A New Coin Weighing Problem and Concealing Information

NICK DIACO

FIFTH ANNUAL MIT-PRIMES CONFERENCE

MENTOR: DR. TANYA KHOVANOVA

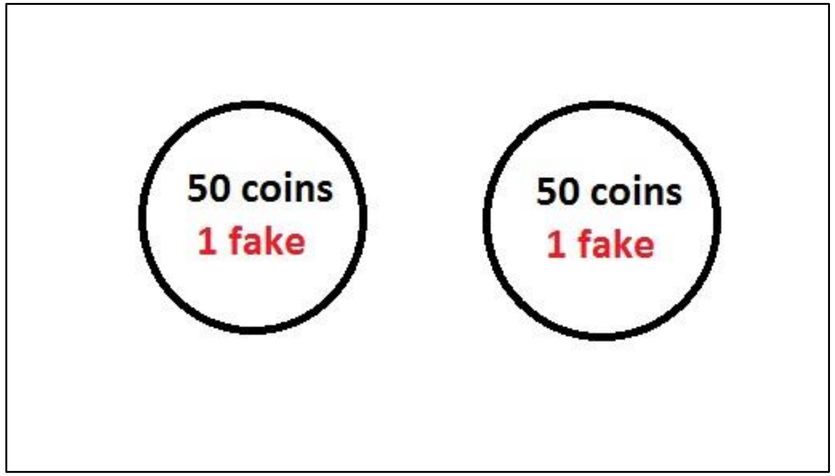
MAY 16, 2015

Getting Our Feet Wet

A simple example: 100 total coins, and the judge knows that there are either 1 or 2 fake coins. We want to show the latter.

Getting Our Feet Wet

A simple example: 100 total coins, and the judge knows that there are either 1 or 2 fake coins. We want to show the latter.



The Original Problem

A judge is presented with 100 coins that look identical, knowing that there are either two or three counterfeits among them. All the real coins have the same weight, and similarly, all the fake coins have the same weight - but are lighter than the real ones.

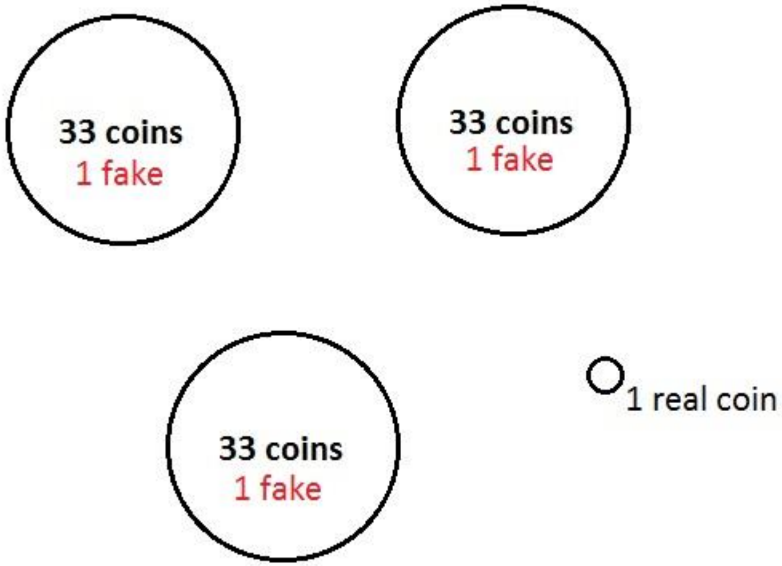
You yourself know that there are exactly three fake coins and you know which ones they are. Can you use a balance scale to convince the judge that there are exactly three fake coins without revealing information about any particular coin?

The Original Problem

The real deal: 100 total coins, 3 fake coins, and showing that there can’t be 2 fake coins.

