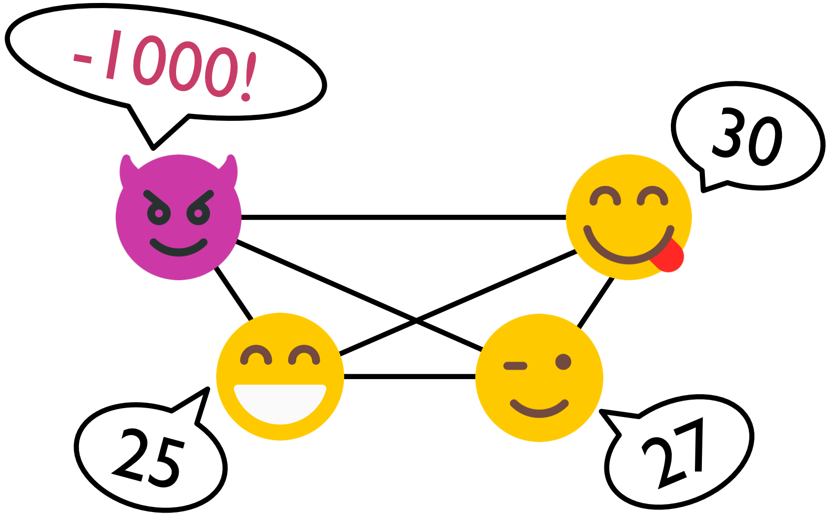
Communication-Optimal Convex Agreement

Diana Ghinea[*], Chen-Da Liu-Zhang[*✣], Roger Wattenhofer[★]

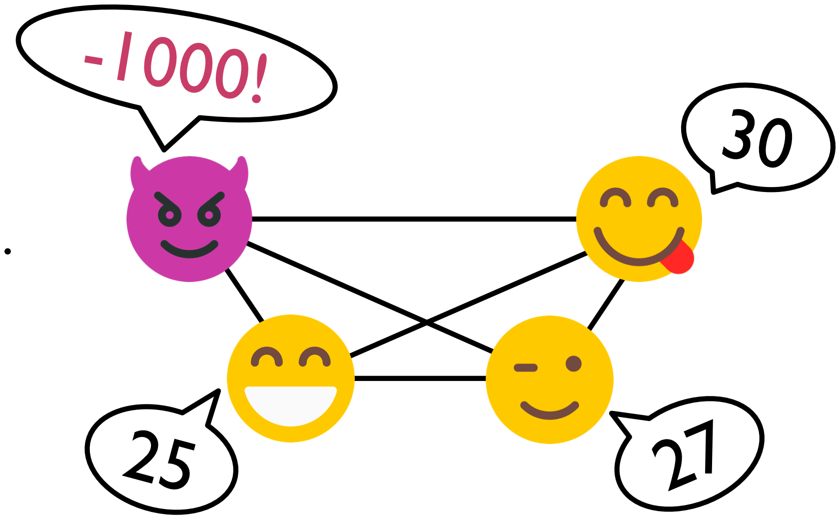
[*] Lucerne University of Applied Sciences and Arts
[✣] Web3 Foundation
[★] ETH Zürich

Byzantine Agreement

- Consider n parties; $t < n/3$ of them byzantine.
- The network is synchronous.
- Each party has an input.
- Honest parties need to **agree** on a value…

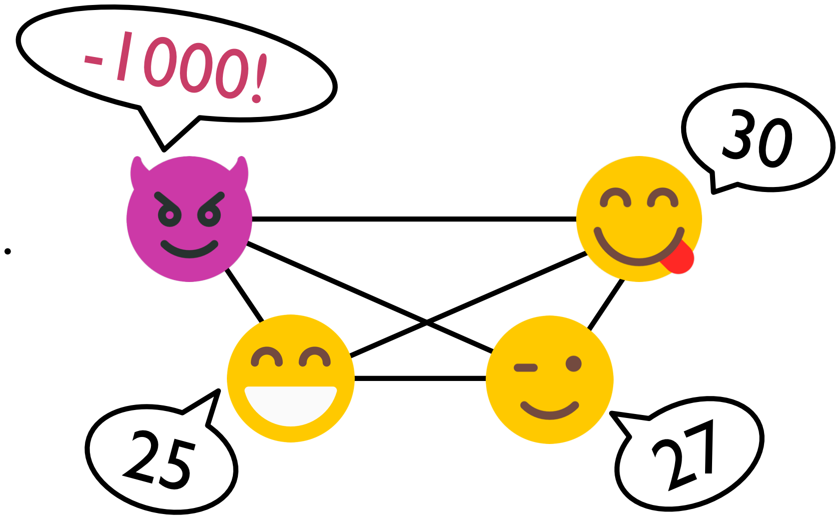


Byzantine Agreement



- Consider n parties; $t < n/3$ of them byzantine.
- The network is synchronous.
- Each party has an input.
- Honest parties need to **agree** on a value…
  - … satisfying the following **validity** condition:
    - **If all honest parties have input v, then the output agreed upon is v.**

