

Dynamic Traitor Tracing for Arbitrary Alphabets: *Divide and Conquer*

Thijs Laarhoven (TU/e), Jan-Jaap Oosterwijk (TU/e), Jeroen Doumen (Irdeto)



Game 1: *Guess Who*

- Each player secretly draws **one out of n** face cards.
- Players take turns asking **yes/no questions**.
- The opponent answers **truthfully** for his secret card.
- The first player to **guess the opponent's card**, wins!

Solution: *Binary search*

- Number of questions needed: $\ell = O(\log n)$
- Always guess correctly after at most ℓ questions.

Game 2: *Guess Them*

- Each player secretly draws **c out of n** cards.
- Players take turns asking yes/no questions.
- The opponent answers truthfully for **one of his c cards**.
- The first player to **guess all opponent's cards**, wins!

Example:



Q: Do you have red hair?
A: No.

Q: Are you a man?
A: Yes.

Solution: *Tardos ('03), Laarhoven ('11)*

- Number of questions needed: $\ell = O(c^2 \log n/\epsilon)$
- Probability of error: ϵ

Game 3: *Guess Them, Multiple Choice*

- Each player secretly draws c out of n cards.
- Players take turns asking **multiple choice questions**.
(Number of choices: $q > 2$)
- The opponent answers truthfully for one of his c cards.
- The first player to guess all opponent's cards, wins!

Example:

Q: Do you have blond, black, brown or red hair?
A: *Black hair*.

Solution: *Divide and Conquer ('12)*

- Divide** the group in smaller groups (men and women)
- Use yes/no questions for **each** group (as in Game 2)
- When no answer is returned, **repeat** the question!

Example:

	Group 1: Men	Group 2: Women
Q1	Blond hair?	Blond hair?
A1	No.	
Q2	Moustache?	Blond hair?
A2		Yes.
Q3	Moustache?	Blue eyes?
A3		No.
Q4	Moustache?	Big nose?
A4	No.	

Results: *Linear tradeoff between q and ℓ*

- For $q = 4$, half as many questions needed as for $q = 2$.
- Can be generalized to arbitrary values of q .
- Number of questions needed: $\ell = O(c^2/q \log n/\epsilon)$

Actual application: *Copyright Protection*

It is difficult to prevent that users create and distribute illegal copies of copyrighted content. However, once it happens, the copyright holder would like to be able to know **who** did so, and accuse them.

For this purpose, each official copy of the content can be **watermarked** so that an illegal copy can be traced back to the source. Even if pirates form a collusion and try to create a **mixture** of their unique contents, our solution to the "Guess who?" game allows the tracer to find all pirates.