

60007

Theory and Practice of
Concurrent Programming
Imperial College London

Contents

1	Introduction	3
1.1	Course Structure & Logistics	3
1.1.1	Structure	3
1.1.2	Extra Materials	3
1.2	Preface for Concurrency	4
1.2.1	Moore's Law	4
1.2.2	Concurrency Difficulties	5
1.2.3	OS Concepts	5
2	Concurrency In C++	6
2.1	Threads	6
2.1.1	Vectors of Threads	7
2.1.2	This Thread	8
2.2	Locks	9
2.2.1	Using Mutexes	10
2.2.2	Lock Guards	11
2.3	Race Conditions in C++	14
2.3.1	Thread Sanitiser	15
2.4	Condition Variables	16
2.4.1	Using Condition Variables	17
2.5	Atomics	18
2.5.1	Atomic Template Class	18
2.5.2	Atomic Integral Types	19
2.6	Memory Order	20
2.7	Message Passing	21
2.7.1	Expensive Approach	21
2.7.2	Incorrect Approach	22
2.7.3	Release-Acquire Consistency	22
3	Mutexes	23
3.1	Spinlocks	23
3.1.1	Test-and-Set Spinlock	23
3.1.2	Local Spinning	24
3.1.3	Fixed Backoff	24
3.1.4	Exponential Backoff	25
3.2	Ticket Locks	26
3.3	Futexes	26
3.3.1	Futex Operations	27
3.3.2	Futex Implementation	27
4	Operational Semantics	28
4.1	Formal Properties	28
4.2	Shared-Memory Concurrency	29
4.2.1	Read-Modify-Write	29
4.2.2	Consistency/Memory Models	29
4.3	Sequential Consistency	30
4.3.1	Configurations	30
4.3.2	Transitions	31
4.3.3	Concurrent Program Transitions	31

4.3.4	Storage Transitions	32
4.3.5	Combining Operational Semantics	32
4.3.6	Traces	33
4.3.7	Properties of Sequential Consistency	33
4.4	Total Store Ordering	33
4.4.1	Storage Transitions	35
4.4.2	Traces	36
4.4.3	Properties of Total Store Ordering	36
5	Declarative Semantics	37
5.1	Label and Event Notation	37
5.2	Consistency Predicates	39
5.3	Sequential Consistency	40
5.4	Total Store Order	43
5.5	Coherent	44
5.5.1	Bad Patterns	45
5.6	Atomicity	46
5.7	Release/Acquire	46
5.8	Ordering Models	47
6	Concurrent Objects	48
6.1	Concurrent Queues	48
6.1.1	Circular Queue	48
6.1.2	Lock Based Queue	49
6.1.3	Wait Free 2-Thread Queue	49
6.2	Sequential and Concurrent Objects	49
6.2.1	Sequential Specifications	49
6.2.2	Concurrent Specifications	49
6.3	Formal Model of Executions	52
6.4	(.	54
7	Credit	55

Chapter 1

Introduction

1.1 Course Structure & Logistics

1.1.1 Structure



Dr Azalea Raad



Prof Alastair Donaldson

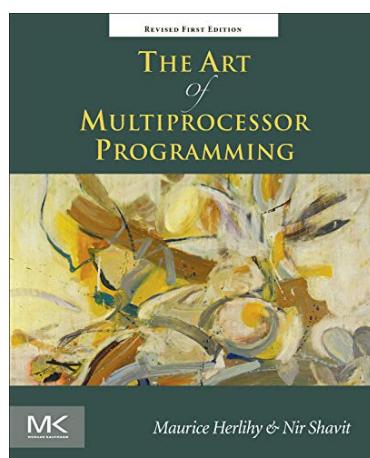
Theory For weeks 2 → 5:

- Intro to synchronisation paradigms (mutual exclusion, readers-writers, producer-consumer)
- Low-level concurrent semantics (sequential consistency, Intel-x86)
- High-level concurrent semantics (concurrent objects, linearisability)
- Transactional memory (serialisability)

Practical For weeks 5 → 8:

- Threads and locks in C++
- Implementing locks
- Concurrency in Haskell
- Race-free concurrency in Rust
- Dynamic data-race detection

1.1.2 Extra Materials



The Art of Multiprocessor Programming
About 65% of the theory course.

1.2 Preface for Concurrency

1.2.1 Moore's Law

Moore's Law

Definition 1.2.1

An empirical (supported by observation) law that states the density of transistors in an integrated circuit will double approximately every two years.

- The observation is named after Gordon Moore (co-founder and later CEO of Intel).
- This law no longer holds, and sequential performance improvements have declined.

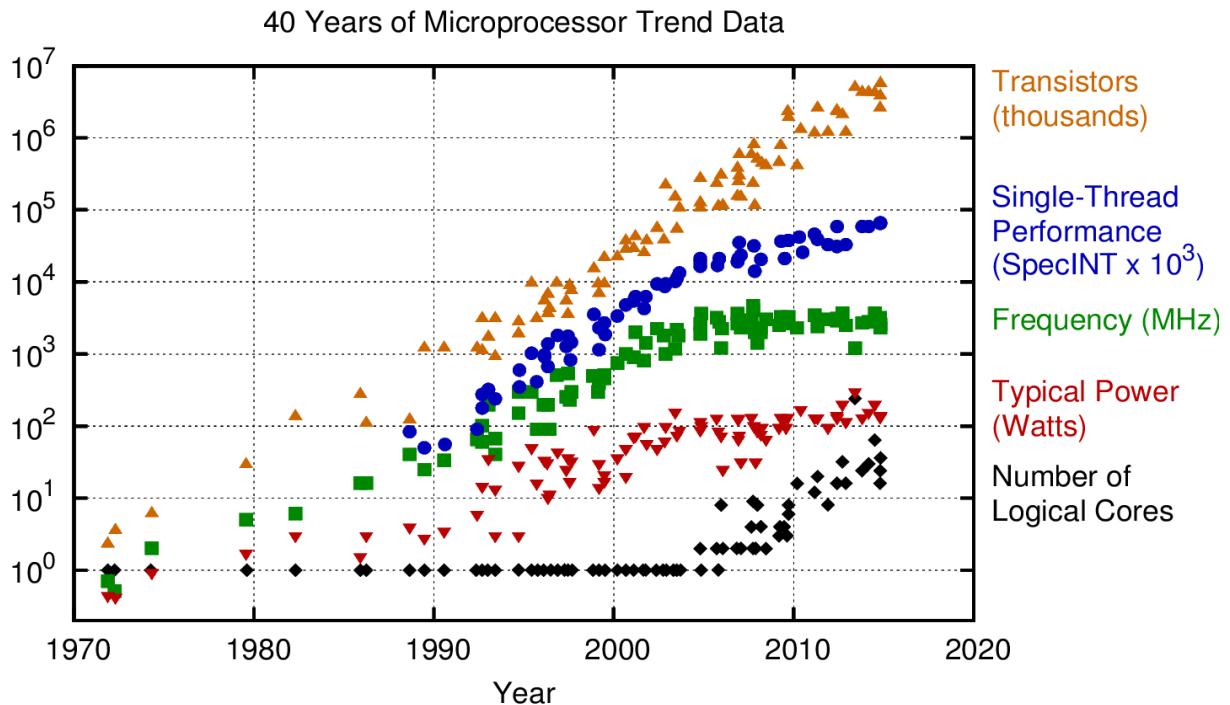
Dennard/MOSFET Scaling

Definition 1.2.2

$$\text{Power} \propto \text{Transistor Size}$$

A scaling law stating that as transistor density increases, the power requirements stay constant.

- Increasing transistor density results in power staying constant (less power per transistor) and lower circuit delay.
- This allows for higher switching frequency \Rightarrow higher clock frequencies \Rightarrow better sequential performance).



The performance improvements typically expected yearly (moore's law and Dennard scaling) no longer apply.

- Sequential (Single-Thread) performance improvements have declined.
- Parallelism is being exploited to improve performance (uniprocessors are virtually extinct).
- Shared-memory multiprocessor systems have lost out to multicore processors.

$$S_{\text{latency}}(s) = \frac{1}{(1-p) + \frac{p}{s}} \text{ where } p = \text{parallel portion and } s = \text{threads}$$

Amdahl's law describes the speedup of a program, associated with the number of threads.

- Can be applied to other resources.
- Versions of the equation exist for different proportions using different numbers of threads.
- As the number of threads increases the sequential part of the program becomes a bottleneck.

1.2.2 Concurrency Difficulties

Writing correct, concurrent code is difficult.

A potential for a situation where the result of a program depends on the non-deterministic timing or interleaving of threads.

- Where multiple threads access data (non-atomically) and at least one writes.
- Where a lack of enforced ordering on some events causes differing results (e.g output to user)

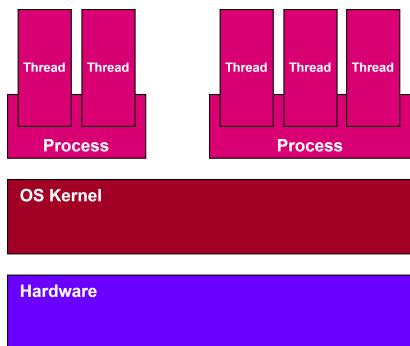
Race conditions can be intentional, where the result of the program is intended to be based off some non-deterministic input.

- Which thread gets to write first?
- Which process is allowed to write to a file?

- A process can have multiple threads executing in parallel.
- Cannot determine at compile time the relative speed of execution of threads (many delays are unpredictable; cache misses, page faults, interrupts).
- Cannot predict how long threads will be blocked (e.g I/O) or when threads will be scheduled (or use up their time quantum).

Hence we must use synchronisation mechanisms to regulate accesses to shared data that can result in a race condition.

1.2.3 OS Concepts



- Operating system provides process and thread abstractions.
- A process contains one or more threads (streams of instructions being executed).
- A process has its own address space, all threads in the process share this address space.
- The OS kernel contains a scheduler which schedules processes & their threads.

Chapter 2

Concurrency In C++

2.1 Threads

To interact with threads the `thread` header must be included.

- It provides a standard, implementation independent, interface for handling threads.
- Provides the `std::thread` class

```
#include <thread>

namespace std {
    class thread {
public:
    // types
    class id;
    using native_handle_type = /* implementation-defined */;

    // construct/copy/destroy
    thread() noexcept;

    // Constructor takes a function to start from, and its arguments (all type checked)
    template<class F, class... Args> explicit thread(F&& f, Args&&... args);

    // Destructor (terminates current thread if the thread has not been joined)
    ~thread();

    // Attempting to copy a thread is not allowed. Hence delete ensures no compile.
    thread(const thread&) = delete;

    // Can create thread from a thread r-value (copy)
    thread(thread&&) noexcept;

    // Attempting to copy a thread (via an immutable reference).
    // This is not allowed, so if this operator is used it will not compile.
    thread& operator=(const thread&) = delete;

    // Assign a thread from an (r value - e.g expression, literal) reference
    thread& operator=(thread&&) noexcept;

    // members
    void swap(thread&) noexcept;
    bool joinable() const noexcept;

    // Wait for this thread to terminate.
    void join();
```

```

// Allow the thread to continue executing after the thread handler (this)
// is destroyed
void detach();

// Get the unique id of the thread
id get_id() const noexcept;

native_handle_type native_handle();

// static members
static unsigned int hardware_concurrency() noexcept;
};

}

```

Lambda

Definition 2.1.1

A lambda is a small function that can be defined in an expression, capture values in its scope (and above), and be passed as a value.

```

// [captures] (arguments) {body}

// a basic lambda with no captures
auto my_lambda = [] (int a, int b) -> int {return a + b;};

// using the lambda
int c = my_lambda(1, 2);

auto another_lambda = [c&] (int d) {return c + d;};

```

We can construct using `std::thread`'s constructors.

```

// idiomatic constructor
std::thread my_thread(StartFunction, arg1, arg2, ...)

// call constructor and assign
std::thread my_thread = std::thread(StartFunction, arg1, arg2, ...)
auto my_thread = std::thread(StartFunction, arg1, arg2, ...)

// pass lambda as function
std::thread my_thread(StartFunction, arg1, arg2, ...)

```

When passing arguments to the thread, if these are by reference, a `std::ref` or `std::cref` must be used.

Reference this!

Example Question 2.1.1

Given some function `static void some_func(const int& a)` create a thread to take a reference to the number 42.

```

int a = 42;
std::thread my_thread(some_func, std::cref(a));
my_thread.join();

```

2.1.1 Vectors of Threads

When adding an object to a container (e.g a vector) we want to avoid allocating the object, and then moving it into the container.

- Some objects may not be movable/copyable.
- The object should be allocated within the container.

For this we can use emplacement.

```
template< class... Args >
void emplace_back( Args&&... args );
```

Emplace

Example Question 2.1.2

Given some function `static void some_func()` create 10 threads and append to the vector using `std::vector::push_back` and another 10 with `std::vector::emplace`.

```
std::vector<std::thread> threads;

for (int i; i < 10; i++) {
    threads.push_back(std::thread(some_func));
}

for (int i; i < 10; i++) {
    threads.emplace_back(some_func);
}

for (auto& t : threads) {
    t.join();
}
```

2.1.2 This Thread

The threads header also provides functionality for interacting with the current thread.

```
#include <compare>

namespace std {
    class thread;

    void swap(thread& x, thread& y) noexcept;

    // class jthread
    class jthread;

    // methods for interacting with the current thread
    namespace this_thread {
        thread::id get_id() noexcept;

        // indicates another thread should be scheduled (e.g long wait expected)
        void yield() noexcept;

        // Sleeping, generic for
        template<class Clock, class Duration>
        void sleep_until(const chrono::time_point<Clock, Duration>& abs_time);

        //
        template<class Rep, class Period>
        void sleep_for(const chrono::duration<Rep, Period>& rel_time);
    }
}
```

Clock watching

Example Question 2.1.3

Create program that prints the thread id, and sleeps.

```
#include <thread>
#include <iostream>
#include <chrono>
```

```

int main() {
    using namespace std::chrono_literals; // to use the ms syntax

    std::cout << std::this_thread::get_id() << " will sleep now!" << std::endl;
    std::this_thread::sleep_for(200ms);

    std::cout << std::this_thread::get_id() << " has awoken!" << std::endl;
}

```

2.2 Locks

RAII

Definition 2.2.1

Resource Acquisition Is Initialization (also called Scope-Bound Resource Management and Constructor Acquires, Destructor Release) is where a resource's allocation and release is bound to the lifetime of an object.

