

A note on the problem of prisoners and hats

Petr Glivický

petr.glivicky@gmail.com

University of Economics, Prague

APLIMAT 2018, Bratislava
February 7, 2018

Slides available at <http://www.glivicky.cz>

A story

A group (not necessarily finite) of mathematicians happens to be captured by an evil hatter.

They know that the next day they will be asked to guess colors of hats the captor would have placed on their heads over the night. In general, of course, they will not be permitted to look at their own hats, but may be allowed to see some of the hats that others will be wearing and hear the guesses of some of their colleagues. Besides that, no communication between them is going to be allowed. If sufficiently many of them guess correctly, the whole group will be set free. Otherwise they are all going to be executed. Fortunately, the hatter gets drunk and quite talkative the night before, and he reveals exactly who of the captives will be allowed to see or hear an other, and also the exact threshold for the number of correct guesses needed.

Now they have the whole night to find out how to save their lives.

Formalization

A game with imperfect information of two players:

mathematicians vs. **evil hatter**

An instance consists of:

- $M \neq \emptyset$ a set of mathematicians (prisoners),
- $C \neq \emptyset$ a set of hat colors,
- $S \subseteq M^2$ a visibility relation,
- $H \subseteq M^2$ without oriented cycles a hearability relation,
- $e : {}^M C \times {}^M C \rightarrow \{0, 1\}$ an evaluation function.

The hatter chooses an assignment $a : M \rightarrow C$ of hat colors to mathematicians.

Each mathematician m says her guess $g(m) \in C$ for the color of the hat she is wearing, knowing $a \upharpoonright S^{-1}[m]$ and $g \upharpoonright H^{-1}[m]$.

A strategy for mathematicians is any function $\sigma : X \rightarrow C$ where X is the set of all triples (m, α, γ) where $m \in M$, $\alpha : S^{-1}[m] \rightarrow C$, $\gamma : H^{-1}[m] \rightarrow C$.

The mathematicians win if $e(a, g) = 1$ and lose otherwise.

See all, hear nothing case

Let every mathematician **see all hats except her own** ($S = M^2 - id_M$), but **hear nothing** ($H = \emptyset$). This is called the **see all, hear nothing case**.

Theorem (See all, hear nothing — finite M, C)

Let M, C be both finite. Then there is a strategy that guarantees $\lfloor |M|/|C| \rfloor$ correct guesses, but no strategy guarantees $\lfloor |M|/|C| \rfloor + 1$ correct guesses.

Proof.

A “ $\lfloor |M|/|C| \rfloor$ strategy”: Assume $M = C = \{0, 1, \dots, c-1\}$, and guarantee one correct guess.

Idea: Compute $s = \sum_{i < c} a(i)$ in the additive group \mathbb{Z}_c (i.e. modulo c). No mathematician knows s , but m knows $s_m = s - a(m)$. Let mathematician m hypothesize that $s = m$ and thus guess that $a(m) = s - s_m = m - s_m$. There is one m whose hypothesis is correct, and therefore his guess is correct as well. \square

See all, hear nothing case

Theorem (See all, hear nothing — finite M, C)

Let M, C be both finite. Then there is a strategy that guarantees $\lfloor |M|/|C| \rfloor$ correct guesses, but no strategy guarantees $\lfloor |M|/|C| \rfloor + 1$ correct guesses.

Proof.

No better strategy: If there were a strategy guaranteeing $n > \lfloor |M|/|C| \rfloor$ correct guesses, there would be

- $\geq n$ correct guesses for each assignment a ,
- $\geq n|A| > \frac{|M||A|}{|C|}$ correct pairs (a, m) ,
- $> |A|/|C|$ correct a 's for some $m \in M$,
- > 1 correct guess of $a(m)$ for one of $|A|/|C|$ possible assignments a' on $M - \{m\}$,

— a contradiction (m 's guess is determined by a'). □

See all, hear nothing case

Theorem (See all, hear nothing — finite M , infinite C)

Let M be finite, C infinite. Then no strategy guarantees even 1 correct guess.

Proof.

Otherwise, by restricting the possible colors to $C' \subseteq C$ with $|C'| = |M| + 1$, we would get a strategy guaranteeing **at least $1 > |M|/|C'|$ correct guess** — a contradiction with the previous. □

See all, hear nothing case

Theorem (See all, hear nothing — infinite M)

Let M be infinite, $|C| > 1$ (finite or infinite). Then there is a strategy guaranteeing at most finitely many incorrect guesses, but no fixed finite number of incorrect guesses can be guaranteed.