The Original Problem

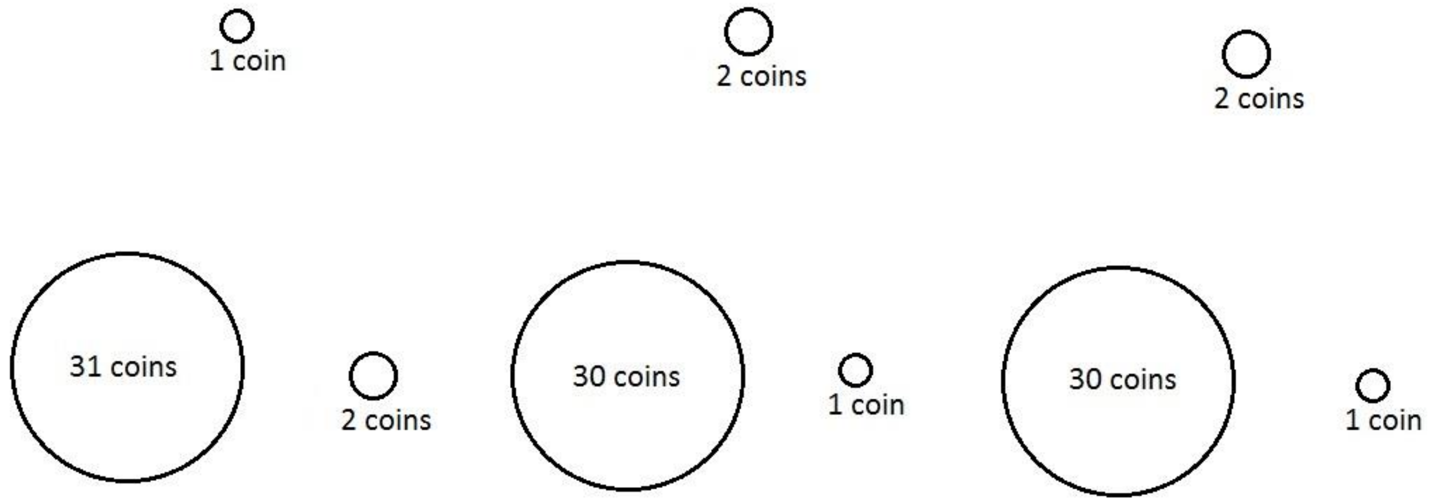
The real deal: 100 total coins, 3 fake coins, and showing that there can't be 2 fake coins.