- a resource may be the memory allocated to an object, or resources such as os provided file handlers.
- When the object goes out of scope (e.g the variable owning the object is destroyed) the resource is released.
- In C++, when a variable goes out of scope, the destructor of the contained object is called, so the destructor must release the resources.
- This concept is heavily embedded in Rust. Lifetimes are a major part of the type system, and ownership rules are enforced by the compiler.
- RAII is used for smart pointers such as Rc in rust or std::shared_ptr.

```

static void my_scope() {
    MyClass my_object; // initialised, default constructor called

    // ... do some stuff ...

    return; // destructor my_object.~MyClass() called.
}

```

The mutex header contains locks for synchronisation.

```

namespace std {
    class mutex; // A regular lock
    class recursive_mutex; // reentrant/recursive lock
    class timed_mutex; // A mutex with timeout
    class recursive_timed_mutex; // A recursive mutex with timeout

    /* used to set the locking strategy when using lock guards
     * e.g create guard (that releases lock on destruction) assuming
     * lock is held.
     */
    struct defer_lock_t { explicit defer_lock_t() = default; }; // do not acquire ownership
    struct try_to_lock_t { explicit try_to_lock_t() = default; }; // try to acquire ownership (no block)
    struct adopt_lock_t { explicit adopt_lock_t() = default; }; // assume calling thread has ownership

    inline constexpr defer_lock_t defer_lock {};
    inline constexpr try_to_lock_t try_to_lock {};
    inline constexpr adopt_lock_t adopt_lock {};

    // A RAII like mechanism that releases the lock it guards when destroyed.
    template<class Mutex> class lock_guard;

    // A RAII style lock guard, when taking ownership of multiple locks it attempts
    // deadlock avoidance.
}

```

```

template<class... MutexTypes> class scoped_lock;

// A movable lock guard.
template<class Mutex> class unique_lock;

template<class Mutex>
void swap(unique_lock<Mutex>& x, unique_lock<Mutex>& y) noexcept;

// attempts to acquire locks from references provided, returns index (in args) of lock
// that could not be acquired.
template<class L1, class L2, class... L3> int try_lock(L1&, L2&, L3&...);

// Acquire one or more locks (blocking) and use deadlock avoidance.
template<class L1, class L2, class... L3> void lock(L1&, L2&, L3&...);

struct once_flag;

template<class Callable, class... Args>
void call_once(once_flag& flag, Callable&& func, Args&&... args);
}

```

2.2.1 Using Mutexes

```

namespace std {
class mutex {
public:

    // Constructor initialises mutex as unlocked. It is a constexpr
    // as can determine all fields at compile time.
    constexpr mutex() noexcept;

    // Destructor, undefined behaviour if the mutex is held by a thread.
    ~mutex();

    // Cannot create mutex from another, or use assignment to move a mutex.
    mutex(const mutex&) = delete;
    mutex& operator=(const mutex&) = delete;

    void lock();
    bool try_lock();
    void unlock();

    using native_handle_type = /* implementation-defined */;
    native_handle_type native_handle();
};

}

```

Locked Out

Example Question 2.2.1

Create a mutex to protect a counter, and use 100 threads to increment the counter 10 times each. Add a wait of 1ms between each increment and only lock for each increment.

```

#include <thread>
#include <iostream>
#include <mutex>
#include <vector>
#include <chrono>

int cnt;
std::mutex cnt_lock;

```

```

static void increment_cnt() {
    for (int i = 0; i < 10; i++) {
        std::this_thread::sleep_for(std::chrono::milliseconds(1));
        cnt_lock.lock();
        cnt++;
        cnt_lock.unlock();
    }
}

int main() {
    std::vector<std::thread> threads;

    for (int i = 0; i < 100; i++) {
        threads.emplace_back(increment_cnt);
    }

    for (auto& t : threads) {
        t.join();
    }

    std::cout << "The counter is: " << cnt << std::endl;
}

```

2.2.2 Lock Guards

We can use `scoped_lock`, `unique_lock` or `lock_guard` to link the time the lock is held to the lifetime of the lock guard object.

- Each has slight differences, separate implementations are provided rather than using complex template magic.
- Deadlock avoidance is used to ensure all threads acquire and release locks in the same order.

Scoped Lock

```

namespace std {
    template<class... MutexTypes>
    class scoped_lock {
public:
    using mutex_type = Mutex; // If MutexTypes... consists of the single type Mutex

    explicit scoped_lock(MutexTypes&... m);
    explicit scoped_lock(adopt_lock_t, MutexTypes&... m);
    ~scoped_lock();

    scoped_lock(const scoped_lock&) = delete;
    scoped_lock& operator=(const scoped_lock&) = delete;

private:
    tuple<MutexTypes&...> pm; // exposition only
    };
}

```

- Constructed from one or more mutexes.
- Locks all mutexes on construction.
- Unlocks all mutexes on destruction.

Does not support deferred locking, early unlocking or ownership transfer (with `std::move`).

```

#include <mutex>
#include <iostream>

std::mutex m1, m2;

static void some_fun() {
    std::scoped_lock lock(m1, m2); // acquire lock on m1 and m2 (or any number of locks)
    std::cout << "Critical region here" << std::endl;
}

```

Unique Lock

```

namespace std {
    template<class Mutex>
    class unique_lock {
public:
    using mutex_type = Mutex;

    // construct/copy/destroy
    unique_lock() noexcept;
    explicit unique_lock(mutex_type& m);

    // locking strategies
    unique_lock(mutex_type& m, defer_lock_t) noexcept;
    unique_lock(mutex_type& m, try_to_lock_t);
    unique_lock(mutex_type& m, adopt_lock_t);

    //

    template<class Clock, class Duration>
    unique_lock(mutex_type& m, const chrono::time_point<Clock, Duration>& abs_time);
    template<class Rep, class Period>
    unique_lock(mutex_type& m, const chrono::duration<Rep, Period>& rel_time);
    ~unique_lock();

    unique_lock(const unique_lock&) = delete;
    unique_lock& operator=(const unique_lock&) = delete;

    unique_lock(unique_lock&& u) noexcept;
    unique_lock& operator=(unique_lock&& u);

    // locking
    void lock();
    bool try_lock();

    template<class Rep, class Period>
    bool try_lock_for(const chrono::duration<Rep, Period>& rel_time);
    template<class Clock, class Duration>
    bool try_lock_until(const chrono::time_point<Clock, Duration>& abs_time);

    void unlock();

    // modifiers
    void swap(unique_lock& u) noexcept;
    mutex_type* release() noexcept;

    // observers
    bool owns_lock() const noexcept;
    explicit operator bool () const noexcept;
    mutex_type* mutex() const noexcept;
}

```

```

private:
    mutex_type* pm;           // exposition only
    bool owns;                // exposition only
};

template<class Mutex>
void swap(unique_lock<Mutex>& x, unique_lock<Mutex>& y) noexcept;
}

```

- Constructed from one mutex.
- Locks mutex on construction by default, but can have locking deferred.
- Allows for unlocking and relocking.
- If mutex held on destruction, unlocks.
- Can transfer lock ownership with `std::move`.

Only works for a single mutex.

Scoped out

Example Question 2.2.2

Create a basic implementation of defer that could be used for a scoped lock.

```

#include <mutex>
#include <iostream>
#include <functional>

class Defer {
private:
    std::function<void(void)> function_;

public:
    Defer(std::function<void(void)> fun) : function_(fun) {}
    ~Defer() {
        function_();
    }
};

int main() {
    std::mutex m;

    Defer lock([&m] () {
        m.unlock();
        std::cout << "Unlocking" << std::endl;
    });

    std::cout << "lets do some racey stuff here" << std::endl;
}

```

We could also implement this pattern in rust. As mutexes already work this way in rust, we create a dummy mutex struct to use.

```

#[feature(fn_traits)]
struct Defer<F: FnMut()>(F);

impl<F: FnMut()> Drop for Defer<F> {
    fn drop(&mut self) {
        self.0()
    }
}

```

```

fn main() {
    let mut m = Mutex();
    m.lock();
    let _d = Defer(|| m.unlock());
    println!("lets do some racey stuff here")
}

```

2.3 Race Conditions in C++

Data Race

Definition 2.3.1

A data race is a race condition on the value of some data shared between threads.

- Distinct threads access a memory location.
- At least one thread modifies the location.
- At least one of the accesses is non-atomic (allows for operations of other threads to be interleaved)
- Accesses are not ordered by synchronisation (e.g for mutual exclusion)

Data races are value-oblivious, meaning a data race is present even if value of some shared data is not affected.

- e.g Two threads write the same value to the same place.
- e.g one thread stores the same value, another thread reads.

Always a bug, considered an unintentional race condition.

Synchronisation is achieved via:

- Mutexes
- Acquire load from release store
- sequentially consistent load from sequentially consistent store

Undefined Behaviour

Definition 2.3.2

"Anything at all can happen; the Standard imposes no requirements. The program may fail to compile, or it may execute incorrectly (either crashing or silently generating incorrect results), or it may fortuitously do exactly what the programmer intended." - C FAQ

- Programmer must avoid relying on undefined behaviour.
- Different compilers implementing the specification can do anything with undefined behaviour.
- Allows compilers to do more optimisation (fewer guarantees to satisfy).
- Among the most cited language design issues with C++.

The behaviour of a C++ program on some input is undefined if a data race can occur. This means specification is saying a program with a data race can do *anything*, there are no guarantees (even that the result depends on the outcome of the race).

Compilers typically optimise on the assumption there is no undefined behaviour.

- If there is no undefined behaviour, then assuming none is fine.
- If there is undefined behaviour, the language specification says *anything goes* and hence any output is valid.

```

#include <thread>

static void set_x(int& x) {
    x = 1;
}

```

```

static void wait_x(int& x) {
    while (x == 0);
}

int main() {
    int x = 0;
    std::thread t1(set_x, std::ref(x));
    std::thread t2(wait_x, std::ref(x));
    t1.join();
    t2.join();
}

```

Here the loop in `wait_x` can be optimised.

```

static void wait_x(int& x) {
    int temp_register = r;
    while (temp == 0);
}

```

```

static void wait_x(int& x) {
    // terminate thread
}

```

1. `x` is a non-atomic variable
2. if another thread modified `x`, then there would be a data race.
3. A data race is undefined behaviour

Place copy of `x` into a register and compare using this.

1. An infinite loop with no side effects is undefined behaviour.
2. Can assume it is *dead code* and remove.

Dead code can be removed.

2.3.1 Thread Sanitiser

A sanitiser to automatically detect data races.

- Available in clang++ and g++ compilers.
- Enabled with `-fsanitize=thread` and add debug symbols with `-g`.

2.4 Condition Variables

Condition Variable	Definition 2.4.1
<p>A condition that can be waited on, and notified.</p> <ul style="list-style-type: none">• Threads can wait on the condition to be signalled.• Can be used to construct a monitor.• In languages without a monitor construct, an explicit lock is required. <pre>#include <semaphore> #include <mutex> #include <deque> #include <cassert> class condition_variable { public: // delete copy constructors condition_variable(const condition_variable&) = delete; condition_variable& operator=(const condition_variable&) = delete; void notify_all(std::unique_lock<std::mutex> monitor_lock) { assert(monitor_lock.owns_lock()) for (auto& sema : wait_semas_) { sema.release(); } wait_semas_.clear(); } void notify_one(std::unique_lock<std::mutex> monitor_lock) { assert(monitor_lock.owns_lock()) wait_semas_.pop_front().release(); } void wait(std::unique_lock<std::mutex> monitor_lock) { assert(monitor_lock.owns_lock()) std::counting_semaphore wait_sema(0); wait_semas_.push_back(std::ref(wait_sema)); monitor_lock.release(); wait_sema.acquire(); monitor_lock.acquire(); } private: std::deque<std::ref<std::counting_semaphore>> wait_semas_; }; }</pre>	Definition 2.4.1

```
#include <condition_variable>

namespace std {
    class condition_variable;
    class condition_variable_any;

    void notify_all_at_thread_exit(condition_variable& cond, unique_lock<mutex> lk);

    enum class cv_status { no_timeout, timeout };
}
```

2.4.1 Using Condition Variables

The `std::condition_variable` class is as follows:

```
namespace std {
    class condition_variable {
public:
    condition_variable();
    ~condition_variable();

    // delete copy constructors
    condition_variable(const condition_variable&) = delete;
    condition_variable& operator=(const condition_variable&) = delete;

    // signal a condition variable
    void notify_one() noexcept;
    void notify_all() noexcept;

    // The current thread waits on the condition variable (until signalled),
    // using the (acquired) lock to synchronise
    void wait(unique_lock<mutex>& lock);

    // Wait on a predict using the provided mutex using the (acquired) lock
    // to synchronise
    template<class Pred>
    void wait(unique_lock<mutex>& lock, Pred pred);

    // wait until time
    template<class Clock, class Duration>
    cv_status wait_until(unique_lock<mutex>& lock,
                        const chrono::time_point<Clock, Duration>& abs_time);
    template<class Clock, class Duration, class Pred>
    bool wait_until(unique_lock<mutex>& lock,
                   const chrono::time_point<Clock, Duration>& abs_time, Pred pred);

    // wait for time
    template<class Rep, class Period>
    cv_status wait_for(unique_lock<mutex>& lock,
                      const chrono::duration<Rep, Period>& rel_time);
    template<class Rep, class Period, class Pred>
    bool wait_for(unique_lock<mutex>& lock,
                  const chrono::duration<Rep, Period>& rel_time, Pred pred);

    using native_handle_type = /* implementation-defined */;
    native_handle_type native_handle();
};

}
```

Wait on Signal

1. Associated a `std::mutex` with the condition variable.
2. Acquire a lock on the mutex with a unique lock.
3. Call wait with the lock.

The thread will block until the condition variable is signalled.

```
#include <mutex>
#include <condition_variable>

std::mutex m;
std::condition_variable cond;

static void some_func() {
    std::unique_lock<std::mutex> lock(m);
    cond.wait(lock);
}
```

Wait on predicate

1. Associated a `std::mutex` with the condition variable.
2. Acquire a lock on the mutex with a unique lock.
3. Call wait with a predicate.

Immediately returns if the predicate is true. Otherwise blocks, when the condition variable is signalled, the predicate will be checked, if true the thread returns, otherwise the thread is blocked again.

```
#include <mutex>
#include <condition_variable>

std::mutex m;
std::condition_variable cond;

static void some_func() {
    std::unique_lock<std::mutex> lock(m);
    cond.wait(lock, [...]() -> bool {...});
}
```

2.5 Atomics

Defined in the `atomic` header. Allow for the construction of atomic variables for integral and arbitrary types (that are TriviallyCopyable, CopyConstructible and CopyAssignable).

