The C1x and C++11 concurrency model

Mark Batty

University of Cambridge

October 27, 2012

With coauthors: J. C. Blanchette, K. Memarian, S. Owens, S. Sarkar, P. Sewell, and T. Weber

Sequential consistency

Sequential consistency

Pthreads

Sequential consistency

Pthreads

Java

Sequential consistency

Pthreads

Java

Expose hardware model (e.g. ClightTSO)

Sequential consistency

Pthreads

Java

Expose hardware model (e.g. ClightTSO)

C++11/C1x: SC for data race free programs, almost...

C++11: the next C++ $\,$

1300 page prose specification defined by the ISO.

The design is a detailed compromise:

- hardware/compiler implementability
- useful abstractions
- broad spectrum of programmers

C++11: the next C++ $\,$

1300 page prose specification defined by the ISO.

The design is a detailed compromise:

- hardware/compiler implementability
- useful abstractions
- broad spectrum of programmers

We fixed serious problems in both C++11 and C1x, both now finalised.

The C1x/C++11 memory model

The C1x/C++11 memory model

- top level
- sequential execution
- simple concurrency
- expert concurrency
- very expert concurrency

The memory model is factored out from a symbolic operational semantics.

1. $P \mapsto E_1, ..., E_n$

The memory model is factored out from a symbolic operational semantics.

- 1. $P \mapsto E_1, ..., E_n$
- 2. $E_i \mapsto X_{i1}, ..., X_{im}$

The memory model is factored out from a symbolic operational semantics.

- 1. $P \mapsto E_1, ..., E_n$
- 2. $E_i \mapsto X_{i1}, ..., X_{im}$

3. is there an X_{ij} with a race? (actually, several kinds...)

A single threaded program





A single threaded program



The relations of a pre-execution

Each symbolic execution, E_i , contains:

- **sb** sequenced before
- asw additional synchronizes with
- dd data-dependence

The relations of a pre-execution

Each symbolic execution, *E_i*, contains: **sb** – sequenced before **asw** – additional synchronizes with **dd** – data-dependence

Each full execution, X_{ij} , also has:

- rf reads from
- sc SC order

mo – modification order

A data race



A data race



```
atomic_int x = 0;
atomic_int y = 0;
x.store(1, seq_cst); | y.store(1, seq_cst);
y.load(seq_cst); | x.load(seq_cst);
```





```
atomic_int x = 0;
atomic_int y = 0;
x.store(1, seq_cst); | y.store(1, seq_cst);
y.load(seq_cst); | x.load(seq_cst);
```



SC atomics

Read the last write in SC order.



Using only seq_cst reads and writes gives SC.

(Initialization is not seq_cst though...)

```
// sender // receiver
x = ...
y.store(1, release); // receiver
while (0 == y.load(acquire));
r = x;
                              a:W<sub>na</sub> x=1
sb
b:W<sub>rel</sub> y=1
                                              rf
                                                  rf c:R<sub>acq</sub> y=1
sb ↓
                                                        d:R_{na}x=1
```







Unlocks and locks synchronise too:



















Non-atomic loads read the most recent write in happens before. (This is unique in DRF programs)

The story is more complex for atomics, as we shall see.

Data races are defined as an absence of happens before.

A data race


Data race definition

```
let data_races actions hb =

{ (a, b) — \forall a \in actions b \in actions |

(a = b)

same_location a b

(is_write a is_write b)

(same_thread a b)

(is_atomic_action a is_atomic_action b)

((a, b) \in hb (b, a) \in hb) }
```

A program with a data race has undefined behaviour.

Relaxed writes: load buffering

```
x.load(relaxed); y.load(relaxed);
y.store(1, relaxed); x.store(1, relaxed);
```



No synchronisation cost, but weakly ordered.

Relaxed writes: independent reads, independent writes

Expert concurrency: fences avoid excess synchronisation



Expert concurrency: fences avoid excess synchronisation



```
// sender
x = ...
```

```
// receiver
while (0 == y.load(relaxed));
```

```
// sender
x = ...
y.store(1, release);
```

```
// receiver
while (0 == y.load(relaxed));
fence(acquire);
r = x;
```

// sender
x = ...
y.store(1, release);

// receiver
while (0 == y.load(relaxed));
fence(acquire);
r = x;



// sender
x = ...
y.store(1, release);

// receiver
while (0 == y.load(relaxed));
fence(acquire);
r = x;



// sender
x = ...
y.store(1, release);

// receiver
while (0 == y.load(relaxed));
fence(acquire);
r = x;



Modification order is a per-location total order over atomic writes of any memory order.

```
x.store(1, relaxed);
x.store(2, relaxed);
```

```
x.load(relaxed);
```

```
x.load(relaxed);
```

Modification order is a per-location total order over atomic writes of any memory order.