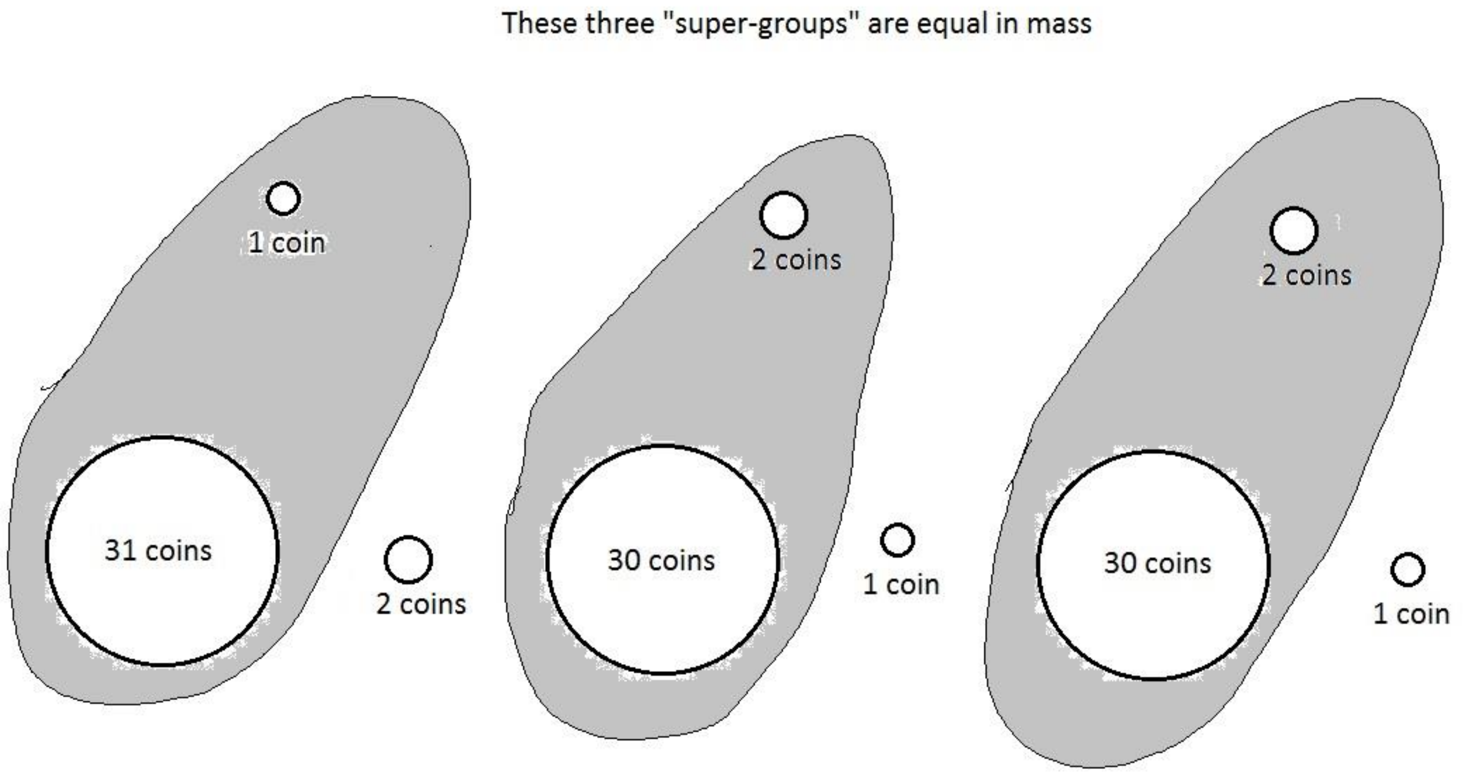
The Original Problem

Second Attempt: 100 total coins, 3 fake coins.