- For integral types atomic operations offer lower overhead alternatives for protecting small amounts of data than using a mutex.
- Atomic declarations prevent data races. This can be useful in declaring an intentional race condition (to prevent undefined behaviour)

2.5.1 Atomic Template Class

```
namespace std {
    template<class T> struct atomic {
        using value_type = T;

        static constexpr bool is_always_lock_free = /* implementation-defined */;
        bool is_lock_free() const volatile noexcept;
        bool is_lock_free() const noexcept;

        // operations on atomic types
        constexpr atomic() noexcept(is_nothrow_default_constructible_v<T>);
        constexpr atomic(T) noexcept;
        atomic(const atomic&) = delete;
        atomic& operator=(const atomic&) = delete;
        atomic& operator=(const atomic&) volatile = delete;

        // load the value (make a non-atomic copy of the current value)
        T load(memory_order = memory_order::seq_cst) const volatile noexcept;
        T load(memory_order = memory_order::seq_cst) const noexcept;

        // implicit conversion from an instance of this class (std::atomic<T>) to T (used by static_cast)
        operator T() const volatile noexcept;
        operator T() const noexcept;

        // Store (overwrite) the the atomic
        void store(T, memory_order = memory_order::seq_cst) volatile noexcept;
    };
}
```

```

void store(T, memory_order = memory_order::seq_cst) noexcept;

// Assignment
T operator=(T) volatile noexcept;
T operator=(T) noexcept;

// Store desired and return the old value atomically
T exchange(T desired, memory_order = memory_order::seq_cst) volatile noexcept;
T exchange(T desired, memory_order = memory_order::seq_cst) noexcept;

// if the old value is expected, then replace with desired and return true.
// if the old value is not expected, then return false
bool compare_exchange_strong(T& expected, T desired, memory_order, memory_order) volatile noexcept;
bool compare_exchange_strong(T& expected, T desired, memory_order, memory_order) noexcept;
bool compare_exchange_strong(T& expected, T desired,
                             memory_order = memory_order::seq_cst) volatile noexcept;
bool compare_exchange_strong(T& expected, T desired, memory_order = memory_order::seq_cst) noexcept;

// Same as compare_exchange_strong on x86, but different on ARM. Can fail spuriously.
bool compare_exchange_weak(T& expected, T desired, memory_order, memory_order) volatile noexcept;
bool compare_exchange_weak(T& expected, T desired, memory_order, memory_order) noexcept;
bool compare_exchange_weak(T& expected, T desired,
                           memory_order = memory_order::seq_cst) volatile noexcept;
bool compare_exchange_weak(T& expected, T desired, memory_order = memory_order::seq_cst) noexcept;

// check value of this against old, if equal => blocks until notify called.
void wait(T old, memory_order = memory_order::seq_cst) const volatile noexcept;
void wait(T old, memory_order = memory_order::seq_cst) const noexcept;

void notify_one() volatile noexcept;
void notify_one() noexcept;
void notify_all() volatile noexcept;
void notify_all() noexcept;
};

}

```

Hence we can use it to make access to complex objects atomic. Large types (i.e not integral types) use locks for this.

```

#include <atomic>

// an atomically accessed struct
typedef struct {
    int a;
    bool c;
} MyStruct;

std::atomic<MyStruct> p({.a=1, .c=true});

```

Weak vs Strong Exchange on ARM

Extra Fun! 2.5.1

The arm architecture allows exchange to spuriously fail.

- This is documented behaviour for `exchange_weak`
- `exchange_strong` contains a loop that makes use of `exchange_weak`
- On x86 strong and weak are identical and do not spuriously fail.

2.5.2 Atomic Integral Types

For integral types, fast assembly supported instructions for atomic integers, booleans and floats can be used.

-

```

namespace std {
    template<> struct atomic</* integral */> {
        // ... normal operations from std::atomic<T>

        // Atomic operations
        /* integral */ fetch_add(/* integral */, memory_order = memory_order::seq_cst) volatile noexcept;
        /* integral */ fetch_add(/* integral */, memory_order = memory_order::seq_cst) noexcept;
        /* integral */ fetch_sub(/* integral */, memory_order = memory_order::seq_cst) volatile noexcept;
        /* integral */ fetch_sub(/* integral */, memory_order = memory_order::seq_cst) noexcept;
        /* integral */ fetch_and(/* integral */, memory_order = memory_order::seq_cst) volatile noexcept;
        /* integral */ fetch_and(/* integral */, memory_order = memory_order::seq_cst) noexcept;
        /* integral */ fetch_or(/* integral */, memory_order = memory_order::seq_cst) volatile noexcept;
        /* integral */ fetch_or(/* integral */, memory_order = memory_order::seq_cst) noexcept;
        /* integral */ fetch_xor(/* integral */, memory_order = memory_order::seq_cst) volatile noexcept;
        /* integral */ fetch_xor(/* integral */, memory_order = memory_order::seq_cst) noexcept;

        // Operator Overloads
        /* integral */ operator++(int) volatile noexcept;
        /* integral */ operator++(int) noexcept;
        /* integral */ operator--(int) volatile noexcept;
        /* integral */ operator--(int) noexcept;
        /* integral */ operator++() volatile noexcept;
        /* integral */ operator++() noexcept;
        /* integral */ operator--() volatile noexcept;
        /* integral */ operator--() noexcept;
        /* integral */ operator+=(/* integral */) volatile noexcept;
        /* integral */ operator+=(/* integral */) noexcept;
        /* integral */ operator-=(/* integral */) volatile noexcept;
        /* integral */ operator-=(/* integral */) noexcept;
        /* integral */ operator&=(/* integral */) volatile noexcept;
        /* integral */ operator&=(/* integral */) noexcept;
        /* integral */ operator|=(/* integral */) volatile noexcept;
        /* integral */ operator|=(/* integral */) noexcept;
        /* integral */ operator^=(/* integral */) volatile noexcept;
        /* integral */ operator^=(/* integral */) noexcept;

        // ... normal operations from std::atomic<T>
    };
}

```

For example we can see a single add is used for the `fetch_add` here.

```
#include <atomic>

int main() {
    std::atomic<int> x(1);
    x += 3;
}
```

```
main:
    mov     DWORD PTR [rsp-4], 1
    lock add  DWORD PTR [rsp-4], 3
    xor     eax,  eax
    ret
```

Operator overloading is available for the integral types, however it can be difficult to determine which operations are atomic.

```
x = 42;          /* equivalent to */ x.store(42);
y = x;           /* equivalent to */ y = x.load();
x++;            /* equivalent to */ x.fetch_add(1);
y = ++x;         /* equivalent to */ y = x.fetch_add(1) + 1;
x += 42;         /* equivalent to */ x.fetch_add(42);
y = (x += 42);  /* equivalent to */ y = x.fetch_add(42) + 42;
```

2.6 Memory Order

The `atomic` header provides several memory orderings:

```

namespace std {
// ...

enum class memory_order : /* unspecified */ {
    relaxed, consume, acquire, release, acq_rel, seq_cst
};
inline constexpr memory_order memory_order_relaxed = memory_order::relaxed;
inline constexpr memory_order memory_order_consume = memory_order::consume;
inline constexpr memory_order memory_order_acquire = memory_order::acquire;
inline constexpr memory_order memory_order_release = memory_order::release;
inline constexpr memory_order memory_order_acq_rel = memory_order::acq_rel;
inline constexpr memory_order memory_order_seq_cst = memory_order::seq_cst;

//...
}

```

Sequential Consistency

Definition 2.6.1

The order of operations are executed as in the order of the program text.

- The default memory ordering for atomics (`std::atomic::memory_order_seq_cst`)
-

Simple Easy to reason about the interleaving of threads.

Expensive Compiler uses memory barriers which restrict how instructions can be reordered and optimised.

Relaxed Memory Order

Definition 2.6.2

Guarantees only sequential consistency per location.

2.7 Message Passing

Threads can communicate without blocking through atomics.

- Poll on an atomic variable (potentially doing some other work while waiting)
- Often used for synchronising access to shared resources (e.g spin locks)

2.7.1 Expensive Approach

We can use sequential consistency to ensure that the

```

#include <atomic>

std::atomic<bool> flag(true);
SharedObj data(some_data);

use_data(data);
flag.store(true);

while (!flag.load()) {
    // do nothing - a pure spinlock
}

use_data(data);

```

Slow On some architectures memory barriers are required for to ensure sequential consistency, are expensive.

Memory Barrier / Fence

Definition 2.7.1

These prevent the reordering of load and store instructions by dynamically scheduled processors.

- On a single core processor this is not an issue (dynamic scheduling commits instructions effects in order)
- On a multicore system instruction reordering in execution stages can result in non-sequentially consistent accesses.
- Dynamic scheduling of instructions improves performance by filling potential *stalls* with useful computation.

2.7.2 Incorrect Approach

One approach could be to use relaxed memory ordering.

- Allows for other values (e.g the data being protected by a spinlock) to be re-ordered around the atomic.
- This removes the protection the spinlock is intended to provide.

```
// These can be reordered
use_data(data);

flag.store(true, std::memory_order_relaxed);
```

```
while (!flag.load(std::memory_order_relaxed)) {
    // do nothing - a pure spinlock
}

use_data(data);
```

2.7.3 Release-Acquire Consistency

Release acquire consistency

```
// These can be reordered
use_data(data);

flag.store(true, std::memory_order_release);
```

```
while (!flag.load(std::memory_order_acquire)) {
    // do nothing - a pure spinlock
}

use_data(data);
```

The load is hence synchronised with the store, and reordering is prevented.

- Ensures correctness
- Potentially uses fewer memory barriers than SC (depends on the architecture)

Chapter 3

Mutexes

3.1 Spinlocks

3.1.1 Test-and-Set Spinlock

Test-and-Set Spinlock	Definition 3.1.1
<p>A single bit is used to determine if the lock is acquired or not.</p> <ul style="list-style-type: none">• Threads can use an atomic test-and-set operation to attempt to acquire the lock.• Avoids making system calls (expensive)• Wastes CPU time while spinning - hence useful only when the expected wait / critical section is short.• Poor worst case behaviour. <p>Hybrid locks that spin before using an OS provided lock mechanism exist to overcome the worst-case behaviour.</p>	

A simple spinlock can be implemented in C++ as:

```
#include <atomic>

class SpinLock {
public:
    SpinLock() : _lock_bit(false) {}

    void Lock() {
        while (_lock_bit.exchange(true));
    }

    void Unlock() {
        _lock_bit.store(false)
    }

private:
    std::atomic<bool> _lock_bit;
}
```

This simple lock has an issue with *cache thrashing*.

- Each core on a multicore CPU has its own caches (L2 (*often*), L1 cache)
- A *cache coherency protocol* is used to ensure different cache lines in different caches on different cores are coherent / if valid contain the correct value (not an outdated one)
- Typically when a location is written to in some cache, invalidation messages are sent to the other caches.

As in every attempt to acquire the lock, the test and set instruction writes to the lock

3.1.2 Local Spinning

To reduce the frequency of invalidations a ticket based spinlock can be used.

- First check if the lock is held (read - does not invalidate)
- Then if the lock is not held, attempt to access with an RMW operation (exchange) which writes & invalidates.

```
class SpinLockLocalSpinning : public SpinLock {
public:
    SpinLock() : _lock_bit(false) {}

    void Lock() {
        while (_lock_bit.exchange(true)) { // <- threads can still have a 'TAS fight' here
            // could not get the lock, so keep reading until it is free
            while (_lock_bit.load());
            // the lock is now free, so we attempt to acquire it again
        }
    }
}
```

Bus traffic is still an issue - we want to reduce the rate of accesses. This will also help to reduce the contention.

3.1.3 Fixed Backoff

Active Backoff

Definition 3.1.2

On each iteration of local spinning, do nothing / wait for some fixed time period. This waiting is *active* (e.g. spin in a loop).

We can implement active backoff by adding a fixed, redundant `for` loop.

```
class SpinLockLocalActiveBackoff : public SpinLock {
public:
    void Lock() {
        while (_lock_bit.exchange(true)) { // <- threads can still have a 'TAS fight' here
            // could not get the lock, so keep reading until it is free
            do {
                // volatile prevents the loop from being eliminated
                // spin for N iterations, we could also use library provided busy-wait functions
                for (volatile size_t i = 0; i < N; i++);
            } while (_lock_bit.load());
            // the lock is now free, so we attempt to acquire it again
        }
    }
}
```

Passive Backoff

Definition 3.1.3

On each iteration of local spinning, do nothing / wait for some fixed time period using a processor instruction that informs the CPU to wait/do nothing.

- `pause` on x86, accessed through the `_mm_pause()` SSE2 intrinsic
- `YIELD` on ARM

These instructions inform the CPU to do nothing for some period of time.

- Less energy consumption than actively spinning.
- Does not induce an OS context switch, simply a *do nothing* instruction.

```
#include <emmintrin.h>

class SpinLockLocalPassiveBackoff : public SpinLock {
```

```

public:
    void Lock() {
        while (_lock_bit.exchange(true)) {
            // could not get the lock, so keep reading until it is free
            do {
                // pause N times
                for (size_t i = 0; i < N; i++) {
                    _mm_pause()
                }
            } while (_lock_bit.load());
            // the lock is now free, so we attempt to acquire it again
        }
    }
}

```

Both active and passive backoff use a fixed backoff period.

- For a short backoff while little time is *wasted* (lock free but threads are backed-off), threads are more likely to TAS at similar times (more potential for contention on the lock acquire)
- For a long backoff the timings of TAS diverge for different threads, however more time can be spent backed-off when the lock is acquirable.

3.1.4 Exponential Backoff

Exponential Backoff

Definition 3.1.4

We can increase the backoff time exponentially for every iteration of local spinning.

- Start from a small value
- Double at each local spin iteration, until some maximum value is hit.

```

// So we can specify backoffs: SpinLockLocalExponentialBackoff<4,4096>()
#ifndef
    size_t MIN_BACKOFFS = 2,
    size_t MAX_BACKOFFS = 2048
>
class SpinLockLocalExponentialBackoff : public SpinLock {
public:
    void Lock() {
        size_t backoffs = MIN_BACKOFFS;
        while (_lock_bit.exchange(true)) {
            // could not get the lock, so keep reading until it is free
            do {
                for (size_t i = 0; i < backoffs; i++) {
                    _mm_pause()
                }
                // double the backoffs up to a limit
                backoffs = std::min(backoffs * 2, MAX_BACKOFFS)
            } while (_lock_bit.load());
        }
    }
}

```

- Much like with fixed backoffs, there may be *wasted* time between the lock being released and a thread acquiring it (thread is backed-off/doing nothing)
- Higher contention means more failed acquisitions and longer backoff periods

3.2 Ticket Locks

Unfairness

There is a tension between fairness and performance for spinlocks:

- Some thread may be unable to acquire a lock continually, while others may be able to reacquire frequently
- Threads reacquiring is good for temporal locality of cache (i.e a thread traversing a data structure will get better cache performance if it does not wait often - waiting allows opportunities for other threads to evict cached parts of the data structure)
- The lack of a fairness guarantee means thread starvation can occur, this can result in longer waits (e.g thread A is waiting on data from thread B, but thread B is being starved of a lock it needs by thread C to M)

A ticket lock a lock implementation that provides fairness guarantees.

Ticket Lock

Definition 3.2.1

A spinlock that uses an integer *ticket* to determine which of some waiting threads can run.

