An Algebraic Language for Specifying Quantum Networks

Anita Buckley[1] Pavel Chuprikov[1] Rodrigo Otoni[1] Robert Soulé[2] Robert Rand[3] Patrick Eugster[1]

[1] USI Lugano, Switzerland
[2] Yale University, USA
[3] University of Chicago, USA

Quantum networks

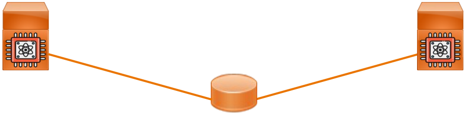
Quantum networks are networks connecting quantum capable devices

Quantum networks

Quantum networks are networks connecting quantum capable devices

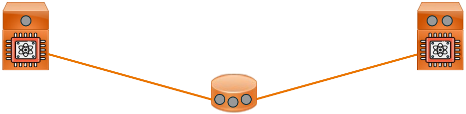
Quantum networks

Quantum networks are networks connecting quantum capable devices



Quantum networks

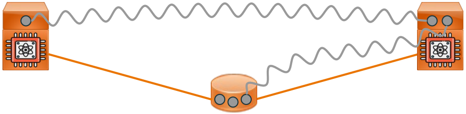
Quantum networks are networks connecting quantum capable devices



– **Communication qubits** designated to establish *connections* between devices

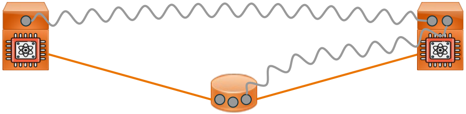
Quantum networks

Quantum networks are networks connecting quantum capable devices



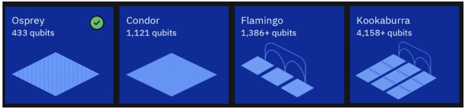
- **Communication qubits** designated to establish *connections* between devices
- Distributed **entanglement:** communication qubits sharing a *correlated random secret*

Quantum networks are networks connecting quantum capable devices



- **Communication qubits** designated to establish *connections* between devices
- Distributed **entanglement:** communication qubits sharing a *correlated random secret*

Benefits: **scaling of quantum computation** and **secure communication**



[1]

- teleportation
- entanglement based QKD

[1] [IBM Quantum: Development Roadmap *2023*]

Quantum networks are coming into reality

DOI:10.1145/3524455

A deep dive into the quantum Internet's potential to transform and disrupt.

BY LASZLO GYONGYOSI AND SANDOR IMRE

Advances in the Quantum Internet

QUANTUM INFORMATION WILL not only reformulate our view of the nature of computation and communication but will also open up fundamentally new possibilities for realizing high-performance computer architecture and telecommunication networks. Since our data will no longer remain safe in the traditional Internet when commercial quantum computers become fully available,[1,2,8,15,34] there will be a need for a fundamentally different network structure: the quantum Internet.[22,25,32,33,45,47] While *quantum computational supremacy* refers to tasks and problems that quantum computers can solve but are beyond the capability of classical computers, the *quantum supremacy of the quantum Internet* identifies the properties and attributes that the quantum Internet offers but are unavailable in the traditional Internet.[a]

The quantum Internet uses the fundamental concepts of quantum mechanics for networking (see Sidebars 1–7 in the online Supplementary Information at https://dl.acm.org/doi/10.1145/3524455). The main attributes of the quantum Internet are **advanced quantum phenomena and protocols** (such as quantum superposition and quantum entanglement, quantum teleportation, and advanced quantum coding methods), **unconditional security** (quantum cryptography), and an **entangled network structure**.

In contrast to traditional repeaters,[b] quantum repeaters cannot apply the receive–copy–retransmit mechanism because of the so-called no-cloning theorem, which states that it is impossible to make a perfect copy of a quantum system (see Sidebar 4). This fundamental difference between the nature of classical and quantum information does not just lead to fundamentally different networking mechanisms; it also necessitates the definition of novel networking services in a quantum Internet scenario. Quantum memories in quantum repeater units are a fundamental part of any global-scale quantum Internet. A challenge connected to quantum memory units is the noise quantum memories adds to storing quantum systems. However, while quantum repeaters can be realized without requiring quantum memories, these units are, in fact, necessary to guarantee optimal performance in any high-performance quantum-networking scenario.

In 2019, the National Quantum

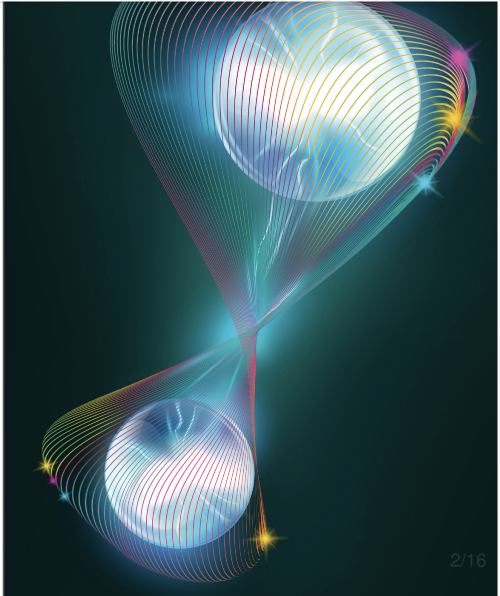
a While "supremacy" is a concept used to describe the theory of computational complexity[1,15] and not a specific device (like a quantum computer), the supremacy of the quantum Internet in the current context refers to the collection of those advanced networking properties and attributes that are beyond the capabilities of the traditional Internet.

b Traditional repeaters rely on signal amplification.

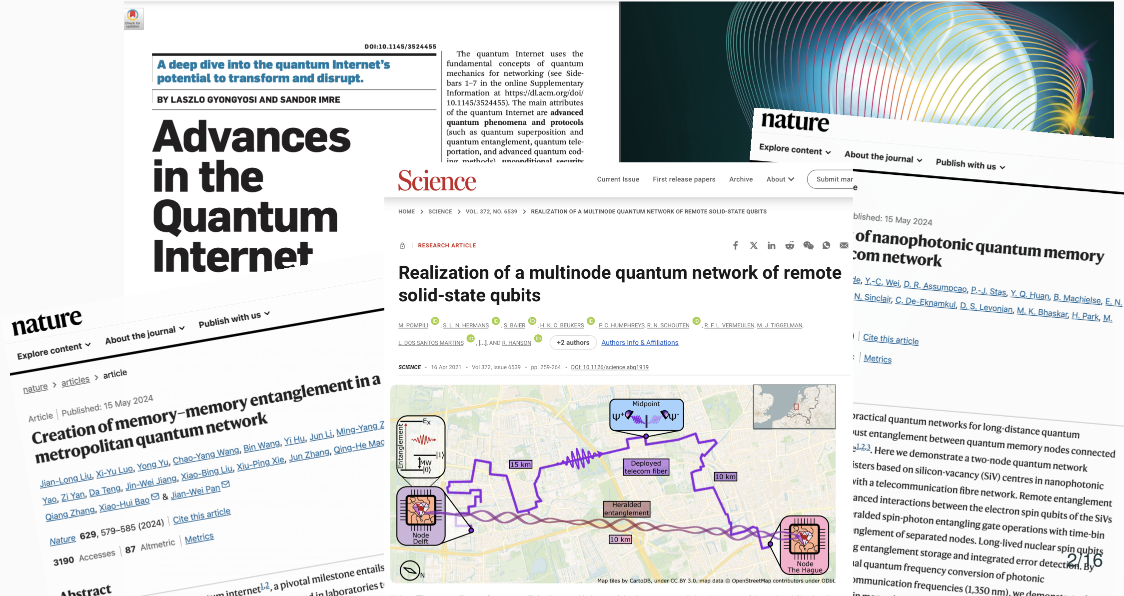
» key insights

- **The quantum Internet is an adequate answer to the security issues that will become relevant as commercial quantum computers hit the market.**
- **The quantum Internet is based on the fundamentals of quantum mechanics to provide advanced, high-security network communications.**
- **The quantum Internet gives users many capabilities and services not available in a traditional Internet setting.**

IMAGE BY ANDRIJ BORYS ASSOCIATES, USING SHUTTERSTOCK



Quantum networks are coming into reality



Quantum networks are coming into reality

NewScientist

Sign in | Enter search keywords

News Features Newsletters Podcasts Video Comment Culture Crosswords | This week's magazine
Health Space Physics Technology Environment Mind Humans Life Mathematics Chemistry Earth Socie

Technology

Quantum internet draws near thanks to entangled memory breakthroughs

Researchers aiming to create a secure quantum version of the inte called a quantum repeater, which doesn't yet exist - but now two te well on the way to building one

By Alex Wilkins

15 May 2024

Quantum networks could spread across a city
Fit Ztudio/Shutterstock

Efforts to build a global quantum internet have received a boost from two devel storage that could one day make it possible to communicate securely across hun

The internet as it exists today involves sending strings of digital bits, or 0s and optical signals, to transmit information. A quantum internet, which could be us ...ications or link up quantum computers, would use quantum bits inste ... can be linked and meas

na
Explo
natur
Artic
Cr
m

...1145/3524455

The quantum Internet uses the fundamental concepts of quantum mechanics for networking (see Sidebars 1–7 in the online Supplementary Information at https://dl.acm.org/doi/10.1145/3524455). The main attributes of the quantum Internet are **advanced quantum phenomena and protocols**

nature

...bout the journal ⌄ Publish with us ⌄

...blished: 15 May 2024

...of nanophotonic quantum memory ...com network

...de, Y.-C. Wei, D. R. Assumpcao, P.-J. Stas, Y. Q. Huan, B. Machielse, E. N. ... N. Sinclair, C. De-Eknamkul, D. S. Levonian, M. K. Bhaskar, H. Park, M.

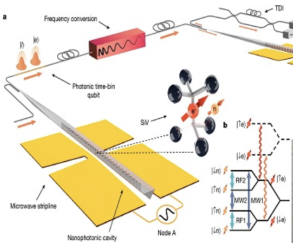
Cite this article

Metrics

...mmunication frequencies (1,350 nm), we demonstr...

AT ACM TechNews <technews-editor@acm.org>

To: Buckley Anita



Quantum Internet Draws Nearer

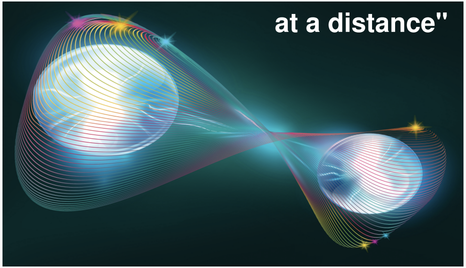
Harvard University researchers assemble... spanning 35 kilometers across Boston, M... two nodes separated by a loop of optical... diamond with an atom-sized hole. Meanwhile, researchers at the University of Science and Technology of China entangled three nodes

Cloud Computing Under the Cover of Quantum

Researchers at the U.K.'s University of Oxford and France's Sorbo... University demonstrated blind quantum computing using trapped i... The quantum cloud system's "server" was made from a strontium (the network qubit) and a calcium ion (the memory qubit). The ser... does not know the electronic state of the network qubit but can sti... process its information via a laser-based process that entangles the network and memory qubits. The system also uses one-time-pad encryption to encode information, concealing the data and operatio... from the server.