Convex ~~Byzantine~~ Agreement

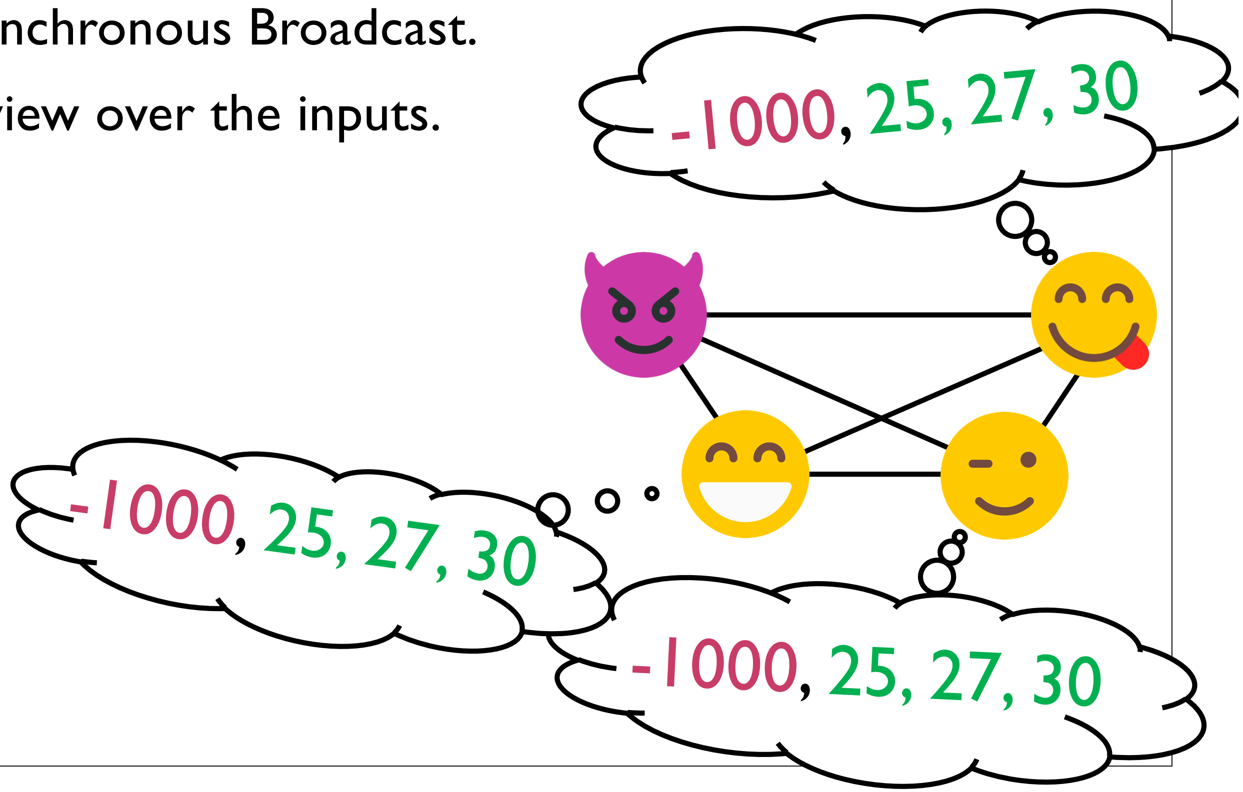


- Consider n parties; $t < n/3$ of them byzantine.
- The network is synchronous.
- Each party has an input **(for today in $\mathbb{Z}$)**.
- Honest parties need to **agree** on a value…
  - … satisfying the following **validity** condition:
    - ~~**If all honest parties have input v, then the output agreed upon is v.**~~
    - **The output agreed upon must be in the honest inputs' range.**

How can we achieve Convex Agreement?

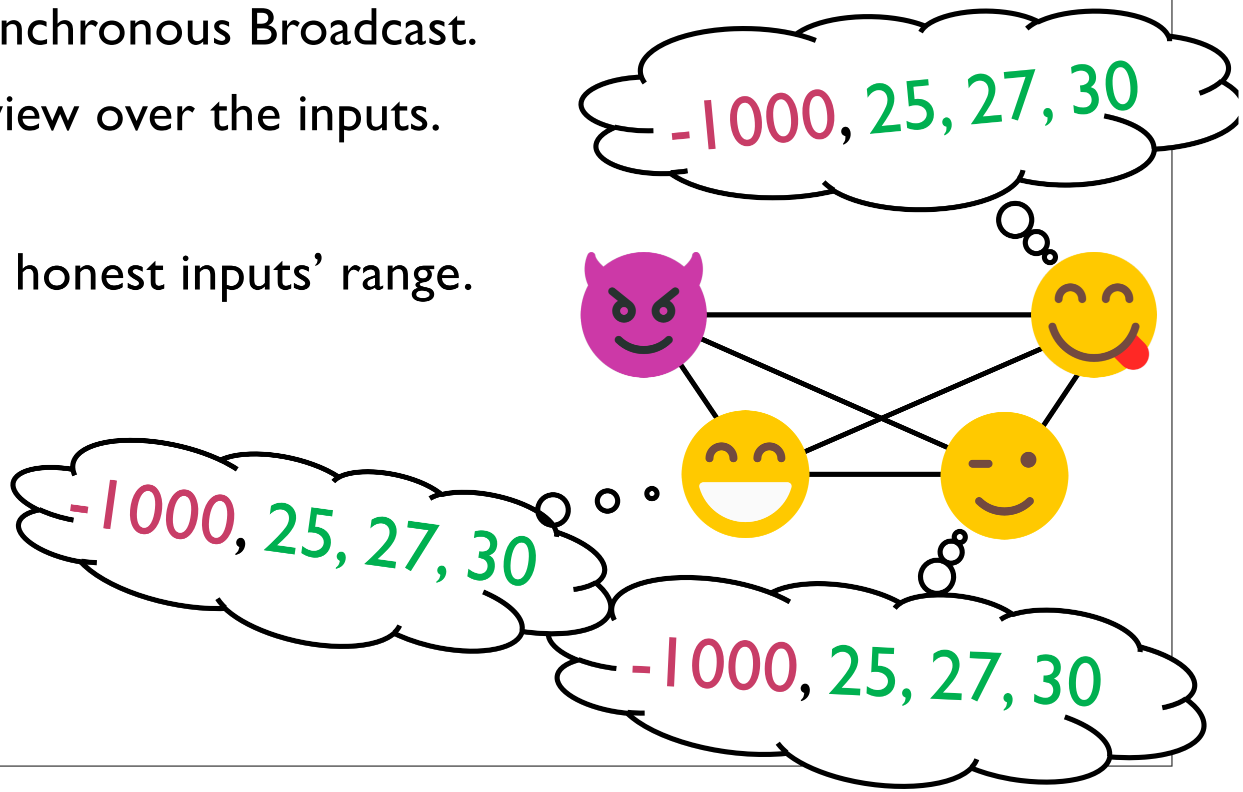
Via Synchronous Broadcast

- Each party sends its input via Synchronous Broadcast.
- The parties obtain an identical view over the inputs.