- To acquire, threads request a ticket, then spin until the lock matches their ticket.
- To release a thread sets the lock to serve the next ticket

```
#include <atomic>

class TicketLock {
public:
    SpinLock() : _next_ticket_(0), _serving_ticket_(0) {}

    void Lock() {
        const auto ticket = _next_ticket_.fetch_add(1);
        while (_serving_ticket_.load() != ticket) {
            _mm_pause();
        }
    }

    void Unlock() {
        _serving_ticket_.store(_serving_ticket_.load() + 1);
    }

private:
    std::atomic<size_t> _next_ticket_;
    std::atomic<size_t> _serving_ticket_;
}
```

3.3 Futexes

Spinlock

- Thread busy-waits until the lock is free.
- Uses atomic RMW operations
- No system calls required, operates entirely in user-space

Staying awake is expensive.

Useful when contention is low and critical sections are short

High contention results in lots of wasteful *spinning* rather than useful work

Sleeping Lock

- Use of a system call to ask the OS to block the thread until the lock is available.
- While the thread is blocked, other threads can be run.

Going to sleep is expensive.

Useful for long critical sections.

Overhead of system call is problematic when critical section is short - lock will be free imminently.

note that `futex` is a name for a linux system call.

- Exposes kernel functionality (so is not userspace).
- Works on userspace data, hence can be used to implement synchronisation primitives (not just mutexes) that operate mostly in userspace.

Fast Userspace Mutex (Futex)

Definition 3.3.1

3.3.1 Futex Operations

```
/* Wait on a futex
 * if *p != v -> Returns immediately
 * else           -> Adds the calling thread to the wait queue associated with p.
 */
void futex_wait(int *p, int v);
```

- The threads can be from different processes

```
/* Wake up a wake_count threads in the thread queue associated with p */
void futex_wake(int *p, int wake_count);
```

- Typically `wake_count` is 1 (wake next/one) or INT_{MAX} (wake all)

Here `int *p` can be a pointer to any *int-sized* data.

3.3.2 Futex Implementation

```
class MutexSimple {
public:
    MutexSimple() : state_(kFree) {}

    void Lock() {
        while (state_.exchange(kLocked) == kLocked) {
            syscall( SYS_futex, &state_, FUTEX_WAIT, kLocked, ...);
        }
    }

    void Unlock() {
        state_.store(kFree);
        syscall(SYS_futex, &state_, FUTEX_WAKE, 1, ...);
    }
private:
    const int kFree = 0;
    const int kLocked = 1;
    std::atomic<int> state_;
};
```

Chapter 4

Operational Semantics

4.1 Formal Properties

Safety Properties	<i>Nothing bad happens</i>	Only violated by finite computations
Liveness Properties	<i>Something good happens eventually</i>	Cannot be violated by finite computation

Deadlock is a **liveness** problem, while Mutual exclusion is a **Safety** problem.

Communication Deadlock	Definition 4.1.1
When using transient communication, messages can be lost. A thread may wait on a reply from another thread, that never received a prompt to reply in the first place, thus causing a deadlock.	

- Mutual Exclusion cannot be solved with transient communication
- Interrupts can also not work?

Mutual Exclusion	Definition 4.1.2
When only one thread can execute in a critical region at a time, there is mutual exclusion. <ul style="list-style-type: none">• Mutual exclusion enforces removes parallelism for the critical section, limiting speedup from parallelism (Amdahl's law)	

Turing Computability	Definition 4.1.3	Shared-Memory Computability	Definition 4.1.4
A model of computation that describes what is computable. <ul style="list-style-type: none">• Efficiency mostly irrelevant• Only covers sequential computation.		A model for concurrent computation. <ul style="list-style-type: none">• Describes what is concurrently computable.• Efficiency mostly irrelevant	

4.2 Shared-Memory Concurrency

4.2.1 Read-Modify-Write

Read-Modify-Write Instructions	Definition 4.2.1
<p>An instruction that reads, modifies (with some function) and writes to a memory location, returning the value prior to the modification.</p> <pre>//! Generically we can express this scheme for any data type struct RMWLocation<A> {data: A} impl<A: Clone> RMWLocation<A> { /// This function is synchronised fn read_modify_write(&mut self, apply: fn(&A) -> A) -> A { let old_value = self.data.clone(); self.data = apply(&self.data); old_value } }</pre>	

There are many different RMW instructions, a read can be considered an RMW instruction (where modification applies is just identity).

Weak RMW	Definition 4.2.2	Strong RMW	Definition 4.2.3
<p>Allows for synchronisation between two threads.</p> <ul style="list-style-type: none">• exchange Write - a new value to the location.• fetch and add - Atomically add to an integer at a location.		<p>Allows for synchronisation between an arbitrary number of threads.</p> <ul style="list-style-type: none">• compare and set (CAS) - If the value is equal to the expected, set to updated and return true, else return false.	

Many early machines provided weak RMW instructions (Test-and-set in IBM 360, Swap in original SPARC), we now understand the limitations of these.

- All intel x86 architectures support CAS.
- ARM supports CAS through load-linked and store-conditional instructions.

4.2.2 Consistency/Memory Models

Sequential Consistency	Definition 4.2.4
<p>Also known as interleaving semantics.</p> <ul style="list-style-type: none">• Instructions for each thread are executed in order.• Instructions from different threads can be interleaved arbitrarily.	

Sequential Consistency Model

- Can work on a uniprocessor system (simple/idealised).
- A good abstraction for concurrency & easier to reason about.
- Not available on any hardware platform by default.
- Inefficient and expensive to implement.

Hardware Consistency Models

- A weak memory model (due to dynamic scheduling on processors)
- Complex for multicore systems.
- Hardware implementation has to deal with complexities such as cache coherence.

Software/Programming Language Consistency Models

- A weak memory model (compiler can reorder instructions, also must accommodate hardware)
- Determined by the language specification, programmer uses this specification, compiler adapts to hardware.
- C/C++ 2011 model (C11 model) (e.g `atomic.h`)
- Java Memory Model

4.3 Sequential Consistency

We can create a basic while-language for sequential consistency.

$$B \in Bool ::= \dots \quad E \in Exp ::= \dots \quad x, y, \dots \in Loc ::= \text{ (Memory Location)} \quad a, b, \dots \in Reg ::= \text{ (Register)}$$

$$\begin{aligned} C \in Com ::= & \ a := E \\ | & \ a := x \\ | & \ x := a \\ | & \ a := \text{CAS}(x, E, E) \\ | & \ FFA(x, E) \\ | & \ \text{skip} \\ | & \ C ; C \\ | & \ \text{while } B \text{ do } C \\ | & \ \text{if } B \text{ then } C \text{ else } C \end{aligned}$$

Concurrent programs are modelled as a map from thread identifiers to sequential commands.

$$\tau \in Tid \quad \text{and} \quad P \in Prog \triangleq Tid \rightarrow Com$$

A concurrent program can be expressed using \parallel as:

$$C_1 \parallel C_2 \parallel C_3 \parallel \dots \parallel C_n \text{ for program } P \text{ where } dom(P) = \{\tau_1, \tau_2, \tau_3, \dots, \tau_n\} \text{ and } P(\tau_i) = C_i \text{ for } i \in \{1, 2, 3, \dots, n\}$$

Racey Increment

Example Question 4.3.1

Write a concurrent program inc that comprises of two threads which increment some shared memory.

$$P_{\text{inc}} \triangleq \begin{array}{c|c} a1 := cnt & a2 := cnt \\ a1 := a1 + 1 & a2 := a2 + 1 \\ \hline cnt := a1 & \end{array}$$

We can also express this as:

$$dom(P_{\text{inc}}) = \{\tau_1, \tau_2\}$$

$$\begin{aligned} P_{\text{inc}}(\tau_1) &= a1 := cnt ; a1 := a1 + 1 ; cnt := a1 \\ P_{\text{inc}}(\tau_2) &= a2 := cnt ; a2 := a2 + 1 ; cnt := a2 \end{aligned}$$

4.3.1 Configurations

$$\text{Shared memory } M \in Mem \triangleq Loc \rightarrow Val$$

$$\text{Thread-local Registers } s \in Store \triangleq Reg \rightarrow Val$$

$$\text{A store map for threads } S \in SMap \triangleq Tid \rightarrow Store \text{ where } S(\tau) = s$$

Hence the configuration is a triple of the concurrent program, shared memory and map to thread local stored.

$$(P, S, M)$$

4.3.2 Transitions

The operational semantics are split into two types of transition.

Program Transitions	A step inb program execution (e.g if condition)
Storage Transitions	Describes behaviour of memory (e.g read/write)

- By splitting operational semantics into two parts we can alter storage transitions later without having to change the program transitions.
- The program and storage transitions are combined through label transitions.

The labels are defined as:

$$l \in Lab ::= \begin{array}{ll} \epsilon & \text{empty label such as when transitioning: } \text{skip} ; C \rightarrow C \\ | (R, x, v) & \text{Read value } v \text{ from memory location } x \\ | (W, x, v) & \text{Write value } v \text{ to memory location } x \\ | (U, x, v_0, v_n) & \text{Successful update of } x \text{ from } v_0 \rightarrow v_n \text{ (FFA or successful CAS)} \\ | (U, x, v_0, \perp) & \text{Failed CAS of } x \text{ where the old value of } x \text{ was not } v_0 \end{array}$$

We also have a total function $\text{eval}(s, E)$ or $\text{eval}(s, B)$ to evaluate expressions.

Total Function	Definition 4.3.1
A function defined for all possible input values.	

Hence any transition is:

$$C, s \xrightarrow{l} C', s' \text{ where } C, C' \in Com, \quad s, s' \in Store \text{ and } l \in Lab$$

The transitions are:

$$\frac{\begin{array}{c} C_1, s \xrightarrow{l} C'_1, s' \\ C_1 ; C_2, s \xrightarrow{l} C'_1 ; C_2, s' \end{array}}{\text{if } B \text{ then } C_1 \text{ else } C_2, s \xrightarrow{\epsilon} C_1, s} \quad \frac{\begin{array}{c} \text{eval}(s, B) = true \\ \text{if } B \text{ then } C_1 \text{ else } C_2, s \xrightarrow{\epsilon} C_1, s \end{array}}{\text{skip} ; C, s \xrightarrow{\epsilon} C, s} \quad \frac{\begin{array}{c} \text{eval}(s, B) = false \\ \text{if } B \text{ then } C_1 \text{ else } C_2, s \xrightarrow{\epsilon} C_2, s \end{array}}{\text{eval}(s, E) = v \quad s' = s[a \mapsto v]} \\ \frac{}{a := E, s \xrightarrow{\epsilon} \text{skip}, s'} \quad \frac{}{\text{while } B \text{ do } C, s \xrightarrow{\epsilon} \text{if } B \text{ then } (C ; \text{while } B \text{ do } C) \text{ else skip}}$$

We must also consider the basic read/write transitions:

$$\frac{s(a) = v}{x := a, s \xrightarrow{(W, x, v)} \text{skip}, s} \quad \frac{s' = s[a \mapsto v]}{a := x, s \xrightarrow{(R, x, v)} \text{skip}, s'}$$

Note that program transitions do not consider memory, so no update takes place here on the memory write.

Finally we need to consider FFA and CAS.

$$\frac{\begin{array}{c} \text{eval}(s, E) = v \quad v_n = v_0 + v \\ \text{FFA}(x, E), s \xrightarrow{(U, x, v_0, v_n)} \text{skip}, s \end{array}}{\text{eval}(s, E_0) = v_0 \quad \text{eval}(s, E_n) = v_n \quad s' = s[a \mapsto 1]} \quad \frac{\begin{array}{c} \text{eval}(s, E_0) = v_0 \quad \text{eval}(s, E_n) = v_n \quad s' = s[a \mapsto 1] \\ a := \text{CAS}(x, E_0, E_n), s \xrightarrow{(U, x, v_0, v_n)} \text{skip}, s' \end{array}}{\text{eval}(s, E_0) = v_0 \quad v \rightarrow v_0 \quad s' = s[a \mapsto 0]} \\ \frac{}{a := \text{CAS}(x, E_0, E_n), s}$$

4.3.3 Concurrent Program Transitions

$$\frac{P(\tau) = C \quad S(\tau) = s \quad C, s \xrightarrow{l} C', s' \quad P' = P[\tau \mapsto C'] \quad S' = S[\tau \mapsto s']}{P, S \xrightarrow{\tau;l} P', S'}$$

4.3.4 Storage Transitions

A storage transition is of the form $M \xrightarrow{\tau:l} M'$ (thread τ updates $M \rightarrow M'$ using label l).

- We will use the thread id τ to combine storage with program transitions later.
- We only consider the labels from program transitions (these affect the shared memory).

$$\frac{M(\textcolor{blue}{x}) = v}{M \xrightarrow{\tau:(R,\textcolor{blue}{x},v)} M} \quad \text{Memory Read}$$

$$\frac{M' = M[\textcolor{blue}{x} \mapsto v]}{M \xrightarrow{\tau:(W,\textcolor{blue}{x},v)} M'} \quad \text{Memory Write}$$

$$\frac{M(x) = v_0 \quad M' = M[\textcolor{blue}{x} \mapsto v_n]}{M \xrightarrow{\tau:(U,\textcolor{blue}{x},v_0,v_n)} M'} \quad \text{Successful CAS or FFA}$$

$$\frac{M(\textcolor{blue}{x}) = v}{M \xrightarrow{\tau:(U,\textcolor{blue}{x},v,\perp)} M} \quad \text{Failed CAS}$$

4.3.5 Combining Operational Semantics

The combined semantics are of the form $P, S, M \rightarrow P', S', M'$

For example with

$$\frac{P, S \xrightarrow{\tau:\epsilon} P', S'}{P, S, M \rightarrow P', S', M}$$

Under ϵ label shared memory is unchanged

If the program and storage transitions are the same, then we can combine into a single transition

Skipping it!

Example Question 4.3.2

Combine the memory and program transitions for skip.

