Lecture 9: Finishing consensus, scalable lock study, and oblivious algorithms

Teaching assistant: Salvatore Di Girolamo

Motivational video: https://www.youtube.com/watch?v=qx2dRIQQnbs
The simplest networking question: ping pong latency!

The latency of Piz Dora is 1.77us!
The simplest networking question: ping pong latency!

The latency of Piz Dora is 1.77us!

How did you get to this?
The latency of Piz Dora is 1.77us!

How did you get to this?

I averaged $10^6$ tests, it must be right!

The simplest networking question: ping pong latency!
The simplest networking question: ping pong latency!

The latency of Piz Dora is 1.77us!

I averaged $10^6$ tests, it must be right!

How did you get to this?

Why do you think so? Can I see the data?
The latency of Piz Dora is 1.77us!

I averaged $10^6$ tests, it must be right!

How did you get to this?

Why do you think so? Can I see the data?
The simplest networking question: ping pong latency!

Rule 5: Report if the measurement values are deterministic. For nondeterministic data, report confidence intervals of the measurement.

- CIs allow us to compute the number of required measurements!
- Can be very simple, e.g., single sentence in evaluation:
  “We collected measurements until the 99% confidence interval was within 5% of our reported means.”
Thou shalt not trust your average textbook!

The confidence interval is 1.765us to 1.775us
Thou shalt not trust your average textbook!

The confidence interval is 1.765us to 1.775us

Did you assume normality?
The confidence interval is 1.765us to 1.775us

Did you assume normality?

Yes, I used the central limit theorem to normalize by summing subsets of size 100!
Thou shalt not trust your average textbook!

The confidence interval is 1.765us to 1.775us.

Yes, I used the central limit theorem to normalize by summing subsets of size 100!

Can we test for normality?
Thou shalt not trust your average textbook!

The confidence interval is 1.765us to 1.775us.

Yes, I used the central limit theorem to normalize by summing subsets of size 100!

Can we test for normality?

Thou shalt not trust your average textbook!

The confidence interval is 1.765us to 1.775us.

Yes, I used the central limit theorem to normalize by summing subsets of size 100!

Can we test for normality?

Ugs, the data is not normal at all! The real CI is actually 1.6us to 1.9us!
Rule 6: Do not assume normality of collected data (e.g., based on the number of samples) without diagnostic checking.

- Most events will slow down performance
  - Heavy right-tailed distributions

- The Central Limit Theorem only applies asymptotically
  - Some papers/textbook mention “30-40 samples”, don’t trust them!
Thou shalt not trust your system!

Look what data I got!

Clearly, the mean/median are not sufficient!

Try quantile regression!
Thou shalt not trust your system!

Look what data I got!

Clearly, the mean/median are not sufficient!

Try quantile regression!
Thou shalt not trust your system!

Look what data I got!

Clearly, the mean/median are not sufficient!

Try quantile regression!

Mean: 1.57
Max: 7.2

Min: 1.48
Max: 11.59
Thou shalt not trust your system!

Look what data I got!

Clearly, the mean/median are not sufficient!

Try quantile regression!

Image credit: nersc.gov
Wow, so Pilatus is better for (worst-case) latency-critical workloads even though Dora is expected to be faster.
Wow, so Pilatus is better for (worst-case) latency-critical workloads even though Dora is expected to be faster.

**Rule 8:** Carefully investigate if measures of central tendency such as mean or median are useful to report. Some problems, such as worst-case latency, may require other percentiles.

Final project presentation: last Monday 12/17 during lecture

Report will be due in January!
Starting to write early is very helpful --- write – rewrite – rewrite (no joke!)

Coordinate your talk! You have 10 minutes (8 talk + 2 Q&A)
What happened since the intermediate report?
Focus on the key aspects (time is tight)!
Try to wrap up – only minor things left for final report.
Engage the audience 😊

Send slides by Sunday night (11:59pm Zurich time) to Salvatore!
We will use a single (windows) laptop to avoid delays when switching
Expect only Windows (powerpoint) or a PDF viewer
The order of talks will again be randomized for fairness
Review of last lecture(s)

- Lock implementation(s)
  - Advanced locks (CLH + MCS)

- Started impossibility of wait-free consensus with atomic registers
  - “perhaps one of the most striking impossibility results in Computer Science” (Herlihy, Shavit)
    
    \[ \text{Will continue/finish proof today as starter!} \]

- Theoretical background for performance
  - Amdahl’s law
  - Models: PRAM, Work/Depth, simple alpha-beta (Hockney) model
  - Simple algorithms: reduce, scan, mergesort,
  - Brent’s scheduling lemma + Little’s law
  - Greedy scheduling + random work stealing

- Practical performance
  - Roofline and balance modeling for practical performance optimization
  - Vectorization
Learning goals for today

- Quickly recap consensus and first part of valence proof
  - impossibility of atomic registers for wait-free consensus
  - Complete proof together

- Case study about scalable locking
  - Complete correctness section!

- Oblivious algorithms
  - How do work-depth graphs relate to practice?

- Strict optimality
  - Work/depth tradeoffs and bounds

- Applications of prefix sums
  - Parallelize seemingly sequential algorithms
DPHPC Overview

- locality
  - caches
  - memory hierarchy
- parallelism
  - vector ISA
  - shared memory
  - distributed memory

- cache coherency
- memory models
- distributed algorithms
- locks
  - lock free
  - wait free
  - linearizability
- group communications

- Amdahl's and Gustafson's law
- PRAM
- LogP

- memory
  - $\alpha - \beta$
- I/O complexity
- balance principles I
- Little's Law
- balance principles II
- scheduling
Remember: lock-free vs. wait-free

- A locked method
- A lock-free method
- A wait-free method
Remember: lock-free vs. wait-free

- A locked method
  - May deadlock (methods may never finish)

- A lock-free method

- A wait-free method
Remember: lock-free vs. wait-free

- A locked method
  - May deadlock (methods may never finish)

- A lock-free method
  - Guarantees that infinitely often some method call finishes in a finite number of steps

- A wait-free method
Remember: lock-free vs. wait-free

- A locked method
  - May deadlock (methods may never finish)

- A lock-free method
  - Guarantees that infinitely often some method call finishes in a finite number of steps

- A wait-free method
  - Guarantees that each method call finishes in a finite number of steps (implies lock-free)
Remember: lock-free vs. wait-free

- A locked method
  - May deadlock (methods may never finish)

- A lock-free method
  - Guarantees that infinitely often some method call finishes in a finite number of steps

- A wait-free method
  - Guarantees that each method call finishes in a finite number of steps (implies lock-free)

- Synchronization instructions are not equally powerful!
  - Indeed, they form an infinite hierarchy; no instruction (primitive) in level $x$ can be used for lock-/wait-free implementations of primitives in level $z>x$. 
Concept: Consensus Number

- Each level of the hierarchy has a “consensus number” assigned.
  - Is the maximum number of threads for which primitives in level x can solve the consensus problem.

- The consensus problem:
  - Has single function: decide(v)
  - Each thread calls it at most once, the function returns a value that meets two conditions:
    - **consistency**: all threads get the same value
    - **validity**: the value is some thread’s input
  - Simplification: binary consensus (inputs in {0,1})
Can a particular class solve n-thread consensus wait-free?
- A class C solves n-thread consensus if there exists a consensus protocol using any number of objects of class C and any number of atomic registers
- The protocol has to be wait-free (bounded number of steps per thread)
- The consensus number of a class C is the largest n for which that class solves n-thread consensus (may be infinite)
- Assume we have a class D whose objects can be constructed from objects out of class C. If class C has consensus number n, what does class D have?
Starting simple ...

- Binary consensus with two threads (A, B):
  - Each thread moves until it decides on a value
  - May update shared objects
  - Protocol state = state of threads + state of shared objects
  - Initial state = state before any thread moved
  - Final state = state after all threads finished
  - States form a tree, wait-free property guarantees a finite tree
    
    Example with two threads and two moves each!

- Define various states
  - Bivalent, univalent, critical

- Two helper lemmata
  - Lemma 1: the initial state is bivalent
  - Lemma 2: every wait-free consensus protocol has a critical state
Atomic Registers

- Theorem [Herlihy’91]: Atomic registers have consensus number one
  - I.e., they cannot be used to solve even two-thread consensus! Really?
Theorem [Herlihy’91]: Atomic registers have consensus number one
  - I.e., they cannot be used to solve even two-thread consensus! Really?

Proof outline:
  - Assume arbitrary consensus protocol, thread A, B
  - Run until it reaches critical state where next action determines outcome (show that it must have a critical state first)
  - Show all options using atomic registers and show that they cannot be used to determine one outcome for all possible executions!
    1) Any thread reads (other thread runs solo until end)
    2) Threads write to different registers (order doesn’t matter)
    3) Threads write to same register (solo thread can start after each write)
Atomic Registers

- Theorem [Herlihy’91]: Atomic registers have consensus number one
- Corollary: It is impossible to construct a wait-free implementation of any object with consensus number of >1 using atomic registers
  - “perhaps one of the most striking impossibility results in Computer Science” (Herlihy, Shavit)
  - We need hardware atomics or Transactional Memory!

- Proof technique borrowed from:

  Impossibility of distributed consensus with one ... - ACM Digital Library
  https://dl.acm.org/citation.cfm?id=214121
  by MJ Fischer - 1985 - Cited by 4669 - Related articles
  Sep 4, 2012 - Michael J. Fischer, Nancy A. Lynch, Michael S. Paterson, Impossibility of distributed consensus with one faulty process, Proceedings of the…

- Very influential paper, always worth a read!
  - Nicely shows proof techniques that are central to parallel and distributed computing!
Other Atomic Operations

- Simple RMW operations (Test&Set, Fetch&Op, Swap, basically all functions where the op commutes or overwrites) have consensus number 2!
  - Similar proof technique (bivalence argument)
Other Atomic Operations

- Simple RMW operations (Test&Set, Fetch&Op, Swap, basically all functions where the op commutes or overwrites) have consensus number 2!
  - Similar proof technique (bivalence argument)

- CAS and TM have consensus number $\infty$
Other Atomic Operations

- Simple RMW operations (Test&Set, Fetch&Op, Swap, basically all functions where the op commutes or overwrites) have consensus number 2!
  - Similar proof technique (bivalence argument)

- **CAS and TM have consensus number ∞**
  - Constructive proof:
    ```
    const int first = -1
    volatile int thread = -1;
    int proposed[n];

    int decide(v) {
        proposed[tid] = v;
        if(CAS(thread, first, tid))
            return v; // I won!
        else
            return proposed[thread]; // thread won
    }
    ```
Other Atomic Operations

- Simple RMW operations (Test&Set, Fetch&Op, Swap, basically all functions where the op commutes or overwrites) have consensus number 2!
  - Similar proof technique (bivalence argument)

- CAS and TM have consensus number ∞
  - Constructive proof:
    ```cpp
    const int first = -1
    volatile int thread = -1;
    int proposed[n];

    int decide(v) {
      proposed[tid] = v;
      if(CAS(thread, first, tid))
        return v; // I won!
      else
        return proposed[thread]; // thread won
    }
    ```

- Machines providing CAS are asynchronous computation equivalents of the Turing Machine i.e., any concurrent object can be implemented in a wait-free manner (not necessarily fast!)
At least a lot ... ;-)  
- We’ll argue more about **performance** now!

*You have all the tools for:*
- Efficient locks
- Efficient lock-based algorithms
- Reasoning about parallelism!

*What now?*
- Now you understand practice and will appreciate theory
  
  *Wasn’t that all too messy 😊?*
- Focus on (parallel) performance, techniques, and algorithms

*But let’s start with another case study about locks*
- Research (best) paper published at a top-tier conference some years ago
  
  *So you get a feeling of the field – and deepen understanding of MCS locks in practice*
Case study: Fast Large-scale Locking in Practice
Case study: Fast Large-scale Locking in Practice
Case study: Fast Large-scale Locking in Practice
Case study: Fast Large-scale Locking in Practice
Case study: Fast Large-scale Locking in Practice
Case study: Fast Large-scale Locking in Practice
Case study: Fast Large-scale Locking in Practice
Case study: Fast Large-scale Locking in Practice

Inuitive semantics
Case study: Fast Large-scale Locking in Practice

Inuitive semantics

Various performance penalties

Proc p

lock

accesses

unlock

Proc q

lock

accesses
Locks: Challenges
Locks: Challenges
Locks: Challenges

Calciu et al.: NUMA-aware reader-writer locks, PPoPP’13
Locks: Challenges

Calciu et al.: NUMA-aware reader-writer locks, PPoPP’13
Locks: Challenges

Calciu et al.: NUMA-aware reader-writer locks, PPoPP’13
Locks: Challenges

Calciu et al.: NUMA-aware reader-writer locks, PPoPP’13
Locks: Challenges
Locks: Challenges
Locks: Challenges

- We need intra- and inter-node topology-awareness
- We need to cover arbitrary topologies
Locks: Challenges
Locks: Challenges
Locks: Challenges

Locks: Challenges

Locks: Challenges

We need to distinguish between readers and writers

We need to distinguish between readers and writers

We need flexible performance for both types of processes

What will we use in the design?
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 1 - MCS Locks

Mellor-Crummey and Scott: Algorithms for Scalable Synchronization on Shared-Memory Multiprocessors, ACM TOCS'91
Ingredient 2 - Reader-Writer Locks
Ingredient 2 - Reader-Writer Locks
Ingredient 2 - Reader-Writer Locks
How to manage the design complexity?
How to manage the design complexity?

What mechanism to use for efficient implementation?
How to manage the design complexity?

How to ensure tunable performance?

What mechanism to use for efficient implementation?
How to manage the design complexity?

How to ensure tunable performance?

What mechanism to use for efficient implementation?
REMOTE MEMORY ACCESS (RMA) PROGRAMMING
REMOTE MEMORY ACCESS (RMA) PROGRAMMING

Process p

Memory A

REMOTE MEMORY ACCESS (RMA) PROGRAMMING

Process p
  Memory
    A

Process q
  Memory
    B

REMOTE MEMORY ACCESS (RMA) PROGRAMMING

Process p
Memory A

Process q
Memory B

Cray BlueWaters

REMOTE MEMORY ACCESS (RMA) PROGRAMMING

Process p

Memory
A

Process q

Memory
B

Cray
BlueWaters

REMOTE MEMORY ACCESS (RMA) PROGRAMMING

REMOTE MEMORY ACCESS (RMA) PROGRAMMING

Process p

Memory

A

Process q

Memory

B

Cray BlueWaters

REMOTE MEMORY ACCESS (RMA) PROGRAMMING

Process p

Memory

Process q

Memory

A put

A

B

Cray
BlueWaters

**REMOTE MEMORY ACCESS (RMA) PROGRAMMING**

Process $p$ (Memory)

- A put

- get B

Process $q$ (Memory)

- A

- B

Cray BlueWaters

REMOTE MEMORY ACCESS (RMA) PROGRAMMING

Process p
Memory
A
B

Process q
Memory
A
B

A put
get B
B flush

Cray
BlueWaters

REMOTE MEMORY ACCESS (RMA) PROGRAMMING

REMOTE MEMORY ACCESS PROGRAMMING

- Implemented in hardware in NICs in the majority of HPC networks (RDMA support).
REMOTE MEMORY ACCESS PROGRAMMING

- Implemented in hardware in NICs in the majority of HPC networks (RDMA support).
REMOTE MEMORY ACCESS PROGRAMMING

- Implemented in hardware in NICs in the majority of HPC networks (RDMA support).
REMOTE MEMORY ACCESS PROGRAMMING

- Implemented in hardware in NICs in the majority of HPC networks (RDMA support).
REMOTE MEMORY ACCESS PROGRAMMING

- Implemented in hardware in NICs in the majority of HPC networks (RDMA support).
RMA-RW - Required Operations

Process p
Memory

Process q
Memory

3
3
3
3
3
3
RMA-RW - Required Operations

Process p
Memory

Process q
Memory

6 put
RMA-RW - Required Operations

Process p

Memory

6 put

Process q

Memory

6

3

3

3
RMA-RW - Required Operations

Process p

Memory

6 put

get

Memory

6

3

3

3

Process q
RMA-RW - Required Operations

Process p

Memory

3

6 put

get

3

Process q

Memory

6

3

3

3

3
RMA-RW - Required Operations

Process p

Memory

Process q

Memory

3

6 put

3

get

6

Fetch-and-Add (FAA)