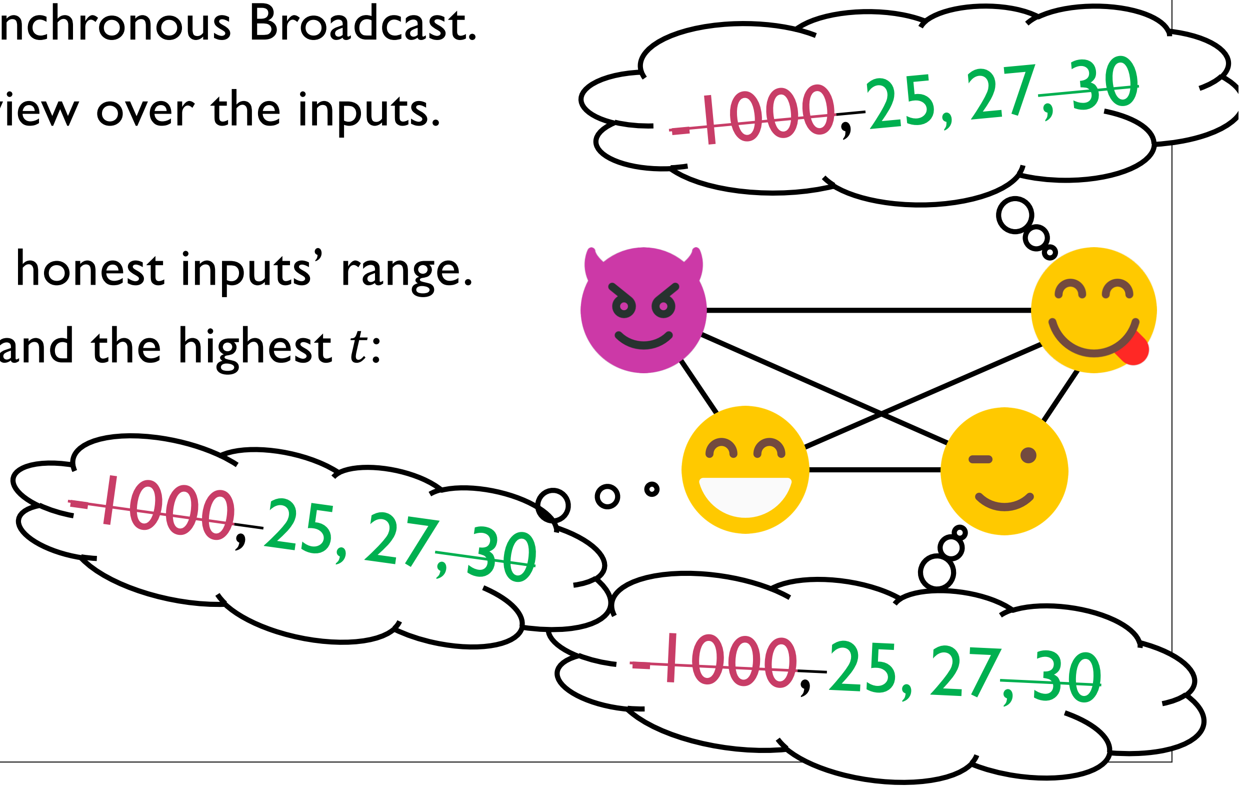
Via Synchronous Broadcast

- Each party sends its input via Synchronous Broadcast.
- The parties obtain an identical view over the inputs.
- Out of the values received:
  - At most t may be outside the honest inputs' range.



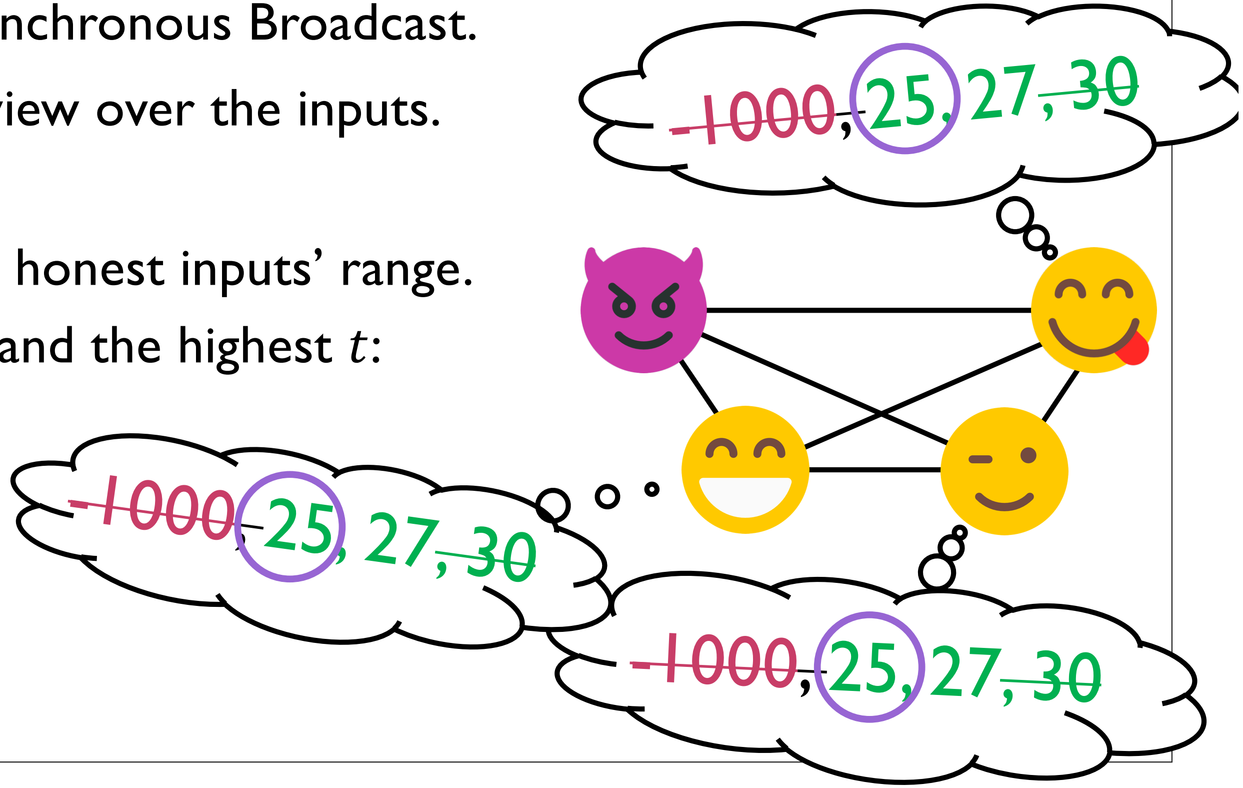
Via Synchronous Broadcast

- Each party sends its input via Synchronous Broadcast.
- The parties obtain an identical view over the inputs.
- Out of the values received:
  - At most t may be outside the honest inputs' range.
  - So, if we discard the lowest t and the highest t:
    - All values remaining are valid.