The program transition can be expressed as:

$$\frac{P(\tau) = \text{skip} ; C \quad S(\tau) = s \quad \text{skip} ; C, s \xrightarrow{\epsilon} C, s \quad P' = P[\tau \mapsto C]}{P, S \xrightarrow{\tau:\epsilon} P', S}$$

As the program transition does not affect memory ($\text{skip} ; C, s \xrightarrow{\epsilon} C, s$) we can directly add M to the transition:

$$\frac{P(\tau) = \text{skip} ; C \quad S(\tau) = s \quad \text{skip} ; C, s \xrightarrow{\epsilon} C, s \quad P' = P[\tau \mapsto C]}{P, S, M \rightarrow P', S, M}$$

Read and Assign

Example Question 4.3.3

Get the program transition for an assignment (reading memory into a register), where the memory value is 7.

$$\frac{M(\textcolor{blue}{x}) = 7}{M \xrightarrow{\tau:(R,\textcolor{blue}{x},7)} M} \quad \frac{s' = s[\textcolor{red}{a} \mapsto 7]}{\textcolor{red}{a} := \textcolor{blue}{x}, s \xrightarrow{(R,\textcolor{blue}{x},7)} \text{skip}, s'}$$

$$\frac{P(\tau) = \textcolor{red}{a} := \textcolor{blue}{x} \quad S(\tau) = s \quad s' = s[\textcolor{red}{a} \mapsto 7] \quad \textcolor{red}{a} := \textcolor{blue}{x}, s \xrightarrow{(R,\textcolor{blue}{x},7)} \text{skip}, s' \quad P' = P[\tau \mapsto \text{skip}] \quad S' = S[\tau \mapsto s']}{P, S \xrightarrow{\tau:(R,\textcolor{blue}{x},7)} P', S'}$$

Hence we can now include the storage transition:

$$\frac{P, S \xrightarrow{\tau:(R,\textcolor{blue}{x},7)} P', S' \quad M \xrightarrow{\tau:(R,\textcolor{blue}{x},7)} M}{P, S, M \rightarrow P', S', M}$$

4.3.6 Traces

\rightarrow^* for SC

Definition 4.3.2

$$P, S, M \rightarrow^* P', S', M' \Leftrightarrow (P, S, M) = (P', S', M') \vee \exists (P'', S'', M''). [P, S, M \rightarrow P'', S'', M'' \wedge P'', S'', M'' \rightarrow^* P', S', M']$$

The reflexive, transitive closure of \rightarrow

- *Initial memory* is all zeros $M_0 \triangleq \lambda x.0$ (for any x , $M_0(x) = 0$).
- *Initial Store* is also originally all zeros. $s_0 \triangleq \lambda a.0$.
- *Initial store map* is $S_0 \triangleq \lambda \tau.s_0$
- *Terminated Program* is P_{skip} expressed as $P_{\text{skip}} \triangleq \tau.\text{skip}$.
- The *initial configuration* is (P, S_0, M_0) .

Given a program P the *SC-trace* is the evaluation path:

$$P, S_0, M_0 \rightarrow^* P_{\text{skip}}, S, M$$

Where (S, M) is the *SC-outcome* of program P .

4.3.7 Properties of Sequential Consistency

Determinism

$$\forall P, P_1, P_2, S, S_1, S_2 M, M_1, M_2. [(P, S, M \rightarrow P_1, S_1, M_1 \wedge P, S, M \rightarrow P_2, S_2, M_2) \Rightarrow ((P_1, S_1, M_1) = (P_2, S_2, M_2))]$$

This does not hold due to the interleavings of the threads of P .

It has been determined...

Example Question 4.3.4

Provide a counter example to SC being deterministic and confluent.

$$P = \frac{a1 := 1}{x := a1} \parallel \frac{a2 := 0}{x := a2}$$

Here we can have $P, S_0, M_0 \rightarrow^* P_{\text{skip}}, S, M$ Where $M(\textcolor{blue}{x}) = 1$ or $M(\textcolor{blue}{x}) = 0$.

Confluence

$$\begin{aligned} \forall P, P_1, P_2, S, S_1, S_2 M, M_1, M_2. & [(P, S, M \rightarrow^* P_1, S_1, M_1 \wedge P, S, M \rightarrow^* P_2, S_2, M_2) \\ & \Rightarrow \exists P', S', M'. [P_1, S_1, M_1 \rightarrow^* P', S', M' \wedge P_2, S_2, M_2 \rightarrow^* P', S', M']] \end{aligned}$$

SC is not confluent for the same reason it is not deterministic (there are many possible *SC-outcomes* for a program)

4.4 Total Store Ordering

Weak Memory Models (WMM)

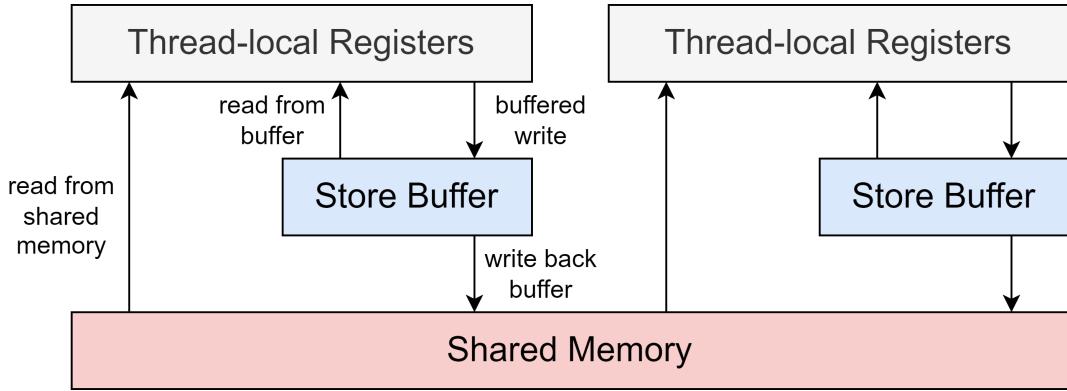
Definition 4.4.1

Allow for instructions in a thread to be reordered (e.g dynamically scheduled processors).

- *Weak behaviours* are states not observable under *sequential consistency*.
- Used by virtually all computer architectures (e.g TSO used by x86).

A weak memory model that allows for write-read reordering between different memory locations.

- A later read on y can be reordered before an earlier write on x when $x \neq y$
- Includes the interleaving semantics from sequential consistency.
- Allows for weak store buffering (where)



$x := 1$	Add $x := 1$ to the store buffer.
$a := x$	If x is in the buffer, read latest entry, else read from shared memory.
unbuffer	Flush buffer to memory (FIFO order)
mfence	Barrier instruction, ensures no delayed writes are in the buffer (hence any subsequent reads happen after the current buffered writes).
RWMS	Act as barriers and ensure no delayed writes are in the buffer, they write directly to memory without delay.

The previous language used for sequential consistency can have fences added.

$$\begin{aligned}
C \in Com ::= & a := E \\
& | a := x \\
& | x := a \\
& | a := \text{CAS}(x, E, E) \\
& | \text{FFA}(x, E) \\
& | \text{skip} \\
& | C ; C \\
& | \text{while } B \text{ do } C \\
& | \text{if } B \text{ then } C \text{ else } C \\
& | \text{mfence}
\end{aligned}$$

$$\overline{\text{mfence}, s \xrightarrow{MF} \text{skip}, s}$$

We model memory similarly to before, but now with a local buffer.

$$M \in Mem \triangleq Loc \rightarrow Val \quad S \in SMap \triangleq Tid \rightarrow Store \quad s \in Store \triangleq Reg \rightarrow Val$$

A buffer is a FIFO queue of delayed write labels.

$$b \in Buff \triangleq Seq\langle WLab \rangle \quad WLab \triangleq \{(W, x, v) | x \in Loc \wedge v \in Val\}$$

$$B \in BMap \triangleq Tid \rightarrow Buff \text{ where } b = B(\tau)$$

Hence a TSO configuration is:

$$(P, S, M, B)$$

4.4.1 Storage Transitions

TSO adds the `mfence` transition label MF

$$l \in Lab ::= \epsilon \quad | \quad (R, \textcolor{blue}{x}, v) \quad | \quad (W, \textcolor{blue}{x}, v) \\ | \quad (U, \textcolor{blue}{x}, v_0, v_n) \quad | \quad (U, \textcolor{blue}{x}, v_0, \perp) \\ | \quad MF$$

Storage transitions are of the form:

$$\frac{B(\tau) = b \quad b' = b.(W, \textcolor{blue}{x}, v) \quad B' = B[\tau \mapsto b']}{{M, B \xrightarrow{\tau: l_m} M', B'}} \quad \text{Memory Write}$$

$$\frac{B(\tau) = b \quad get(M, b, \textcolor{blue}{x}) = v}{\frac{B(\tau) = b \quad get(M, b, \textcolor{blue}{x}) = v}{M, B \xrightarrow{\tau: (R, \textcolor{blue}{x}, v)} M, B}} \quad \text{Memory Read}$$

$$\frac{B(\tau) = \emptyset \quad M(\textcolor{blue}{x}) = v_0 \quad M' = M[\textcolor{blue}{x} \mapsto v_n]}{{M, B \xrightarrow{\tau: (U, \textcolor{blue}{x}, v_0, v_n)} M', B'}} \quad \frac{B(\tau) = \emptyset \quad M(\textcolor{blue}{x}) = v}{M, B \xrightarrow{\tau: (U, \textcolor{blue}{x}, v, \perp)} MB} \quad \text{Failed RMW}$$

Memory Fence ensures no buffering

The buffered writes may be propagated at any time through a silent step, this is done using an ϵ storage transition.

If the program takes a silent step, the storage system is unchanged.
If both the program and storage systems make the same transition l then we can combine this into a transition over

the TSO configuration.

$$\frac{P, S \xrightarrow{\tau: l_p} P', S' \quad M, B \xrightarrow{\tau: l_m} M', B'}{P, S, M, B \rightarrow P', S', M', B'}$$

$$\frac{M, B \xrightarrow{\tau: \epsilon} M', B'}{P, S, M, B \rightarrow P, S, M', B'}$$

If the storage system takes a silent step, the program & program's register store remains the same.

sFence

Example Question 4.4.1

The x86-64 instruction set includes an `sfence` instruction. This is similar to `mfence`, however allows for read reordering.

$$\begin{array}{ccc} \begin{array}{c} x := 1 \parallel y := 1 \\ \text{sfence} \parallel \text{sfence} \\ a := y \parallel b := x \end{array} & \approx & \begin{array}{c} x := 1 \parallel y := 1 \\ a := y \parallel b := x \\ \text{sfence} \parallel \text{sfence} \end{array} \\ \text{Original} & & \text{sfence-read-reordering} \end{array} \quad \approx \quad \begin{array}{c} a := y \parallel b := x \\ x := 1 \parallel y := 1 \\ \text{sfence} \parallel \text{sfence} \end{array} \quad \text{TSO allowed reorder}$$

Adapt the rules of TSO to implement `sfence`.

`sfence` make no changes to registers/local store, but requires an SF memory transition:

$$\overline{\text{sfence}, s \xrightarrow{SF} \text{skip}, s}$$

In order to implement, we will add `sfences` to the store buffer, hence we must redefine the buffer:

$$b \in Buff \triangleq Seq\langle WLab \cup \{SF\} \rangle$$

- `sfence` adds `SF` to the store buffer.
- When executing an `sfence` transition, we do not need to check if the buffer is empty.
- Since `sfence` and write instructions are still ordered with respect to each other, the buffers are still a FIFO queue.

Hence:

$$\frac{B(\tau) = b \quad B' = B[\tau \mapsto b.SF]}{M, B \xrightarrow{\tau:SF} M, B'} \quad \frac{B(\tau) = SF.b \quad B' = B[\tau \mapsto b]}{M, B \xrightarrow{\tau:e} M, B'}$$

We can consider an `sfence` as a kind of dummy write, much like normal writes other writes cannot be reordered, but reads can. However unlike a write it has no effect on memory.

4.4.2 Traces

TSO inherits much of the initial state from SC:

$$M_0 \triangleq \lambda x.0 \quad S_0 \triangleq \lambda \tau.s_0 \text{ with } s_0 \triangleq \lambda a.0 \quad P_{\text{skip}} \triangleq \lambda \tau.\text{skip}$$

However we add the *initial buffer map*:

$$B_0 \triangleq \lambda \tau.\emptyset$$

The *initial TSO-configuration* is hence:

$$(P, S_0, M_0, B_0)$$

Given some program P the *TSO-trace* is an evaluation path that starts from the *initial TSO-configuration* of P and terminates with P_{skip} and empty buffers.

$$P, S_0, M_0, B_0 \xrightarrow{*} P_{\text{skip}}, S, M, B_0 \text{ where } (S, M) \text{ is the } TSO\text{-outcome}$$

4.4.3 Properties of Total Store Ordering

Determinism

Much like *sequential consistency* the interleaving of different threads makes TSO non-deterministic.

Confluence

Likewise, TSO is not confluent.

Chapter 5

Declarative Semantics

Declarative/Axiomatic Semantics	Definition 5.0.1
An alternative to operational semantics.	
<ul style="list-style-type: none"> • Defines the notion of program execution (generalisation of execution trace) • Maps a program to a set of candidate executions • Define a consistency predicate on executions 	
Semantics are defined as the set of consistent executions of a program.	
Catch Fire Semantics	Definition 5.0.2
The existence of one <i>bad</i> consistent execution implies undefined behaviour.	
Executions are expressed as graphs.	
Events Graph Nodes Reads, Writes, Updates & Fences Relations Graph Edges Program order (<i>po</i>) and reads-from (<i>rf</i>).	
Event	Definition 5.0.3
$\langle n, \tau, l \rangle$ $n \in \mathbb{N}$ Unique Event Identifier $\tau \in Tid \cup \{0\}$ Thread Identifier l Non-empty label	
Non-empty Label	Definition 5.0.4
As labels are only associated with events, and events interact with memory, there is no concept of a ϵ empty label as in operational semantics.	
Labels are model specific, so for sequential consistency they are:	
(R, \underline{x}, v_r) (W, \underline{x}, v_w) $(U, \underline{x}, v_r, v_w)$	
where $x \in Loc$ and $v_r, v_w \in Val$	

5.1 Label and Event Notation

$\text{typ}((R, \underline{x}, v_r)) \triangleq R$ $\text{typ}((W, \underline{x}, v_w)) \triangleq W$ $\text{typ}((U, \underline{x}, v_r, v_w)) \triangleq U$	$\text{val}_r((R, \underline{x}, v_r)) \triangleq v_r$ $\text{val}_r((U, \underline{x}, v_r, v_w)) \triangleq v_r$ $\text{val}_w((W, \underline{x}, v_w)) \triangleq v_w$ $\text{val}_w((U, \underline{x}, v_r, v_w)) \triangleq v_w$	$\text{loc}((R, \underline{x}, v_r)) \triangleq \underline{x}$ $\text{loc}((W, \underline{x}, v_w)) \triangleq \underline{x}$ $\text{loc}((U, \underline{x}, v_r, v_w)) \triangleq \underline{x}$
Get Label Type	Get read & write values.	Get read & write values.