3

3

3

3

3

3

3
RMA-RW - Required Operations

- Process p
  - Memory
  - 3
  - 6 put
  - 6 Fetch-and-Add (FAA)
  - 3

- Process q
  - Memory
  - 3
  - 6 get
  - 6
  - 3
  - 3
RMA-RW - Required Operations

```
Process p

Memory

3
3

6 put

3
3

Fetch-and-Add (FAA)

6

Process q

Memory

6
3
9
3
3
3
```
RMA-RW - Required Operations

Process p

Memory

6 put

3

get

3

Fetch-and-Add (FAA)

6

replace

3

Process q

Memory

6

3

9

3

3
RMA-RW - Required Operations

Process p

Memory

Process q

Memory

6 put

get

3

9

6 Fetch-and-Add (FAA)

replace

6

6

223x274 Fetch-and-Add (FAA)
RMA-RW - Required Operations

Process p

Memory

Process q

Memory

put 6
get
0
Fetch-and-Add (FAA) 6
replace 6
Compare-and-Swap (CAS) 3 8

Required Operations
RMA-RW - Required Operations

**Process p**
- Memory
- **6** put
- **3**
- **6** Fetch-and-Add (FAA)
- **3**
- **6** replace
- **3**
- **3** Compare-and-Swap (CAS)

**Process q**
- Memory
- **6**
- **3**
- **6**
- **9**
- **6**
- **8**
RMA-RW - Required Operations

**Process p**

- Memory
- 3
- 6 put
- 3
- 6 Fetch-and-Add (FAA)
- 3
- 6 replace
- 3
- 8 Compare-and-Swap (CAS)
- 1

**Process q**

- Memory
- 6
- 3
- 6 Fetch-and-Add (FAA)
- 9
- 6 replace
- 6
- 8 Compare-and-Swap (CAS)
MPI RMA primer ([much] more in the recitation sessions)

- **Windows expose memory**
  - Created explicitly

- **Remote accesses**
  - Put, get
  - Atomics
    - Accumulate (also atomic Put)
    - Get_accumulate (also atomic Get)
    - Fetch and op (faster single-word get_accumulate)
    - Compare and swap

- **Synchronization**
  - Two modes: passive and active target
    - *We use passive target today, similar to shared memory!*
    - Synchronization: flush, flush_local

- **Memory model**
  - Unified (coherent) and separate (not coherent) view - it’s complicated but versatile
MPI RMA primer ([much] more in the recitation sessions)

- **Windows expose memory**
  - Created explicitly

- **Remote accesses**
  - Put, get
  - Atomics
    - Accumulate (also atomic Put)
    - Get_accumulate (also atomic Get)
    - Fetch and op (faster single-word get_accumulate)
    - Compare and swap

- **Synchronization**
  - Two modes: passive and active target
    - *We use passive target today, similar to shared memory!*
    - *Synchronization: flush, flush_local*

- **Memory model**
  - Unified (coherent) and separate (not coherent) view - it’s complicated but versatile
MPI RMA primer ([much] more in the recitation sessions)

- **Windows expose memory**
  - Created explicitly

- **Remote accesses**
  - Put, get
  - Atomics
    - Accumulate (also atomic Put)
    - Get_accumulate (also atomic Get)
    - Fetch and op (faster single-word get_accumulate)
    - Compare and swap

- **Synchronization**
  - Two modes: passive and active target
    - *We use passive target today, similar to shared memory!*
    - Synchronization: flush, flush_local

- **Memory model**
  - Unified (coherent) and separate (not coherent) view - it’s complicated but versatile
### MPI RMA primer ([much] more in the recitation sessions)

- **Windows expose memory**
  - Created explicitly

- **Remote accesses**
  - Put, get
  - Atomics
    - Accumulate (also atomic Put)
    - Get_accumulate (also atomic Get)
    - Fetch and op (faster single-word get_accumulate)
    - Compare and swap

- **Synchronization**
  - Two modes: passive and active target
    - *We use passive target today, similar to shared memory!*
    - *Synchronization: flush, flush_local*

- **Memory model**
  - Unified (coherent) and separate (not coherent) view - it’s complicated but versatile
MPI RMA primer ([much] more in the recitation sessions)

- **Windows expose memory**
  - Created explicitly

- **Remote accesses**
  - Put, get
  - Atomics
    - Accumulate (also atomic Put)
    - Get_accumulate (also atomic Get)
    - Fetch and op (faster single-word get_accumulate)
    - Compare and swap

- **Synchronization**
  - Two modes: passive and active target
    - We use passive target today, similar to shared memory!
    - Synchronization: flush, flush_local

- **Memory model**
  - Unified (coherent) and separate (not coherent) view - it’s complicated but versatile
How to manage the design complexity?

How to ensure tunable performance?

What mechanism to use for efficient implementation?
How to manage the design complexity?

How to ensure tunable performance?

What mechanism to use for efficient implementation?
How to manage the design complexity?

How to ensure tunable performance?

What mechanism to use for efficient implementation?
How to manage the design complexity?

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to manage the design complexity?

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to manage the design complexity?

Modular design

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to manage the design complexity?

Modular design

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to manage the design complexity?

Modular design

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Each element has its own distributed MCS queue (DQ) of writers.

How to manage the design complexity?

Modular design

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to manage the design complexity?

Each element has its own distributed MCS queue (DQ) of writers.

Modular design

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Each element has its own distributed MCS queue (DQ) of writers.

How to manage the design complexity?

Modular design

R2 R1 W1
R3 R4 W2 W3
R5 R6 W4 W5
R7
R8 R9 W6 W7 W8
How to manage the design complexity?

Each element has its own distributed MCS queue (DQ) of writers.

Modular design

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to manage the design complexity?

Each element has its own distributed MCS queue (DQ) of writers

Modular design

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC'16, best paper
How to manage the design complexity?

Each element has its own distributed MCS queue (DQ) of writers.

MCS queues form a distributed tree (DT).

Modular design.

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Each element has its own distributed MCS queue (DQ) of writers.

How to manage the design complexity?

Modular design

MCS queues form a distributed tree (DT)

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to manage the design complexity?

Each element has its own distributed MCS queue (DQ) of writers.

Readers and writers synchronize with a distributed counter (DC).

MCS queues form a distributed tree (DT).

Modular design.
How to manage the design complexity?

- Each element has its own distributed MCS queue (DQ) of writers
- Readers and writers synchronize with a distributed counter (DC)
- MCS queues form a distributed tree (DT)

Modular design

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to ensure tunable performance?

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to ensure tunable performance?

A tradeoff parameter for every structure

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to ensure tunable performance?

Each DQ: fairness vs throughput of writers

A tradeoff parameter for every structure

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to ensure tunable performance?

Each DQ: fairness vs throughput of writers

A tradeoff parameter for every structure

DT: a parameter for the throughput of readers vs writers

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
How to ensure tunable performance?

Each DQ: fairness vs throughput of writers

DC: a parameter for the latency of readers vs writers

DT: a parameter for the throughput of readers vs writers

A tradeoff parameter for every structure

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed MCS Queues (DQs) - Throughput vs Fairness

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed MCS Queues (DQs) - Throughput vs Fairness

Each DQ: The maximum number of lock passings within a DQ at level i, before it is passed to another $T_{L,i}$ DQ at i.

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Each DQ: The maximum number of lock passings within a DQ at level i, before it is passed to another $T_{L,i}$ DQ at i.
Distributed MCS Queues (DQs) - Throughput vs Fairness

Each DQ: The maximum number of lock passings within a DQ at level i, before it is passed to another $T_{L,i}$ DQ at i.

$T_{L,1}$, $T_{L,2}$

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed MCS Queues (DQs) - Throughput vs Fairness

Each DQ: The maximum number of lock passings within a DQ at level i, before it is passed to another $T_{L,i}$ DQ at i.

$T_{L,3}$

$T_{L,2}$

$T_{L,1}$

$T_{L,1}$

$T_{L,1}$

$T_{L,1}$

$T_{L,1}$

$T_{L,1}$

$T_{L,1}$

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed MCS Queues (DQs) - Throughput vs Fairness

Each DQ: The maximum number of lock passings within a DQ at level $i$, before it is passed to another $T_{L,i}$ DQ at $i$.

Larger $T_{L,i}$: more throughput at level $i$. Smaller $T_{L,i}$: more fairness at level $i$. 

$T_{L,1}$, $T_{L,2}$, $T_{L,3}$

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC'16, best paper
Distributed Tree of Queues (DT) - Throughput of readers vs writers

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed Tree of Queues (DT) - Throughput of readers vs writers

DT: The maximum number of consecutive lock passings within readers ($T_R$).

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed Tree of Queues (DT) - Throughput of readers vs writers

DT: The maximum number of consecutive lock passings within readers ($T_R$).

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed Counter (DC) - Latency of readers vs writers
DC: every \( k \)th compute node hosts a partial counter, all of which constitute the DC.

\[ k = T_{DC} \]
Distributed Counter (DC) - Latency of readers vs writers

DC: every $k$th compute node hosts a partial counter, all of which constitute the DC.

$$k = T_{DC}$$
DC: every $k$th compute node hosts a partial counter, all of which constitute the DC.

$$k = T_{DC}$$

A writer holds the lock $b|x|y$
Distributed Counter (DC) - Latency of readers vs writers

DC: every $k$th compute node hosts a partial counter, all of which constitute the DC.

$$k = T_{DC}$$

A writer holds the lock

Readers that arrived at the CS
DC: every $k$th compute node hosts a partial counter, all of which constitute the DC.

$$k = T_{DC}$$

A writer holds the lock $b|x|y$

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
DC: every \( k \)th compute node hosts a partial counter, all of which constitute the DC.

\[ k \equiv T_{DC} \]

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed Counter (DC) - Latency of readers vs writers

$T_{DC} = 1$

DC: every $k$th compute node hosts a partial counter, all of which constitute the DC.

$k = T_{DC}$

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed Counter (DC) - Latency of readers vs writers

DC: every $k$th compute node hosts a partial counter, all of which constitute the DC.

$\bbox[white]{k = T_{DC}}$

$T_{DC} = 1$

A writer holds the lock $\bbox[white]{b|x|y}$

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper

Distributed Counter (DC) - Latency of readers vs writers

DC: every kth compute node hosts a partial counter, all of which constitute the DC.

\[ k = T_{DC} \]

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS
Distributed Counter (DC) - Latency of readers vs writers

DC: every $k$th compute node hosts a partial counter, all of which constitute the DC.

$$k = T_{DC}$$

A writer holds the lock $b|x|y$

Readers that arrived at the CS

Readers that left the CS

$T_{DC} = 2$

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Distributed Counter (DC) - Latency of readers vs writers

DC: every $k$th compute node hosts a partial counter, all of which constitute the DC.

$k = T_{DC}$

A writer holds the lock $b|x|y$

Readers that arrived at the CS

Readers that left the CS

$T_{DC} = 2$
Design space
Design space

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Design space

\( T_R \)
Design space

Higher throughput of writers vs readers

$T_R$
Design space

Higher throughput of **writers** vs **readers**

\[ T_{DC}, T_R \]
Design space

Higher throughput of writers vs readers

Lower latency of writers vs readers

$T_{DC}$

$T_R$
Design space

Higher throughput of \textit{writers} vs \textit{readers}

Lower latency of \textit{writers} vs \textit{readers}
Design space

Higher throughput of **writers** vs **readers**

Lower latency of **writers** vs **readers**

Locality vs fairness (for writers)
Higher throughput of writers vs readers

Locality vs fairness (for writers)

Lower latency of writers vs readers

Design space

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Design space

Design A
Design B

Higher throughput of writers vs readers

Lower latency of writers vs readers

Locality vs fairness (for writers)

$T_{DC}$
$T_L,i$
$T_R$
Lock Acquire by Readers

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation.

A writer holds the lock $b|x|y$

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock
Readers that arrived at the CS
Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation.

A writer holds the lock.

Readers that arrived at the CS.

Readers that left the CS.
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock

Readers that arrived at the CS

Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Readers

A lightweight acquire protocol for readers: only one atomic fetch-and-add (FAA) operation

A writer holds the lock
Readers that arrived at the CS
Readers that left the CS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire MCS

0|9|9

W9 → W1

0|3|3

W2 → W3

0|8|8

W4 → W5

0|5|5

W6 → W7 → W8

W1 → W3

W5 → W8

W3 → W8

R1 ... R9

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire MCS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire MCS

R1 ... R9

W9 → W1 → W3

0|9|9

W9 → W1
0|9|9

W2 → W3
0|3|3

W4 → W5
0|8|8

W6 → W7 → W8
0|5|5

Acquire MCS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire MCS

Acquire MCS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire the main MCS lock

Acquire MCS

Acquire MCS

0|9|9
W9 → W1

0|3|3
W2 → W3

0|8|8
W4 → W5

0|5|5
W6 → W7

W9 → W3 → W8

0|9|9

W9

W1

W3

W5

W8

W2

W4

W5

W6

W7

W8

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire the main MCS lock

Acquire MCS

Acquire MCS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC'16, best paper
Acquire the main MCS lock

Acquire MCS

Acquire MCS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire the main MCS lock

Acquire MCS

Acquire MCS

Acquire MCS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire the main MCS lock

Acquire MCS

Acquire MCS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Lock Acquire by Writers

Acquire the main lock

Acquire the main MCS lock

Acquire MCS

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
EVALUATION

- CSCS Piz Daint (Cray XC30)
- 5272 compute nodes
- 8 cores per node
- 169TB memory
- Microbenchmarks: acquire/release: latency, throughput
- Distributed hashtable
Evaluation - Distributed Counter Analysis

Throughput, 2% writers
Single-operation benchmark

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Evaluation - Reader Threshold Analysis

Throughput, 0.2% writers,
Empty-critical-section benchmark

Throughput [mln locks/s]

\( T_R \)
- 6000
- 5000
- 4000
- 3000
- 2000
- 1000

MPI processes (P)

P. Schmid, M. Besta, TH: High-Performance Distributed RMA Locks, ACM HPDC’16, best paper
Evaluation - Comparison to the State-of-the-Art

Percentages are values of $F_W$

Evaluation - Comparison to the State-of-the-Art

Throughput, single-operation benchmark

Evaluation - Distributed Hashtable

20% writers

10% writers

Evaluation - Distributed Hashtable

2% of writers

0% of writers

Another application area - Databases

- MPI-RMA for distributed databases?

C. Barthels, et al., TH: Distributed Join Algorithms on Thousands of Cores presented in Munich, Germany, VLDB Endowment, Aug. 2017
Another application area - Databases

- MPI-RMA for distributed databases on Piz Daint

C. Barthels, et al., TH: Distributed Join Algorithms on Thousands of Cores presented in Munich, Germany, VLDB Endowment, Aug. 2017
Another application area - Databases

- MPI-RMA for distributed databases on Piz Daint
Now on to parallel algorithms!

- Oblivious parallel algorithms
  - Fixed structure work-depth graphs

- Nonoblivious parallel algorithms
  - Data-dependent structure work-depth graphs

- Data movement and I/O complexity
  - Communication complexity
Work/Depth in Practice – Oblivious Algorithms

“An algorithm is execution-oblivious if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs”
Work/Depth in Practice – Oblivious Algorithms

“An algorithm is **execution-oblivious** if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs”

Execution oblivious or not?
"An algorithm is execution-oblivious if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs."

Execution oblivious or not?

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}
```
An algorithm is execution-oblivious if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs.

Execution oblivious or not?

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}
```

```c
int findmin(int n, a[n]) {
    for(int i=1; i<n; i++)
        if(a[i]<a[0]) a[0] = a[i];
}
```
An algorithm is *execution-oblivious* if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs.

Execution oblivious or not?

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}

int findmin(int n, a[n]) {
    for(int i=1; i<n; i++)
        if(a[i]<a[0]) a[0] = a[i];
}

int finditem(list_t list) {
    item = list.head;
    while(item.value!=0 && item.next!=NULL)
        item = item.next;
}
```
Work/Depth in Practice – Oblivious Algorithms

“An algorithm is **execution-oblivious** if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs”

Execution oblivious or not?

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}

int findmin(int n, a[n]) {
    for(int i=1; i<n; i++)
        if(a[i]<a[0]) a[0] = a[i];
}

int finditem(list_t list)
    item = list.head;
    while(item.value!=0 && item.next!=NULL)
        item = item.next;
}
```

- Quicksort?
Work/Depth in Practice – Oblivious Algorithms

“An algorithm is execution-oblivious if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs”

Execution oblivious or not?

