Byzantine Preferential Voting

Darya Melnyk, Yuyi Wang, Roger Wattenhofer
Wishlist for Christmas

1.
2.
3.
Help from Elfs
Synchronous Communication

One round:
- broadcast input
- receive input from neighbors
- do local computation
While the Grinch...

- lies about inputs
- pretends to have different inputs
- knows all other rankings
- knows the protocol
- is unpredictable
Synchronous Byzantine Agreement
Agreement, Termination, Validity
Agreement, Termination, Validity

t < n/3 Byzantines
King-Algorithm

- pick t+1 kings
- check validity
King-Algorithm

King round:
• adapt input
King round:
• adapt input
Rankings vs. Top Alternatives
<table>
<thead>
<tr>
<th></th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>B</td>
<td>A</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>B</td>
<td>A</td>
<td>C</td>
</tr>
<tr>
<td>3.</td>
<td>C</td>
<td>C</td>
<td>B</td>
</tr>
</tbody>
</table>

Pareto-Validity
King-Algorithm

- Pick $t+1$ kings
- Check validity

Fix A > B
Fix B > C
Fix A > B
Better: Kemeny Median
Kendall tau Distance

A B C
B A C
B C A
C B A

1 1 1

3
Kendall tau Distance

Kemeny median

A
B
C

B
A
C

B
C
A

C
B
A

1
1
1

3
<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>A</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>C</td>
<td>C</td>
<td>B</td>
<td>A</td>
</tr>
</tbody>
</table>

A B C

A

B

C
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>C</td>
</tr>
<tr>
<td>2.</td>
<td>B</td>
<td>A</td>
<td>C</td>
<td>B</td>
</tr>
<tr>
<td>3.</td>
<td>C</td>
<td>C</td>
<td>B</td>
<td>A</td>
</tr>
</tbody>
</table>

- **A**
- **B**
- **C**
Best Possible Approximation of the Kemeny-Median
Binary Rankings

\[ \begin{align*}
A & \rightarrow B \\
B & \rightarrow C \\
C & \rightarrow A \\
\end{align*} \]

\[ n/2 + n/2 - t = t \]

\[ \begin{align*}
A & \rightarrow B \\
B & \rightarrow C \\
C & \rightarrow A \\
\end{align*} \]
Binary Rankings

\[ \frac{n/2}{n/2 - t} < 3 \]
Non-Binary Rankings

Different Kemeny median, but indistinguishable after Byzantine manipulation
Algorithm for Kemeny-Median

• Broadcast own ranking
• Choose Kemeny Median locally
• Apply King algorithm with Pareto-Validity
Byzantine Preferential Voting

- Other voting rules
  - e.g. Scoring rules

- Alternative communication models
  - Asynchronous model
  - Graphs
Thank You!
Questions & Comments?

Thanks to my co-authors
Yuyi Wang, Roger Wattenhofer