Via Synchronous Broadcast

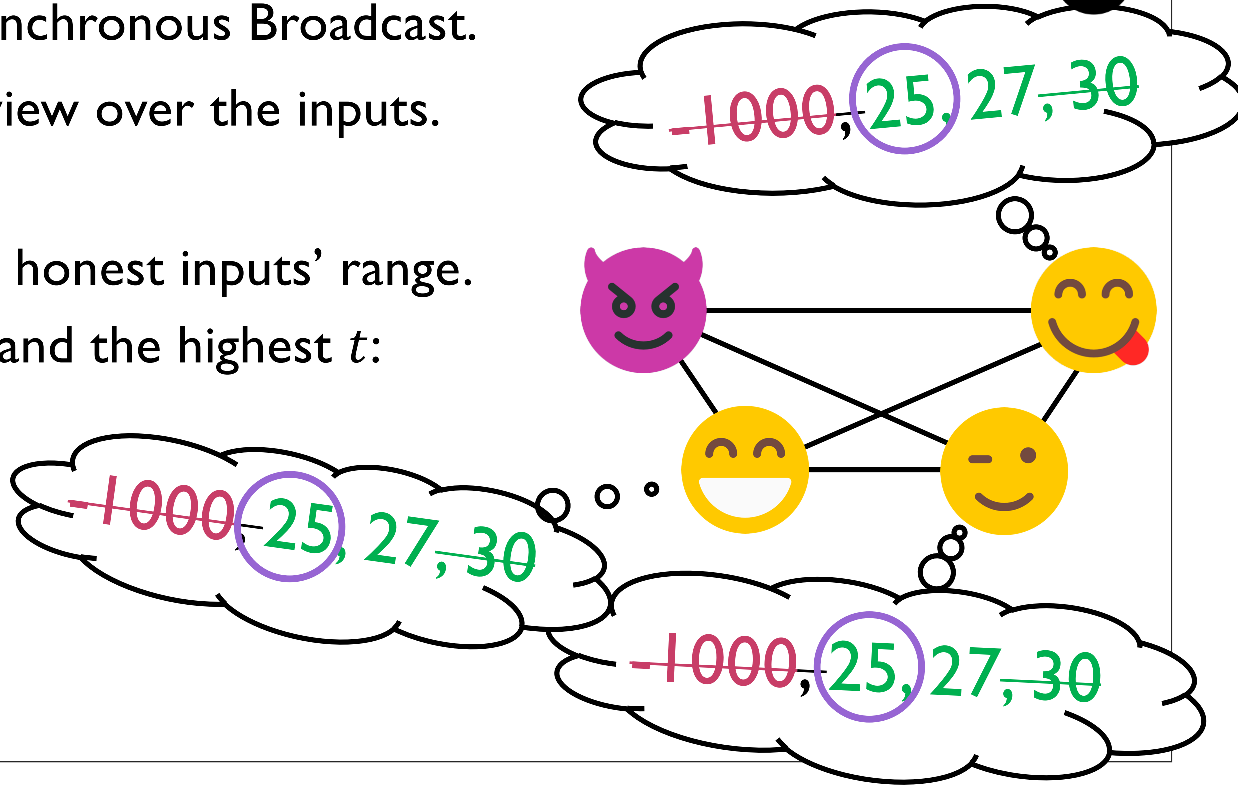
- Each party sends its input via Synchronous Broadcast.
- The parties obtain an identical view over the inputs.
- Out of the values received:
  - At most t may be outside the honest inputs' range.
  - So, if we discard the lowest t and the highest t:
    - All values remaining are valid.
    - Output the lowest.



Via Synchronous Broadcast

Optimal resilience ☑
Optimal round complexity ☑
Optimal communication complexity ?

- Each party sends its input via Synchronous Broadcast.
- The parties obtain an identical view over the inputs.
- Out of the values received:
  - At most t may be outside the honest inputs' range.
  - So, if we discard the lowest t and the highest t:
    - All values remaining are valid.
    - Output the lowest.



What is the optimal **communication complexity** for Convex Agreement?

= number of bits sent by the honest parties

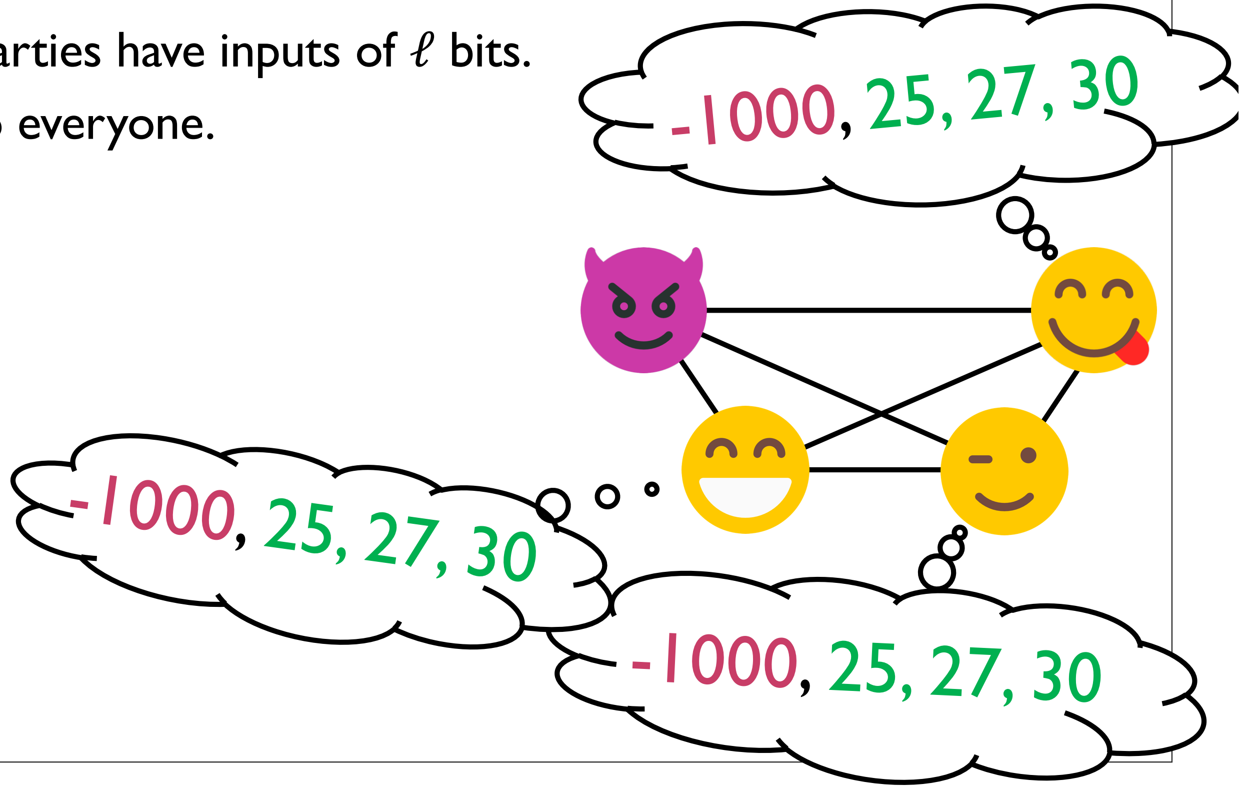
assuming they have ℓ-bit inputs.

