Discreet Coin Weighings and the Frobenius Problem

Rafael M. Saavedra

Mentor: Dr. Tanya Khovanova

Sixth Annual PRIMES Conference
May 21, 2016

Classical Coin Weighing Problems

The Classical Situation:

- A pile of identical-looking coins. Some may be fake.
- All real coins weigh the same. Any fake coins weigh the same, but less.
- A balance scale that can weigh equal numbers of coins.

Classical Coin Weighing Problems

The Classical Situation:

- A pile of identical-looking coins. Some may be fake.
- All real coins weigh the same. Any fake coins weigh the same, but less.
- A balance scale that can weigh equal numbers of coins.

Generalizations:

- You have n coins, and k are fake. What is the least number of weighings needed to find them?

Classical Coin Weighing Problems

The Classical Situation:

- A pile of identical-looking coins. Some may be fake.
- All real coins weigh the same. Any fake coins weigh the same, but less.
- A balance scale that can weigh equal numbers of coins.

Generalizations:

- You have n coins, and k are fake. What is the least number of weighings needed to find them?
- Several scales/pans that can be used in parallel.

A Discreet Coin Weighing Problem

A Discreet Coin Weighing Problem

- You are a lawyer who has 16 coins and need to prove to a judge that 9 of them are fake by using a balance scale.
- The judge already knows that there are either 9 or 4 fake coins.
- You cannot reveal whether any *individual* coin is real or fake.

A Discreet Coin Weighing Problem

A Discreet Coin Weighing Problem

- You are a lawyer who has 16 coins and need to prove to a judge that 9 of them are fake by using a balance scale.
- The judge already knows that there are either 9 or 4 fake coins.
- You cannot reveal whether any *individual* coin is real or fake.

Solution

Divide the coins into four piles of equal size, A, B, C, D:

$$A > B > C = D$$

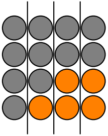
A Discreet Coin Weighing Problem

A Discreet Coin Weighing Problem

- You are a lawyer who has 16 coins and need to prove to a judge that 9 of them are fake by using a balance scale.
- The judge already knows that there are either 9 or 4 fake coins.
- You cannot reveal whether any *individual* coin is real or fake.

Solution

Divide the coins into four piles of equal size, A, B, C, D:



$$A > B > C = D$$

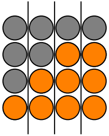
A Discreet Coin Weighing Problem

A Discreet Coin Weighing Problem

- You are a lawyer who has 16 coins and need to prove to a judge that 9 of them are fake by using a balance scale.
- The judge already knows that there are either 9 or 4 fake coins.
- You cannot reveal whether any *individual* coin is real or fake.

Solution

Divide the coins into four piles of equal size, A, B, C, D:



$$A > B > C = D$$

Discreet Coin Weighings

Definition

A series of coin weighings can **discreetly** prove that the number of fake coins is f if the coin configurations with f fake coins that satisfy the weighings do not all agree on whether any specific coin is real or fake.

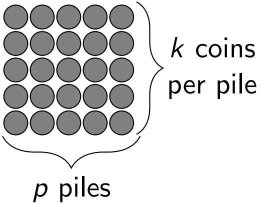
Discreet Coin Weighings

Definition

A series of coin weighings can **discreetly** prove that the number of fake coins is f if the coin configurations with f fake coins that satisfy the weighings do not all agree on whether any specific coin is real or fake.

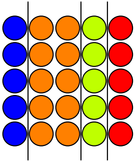
- In 2015 as a PRIMES USA project, Diaco and Khovanova studied discreet weighings for different total numbers of coins and values of f.

The Sorting Strategy



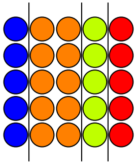
The Sorting Strategy

- Compare and sort all the piles by weight.



The Sorting Strategy

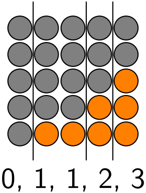
- Compare and sort all the piles by weight.
- The pile relations are described by a *sorting sequence*.



0, 1, 1, 2, 3

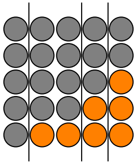
The Sorting Strategy

- Compare and sort all the piles by weight.
- The pile relations are described by a *sorting sequence*.
- The sorting sequence gives the minimum number of fake coins.



The Sorting Strategy

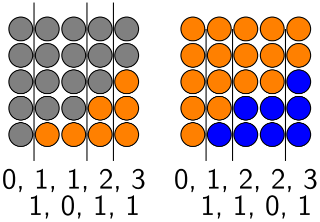
- Compare and sort all the piles by weight.
- The pile relations are described by a *sorting sequence*.
- The sorting sequence gives the minimum number of fake coins.