The Original Problem

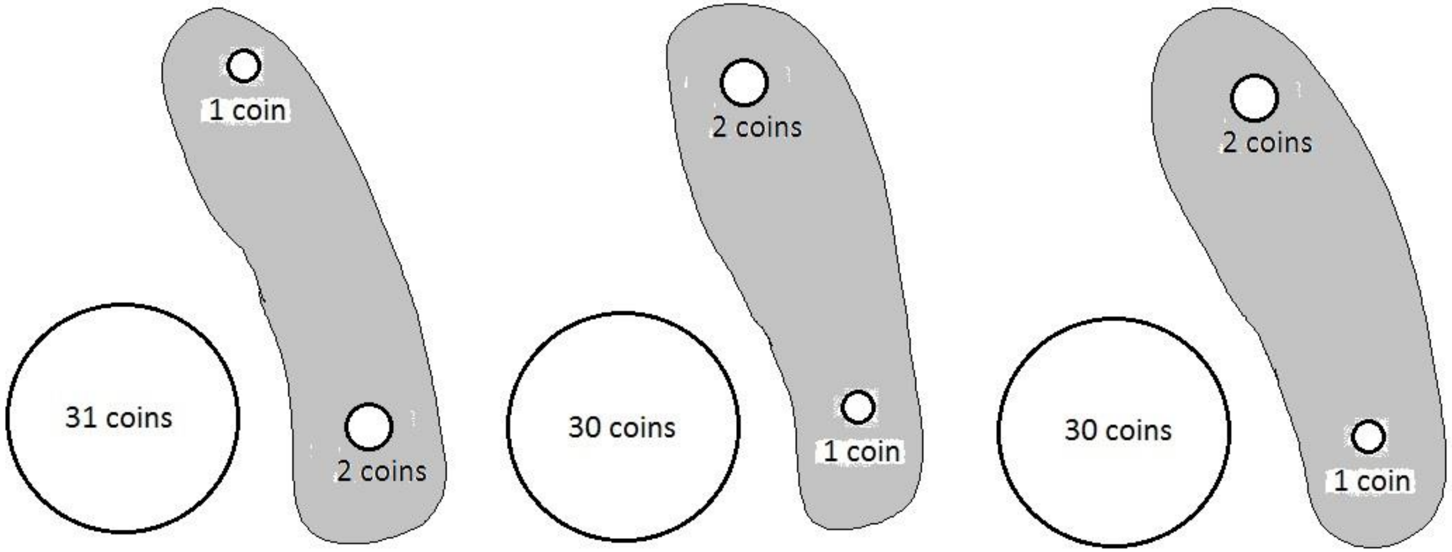


The Original Problem



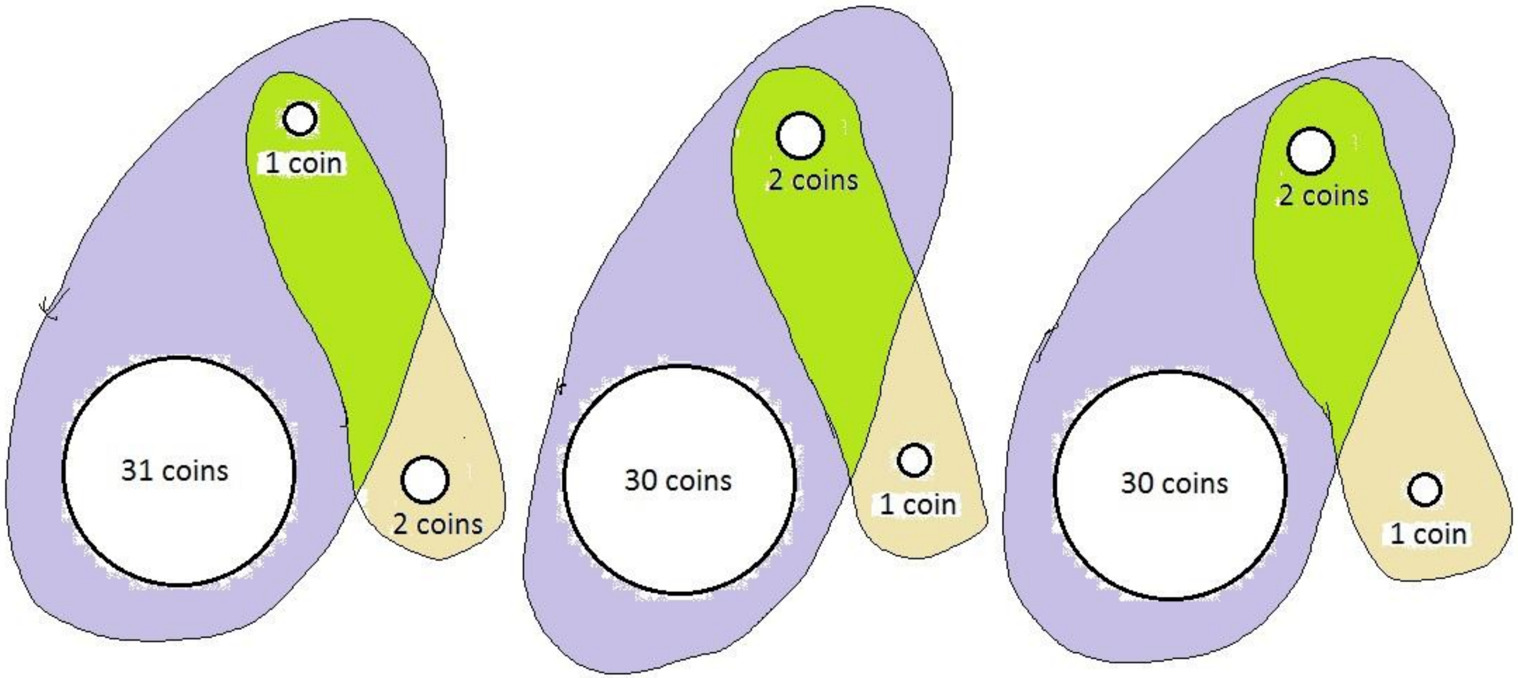
The Original Problem

These three combined groups are also equal in mass.