Given a set of events A , the relations $r, r' \subseteq A \times A$ and memory location $\textcolor{blue}{x}$ we have:

Identity on A	$[A] \triangleq \{(a, a) \mid a \in A\}$
Domain of r	$\text{dom}(r) \triangleq \{a \mid (a, -) \in r\}$
Range of r	$\text{rng}(r) \triangleq \{a \mid (-, a) \in r\}$
Inverse of r	$r^{-1} \triangleq \{(b, a) \mid (a, b) \in r\}$
Composition of r and r'	$r; r' \triangleq \{(a, c) \mid (a, b) \in r \wedge (b, c) \in r'\}$
Reflexive Closure of r	$r^? \triangleq r \cup [\text{dom}(r) \cup \text{rng}(r)]$
Transitive Closure of r	$r^+ \triangleq \bigcup_{i=0}^{\infty} r^i$ where $r^0 \triangleq r$ and $r^{i+1} \triangleq r; r^i$ for $i > 0$
Reflexive & Transitive closure of r	$r^* \triangleq (r^+)^?$
	$A_{\textcolor{blue}{x}} \triangleq \{e \in A \mid \text{loc}(e) = \textcolor{blue}{x}\}$ and $r_{\textcolor{blue}{x}} \triangleq r \cap (A_{\textcolor{blue}{x}} \times A_{\textcolor{blue}{x}})$
	$r _{\text{loc}} \triangleq \{(a, b) \in r \mid \text{loc}(a) = \text{loc}(b)\}$

Given an event set A , a relation $r \in A \times A$ and a thread τ we have:

Initialisation of events in A	$A_0 \triangleq \{e \in A \mid \text{tid}((\)a) = 0\}$
	$A_\tau \triangleq \{e \in A \mid \text{tid}(a) = \tau\}$ and $r_\tau \triangleq \cap(A_\tau \times A_\tau)$
For internal edges (of the same thread)	$ri \triangleq \{(a, b) \in r \mid \text{tid}(a) = \text{tid}(b)\}$
For external edges	$re \triangleq \{(a, b) \in r \mid \text{tid}(a) \neq \text{tid}(b)\}$
$\text{irreflexive}(r)$	$\overset{\text{def}}{\Leftrightarrow} \neg \exists a. [(a, a) \in r]$
$\text{acyclic}(r)$	$\overset{\text{def}}{\Leftrightarrow} \text{irreflexive}(r^+)$

Relational Composition

Definition 5.1.1

Given some relations $R \in X \times Y$ and $S \in Y \times Z$:

$$R; S \triangleq \{(x, z) \in X \times Z \mid \exists y \in Y. [(x, y) \in R \wedge (y, z) \in S]\}$$

$$\begin{aligned} \text{injective}(R; S) &\Rightarrow \text{injective}(R) & \text{injective}(R) \wedge \text{injective}(S) &\Rightarrow \text{injective}(R; S) \\ \text{surjective}(R; S) &\Rightarrow \text{surjective}(R) & \text{surjective}(R) \wedge \text{surjective}(S) &\Rightarrow \text{surjective}(R; S) \\ R; (S; T) &= (R; s); T & (R; S)^T &= S^T; R^T \end{aligned}$$

Partial Orders

Definition 5.1.2

Given some set A and relation $R \subseteq (A \times A)$:

R is reflexive	$\forall x \in A. [x R x]$
R is irreflexive	$\forall x \in A. [\neg(x R x)]$
R is symmetric	$\forall x, y \in A. [x R y \Rightarrow y R x]$
R is anti-symmetric	$\forall x, y \in A. [(x R y \wedge y R x) \rightarrow x = y]$
R is transitive	$\forall x, y, z \in A. [(x R y \wedge y R z) \Rightarrow x R z]$

Pre-order	Reflexive and Transitive
Partial order	Anti-symmetric & pre-order. Hence is reflexive, transitive and anti-symmetric.
Strict partial order	Irreflexive and transitive
Total order	Partial order with $\forall x, y \in A. [x R y \vee y R x]$
Strict total order	Strict partial order with $\forall x, y \in A. [x \neq y \Rightarrow (x R y \vee y R x)]$

Function Types

Definition 5.1.3

$$f : A \rightarrow B \quad \text{dom}(f) = A \quad \text{codom}(f) = B$$

Injective/one-to-one	Each output is mapped to by at most one input.	$\forall x_1, x_2 \in A. [f(x_1) = f(x_2) \Rightarrow x_1 = x_2]$
Surjective/onto	Each output is mapped to by at least one input.	$\forall y \in B. \exists x \in A. [f(x) = y]$
Bijective	Each output is mapped to by one input.	$\text{bijective}(f) = \text{injective}(f) \wedge \text{surjective}(f)$

Execution Graph

Definition 5.1.4

$$\langle E, \text{po}, \text{rf} \rangle$$

E Finite set of events.

po The Program order binary relation.

rf Reads-from binary relation.

po is such that:

$$\text{po} \triangleq \left(\bigcup_{\tau \in \text{tid}} \text{po}_\tau \right) \cup (E_0 \times (E \setminus E_0))$$

Each po_τ is a strict total order on E_τ .

rf is such that $\forall \langle w, r \rangle \in \text{rf}$, (maps a write event, to an event that reads from it).

$$\begin{aligned} w &\neq r \\ \text{typ}(w) &\in \{W, U\} \wedge \text{typ}(r) \in \{R, U\} \\ \text{loc}(w) &= \text{loc}(r) \\ \text{val}_w(w) &= \text{val}_r(r) \end{aligned}$$

rf^{-1} is a function (if $\langle w_1, r \rangle, \langle w_2, r \rangle \in \text{rf}$ then $w_1 = w_2$)

The notation for a graph G is:

$$G = \langle E, \text{po}, \text{rf} \rangle$$

$$G.E \triangleq E$$

$$G.\text{po} \triangleq \text{po}$$

$$G.R \triangleq \{r \in E \mid \text{typ}(r) = R\}$$

$$G.W \triangleq \{w \in E \mid \text{typ}(w) = W\}$$

$$G.U \triangleq \{u \in E \mid \text{typ}(u) = U\}$$

$$G.RU \triangleq G.R \cup G.U$$

$$G.WU \triangleq G.W \cup G.U$$

$$G.R_{\textcolor{blue}{x}} \triangleq G.R \cap \{r \in E \mid \text{loc}(r) = \textcolor{blue}{x}\}$$

$$G.W_{\textcolor{blue}{x}} \triangleq G.W \cap \{w \in E \mid \text{loc}(w) = \textcolor{blue}{x}\}$$

5.2 Consistency Predicates

A program is mapped to a set of candidate executions. A consistency predicate filters these candidates.

- The semantics of a program are the consistent executions of a program.
- Consistency predicates include sequential consistency and total store ordering.

Completeness

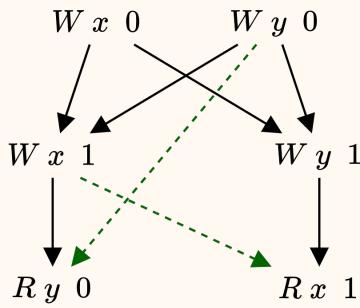
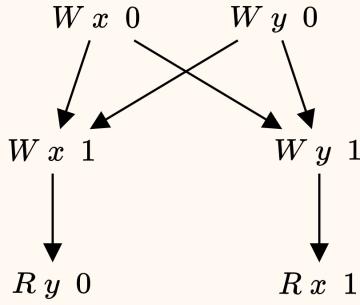
Definition 5.2.1

A graph G is complete if:

$$\text{rng}(G.\text{rf}) = G.RU$$

Every read/update reads from some write/update.

Define $G.\text{rf}$ to complete the following graph:



$$G.UW = \{W x 0, W y 0, W x 1, W y 1\}$$

$$G.RU = \{R y 0, R x 1\}$$

The location and value must match.

$$G.\text{rf} = \{(W y 0, R y 0), (W x 1, R x 1)\}$$

5.3 Sequential Consistency

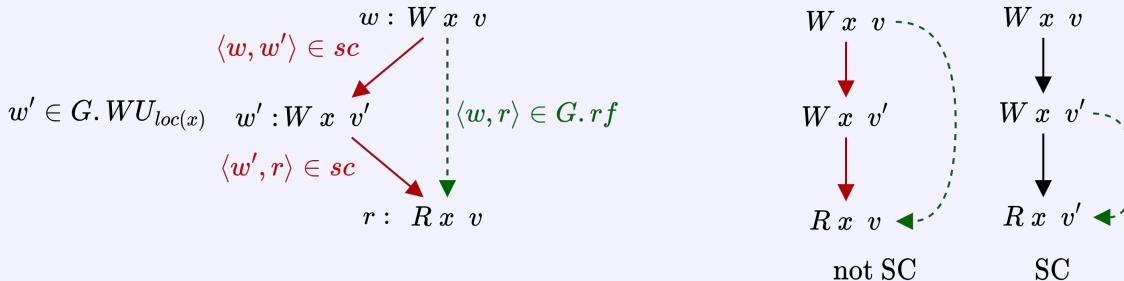
Sequential Consistency (Lamport SC)

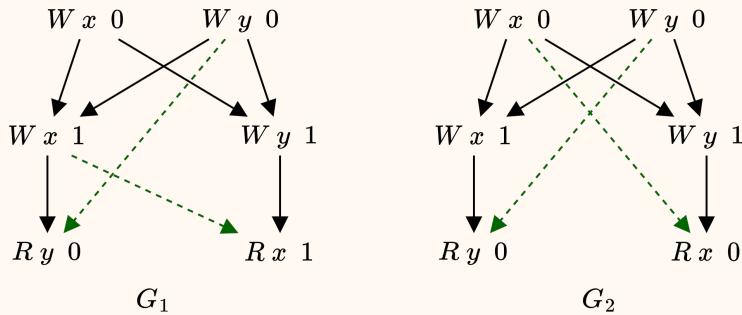
Definition 5.3.1

sc is a strict total order on $G.E$. G is *SC-consistent* if the following hold:

- $\langle a, b \rangle \in G.\text{po} \Rightarrow \langle a, b \rangle \in \text{sc}$ i.e $G.\text{po} \subseteq \text{sc}$
- $\wedge \quad \langle w, r \rangle \in G.\text{rf} \Rightarrow \langle w, r \rangle \in \text{sc}$ i.e $G.\text{rf} \subseteq \text{sc}$
- $\wedge \quad \langle w, r \rangle \in G.\text{rf} \Rightarrow \neg \exists w' \in G.WU_{\text{loc}(r)}.[\langle w, w' \rangle \in \text{sc} \wedge \langle w', r \rangle \in \text{sc}]$ i.e There is no w' between w and r

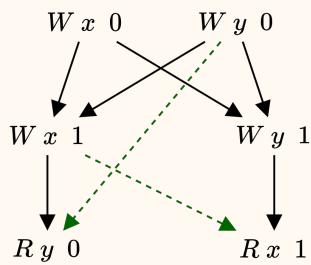
- G must be complete
- G is SC-consistent with respect to some strict total order sc on $G.E$



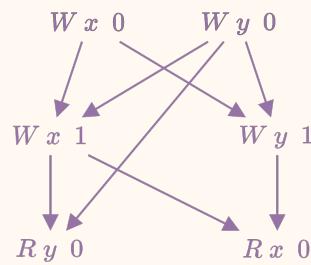


Determine which of these are sequentially consistent using Lamport's definition.

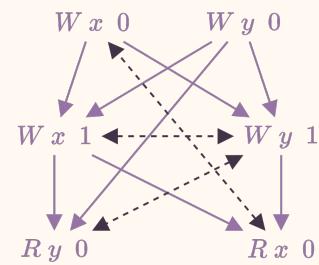
For the graph G_1 :



The original graph G



sc must contain all of $G.rf$ and $G.po$

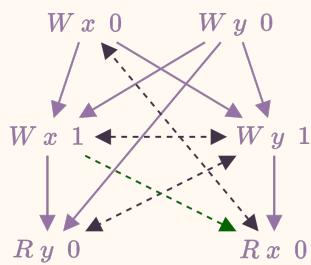


sc is a total order, add in some faux edges to ensure all connected (we will sort direction later)

(1)

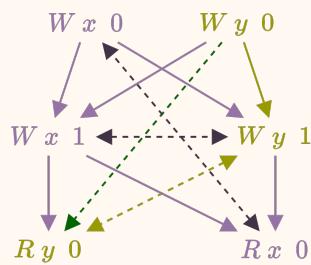
(2)

(3)



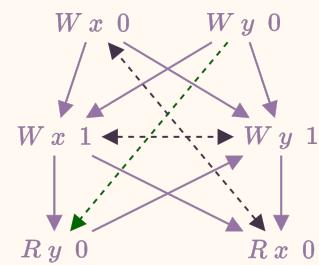
We select an rf edge, we cannot find a write to make this read from non-
SC

(4)



We move to the other rf edge, and find a potential issue, we
need $Ry 0$ to occur before $Wy 1$

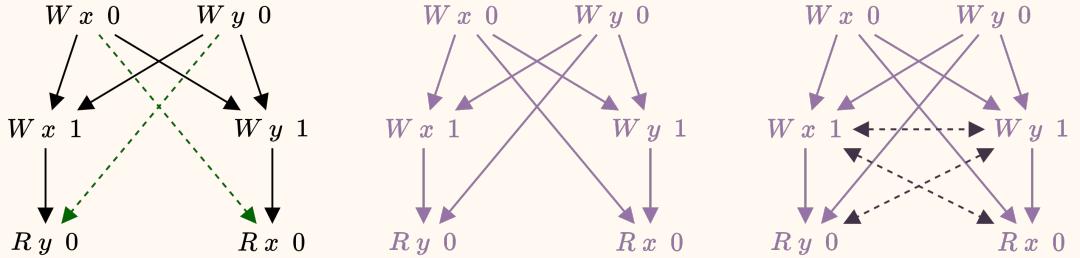
(5)



By setting $Ry 0$ to occur before $Wy 1$ we order the other edges by
transitivity (sc is a total order)

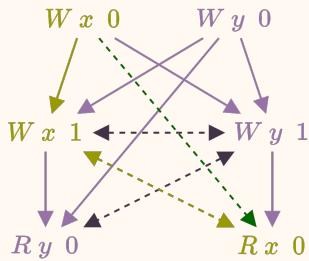
(6)

Hence G_1 is SC-consistent. For the graph G_2 :



The provided graph G

(1)



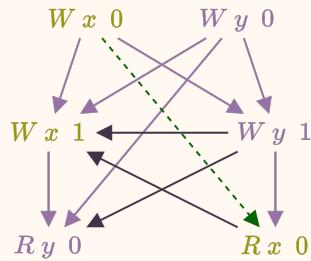
We choose one of the rf edges and immediately see a potential issue.

If Rx 0 comes after Wx 1, then we have breached sequential consistency

(4)

sc must contain all of G.rf and G.po

(2)

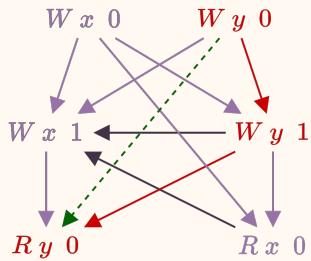


Hence we choose an sc where Wx 1 comes after Rx 0. The other edges directions are then set as a result (transitivity)

(5)

sc is a total order, add in some faux edges to ensure all connected (we will sort direction later)

(3)



We then take the other rf edge, however this is unreconcilable. If we picked the other direction in (5) we would have lost sequential consistency there. Hence this graph is not SC

(6)

Hence G_2 is not SC-consistent.

