MADALGO
CENTER FOR MASSIVE DATA ALGORITHMICS

Gabriel Moruz
University of Frankfurt

JOHANN WOLFGANG GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Dictionaries Resilient to Memory Faults

Soft memory errors

Nowadays memories

- High frequencies, small geometries, complex circuitry, low voltages
- These improvements come at the cost of reliability

Soft memory errors

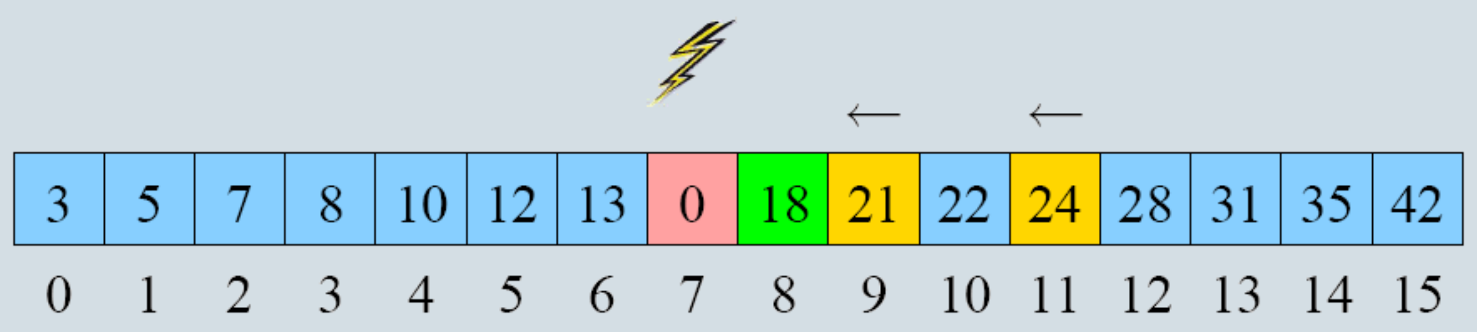
- Random bit flips, corrupting the content of the affected memory cells
- Multiple causes, e.g. power failures, alpha particles, cosmic rays

Occurrence rates

- Every few months for an usual RAM
- Becomes a serious concern when many memories are involved, e.g. large clusters
- Trends point that soft memory error rates are expected to grow

Algorithms in unreliable memory

Most algorithms assume reliable storage



									←		←				
3	5	7	8	10	12	13	0	18	21	22	24	28	31	35	42
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Figure 1. *Classical binary search in corrupted memory. The search key e=3.*

