s)$ matrix

$$A'_{m+1} = \begin{pmatrix} A & V \\ A & W \end{pmatrix}.$$

Let $x \in \mathbb{Z}^k \times \mathbb{Z}_2^{n-k}, y \in \mathbb{Z}^r \times \mathbb{Z}_2^{s-r}$ and

$$A'_{m+1} \cdot \begin{pmatrix} x, & y \end{pmatrix}^T = \begin{pmatrix} \lambda'_1, & \cdots, & \lambda'_n, & \lambda''_1, & \cdots, & \lambda''_r \end{pmatrix}^T.$$

Let $(a_{ij}) = A'_{m+1}$. For all $i = 1, \ldots, r$ we have

$$\begin{aligned} \lambda'_i &= \sum_{j=1}^{n} a_{ij} x_j + \sum_{j=1}^{s} v_{ij} y_j, \\ \lambda''_i &= \sum_{j=1}^{n} a_{ij} x_j + \sum_{j=1}^{s} w_{ij} y_j. \end{aligned}$$

Since B_m is strongly detecting, the differences $\lambda'_i - \lambda''_i$ determine y_j uniquely for each $j = 1, \ldots, s$. By induction hypothesis, λ'_i and λ''_i's determine both x_j and y_j's. Moreover, since the last row of A'_{m+1} consists of all 0's, it can be removed. By a similar permutation as in the proof of Lemma 8 we obtain the desired binary strongly detecting matrix A_{m+1}. ■

It is known that equality holds in (2) in Theorem 9. Using the inequality $f'(n+m) \leq f'(n) + f'(m)$ for any $n, m \geq 0$ (proof omitted) we obtain the following corollary.

Corollary 10

$$f(n) \leq f'(n) \leq \frac{2n}{\log n} + O\left(\frac{n \log \log n}{\log^2 n}\right).$$

Combining the above lower and upper bounds we obtain the following corollary.

Corollary 11

$$m(Q_n) = (2 + o(1)) \frac{n}{\log n}.$$

This result can be generalized for *Hamming graphs*, i.e. K_q^n for any $q \geq 2$. An example of an application is the Mastermind game with only "black pegs". In such setting each guess corresponds to a vector $y \in \mathbb{Z}_q^n$ and the answer is the number of matches of a secret vector $x \in \mathbb{Z}_q^n$.

Remark 12 *It is known that*

- $m(K_q^n) = (2 + o(1)) \frac{n}{\log_q n}$ *for all* $q \geq 2$ *[5],*
- $m(K_q^2) = \lfloor \frac{2}{3}(2q - 1) \rfloor$ *for all* $q \geq 1$ *[2].*

There are many results on metric dimension of other graphs and adaptive algorithms for variants of coin weighing. In particular, there is a deterministic polynomial algorithm to detect m counterfeit coins, which are heavier than genuine coins, among n coins using $O(\frac{m \log n}{\log m} + m \log \log m)$ weighings.

Notes

The lower bound in Theorem 6 based on entropy is from [8]. Originally, it was proven without tools from information theory [4], and can be also proven by the second moment method [7]. The upper bound construction in Theorem 9 is from [3], an alternative construction is known by the Möbius function [6], or by Fourier transform [1].

References

[1] N. H. Bhouty, *Optimal algorithms for the coin weighing problem with a spring scale*, In Proc. of the 22nd Annual Conference on Learning Theory, Montreal, 2009.

[2] J. Cáceres, C. Hernando, M. Mora, I. M. Pelyao, M. L. Puertas, C. Seara, and D. R. Wood, *On the metric dimension of Cartesian products of graphs*, SIAM J. Discrete Math., 21:423–441, 2007.

[3] D. G. Cantor and W. H. Mills, *Determination of a subset from certain combinatorial properties*, Canad. J. Math., 18:42–48, 1966.

[4] P. Erdös, A. Rényi, *On two problems of information theory*, Magyar Tud. Akad. Mat. Kutató Int. Közl., 8:229–243, 1963.

[5] Z. Jiang, N. Polyanskii, *On the metric dimension of Cartesian powers of a graph*, arXiv:1712.02723, 2019.

[6] B. Lindström, *On Möbius functions and a problem in combinatorial number theory*, Canad. Math. Bull., 14:513–516, 1971.

[7] L. Moser, *The second moment method in combinatorial analysis*, In: Combinatorial Structures and their Applications, Gordon and Breach, 283–384, 1970.

[8] N. Pippenger, *An information-theoretic method in combinatorial theory*, J. Combin. Theory Ser. A, 23:99–104, 1977.