Communication Complexity

◦ Prior solutions: At least $O(\ell n^2)$ bits,

assuming honest parties have inputs of ℓ bits.

~ as every party sends its input to everyone.



Communication Complexity

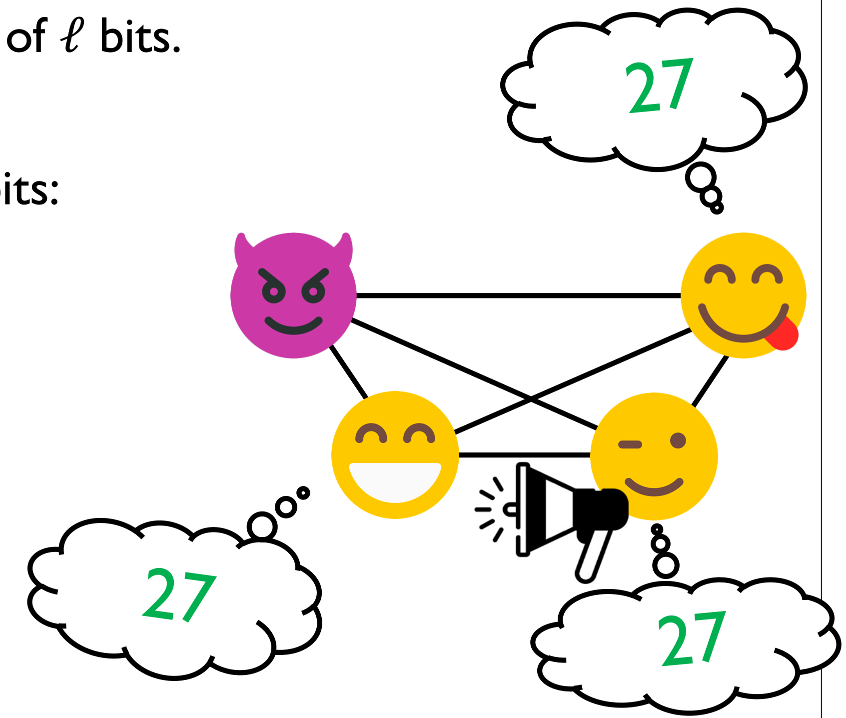
- Prior solutions: At least $O(\ell n^2)$ bits,

  assuming honest parties have inputs of ℓ bits.

  ~ as every party sends its input to everyone.
- A **lower bound**, if honest parties have inputs of ℓ bits:

  $\Omega(\ell n)$.

  ~ one honest party sends its input to everyone.



Communication Complexity

- Prior solutions: At least $O(\ell n^2)$ bits,

  assuming honest parties have inputs of ℓ bits.

  ~ as every party sends its input to everyone.

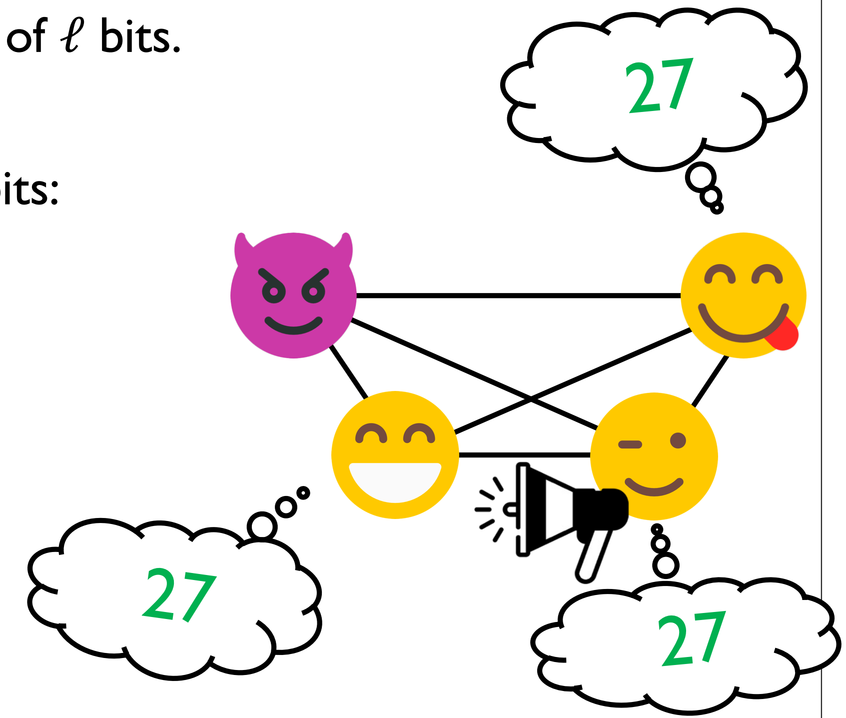
- A **lower bound**, if honest parties have inputs of ℓ bits:

  $\Omega(\ell n)$.

  ~ one honest party sends its input to everyone.

For **Byzantine Agreement**, $O(\ell n)$ bits are sufficient (for large enough ℓ)!

However, existing solutions lose information about the honest inputs' range.



Communication Complexity

Are $O(\ell n)$ bits are **sufficient** for Convex Agreement as well? Or do we ***need*** more?

- Prior solutions: At least $O(\ell n^2)$ bits,

  assuming honest parties have inputs of ℓ bits.