The Original Problem

The only way to satisfy the weight equality conditions is to have one fake coin in the same group of each "triplet."



Notation

Notation

t = Total number of coins

Notation

t = Total number of coins

n_f = “n-fake” (Actual number of fake coins)

Notation

t = Total number of coins

n_f = “n-fake” (Actual number of fake coins)

n_d = “n-disprove” (Number of fake coins that we’re trying to disprove)

The Revealing Coefficient: Our Main Objective

The primary goal of this project is to make the revealing coefficient, or the amount of information we have to give away to prove how many counterfeit coins there truly are, as small as possible.

The Revealing Coefficient: Our Main Objective

The primary goal of this project is to make the revealing coefficient, or the amount of information we have to give away to prove how many counterfeit coins there truly are, as small as possible.

General Formula:

$$R_c = \frac{\text{Original Number of Possibilities} - \text{New Number of Possibilities}}{\text{Original Number of Possibilities}}$$

Or alternatively:

$$R_c = 1 - \frac{\text{New Number of Possibilities}}{\text{Original Number of Possibilities}}$$

The Revealing Coefficient: Our Main Objective

Example: t = 100,

n_f = 2, n_d = 1

The Revealing Coefficient: Our Main Objective

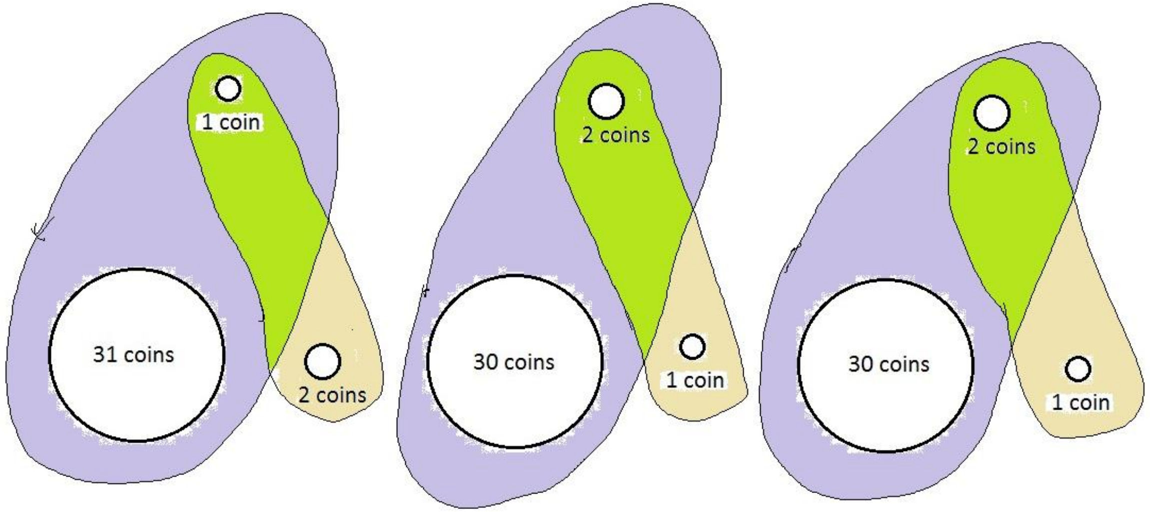
Example: t = 100,

n_f = 2, n_d = 1

$$R_c = 1 - \frac{50^2}{\binom{100}{2}} = 49/99 \approx 0.4949$$

The Revealing Coefficient: Our Main Objective

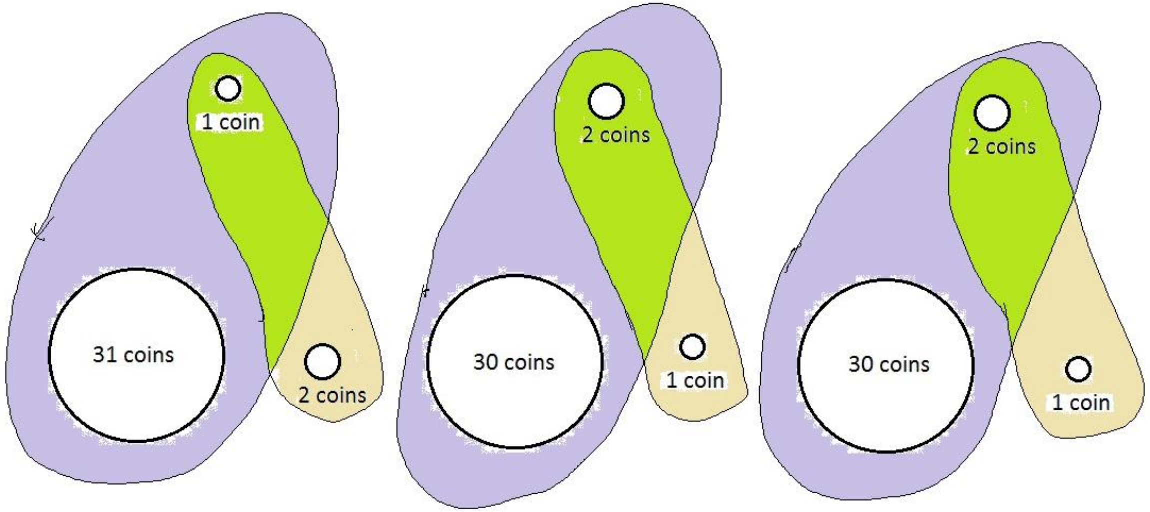
Example: t = 100, n_f = 3, n_d = 2



The Revealing Coefficient: Our Main Objective

Example: t = 100, n_f = 3, n_d = 2

$$R_c = 1 - \frac{31 \cdot 30 \cdot 30 + 1 \cdot 2 \cdot 2 + 2 \cdot 1 \cdot 1}{\binom{100}{3}} \approx 0.8274$$



A (New) New Coin Weighing Problem

For some initial values of the total number of coins and fake coins, it turns out that it is impossible to generate a non-revealing strategy with our current.

For example, it is impossible to prove that n_f = 1 without fully divulging information about any specific coin.

Is there an alternate method?

A (New) New Coin Weighing Problem

New Rules:

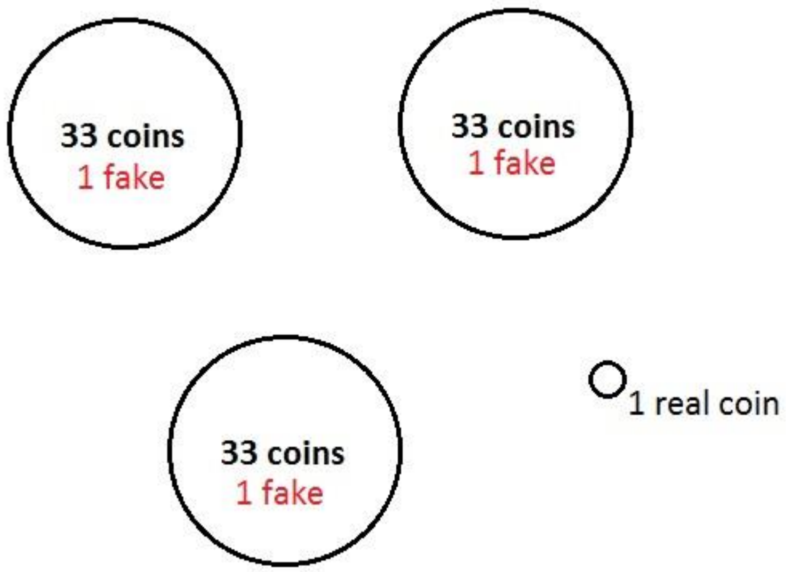
1. You are allowed to fully reveal information about a few coins.
2. Everything else is the same as before.

A (New) New Coin Weighing Problem

The New Rules: t = 100, n_f = 3, n_d = 2

A (New) New Coin Weighing Problem

The New Rules: t = 100, n_f = 3, n_d = 2



A (New) New Coin Weighing Problem

The New Rules: t = 100, n_f = 3, n_d = 2

$$1 - \frac{33 \cdot 33 \cdot 33}{\binom{100}{3}} = 0.7778$$

- A clear improvement from the previous value of 0.8274.