Bell pair: a pair of entangled qubits

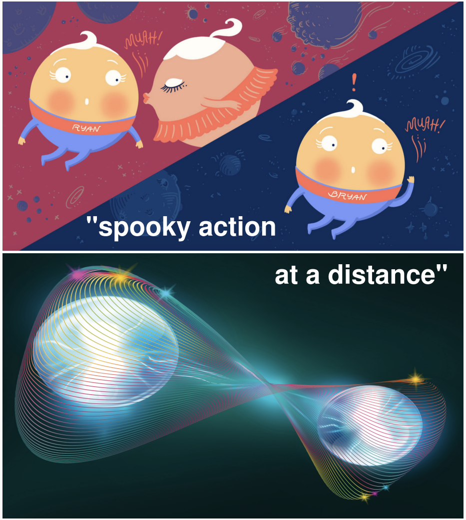
- Fundamental *resource* in quantum networks
- *Bell pair* is a pair of entangled qubits: $R{\sim}B$ distributed between nodes R and B
- No headers: control information needs to be sent via separate classical channels



Artwork by Sandbox Studio, Chicago with Ana Kova
Image by Andrij Borys Associates, using Shutterstock

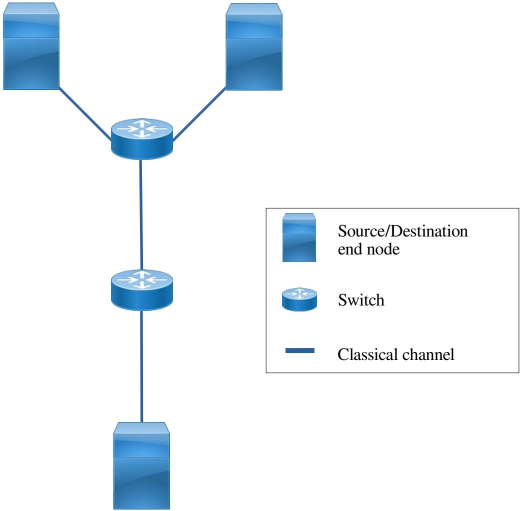
Bell pair: a pair of entangled qubits

- Fundamental *resource* in quantum networks
- *Bell pair* is a pair of entangled qubits: $R \sim B$ distributed between nodes R and B
- No headers: control information needs to be sent via separate classical channels

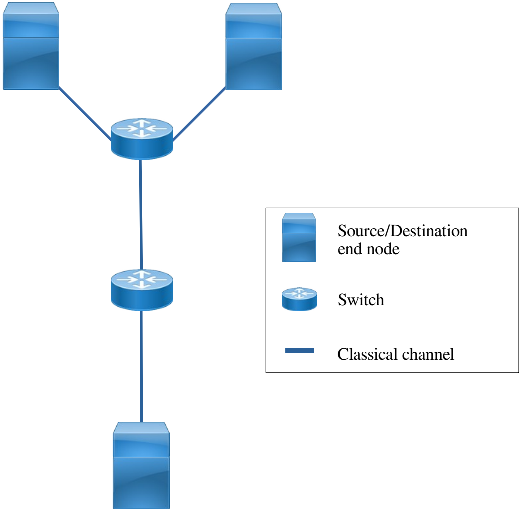


Artwork by Sandbox Studio, Chicago with Ana Kova
Image by Andrij Borys Associates, using Shutterstock

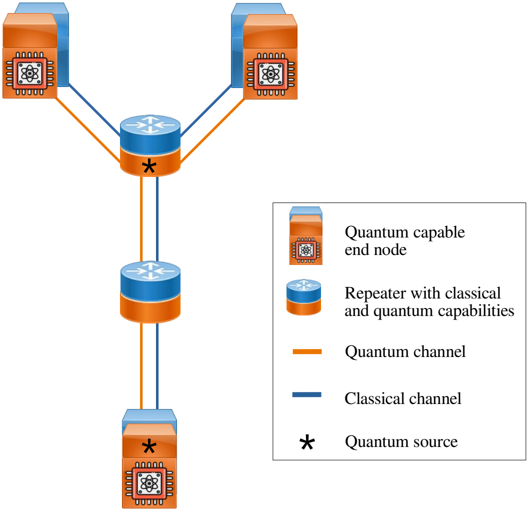
Classical network



Classical network

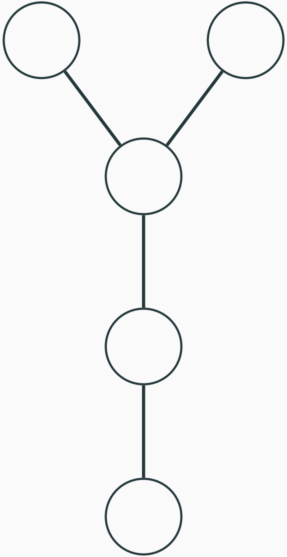


Quantum network [1,2]

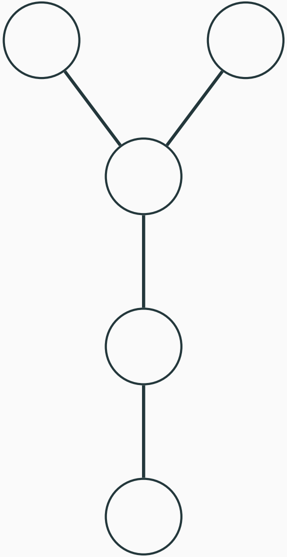


[1] [Kozlowski and Wehner: NANOCOM *2019*], [2] [Quantum Internet Research Group: RFC 9340 *2023*]