Proof.

A “ $< \omega$ strategy”: Say that two color assignments $a, a' : M \rightarrow C$ are equivalent, write $a \sim a'$, if they differ in at most finitely many positions. Fix a selector s that chooses one element $s([a]_{\sim})$ from each equivalence class $[a]_{\sim}$.

Each mathematician m knows the class $[a]_{\sim}$ (she can see all of a except the value at m), and thus she can take $a' = s([a]_{\sim})$ and guess that $a(m) = a'(m)$.

As a and a' differ in at most finitely many positions, at most finitely many mathematicians will get a wrong guess. □

See all, hear nothing case

Theorem (See all, hear nothing — infinite M)

Let M be infinite, $|C| > 1$ (finite or infinite). Then there is a strategy guaranteeing at most finitely many incorrect guesses, but no fixed finite number of incorrect guesses can be guaranteed.

Proof.

No “ $\leq n$ strategy”: Suppose there is a strategy that guarantees at most n incorrect guesses. By restricting it to just **two colors** ($|C'| = 2$) and **$2n + 1$ mathematicians** ($|M'| = 2n + 1$), we get a strategy that guarantees **at least $n + 1$ correct** guesses.

But $n + 1 > \frac{2n+1}{2} = |M'|/|C'|$ — a contradiction with the finite case. □

See forward, hear nothing case

Now suppose mathematicians are **standing in a well-ordered line** (i.e. $\langle M, \prec \rangle$ is a well-ordering) and they are all **facing the tail of the line**. Then they can **see only the hats in front of them** ($S = \succ$). Let them **hear nothing** ($H = \emptyset$), as previously. This is called the **see forward, hear nothing case**.

Theorem (See forward, hear nothing — finite M)

Let M be finite, $|C| > 1$ (finite or infinite). Then no strategy guarantees even 1 correct guess.

Proof.

For any possible strategy σ , we inductively construct an color assignment a , for which **the strategy always fails**: **Start from the greatest element** m_{n-1} from the enumeration $m_0 < \dots < m_{n-1}$ of M and **choose $a(m_{n-1})$ different from what σ suggests**, then successively do the same for m_{n-2}, \dots, m_0 (the part of a that m_i sees will always be known at the time we get to m_i). □

Theorem (See forward, hear nothing — infinite M)

Let M be infinite, $|C| > 1$ (finite or infinite). Then there is a strategy guaranteeing at most finitely many incorrect guesses, but no fixed finite number of incorrect guesses can be guaranteed.

Proof.

Analogous to the “see all, hear nothing” case.

A “ $< \omega$ strategy”: Let $a \sim_m a'$ if $a(x) = a'(x)$ for all $x \succ m$ (i.e. all x that m sees). Fix a well ordering $<^A$ of all assignments.

Every $m \in M$ knows $[a]_{\sim_m}$. Let m guess $a(m) = a_m(m)$, where a_m is the $<^A$ -minimal element of $[a]_{\sim_m}$. For $m \prec m'$, we have $[a]_{\sim_m} \subseteq [a]_{\sim_{m'}}$, and thus $a_m \geq^A a_{m'}$.

If infinitely many mathematicians $m_0 < m_1 < \dots$ guess wrong, then in $a_{m_0} \geq^A a_{m_1} \geq^A \dots$ the equalities are impossible (a_{m_i} agrees with a in m_{i+1} , while $a_{m_{i+1}}$ does not). We've got an infinite strictly decreasing sequence in a well-ordering $<^A$ — a contradiction. \square

Theorem (See forward, hear nothing — infinite M)

Let M be infinite, $|C| > 1$ (finite or infinite). Then there is a strategy guaranteeing at most finitely many incorrect guesses, but no fixed finite number of incorrect guesses can be guaranteed.

Proof.

No “ $\leq n$ strategy”: If there were a strategy guaranteeing **at most n incorrect guesses**, then by **reduction to $|M'| = n + 1$** , we would get at least 1 correct guess — a contradiction with the finite case. □

See forward, hear backward case

Again suppose that mathematicians are **standing in a well-ordered line** ($\langle M, \prec \rangle$) and that they can **see only the hats in front of them** ($S = \succ$). But this time they are guessing in the order given by \prec and they can **hear all the guesses of their colleagues behind them** ($H = \prec$). This is called the **see forward, hear backward case**.