0, 1, 1, 2, 3
1, 0, 1, 1

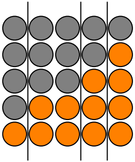
The Sorting Strategy

- Compare and sort all the piles by weight.
- The pile relations are described by a *sorting sequence*.
- The sorting sequence gives the minimum number of fake coins.
- The reverse sequence describes the reverse relations, and gives the maximum number of fake coins.



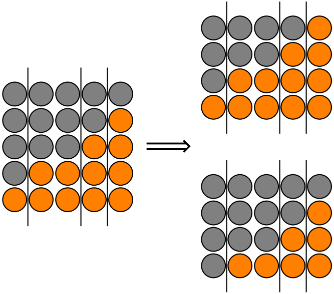
Discreetness in the Sorting Strategy

- To be discreet, there must be a configuration with a fake coin in every pile, and one with a real coin in every pile.



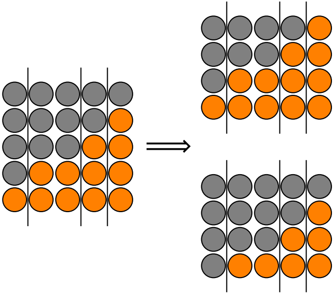
Discreetness in the Sorting Strategy

- To be discreet, there must be a configuration with a fake coin in every pile, and one with a real coin in every pile.



Discreetness in the Sorting Strategy

- To be discreet, there must be a configuration with a fake coin in every pile, and one with a real coin in every pile.



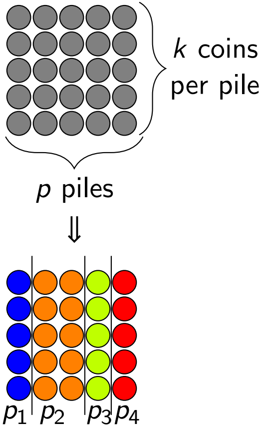
Theorem

The sorting strategy corresponding to a sorting sequence discreetly proves that the number of fake coins is f, with pk total coins, if and only if it can show that the number of fake coins is f and $f - p$ with $p(k-1)$ total coins.

How Many Coins Are Possible?

- Partition the piles into r different classes based on weight. The ith class has size p_i.

$$p_1 + \cdots + p_r = p.$$



How Many Coins Are Possible?

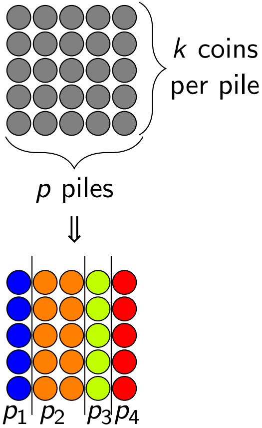
- Partition the piles into r different classes based on weight. The ith class has size p_i.

$$p_1 + \cdots + p_r = p.$$

- If we have f_i fake coins in pile i, then the number of fake coins is

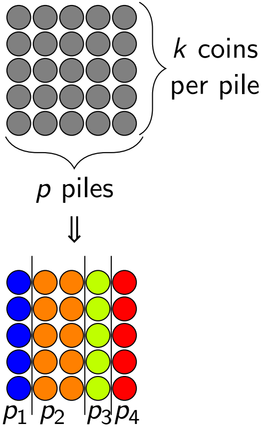
$$p_1 f_1 + \cdots + p_r f_r = f$$

with $0 \leq f_i < f_{i+1} \leq k$.



How Many Coins Are Possible?

- Partition the piles into r different classes based on weight. The ith class has size p_i.
$$p_1 + \cdots + p_r = p.$$
- If we have f_i fake coins in pile i, then the number of fake coins is
$$p_1 f_1 + \cdots + p_r f_r = f$$
with $0 \le f_i < f_{i+1} \le k$.
- Using a substitution $x_i = f_i - f_{i-1} - 1$ this can be reduced to
$$\sum_{i=1}^{r} \left(\sum_{m=i}^{r} p_m \right) x_i = f - \sum_{i=2}^{r} \sum_{m=i}^{r} p_m$$
with $x_1, \ldots, x_r \ge 0$ and the requirement that the piles do not overflow.



The Frobenius Problem

The Frobenius Problem

Given positive integers $a_1, \dots, a_r, n$, what are the nonnegative integer solutions of the following equation?

$$a_1 x_1 + \cdots + a_r x_r = n$$

$$\sum_{i=1}^{r} \left(\sum_{m=i}^{r} p_m \right) x_i = f - \sum_{i=2}^{r} \sum_{m=i}^{r} p_m \qquad \text{(Nondecreasing condition)}$$

$$a_i = \sum_{m=i}^{r} p_m \qquad n = f - \sum_{i=2}^{r} \sum_{m=i}^{r} p_m$$

The Frobenius Problem

Theorem (Existence of the Frobenius Number)

If $a_1, \ldots, a_r$ are relatively prime, then for all sufficiently large n,

$$a_1 x_1 + \cdots + a_r x_r = n$$

has a solution in nonnegative $x_1, \ldots, x_r$.