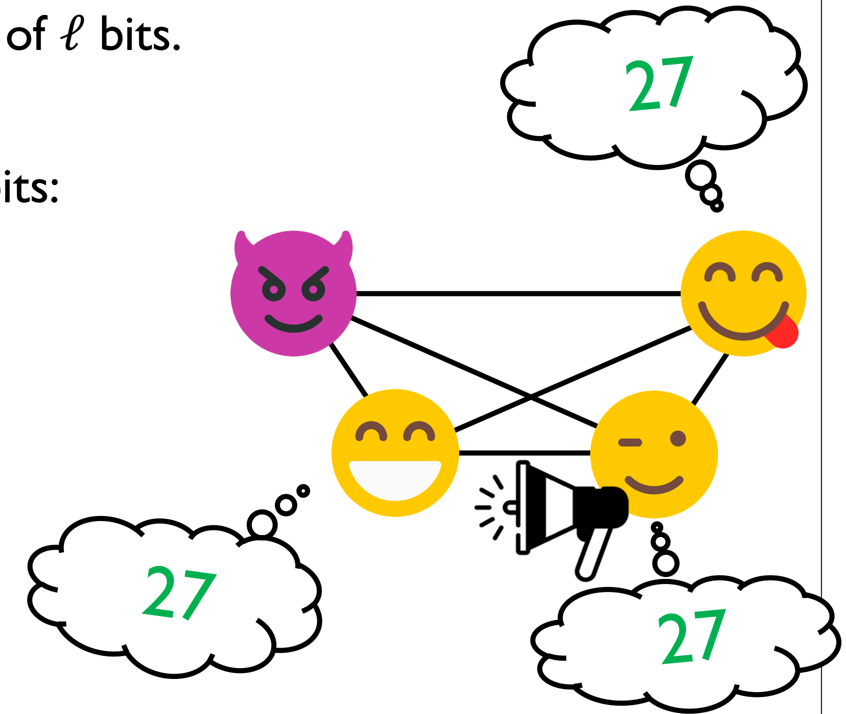
  ~ as every party sends its input to everyone.
- A **lower bound**, if honest parties have inputs of ℓ bits:

  $\Omega(\ell n)$.

  ~ one honest party sends its input to everyone.

For **Byzantine Agreement**, $O(\ell n)$ bits are sufficient (for large enough ℓ)!

However, existing solutions lose information about the honest inputs' range.

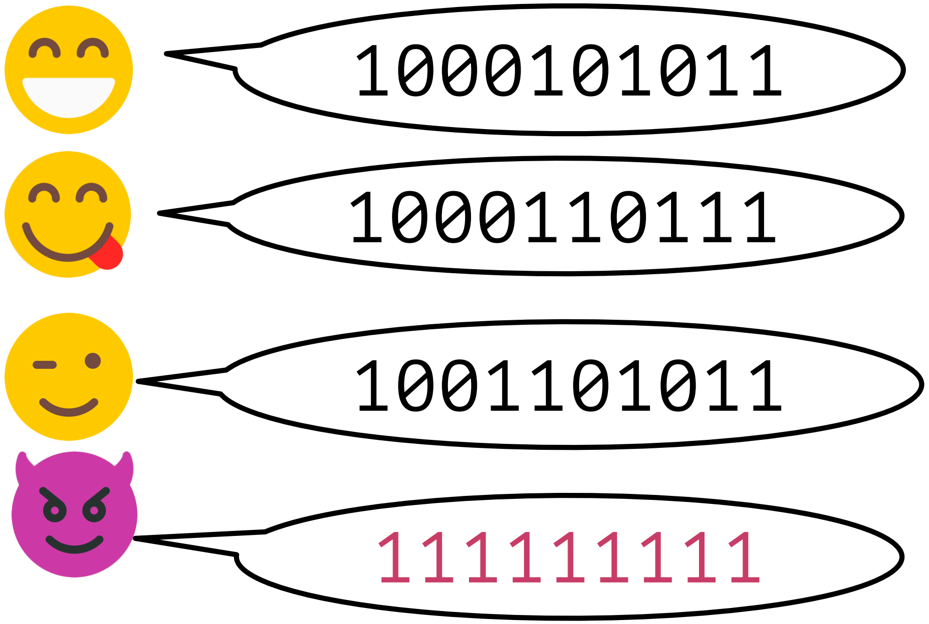


$O(\ell n)$ bits are sufficient for Convex Agreement

given that $\ell \in \Omega(\kappa\, n \log^2 n)$.

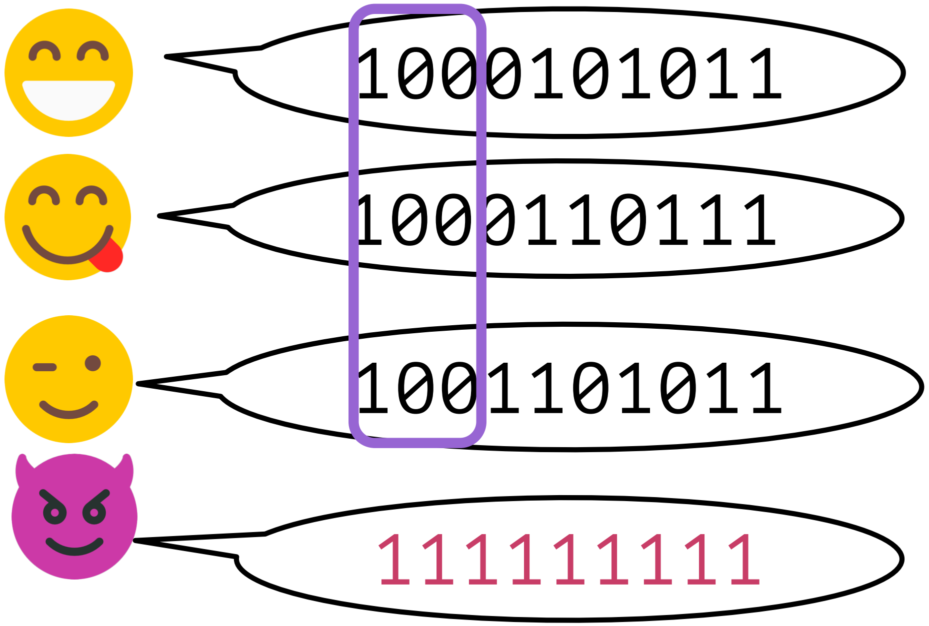
Key Idea

- Represent the inputs (in $\mathbb{N}$) as bitstrings of ℓ bits.