- Quicksort?
- Prefix sum on an array?

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}

int findmin(int n, a[n]) {
    for(int i=1; i<n; i++)
        if(a[i]<a[0]) a[0] = a[i];
}

int finditem(list_t list)
    item = list.head;
    while(item.value!=0 && item.next!=NULL)
        item = item.next;
```
Work/Depth in Practice – Oblivious Algorithms

“An algorithm is **execution-oblivious** if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs”

Execution oblivious or not?

- Quicksort?
- Prefix sum on an array?
- Simple dense matrix multiplication?

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}

int findmin(int n, a[n]) {
    for(int i=1; i<n; i++)
        if(a[i]<a[0]) a[0] = a[i];
}

int finditem(list_t list)
    item = list.head;
    while(item.value!=0 && item.next!=NULL)
        item = item.next;
```
An algorithm is execution-oblivious if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs.

Execution oblivious or not?

- Quicksort?
- Prefix sum on an array?
- Simple dense matrix multiplication?
- Dense matrix vector product?
Work/Depth in Practice – Oblivious Algorithms

“An algorithm is **execution-oblivious** if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs”

**Execution oblivious or not?**

- Quicksort?
- Prefix sum on an array?
- Simple dense matrix multiplication?
- Dense matrix vector product?
- Sparse matrix vector product?

```c
int reduce(int n, int arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}

int findmin(int n, int arr[n]) {
    for(int i=1; i<n; i++)
        if(arr[i]<arr[0]) arr[0] = arr[i];
}
```

```c
int finditem(list_t list) {
    item = list.head;
    while(item.value!=0 && item.next!=NULL) {
        item = item.next;
    }
}
```
Work/Depth in Practice – Oblivious Algorithms

“An algorithm is execution-oblivious if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs”

Execution oblivious or not?

```
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}
```

```
int findmin(int n, a[n]) {
    for(int i=1; i<n; i++)
        if(a[i]<a[0]) a[0] = a[i];
}
```

```
int finditem(list_t list)
    item = list.head;
    while(item.value!=0 && item.next!=NULL)
        item = item.next;
```

- Quicksort?
- Prefix sum on an array?
- Simple dense matrix multiplication?
- Dense matrix vector product?
- Sparse matrix vector product?
- Queue-based breadth-first search?
Obliviousness as property of an execution

“An algorithm is execution-oblivious if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs”

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}

int findmin(int n, a[n]) {
    for(int i=1; i<n; i++)
        if(a[i]<a[0]) a[0] = a[i];
}

int finditem(list_t list)
    item = list.head;
    while(item.value!=0 && item.next!=NULL)
        item=item.next;
}```

- Class question: Can an algorithm decide whether a program is oblivious or not?
Obliviousness as property of an execution

“An algorithm is **execution-oblivious if, for each problem size, the sequence of instructions executed, the set of memory locations read and the set of memory locations written by each executed instruction are determined by the input size and are independent of the values of the other inputs**”

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}
```

```c
int findmin(int n, a[n]) {
    for(int i=1; i<n; i++)
        if(a[i]<a[0]) a[0] = a[i];
}
```

```c
int finditem(list_t list)
    item = list.head;
    while(item.value!=0 && item.next!=NULL)
        item=item.next;
}
```

- **Class question:** Can an algorithm decide whether a program is oblivious or not?
  - **Answer:** no, proof similar to decision problem whether a program always outputs zero or not
“A program is **structurally-oblivious** if any value used in a conditional branch, and any value used to compute indices or pointers is structurally-dependent only in the input variable(s) that contains the problem size but not on any other input”
Structural obliviousness as stronger property

“A program is structurally-oblivious if any value used in a conditional branch, and any value used to compute indices or pointers is structurally-dependent only in the input variable(s) that contains the problem size but not on any other input”

Structurally oblivious or not?
Structural obliviousness as stronger property

“A program is **structurally-oblivious** if any value used in a conditional branch, and any value used to compute indices or pointers is structurally-dependent only in the input variable(s) that contains the problem size but not on any other input”

Structurally oblivious or not?

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}
```
“A program is **structurally-oblivious** if any value used in a conditional branch, and any value used to compute indices or pointers is structurally-dependent only in the input variable(s) that contains the problem size but not on any other input.”

**Structurally oblivious or not?**

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}
```

```c
int oblivious(int n, a[n], b[n]) {
    for(int i=0; i<n; ++i) {
        x = a[i] + 1;
        if (x > a[i]) b[i] = 1;
        else b[i] = 2;
    }
}
```
A program is **structurally-oblivious** if any value used in a conditional branch, and any value used to compute indices or pointers is structurally-dependent only in the input variable(s) that contains the problem size but not on any other input.

```c
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}
```

```c
int oblivious(int n, a[n], b[n]) {
    for(int i=0; i<n; ++i) {
        x = a[i] + 1;
        if (x > a[i]) b[i] = 1;
        else b[i] = 2;
    }
}
```

```c
int finditem(list_t list)
    item = list.head;
    while(item.value!=0 && item.next!=NULL) {
        item = item.next;
    }
```
Structural obliviousness as stronger property

“A program is structurally-oblivious if any value used in a conditional branch, and any value used to compute indices or pointers is structurally-dependent only in the input variable(s) that contains the problem size but not on any other input”

Structurally oblivious or not?

```
int reduce(int n, arr[n]) {
    for(int i=0; i<n; ++i)
        sum += arr[i];
}

int oblivious(int n, a[n], b[n]) {
    for(int i=0; i<n; ++i) {
        x = a[i] + 1;
        if (x > a[i]) b[i] = 1;
        else b[i] = 2;
    }
}

int finditem(list_t list) {
    item = list.head;
    while(item.value!=0 && item.next!=NULL) {
        item = item.next;
    }
}
```

- Clear that structurally oblivious programs are also execution oblivious
  - Can be programmatically (statically decided)
  - Sufficient for practical use
Structural obliviousness as stronger property

“A program is structurally-oblivious if any value used in a conditional branch, and any value used to compute indices or pointers is structurally-dependent only in the input variable(s) that contains the problem size but not on any other input”

Structurally oblivious or not?

- Clear that structurally oblivious programs are also execution oblivious
  - Can be programmatically (statically decided)
  - Sufficient for practical use
- The middle example is not structurally oblivious but execution oblivious
  - First branch is always taken (assuming no overflow) but static dependency analysis is conservative
Why obliviousness?

We can easily reason about oblivious algorithms

- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

\[ \log_2 n \]

Are both $W$ and $D$ optimal?

Yes!
Why obliviousness?

We can easily reason about oblivious algorithms

- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

- Simple example (that you know): parallel summation

\[ \log_2 n \]

Are both W and D optimal?

Yes!
Why obliviousness?

We can easily reason about oblivious algorithms
- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

- Simple example (that you know): parallel summation
  - Question: what is \( W(n) \) and \( D(n) \) of sequential summation?

\[
\log_2 n
\]

Are both \( W \) and \( D \) optimal?
Yes!
Why obliviousness?

We can easily reason about oblivious algorithms
- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

- Simple example (that you know): parallel summation
  - Question: what is $W(n)$ and $D(n)$ of sequential summation?
    - $W(n)=D(n)=n-1$

\[
\log_2 n \\
Are both $W$ and $D$ optimal? \\
Yes!
\]
Why obliviousness?

We can easily reason about oblivious algorithms

- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

- Simple example (that you know): parallel summation
  - Question: what is W(n) and D(n) of sequential summation?
    \[ W(n) = D(n) = n - 1 \]
  - Question: is this optimal? How would you define optimality?

\[ \log_2 n \]

Are both W and D optimal?
Yes!
Why obliviousness?

We can easily reason about oblivious algorithms
- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

- Simple example (that you know): parallel summation
  - Question: what is W(n) and D(n) of sequential summation?
    \[ W(n) = D(n) = n - 1 \]
  - Question: is this optimal? How would you define optimality?
    Separate for W and D! Typically try to achieve both!

\[ \log_2 n \]

Are both W and D optimal?
Yes!
Why obliviousness?

- **We can easily reason about oblivious algorithms**
  - Execution DAG can be constructed “statically”
  - We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

- **Simple example (that you know): parallel summation**
  - Question: what is $W(n)$ and $D(n)$ of sequential summation?
    \[ W(n) = D(n) = n - 1 \]
  - Question: is this optimal? How would you define optimality?
    *Separate for $W$ and $D$! Typically try to achieve both!*
  - Question: what is $W(n)$ and $D(n)$ of the optimal parallel summation?
    \[ \log_2 n \]
    *Are both $W$ and $D$ optimal?*
    *Yes!*
Why obliviousness?

\[ \log_2 n \] \log_2 \log_2 2 \log_2 n \]

We can easily reason about oblivious algorithms

- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

Simple example (that you know): parallel summation

- Question: what is W(n) and D(n) of sequential summation?
  \[ W(n)=D(n)=n-1 \]

- Question: is this optimal? How would you define optimality?
  Separate for W and D! Typically try to achieve both!

- Question: what is W(n) and D(n) of the optimal parallel summation?
  \[ W(n)=n-1 \quad D(n)=\lceil \log_2 n \rceil \]
  Are both W and D optimal?
  Yes!
We can easily reason about oblivious algorithms

- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

Simple example (that you know): parallel summation

- Question: what is W(n) and D(n) of sequential summation?
  \[ W(n) = D(n) = n - 1 \]

  Question: is this optimal? How would you define optimality?
  *Separate for W and D! Typically try to achieve both!*

- Question: what is W(n) and D(n) of the optimal parallel summation?
  
  *Are both W and D optimal?*
  
  *Yes!*

\[
\log_2 n \]
\[
\log_2 \log_2 n \]
\[
\log_2 \log_2 \log_2 n \]
\[
\log_2 n \]
\[
\log_2 n \]
\[
\log_2 n \]
Why obliviousness?

\[
\log_2 n \mid \log_2 \log_2 2 \log_2 2 \log_2 n \mid \log_2 n
\]

*We can easily reason about oblivious algorithms*

- Execution DAG can be constructed “statically”
- We have done this in the last weeks intuitively but you never asked how to do it for BFS for example 😊

### Simple example (that you know): parallel summation

- Question: what is \( W(n) \) and \( D(n) \) of sequential summation?
  \[ W(n) = D(n) = n - 1 \]

  Question: is this optimal? How would you define optimality?
  *Separate for \( W \) and \( D \)! Typically try to achieve both!*

- Question: what is \( W(n) \) and \( D(n) \) of the optimal parallel summation?
  *Are both \( W \) and \( D \) optimal?*
    - Yes!
    - Yes!
Starting simple: optimality?

- Next example you know: scan!
  - For a vector \([x_1, x_2, ..., x_n]\) compute vector of n results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
  - Simple serial schedule
Next example you know: scan!

- For a vector \([x_1, x_2, ..., x_n]\) compute vector of \(n\) results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
- Simple serial schedule

\[
\begin{array}{cccccccc}
  x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\
\end{array}
\]
Starting simple: optimality?

- Next example you know: scan!
  - For a vector $[x_1, x_2, \ldots, x_n]$ compute vector of $n$ results: $[x_1; x_1 + x_2; x_1 + x_2 + x_3; \ldots; x_1 + x_2 + x_i \ldots + x_{n-1} + x_n]$
  - Simple serial schedule
Starting simple: optimality?

- **Next example you know: scan!**
  - For a vector \([x_1, x_2, ..., x_n]\) compute vector of n results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
  - Simple serial schedule

![Diagram](image.png)
Starting simple: optimality?

- Next example you know: scan!
  - For a vector $[x_1, x_2, \ldots, x_n]$ compute vector of n results: $[x_1; x_1 + x_2; x_1 + x_2 + x_3; \ldots; x_1 + x_2 + x_i \ldots + x_{n-1} + x_n]$
  - Simple serial schedule
Starting simple: optimality?

- **Next example you know: scan!**
  - For a vector \([x_1, x_2, ..., x_n]\) compute vector of n results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
  - Simple serial schedule

![Diagram of vector addition process]

\begin{align*}
  x_1 & \rightarrow x_2 \rightarrow x_3 \rightarrow x_4 \rightarrow x_5 \rightarrow x_6 \rightarrow x_7 \rightarrow x_8 \\
  x_1 & \rightarrow \sum \rightarrow \sum \rightarrow \sum \\
  x_1 & \rightarrow x_1 + x_2 \rightarrow x_1 + \cdots + x_4 \\
  x_1 & \rightarrow \sum \\
  x_1 & \rightarrow x_1 + \cdots + x_3
\end{align*}
Starting simple: optimality?

- Next example you know: scan!
  - For a vector \([x_1, x_2, ..., x_n]\) compute vector of \(n\) results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
  - Simple serial schedule

```
\begin{array}{cccccccc}
  x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\
  \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
  x_1 & x_1 + x_2 & x_1 + \cdots + x_4 & x_1 + \cdots + x_5 \\
\end{array}
```
Next example you know: scan!

- For a vector \([x_1, x_2, \ldots, x_n]\) compute vector of n results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; \ldots; x_1 + x_2 + x_i \ldots + x_{n-1} + x_n]\)
- Simple serial schedule
Starting simple: optimality?

- Next example you know: scan!
  - For a vector \([x_1, x_2, ..., x_n]\) compute vector of \(n\) results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
  - Simple serial schedule
Starting simple: optimality?

- Next example you know: scan!
  - For a vector $[x_1, x_2, \ldots, x_n]$ compute vector of $n$ results: $[x_1; x_1 + x_2; x_1 + x_2 + x_3; \ldots; x_1 + x_2 + x_i \ldots + x_{n-1} + x_n]$
  - Simple serial schedule

\[
\begin{array}{cccccccc}
  x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\
  \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
  x_1 & x_1 + x_2 & x_1 + \cdots + x_4 & x_1 + \cdots + x_6 & x_1 + \cdots + x_8 \\
  \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
  x_1 + \cdots + x_3 & x_1 + \cdots + x_4 & x_1 + \cdots + x_5 & x_1 + \cdots + x_7 \\
\end{array}
\]
Starting simple: optimality?

- Next example you know: scan!
  - For a vector \([x_1, x_2, ..., x_n]\) compute vector of n results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
  - Simple serial schedule

Class question: work and depth?
Starting simple: optimality?

- Next example you know: scan!
  - For a vector \([x_1, x_2, ..., x_n]\) compute vector of n results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
  - Simple serial schedule

\[W(n) = n-1, \quad D(n) = n-1\]
Starting simple: optimality?

- **Next example you know: scan!**
  - For a vector \([x_1, x_2, ..., x_n]\) compute vector of \(n\) results: \([x_1; x_1 + x_2; x_1 + x_2 + x_3; ...; x_1 + x_2 + x_i ... + x_{n-1} + x_n]\)
  - Simple serial schedule

Class question: work and depth?

\[W(n) = n-1, \quad D(n) = n-1\]

Class question: is this optimal?
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm
What did we learn earlier?

- Recursive to get to \( W = O(n) \) and \( D = O(\log n) \)! Assume \( n = 2^k \) for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm

```
\begin{align*}
\sum & 1 \quad \sum 3 \\
\sum & 2 \quad \sum 4
\end{align*}
```

```
\begin{align*}
\sum & 5 \quad \sum 7 \\
\sum & 6 \quad \sum 8
\end{align*}
```

```
\begin{align*}
\sum & 1 \\
\sum & 2
\end{align*}
```

```
\begin{align*}
\sum & 4 \\
\sum & 6 \quad \sum 8
\end{align*}
```
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm

\[
\begin{align*}
\sum_1^8 & \sum_1^4 \sum_1^2 \sum_1^1 x_1 \\
\sum_1^8 & \sum_3^4 \sum_3^2 \sum_3^1 x_2 \\
\sum_1^8 & \sum_5^6 \sum_5^3 \sum_5^1 x_3 \\
\sum_1^8 & \sum_7^8 \sum_7^5 \sum_7^1 x_4 \\
\sum_1^8 & \sum_5^6 \sum_5^3 \sum_5^1 x_5 \\
\sum_1^8 & \sum_7^8 \sum_7^5 \sum_7^1 x_6 \\
\sum_1^8 & \sum_7^8 \sum_7^5 \sum_7^1 x_7 \\
\sum_1^8 & \sum_7^8 \sum_7^5 \sum_7^1 x_8
\end{align*}
\]
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm

```
\[ \begin{align*}
&x_1 \quad x_2 \quad x_3 \quad x_4 \\
&x_5 \quad x_6 \quad x_7 \quad x_8 \\
\end{align*} \]
```

```
\[ \begin{align*}
\sum_1 & 1 \quad \sum_3 & 4 \\
\sum_1 & 1 \quad \sum_3 & 4 \\
\sum_1 & 3 \quad \sum_1 & 5 \\
\sum_1 & 5 \quad \sum_1 & 6 \\
\end{align*} \]
```

```
\[ \begin{align*}
\sum_1 & 1 \\
\sum_1 & 3 \\
\sum_1 & 5 \\
\sum_1 & 6 \\
\end{align*} \]

```

```
\[ \begin{align*}
\sum_1 & 1 \\
\sum_1 & 3 \\
\sum_1 & 5 \\
\sum_1 & 6 \\
\end{align*} \]

```

```
\[ \begin{align*}
\sum_1 & 1 \\
\sum_1 & 3 \\
\sum_1 & 5 \\
\sum_1 & 6 \\
\end{align*} \]

```

What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!

- Algorithm

\[
\begin{align*}
\sum_{1}^{1} & \quad \sum_{1}^{3} \\
\sum_{1}^{2} & \quad \sum_{1}^{4} \\
\sum_{1}^{4} & \quad \sum_{1}^{8}
\end{align*}
\]
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm

Class question: work? (hint: after the way up, all powers of two are done, all others require another operation each)
What did we learn earlier?

- Recursive to get to \( W = O(n) \) and \( D = O(\log n) \)! Assume \( n = 2^k \) for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm

\[
W(n) = 2n - \log_2 n - 1
\]

Class question: work?
(hint: after the way up, all powers of two are done, all others require another operation each)
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm

\[
W(n) = 2n - \log_2 n - 1
\]

Class question: work?
(hint: after the way up, all powers of two are done, all others require another operation each)

Class question: depth?
(needs to go up and down the tree)
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm

\[ W(n) = 2n - \log_2 n - 1 \]

Class question: work?
(hint: after the way up, all powers of two are done, all others require another operation each)

\[ D(n) = 2 \log_2 n - 1 \]

Class question: depth?
(needs to go up and down the tree)
What did we learn earlier?

- Recursive to get to $W = O(n)$ and $D = O(\log n)$! Assume $n = 2^k$ for simplicity!
  - Sounds “optimal”, doesn’t it? Well, let’s look at the constants!
- Algorithm

Mathematical expressions:

\[ W(n) = 2n - \log_2 n - 1 \]

Class question: work?
(hint: after the way up, all powers of two are done, all others require another operation each)

\[ W(n) = 2n - \log_2 n - 1 \]

Class question: depth?
(needs to go up and down the tree)

\[ D(n) = 2 \log_2 n - 1 \]

Class question: what happened to optimality?
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees

\[ x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6 \quad x_7 \quad x_8 \]
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees

Class question: work? (hint: number of count number of omitted ops)
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees

Class question: work?
(hint: number of count number of omitted ops)

\[ W(n) = n \log_2 n - n + 1 \]
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees

Class question: work?
(hint: number of count number of omitted ops)

\[ W(n) = n \log_2 n - n + 1 \]

Class question: depth?
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees

Class question: work?  
(hint: number of count number of omitted ops)

\[ W(n) = n \log_2 n - n + 1 \]

Class question: depth?

\[ D(n) = \log_2 n \]
Oh no, not good, another algorithm to the rescue!

- Dissemination/recursive doubling – another well-known algorithmic technique – similar to trees

Class question: work?
(hint: number of count number of omitted ops)

\[ W(n) = n \log_2 n - n + 1 \]

Class question: depth?

\[ D(n) = \log_2 n \]

Class question: is this now optimal?
Oh no, three non-optimal algorithms so far!

- **Obvious question: is there a depth- and work-optimal algorithm?**
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: $W + D \geq 2n - 2$
Oh no, three non-optimal algorithms so far!

- **Obvious question: is there a depth- and work-optimal algorithm?**
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: \( W + D \geq 2n - 2 \)
Oh no, three non-optimal algorithms so far!

- **Obvious question: is there a depth- and work-optimal algorithm?**
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: $W + D \geq 2n - 2$
Oh no, three non-optimal algorithms so far!

- **Obvious question:** is there a depth- and work-optimal algorithm?
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: \( W + D \geq 2n - 2 \)

![Diagram showing a sequence of variables](image)
Oh no, three non-optimal algorithms so far!

- **Obvious question: is there a depth- and work-optimal algorithm?**
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: $W + D \geq 2n - 2$

Output tree:
- leaves are all inputs, rooted at $x_n$
- binary due to binary operation
- $W = n - 1$, $D = D_o$
Oh no, three non-optimal algorithms so far!

- **Obvious question:** is there a depth- and work-optimal algorithm?
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: \( W + D \geq 2n - 2 \)

Output tree:
- leaves are all inputs, rooted at \( x_n \)
- binary due to binary operation
- \( W = n - 1, D = D_o \)
Oh no, three non-optimal algorithms so far!

- Obvious question: is there a depth- and work-optimal algorithm?
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: $W + D \geq 2n - 2$

Output tree:
- leaves are all inputs, rooted at $x_n$
- binary due to binary operation
- $W = n - 1$, $D = D_o$

Input tree:
- rooted at $x_1$, leaves are all outputs
- not binary (simultaneous read)
- $W = n - 1$
Oh no, three non-optimal algorithms so far!

- **Obvious question: is there a depth- and work-optimal algorithm?**
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: \( W + D \geq 2n - 2 \)

Output tree:
- leaves are all inputs, rooted at \( x_n \)
- binary due to binary operation
- \( W = n - 1, D = D_o \)

Input tree:
- rooted at \( x_1 \), leaves are all outputs
- not binary (simultaneous read)
- \( W = n - 1 \)
Oh no, three non-optimal algorithms so far!

- **Obvious question: is there a depth- and work-optimal algorithm?**
  - This took years to settle! The answer is surprisingly: no
  - We know, for parallel prefix: $W + D \geq 2n - 2$

Output tree:
- leaves are all inputs, rooted at $x_n$
- binary due to binary operation
- $W = n - 1, D = D_o$

Input tree:
- rooted at $x_1$, leaves are all outputs
- not binary (simultaneous read)
- $W = n - 1$

Ridge can be at most $D_o$ long!
Now add trees and subtract shared vertices:

\[(n - 1) + (n - 1) - D_o = 2n - 2 - D_o \leq W\]

q.e.d.
Work-Depth Tradeoffs and deficiency

“The deficiency of a prefix circuit $c$ is defined as $\text{def}(c) = W_c + D_c - (2n - 2)$”

From Zhu et al.: “Construction of Zero-Deficiency Parallel Prefix Circuits”

Latest 2006 result for zero-deficiency construction for $n > F(D + 3) - 1$ ($f(n)$ is inverse)
Work- and depth-optimal constructions

Work-optimal?

- \( n - 1 \), thus \( D = 2n - 2 - W = n - 1 \) q.e.d. ☺

Depth-optimal?

- Ladner and Fischer propose a construction for work-efficient circuits with minimal depth
  \( D = \lceil \log_2 n \rceil, W \leq 4n \)
  
  *Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)*
  
  *Has an unbounded fan-out! May thus not be practical* ☺

Depth-optimal with bounded fan-out?

- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
Work- and depth-optimal constructions

Work-optimal?
- Only sequential! Why?
- \( = n - 1 \), thus \( D = 2n - 2 - W = n - 1 \) q.e.d. 😊

Depth-optimal?
- Ladner and Fischer propose a construction for work-efficient circuits with minimal depth
  \( D = \lceil \log_2 n \rceil \), \( W \leq 4n \)
  Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)
  Has an unbounded fan-out! May thus not be practical 😞

Depth-optimal with bounded fan-out?
- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
Work- and depth-optimal constructions

\(n\!-\!1\), thus \(D=2n\!-\!2-W=W=n\!-\!1\) q.e.d.

Work-optimal?
- Only sequential! Why?
- \(W=n-1\), thus \(D=2n-2-W=n-1\) q.e.d.

Depth-optimal?
- Ladner and Fischer propose a construction for work-efficient circuits with minimal depth \(D=\lceil\log_2 n\rceil, W \leq 4n\)
  - Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)
  - Has an unbounded fan-out! May thus not be practical

Depth-optimal with bounded fan-out?
- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
Work- and depth-optimal constructions

\( n \) \(-1, \) thus \( DD = 2nn - 2 - WW = nn - 1 \) q.e.d.

Work-optimal?
- Only sequential! Why?
- \( W = n - 1, \) thus \( D = 2n - 2 - W = n - 1 \) q.e.d.

Depth-optimal?

Depth-optimal?
- Ladner and Fischer propose a construction for work-efficient circuits with minimal depth
  \( D = \lceil \log_2 n \rceil, \) \( W \leq 4n \)
  Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)
  Has an unbounded fan-out! May thus not be practical

Depth-optimal with bounded fan-out?
- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
Work- and depth-optimal constructions

\[ \lceil \log_2 n \rceil \log_2 \log_2 \log_2 2 \log 2 \log 2 \n \rceil \log_2 n, \quad WW \leq 4nn, \quad \text{for } nn-1, \text{ thus } DD=2nn-2-WW=nn-1 \text{ q.e.d.} \]

Work-optimal?
- Only sequential! Why?
- \( W = n - 1 \), thus \( D = 2n - 2 - W = n - 1 \) q.e.d.

Depth-optimal?
- Ladner and Fischer propose a construction for work-efficient circuits with minimal depth
  - Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)
  - Has an unbounded fan-out! May thus not be practical

Depth-optimal with bounded fan-out?
- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
Work- and depth-optimal constructions

\[
\left\lceil \log_2 n \right\rceil \log_2 \log_2 2 \log_2 2 \log_2 \log_2 n\rceil, WW \leq 4nn
\]

\(nn-1\), thus \(DD=2nn-2-WW=nn-1\) q.e.d. ④

Work-optimal?
- Only sequential! Why?
- \(W = n - 1\), thus \(D = 2n - 2 - W = n - 1\) q.e.d. ⑤

Depth-optimal?
- Ladner and Fischer propose a construction for work-efficient circuits with minimal depth
  - *Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)*
  - *Has an unbounded fan-out! May thus not be practical* ③
    - *Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)*

Depth-optimal with bounded fan-out?

Depth-optimal with bounded fan-out?
- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
Work- and depth-optimal constructions

\[ \lceil \log_2 n \rceil \log_2 \log_2 2 \log_2 2 \log_2 n \rceil \log_2 n \rceil, WW \leq 4nn \]

\[ nn-1, \text{ thus } DD = 2nn - 2 - WW = nn - 1 \text{ q.e.d. } \]

Work-optimal?
- Only sequential! Why?
- \( W = n - 1 \), thus \( D = 2n - 2 - W = n - 1 \text{ q.e.d. } \)

Depth-optimal?
- Ladner and Fischer propose a construction for work-efficient circuits with minimal depth
  - Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)
  - Has an unbounded fan-out! May thus not be practical

Depth-optimal with bounded fan-out?
- Some constructions exist, interesting open problem

Depth-optimal with bounded fan-out?
- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
Work- and depth-optimal constructions

\[ \left\lceil \log_2 n \right\rceil \log_2 \log_2 2 \log_2 \log_2 n, \, WW \leq 4nn \]

\( nn-1 \), thus \( DD=2nn-2-WW=nn-1 \) q.e.d. ✖

Work-optimal?
- Only sequential! Why?
- \( W = n - 1 \), thus \( D = 2n - 2 - W = n - 1 \) q.e.d. ☹️

Depth-optimal?
- Ladner and Fischer propose a construction for work-efficient circuits with minimal depth
  - Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)
  - Has an unbounded fan-out! May thus not be practical ☹️
  - Simple set of recursive construction rules (boring for class, check 1980’s paper if needed)

Depth-optimal with bounded fan-out?
- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
- Some constructions exist, interesting open problem
- Nice research topic to define optimal circuits
But why do we care about this prefix sum so much?

It’s the simplest problem to demonstrate W-D tradeoffs
- And it’s one of the most important parallel primitives

= \ a + b \ (n\text{-bit numbers})
- Starting with single-bit (full) adder for bit $i$
But why do we care about this prefix sum so much?

It’s the simplest problem to demonstrate W-D tradeoffs

- And it’s one of the most important parallel primitives

- Prefix summation as function composition is extremely powerful!
  - Many seemingly sequential problems can be parallelized!

\[ = a + b \text{ (n-bit numbers)} \]

- Starting with single-bit (full) adder for bit i
But why do we care about this prefix sum so much?

= \( aa + bb \) (n-bit numbers)

It’s the simplest problem to demonstrate W-D tradeoffs
  - And it’s one of the most important parallel primitives

- **Prefix summation as function composition is extremely powerful!**
  - Many seemingly sequential problems can be parallelized!

- **Simple first example: binary adder** \(- s = a + b \) (n-bit numbers)
  - Starting with single-bit (full) adder for bit \( i \)
But why do we care about this prefix sum so much?

\[ aa + bb \] (n-bit numbers)

It’s the simplest problem to demonstrate W-D tradeoffs

- And it’s one of the most important parallel primitives

- Prefix summation as function composition is extremely powerful!
  - Many seemingly sequential problems can be parallelized!

- Starting with single-bit (full) adder for bit i
- Starting with single-bit (full) adder for bit i
But why do we care about this prefix sum so much?

= \( aa + bb \) (n-bit numbers)

It’s the simplest problem to demonstrate W-D tradeoffs
- And it’s one of the most important parallel primitives

- Prefix summation as function composition is extremely powerful!
  - Many seemingly sequential problems can be parallelized!
  - Starting with single-bit (full) adder for bit \( i \)
  - Starting with single-bit (full) adder for bit \( i \)
But why do we care about this prefix sum so much?

= \( aa + bb \) (n-bit numbers)

It’s the simplest problem to demonstrate W-D tradeoffs

- And it’s one of the most important parallel primitives

- Prefix summation as function composition is extremely powerful!
  - Many seemingly sequential problems can be parallelized!

- Starting with single-bit (full) adder for bit \( i \)
- Starting with single-bit (full) adder for bit \( i \)

Question: what are the functions for \( s_i \) and \( c_{out,i} \)?
But why do we care about this prefix sum so much?

= \( aa+bb \) (n-bit numbers)

It’s the simplest problem to demonstrate W-D tradeoffs

- And it’s one of the most important parallel primitives

- **Prefix summation as function composition is extremely powerful!**
  - Many seemingly sequential problems can be parallelized!

- Starting with single-bit (full) adder for bit \( i \)
- Starting with single-bit (full) adder for bit \( i \)

![Diagram](image)

Question: what are the functions for \( s_i \) and \( c_{out,i} \)?

\[
\begin{align*}
  s_i &= a_i \text{xor} \ b_i \text{xor} \ c_{in,i} \\
  c_{out,i} &= a_i \text{ and} \ b_i \text{ or} \ c_{in,i} \text{ and} \ (a_i \text{xor} \ b_i)
\end{align*}
\]
But why do we care about this prefix sum so much?

\[ = aa+bb \text{ (n-bit numbers)} \]

It’s the simplest problem to demonstrate W-D tradeoffs
- And it’s one of the most important parallel primitives

- Prefix summation as function composition is extremely powerful!
  - Many seemingly sequential problems can be parallelized!

- Starting with single-bit (full) adder for bit \( i \)
- Starting with single-bit (full) adder for bit \( i \)

Question: what are the functions for \( s_i \) and \( c_{out,i} \)?
\[
\begin{align*}
  s_i &= a_i \text{xor} \ b_i \text{xor} \ c_{in,i} \\
  c_{out,i} &= a_i \text{ and} \ b_i \text{ or} \ c_{in,i} \text{ and} (a_i \text{xor} \ b_i)
\end{align*}
\]

Example 4-bit ripple carry adder

source: electronics-tutorials.ws
But why do we care about this prefix sum so much?

= $aa+bb$ (n-bit numbers)

It’s the simplest problem to demonstrate W-D tradeoffs

- And it’s one of the most important parallel primitives

- Prefix summation as function composition is extremely powerful!
  - Many seemingly sequential problems can be parallelized!