Modification/Coherence Order (Alternative SC)

Definition 5.3.2

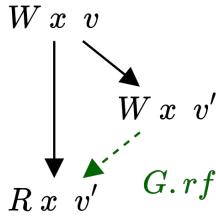
mo is a *modification order* for an execution graph G if:

$$\text{mo} = \bigcup_{x \in \text{Loc}} \text{mo}_x \text{ where } \text{mo}_x \text{ is a strict total order on } G.WU_x$$

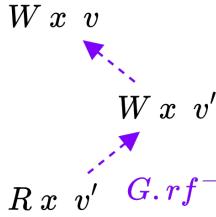
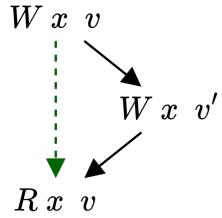
We can then create an alternative definition for sequential consistency.

$$\begin{aligned} & G \text{ is complete} \\ \wedge \quad & \exists \text{ mo for } G. [\text{acyclic}(G.\text{po} \cup G.\text{rf} \cup \text{mo} \cup \text{rb})] \\ & \text{where } \text{rb} \triangleq G. \text{rf}^{-1}; \text{mo} \setminus \text{id} \end{aligned}$$

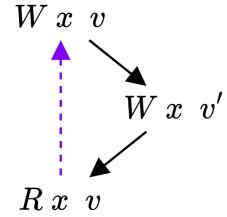
- On all architectures there is a strict total order or writes on a given cache line (here we consider location).
- Applies to each memory location.



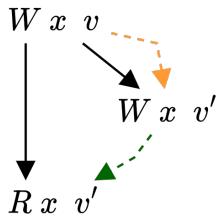
A simple example, with only one location x



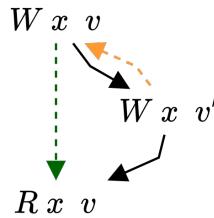
choose any mo



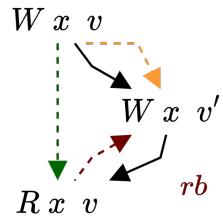
we try both possible mo



acyclic $\Rightarrow SC$



no mo for which it is acyclic \Rightarrow not SC



SC Equivalence

Extra Fun! 5.3.1

Lamport SC \Rightarrow Alternative SC

1. Take $mo_x \triangleq [WU_x]; sc; [WU_x]$
2. The $G.po \cup G.rf \cup mo \cup rb \subseteq sc$

Alternative SC \Rightarrow Lamport SC

1. Take sc to be any strict total order extending $G.po \cup G.rf \cup mo \cup rb$

5.4 Total Store Order

Total Store Order

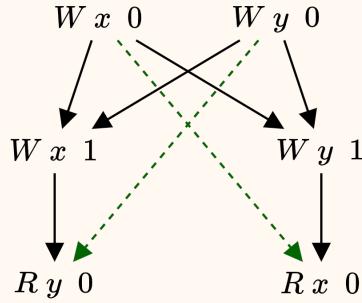
Definition 5.4.1

tso is a strict partial order on $G.E$ where the following holds:

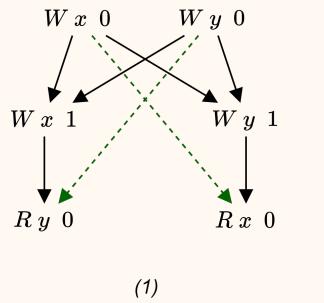
- tso is total on $G.E \setminus G.R$
- $\wedge \quad G.po \setminus (G.W \times G.R) \subseteq tso$
- $\wedge \quad G.rf \subseteq tso \cup G.po$ This implies $G.rfe \subseteq tso$
- $\wedge \quad \langle w, r \rangle \in G.rf \Rightarrow \neg \exists w' \in G.WU_{loc(r)}. [\langle w, w' \rangle \in tso \wedge \langle w', r \rangle \in tso \cup G.po]$

An execution is TSO-consistent if:

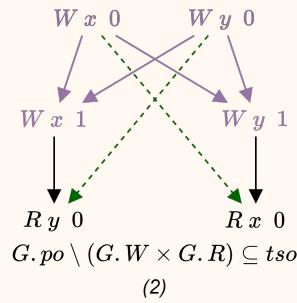
- G is complete
- G is TSO consistent with respect to some strict partial order tso on $G.E$
- The writes have a total order, and the program ordering for (write \rightarrow write) and (read \rightarrow read) are in tso .



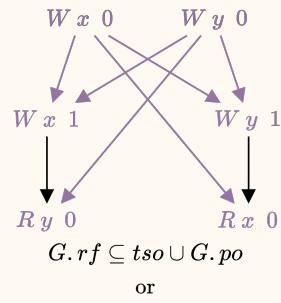
Show the graph is TSO-Consistent.



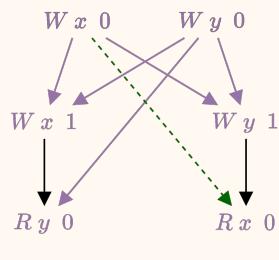
(1)



(2)



(3)



(4)

We now look for:
 $W x 0 \xrightarrow{\text{and}} W x v$
 $W x v \xrightarrow{\text{or}} R x 0$

But none is present

Likewise for
the other rf

Hence it is
TSO-consistent

(5)

Alternative TSO

Definition 5.4.2

An execution graph G is TSO-Consistent if:

$$\begin{aligned} & G \text{ is complete} \\ \wedge \quad & \exists \text{ modification order } \text{mo}. [G.\text{rfi} \cup G.\text{rbi} \subseteq G.\text{po} \wedge \text{acyclic}(\text{ppo} \cup G.\text{rfe} \cup \text{mo} \cup \text{rbe})] \end{aligned}$$

Where $\text{ppo} \triangleq (G.\text{po} \setminus (G.W \times G.R))^+$ (preserved program order) and $\text{rb} \triangleq G.\text{rf}^{-1}; \text{mo} \setminus \text{id}$.

5.5 Coherent

Coherence (COH)

Definition 5.5.1

Considered "sc per location"

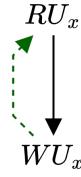
$$\begin{aligned} & G \text{ is complete} \\ \wedge \quad & \text{for each location } \textcolor{blue}{x} \text{ there is a strict total order } \text{sc}_x \text{ such that:} \\ & \langle a, b \rangle \in G.\text{po} \Rightarrow \langle a, b \rangle \in \text{sc}_x \\ \wedge \quad & \langle a, b \rangle \in G.\text{rf}_x \Rightarrow \langle a, b \rangle \in \text{sc}_x \wedge \neg \exists c \in G.WU_{\textcolor{blue}{x}}. [\langle a, c \rangle \in \text{sc}_x \wedge \langle c, b \rangle \in \text{sc}_x] \end{aligned}$$

$$SC : \text{acyclic}(\text{po} \cup \text{rf} \cup \text{mo} \cup \text{rb})$$

$$SC : \text{acyclic}(\text{po}_{loc} \cup \text{rf} \cup \text{mo} \cup \text{rb})$$

5.5.1 Bad Patterns

As coherence is the weakest model, any pattern disallowed under coherence is disallowed under all models.



$r := x$ Read v
 $x := v$

rf; po is irreflexive

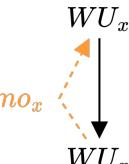
No Future Read



$r := \text{CAS}(x, v, v)$ Read v

rf is irreflexive

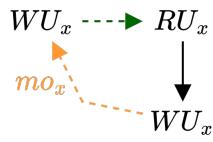
RMW 1 Cannot Read from Self



$x := v$ Write v'
 $x := v'$ Write v

mo; po is irreflexive

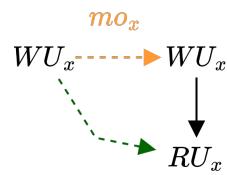
Coherence WW



$x := v$ Write $v' \parallel r := x$ Read v
 $x := v'$ Write v

mo; rf; po is irreflexive

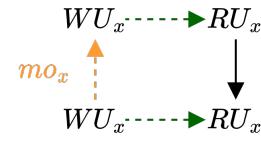
Coherence RW



$x := v \parallel x := v'$
 $r := x$ Read v

$r^{-1}; mo; po$ is irreflexive

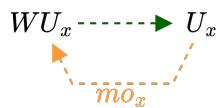
Coherence WR



$x := v \parallel r := x$ Read v'
 $x := v' \parallel r := x$ Read v

$r^{-1}; mo; rf$ is irreflexive

Coherence RR



mo; rf is irreflexive

RMW 2

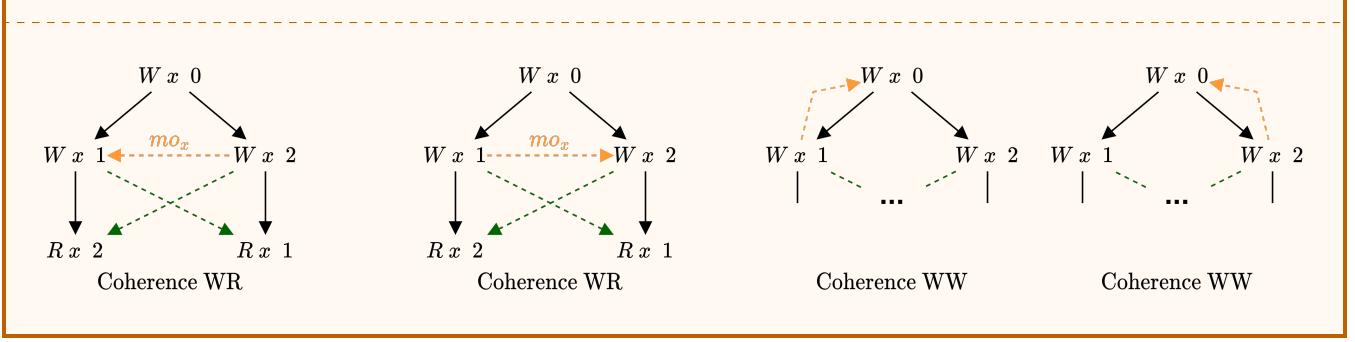


$r^{-1}; mo; mo$ is irreflexive

Atomicity

Determine if the following is COH-Consistent:

$$\begin{array}{l} x := 0 \\ x := 1 \parallel a := x \quad \text{Read 1} \\ \qquad \qquad \qquad b := x \quad \text{Read 2} \end{array}$$



5.6 Atomicity

COH is often too weak to be useful. As an example if we attempt to implement a lock

$$\begin{array}{l} \textcolor{violet}{x} := 0 \\ a := \textcolor{orange}{FFA}(x, 1) \parallel b := \textcolor{red}{FFA}(x, 1) \end{array}$$

Guarantees that $a = 1 \vee b = 1$.

We could attempt to implement spinlocks with a basic CAS

Lock(l)

$$\begin{array}{l} a := 0 \\ \text{while } \neg r \text{ do } r := \text{CAS}(l, 0, 1) \end{array}$$

Unlock(l)

$$l := 0$$

However this will not provide mutual exclusion as we are relying on the ordering of memory accesses to multiple locations. COH only guarantees sequential consistency per location.

Here we attempt to do basic message passing using the location y . Given initially $x = y = 0$:

$$\begin{array}{c} \textcolor{violet}{x} := 42 \parallel \textcolor{violet}{a} := y \\ \textcolor{blue}{y} := 1 \parallel \text{while } \neg a \text{ do } a := y \\ \qquad\qquad\qquad \textcolor{violet}{b} := x \end{array} \quad \text{Read 0}$$

5.7 Release/Acquire

Release/Acquire Memory Model (RA)

Definition 5.7.1

Where mo is a modification order on execution graph G , G is RA-Consistent if:

$$G \text{ is complete} \wedge \text{acyclic}(\text{hb}_{ra} \cup \text{mo} \cup \text{rb}) \text{ where } \text{hb}_{ra} \triangleq (\text{po} \cup \text{rf})^+|_{loc}$$

We can also define it as if:

$(\text{po} \cup \text{rf})^+$	is irreflexive	(No Future Read)
$\text{mo}; (\text{po} \cup \text{rf})^+$	is irreflexive	(Coherence WW)
$\text{rf}^{-1}; \text{mo}; (\text{po} \cup \text{rf})^+$	is irreflexive	(Coherence WR)
$\text{rf}^{-1}; \text{mo}; \text{mo}$	is irreflexive	(RMW Atomicity)

For comparison:

$$\begin{array}{l} SC \sim \text{acyclic}(\text{po} \cup \text{rf} \cup \text{mo} \cup \text{rb}) \\ RA \sim \text{acyclic}((\text{po} \cup \text{rf})|_{loc} \cup \text{mo} \cup \text{rb}) \\ COH \sim \text{acyclic}(\text{po}|_{loc} \cup \text{rf} \cup \text{mo} \cup \text{rb}) \end{array}$$

We can see that the addition of rf to the per location ordering strengthens it over COH.

5.8 Ordering Models

$$COH < RA < TSO < SC$$

We can also express this in terms of the set of consistent executions:

$$\text{execs}(SC) \subset \text{execs}(TSO) \subset \text{execs}(RA) \subset \text{execs}(COH)$$

Hence for two memory models $MM_A < MM_B$:

$$\begin{aligned} G \in \text{execs}(MM_B) &\Rightarrow G \in \text{execs}(MM_A) \\ G \notin \text{execs}(MM_A) &\Rightarrow G \notin \text{execs}(MM_B) \end{aligned}$$

Chapter 6

Concurrent Objects

6.1 Concurrent Queues

We start with a basic interface defining the behaviour of a queue.

```
interface Queue<T> {
    val count: Int
        get

    val isEmpty: Boolean
        get() = count == 0

    fun enq(item: T): Boolean
    fun deq(): T?
}
```

6.1.1 Circular Queue

```
class CircularQueue<T>(val capacity: Int) : Queue<T> {
    var head: Int = 0 // next pop present here
    var tail: Int = 0 // next item pushed here
    var items = mutableListOf<T?>(capacity){null}

    override val count: Int
        get() = if (head >= tail) head - tail else head + (capacity - tail)

    override fun enq(item: T): Boolean {
        if (count < capacity) {
            items[head] = item
            head = (head + 1) % capacity
            return true
        } else {
            return false
        }
    }

    override fun deq(): T? {
        if (isEmpty) {
            return null
        } else {
            val retval: T = items[tail]!!
            tail = (tail + 1) % capacity
            return retval
        }
    }
}
```

6.1.2 Lock Based Queue

Mutual exclusion is used to prevent concurrent modification, and hence make thread safe.

6.1.3 Wait Free 2-Thread Queue

UNFINISHED!!!

6.2 Sequential and Concurrent Objects

Object	Definition 6.2.1
Objects are data structures containing internal state (fields/attributes/members) and methods (functions that can be provided input, and access/mutate the object's internal state).	

In concurrent programming, the liveness and safety properties of an object must be specified.

- Need to define how to assess the implementation as correct
- Need to define under which conditions progress (e.g no livelock/deadlock) is guaranteed

6.2.1 Sequential Specifications

Precondition Object state before method call

Postcondition (Result) Value returned by the method, or exceptions thrown

Postcondition (State) The state of the object when the method returns

We do not need to consider the state of the object between the rep and post conditions.