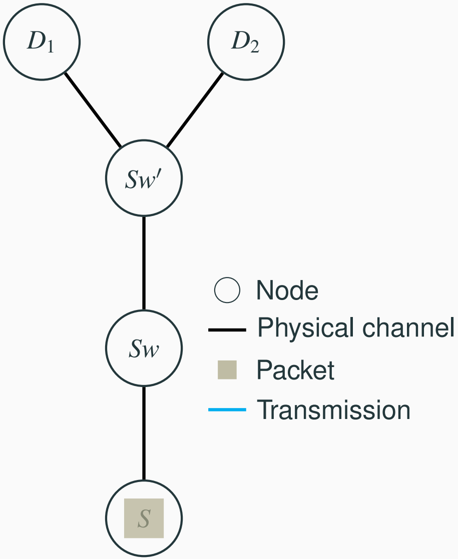
Classical network



Quantum network

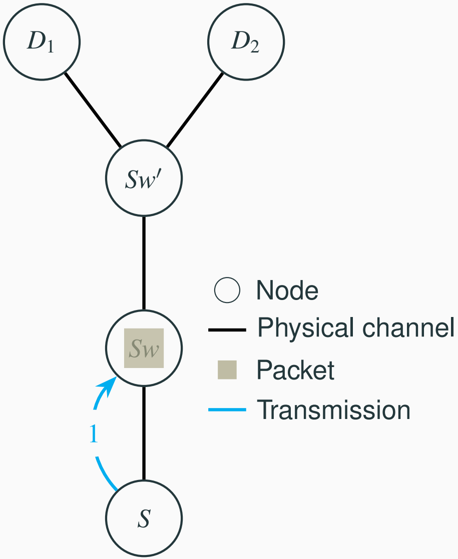


Forwarding packets



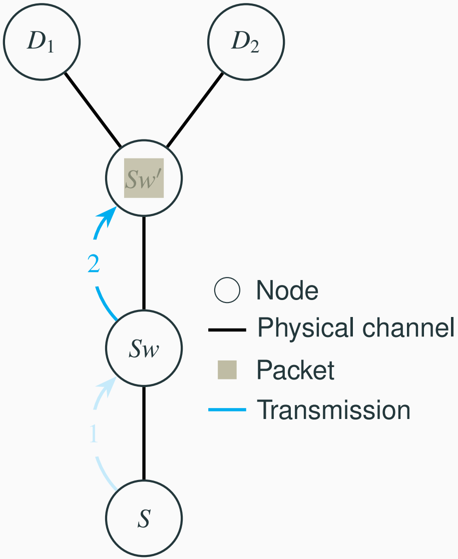
Distributing Bell pairs

Forwarding packets



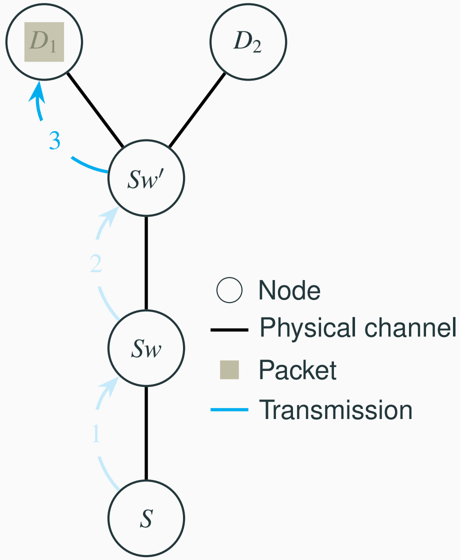
Distributing Bell pairs

Forwarding packets



Distributing Bell pairs

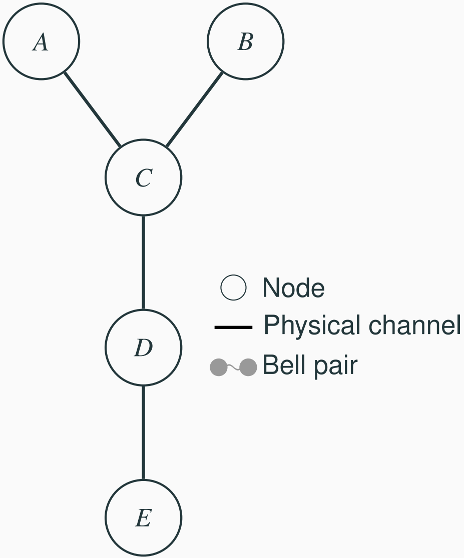
Forwarding packets



Distributing Bell pairs

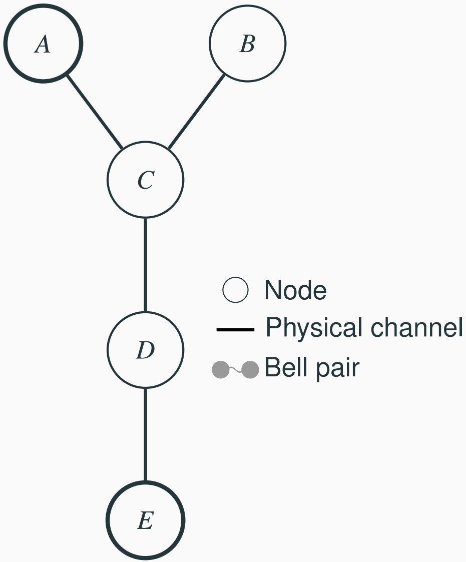
Forwarding packets

Distributing Bell pairs



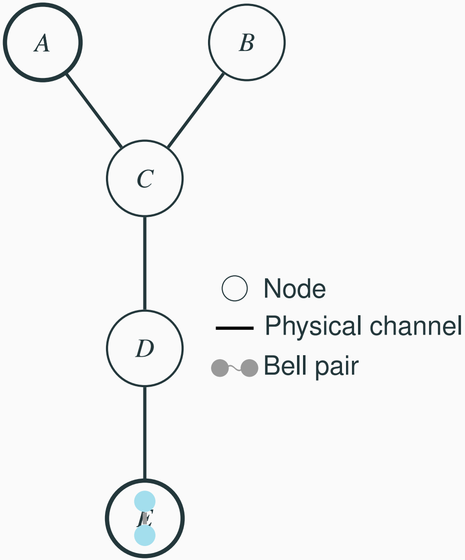
Forwarding packets

Distributing Bell pairs



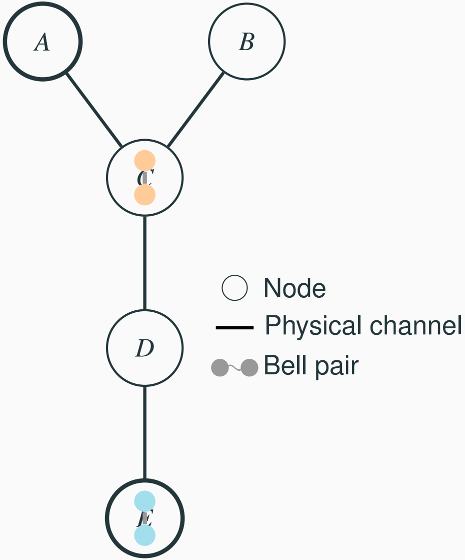
Forwarding packets

Distributing Bell pairs



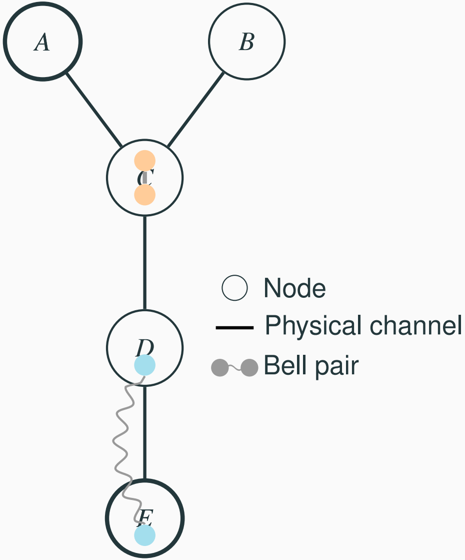
Forwarding packets

Distributing Bell pairs



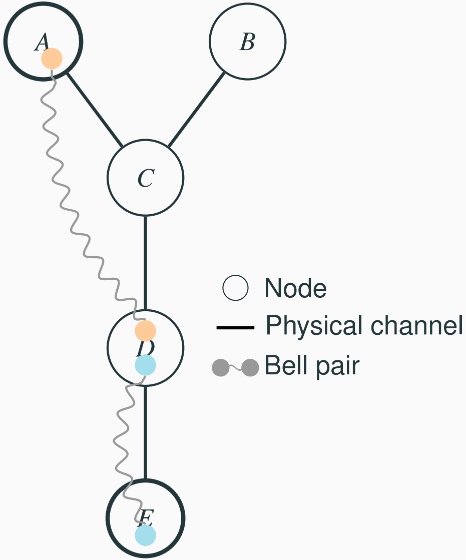
Forwarding packets

Distributing Bell pairs



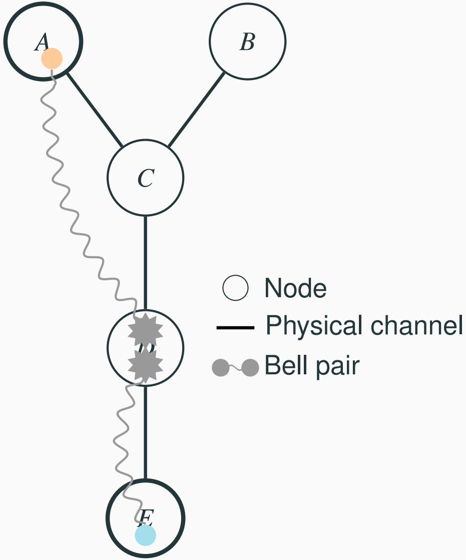
Forwarding packets

Distributing Bell pairs



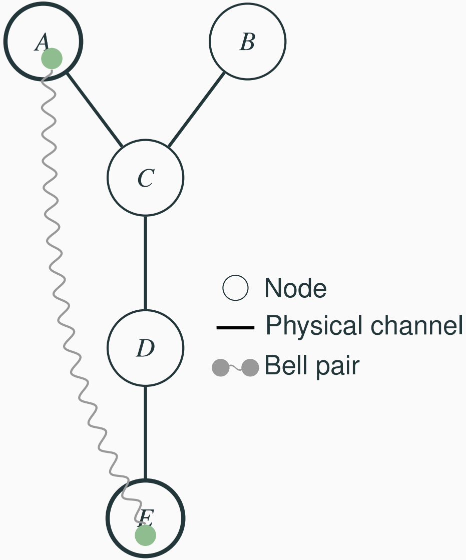
Forwarding packets

Distributing Bell pairs

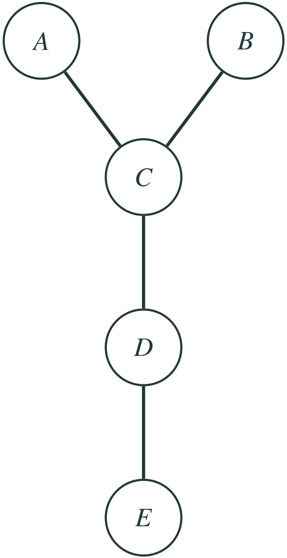


Forwarding packets

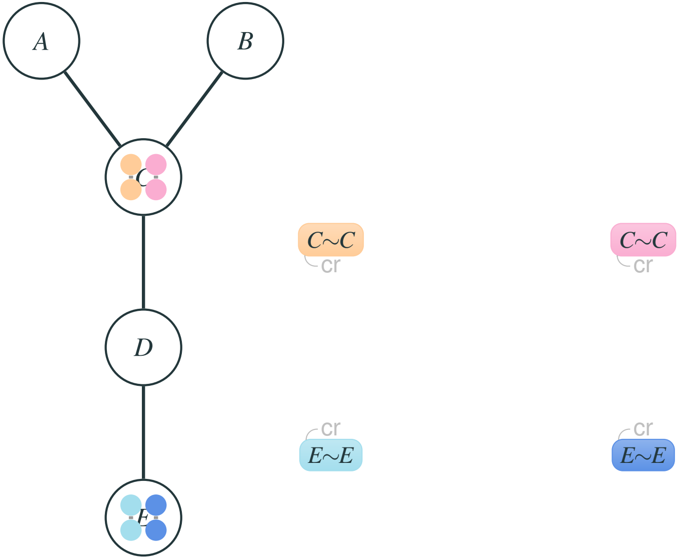
Distributing Bell pairs



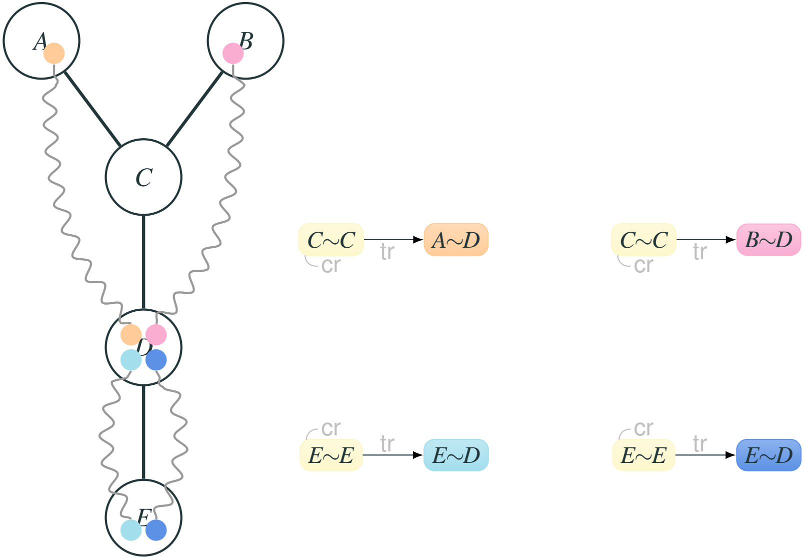
End-to-end Bell pair generation protocol



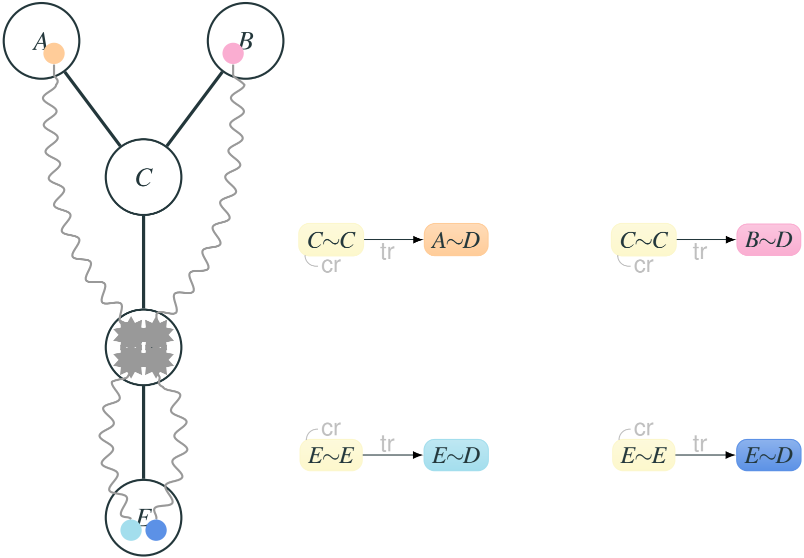
End-to-end Bell pair generation protocol



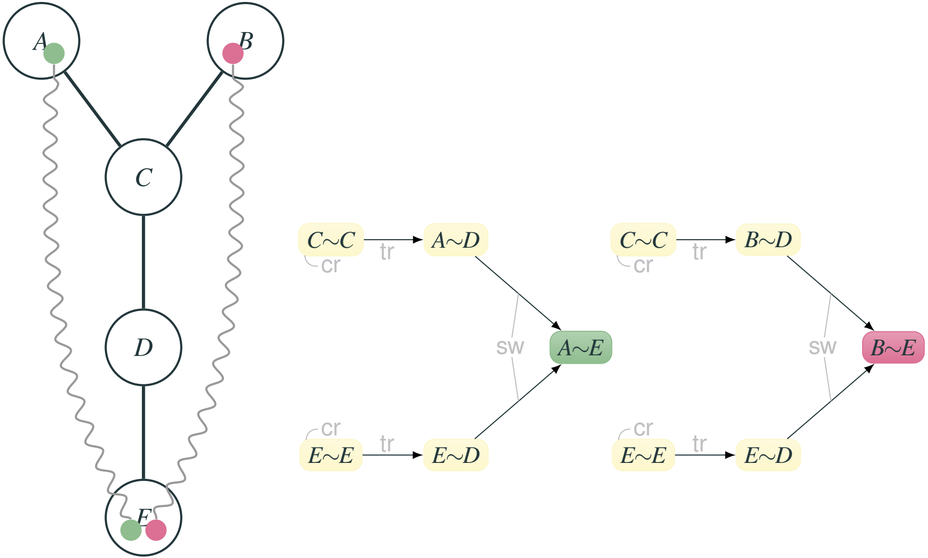
End-to-end Bell pair generation protocol



End-to-end Bell pair generation protocol



End-to-end Bell pair generation protocol



Verification and optimization

Verification and optimization

PROBLEM

How to make sure that quantum networks behave as intended?