- Starting with single-bit (full) adder for bit $i$
- Starting with single-bit (full) adder for bit $i$

![Diagram of 4-bit ripple carry adder](source: electronics-tutorials.ws)

Example 4-bit ripple carry adder

**Question:** what are the functions for $s_i$ and $c_{out,i}$?

- $s_i = a_i \text{ xor } b_i \text{ xor } c_{in,i}$
- $c_{out,i} = a_i \text{ and } b_i \text{ or } c_{in,i} \text{ and } (a_i \text{ xor } b_i)$

Show example 4-bit addition!
But why do we care about this prefix sum so much?

= aa + bb (n-bit numbers)

It’s the simplest problem to demonstrate W-D tradeoffs
  - And it’s one of the most important parallel primitives

- Prefix summation as function composition is extremely powerful!
  - Many seemingly sequential problems can be parallelized!

- Starting with single-bit (full) adder for bit i
- Starting with single-bit (full) adder for bit i

\[
\begin{align*}
    a_i & \quad b_i \\
    c_{in,i} & \quad + \quad c_{out,i} \\
    s_i & \quad c_{out,i} = a_i \text{ xor } b_i \text{ xor } c_{in,i} \\
    & \quad c_{out,i} = a_i \text{ and } b_i \text{ or } c_{in,i} \text{ and } (a_i \text{ xor } b_i)
\end{align*}
\]

Example 4-bit ripple carry adder

Question: what are the functions for \( s_i \) and \( c_{out,i} \)?

\[
\begin{align*}
    s_i &= a_i \text{ xor } b_i \text{ xor } c_{in,i} \\
    c_{out,i} &= a_i \text{ and } b_i \text{ or } c_{in,i} \text{ and } (a_i \text{ xor } b_i)
\end{align*}
\]

Show example 4-bit addition!

Question: what is work and depth?
We only want $s$!

- $c_{in,2}, \ldots, c_{in,n}$ though ☺️

- **Carry bits can be computed with a scan!**
  - Model carry bit as state starting with 0
    - Encode state as 1-hot vector: $q_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $q_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
  - Each full adder updates the carry bit state according to $a_i$ and $b_i$
    - State update is now represented by matrix operator, depending on $a_i$ and $b_i$ ($M_{a_ib_i}$):
      $$M_{00} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad M_{10} = M_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$
  - Operator composition is defined on algebraic ring (\{0, 1, or, and\}) – i.e., replace “+” with “and” and “*” with “or”
    - Prefix sum on the states computes now all carry bits in parallel!

- **Example: a=011, b=101 $\rightarrow M_{11}, M_{10}, M_{01}$**
  - Scan computes: $M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$; $M_{11}M_{10} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$; $M_{11}M_{10}M_{01} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ in parallel
  - All carry states and $s_i$ can now be computed in parallel by multiplying scan result with $q_0$
Seems very sequential, can this be parallelized?

\[ c_{in,1}, c_{in,2}, c_{in,3}, \ldots, c_{in,n} \]

We only want \( s \)!
- Requires \( c_{in}, n, 1_{in}, 1, c_{in,2}, \ldots, c_{in,n} \) though 

- **Carry bits can be computed with a scan!**
  - Model carry bit as state starting with 0
  - **Encode state as 1-hot vector:** \( q_0 = (0, 1), q_1 = (1, 0) \)
  - Each full adder updates the carry bit state according to \( a_i \) and \( b_i \)
  - **State update is now represented by matrix operator, depending on \( a_i \) and \( b_i \) (\( M_{a_ib_i} \)):**
    \[
    M_{00} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad M_{10} = M_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}
    \]
  - Operator composition is defined on algebraic ring \( \{0, 1, \text{or, and}\} \) – i.e., replace “+” with “and” and “*” with “or”
  - **Prefix sum on the states computes now all carry bits in parallel!**

- **Example:** \( a = 011, b = 101 \rightarrow M_{11}, M_{10}, M_{01} \)
  - Scan computes: \( M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}; \quad M_{11}M_{10} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}; \quad M_{11}M_{10}M_{01} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \) in parallel
  - All carry states and \( s_i \) can now be computed in parallel by multiplying scan result with \( q_0 \)
Seems very sequential, can this be parallelized?

1 c \text{in}, 1, c \text{in}, 2 c c \text{in}, 2 i \text{inn}, 2 c c \text{in}, 2 i i \text{inn}, 2 c c \text{in}, 2 i i \text{inn}, 2 ... a_i and b_i or i in, a_i xor b_i though

We only want $s_i$!

- Requires $c \text{in}, n, 1 \text{in}, 1, c_{\text{in}, 2}, ... , c_{\text{in}, n}$ though $\otimes$
- Carry bits can be computed with a scan!
- Carry bits can be computed with a scan!
  - Model carry bit as state starting with 0
    - Encode state as 1-hot vector: $q_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $q_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
  - Each full adder updates the carry bit state according to $a_i$ and $b_i$
    - State update is now represented by matrix operator, depending on $a_i$ and $b_i$ ($M_{a_i b_i}$):
      - $M_{00} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $M_{10} = M_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$
    - Operator composition is defined on algebraic ring ($\{0, 1, \text{or, and}\}$) – i.e., replace “+” with “and” and “*” with “or”
    - Prefix sum on the states computes now all carry bits in parallel!

- Example: $a=011, b=101 \rightarrow M_{11}, M_{10}, M_{01}$
  - Scan computes: $M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$; $M_{11} M_{10} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$; $M_{11} M_{10} M_{01} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$ in parallel
  - All carry states and $s$ can now be computed in parallel by multiplying the result with
Seems very sequential, can this be parallelized?

\[ q_0 = 101011001010, q_1 = 101011001010, 1 c_{in,1}, c_{in,2}, c_{in,2}, i_{in,2}, c_{in,2}, \ldots, c_{in,n} \text{ or } c_{in,1}, c_{in,2}, i_{in,1}, c_{in,2}, \ldots, c_{in,n} \text{ though } \odot \]

- **Requires** \( c_{in,1}, 1 \text{ in, } 1, c_{in,2}, \ldots, c_{in,n} \text{ though } \odot \)

- **Carry bits can be computed with a scan!**
  - **Model carry bit as state starting with 0**
    - **Encode state as 1-hot vector:** \( q_0 = 1000 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, q_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \)
    - **Encode state as 1-hot vector:** \( q_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, q_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \)
  - **Each full adder updates the carry bit state according to** \( a_i \) and \( b_i \)
    - **State update is now represented by matrix operator, depending on** \( a_i \) and \( b_i \) \((M_{a_i b_i})\):
      \[
      M_{00} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, M_{10} = M_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}
      \]
  - **Operator composition is defined on algebraic ring \((\{0, 1, \text{or, and}\}) – i.e., replace “+” with “and” and “*” with “or”**
    - **Prefix sum on the states computes now all carry bits in parallel!**

- **Example:** \( a=011, b=101 \rightarrow M_{11}, M_{10}, M_{01} \)
  - **Scan computes:** \( M_a = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, M_a M_b = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, M_a M_b M_c = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \) in parallel
Seems very sequential, can this be parallelized?

\[ 0 M 00 = 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 0, \]
\[ 0101 M 01 = 0 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0 1 1 0 1 \]
\[ 0011000111011100111001110011 \]
and
\[ b i b b i i b i (M a i b i M M M a i b i a i a a a i i a i b i b b i i b i M _ { 3 } a i b i ) ; \]
and
\[ b i b b i i b i \]

\[ q 0 = 1 0 1 1 1 1 0 0 1 0 1 0 , q 1 q q q 1 1 q 1 = 0 1 0 1 0 0 1 1 0 1 0 1 \]

\[ 1 c i n , 1, c i n , 2 c c c i n , 2 i i n n , 2 c i n , 2 , . . . , c i n , n c c c i n , n i i n n , n n c i n , n \] though ☹

We only want \( s \)!

- Requires \( c i n , n , 1 i n , 1 , c _ { i n , 2 } , . . . , c _ { i n , n } \) though ☺

- **Carry bits can be computed with a scan!**
  - Model carry bit as state starting with 0
    \[
    M 0 0 0 0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, M_{10} = M_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, M_{11} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}
    \]
  - Encode state as 1-hot vector: \( q 0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, q 1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \)
  - Each full adder updates the carry bit state according to \( a _ { i } \) and \( b _ { i } \)
  - State update is now represented by matrix operator, depending on \( a _ { i } \) and \( b _ { i } \) (\( M _ { a _ { i } b _ { i } } \)):
    \[
    M_{00} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, M_{10} = M_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, M_{11} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}
    \]
Seems very sequential, can this be parallelized?

\[ M_{00} = 1100110011001100, M_{10} = M_{01} = 0110011001100110, M_{11} = 00110001100110011010 \]

and \( b_i b_i i_i b_i (M_{a_i b_i} M i b_i a i b_i a i a a a i i a i b b b i i b i M_{a_i b_i}) \):

\[ q_0 = 1010110010, q_1 = 0101001101 \]

We only want \( s! \)

- Requires \( c_i n, 1, i n, 1, c_i n, 2, i n, 2, i n, n c c c i n, n i n, n n c i n, n \) though 😞

- Carry bits can be computed with a scan!
  - Model carry bit as state starting with 0
  - Operator composition is defined on algebraic ring \( \{0, 1, or, and\} \) – i.e., replace “+” with “and” and “*” with “or”
  - Prefix sum on the states computes now all carry bits in parallel!
  - Each full adder updates the carry bit state according to \( a_i \) and \( b_i \)

State update is now represented by matrix operator, depending on \( a_i \) and \( b_i \) \( (M_{a_i b_i}) \):

\[
M_{00} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, M_{10} = M_{01} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, M_{11} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}
\]
Seems very sequential, can this be parallelized?

\[
\begin{align*}
&M_{10} M M M_{10} 1100 M_{10} M_{10}, \quad \text{and} \quad (a_i \text{xor} b_i) \\
0 M_{00} = 1100 1100 1110011100 1100 0101 M_{01} = 0110 0110 0110 0110 0110 0110 0110 0110, \quad M_{11} M M M_{11} 11 11 M_{11} = 0011 0011 0011 0011 0011 0011 0011 0011
\end{align*}
\]

and \( b \overline{i} b \overline{i} b i i b i (M a i b i M M M a i b i a i a a a i i a i b i b b b i i b i M a i b i) \):

\[q_0 = 10 10 11 00 10 10, \quad q_1 q_0 q 1 1 q 1 = 01 01 00 11 01 01\]

\(1 c i n, 1, c i n, 2 c c c i n, 2 i i n, 2 c i n, 2, \ldots, c i n, n c c c i n, n i i n, n n c i n, n \) though ☹️

We only want \( s! \)

- Requires \( c i n, n, 1 i n, 1, c i n, 2, \ldots, c i n, n \) though ☹️

- **Carry bits can be computed with a scan!**
  - Model carry bit as state starting with 0
  - Operator composition is defined on algebraic ring (\{0, 1, or, and\}) – i.e., replace “+” with “and” and “*” with “or”
  - **Prefix sum on the states computes now all carry bits in parallel!**
  - Each full adder updates the carry bit state according to \( a_i \) and \( b_i \)

- **Example:** \( a=011, b=101 \rightarrow M_{11}, 11 11 11, M_{10}, M_{01} \)
  - \( M_{10} \rightarrow \begin{pmatrix} 1 \\ 1 \end{pmatrix} \), \( M_{00} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \), \( M_{10} \rightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix} \)
Seems very sequential, can this be parallelized?

\[ M_{11} = \begin{array}{ccccccccccccccccccccccc} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{array} \]

\[ M_{10} = \begin{array}{ccccccccccccccccccccccc} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{array} \]

\[ M_{10} M_{10} M_{10} M_{10} M_{10} = M_{01} M_{01} M_{01} M_{01} M_{01} = \begin{array}{ccccccccccccccccccccccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{array} \]

\[ M_{10} M_{01} M_{01} M_{01} M_{01} = 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \]

and \( b b b b i i i i (M a i b i M M a i b i a i a a a i i a i b i b b b i i b i M a i b i) \):

\[ q_0 = 10 10110010 10, q_1 q_2 q_1 q_1 q_1 = 01 01001101 01 \]

We only want \( s \)!

- Requires \( c_{in}, n, 1_{in}, 1, c_{in}, 2, ..., c_{in}, n \) though \( \neq \)

- **Carry bits can be computed with a scan!**
  - Model carry bit as state starting with 0
  - Operator composition is defined on algebraic ring \( \{0, 1, \text{or}, \text{and}\} \) – i.e., replace “+” with “and” and “*” with “or”
  - Prefix sum on the states computes now all carry bits in parallel!
spcl.inf.ethz.ch
@spcl_eth

Seems very sequential, can this be parallelized?
𝑐𝑜𝑢𝑡,𝑖
= 𝑎𝑖 and scan
𝑏𝑖 orresult
𝑐𝑖𝑛,𝑖 and
can now be computed in parallel
by multiplying
with(𝑎𝑞𝑖 0xor
𝑞𝑞𝑏𝑞𝑖 )0 0 𝑞 0
1 𝑀 11 = 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 1 0𝑠𝑖0 =
1 1𝑎1𝑖 xor
0 0 1𝑏𝑖1xor
0 0𝑐𝑖𝑛,𝑖
1 1 ; 𝑀 11 𝑀𝑀 𝑀 11 11 𝑀 11 𝑀 10 𝑀𝑀 𝑀 10

10 𝑀 10 = 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 ; 𝑀 11 𝑀𝑀 𝑀 11 11 𝑀 11 𝑀 10 𝑀𝑀 𝑀
10 10 𝑀 10 𝑀 01 𝑀𝑀 𝑀 01 01 𝑀 01 = 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 1 1 0 0 1 1 1 0 0 1 1 0 0 1 1 in parallel
source: electronics-tutorials.ws
𝑴 𝟏𝟎 𝑴𝑴 𝑴 𝟏𝟎 𝟏𝟏𝟎𝟎 𝑴 𝟏𝟎 , 𝑴 𝟎𝟏 𝑴𝑴 𝑴 𝟎𝟏 𝟎𝟎𝟏𝟏 𝑴 𝟎𝟏
0 𝑀 00 = 1 1 0 0 1 1 0 0 1 1 1 0 0 1 1 1 0 0 0 1 1 0 0 0 1 1 0 0 1 1 0 0 , 𝑀 10 𝑀𝑀 𝑀 10 10 𝑀 10 = 𝑀 01 𝑀𝑀 𝑀
01 01 𝑀 01 = 0 1 1 0 0 1 1 0 0 0 1 1 0 1 0 1 1 0 1 0 1 1 0 0 0 1 1 0 0 1 1 0 , 𝑀 11 𝑀𝑀 𝑀 11 11 𝑀 11 = 0 0 1 1
001100011000111001110011 0011
and 𝑏 𝑖 𝑏𝑏 𝑏 𝑖 𝑖𝑖 𝑏 𝑖 ( 𝑀 𝑎 𝑖 𝑏 𝑖 𝑀𝑀 𝑀 𝑎 𝑖 𝑏 𝑖 𝑎 𝑖 𝑎𝑎 𝑎 𝑖 𝑖𝑖 𝑎 𝑖 𝑏 𝑖 𝑏𝑏 𝑏 𝑖 𝑖𝑖 𝑏 𝑖 𝑀 𝑎 𝑖 𝑏 𝑖 ):
and 𝑏 𝑖 𝑏𝑏 𝑏 𝑖 𝑖𝑖 𝑏 𝑖
𝑞 0 = 1 0 1 0 1 1 0 0 1 0 1 0 , 𝑞 1 𝑞𝑞 𝑞 1 1 𝑞 1 = 0 1 0 1 0 0 1 1 0 1 0 1
1 𝑐 𝑖𝑛,1 , 𝑐 𝑖𝑛,2 𝑐𝑐 𝑐 𝑖𝑛,2 𝑖𝑖𝑛𝑛,2 𝑐 𝑖𝑛,2 ,…, 𝑐 𝑖𝑛,𝑛 𝑐𝑐 𝑐 𝑖𝑛,𝑛 𝑖𝑖𝑛𝑛,𝑛𝑛 𝑐 𝑖𝑛,𝑛 though
We only want 𝒔!
 Requires 𝑐 𝑖𝑛, 𝑛, 1 𝑖𝑛, 1 , 𝑐𝑖𝑛,2 , … , 𝑐𝑖𝑛,𝑛 though 

 Carry bits can be computed with a scan!
 Model carry bit as state starting with 0
 Operator composition is defined on algebraic ring ({0, 1, or, and}) – i.e., replace “+” with “and” and “*” with “or”

62


Prefix sums as magic bullet for other seemingly sequential algorithms

Any time a sequential chain can be modeled as function composition!

- \( f_1 \ldots f_n \) be an ordered set of functions and \( f_0(x) = x \)
- Define ordered function compositions: \( f_1(x); f_2(f_1(x)); \ldots ; f_n(\ldots f_1(x)) \)
- If we can write function composition \( g(x) = f_i(f_{i-1}(x)) \) as \( g = f_i \circ f_{i-1} \) then we can compute \( \circ \) with a prefix sum!
  
  *We saw an example with the adder \((M_{ab} \text{ were our functions})\)*

- **Example: linear recurrence** \( f_i(x) = a_i f_{i-1}(x) + b_i \) with \( f_0(x) = x \)
  - Write as matrix form \( f_i(x) = \begin{pmatrix} a_i & b_i \\ 0 & 1 \end{pmatrix} f_{i-1}(x) \)
  - Function composition is now simple matrix multiplication!
    
    *For example: \( f_2(x) = \begin{pmatrix} a_2 \\ 0 \end{pmatrix} \begin{pmatrix} b_2 & a_1 \\ 1 & b_1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} a_1 a_2 \\ 0 \end{pmatrix} \begin{pmatrix} a_2 b_1 + b_2 \\ 1 \end{pmatrix} x \)*

- **Most powerful! Homework:**
  - Parallelize tridiagonal solve
  - Parallelize string parsing
Prefix sums as magic bullet for other seemingly sequential algorithms

\( f_1, \ldots, f_n \) be an ordered set of functions and \( f_0 f f f 0 f 0 x x x x = x x \)

Any time a sequential chain can be modeled as function composition!

- Let \( f_1 \ 1 \ 1, \ldots, f_n \) be an ordered set of functions and \( f_0(x) = x \)

- Define ordered function compositions: \( f_1(x); f_2(f_1(x)); \ldots; f_n(... f_1(x)) \)

- If we can write function composition \( g(x) = f_i(f_{i-1}(x)) \) as \( g = f_i \circ f_{i-1} \) then we can compute \( \circ \) with a prefix sum!

  We saw an example with the adder (\( M_{ab} \) were our functions)

- Example: linear recurrence \( f_i(x) = a_i f_{i-1}(x) + b_i \) with \( f_0(x) = x \)