$$\sum_{i=1}^{r} \left(\sum_{m=i}^{r} p_m \right) x_i = f - \sum_{i=2}^{r} \sum_{m=i}^{r} p_m \qquad \text{(Nondecreasing condition)}$$

Ranges Within the Possible Values

Example (Sorting strategy with 5 coins per pile)

Sorting sequence	Possible number of fake coins
$0, 0, 0, 0, 1$	$\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}, \mathbf{7}, \mathbf{8}, \mathbf{9}, 11, 12, 13, 16, 17, 21$
$0, 0, 0, 1, 1$	$2, 4, 6, \mathbf{7}, \mathbf{8}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{13}, \mathbf{14}, 16, 17, 19, 22$
$0, 0, 0, 1, 2$	$\mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}, \mathbf{7}, \mathbf{8}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{13}, \mathbf{14}, \mathbf{15}, 18$
$0, 0, 1, 1, 1$	$3, 6, 8, 9, \mathbf{11{,}12{,}13{,}14{,}15{,}16{,}17{,}18{,}19}, 21, 23$

Ranges Within the Possible Values

Example (Sorting strategy with 5 coins per pile)

Sorting sequence	Possible number of fake coins
0, 0, 0, 0, 1	**1**, **2**, **3**, **4**, **5**, **6**, **7**, **8**, **9**, 11, 12, 13, 16, 17, 21
0, 0, 0, 1, 1	2, 4, 6, **7**, **8**, **9**, **10**, **11**, **12**, **13**, **14**, 16, 17, 19, 22
0, 0, 0, 1, 2	**3**, **4**, **5**, **6**, **7**, **8**, **9**, **10**, **11**, **12**, **13**, **14**, **15**, 18
0, 0, 1, 1, 1	3, 6, 8, 9, **11,12,13,14,15,16,17,18,19**, 21, 23

The Two Conditions

1. The nondecreasing condition for the sorting sequence.
2. The number of fake coins must not be greater than k in any pile.

Ranges Within the Possible Values

Example (Sorting strategy with 5 coins per pile)

Sorting sequence	Possible number of fake coins
0, 0, 0, 0, 1	**1**, **2**, **3**, **4**, **5**, **6**, **7**, **8**, **9**, 11, 12, 13, 16, 17, 21
0, 0, 0, 1, 1	2, 4, 6, **7**, **8**, **9**, **10**, **11**, **12**, **13**, **14**, 16, 17, 19, 22
0, 0, 0, 1, 2	**3**, **4**, **5**, **6**, **7**, **8**, **9**, **10**, **11**, **12**, **13**, **14**, **15**, 18
0, 0, 1, 1, 1	3, 6, 8, 9, **11,12,13,14,15,16,17,18,19**, 21, 23

The Two Conditions

1. The nondecreasing condition for the sorting sequence.
2. The solution to the nondecreasing condition must be consistent with the nondecreasing condition for the reverse sorting sequence.

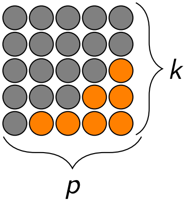
Results

Conjecture

When $k \geq p$,

1. *if there exists a solution to the nondecreasing condition of the sorting sequence for f and*
2. *if there exists a solution to the nondecreasing condition of the reverse sorting sequence for $pk - f$,*

then there exists a solution consistent with both equations.



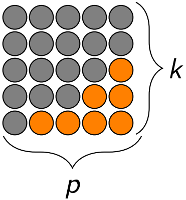
Results

Conjecture

When $k \geq p$,

1. *if there exists a solution to the nondecreasing condition of the sorting sequence for f and*
2. *if there exists a solution to the nondecreasing condition of the reverse sorting sequence for $pk - f$,*

then there exists a solution consistent with both equations.



Theorem

Consider a sorting sequence such that $p_1, \ldots, p_r$ are relatively prime. Let g and g' be the Frobenius numbers for the nondecreasing conditions of the sorting sequence and the reverse sequence respectively. Assuming the conjecture, the sorting strategy can prove that the number of fake coins can be any number from g to $pk - g'$.

Future Work

- Prove the conjecture.
- Generalize the sorting strategy: two different sizes of piles.
- Tailor-made strategies that prove only certain values we want.
- Minimum number of weighings needed to prove something discreetly.
- Generalizing the concept of discreetness.

Acknowledgements

- Dr. Tanya Khovanova
- The MIT PRIMES Program
- Nicholas Diaco
- My parents Rafael H. Saavedra and Claudia Mazzotti

References

J. L. Ramírez Alfonsín
The Diophantine Frobenius Problem.
Oxford University Press, 2005.

N. Diaco and T. Khovanova
Weighing Coins and Keeping Secrets
arXiv:1508.05052, 2015.