Verification and optimization

PROBLEM

How to make sure that quantum networks behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?

Verification and optimization

PROBLEM

How to make sure that quantum networks behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?
- Are two protocols equivalent?

Verification and optimization

PROBLEM

How to make sure that quantum networks behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?
- Are two protocols equivalent?
- Can a protocol execute with a given number of resources?

Verification and optimization

PROBLEM

How to make sure that quantum networks behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?
- Are two protocols equivalent?
- Can a protocol execute with a given number of resources?
- Can protocols run in parallel without interfering with each other?

Verification and optimization

PROBLEM

How to make sure that quantum networks behave as intended?

- Does a protocol establish Bell pairs between the specified end nodes?
- Are two protocols equivalent?
- Can a protocol execute with a given number of resources?
- Can protocols run in parallel without interfering with each other?

SOLUTION

Provide formalism to answer these types of questions about quantum networks

BellKAT language

BellKAT language

Specification language for end-to-end Bell pairs generation – BellKAT

BellKAT language

Specification language for end-to-end Bell pairs generation – **Bell**KAT

BellKAT language

Specification language for end-to-end Bell pairs generation – Bell**KAT**

BellKAT language

Specification language for end-to-end Bell pairs generation – **BellKAT**

- Syntax and semantics
  - provide abstractions for quantum network primitives: create cr, transmit tr, swap sw, . . .
  - model multiround behavior, catering for highly synchronized nature of quantum networks
  - capture resource sharing (protocols competing for available Bell pairs)

BellKAT language

Specification language for end-to-end Bell pairs generation – **BellKAT**

- Syntax and semantics
  - provide abstractions for quantum network primitives: create cr, transmit tr, swap sw, . . .
  - model multiround behavior, catering for highly synchronized nature of quantum networks
  - capture resource sharing (protocols competing for available Bell pairs)
- Algebraic structure based on Kleene algebra with tests (KAT)
  - with (novel) axioms capturing round synchronization

BellKAT language

Specification language for end-to-end Bell pairs generation – **BellKAT**

- Syntax and semantics
  - provide abstractions for quantum network primitives: create cr, transmit tr, swap sw, . . .
  - model multiround behavior, catering for highly synchronized nature of quantum networks
  - capture resource sharing (protocols competing for available Bell pairs)
- Algebraic structure based on Kleene algebra with tests (KAT)
  - with (novel) axioms capturing round synchronization
- Formal results
  - proofs of soundness and completeness of equational theory
  - decidability of semantic equivalences

BellKAT primitives – basic actions

BellKAT primitives – basic actions

$$r \triangleright o : \quad a \mapsto \begin{cases} o \bowtie a \backslash r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

r, o, a : multisets of Bell pairs $\quad \bowtie$: pair of multisets of Bell pairs

BellKAT primitives – basic actions

required BPs

$$r \triangleright o\colon\ a \mapsto \begin{cases} o \bowtie a \backslash r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

r, o, a : multisets of Bell pairs $\bowtie$: pair of multisets of Bell pairs

BellKAT primitives – basic actions

required BPs

$$r \triangleright o: \quad a \mapsto \begin{cases} o \bowtie a \backslash r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

output BPs

---

r, o, a : multisets of Bell pairs $\quad \bowtie$: pair of multisets of Bell pairs

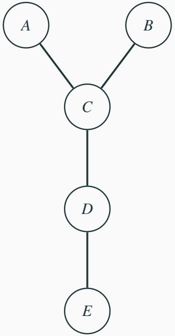
BellKAT primitives – basic actions

required BPs

$$r \triangleright o\colon\ a \mapsto \begin{cases} o \bowtie a \backslash r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

output BPs

Swap $\{\!\{A{\sim}D, D{\sim}E\}\!\} \triangleright \{\!\{A{\sim}E\}\!\}$



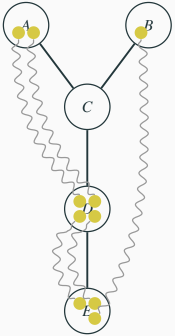
BellKAT primitives – basic actions

required BPs

input BPs

output BPs

$$r \triangleright o \colon\ a \mapsto \begin{cases} o \bowtie a \setminus r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$



Swap $\{\!\{A{\sim}D, D{\sim}E\}\!\} \triangleright \{\!\{A{\sim}E\}\!\}$ acting on input $\{\!\{A{\sim}D, A{\sim}D, D{\sim}E, D{\sim}E, B{\sim}E\}\!\}$

$A{\sim}D$ $D{\sim}E$ $A{\sim}D$ $D{\sim}E$ $B{\sim}E$

Input Bell pairs

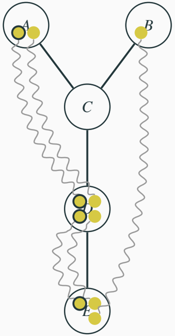
BellKAT primitives – basic actions

required BPs

input BPs

$$r \triangleright o : \; a \mapsto \begin{cases} o \bowtie a \setminus r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

output BPs



Swap $\{\!\{A{\sim}D, D{\sim}E\}\!\} \triangleright \{\!\{A{\sim}E\}\!\}$ acting on input $\{\!\{\underline{A{\sim}D}, A{\sim}D, \underline{D{\sim}E}, D{\sim}E, B{\sim}E\}\!\}$

$A{\sim}D$ $D{\sim}E$ $A{\sim}D$ $D{\sim}E$ $B{\sim}E$

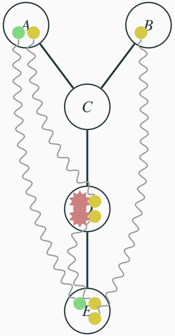
Input Bell pairs

BellKAT primitives – basic actions

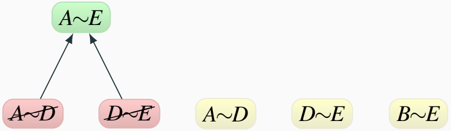
required BPs · input BPs · consumed BPs

$$r \triangleright o :\; a \mapsto \begin{cases} o \bowtie a \setminus r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

output BPs · produced BPs



Swap $\{\!\{A{\sim}D, D{\sim}E\}\!\} \triangleright \{\!\{A{\sim}E\}\!\}$ acting on input $\{\!\{\cancel{A{\sim}D}, A{\sim}D, \cancel{D{\sim}E}, D{\sim}E, B{\sim}E\}\!\}$



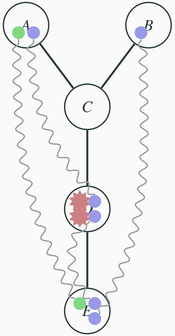
Input, consumed and produced Bell pairs

BellKAT primitives – basic actions

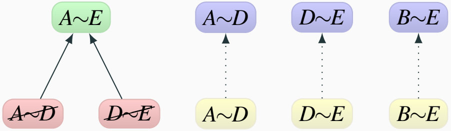
required BPs — input BPs — consumed BPs

$$r \triangleright o :\; a \mapsto \begin{cases} o \bowtie a \setminus r & \text{if } r \subseteq a \\ \emptyset \bowtie a & \text{otherwise} \end{cases}$$

output BPs — produced BPs — untouched BPs



Swap $\{\{A{\sim}D, D{\sim}E\}\} \triangleright \{\{A{\sim}E\}\}$ acting on input $\{\{\cancel{A{\sim}D}, A{\sim}D, \cancel{D{\sim}E}, D{\sim}E, B{\sim}E\}\}$



Input, consumed, produced and untouched Bell pairs

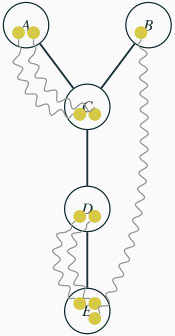
BellKAT primitives – basic actions

required BPs

input BPs

output BPs

$$r \triangleright o : \; a \mapsto \begin{cases} o \bowtie a \setminus r & \text{if } r \subseteq a \\ \boxed{\emptyset \bowtie a} & \text{otherwise} \end{cases}$$



Swap $\{\!\{A{\sim}D, D{\sim}E\}\!\} \triangleright \{\!\{A{\sim}E\}\!\}$ acting on input $\{\!\{A{\sim}C, A{\sim}C, D{\sim}E, D{\sim}E, B{\sim}E\}\!\}$

$A{\sim}C$ $D{\sim}E$ $A{\sim}C$ $D{\sim}E$ $B{\sim}E$

Input, consumed, produced and untouched Bell pairs

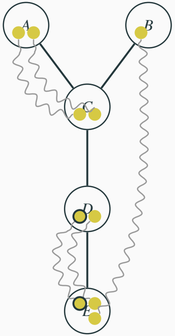
BellKAT primitives – basic actions

required BPs

input BPs

$$r \triangleright o:\ a \mapsto \begin{cases} o \bowtie a \backslash r & \text{if } r \subseteq a \\ \boxed{\emptyset \bowtie a} & \text{otherwise} \end{cases}$$

output BPs



Swap $\{\!\{A{\sim}D, D{\sim}E\}\!\} \triangleright \{\!\{A{\sim}E\}\!\}$ acting on input $\{\!\{A{\sim}C, A{\sim}C, \underline{D{\sim}E}, D{\sim}E, B{\sim}E\}\!\}$

$A{\sim}C$ $D{\sim}E$ $A{\sim}C$ $D{\sim}E$ $B{\sim}E$

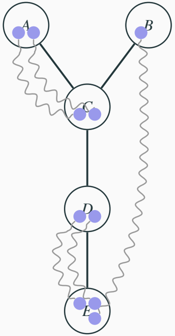
Input, consumed, produced and untouched Bell pairs

BellKAT primitives – basic actions

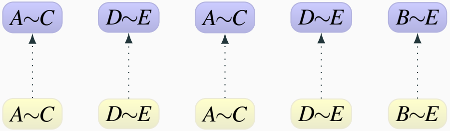
required BPs — input BPs

$$r \triangleright o : \; a \mapsto \begin{cases} o \bowtie a \backslash r & \text{if } r \subseteq a \\ \boxed{\emptyset \bowtie a} & \text{otherwise} \end{cases}$$

output BPs — produced BPs — untouched BPs



Swap $\{\!\{A{\sim}D, D{\sim}E\}\!\} \triangleright \{\!\{A{\sim}E\}\!\}$ acting on input $\{\!\{A{\sim}C, A{\sim}C, \underline{D{\sim}E}, D{\sim}E, B{\sim}E\}\!\}$