Modification order is a per-location total order over atomic writes of any memory order.

x.store(1, relaxed); x.store(2, relaxed);

x.load(relaxed);



Coherence and atomic reads

All forbidden!



Atomics cannot read from later writes in happens before.

A successful compare_exchange is a read-modify-write.

compare_exchange(&x, 2, 3, relaxed, relaxed);

```
x.store(1, relaxed);
x.store(2, relaxed);
x.store(4, relaxed);
```

A successful compare_exchange is a read-modify-write.

```
x.store(1, relaxed); | compare_exchange(&x, 2, 3, relaxed, relaxed);
x.store(2, relaxed);
x.store(4, relaxed); |
```

a:
$$W_{rlx} x=1$$
 d:RMW_{rlx} $x=2/3$
sb
b: $W_{rlx} x=2$
sb
c: $W_{rlx} x=4$

A successful compare_exchange is a read-modify-write.

```
x.store(1, relaxed); | compare_exchange(&x, 2, 3, relaxed, relaxed);
x.store(2, relaxed);
x.store(4, relaxed); |
```



A successful compare_exchange is a read-modify-write.

```
x.store(1, relaxed); | compare_exchange(&x, 2, 3, relaxed, relaxed);
x.store(2, relaxed);
x.store(4, relaxed); |
```



Weaker than acquire

Stronger than relaxed

Non-transitive happens before! (only fully transitive through data dependence, dd)

C1x and C++11 support many modes of programming: • sequential

- sequential
- concurrent with locks

- sequential
- concurrent with locks
- with seq_cst atomics

- sequential
- concurrent with locks
- with seq_cst atomics
- with release and acquire

- sequential
- concurrent with locks
- with seq_cst atomics
- with release and acquire
- with relaxed, fences and the rest

- sequential
- concurrent with locks
- with seq_cst atomics
- with release and acquire
- with relaxed, fences and the rest
- with all of the above plus consume

C1x and C++11 support many modes of programming:

- sequential
- concurrent with locks
- with seq_cst atomics
- with release and acquire
- with relaxed, fences and the rest
- with all of the above plus consume

Mathematizing C++ concurrency. M. Batty, S. Owens, S. Sarkar, P. Sewell, and T. Weber. In Proc. 38th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages (POPL), 2011.