  - Write as matrix form \( f_i(x) = \begin{pmatrix} a_i & b_i \\ 0 & 1 \end{pmatrix} f_{i-1} \begin{pmatrix} x \\ 1 \end{pmatrix} \)

  - Function composition is now simple matrix multiplication!

  For example: \( f_2 \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} f_0 \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_2 b_1 + b_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} \)

- Most powerful! Homework:
  - Parallelize tridiagonal solve
  - Parallelize string parsing
Prefix sums as magic bullet for other seemingly sequential algorithms

\[ f_1(x); f_2(x); f_2(x); f_2(x); f_2(x); \ldots; f_n(x); f_n(x); f_n(x); f_n(x) \]

\[ f_1, \ldots, f_n \] be an ordered set of functions and \[ f_0(x) = x \]

**Any time a sequential chain can be modeled as function composition!**

- Define ordered function compositions: \[ f_1(x); f_2(f_1(x)); \ldots; f_n(\ldots f_1(x)) \]
- Define ordered function compositions: \[ f_1(x); f_2(f_1(x)); \ldots; f_n(\ldots f_1(x)) \]
- If we can write function composition \( g(x) = f_i(f_{i-1}(x)) \) as \( g = f_i \circ f_{i-1} \) then we can compute \( \circ \) with a prefix sum!

*We saw an example with the adder (\( M_{ab} \) were our functions)*

- **Example: linear recurrence** \( f_i(x) = a_if_{i-1}(x) + b_i \) with \( f_0(x) = x \)
  - Write as matrix form \( f_i(x) = \begin{pmatrix} a_i & b_i \\ 0 & 1 \end{pmatrix} f_{i-1}(x) \)
  - Function composition is now simple matrix multiplication!

*For example:* \( f_2(x) = \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} f_0(x) = \begin{pmatrix} a_1a_2 & a_2 b_1 + b_2 \\ 0 & 1 \end{pmatrix} f_0(x) \)

- **Most powerful! Homework:**
  - Parallelize tridiagonal solve
Prefix sums as magic bullet for other seemingly sequential algorithms

were our functions)

\[ f f g x = f i i g x = f i ( f i-1 f f i-1 i i-1 f i-1 x x x x) \] as \( gg = f i f f i i f i \circ f i-1 f f i-1 i i-1 f i-1 \) then we can compute \( \circ \) with a prefix sum!

\[ f 1 (x x); f 2 f f f 2 2 f 2 (f 1 f f 1 1 f 1 x x x x); ... ; f n f f f n n f n (f ... f 1 f f 1 1 f 1 x x x x) \]

\( f 1,..., f n ) \) \( f f f n n f n \) be an ordered set of functions and \( f 0 f f 0 0 f 0 x x x x = x x \)

Any time a sequential chain can be modeled as function composition!

We saw an example with the adder (\( M a b a b b a b \) were our functions)

- Define ordered function compositions: \( f_1 (x); f_2 (f_1 (x)); ... ; f_n (f ... f_1 (x)) \)
- If we can write function composition \( g(x) = f_i (f_{i-1} (x)) \) as \( g = f_i \circ f_{i-1} \) then we can compute \( \circ \) with a prefix sum!

We saw an example with the adder (\( M_{a b} \) were our functions)

- Example: linear recurrence \( f_i (x) = a_i f_{i-1} (x) + b_i \) with \( f_0 (x) = x \)
  - Write as matrix form \( f_i (x)_1 = (a_i b_i) f_{i-1} (x)_1 \)
  - Function composition is now simple matrix multiplication!

\[ \text{For example: } f_2 (x)_1 = \begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix} f_0 (x)_1 = \begin{pmatrix} a_1 a_2 & a_2 b_1 + b_2 \\ 0 & 1 \end{pmatrix} (x)_1 \]

Prefix sums as magic bullet for other seemingly sequential algorithms

\[ a \ i \ aa \ a \ i \ il \ a \ i \ f \ i-1 \ ff \ f \ i-1 \ il-11 \ f \ i-1 \ x \ xx \ x + b \ i \ bb \ b \ i \ il \ b \ i \ with \ f \ 0 \ ff \ f \ 00 \ f \ 0 \ x \ xx \ x = x \]

were our functions

\[ f \ g \ x = f \ i \ ii \ g \ x = f \ i \ f \ i-1 \ ff \ f \ i-1 \ ii-1 \ f \ i-1 \ x \ xx \ x \ as \ g g = f \ i \ f \ i \ ii \ f \ i \ f \ i-1 \ ff \ f \ i-1 \ ii-1 \ f \ i-1 \ f \ i-1 \ then \ we \ can \ compute \ o \ with \ a \ prefix \ sum! \]

\[ f \ 1 \ (xx); \ f \ 2 \ ff \ f \ 22 \ f \ 2 \ (f \ 1 \ ff \ f \ 11 \ f \ 1 \ x \ xx \ x); \ ... ; \ f \ n \ ff \ f \ n \ nn \ f \ n \ (\ ... \ f \ 1 \ ff \ f \ 11 \ f \ 1 \ x \ xx \ x) \]

\[ f \ 1 ,..., \ f \ n \ ff \ f \ n \ nn \ f \ n \ be \ an \ ordered \ set \ of \ functions \ and \ f \ 0 \ ff \ f \ 00 \ f \ 0 \ x \ xx \ x = xx \]

Any time a sequential chain can be modeled as function composition!

- Example: linear recurrence \( f \ i \ x = i \ ii \ i \ (x) = a_i f_{i-1}(x) + b_i \) with \( f_0(x) = x \)
  - If we can write function composition \( g(x) = f_i(f_{i-1}(x)) \) as \( g = f_i \circ f_{i-1} \) then we can compute \( \circ \) with a prefix sum!

  We saw an example with the adder \( (M \ a \ b \ a \ b \ a \ b \ a \ b \ a \ b \ were \ our \ functions) \)

- Example: linear recurrence \( f_i(x) = a_i f_{i-1}(x) + b_i \) with \( f_0(x) = x \)
  - Write as matrix form \( f_i(x) = \begin{pmatrix} a_i & b_i \\ 0 & 1 \end{pmatrix} f_{i-1}(x) \)
  - Function composition is now simple matrix multiplication!

  For example:
Prefix sums as magic bullet for other seemingly sequential algorithms

\[ x_1 x_1 = a_i b_i 0 1 a_i b_i 0 1 a_i a_i a_i i a_i a_i b_i 0 1 b_i b_i b_i i b_i a_i b_i 0 1 1 a_i b_i 0 1 a_i b_i 0 1 f_i-1 f_f f_i-1 i_i-1 f_i-1 x_1 x_1 x x 1 x 1 a_i a_i a_i i a_i f_i-1 f_f f_i-1 i_i-1 f_i-1 x x x + b_i b_i b_i i i b_i \]

with \( f_0 f_f 0 0 0 f_0 x x x = x \) were our functions

\[ f f g x = f i i g x = f i ( f i-1 f_f f_i-1 i_i-1 f_i-1 x x x ) \]
as \( g g = f i f_f f_i i i f_i \circ f_i-1 f_f f_i-1 i_i-1 f_i-1 \) then we can compute \( \circ \) with a prefix sum!

\[ f 1 (x x); f 2 f_f f_2 f_2 ( f 1 f_f f_1 1 f_1 x x x ); \ldots ; f n f_f f_n n n f_n ( \ldots f 1 f_f f_1 1 f_1 x x x ) \]

\( f 1, \ldots, f n f_f f_n n n f_n \) be an ordered set of functions and \( f_0 f_f f_0 0 f_0 x x x = x x \)

Any time a sequential chain can be modeled as function composition!

We saw an example with the adder ( \( M a b a b b a b \) were our functions)

- Write as matrix form \( f_i x 1 1 1 x 1 i_i i ( x ) = \begin{pmatrix} a_i & b_i \\ 0 & 1 \end{pmatrix} f_{i-1} ( x ) \)
- If we can write function composition \( g(x) = f_i(f_{i-1}(x)) \) as \( g = f_i \circ f_{i-1} \) then we can compute \( \circ \) with a prefix sum!

We saw an example with the adder ( \( M_{a b} \) were our functions)

- Example: linear recurrence \( f_i(x) = a_i f_{i-1}(x) + b_i \) with \( f_0(x) = x \)

Prefix sums as magic bullet for other seemingly sequential algorithms
Prefix sums as magic bullet for other seemingly sequential algorithms

\[ f(x) = \sum_{i=1}^{n} x_i \]

with a prefix sum! Any time a sequential chain can be modeled as function composition!

\[ f(x) \circ g(x) = \sum_{i=1}^{n} (f \circ g)(x) \]

were our functions)

\[ f \circ g(x) = f(g(x)) \]

then we can compute \( \circ \) with a prefix sum!

\[ f(x); f \circ f(x) \]

be an ordered set of functions and \( f \circ f(0 \circ f \circ f(0 \circ f \circ f(x)) \]

Any time a sequential chain can be modeled as function composition!

We saw an example with the adder (\( M_{ab} = ab \), \( ab \) were our functions).
Prefix sums as magic bullet for other seemingly sequential algorithms

\[
f 2 \ x 1 \ x 1 \ x x x \ x 1 \ x 1 = a 2 \ b 2 \ 0 1 \ a 2 \ b 2 \ 0 1 \ a 2 a a a 2 \ a 2 \ a 2 \ b 2 \ 0 1 \ b 2 b b b 2 2 b 2 a 2 \ b 2 \ 0 1 a 2 \ b 2 \ 0 1 \ a 1 \ b 1 \ 0 1 \ a 1 b 1 \ 0 1 a 1 b 1 \ 0 1 f 0 f f f 0 0 f 0 \ x 1 \ x 1 \ x x x \ x 1 x 1 = a 1 a 2 \ a 2 b 1 \ b 2 0 1 \ a 1 a 2 \ a 2 b 1 \ b 2 0 1 a 1 a a a 1 a 1 a 2 b 1 b 2 0 1 a 2 b 1 a 2 a a a 2 a 2 bb b 2 2 b 2 a 1 a 2 a 2 b 1 \ b 2 0 1 a 1 a 2 a 2 b 1 \ b 2 0 1 a 1 a 2 a 2 b 1 \ b 2 0 1 \ x 1 x 1 \ x x x \ x 1 x 1 = a 1 \ b i 0 1 \ a i b i 0 1 a i a a a a i i a i a i b i 0 1 b i b b b i i b i a i b i 0 1 a i b i 0 1 f i-1 f f f i-1 i i-1 f i-1 \ x 1 x 1 \ x x x \ x 1 x 1 = a i a a a a i i a i f i-1 f f f i-1 i i-1 f i-1 x x x \ b i b b i i b i \text{ with } f 0 f f f 0 0 f 0 x x x = x \]
were our functions

\[
f f g x = f i i g x = f i (f i-1 f f f i-1 i i-1 f i-1 x x x) \text{ as } g g = f i f f f i i f i \circ f i-1 f f f i-1 i i-1 f i-1 \text{ then we can compute } \circ \text{ with a prefix sum!}
\]

\[
f 1 (x x) ; f 2 f f f 2 2 f 2 (f 1 f f f 1 1 f 1 x x x) ; \ldots ; f n f f f n n n f n (f n 1 f f f 1 1 f 1 x x x)
\]

\[f 1, \ldots, f n f f f n n n f n\] be an ordered set of functions and \(f 0 f f f 0 f 0 f 0 x x x = x x\)

Any time a sequential chain can be modeled as function composition!

We saw an example with the adder \((M a h a h b a h a, a h b a h a, a h b a h a, a h b a h a, a h b a h a, a h b a h a)\) were our functions.
Prefix sums as magic bullet for other seemingly sequential algorithms

\[
f 2 \times 1 \times 1 \times x \times x = 1 \times 1 = a 2 b 2 0 1 a 2 b 2 0 1 a 2 a a a 2 a 2 a 2 b 2 0 1 b 2 b b b 2 2 b 2 a 2 b 2 0 1 a 2 b 2 0 1 a 2 b 2 0 1 a 1 b 1 0 1 a 1 b 1 0 1 a 1 b 1 0 1 a 1 b 1 0 1 f 0 f f f 0 f 0 x 1 x 1 x x x 1 x 1 = a 1 a 2 a 2 b 1 + b 2 0 1 a 1 b 0 1 0 1 a 1 b 0 1 0 1 a 1 b 0 1 0 1 a 1 b 0 1 0 1 f 0 f f f 0 f 0 x 1 x 1 x x x 1 x 1
\]

\[
x 1 x 1 = a i b i 0 1 a i b i 0 1 a i a a a i i a i a i b i 0 1 b i b b b i i b i a i b i 0 1 a i b i 0 1 a i b i 0 1 f i 1 f f f f 1 i i 1 i 1 i 1 i 1 x 1 x 1 x x x 1 x 1 a i a a a i i a i f i 1 f f f f i 1 i i 11 f i 1 x x x + b i b b b i i b i \text{ with } f 0 f f f 0 0 0 f 0 x x x = x
\]

were our functions)

\[
ff g x = f i i g x = f i (f i 1 f f f i 1 i i 1 f i 1 x x x \text{ as } g g = f i f f i i f i \circ f i 1 f f f i 1 i i 1 f i 1 \text{ then we can compute } \circ \text{ with a prefix sum!}
\]

\[
f 1 (x x) ; f 2 f f f 2 2 f 2 (f 1 f f f 1 1 f 1 x x x) ; \ldots ; f n f f f n n n f n \ldots f 1 f f f 1 1 f 1 x x x
\]

\[
f 1 , \ldots , f n f f f n n n f n \text{ be an ordered set of functions and } f 0 f f f 0 0 f 0 x x x = x x
\]

Any time a sequential chain can be modeled as function composition!

We saw an example with the adder (\( M_{ab} = ab + ah \), were our functions).
Another use for prefix sums: Parallel radix sort

- stably sort all values by the $i$-th bit
Another use for prefix sums: Parallel radix sort

- Radix sort works bit-by-bit
  - stably sort all values by the \( i \)-th bit
Another use for prefix sums: Parallel radix sort

- Radix sort works bit-by-bit
  - Sorts k-bit numbers in k iterations
  - stably sort all values by the $i$-th bit
Another use for prefix sums: Parallel radix sort

- Radix sort works bit-by-bit
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
Another use for prefix sums: Parallel radix sort

- Radix sort works bit-by-bit
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    
    \begin{verbatim}
    Iteration 0: 101 111 010 011 110 001
    \end{verbatim}
Another use for prefix sums: Parallel radix sort

- Radix sort works bit-by-bit
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, k=1:

  *Iteration 0*: 101 111 010 011 110 001

  *Iteration 1*: 010 110 101 111 011 001
Another use for prefix sums: Parallel radix sort

- Radix sort works bit-by-bit
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    - Iteration 0: 101 111 010 011 110 001
    - Iteration 1: 010 110 101 111 011 001
    - Iteration 2: 101 001 010 110 111 011

Another use for prefix sums: Parallel radix sort
Another use for prefix sums: Parallel radix sort

- Radix sort works bit-by-bit
  - Sorts k-bit numbers in k iterations
  - In each iteration \( i \) stably sort all values by the \( i \)-th bit
  - Example, \( k=1 \):
    
    Iteration 0: 101 111 010 011 110 001
    Iteration 1: 010 110 101 111 011 001
    Iteration 2: 101 001 010 110 111 011
    Iteration 3: 001 010 011 101 110 111
Another use for prefix sums: Parallel radix sort

- **Radix sort works bit-by-bit**
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    - *Iteration 0*: 101 111 010 011 110 001
    - *Iteration 1*: 010 110 101 111 011 001
    - *Iteration 2*: 101 001 010 110 111 011
    - *Iteration 3*: 001 010 011 101 110 111

- **Now on n processors**
Another use for prefix sums: Parallel radix sort

- **Radix sort works bit-by-bit**
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    
    **Iteration 0:** 101 111 010 011 110 001
    **Iteration 1:** 010 110 101 111 011 001
    **Iteration 2:** 101 001 010 110 111 011
    **Iteration 3:** 001 010 011 101 110 111

- **Now on n processors**
  - Each processor owns single k-bit number, each iteration
Another use for prefix sums: Parallel radix sort

- **Radix sort works bit-by-bit**
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    
    Iteration 0: 101 111 010 011 110 001
    
    Iteration 1: 010 110 101 111 011 001
    
    Iteration 2: 101 001 010 110 111 011
    
    Iteration 3: 001 010 011 101 110 111

- **Now on n processors**
  - Each processor owns single k-bit number, each iteration
    
    $low = prefix\_scan(!bit, sum)$
Another use for prefix sums: Parallel radix sort

- **Radix sort works bit-by-bit**
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    - Iteration 0: 101 111 010 011 110 001
    - Iteration 1: 010 110 101 111 011 001
    - Iteration 2: 101 001 010 110 111 011
    - Iteration 3: 001 010 011 101 110 111

- **Now on n processors**
  - Each processor owns single k-bit number, each iteration
    - $low = \text{prefix\_scan}(!\text{bit}, \text{sum})$
    - $high = n-1\text{-backwards\_prefix\_scan}(\text{bit}, \text{sum})$
Another use for prefix sums: Parallel radix sort

- **Radix sort works bit-by-bit**
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    - Iteration 0: 101 111 010 011 110 001
    - Iteration 1: 010 110 101 111 011 001
    - Iteration 2: 101 001 010 110 111 011
    - Iteration 3: 001 010 011 101 110 111

- **Now on n processors**
  - Each processor owns single k-bit number, each iteration
    - $low = \text{prefix\_scan}(\text{!bit, sum})$
    - $high = n-1\text{-backwards\_prefix\_scan}(\text{bit, sum})$
    - $new\_idx = (\text{bit} == 0) : low \ ? \ high$
Another use for prefix sums: Parallel radix sort

- **Radix sort works bit-by-bit**
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    - Iteration 0: 101 111 010 011 110 001
    - Iteration 1: 010 110 101 111 011 001
    - Iteration 2: 101 001 010 110 111 011
    - Iteration 3: 001 010 011 101 110 111

- **Now on n processors**
  - Each processor owns single k-bit number, each iteration
    - $low = \text{prefix\_scan}(\neg bit, sum)$
    - $high = n\text{-1\_backwards\_prefix\_scan}(bit, sum)$
    - $new\_idx = (bit == 0) : low \ ? high$
    - $b[new\_idx] = a[i]$
    - $\text{swap}(a,b)$
Another use for prefix sums: Parallel radix sort

- **Radix sort works bit-by-bit**
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    - **Iteration 0**: 101 111 010 011 110 001
    - **Iteration 1**: 010 110 101 111 011 001
    - **Iteration 2**: 101 001 010 110 111 011
    - **Iteration 3**: 001 010 011 101 110 111

- **Now on n processors**
  - Each processor owns single k-bit number, each iteration
    
    ```c
    low = prefix_scan(!bit, sum)
    high = n-1-backwards_prefix_scan(bit, sum)
    new_idx = (bit == 0) : low ? high
    b[new_idx] = a[i]
    swap(a, b)
    ```

  Show one example iteration!
Another use for prefix sums: Parallel radix sort

- Radix sort works bit-by-bit
  - Sorts k-bit numbers in k iterations
  - In each iteration $i$ stably sort all values by the $i$-th bit
  - Example, $k=1$:
    
    Iteration 0: 101 111 010 011 110 001
    Iteration 1: 010 110 101 111 011 001
    Iteration 2: 101 001 010 110 111 011
    Iteration 3: 001 010 011 101 110 111

- Now on $n$ processors
  - Each processor owns single k-bit number, each iteration
    
    $low = \text{prefix\_scan}(\neg bit, \text{sum})$
    $high = n-1\text{-backwards\_prefix\_scan}(bit, \text{sum})$
    $new\_idx = (bit == 0) : low \ ? \ high$
    $b[new\_idx] = a[i]$
    $\text{swap}(a,b)$

Show one example iteration!

Question: work and depth?
Oblivious graph algorithms

- Seems paradoxical but isn’t (may just not be most efficient)
  - Use adjacency matrix representation of graph – “compute with all zeros”
Oblivious graph algorithms

- Seems paradoxical but isn’t (may just not be most efficient)
  - Use adjacency matrix representation of graph – “compute with all zeros”

**Unweighted graph – binary matrix**