Input, consumed, produced and untouched Bell pairs

BellKAT primitives – basic actions

swap	$\mathsf{sw}\langle A{\sim}B \,@\, C\rangle \triangleq \{\!\{A{\sim}C, B{\sim}C\}\!\} \triangleright \{\!\{A{\sim}B\}\!\}$
transmit	$\mathsf{tr}\langle A \rightarrow B{\sim}C\rangle \triangleq \{\!\{A{\sim}A\}\!\} \triangleright \{\!\{B{\sim}C\}\!\}$
create	$\mathsf{cr}\langle A\rangle \triangleq \emptyset \triangleright \{\!\{A{\sim}A\}\!\}$
wait	$\mathsf{wait}\langle r\rangle \triangleq r \triangleright r$
fail	$\mathsf{fail}\langle r\rangle \triangleq r \triangleright \emptyset$

BellKAT primitives – basic actions

swap	$\mathsf{sw}\langle A{\sim}B \,@\, C\rangle \triangleq \{\!\{A{\sim}C, B{\sim}C\}\!\} \triangleright \{\!\{A{\sim}B\}\!\}$
transmit	$\mathsf{tr}\langle A \rightarrow B{\sim}C\rangle \triangleq \{\!\{A{\sim}A\}\!\} \triangleright \{\!\{B{\sim}C\}\!\}$
create	$\mathsf{cr}\langle A\rangle \triangleq \emptyset \triangleright \{\!\{A{\sim}A\}\!\}$
wait	$\mathsf{wait}\langle r\rangle \triangleq r \triangleright r$
fail	$\mathsf{fail}\langle r\rangle \triangleq r \triangleright \emptyset$

BellKAT primitives – basic actions

swap	$\mathsf{sw}\langle A{\sim}B \,@\, C\rangle \triangleq \{\!\{A{\sim}C, B{\sim}C\}\!\} \triangleright \{\!\{A{\sim}B\}\!\}$
transmit	$\mathsf{tr}\langle A \rightarrow B{\sim}C\rangle \triangleq \{\!\{A{\sim}A\}\!\} \triangleright \{\!\{B{\sim}C\}\!\}$
create	$\mathsf{cr}\langle A\rangle \triangleq \emptyset \triangleright \{\!\{A{\sim}A\}\!\}$
wait	$\mathsf{wait}\langle r\rangle \triangleq r \triangleright r$
fail	$\mathsf{fail}\langle r\rangle \triangleq r \triangleright \emptyset$

BellKAT primitives – basic actions

swap	$\mathsf{sw}\langle A{\sim}B @ C\rangle \triangleq \{\!\{A{\sim}C, B{\sim}C\}\!\} \triangleright \{\!\{A{\sim}B\}\!\}$
transmit	$\mathsf{tr}\langle A \to B{\sim}C\rangle \triangleq \{\!\{A{\sim}A\}\!\} \triangleright \{\!\{B{\sim}C\}\!\}$
create	$\mathsf{cr}\langle A\rangle \triangleq \emptyset \triangleright \{\!\{A{\sim}A\}\!\}$
wait	$\mathsf{wait}\langle r\rangle \triangleq r \triangleright r$
fail	$\mathsf{fail}\langle r\rangle \triangleq r \triangleright \emptyset$

BellKAT primitives – basic actions

swap	$\text{sw}\langle A{\sim}B \mathbin{@} C\rangle \triangleq \{\{A{\sim}C, B{\sim}C\}\} \triangleright \{\{A{\sim}B\}\}$
transmit	$\text{tr}\langle A \to B{\sim}C\rangle \triangleq \{\{A{\sim}A\}\} \triangleright \{\{B{\sim}C\}\}$
create	$\text{cr}\langle A\rangle \triangleq \emptyset \triangleright \{\{A{\sim}A\}\}$
wait	$\text{wait}\langle r\rangle \triangleq r \triangleright r$
fail	$\text{fail}\langle r\rangle \triangleq r \triangleright \emptyset$

BellKAT primitives – basic actions

swap	$\mathsf{sw}\langle A{\sim}B \mathbin{@} C\rangle \triangleq \{\!\{A{\sim}C, B{\sim}C\}\!\} \triangleright \{\!\{A{\sim}B\}\!\}$
transmit	$\mathsf{tr}\langle A \to B{\sim}C\rangle \triangleq \{\!\{A{\sim}A\}\!\} \triangleright \{\!\{B{\sim}C\}\!\}$
create	$\mathsf{cr}\langle A\rangle \triangleq \emptyset \triangleright \{\!\{A{\sim}A\}\!\}$
wait	$\mathsf{wait}\langle r\rangle \triangleq r \triangleright r$
fail	$\mathsf{fail}\langle r\rangle \triangleq r \triangleright \emptyset$

BellKAT syntax

BellKAT syntax

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p ; q \mid p^\star$$

BellKAT syntax

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p; q \mid p^{\star}$$

basic action

BellKAT syntax

abort

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p ; q \mid p^{\star}$$

basic action

BellKAT syntax

skip

abort

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p ; q \mid p^{\star}$$

basic action

BellKAT syntax

skip

abort

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p; q \mid p^\star$$

basic action

nondeterministic choice

BellKAT syntax

skip

abort

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p ; q \mid p^{\star}$$

basic action

nondeterministic choice

sequential composition

BellKAT syntax

skip

abort

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p ; q \mid p^{\star}$$

basic action

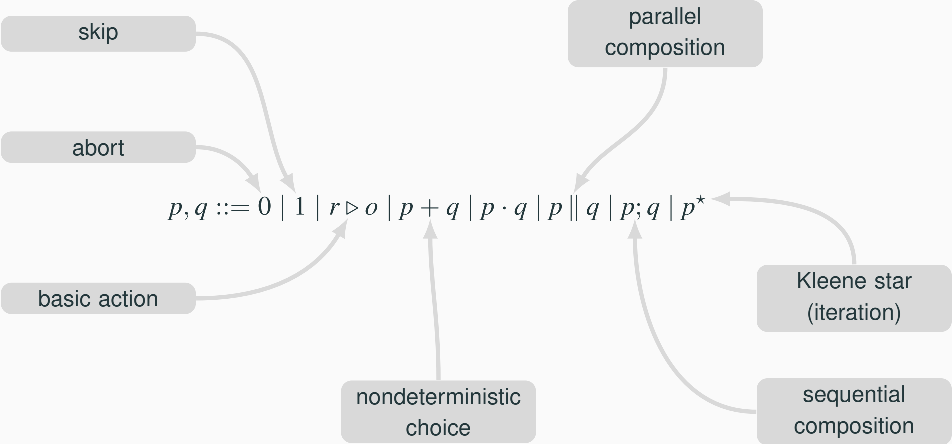
nondeterministic choice

Kleene star (iteration)

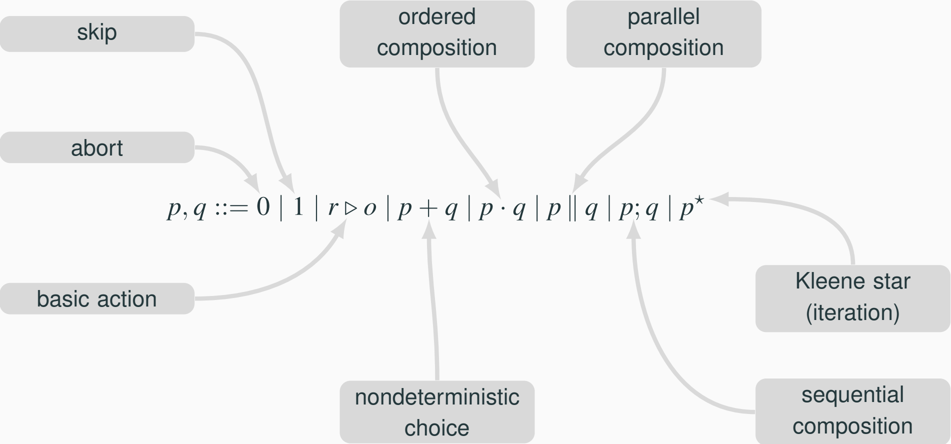
sequential composition

BellKAT syntax

$$p, q ::= 0 \mid 1 \mid r \triangleright o \mid p + q \mid p \cdot q \mid p \parallel q \mid p ; q \mid p^{\star}$$



BellKAT syntax



Protocol specification in BellKAT

Protocol specification in BellKAT

Protocol specification in BellKAT

$$(\mathsf{cr}\langle C\rangle \parallel \mathsf{cr}\langle C\rangle \parallel \mathsf{cr}\langle E\rangle \parallel \mathsf{cr}\langle E\rangle);$$

$$(\mathsf{tr}\langle C \rightarrow A{\sim}D\rangle \parallel \mathsf{tr}\langle C \rightarrow B{\sim}D\rangle \parallel \mathsf{tr}\langle E \rightarrow E{\sim}D\rangle \parallel \mathsf{tr}\langle E \rightarrow E{\sim}D\rangle);$$

$$(\mathsf{sw}\langle A{\sim}E \,@\, D\rangle \parallel \mathsf{sw}\langle B{\sim}E \,@\, D\rangle)$$

BellKAT at a glance

BellKAT at a glance

Syntax

Nodes	$\mathrm{N} ::=$	$A, B, C, \ldots$	
Bell pairs	$\mathrm{BP} \ni bp ::=$	$\mathrm{N}{\sim}\mathrm{N}$	
Multisets	$\mathcal{M}(\mathrm{BP}) \ni a, b, r, o ::=$	$\{\!\{bp_1, \ldots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$\mathrm{P} \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \,;\, q$	*sequential composition*
	$\mid$	$p^\star$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$	

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \,\square\, t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$
\begin{aligned}
(\!| p |\!) &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))\\
(\!| 0 |\!) a &\triangleq \emptyset\\
(\!| 1 |\!) a &\triangleq \{\emptyset \bowtie a\}\\
(\!| [t]r \blacktriangleright o |\!) a &\triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}\\
(\!| p + q |\!) a &\triangleq (\!| p |\!) a \cup (\!| q |\!) a\\
(\!| p \cdot q |\!) a &\triangleq ((\!| p |\!) \cdot (\!| q |\!)) a\\
(\!| p \parallel q |\!) a &\triangleq ((\!| p |\!) \parallel (\!| q |\!)) a
\end{aligned}
$$

Multi-round semantics

$$
\begin{aligned}
[\![p]\!] &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))\\
[\![\omega]\!]_I &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \mathbin{;} \pi_2 \mathbin{;} \ldots \mathbin{;} \pi_k\\
[\![p]\!] a &\triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a\\
[\![\epsilon]\!]_I a &\triangleq \{a\}\\
[\![[t]r \blacktriangleright o]\!]_I a &\triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}\\
[\![\pi_1 \mathbin{;} \pi_2 \mathbin{;} \ldots \mathbin{;} \pi_k]\!]_I a &\triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \mathbin{;} \ldots \mathbin{;} \pi_k]\!]_I) a
\end{aligned}
$$