Theorem (See forward, hear backward)

Let M be arbitrary, $|C| > 1$ (finite or infinite). Then there is a strategy that guarantees at most 1 incorrect guess, but no strategy that would guarantee all guesses correct.

Proof.

No “all correct” strategy: Let m_0 be the first element of M . Further let $a(m) = a'(m)$ for all $m \neq m_0$, but $a(m_0) \neq a'(m_0)$. Then any strategy **gives the same guess for $a(m_0)$ and $a'(m_0)$** — one of them must be wrong. □

See forward, hear backward case

Theorem (See forward, hear backward)

Let M be arbitrary, $|C| > 1$ (finite or infinite). Then there is a strategy that guarantees at most 1 incorrect guess, but no strategy that would guarantee all guesses correct.

A “ ≤ 1 incorrect” strategy. Proof idea:

The first $m \in M$ computes the “sum” s of all colors that she sees (all except her own) and encodes the result as her guess (which may be incorrect).

Each other $m \in M$ can then compute $a(m) = s - s(m) - h(m)$, where $s(m)$ is the “sum” of all colors that m sees and $h(m)$ is the “sum” of all (correct) guesses of her predecessors excluding the first one. This is necessarily correct.

It needs to be specified, what “sum” means.

See forward, hear backward case

A precise proof is algebraic. “Sum” is a group homomorphism.

For an additive group G and ordinal δ :

- $G^\delta = \{f; f : \delta \rightarrow G\}$... a product,
- $G^{(\delta)} = \{f; f : \delta \rightarrow G \text{ with finitely many nonzero values}\}$... a direct sum,
- $\Sigma : G^{(\delta)} \rightarrow G$... the natural sum homomorphism.

Lemma

For any ordinal $\delta > 0$ and cardinal $\mu > 0$ there is an Abelian group G of size μ such that the sum homomorphism $\Sigma : G^{(\delta)} \rightarrow G$ can be extended to a homomorphism $\Sigma' : G^\delta \rightarrow G$.

Proof.

For $\mu \geq \omega$ take $G = \mathbb{Q}^{(\mu)}$. Then G is divisible, thus **injective**.

Therefore Σ factors through the inclusion $G^{(\delta)} \subseteq G^\delta$, yielding Σ' .

For $0 < \mu < \omega$ take $G = \mathbb{Z}/\mu\mathbb{Z}$. Then G is **purely injective**, the inclusion $G^{(\delta)} \subseteq G^\delta$ is **pure**, and we get Σ' as above. □

See forward, hear backward case

Theorem (See forward, hear backward)

Let M be arbitrary, $|C| > 1$ (finite or infinite). Then there is a strategy that guarantees at most 1 incorrect guess, but no strategy that would guarantee all guesses correct.

Proof.

A “ ≤ 1 incorrect” strategy: Assume $|M| > 1$ and $M = \delta \cup \{-1\}$ for an ordinal $\delta > 0$. Further assume $C = \mu$ for a cardinal $\mu > 1$, and take a **group G from the Lemma** such that the underlying set of G is μ as well. (So $G = C = \mu$ as sets.)

Now let $m = -1$ guess $g(-1) = \Sigma'(a \upharpoonright \delta)$, and then let inductively $m = \alpha \in \delta$ guess $g(\alpha) = g(-1) - \Sigma'(a_\alpha)$, where

- $a_\alpha(\beta) = a(\beta)$ for $\alpha < \beta < \delta$ (where α sees),
- $a_\alpha(\alpha) = 0$ (his own color?),
- $a_\alpha(\beta) = g(\beta)$ for $0 \leq \beta < \alpha$ (what α heard, except -1).

We get, inductively for any $\alpha \in \delta$:

$$g(\alpha) = \Sigma'(a \upharpoonright \delta) - \Sigma'(a_\alpha) = \Sigma'(a \upharpoonright \delta - a_\alpha) = \Sigma(a \upharpoonright \delta - a_\alpha) = a(\alpha). \quad \square$$

Thank you for your attention.

References: [*P. Glivický, A note on the problem of prisoners and hats, to appear in the proceedings of APLIMAT 2018, arXiv: 1801.01184*]