```
 0 1 1 0 0 0
0 0 0 0 1 1
0 0 0 0 0 1
0 0 1 0 0 0
0 0 0 1 0 0
0 0 0 0 1 0
```
Oblivious graph algorithms

- Seems paradoxical but isn’t (may just not be most efficient)
  - Use adjacency matrix representation of graph – “compute with all zeros”

Unweighted graph – binary matrix

Weighted graph – general matrix
Algebraic semirings

A semiring is an algebraic structure that

\[(+, *, 0, 1)\]

Boolean semiring: \([\{0,1\}, \lor, \land, 0, 1]\)

Tropical semiring: \([\mathbb{R} \cup \{\infty\}, \text{min}, +, \infty, 0]\) (also called min-plus semiring)
Algebraic semirings

A semiring is an algebraic structure that

- Has two binary operations called “addition” and “multiplication”

\[ , +, \ast, 0, 1 \]

Boolean semiring: \( \{0,1\}, \lor, \land, 0, 1 \)

Tropical semiring: \( \mathbb{R} \cup \{\infty\}, \min, +, \infty, 0 \) (also called min-plus semiring)
Algebraic semirings

A semiring is an algebraic structure that

- Has two binary operations called “addition” and “multiplication”
- Addition must be associative \((a+b)+c = a+(b+c)\) and commutative \((a+b=b+a)\) and have an identity element

\(, +, \ast, 0, 1\)

Boolean semiring: \(\{0,1\}, \lor, \land, 0, 1\)

Tropical semiring: \(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0\) (also called min-plus semiring)
Algebraic semirings

A semiring is an algebraic structure that
- Has two binary operations called “addition” and “multiplication”
- Addition must be associative ((a+b)+c = a+(b+c)) and commutative ((a+b=b+a)) and have an identity element
- Multiplication must be associative and have an identity element

\(, +, *, 0, 1)\)

Boolean semiring: \(\{0,1\}, \lor, \land, 0, 1\)

Tropical semiring: \((\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)\) (also called min-plus semiring)
A semiring is an algebraic structure that

- Has two binary operations called “addition” and “multiplication”
- Addition must be associative \((a+b)+c = a+(b+c)\) and commutative \((a+b=b+a)\) and have an identity element
- Multiplication must be associative and have an identity element
- Multiplication distributes over addition \((a*(b+c) = a*b+a*c)\) and multiplication by additive identity annihilates

\[ , +, *, 0, 1\]

*Boolean semiring:* \(\{0,1\}, \lor, \land, 0, 1\)

*Tropical semiring:* \((\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)\) (also called min-plus semiring)
A semiring is an algebraic structure that

- Has two binary operations called “addition” and “multiplication”
- Addition must be associative \(((a+b)+c = a+(b+c))\) and commutative \(((a+b=b+a))\) and have an identity element
- Multiplication must be associative and have an identity element
- Multiplication distributes over addition \((a*(b+c) = a*b+a*c)\) and multiplication by additive identity annihilates
- Semirings are denoted by tuples \((S, +, *, 0, 1)\)

**Boolean semiring**: \((\{0,1\}, \lor, \land, 0, 1)\)

**Tropical semiring**: \((\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)\) (also called min-plus semiring)
Algebraic semirings

, +, *, 0, 1)

A semiring is an algebraic structure that

- Has two binary operations called “addition” and “multiplication”
- Addition must be associative ((a+b)+c = a+(b+c)) and commutative ((a+b=b+a)) and have an identity element
- Multiplication must be associative and have an identity element
- Multiplication distributes over addition (a*(b+c) = a*b+a*c) and multiplication by additive identity annihilates
- Semirings are denoted by tuples (S, +, *, 0, 1)

“Standard” ring of rational numbers: (ℝ, +, *, 0, 1)

Boolean semiring: ({0,1}, ∨, ∧, 0, 1)

Tropical semiring: (ℝ ∪ {∞}, min, +, ∞, 0) (also called min-plus semiring)
Algebraic semirings

, ∧, 0, 1
, +, *, 0, 1

A semiring is an algebraic structure that

- Has two binary operations called “addition” and “multiplication”
- Addition must be associative ((a+b)+c = a+(b+c)) and commutative ((a+b=b+a)) and have an identity element
- Multiplication must be associative and have an identity element
- Multiplication distributes over addition (a*(b+c) = a*b+a*c) and multiplication by additive identity annihilates
- Semirings are denoted by tuples (S, +, *, 0, 1)

Boolean semiring: ({0,1}, ∨, ∧, 0, 1)

Boolean semiring: ({0,1}, ∨, ∧, 0, 1)

Tropical semiring: (ℝ ∪ {∞}, min, +, ∞, 0) (also called min-plus semiring)
Algebraic semirings

$\mathcal{U}\{\infty\}, \min, +, \infty, 0$ (also called min-plus semiring)

$\wedge, 0, 1$

$+, *, 0, 1$

A semiring is an algebraic structure that

- Has two binary operations called “addition” and “multiplication”
- Addition must be associative ($(a+b)+c = a+(b+c)$) and commutative ($(a+b=b+a)$) and have an identity element
- Multiplication must be associative and have an identity element
- Multiplication distributes over addition ($(a*(b+c) = a*b+a*c)$) and multiplication by additive identity annihilates
- Semirings are denoted by tuples $(S, +, *, 0, 1)$

Tropical semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$ (also called min-plus semiring)

Boolean semiring: $(\{0,1\}, \lor, \land, 0, 1)$

Tropical semiring: $(\mathbb{R} \cup \{\infty\}, \min, +, \infty, 0)$ (also called min-plus semiring)
Oblivious shortest path search

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>2</th>
<th>3</th>
<th>∞</th>
<th>∞</th>
<th>∞</th>
</tr>
</thead>
<tbody>
<tr>
<td>∞</td>
<td>0</td>
<td>∞</td>
<td>∞</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>∞</td>
<td>∞</td>
<td>0</td>
<td>∞</td>
<td>∞</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>∞</td>
<td>∞</td>
<td>4</td>
<td>0</td>
<td>∞</td>
<td>∞</td>
<td></td>
</tr>
<tr>
<td>∞</td>
<td>∞</td>
<td>∞</td>
<td>7</td>
<td>0</td>
<td>∞</td>
<td></td>
</tr>
<tr>
<td>∞</td>
<td>∞</td>
<td>∞</td>
<td>∞</td>
<td>8</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Oblivious shortest path search

- Construct distance matrix from adjacency matrix by replacing all off-diagonal zeros with $\infty$
Oblivious shortest path search

- Construct distance matrix from adjacency matrix by replacing all off-diagonal zeros with $\infty$
Oblivious shortest path search

- f size n to $\infty$ everywhere but zero at start vertex
- Initialize distance vector $d_0$ of size n to $\infty$ everywhere but zero at start vertex
Oblivious shortest path search

- $\infty, 0, \infty, \infty, \infty, \infty \ T \ \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, \infty$ $0, \infty, \infty, \infty \ T$
- $f$ size $n$ to $\infty$ everywhere but zero at start vertex
- Show evolution when multiplied!
Oblivious shortest path search

- $\infty, 0, \infty, \infty, \infty, \infty \ T \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty \infty, 0, \infty, \infty, \infty, \infty \infty, 0, \infty, \infty, \infty, \infty \infty, 0, \infty, \infty, \infty, \infty \infty, 0, \infty, \infty, \infty, \infty

- Show evolution when multiplied!

- SSSP can be performed with $n+1$ matrix-vector multiplications!
Oblivious shortest path search

- $\infty, 0, \infty, \infty, \infty, \infty T \infty, 0, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty T$
- $f$ size $n$ to $\infty$ everywhere but zero at start vertex
- Show evolution when multiplied!

- SSSP can be performed with $n+1$ matrix-vector multiplications!
  - Question: total work and depth?
Oblivious shortest path search

- $O(n^3 \cdot n \cdot \log n)$, $DD=O(n \cdot \log n)$
- $\infty, 0, \infty, \infty, \infty, \infty T \infty, 0, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty T$
- $f$ size $n$ to $\infty$ everywhere but zero at start vertex
- Show evolution when multiplied!

- SSSP can be performed with $n+1$ matrix-vector multiplications!
  - Question: total work and depth?
  - $W = O(n^3)$, $D = O(n \cdot \log n)$
Oblivious shortest path search

- $O(n^3 \log n)$, $DD=O(n^3 \log n)$
- $\infty, 0, \infty, \infty, \infty, \infty, T, 0, \infty, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty$; $\infty, 0, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty$
- $f$ size $n$ to $\infty$ everywhere but zero at start vertex
- Show evolution when multiplied!

- SSSP can be performed with $n+1$ matrix-vector multiplications!
  - Question: total work and depth?
  - Question: Is this good? Optimal?
Oblivious shortest path search

- \( E \in E + VVVV \log VVVV \)
- \( \mathcal{O}(n^3) \in \mathcal{O}(n^3 n \log n) \), \( DD = \mathcal{O}(nn \log nn) \)
- \( \infty, 0, \infty, \infty, \infty, \infty, T \infty, 0, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty \)
- \( 0, \infty, \infty, \infty, \infty, T \)
- \( f \text{ size } n \text{ to } \infty \text{ everywhere but zero at start vertex} \)

Show evolution when multiplied!

- SSSP can be performed with \( n+1 \) matrix-vector multiplications!
  - Question: total work and depth?
  - Question: Is this good? Optimal?
  - \( \text{Dijkstra} = \mathcal{O}(|E| + |V| \log |V|) \)
Oblivious shortest path search

- \( O(n^3 \log n) \), \( DD=O(O(n \log n)) \)
- \( E E E E + V V V V \log V V V V \)
- \( O(n^3 \log n) \), \( DD=O(nn \log n) \)

- \( \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty, \infty, \infty, 0, 0, \infty, 0, \infty, 0, \infty, \infty, \infty, \infty, \infty, \infty T \)

- \( f \) size \( n \) to \( \infty \) everywhere but zero at start vertex

Show evolution when multiplied!

SSSP can be performed with \( n+1 \) matrix-vector multiplications!
- Question: total work and depth?
- Question: Is this good? Optimal?

Dijkstra = \( O(|E| + |V| \log |V|) \)

Homework:
- Define a similar APSP algorithm with
  \( W = O(n^3 \log n), D = O(\log^2 n) \)
Oblivious connected components

Question: How could we compute the transitive closure of a graph?

- \((A + I)^n\) times with itself in the Boolean semiring!

- Why?
  
  Demonstrate that \((A + I)^2\) has 1s for each path of at most length 1

  By induction show that \((A + I)^k\) has 1s for each path of at most length \(k\)

- What is work and depth of transitive closure?
  
  Repeated squaring! \(W = O(n^3 \log n)\), \(D = O(\log^2 n)\)

- How to get to connected components from a transitive closure matrix?
  
  Each component needs unique label

  Create label matrix \(L_{ij} = j\) iff \((A_1)^{n}_{ij} = 1\) and \(L_{ij} = \infty\) otherwise

  For each row (vertex) perform min-reduction to determine its component label!

  Overall work and depth?

  \(W = O(n^3 \log n), D = O(\log^2 n)\)
Question: How could we compute the transitive closure of a graph?

- $A + I$ $n$ times with itself in the Boolean semiring!
- Why?
  
  \[ (A + I)^2 \] has 1s for each path of at most length 1
  
  By induction show that $(A + I)^k$ has 1s for each path of at most length $k$

- What is work and depth of transitive closure?
  
  - Repeated squaring! $W = O(n^3 \log n)$ $D = O(\log^2 n)$

- How to get to connected components from a transitive closure matrix?
  
  - Each component needs unique label
  - Create label matrix $L_{ij} = j$ iff $(A_I)^n_{ij} = 1$ and $L_{ij} = \infty$ otherwise
  - For each row (vertex) perform min-reduction to determine its component label!
  - Overall work and depth?
    
    $W = O(n^3 \log n), D = O(\log^2 n)$
Oblivious connected components

\((A + I)^n\) times with itself in the Boolean semiring!

Question: How could we compute the transitive closure of a graph?

- Multiply the matrix \((A + I)\) \(n\) times with itself in the Boolean semiring!
- Why?
  
  *Demonstrate that \((A + I)^2\) has 1s for each path of at most length 1*
  
  *By induction show that \((A + I)^k\) has 1s for each path of at most length \(k\)*

- What is work and depth of transitive closure?
  
  - Repeated squaring! \(W = O(n^3 \log n), D = O(\log^2 n)\)

- How to get to connected components from a transitive closure matrix?
  
  - Each component needs unique label
  - Create label matrix \(L_{ij} = j\) iff \((A_i)^n_{ij} = 1\) and \(L_{ij} = \infty\) otherwise
  - For each row (vertex) perform min-reduction to determine its component label!
  - Overall work and depth?
    
    \(W = O(n^3 \log n), D = O(\log^2 n)\)
Oblivious connected components

\[ A + I = A + 2 \ 2 \ A + I = A + I + I \ \text{has 1s for each path of at most length 1} \]

\[ A A + I \] \( n \) times with itself in the Boolean semiring!

**Question:** How could we compute the transitive closure of a graph?

- **Why?**
  
  Demonstrate that \( A + I = A + I + I \) has 1s for each path of at most length 1
  
  Demonstrate that \( (A + I)^2 \) has 1s for each path of at most length 1
  
  By induction show that \( (A + I)^k \) has 1s for each path of at most length \( k \)

- **What is work and depth of transitive closure?**
  