- State is meaningful between method calls (postcondition (state) → precondition)
- Each method call can be considered a single atomic event
- Methods can be described in isolation
- New methods can be added without changing the descriptions of older methods

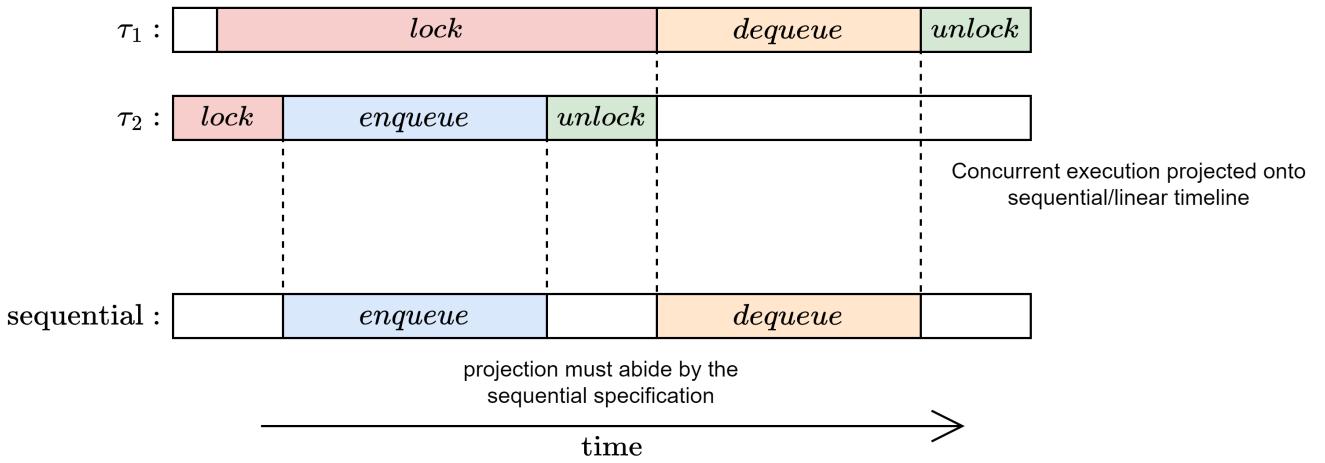
6.2.2 Concurrent Specifications

A method call is no longer an atomic event.

- A method call is a sequence of interval events.
- Method calls overlap in time.
- Object may never be *between method calls* as many calls may constantly overlap
- All interactions between concurrent calls must be characterised
- When adding a new method, it must be considered in the context of all existing method definitions
- **everything can interact with everything else**

Linearisable	Definition 6.2.2
A set of operations are linearisable if it can be re-expressed as a sequential history.	

Object Linearisability	Definition 6.2.3	Execution Linearisability	Definition 6.2.4
An object is linearisable if all its possible executions are linearisable. <i>Not studied in this course</i>		<ul style="list-style-type: none">• Method takes effect instantaneously somewhere between the invocation and response events.• If the <i>sequential</i> behaviour is correct then the execution is linearisable.	

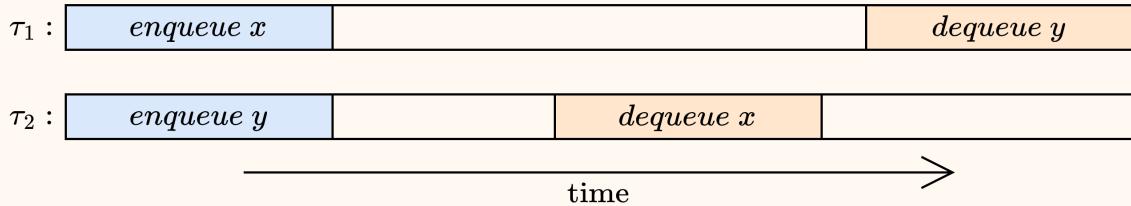


- To show an execution is linearisable, we find the linearization points (where the method *instantaneously* occurs)
- Typically arrows are used, where a bold arrow shows the time for the execution of some method, and an arrow with a dotted tail is one that never responds/returns (e.g. thread killed).
- For invocations that never respond/return, we can decide if the method occurred or not (depending on what *makes sense*/is required to justify the execution).

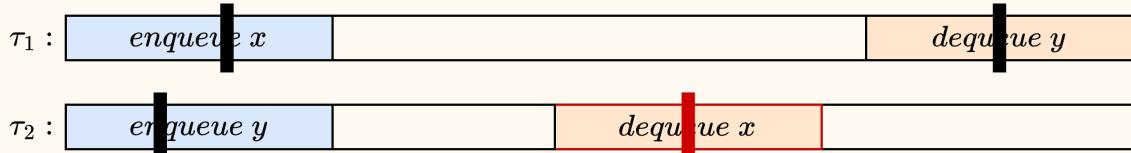
Valid Linearisations

Example Question 6.2.1

Determine the valid linearisation for the following execution.



invalid linearisation :



Breaks specification for dequeue, as y was enqueued first, it should be first to dequeue

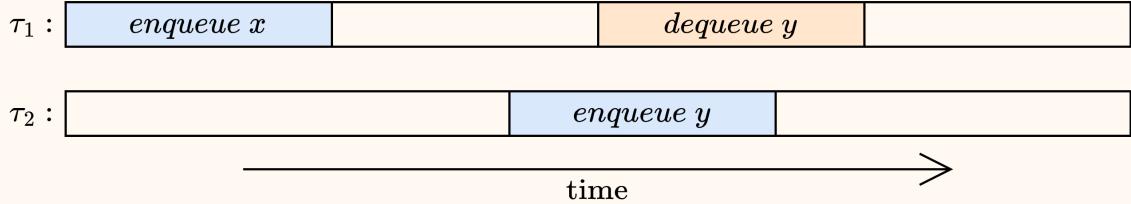
valid linearisation :



Valid Linearisation

Example Question 6.2.2

Determine if there is a valid linearisation for the following execution.

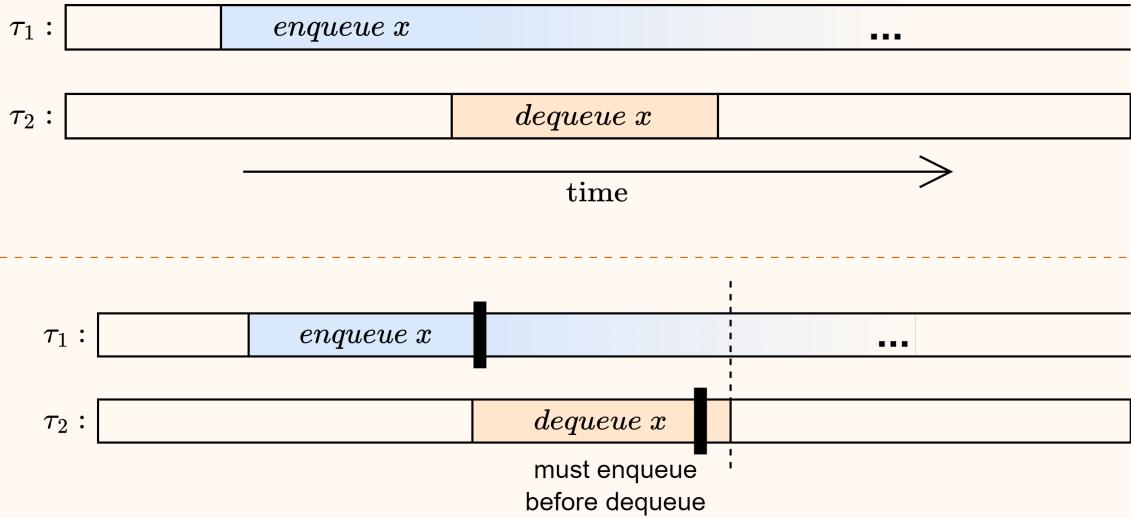


There is none, this is as the entry to *enqueue x* is before the entry to *enqueue y*, hence in any linearisation *enqueue x* comes first. This means that the *dequeue y* breaches the specification of *dequeue*.

No Return

Example Question 6.2.3

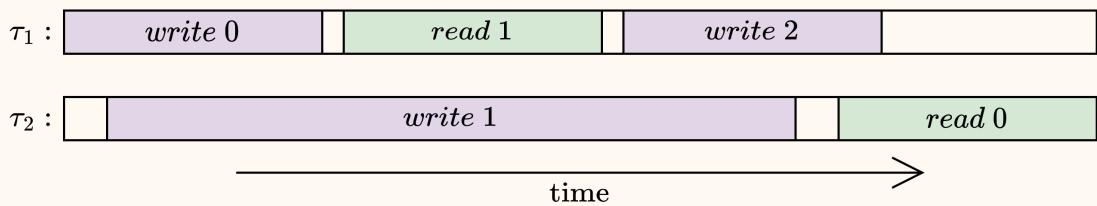
Is the following linearisable?

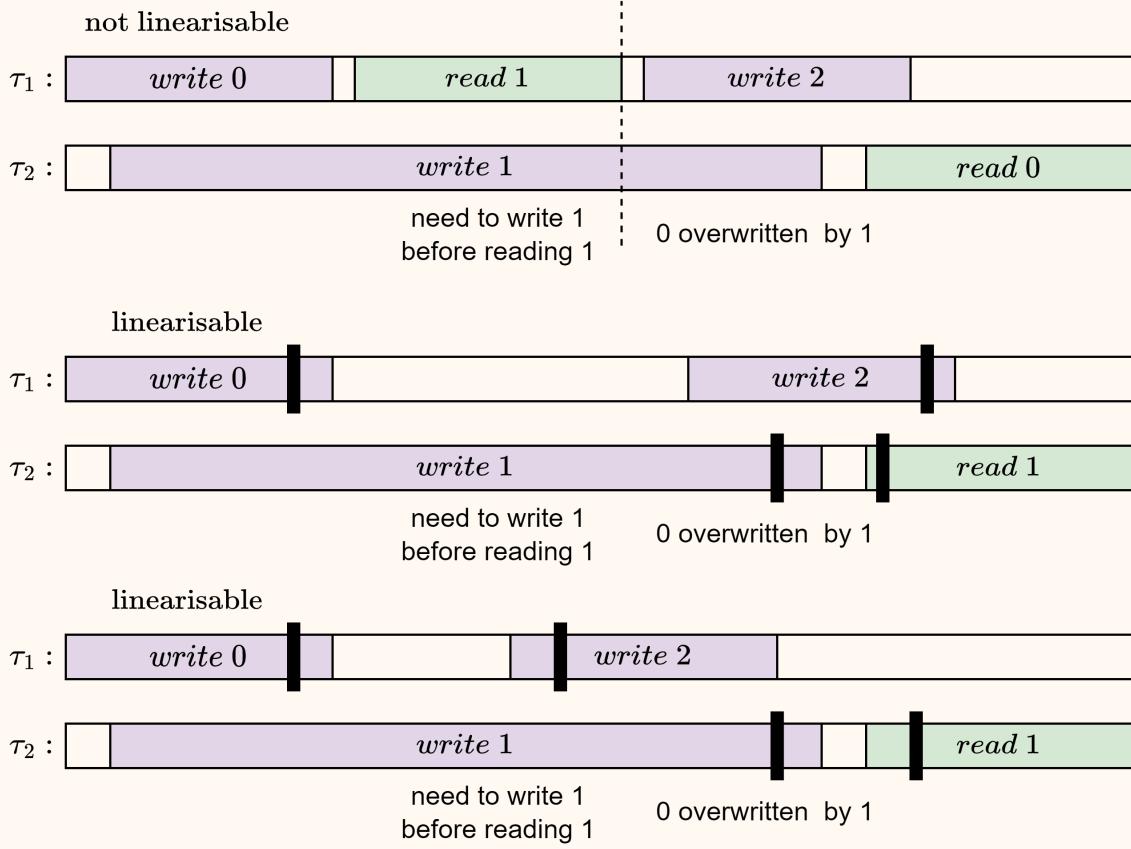


Register Writing

Example Question 6.2.4

Is the following execution linearisable, and if not then provide modified examples of how it could be linearisable.





6.3 Formal Model of Executions

Invocation and Response Notation

Definition 6.3.1

Invocation $Thread \ object . method(args\dots)$	Response $Thread \ object : return$
---	--

- Method name is implicit for response (a thread can only execute one method at once, so response directly follows that thread's last invocation)
- An invocation is pending if there is no matching response

Histories

Definition 6.3.2

A history H is a sequence of invocations and responses. For example:

$$H = \begin{array}{ll} A & q.enq(7) \\ B & p.enq(6) \\ B & p : void \\ B & q.deq() \\ A & q : void \\ B & q : 7 \end{array}$$

$$H|A = \begin{array}{ll} A & q.enq(7) \\ A & q : void \end{array} \quad H|B = \begin{array}{ll} B & p.enq(6) \\ B & p : void \\ B & q.deq() \\ B & q : 7 \end{array} \quad H|q = \begin{array}{ll} A & q.enq(7) \\ A & q : void \end{array} \quad H|p = \begin{array}{ll} B & p.enq(6) \\ B & p : void \end{array}$$

- A history is *well formed* if the per-thread projections are sequential.
- A history is *sequential* if every invocation is immediately followed by its corresponding response.
- Histories are *equivalent* if the per-thread projections are equivalent.
- A history is *legal* if for every object x , $H|x$ is in the sequential spec for x .

Equivalent Histories

Example Question 6.3.1

Are H and G equivalent?

$$H = \begin{array}{ll} A & q.enq(7) \\ B & p.enq(6) \\ B & p : void \\ B & q.deq() \\ A & q : void \\ B & q : 7 \end{array} \quad \text{and } G = \begin{array}{ll} A & q.enq(7) \\ B & q : 7 \\ B & q.deq() \\ A & q : void \end{array}$$

Yes, as $H|A = G|A$ and $H|B = G|B$.

Precedence

Definition 6.3.3

A method call x precedes another y if the response of x is before the invocation of y . This is written as:

Given $H \quad m_0 \rightarrow_H m_1$ if m_0 precedes m_1

- Precedence is a partial order (some methods overlap)
- For a fully sequential history, it is a total order.

Linearisability Formally

Definition 6.3.4

A history H is linearisable if it can be extended to G by:

- Appending zero or more responses to pending invocations.
- Discarding pending invocations.

Where G will be equivalent to the *legal sequential* history S and $(\rightarrow_G \subseteq \rightarrow_S)$

Composability Theorem

Definition 6.3.5

$$\text{linearisable}(H) \Leftrightarrow \forall x. [\text{linearisable}(H|x)]$$

A history H is linearisable if and only if for every object x , $H|x$ is linearisable.

- This allows for the linearisability of objects to be considered independently, and then composed.

6.4 (

Sequential Consistency) A history H is Sequentially Consistent if it can be extended to G by:

- Appending zero or more responses to pending invocations.
- Discarding pending invocations.

Where G will be equivalent to the *legal sequential* history S . Unlike with linearisability, G does not have to be a subset of S .

UNFINISHED!!!

Chapter 7

Credit

Image Credit

Front Cover Intel Xeon e7 on wikichip here.

Content

Based on the Concurrency course taught by Dr Azalea Raad and Prof Alastair Donaldson.

These notes were written by Oliver Killane.