The full model

- K-4 K 1 [K/I] (7			· · · · · · · · · · · · · · · · · · ·
]	control and get of a strategy from the set of the set o
which do a		The second se	In the property when these is come in terms of these particular and the operatory ratio dependence of
	Teleforgeneties an telefor an teleford a		
AND DECK		The second	(a single and a si
200	Substituted of the data and the second second	(here and here and he	19 Million State of the State o
		(Contrast as (Contrast as a second as a se	and the international state
alabraianala	And the second	(America)	
	August an	streaments of all the Truck balance of a second black attracts on the second and the dealers with development at the development of the second se	
and a second sec	inclusion and a reaction are an ended a	The second state that have all associated at the second of the design of the design of the second seco	Configuration of party data is a strategy party data is
$\mathcal{F}(c_{i}^{*}+i\theta) \cap \{i,j,k\}$	Applie as		The second
	spender revenuer reven	Application provide a second sec	(minute) =
ad rate brief	A Second Se	(b) 40 and b) a sublimination (c)	
Security of	has seeing at -	The advances of the second sec	
	(Margaret) (Margaret Margaret Margaret) -	dame of a	
M_10000000	" di kita dalar dadi samata farma an argan kanan "y	Application and a special stress from a subscription of the advancement on Application and a stress of the	
and poster of a radiant of time of	(New code)	Application stress operation where the end operation and the end of the end operation, so that dependency control and a stress of	The local diversity of the local diversity of the
			Samp
Midward a set o Midward a set o	wand a transmit whe an firm Mr. remented	* - attitude publications, faith Read Joint AC - *)	an Granden
- prody carding line of			(1) Specific Constraints (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
AND AND AND AND A REAL	the statigetters of	Comparison of the second se	Ban (1/2) and () and asymptotic field of the (P = 2.5) (1/2) (and () and () and ()
minutes are set	And and a first parameter the program (the program (the	Company and an and a second seco	an (h.1)
(Sec)	(post-college)	Section at any section of the sectio	Photo 2
partie Synchologie (* partie Sie Syn	Annual a characturate a characturate		a second as
(and a second s		Service and approximate and approximate the service and ap	many beams and a perpendicular to a
-5,	human and a	Pagetoning of the schlaged managed many schlaged managed and	Practice Control of Co
	Non-mark	(max because a diagonal diag	
anyone contra		Sydnes at hydrose at	The second secon
Spectra share and	and the second sector of the s	Sector server in the sector in the sector is	parage in the second se
	And house and house the	Laster and the set for the set.	Physics and the second se
Contraction and	NUMBER OF STREET, STREET, ST.	(we a summarized and a set of the set	(3).41 Spirit A Longentine add toppening proton in
tips offer house strag	(Attack - sparpspare attacked attack at (Attack - S	(Section and Section and Secti	to a design of the second se
	<u></u>	(In considering an implementation of a second	(1943) - S. Sagarang and A.
Spectrum and any	And the stand of the stand stand of the stand s	(w. a minimum a di 400	
providence :	Total 1 - (Andread 1 - M)		(PAR) - Annual A
Million Control of Con		and an analysis of the basis and approximate address of the specific contraction of th	this gas suggested ()
Marcana Contractor	Party and the second seco	concerning the attem to the terrely our advanced on advanced on the expension of the advanced of the second of the expension	("An alterna")
The print of the p		and a second	(1997)
	Technic class during a 1	again the second se	Depine of species of higher price and methods and and an
where a state of sectors and sectors		and a second second second second second data and the second	allow for
Without all adding a band of bands and the second s	Part of the experiment of a state of the second state of the secon	and apply and a provide the second second advantation of the experiment with the appendix provide advantation of a transmission of a second seco	- Part - Pa - Part - Pa
Arrest officer of article finance and provide state burdles of			1964 (1964 (1
These of action of ficing of function and Within all actions of ficing of functions and	semplement at a transport or a transport to	Appendix y when i do not a demander on p y	Particular to a second a sec
Process of actions of fease of memory action process		The system of systems in the system of the s	and the proceeding of the second seco
processing on an exactly	sentences a set of a disc of sense band a di-	(a	
			1
present of the second s			Provide and the second s
	emploties of closelse a choice (The contraction of the contracti
And an and a second sec	magnetia el c(octo e tocho i) heritagi altare (1-le fontes e font i)	Republic generative states trans to the state and a point and a difference of the spectra generative state approximation of the spectra state approximation	**Perceivante en estadores e entretante en el conservante en el conservante en el conservante en e
Terrate (Marcal Marca) provide provide (Marca) provide provide (Marca) provide provide (Marca) provide provide (Marca) provide (Marca) p	magneties of a location of a bandward () Andreage address (). No (Northean a t-Street ())		
	emploties at a (horizo a chaoles i) horizograf advance (chaoles a chaole ii) horizograf advance (chaoles a chaole iii) horizontal (chaoles a chaole iii) horizontal (chaoles a chaoles iii)	A participative and the two tests are particles attracted and the participation of the type of the typ	Programme and a second
	energianten edi - (Section e i Section d) horizongal anteno () (% (Section a r Section d) sectionary anteno () (% (Section a r Section d) sectionary anteno () (% (Section a r Section d)) (Sectionary anteno () (Sectionary d) (Sectionary d)) (Sectionary d) (Sectionary d) (Sectionary d)) (Sectionary d) (Sectionary d) (Sectionary d) (Sectionary d)) (Sectionary d) (Secti	Epidegalangkang dan kuta kuta kuta kuta kuta pana kuta dan pana kuta pana pana pana pana pana pana pana pa	
$\label{eq:started} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0$	Interpreter at 1 (South 4) Entiting of addres () is (South 4) Interpreter at 1 (South 4) Interpreter at 2 (South 4) Interpre		I Per Bernard Base market in Series and Series and Ser
	emplote of closes a closes (term of the closes of the cl		
	Integrated all (Johns 1 (Malls 1)) Integrating a street () is descent as from () Integrating a street () is descent as from () Integrating a street () is descent as from () Integrating a street () Integrating a stree		
Turning (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	Singless 44 - (bits 4 - bits 5) B Singless 44 - (bits bits 4 - bits 5) B Singless 5 - (bits bits 4 - bits 5) B Singless 5 - (bits bits 4 - bits 5) B Singless 5 - (bits 5) B	An appropriate the second and appropriate the second appropriat	
	Exception of theme is sense if a finite in the left of		
and a second sec	Employee and the set of the set o		
	Experimental and a second and a		
	Experimental actions a state of the second sta		The second secon
			<pre>Procession Proces</pre>
	International control of the second s		
			The second secon
			* Particular State St
			Production of the second
	The second secon		Programme and an an and a
			* Particular sectors of the sector sector sector
			* Series of the series of t
	American constraints and an an analysis of the analysis of th		Bernson and B
	And the second s		Programme and
	International Action of the second se		<pre> transmission transmission</pre>
			<pre>************************************</pre>