Algorithms which are unaware of memory corruptions may be seriously affected

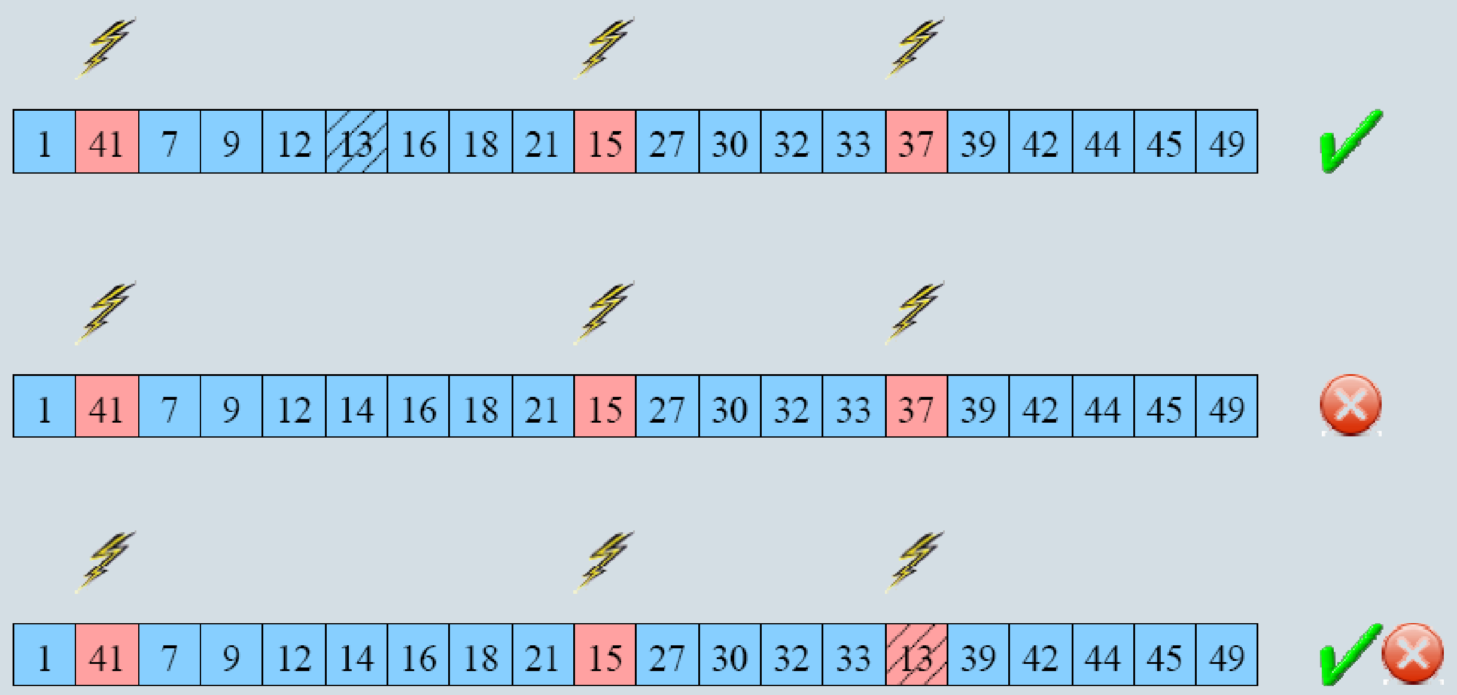
Classical binary search in a sorted array in Figure 1:

- Output is incorrect (algorithm outputs NO)
- Search path ends very far from the correct position
- A single corruption suffices

Resilient dictionaries

Searching operation returns

- **YES**, if there exists an uncorrupted value equal to the search key
- **NO**, if there are no elements, corrupted or uncorrupted, matching the search key
- **YES/NO**, if a corrupted element matches the search key.



1	41	7	9	12	13	16	18	21	15	27	30	32	33	37	39	42	44	45	49	✓
1	41	7	9	12	14	16	18	21	15	27	30	32	33	37	39	42	44	45	49	✗
1	41	7	9	12	14	16	18	21	15	27	30	32	33	13	39	42	44	45	49	✓✗

Figure 2. *Outputs of resilient dictionaries for search key e=13.*

Resilient dictionaries

- Static: $\theta(\log n+\delta)$ worst case time [1-3]
- Dynamic: $\theta(\log n+\delta)$ worst case time for searches, $\theta(\log n+\delta)$ amortized time for updates [3]

Malicious usages

Break two JVM implementations

- Increase the occurrence rate of soft memory errors by heating the RAM

Cryptography

- Cryptographic protocols provably secure become insecure

Break smart-cards

Faulty-memory RAM

- A Random Access Machine (RAM) with possibly corrupted cells
- Corruptions occur at any time and at any place
- Corrupted and uncorrupted cells cannot be distinguished
- No increase in space complexity
- At most δ corruptions possible, $O(1)$ corruption-free cells
- Resilient algorithms: work correctly on uncorrupted cells

References

[1] I. Finocchi and G. F. Italiano. *Sorting and searching in faulty memories*. In ACM STOC'04, 101–110.

[2] I. Finocchi, F. Grandoni, and G. F. Italiano. *Optimal sorting and searching in the presence of memory faults*. In ICALP'06, 286–298.

[3] G.S. Brodal, R. Fagerberg, I. Finocchi, F. Grandoni, G.F. Italiano, A. Jørgensen, G. Moruz, and T. Mølhave. *Optimal resilient dictionaries*. In ESA'07, 347-358.

MADALGO – Center for Massive Data Algorithmics, a Center of the Danish National Research Foundation