  - Repeated squaring! \( W = O(n^3 \log n) \) \( D = O(\log^2 n) \)

- **How to get to connected components from a transitive closure matrix?**
  
  - Each component needs unique label
  
  - Create label matrix \( L_{ij} = j \) iff \( (A_i)^n_{ij} = 1 \) and \( L_{ij} = \infty \) otherwise
  
  - For each row (vertex) perform min-reduction to determine its component label!

  **Overall work and depth?**
Oblivious connected components

\[ \text{II } A + I \quad A + I \ k \ k \ k \ A + I \ k \text{ has } 1\text{s for each path of at most length } k \]
\[ \text{II } A + I \quad A + I \ 2 \ 2 \ A + I \ 2 \text{ has } 1\text{s for each path of at most length } 1 \]
\[ AA + II \] \text{nn} \text{ times with itself in the Boolean semiring!} 

Question: How could we compute the transitive closure of a graph?

- Why?
  
  \text{By induction show that } A + I \ A + I \ k \text{ has } 1\text{s for each path of at most length } k

-Demonstrate that \((A + I)^2\) has 1s for each path of at most length 1

-By induction show that \((A + I)^k\) has 1s for each path of at most length \(k\)

- What is work and depth of transitive closure?
  - Repeated squaring! \(W = O(n^3 \log n)\) \(D = O(\log^2 n)\)

- How to get to connected components from a transitive closure matrix?
  - Each component needs unique label
  - Create label matrix \(L_{ij} = j\) iff \((A_t)^n\) \(i,j = 1\) and \(L_{ij} = \infty\) otherwise
  - For each row (vertex) perform min-reduction to determine its component label!
Oblivious connected components

\[ A + I \ k \ k k \ A + I \ k \] has 1s for each path of at most length \( k \)

\[ A + I \ 2 \ 2 \ A + I \ 2 \] has 1s for each path of at most length 1

\( AA + II \) \( nn \) times with itself in the Boolean semiring!

**Question:** How could we compute the transitive closure of a graph?

- **Why?**
  - By induction show that \( A + I \ A + I \ k \) has 1s for each path of at most length \( k \)

- **What is work and depth of transitive closure?**
  - By induction show that \( (A + I)^k \) has 1s for each path of at most length \( k \)

- **What is work and depth of transitive closure?**
  - Repeated squaring! \( W = O(n^3 \log n) \) \( D = O(\log^2 n) \)

- **How to get to connected components from a transitive closure matrix?**
  - Each component needs unique label
  - Create label matrix \( L_{ij} = j \) iff \( (A_j)^n_{ij} = 1 \) and \( L_{ij} = \infty \) otherwise
  - For each row (vertex) perform min-reduction to determine its component label!
Oblivious connected components

\[ O(n^3 \log n) DD = O(\log 2 \log 2 \log 2 \log 2 n) \]

Why? By induction show that \( A + I \times A \times I \times \ldots \times I \) has 1s for each path of at most length \( k \).

What is work and depth of transitive closure?

- Repeated squaring! \( W = O(n^3 \log n) D = O(\log^2 n) \)

What is work and depth of transitive closure?

- Repeated squaring! \( W = O(n^3 \log n) D = O(\log^2 n) \)

How to get to connected components from a transitive closure matrix?

- Each component needs unique label
- Create label matrix \( L_{ij} = j \) iff \( (A_k)^n_{ij} = 1 \) and \( L_{ij} = \infty \) otherwise

<table>
<thead>
<tr>
<th>i</th>
<th>j</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ +I \]
Oblivious connected components

\[ O( n^3 \log n) \quad DD = O( \log^2 n) \]

II A+I A+I k kk A+I k has 1s for each path of at most length k

II A+I A+I 2 2 A+I 2 has 1s for each path of at most length 1

\[ AA+II) n \]n times with itself in the Boolean semiring!

Question: How could we compute the transitive closure of a graph?

- Why?
  
  By induction show that \( A + I A + I k \) has 1s for each path of at most length k

- What is work and depth of transitive closure?
  
  Repeated squaring! \( W = O(n^3 \log n) \) \( D = O(\log^2 n) \)

- How to get to connected components from a transitive closure matrix?

- What is work and depth of transitive closure?
  
  Repeated squaring! \( W = O(n^3 \log n) \) \( D = O(\log^2 n) \)

- How to get to connected components from a transitive closure matrix?
  
  Each component needs unique label
  
  Create label matrix \( L_{ij} = j \) iff \((A_I)^n_{ij} = 1\) and \( L_{ij} = \infty \) otherwise
Oblivious connected components

\[ O(n^3 n n^3 n^3 n \log n) D D = O(\log 2 \log \log 2 \log 2 n) \]

II A+I A+I k k k A+I k has 1s for each path of at most length k
II A+I A+I 2 2 A+I 2 has 1s for each path of at most length 1
AA+II) nn times with itself in the Boolean semiring!

Question: How could we compute the transitive closure of a graph?

- Why?
  
  By induction show that A + I A + I k has 1s for each path of at most length k

- What is work and depth of transitive closure?
  
  Repeated squaring! \( W = O(n^3 \log n) D = O(\log^2 n) \)

- How to get to connected components from a transitive closure matrix?
  
  Each component needs unique label
  
  Repeated squaring! \( W = O(n^3 \log n) D = O(\log^2 n) \)

- How to get to connected components from a transitive closure matrix?
  
  Each component needs unique label
  
  Create label matrix \( L_{ij} = j \) iff \( (A_I)^n_{ij} = 1 \) and \( L_{ij} = \infty \) otherwise
Oblivious connected components

\[ jj \text{ iff } A I n ij AI n AI AIAAAAIIIAI A I A I n nn A I n AI n ij iiijj A I n iiijj L ij = \infty \text{ otherwise} \]

\[ O O(n 3 nn n 3 3 n 3 \log nn) DD = O O(\log 2 \log 2 \log 2 2 \log 2 2 nn) \]

\[ II A+I A+I k kk A+I k \text{ has 1s for each path of at most length } k \]

\[ II A+I A+I 2 2 A+I 2 \text{ has 1s for each path of at most length 1} \]

\[ AA+II) nn \text{ times with itself in the Boolean semiring!} \]

Question: How could we compute the transitive closure of a graph?

- Why?
  
  By induction show that \( A + I A + I k \text{ has 1s for each path of at most length } k \)

- What is work and depth of transitive closure?
  
  ▪ Repeated squaring! \( W = O(n^3 \log n) \) \( D = O(\log^2 n) \)

- How to get to connected components from a transitive closure matrix?
  
  ▪ Each component needs unique label
  ▪ Create label matrix \( L ij = ij j ij = j \text{ iff } (A_I)^n_{ij} = 1 \text{ and } L_{ij} = \infty \text{ otherwise} \)

- How to get to connected components from a transitive closure matrix?
Oblivious connected components

\[ jj \iff A I n ij A I n A I A I A A A I I I A I A I A I n nn A I n A I n i j i j j A I n \]
\[ i j j L i j = \infty \text{ otherwise} \]

\[ O O (n 3 nn n 3 n 3 n 3 \log nn) D D = O O (\log 2 \log 2 \log 2 2 \log 2 2 nn) \]

II A+I A+I k kk A+I k has 1s for each path of at most length \( k \)

II A+I A+I 2 2 A+I 2 has 1s for each path of at most length 1

AA+II) nn times with itself in the Boolean semiring!

Question: How could we compute the transitive closure of a graph?

- Why?
  - By induction show that \( A + I A + I k \) has 1s for each path of at most length \( k \)

- What is work and depth of transitive closure?
  - Repeated squaring! \( W = O(n^3 \log n) \) \( D = O(\log^2 n) \)

- How to get to connected components from a transitive closure matrix?
  - Each component needs unique label
  - For each row (vertex) perform min-reduction to determine its component label!

- How to get to connected components from a transitive closure matrix?
Oblivious connected components

\[ jj \text{ iff } A I n ij A I n A I A I A A I II A I A I A I n \text{ nn } A I n A I n ij ij ij II A I \]

\[ iijj L ij = \infty \text{ otherwise} \]

\[ OO( n 3 \text{ nn } n 3 3 n 3 \log \text{ nn} ) DD = OO( \log 2 \log 2 \log 2 \log 2 \log \text{ nn}) \]

\[ II A + I A + I k k k A + I k \text{ has } 1\text{s for each path of at most length } k \]

\[ II A + I A + I 2 2 A + I 2 \text{ has } 1\text{s for each path of at most length } 1 \]

\[ AA + II \text{ } \text{nn} \text{ times with itself in the Boolean semiring!} \]

Question: How could we compute the transitive closure of a graph?

- Why?
  By induction show that \( A + I A + I k \) has 1s for each path of at most length \( k \)

- What is work and depth of transitive closure?
  - Repeated squaring! \( W = O(n^3 \log n) \) \( D = O(\log^2 n) \)

- How to get to connected components from a transitive closure matrix?
  - Each component needs unique label
  - For each row (vertex) perform min-reduction to determine its component label!
  - Overall work and depth?

- How to get to connected components from a transitive closure matrix?
  - Each component needs unique label
Oblivious connected components

\[ O(n^3 \log n) \quad D = O(\log 2 \log \log 2 \log 2 \log n) \]

\[ I + A^k \quad \text{k has 1s for each path of at most length k} \]

\[ I + A^1 \quad \text{2 has 1s for each path of at most length 1} \]

**Question**: How could we compute the transitive closure of a graph?
- **Why?**
  - By induction show that \( A + I \quad A + I \quad k \) has 1s for each path of at most length k
- **What is work and depth of transitive closure?**
  - Repeated squaring! \( W = O(n^3 \log n) \quad D = O(\log^2 n) \)
- **How to get to connected components from a transitive closure matrix?**
  - Each component needs unique label
  - For each row (vertex) perform min-reduction to determine its component label!
  - Overall work and depth?
    - \( W = O(n^3 \log n) \quad D = O(\log^2 n) \)
Oblivious connected components

\[ \mathcal{O}(n^3 \log n), \mathcal{D} = \mathcal{O}(\log 2 \log 2 \log 2 \log 2 \log 2 n) \]

\[ \mathcal{O}(n^3 \log n), \mathcal{D} = \mathcal{O}(\log 2 \log 2 \log 2 \log 2 \log 2 n) \]

\( j \leftrightarrow A \iff A(n)A \| A \| A \| A \| A \| A \| A \| A \| A \| A \| A \| A \| A \| A \| A \| A \| A \]

\( i \) otherwise

\[ \mathcal{O}(n^3 \log n), \mathcal{D} = \mathcal{O}(\log 2 \log 2 \log 2 \log 2 \log 2 n) \]

\( II \ A + I \ A + I \ k \) has 1s for each path of at most length \( k \)

\( II \ A + I \ A + I \ 2 \ 2 \ A + I \ 2 \) has 1s for each path of at most length 1

\( AA + II \) \( n \) times with itself in the Boolean semiring!

**Question:** How could we compute the transitive closure of a graph?

- **Why?**
  
  By induction show that \( A + I \ A + I \ k \) has 1s for each path of at most length \( k \)

- **What is work and depth of transitive closure?**
  
  - Repeated squaring: \( W = O(n^3 \log n) \) \( D = O(\log^2 n) \)

- **How to get to connected components from a transitive closure matrix?**
  
  - Each component needs unique label
  
  - For each row (vertex) perform min-reduction to determine its component label!

\( W = O(n^3 \log n), D = O(\log^2 n) \)
Many if not all graph problems have oblivious or tensor variants!

\[ < |V|^2 / \log |V| \]
Many if not all graph problems have oblivious or tensor variants!

- Not clear whether they are most efficient
  - Efforts such as GraphBLAS exploit existing BLAS implementations and techniques

\[ < |V|^2 / \log |V| \)
Many if not all graph problems have oblivious or tensor variants!

- Not clear whether they are most efficient
  - Efforts such as GraphBLAS exploit existing BLAS implementations and techniques

- Generalizations to other algorithms possible
  - Can everything be modeled as tensor computations on the right ring?
  - E. Solomonik, TH: “Sparse Tensor Algebra as a Parallel Programming Model”
  - Much of machine learning/deep learning is oblivious

\[ V^2 / \log |V| \]
Many if not all graph problems have oblivious or tensor variants!

- \( V \cdot 2^V V V V \cdot 2^V 2 \cdot V / \log|V^V| \)
- *Not clear whether they are most efficient*
  - Efforts such as GraphBLAS exploit existing BLAS implementations and techniques

- **Generalizations to other algorithms possible**
  - Can everything be modeled as tensor computations on the right ring?
  - E. Solomonik, TH: “Sparse Tensor Algebra as a Parallel Programming Model”
  - Much of machine learning/deep learning is oblivious

- **Many algorithms get non-oblivious though**
  - All sparse algorithms are data-dependent!
    - *May recover some of the lost efficiency by computing zeros!*
Many if not all graph problems have oblivious or tensor variants!

- $V^2 V V V V 2 V^2 2 V^2 /\log |VV|$
- Not clear whether they are most efficient
  - Efforts such as GraphBLAS exploit existing BLAS implementations and techniques

- Generalizations to other algorithms possible
  - Can everything be modeled as tensor computations on the right ring?
  - E. Solomonik, TH: “Sparse Tensor Algebra as a Parallel Programming Model”
  - Much of machine learning/deep learning is oblivious

- Many algorithms get non-oblivious though
  - All sparse algorithms are data-dependent!
    - May recover some of the lost efficiency by computing zeros!

- Now moving to non-oblivious 😊