The full model

		with all offer at a first from the basis and operated with an all states of all independency control dynamics (loggers and as)
	Second optimizers	[4] A dependencies (1) (1) (-4) Ib only on a product where the base and aspects before approximately on dependency control dependency control dependency control dependency.
Telephone and a second s		
		The product of the pr
	Technic and T	is any data and the second sec
Second construction of the second second	and the second s	(h singled million of a million of a
	The second	
	American Collinson	
Appendix of		
Technical entrement entrement et la construction et la construction et la construction et la construction et la		Internet and a second
		Constant C
	Transferration and the second s	(and of)
	Topological and	
	Suppose at a substant at	
Topper I	System (1)	with proving a period of the second state and a
(An and the second seco		in processing of the section of the
P. A. E. Martin and A. Arrange Street and Array Street Street.	Application and a second active from the second active product of the second seco	
The second of the second of the second secon	Application of the second se	(16) Second A Line and A second and A second at the second
		P (the second se
Approximate and a second point and the province)	Contraction of the second seco	an (112-0).
	a demonstration of the second se	(16 Secold Conjecture and the Co
	(see gravity with a classifier of a state of	F (1) and (a) anti-approximation data (F = 1) from (F) and (a) anti-approximation data (F).
NAME AND ADDRESS OF A	System of space time to the time of the second s	(F = 4) (F = 4 and (F = 4))
And a standard	Providence advances - 1	and (in a real).
(provide a Margaret a)	 Section of provide the complete test 	Press A
And a characteristic contract the second		a Statistica A.
	Septem at higher at regime to receipt to	many pointing of a 1 styp physical pointing in the second se
Instrument is	(No No anno-Jacobian a p.). Pagatanti parlam a 1 agustant parlam p. 1 agustan a 1.	Proceeding of the second se
1	A manufacture and a second and a	Part
and a second sec	Contraction of the Contraction o	2 Sax.
	A Second Se	the part of the second s
2. Contraction of the contractio	The comparison of the	Para UNITY
(max more part of	a manufacture of the second	1 Martine Control of C
The second	la - contra	Sprite & suspenses and representations of
Contract - Appropriate and Approximate and	Section of the sectio	
	The comparison of the first sector and the sector a	Charles & Sector and A
Page processing devices and approximate processing devices	the a statement of the second s	
The second secon		PROF. A MARKAN
The second secon	and the state of the state to be a state of the addition of the addition of the state of the sta	the second se
Telephone and the second se	(choose of the street from the street process where a process of the street proces of the street process of the street proces of the	Character 7
appendent term		1997
	and a second sec	The Wey Ally American Stream of the Index and the All
Systematic Congress		and the second sec
	and a particular provide the second second second states and second with the second seco	1 () () () () () () () () () (
Type process produces a company of the terms of	and apply and any provide the second second and an additional production of the adjustment product second	(1997)
(The All States of the All Stat
sugeries at changes a changes to	Appendix present secure a demonstration of a contract of the secure secu	Performance at a second of a s
employed at a linearphysic to the applied of the second se	Angebang period period and a constraint	Destinguistication of compared is specifies in specifies and specific spec
Interference (Conservation of Conservation of	a papara para para para para para para	Inclusion and a failed in a Chapter A. Second Street Stree
anaginal all - (tradigligt a - thoughful 6) Mentopolitikasi Mentopolitik	n parte (and a second and a second a se	Production of Selection (Selection (Sel
emplored at 1 (Interplat + Headport 6) Mediate products at 1 (Interplat + Mediate 4) Headport at 1 (Interplat + Mediate 4) Headport at 1 (Interplat + Mediate 6)	Balance produces a temperature of temperature of the spectra set of the spectra production of temperature of te	 Province and address content of a second seco
emplote at 1 (brought i i trought i) Records at 2 (brought i i trought i) Records at 2 (brought i i trought i) - strought i i trought i i trought i i Records at 2 (brought i trought i) Records at 2 (brough	Representation of a set of the se	The second and a second and as second and a
Lengende et al Elengények et tendények () Recellengenségése () et al. Services et al. () elengén () et al. () elengén () Lengensége et al. () elengén () el al. () elengén () Tennények etters () () él () elense () elense ()	Example of the second s	Hearing and a constraint of the second
Internet al (Dampy 4) a many 40 Internet and (Dampy 4) a many 40 Internet and (Damp) Internet and (Damp) Inter		r angelegie and angelegie and angelegie angele
sergence of a prompet of sensingly 0 Series of a prompet of a sensingly 0 Series of a series of a sensingly 0 Series of a series of a s		r Participa de la construcción d
sequences of the company's in second of the company's in the company's in the company's in the company's intervention of the company's interventintervention of the company's interventintervention of the company'		
Imperied a compared to a compa		
emperation of the second secon		r special sector
segment and analogies in the segment of the se		
memory of a consequence of a consequenconsequenconsequence of a consequence of a consequence of a cons		Provide a second s
Englisher (Single) - Single)		
Experimental Sector Secto		
Experimental Control of Cont		Section 2012 S
experimental energy of a second		Section 2012 S
september 1		
		Section 2012 S
	A set of the set	Section 2015 S
Applied and applied appli	And Section Control Contr	Section 2015 S
		Section 2015 S
	Experiment E	Section 2015 S
Extension American Americ	A second se	Series of the series of t
	A region of the second se	
	Provide a second s	Section 2015 S
	Programmer Programe Programmer Programmer Programmer Programmer	Bernselsensel
	Bernsteinen Bernstein	Procession of the second
Second se		Sector
	Programmer Programer Programmer Programmer Programmer Programmer	Section 2015 S
	Provide a second s	Section 2012 S
	Add add add add add add add add add	Section 2012 S
	Provide a constraint of the constraint of t	Section 2012 S
	A second se	Image: Section of the sectio