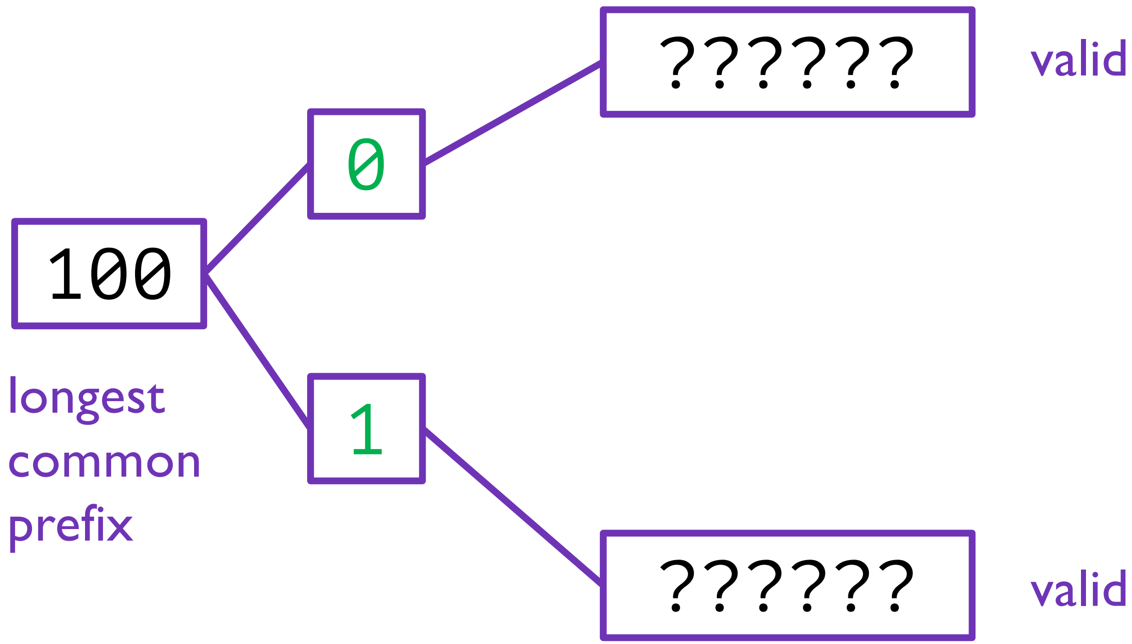
Key Idea: Longest Common Prefix

- Represent the inputs (in $\mathbb{N}$) as bitstrings of ℓ bits.



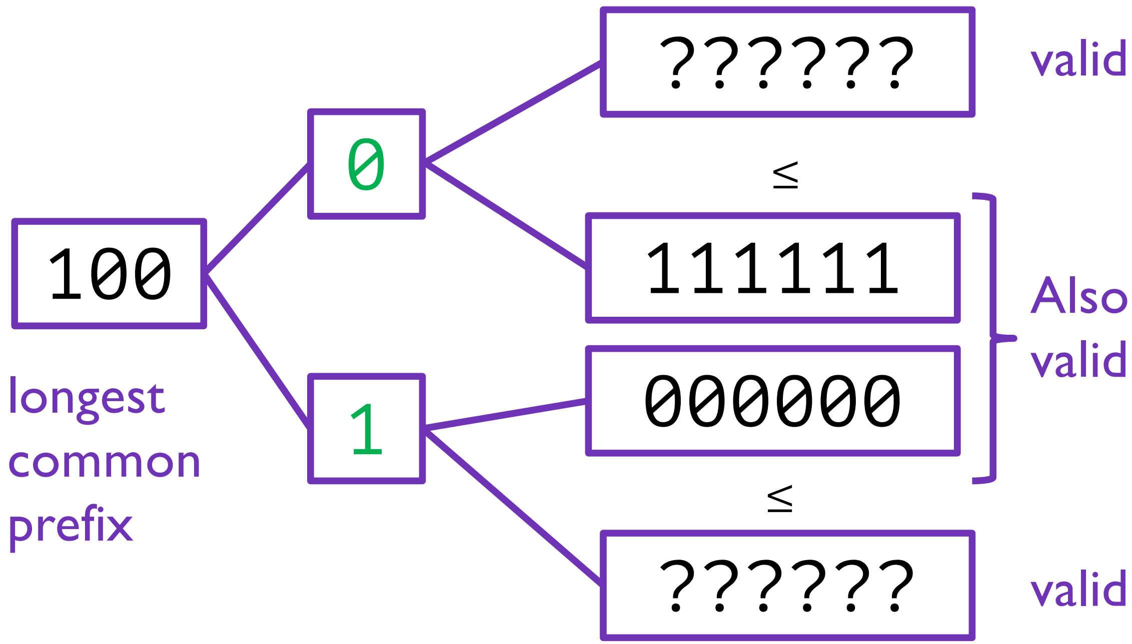
Key Idea: Longest Common Prefix

- Represent the inputs (in $\mathbb{N}$) as bitstrings of ℓ bits.



Key Idea: Longest Common Prefix

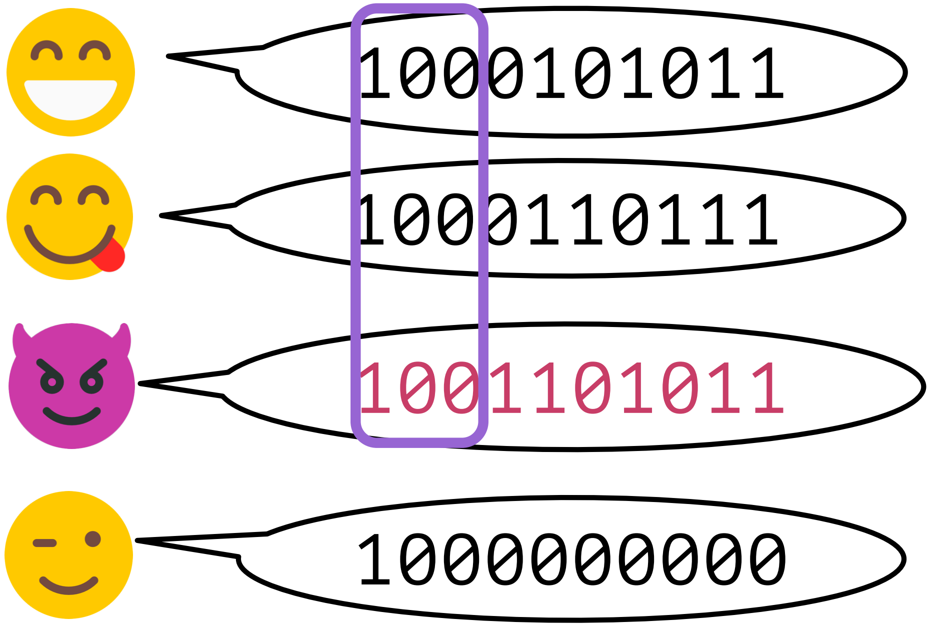
- Represent the inputs (in $\mathbb{N}$) as bitstrings of ℓ bits.