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p \,;\, 1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1 \,;\, p \equiv p$	KA-One-Seq
$p+0 \equiv p$	KA-Plus-Zero	$0 \,;\, p \equiv 0$	KA-Zero-Seq
$p+p \equiv p$	KA-Plus-Idem	$p \,;\, 0 \equiv 0$	KA-Seq-Zero
$(p \,;\, q) \,;\, r \equiv p \,;\, (q \,;\, r)$	KA-Seq-Assoc	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q+r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^\star \,;\, r \leq r$	KA-Lfp-L
$(p+q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^\star \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-Prl-Assoc	$p \parallel q \equiv q \parallel p$	SKA-Prl-Comm
$p \parallel (q+r) \equiv p \parallel q + p \parallel r$	SKA-Prl-Dist	$1 \parallel p \equiv p$	SKA-One-Prl
$(x \,;\, p) \parallel (y \,;\, q) \equiv (x \parallel y) \,;\, (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q+r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p+q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x \,;\, p) \cdot (y \,;\, q) \equiv (x \cdot y) \,;\, (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$\mathrm{N} ::=$	$A, B, C, \ldots$	
Bell pairs	$\mathrm{BP} \ni bp ::=$	$\mathrm{N}{\sim}\mathrm{N}$	
Multisets	$\mathcal{M}(\mathrm{BP}) \ni a, b, r, o ::=$	$\{\!\{bp_1, \ldots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$\mathrm{P} \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \,;\, q$	*sequential composition*
	$\mid$	$p^\star$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$	

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \,\square\, t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!| 0 |\!) a \triangleq \emptyset$$

$$(\!| 1 |\!) a \triangleq \{\emptyset \bowtie a\}$$

$$(\!| [t]r \blacktriangleright o |\!) a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!) a \triangleq (\!| p |\!) a \cup (\!| q |\!) a$$

$$(\!| p \cdot q |\!) a \triangleq ((\!| p |\!) \cdot (\!| q |\!)) a$$

$$(\!| p \parallel q |\!) a \triangleq ((\!| p |\!) \parallel (\!| q |\!)) a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k$$

$$[\![p]\!] a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I) a$$

KA axioms

$(p + q) + r \equiv p + (q + r)$	KA-Plus-Assoc	$p \,;\, 1 \equiv p$	KA-Seq-One
$p + q \equiv q + p$	KA-Plus-Comm	$1 \,;\, p \equiv p$	KA-One-Seq
$p + 0 \equiv p$	KA-Plus-Zero	$0 \,;\, p \equiv 0$	KA-Zero-Seq
$p + p \equiv p$	KA-Plus-Idem	$p \,;\, 0 \equiv 0$	KA-Seq-Zero
$(p \,;\, q) \,;\, r \equiv p \,;\, (q \,;\, r)$	KA-Seq-Assoc	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q + r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^\star \,;\, r \leq r$	KA-Lfp-L
$(p + q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^\star \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-Prl-Assoc	$p \parallel q \equiv q \parallel p$	SKA-Prl-Comm
$p \parallel (q + r) \equiv p \parallel q + p \parallel r$	SKA-Prl-Dist	$1 \parallel p \equiv p$	SKA-One-Prl
$(x \,;\, p) \parallel (y \,;\, q) \equiv (x \parallel y) \,;\, (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q + r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p + q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x \,;\, p) \cdot (y \,;\, q) \equiv (x \cdot y) \,;\, (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$N ::=$	$A, B, C, \ldots$	
Bell pairs	$BP \ni bp ::=$	$N \sim N$	
Multisets	$\mathcal{M}(BP) \ni a, b, r, o ::=$	$\{\!\{bp_1, \ldots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$P \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \,;\, q$	*sequential composition*
	$\mid$	$p^\star$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$	

Basic actions $r \triangleright o ::= [\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(BP) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \sqcap t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \sqcap \langle\!| t' |\!\rangle a, \text{ with } \sqcap \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$$

$$(\!| 0 |\!)a \triangleq \emptyset$$

$$(\!| 1 |\!)a \triangleq \{\emptyset \bowtie a\}$$

$$(\!| [t]r \blacktriangleright o |\!)a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \ldots \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!)a \triangleq (\!| p |\!)a \cup (\!| q |\!)a$$

$$(\!| p \cdot q |\!)a \triangleq ((\!| p |\!) \cdot (\!| q |\!))a$$

$$(\!| p \parallel q |\!)a \triangleq ((\!| p |\!) \parallel (\!| q |\!))a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$$

$$[\![\omega]\!]_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k$$

$$[\![p]\!]a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I)a$$

KA axioms

$(p + q) + r \equiv p + (q + r)$	KA-Plus-Assoc	$p \,;\, 1 \equiv p$	KA-Seq-One
$p + q \equiv q + p$	KA-Plus-Comm	$1 \,;\, p \equiv p$	KA-One-Seq
$p + 0 \equiv p$	KA-Plus-Zero	$0 \,;\, p \equiv 0$	KA-Zero-Seq
$p + p \equiv p$	KA-Plus-Idem	$p \,;\, 0 \equiv 0$	KA-Seq-Zero
$(p \,;\, q) \,;\, r \equiv p \,;\, (q \,;\, r)$	KA-Seq-Assoc	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q + r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^\star \,;\, r \leq r$	KA-Lfp-L
$(p + q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^\star \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-Prl-Assoc	$p \parallel q \equiv q \parallel p$	SKA-Prl-Comm
$p \parallel (q + r) \equiv p \parallel q + p \parallel r$	SKA-Prl-Dist	$1 \parallel p \equiv p$	SKA-One-Prl
$(x \,;\, p) \parallel (y \,;\, q) \equiv (x \parallel y) \,;\, (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q + r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p + q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x \,;\, p) \cdot (y \,;\, q) \equiv (x \cdot y) \,;\, (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$N ::=$	$A, B, C, \ldots$	
Bell pairs	$BP \ni bp ::=$	$N{\sim}N$	
Multisets	$\mathcal{M}(BP) \ni a, b, r, o ::=$	$\{\!\{bp_1, \ldots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$P \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \,;\, q$	*sequential composition*
	$\mid$	$p^\star$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$	

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(BP) \to \{\top, \bot\}$$

$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top$ $\quad$ $\langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$

$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a$ $\quad$ $\langle\!| t \,\square\, t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a$, with $\square$ is either $\wedge$ or $\vee$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$$
$$(\!| 0 |\!)a \triangleq \emptyset$$
$$(\!| 1 |\!)a \triangleq \{\emptyset \bowtie a\}$$
$$(\!| [t]r \blacktriangleright o |\!)a \triangleq \begin{cases}\{o \bowtie a \setminus r\} & \text{if } r \subseteq a \ldots \\ \emptyset & \text{otherwise}\end{cases}$$
$$(\!| p + q |\!)a \triangleq (\!| p |\!)a \cup (\!| q |\!)a$$
$$(\!| p \cdot q |\!)a \triangleq ((\!| p |\!) \cdot (\!| q |\!))a$$
$$(\!| p \parallel q |\!)a \triangleq ((\!| p |\!) \parallel (\!| q |\!))a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$$
$$[\![\omega]\!]_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 ⨾ \pi_2 ⨾ \ldots ⨾ \pi_k$$
$$[\![p]\!]a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$
$$[\![\epsilon]\!]_I a \triangleq \{a\}$$
$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases}\{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise}\end{cases}$$
$$[\![\pi_1 ⨾ \pi_2 ⨾ \ldots ⨾ \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 ⨾ \ldots ⨾ \pi_k]\!]_I)a$$

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p\,;1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1\,;p \equiv p$	KA-One-Seq
$p+0 \equiv p$	KA-Plus-Zero	$0\,;p \equiv 0$	KA-Zero-Seq
$p+p \equiv p$	KA-Plus-Idem	$p\,;0 \equiv 0$	KA-Seq-Zero
$(p\,;q)\,;r \equiv p\,;(q\,;r)$	KA-Seq-Assoc	$1+p\,;p^\star \equiv p^\star$	KA-Unroll-L
$p\,;(q+r) \equiv p\,;q+p\,;r$	KA-Seq-Dist-L	$p\,;r \leq r \Rightarrow p^\star\,;r \leq r$	KA-Lfp-L
$(p+q)\,;r \equiv p\,;r+q\,;r$	KA-Seq-Dist-R	$1+p^\star\,;p \equiv p^\star$	KA-Unroll-R
		$r\,;p \leq r \Rightarrow r\,;p^\star \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

Atomic actions $\quad \Pi \ni \pi, x, y ::= \quad [t]r \blacktriangleright o$

$(x\,;p) \parallel (y\,;q) \equiv (x \parallel y)\,;(p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q+r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p+q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x\,;p) \cdot (y\,;q) \equiv (x \cdot y)\,;(p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$ $\quad$ Bool-One-U $\quad$ $(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$ $\quad$ Bool-Conj-U-Dist

Basic actions $\quad r \triangleright o ::= \quad [\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$N ::=$	$A, B, C, \ldots$	
Bell pairs	$BP \ni bp ::=$	$N{\sim}N$	
Multisets	$\mathcal{M}(BP) \ni a, b, r, o ::=$	$\{\!\{bp_1, \ldots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$P \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \,;\, q$	*sequential composition*
	$\mid$	$p^\star$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$	

Test semantics

$$\langle\!|t|\!\rangle \in \mathcal{M}(BP) \to \{\top, \bot\}$$

$$\langle\!|\mathbb{1}|\!\rangle a \triangleq \top \qquad \langle\!|t \uplus b|\!\rangle a \triangleq (\langle\!|t|\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!|b|\!\rangle a$$

$$\langle\!|b|\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!|t \sqcap t'|\!\rangle a \triangleq \langle\!|t|\!\rangle a \sqcap \langle\!|t'|\!\rangle a, \text{ with } \sqcap \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!|p|\!) \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$$

$$(\!|0|\!)a \triangleq \emptyset$$

$$(\!|1|\!)a \triangleq \{\emptyset \bowtie a\}$$

$$(\!|[t]r \blacktriangleright o|\!)a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \ldots \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!|p + q|\!)a \triangleq (\!|p|\!)a \cup (\!|q|\!)a$$

$$(\!|p \cdot q|\!)a \triangleq ((\!|p|\!) \cdot (\!|q|\!))a$$

$$(\!|p \parallel q|\!)a \triangleq ((\!|p|\!) \parallel (\!|q|\!))a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$$

$$[\![\omega]\!]_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 \,⨾\, \pi_2 \,⨾ \ldots ⨾\, \pi_k$$

$$[\![p]\!]a \triangleq \bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!|t|\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 ⨾ \pi_2 ⨾ \ldots ⨾ \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 ⨾ \ldots ⨾ \pi_k]\!]_I)a$$

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p\,;1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1\,;p \equiv p$	KA-One-Seq
$p+0 \equiv p$	KA-Plus-Zero	$0\,;p \equiv 0$	KA-Zero-Seq
$p+p \equiv p$	KA-Plus-Idem	$p\,;0 \equiv 0$	KA-Seq-Zero
$(p\,;q)\,;r \equiv p\,;(q\,;r)$	KA-Seq-Assoc	$1 + p\,;p^\star \equiv p^\star$	KA-Unroll-L
$p\,;\ldots$			KA-Lfp-L
$(p\ldots$			KA-Unroll-R
		$r\,;p \le r \Rightarrow r\,;p^\star \le r$	KA-Lfp-R

Tests $T \ni t, t'$

SKA axioms for ∥ …

Atomic actions $\Pi \ni \pi, x, y ::= [t]r \blacktriangleright o$

$(x\,;p) \parallel (y\,;q) \equiv (x \parallel y)\,;(p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for ·

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q+r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p+q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x\,;p) \cdot (y\,;q) \equiv (x \cdot y)\,;(p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist

Basic actions $r \triangleright o ::= [\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \le (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$\mathrm{N} ::=$	$A, B, C, \dots$	
Bell pairs	$\mathrm{BP} \ni bp ::=$	$\mathrm{N}{\sim}\mathrm{N}$	
Multisets	$\mathcal{M}(\mathrm{BP}) \ni a, b, r, o ::=$	$\{\!\{bp_1, \dots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$\mathrm{P} \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \mathbin{;} q$	*sequential composition*
	$\mid$	$p^\star$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$	

Test semantics

$$\{\!|t|\!\} \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\{\!|\mathbb{1}|\!\}a \triangleq \top \qquad \{\!|t \uplus b|\!\}a \triangleq (\{\!|t|\!\}a \setminus b \wedge b \subseteq a) \vee \{\!|b|\!\}a$$

$$\{\!|b|\!\}a \triangleq b \not\subseteq a \qquad \{\!|t \mathbin{\square} t'|\!\}a \triangleq \{\!|t|\!\}a \mathbin{\square} \{\!|t'|\!\}a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!|p|\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!|0|\!)a \triangleq \emptyset$$

$$(\!|1|\!)a \triangleq \{\emptyset \bowtie a\}$$

$$(\!|[t]r \blacktriangleright o|\!)a \triangleq \begin{cases} \{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } \{\!|t|\!\}a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!|p + q|\!)a \triangleq (\!|p|\!)a \cup (\!|q|\!)a$$

$$(\!|p \cdot q|\!)a \triangleq ((\!|p|\!) \cdot (\!|q|\!))a$$

$$(\!|p \parallel q|\!)a \triangleq ((\!|p|\!) \parallel (\!|q|\!))a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \dots \fatsemi \pi_k$$

$$[\![p]\!]a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \{\!|t|\!\}a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \dots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \dots \fatsemi \pi_k]\!]_I)a$$

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p \mathbin{;} 1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1 \mathbin{;} p \equiv p$	KA-One-Seq
$p+0 \equiv p$	KA-Plus-Zero	$0 \mathbin{;} p \equiv 0$	KA-Zero-Seq
$p+p \equiv p$	KA-Plus-Idem	$p \mathbin{;} 0 \equiv 0$	KA-Seq-Zero
$(p \mathbin{;} q) \mathbin{;} r \equiv p \mathbin{;} (q \mathbin{;} r)$	KA-Seq-Assoc	$1 + p \mathbin{;} p^\star \equiv p^\star$	KA-Unroll-L
$p \mathbin{;} (q+r) \equiv p \mathbin{;} q + p \mathbin{;} r$	KA-Seq-Dist-L	$p \mathbin{;} r \leq r \Rightarrow p^\star \mathbin{;} r \leq r$	KA-Lfp-L
$(p+q) \mathbin{;} r \equiv p \mathbin{;} r + q \mathbin{;} r$	KA-Seq-Dist-R	$1 + p^\star \mathbin{;} p \equiv p^\star$	KA-Unroll-R
		$r \mathbin{;} p \leq r \Rightarrow r \mathbin{;} p^\star \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-Prl-Assoc	$p \parallel q \equiv q \parallel p$	SKA-Prl-Comm
$p \parallel (q+r) \equiv p \parallel q + p \parallel r$	SKA-Prl-Dist	$1 \parallel p \equiv p$	SKA-One-Prl
$(x \mathbin{;} p) \parallel (y \mathbin{;} q) \equiv (x \parallel y) \mathbin{;} (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q+r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p+q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x \mathbin{;} p) \cdot (y \mathbin{;} q) \equiv (x \cdot y) \mathbin{;} (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

		$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$N ::=$	$A, B, C, \ldots$	
Bell pairs	$BP \ni bp ::=$	$N \sim N$	
Multisets	$\mathcal{M}(BP) \ni a, b, r, o ::=$	$\{\!\{ bp_1, \ldots, bp_k \}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p\,;1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1\,;p \equiv p$	KA-One-Seq

Multi-round semantics

$$\llbracket p \rrbracket \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$$

$$\llbracket \omega \rrbracket_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 \mathbin{;} \pi_2 \mathbin{;} \ldots \mathbin{;} \pi_k$$

$$\llbracket p \rrbracket a \triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a$$

$$\llbracket \epsilon \rrbracket_I a \triangleq \{a\}$$

$$\llbracket [t]r \blacktriangleright o \rrbracket_I a \triangleq \begin{cases} \{o \uplus a \backslash r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$\langle\!| \mathbb{1} |\!\rangle a \equiv \top \qquad \langle\!| t \uplus b |\!\rangle a \equiv (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \,\square\, t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$$

$$(\!| 0 |\!) a \triangleq \emptyset$$

$$(\!| 1 |\!) a \triangleq \{\emptyset \bowtie a\}$$

$$(\!| [t]r \blacktriangleright o |\!) a \triangleq \begin{cases} \{o \bowtie a \backslash r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p+q |\!) a \triangleq (\!| p |\!) a \cup (\!| q |\!) a$$

$$(\!| p \cdot q |\!) a \triangleq ((\!| p |\!) \cdot (\!| q |\!)) a$$

$$(\!| p \parallel q |\!) a \triangleq ((\!| p |\!) \parallel (\!| q |\!)) a$$

Multi-round semantics

$$\llbracket p \rrbracket \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$$

$$\llbracket \omega \rrbracket_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 \mathbin{;} \pi_2 \mathbin{;} \ldots \mathbin{;} \pi_k$$

$$\llbracket p \rrbracket a \triangleq \bigcup_{\omega \in I(p)} \llbracket \omega \rrbracket_I a$$

$$\llbracket \epsilon \rrbracket_I a \triangleq \{a\}$$

$$\llbracket [t]r \blacktriangleright o \rrbracket_I a \triangleq \begin{cases} \{o \uplus a \backslash r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$\llbracket \pi_1 \mathbin{;} \pi_2 \mathbin{;} \ldots \mathbin{;} \pi_k \rrbracket_I a \triangleq (\llbracket \pi_1 \rrbracket_I \bullet \llbracket \pi_2 \mathbin{;} \ldots \mathbin{;} \pi_k \rrbracket_I) a$$

$(x\,;p)\cdot(y\,;q) \equiv (x\cdot y)\,;(p\cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p')\cdot(q \parallel q') \leq (p\cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$\mathrm{N} ::=$	$A, B, C, \ldots$
Bell pairs	$\mathrm{BP} \ni bp ::=$	$\mathrm{N}{\sim}\mathrm{N}$
Multisets		
Tests		
Atomic action		
Policies		
	$\mid$	$p^\star$ *Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$

Single round semantics

$$
\begin{aligned}
\llparenthesis p \rrparenthesis &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))\\
\llparenthesis 0 \rrparenthesis a &\triangleq \emptyset\\
\llparenthesis 1 \rrparenthesis a &\triangleq \{\emptyset \bowtie a\}\\
\llparenthesis [t]r \blacktriangleright o \rrparenthesis a &\triangleq \begin{cases} \{o \bowtie a \backslash r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}
\end{aligned}
$$

Test semantics

$$
\begin{aligned}
\langle\!| t |\!\rangle &\in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}\\
\langle\!| \mathbb{1} |\!\rangle a &\triangleq \top \qquad\qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a\\
\langle\!| b |\!\rangle a &\triangleq b \not\subseteq a \qquad \langle\!| t \sqcap t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \sqcap \langle\!| t' |\!\rangle a, \text{ with } \sqcap \text{ is either } \wedge \text{ or } \vee
\end{aligned}
$$

Single round semantics

$$
\begin{aligned}
\llparenthesis p \rrparenthesis &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))\\
\llparenthesis 0 \rrparenthesis a &\triangleq \emptyset\\
\llparenthesis 1 \rrparenthesis a &\triangleq \{\emptyset \bowtie a\}\\
\llparenthesis [t]r \blacktriangleright o \rrparenthesis a &\triangleq \begin{cases} \{o \bowtie a \backslash r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}\\
\llparenthesis p + q \rrparenthesis a &\triangleq \llparenthesis p \rrparenthesis a \cup \llparenthesis q \rrparenthesis a\\
\llparenthesis p \cdot q \rrparenthesis a &\triangleq (\llparenthesis p \rrparenthesis \cdot \llparenthesis q \rrparenthesis) a\\
\llparenthesis p \parallel q \rrparenthesis a &\triangleq (\llparenthesis p \rrparenthesis \parallel \llparenthesis q \rrparenthesis) a
\end{aligned}
$$

Multi-round semantics

$$
\begin{aligned}
[\![p]\!] &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))\\
[\![\omega]\!]_I &\in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k\\
[\![p]\!] a &\triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a\\
[\![\epsilon]\!]_I a &\triangleq \{a\}\\
[\![[t]r \blacktriangleright o]\!]_I a &\triangleq \begin{cases} \{o \uplus a \backslash r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}\\
[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a &\triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I) a
\end{aligned}
$$

KA axioms

SKA axioms for ·

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q + r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p + q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x \,;\, p) \cdot (y \,;\, q) \equiv (x \cdot y) \,;\, (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$N ::=$	$A, B, C, \ldots$	
Bell pairs	$BP \ni bp ::=$	$N\sim N$	
Multisets	$\mathcal{M}(BP) \ni a, b, r, o ::=$	$\{\!\{bp_1, \ldots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$P \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \ ; \ q$	*sequential composition*
	$\mid$	$p^{\star}$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$	

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(BP) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \square t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP) \times \mathcal{M}(BP))$$

$$(\!| 0 |\!)a \triangleq \emptyset$$

$$(\!| 1 |\!)a \triangleq \{\emptyset \bowtie a\}$$

$$(\!| [t]r \blacktriangleright o |\!)a \triangleq \begin{cases} \{o \bowtie a \backslash r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!)a \triangleq (\!| p |\!)a \cup (\!| q |\!)a$$

$$(\!| p \cdot q |\!)a \triangleq ((\!| p |\!) \cdot (\!| q |\!))a$$

$$(\!| p \parallel q |\!)a \triangleq ((\!| p |\!) \parallel (\!| q |\!))a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP))$$

$$[\![\omega]\!]_I \in \mathcal{M}(BP) \to \mathcal{P}(\mathcal{M}(BP)), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k$$

$$[\![p]\!]a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \backslash r\} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I)a$$