A (New) New Coin Weighing Problem

A General Method for n_d = n_f - 1:

- For $t \equiv 1, 2, 3, \ldots, n_f - 2 \mod n_f$, remove the smallest possible number of real coins such that n_f evenly divides t, then split the coins up into equal groups with one fake coin in each group. These n_f larger groups all equal in weight, so the number of fake coins must be divisible by n_f.

- For $t \equiv -1 \mod n_f$, we can use the same method as above, but because there will be exactly n_d = n_f - 1 real coins left over, we have to swap one of these for a real coin in one of the larger piles.

- This method can be modified to fit any initial set of parameters. (eg: n_d = n_f - c, 0 < c < n_f)

A (New) New Coin Weighing Problem

A General Method for $n_d = n_f - 1$:

For $t \equiv 1, 2, 3, \ldots, n_f - 2 \mod n_f$, $\quad R_c = 1 - \dfrac{\lfloor \frac{t}{n_f} \rfloor^{n_f}}{\binom{t}{n_f}}$

For $t \equiv -1 \mod n_f$, $\quad R_c = 1 - \dfrac{\lfloor \frac{t}{n_f} \rfloor^{n_f - 1} (\lfloor \frac{t}{n_f} \rfloor - 1)}{\binom{t}{n_f}}$

A (New) New Coin Weighing Problem

Back to the revealing coefficient: It is easy to show in all cases that as t grows large the revealing coefficient for our new method always approaches the value

$$1-\frac{n_f!}{n_f^{n_f}}$$

A (New) New Coin Weighing Problem

Back to the revealing coefficient: It is easy to show in all cases that as t grows large the revealing coefficient for our new method always approaches the value

$$1 - \frac{n_f!}{n_f^{n_f}}$$

For example: t = 100, n_f = 3, n_d = 2, we have R_c =

$$1 - \frac{33 \cdot 33 \cdot 33}{\binom{100}{3}} = 0.7778 \approx 1 - \frac{3!}{3^3} = 0.7778$$

A (New) New Coin Weighing Problem

- Unfortunately, as n_f grows larger, the value of $1-\frac{n_f!}{n_f^{n_f}}$ approaches 1 extremely fast.

- For example, if we have t = 1500 and n_f = 15, our current method yields R_c = 0.999997, equivalent to saying that our fake coins are concealed by a factor of 0.0003% of their initial concealment.

A New ((New) New) Coin Weighing Problem?

Fortunately, there is a way around this problem if $\gcd(t, n_f) > 1$:

Choose the lowest common divisor of t and n_f that is greater than 1 (call this value h), and divide the coins into h equal groups of coins with equal numbers of fake coins.

A New ((New) New) Coin Weighing Problem?

The revealing coefficient, or the measure of information lost, for this case is calculated as follows:

$$R_c = 1 - \frac{\binom{\frac{t}{h}}{\frac{n_f}{h}}^h}{\binom{t}{n_f}}$$

A New ((New) New) Coin Weighing Problem?

How well it works:

Take our previous example, t = 1500, n_f = 15, R_c = 0.999997.

If we take h to be 3, then

$$R_c = 1 - \frac{\binom{\frac{1500}{3}}{\frac{15}{3}}^3}{\binom{1500}{15}} = 0.946728$$

Vast improvement: the ratio of 1 -R_c for the two methods is approximately 16000.

Objectives For Future Research

-We would like to create algorithms for both the original and the modified rules in order to minimize the revealing coefficient.

-Find a general method to determine the rate of convergence of the revealing coefficients to a set limit as t → infinity (and better yet, determining these limits).

-Generalize the original problem even more (eg. Counterfeit coins of multiple weights, limited number of weighings, proving the number of fake coins where the judges know nothing about the number, etc)

Acknowledgements

-Dr. Tanya Khovanova

-My family

-MIT’s PRIMES and all of its fantastic staff