Theorems

Are C1x and C++11 hopelessly complicated?

Programmers cannot be given this model!

With a formal definition, we can do proof, and even mechanise it.

What do we need to prove?

Are C1x and C++11 hopelessly complicated?

Programmers cannot be given this model!

With a formal definition, we can do proof, and even mechanise it.

What do we need to prove?

- implementability
- simplifications
- libraries

Implementability

Can we compile to x86?

Implementability

Can we compile to x86?

Operation	x86 Implementation
load(non-seq_cst)	mov
load(seq_cst)	lock xadd(0)
store(non-seq_cst)	mov
store(seq_cst)	lock xchg
fence(non-seq_cst)	no-op

x86-TSO is stronger and simpler.

Recall the C/C++ semantics for program P:

1. $P \mapsto E_1, ..., E_n$,

Recall the C/C++ semantics for program P:

1. $P \mapsto E_1, ..., E_n$, each an E_{opsem}

Recall the C/C++ semantics for program P:

1.
$$P \mapsto E_1, ..., E_n$$
, each an E_{opsem}
2. $E_i \mapsto X_{i1}, ..., X_{im}$,

Recall the C/C++ semantics for program P:

1. $P \mapsto E_1, ..., E_n$, each an E_{opsem} 2. $E_i \mapsto X_{i1}, ..., X_{im}$, collectively X_{witness}
Recall the C/C++ semantics for program P:

1. $P \mapsto E_1, ..., E_n$, each an E_{opsem} 2. $E_i \mapsto X_{i1}, ..., X_{im}$, collectively X_{witness} 3. is there an X_{ij} with a race? (actually, several kinds...)

Recall the C/C++ semantics for program P:

1. $P \mapsto E_1, ..., E_n$, each an E_{opsem} 2. $E_i \mapsto X_{i1}, ..., X_{im}$, collectively X_{witness} 3. is there an X_{ij} with a race? (actually, several kinds...)

In x86-TSO:

Events and dependencies, $E_{\rm x86}$ are analogous to $E_{\rm opsem}$.

Recall the C/C++ semantics for program P:

1. $P \mapsto E_1, ..., E_n$, each an E_{opsem} 2. $E_i \mapsto X_{i1}, ..., X_{im}$, collectively X_{witness} 3. is there an X_{ij} with a race? (actually, several kinds...)