The honest parties can output 1000111111

Key Idea: Longest Common Prefix

- Represent the inputs (in $\mathbb{N}$) as bitstrings of ℓ bits.



The byzantine parties prevent us from finding the *actual* longest common prefix.

Key Idea: ~~Longest Common Prefix~~

Longest prefix of a valid value that we can agree upon using Byzantine Agreement*

Reminder:

Byzantine Agreement enables the honest parties to agree on an output such that:
If all honest parties hold the same input, this is the output agreed upon.

Key Idea: ~~Longest Common Prefix~~

Longest prefix of a valid value that we can agree upon using Byzantine Agreement*

*returns either an honest input or ⊥

*returns ⊥ only if "it's hard to identify an honest input"

*with communication complexity $O(\ell n + poly(n, \kappa))$

Reminder:

Byzantine Agreement enables the honest parties to agree on an output such that:
If all honest parties hold the same input, this is the output agreed upon.

Key Idea: ~~Longest Common Prefix~~

Longest prefix of a valid value that we can agree upon using Byzantine Agreement*

- Binary search:
  - Run Byzantine Agreement* on the first half of the inputs' bitstrings:
    - Returns an honest prefix:
      - Continue the search 'on the right'
    - Returns $\perp$:
      - Continue the search 'on the left'.

*returns either an honest input or $\perp$

*returns $\perp$ only if "it's hard to identify an honest input"

*with communication complexity $O(\ell n + poly(n, \kappa))$

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.

✨011100011111✨??????????

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.
  - Extend so that there is an ℓ-bit valid value that does not have this prefix.

✨0111000111110✨?????????

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.
  - Extend so that there is an ℓ-bit valid value that does not have this prefix.

✨0111000111110✨0000...0000

$\leq$

✨0111000111110✨?????????

$\leq$

✨0111000111110✨1111...1111

At least one of these two options is valid.

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.
  - Extend so that there is an ℓ-bit valid value that does not have this prefix.
  - At least $t + 1$ honest parties *know* ℓ-bit valid values that do not have this prefix.

✨0111000111110✨0000...0000

≤

✨0111000111110✨?????????

≤

✨0111000111110✨1111...1111

At least one of these two options is valid.

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.
  - Extend so that there is an ℓ-bit valid value that does not have this prefix.
  - At least $t + 1$ honest parties *know* ℓ-bit valid values that do not have this prefix.

01110000... => I believe the lowest option is valid

≤

✨0111000111110✨0000...0000

≤

✨0111000111110✨?????????

≤

✨0111000111110✨1111...1111

At least one of these two options is valid.

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.
  - Extend so that there is an ℓ-bit valid value that does not have this prefix.
  - At least $t + 1$ honest parties *know* ℓ-bit valid values that do not have this prefix.

Each honest party that has an opinion sends:
- `0` if it believes ✨`0111000111110`✨`0000...0000` is valid.
- `1` if it believes ✨`011100011110`✨`1111...1111` is valid.

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.
  - Extend so that there is an ℓ-bit valid value that does not have this prefix.
  - At least $t + 1$ honest parties *know* ℓ-bit valid values that do not have this prefix.

Each honest party that has an opinion sends:
- `0` if it believes ✨`01110001111110`✨`0000`...`0000` is valid.
- `1` if it believes ✨`01110001111110`✨`1111`...`1111` is valid.

Each party believes the majority bit received.
Final decision: Byzantine Agreement with the majority bit received as input.

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.
  - Extend so that there is an ℓ-bit valid value that does not have this prefix.
  - At least $t + 1$ honest parties *know* ℓ-bit valid values that do not have this prefix.

Each honest party that has an opinion sends:
- 0 if it believes ✨01110001111110✨0000...0000 is valid.
- 1 if it believes ✨01110001111110✨1111...1111 is valid.

Each party believes the majority bit received.
Final decision: Byzantine Agreement with the majority bit received as input.

If Byzantine Agreement returns 0:
The honest parties output ✨01110001111110✨0000...0000
If Byzantine Agreement returns 1:
The honest parties output ✨01110001111110✨1111...1111

Convex Agreement is achieved with $O(\ell n + \kappa n^2 \log^2 n)$ bits of communication!

At the end of the search

- The parties agree on a prefix of an ℓ-bit valid value.
  - Extend so that there is an ℓ-bit valid value that does not have this prefix.
  - At least $t+1$ honest parties *know* ℓ-bit valid values that do not have this prefix.

Each honest party that has an opinion sends:
- `0` if it believes ✨`0111000111110`✨`0000…0000` is valid.
- `1` if it believes ✨`0111000111110`✨`1111…1111` is valid.

Each party believes the majority bit received.
Final decision: Byzantine Agreement with the majority bit received as input.

If Byzantine Agreement returns `0`:
The honest parties output ✨`0111000111110`✨`0000…0000`
If Byzantine Agreement returns `1`:
The honest parties output ✨`0111000111110`✨`1111…1111`

Thanks & Summary

- For ℓ-bit inputs in $\mathbb{Z}$ (with $\ell \in \Omega(\kappa\, n\, log^2 n)$), Convex Agreement can be achieved in the synchronous model up to $t < n/3$ byzantine corruptions with communication complexity $O(\ell n)$.
- This is asymptotically optimal.
- Our solution relies on ~a byzantine variant of the ***longest common prefix*** problem.
- Take a look at our paper!

eprint.iacr.org/2024/251