In x86-TSO:

Events and dependencies, E_{x86} are analogous to E_{opsem} . Execution witnesses, X_{x86} are analogous to $X_{witness}$.

Recall the C/C++ semantics for program P:

1. $P \mapsto E_1, ..., E_n$, each an E_{opsem} 2. $E_i \mapsto X_{i1}, ..., X_{im}$, collectively X_{witness} 3. is there an X_{ij} with a race? (actually, several kinds...)

In x86-TSO:

Events and dependencies, E_{x86} are analogous to E_{opsem} . Execution witnesses, X_{x86} are analogous to $X_{witness}$. There is not a DRF semantics.

Theorem



Theorem



We have a mechanised proof that C1x/C++11 behaviour is preserved.

Implementability

Can we compile to IBM Power?

Implementability

Can we compile to IBM Power?

C++0x Operation	POWER Implementation
Non-atomic Load	ld
Load Relaxed	ld
Load Consume	ld (and preserve dependency)
Load Acquire	ld; cmp; bc; isync
Load Seq Cst	<pre>sync; ld; cmp; bc; isync</pre>
Non-atomic Store	st
Store Relaxed	st
Store Release	lwsync; st
Store Seq Cst	sync; st

We have a hand proof that C1x/C++11 behaviour is preserved.

Implementability

Can we compile to IBM Power?

C++0x Operation	POWER Implementation
Non-atomic Load	ld
Load Relaxed	ld
Load Consume	ld (and preserve dependency)
Load Acquire	ld; cmp; bc; isync
Load Seq Cst	<pre>sync; ld; cmp; bc; isync</pre>
Non-atomic Store	st
Store Relaxed	st
Store Release	lwsync; st
Store Seq Cst	sync; st

We have a hand proof that C1x/C++11 behaviour is preserved.

Clarifying and compiling C/C++ concurrency: from C++0x to POWER. M. Batty, K. Memarian, S. Owens, S. Sarkar, and P. Sewell. In Proc. 39th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL), 2012.

Simplifications and meta-theorems

Full model – visible sequences of side effects are unneeded (HOL4).

Simplifications and meta-theorems

Full model – visible sequences of side effects are unneeded (HOL4).

Derivative models:

- without consume, happens-before is transitive (HOL4).
- DRF programs using only seq_cst atomics are SC (false).

Full model – visible sequences of side effects are unneeded (HOL4).

Derivative models:

- without consume, happens-before is transitive (HOL4).
- DRF programs using only seq_cst atomics are SC (false).

```
atomic_int x = 0;
atomic_int y = 0;
if (1 == x.load(seq_cst)) | if (1 == y.load(seq_cst))
atomic_init(&y, 1); | atomic_init(&x, 1);
```

atomic_init is a non-atomic write, and in C1x/C++11 they race...

- Provide simplified models for higher level constructs.
- Formal description of mutual exclusion in terms of happens-before.
- We need libraries that provide a simpler model to programmers.

$$\ensuremath{\operatorname{CPPMEM}}$$ helps explore and understand the model

Code in, all executions out

Confidence and speed

Communication

1. $P \mapsto E_1, ..., E_n$ — tracking constraints

2. $E_i \mapsto X_{i1}, ..., X_{im}$ — automatically uses formal model

3. is there an X_{ij} with a race?

Refinements to the standards

The current state of the standard

Fixed:

- Happens-before
- Coherence
- seq_cst atomics were more broken

The current state of the standard

Fixed:

- Happens-before
- Coherence
- seq_cst atomics were more broken

Not fixed:

- Self satisfying conditionals
- seq_cst atomics are still not SC

Self-satisfying conditionals



- Syntactic divide supported by simpler memory models.
- Increasingly reasonable, consistent specification.
- Remaining problems far less serious than Java.
- Implementable above key architectures.

Conclusion

It's OK to like the C++0x memory model design

Our formal model lets us make fun things (go use it!)

- Optimized compilation?
- Static analysis?
- Dynamic analysis?
- Observational congruence?
- Program logics?

Conclusion

It's OK to like the C++0x memory model design

Our formal model lets us make fun things (go use it!)

- Optimized compilation?
- Static analysis?
- Dynamic analysis?
- Observational congruence?
- Program logics?

Nitpicking C++ concurrency. J. C. Blanchette, T. Weber, M. Batty, S. Owens, and S. Sarkar. In Proc. 13th International ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP), 2011.