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p ; 1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1 ; p \equiv p$	KA-One-Seq
$p+0 \equiv p$	KA-Plus-Zero	$0 ; p \equiv 0$	KA-Zero-Seq
$p+p \equiv p$	KA-Plus-Idem	$p ; 0 \equiv 0$	KA-Seq-Zero
$(p ; q) ; r \equiv p ; (q ; r)$	KA-Seq-Assoc	$1 + p ; p^{\star} \equiv p^{\star}$	KA-Unroll-L
$p ; (q+r) \equiv p ; q + p ; r$	KA-Seq-Dist-L	$p ; r \leq r \Rightarrow p^{\star} ; r \leq r$	KA-Lfp-L
$(p+q) ; r \equiv p ; r + q ; r$	KA-Seq-Dist-R	$1 + p^{\star} ; p \equiv p^{\star}$	KA-Unroll-R
		$r ; p \leq r \Rightarrow r ; p^{\star} \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-Prl-Assoc	$p \parallel q \equiv q \parallel p$	SKA-Prl-Comm
$p \parallel (q+r) \equiv p \parallel q + p \parallel r$	SKA-Prl-Dist	$1 \parallel p \equiv p$	SKA-One-Prl
$(x ; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q+r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p+q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x ; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$\mathsf{N} ::=$	$A, B, C, \ldots$	
Bell pairs	$\mathsf{BP} \ni bp ::=$	$\mathsf{N}{\sim}\mathsf{N}$	
Multisets	$\mathcal{M}(\mathsf{BP}) \ni a, b, r, o ::=$	$\{\!\{bp_1, \ldots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$\mathsf{P} \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \,;\, q$	*sequential composition*
	$\mid$	$p^{\star}$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}]r \blacktriangleright o + [r]\emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t]p ::=$	$[t]\emptyset \blacktriangleright \emptyset \cdot p$	

Test semantics

$$\langle\!|t|\!\rangle \in \mathcal{M}(\mathsf{BP}) \to \{\top, \bot\}$$

$$\langle\!|\mathbb{1}|\!\rangle a \triangleq \top \qquad \langle\!|t \uplus b|\!\rangle a \triangleq (\langle\!|t|\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!|b|\!\rangle a$$

$$\langle\!|b|\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!|t \mathbin{\square} t'|\!\rangle a \triangleq \langle\!|t|\!\rangle a \mathbin{\square} \langle\!|t'|\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$\begin{aligned}
(\!|p|\!) &\in \mathcal{M}(\mathsf{BP}) \to \mathcal{P}(\mathcal{M}(\mathsf{BP}) \times \mathcal{M}(\mathsf{BP}))\\
(\!|0|\!)a &\triangleq \emptyset\\
(\!|1|\!)a &\triangleq \{\emptyset \bowtie a\}\\
(\!|[t]r \blacktriangleright o|\!)a &\triangleq \begin{cases}\{o \bowtie a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!|t|\!\rangle a = \top\\ \emptyset & \text{otherwise}\end{cases}\\
(\!|p + q|\!)a &\triangleq (\!|p|\!)a \cup (\!|q|\!)a\\
(\!|p \cdot q|\!)a &\triangleq ((\!|p|\!) \cdot (\!|q|\!))a\\
(\!|p \parallel q|\!)a &\triangleq ((\!|p|\!) \parallel (\!|q|\!))a
\end{aligned}$$

Multi-round semantics

$$\begin{aligned}
[\![p]\!] &\in \mathcal{M}(\mathsf{BP}) \to \mathcal{P}(\mathcal{M}(\mathsf{BP}))\\
[\![\omega]\!]_I &\in \mathcal{M}(\mathsf{BP}) \to \mathcal{P}(\mathcal{M}(\mathsf{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k\\
[\![p]\!]a &\triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a\\
[\![\epsilon]\!]_I a &\triangleq \{a\}\\
[\![[t]r \blacktriangleright o]\!]_I a &\triangleq \begin{cases}\{o \uplus a \setminus r\} & \text{if } r \subseteq a \text{ and } \langle\!|t|\!\rangle a = \top\\ \emptyset & \text{otherwise}\end{cases}\\
[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a &\triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I)a
\end{aligned}$$

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p \,;\, 1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1 \,;\, p \equiv p$	KA-One-Seq
$p+0 \equiv p$	KA-Plus-Zero	$0 \,;\, p \equiv 0$	KA-Zero-Seq
$p+p \equiv p$	KA-Plus-Idem	$p \,;\, 0 \equiv 0$	KA-Seq-Zero
$(p \,;\, q) \,;\, r \equiv p \,;\, (q \,;\, r)$	KA-Seq-Assoc	$1 + p \,;\, p^{\star} \equiv p^{\star}$	KA-Unroll-L
$p \,;\, (q+r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \leq r \Rightarrow p^{\star} \,;\, r \leq r$	KA-Lfp-L
$(p+q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^{\star} \,;\, p \equiv p^{\star}$	KA-Unroll-R
		$r \,;\, p \leq r \Rightarrow r \,;\, p^{\star} \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-Prl-Assoc	$p \parallel q \equiv q \parallel p$	SKA-Prl-Comm
$p \parallel (q+r) \equiv p \parallel q + p \parallel r$	SKA-Prl-Dist	$1 \parallel p \equiv p$	SKA-One-Prl
$(x \,;\, p) \parallel (y \,;\, q) \equiv (x \parallel y) \,;\, (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q+r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p+q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x \,;\, p) \cdot (y \,;\, q) \equiv (x \cdot y) \,;\, (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$\mathrm{N} ::=$	$A, B, C, \ldots$	
Bell pairs	$\mathrm{BP} \ni bp ::=$	$\mathrm{N} \sim \mathrm{N}$	
Multisets	$\mathcal{M}(\mathrm{BP}) \ni a, b, r, o ::=$	$\{\!\{ bp_1, \ldots, bp_k \}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t] r \blacktriangleright o$	
Policies	$\mathrm{P} \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t] p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*
	$\mid$	$p \parallel q$	*parallel composition*
	$\mid$	$p \,;\, q$	*sequential composition*
	$\mid$	$p^\star$	*Kleene star*
Basic actions	$r \triangleright o ::=$	$[\mathbb{1}] r \blacktriangleright o + [r] \emptyset \blacktriangleright \emptyset$	
Guarded policy	$[t] p ::=$	$[t] \emptyset \blacktriangleright \emptyset \cdot p$	

Test semantics

$$\langle\!| t |\!\rangle \in \mathcal{M}(\mathrm{BP}) \to \{\top, \bot\}$$

$$\langle\!| \mathbb{1} |\!\rangle a \triangleq \top \qquad \langle\!| t \uplus b |\!\rangle a \triangleq (\langle\!| t |\!\rangle a \setminus b \wedge b \subseteq a) \vee \langle\!| b |\!\rangle a$$

$$\langle\!| b |\!\rangle a \triangleq b \not\subseteq a \qquad \langle\!| t \,\square\, t' |\!\rangle a \triangleq \langle\!| t |\!\rangle a \,\square\, \langle\!| t' |\!\rangle a, \text{ with } \square \text{ is either } \wedge \text{ or } \vee$$

Single round semantics

$$(\!| p |\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!| 0 |\!) a \triangleq \emptyset$$

$$(\!| 1 |\!) a \triangleq \{ \emptyset \bowtie a \}$$

$$(\!| [t] r \blacktriangleright o |\!) a \triangleq \begin{cases} \{ o \bowtie a \setminus r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!| p + q |\!) a \triangleq (\!| p |\!) a \cup (\!| q |\!) a$$

$$(\!| p \cdot q |\!) a \triangleq ((\!| p |\!) \cdot (\!| q |\!)) a$$

$$(\!| p \parallel q |\!) a \triangleq ((\!| p |\!) \parallel (\!| q |\!)) a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k$$

$$[\![p]\!] a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{ a \}$$

$$[\![[t] r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{ o \uplus a \setminus r \} & \text{if } r \subseteq a \text{ and } \langle\!| t |\!\rangle a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 \fatsemi \pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 \fatsemi \ldots \fatsemi \pi_k]\!]_I) a$$

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p \,;\, 1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1 \,;\, p \equiv p$	KA-One-Seq
$p+0 \equiv p$	KA-Plus-Zero	$0 \,;\, p \equiv 0$	KA-Zero-Seq
$p+p \equiv p$	KA-Plus-Idem	$p \,;\, 0 \equiv 0$	KA-Seq-Zero
$(p \,;\, q) \,;\, r \equiv p \,;\, (q \,;\, r)$	KA-Seq-Assoc	$1 + p \,;\, p^\star \equiv p^\star$	KA-Unroll-L
$p \,;\, (q+r) \equiv p \,;\, q + p \,;\, r$	KA-Seq-Dist-L	$p \,;\, r \le r \Rightarrow p^\star \,;\, r \le r$	KA-Lfp-L
$(p+q) \,;\, r \equiv p \,;\, r + q \,;\, r$	KA-Seq-Dist-R	$1 + p^\star \,;\, p \equiv p^\star$	KA-Unroll-R
		$r \,;\, p \le r \Rightarrow r \,;\, p^\star \le r$	KA-Lfp-R

SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-Prl-Assoc	$p \parallel q \equiv q \parallel p$	SKA-Prl-Comm
$p \parallel (q+r) \equiv p \parallel q + p \parallel r$	SKA-Prl-Dist	$1 \parallel p \equiv p$	SKA-One-Prl
$(x \,;\, p) \parallel (y \,;\, q) \equiv (x \parallel y) \,;\, (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

SKA axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q+r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p+q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$(x \,;\, p) \cdot (y \,;\, q) \equiv (x \cdot y) \,;\, (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

Boolean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t] r \blacktriangleright o \cdot [t'] r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)] \hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t] r \blacktriangleright o \parallel [t'] r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)] \hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}] \emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \le (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset] r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t] r \blacktriangleright o \equiv [(r \cup b) \wedge t] r \blacktriangleright o$	Sr-Can
		$[t] r \blacktriangleright o + [t'] r \blacktriangleright o \equiv [t \vee t'] r \blacktriangleright o$	Sr-Plus

BellKAT at a glance

Syntax

Nodes	$\mathrm{N} ::=$	$A, B, C, \ldots$	
Bell pairs	$\mathrm{BP} \ni bp ::=$	$\mathrm{N}{\sim}\mathrm{N}$	
Multisets	$\mathcal{M}(\mathrm{BP}) \ni a, b, r, o ::=$	$\{\!\{bp_1, \ldots, bp_k\}\!\}$	
Tests	$T \ni t, t' ::=$	$\mathbb{1}$	*no test*
	$\mid$	b	*multiset absence*
	$\mid$	$t \wedge t'$	*conjunction*
	$\mid$	$t \vee t'$	*disjunction*
	$\mid$	$t \uplus b$	*multiset union*
Atomic actions	$\Pi \ni \pi, x, y ::=$	$[t]r \blacktriangleright o$	
Policies	$\mathrm{P} \ni p, q ::=$	0	*abort*
	$\mid$	1	*skip or no-round*
	$\mid$	π	*atomic action*
	$\mid$	$r \triangleright o$	*basic action*
	$\mid$	$[t]p$	*guarded policy*
	$\mid$	$p + q$	*nondeterministic choice*
	$\mid$	$p \cdot q$	*ordered composition*

Network axioms

$$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$$

$$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$$

$$(\!|p|\!) \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}) \times \mathcal{M}(\mathrm{BP}))$$

$$(\!|0|\!)a \triangleq \emptyset$$

$$(\!|1|\!)a \triangleq \{\emptyset \bowtie a\}$$

$$(\!|[t]r \blacktriangleright o|\!)a \triangleq \begin{cases} \{o \bowtie a \backslash r\} & \text{if } r \subseteq a \text{ and } (\!|t|\!)a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$(\!|p + q|\!)a \triangleq (\!|p|\!)a \cup (\!|q|\!)a$$

$$(\!|p \cdot q|\!)a \triangleq ((\!|p|\!) \cdot (\!|q|\!))a$$

$$(\!|p \parallel q|\!)a \triangleq ((\!|p|\!) \parallel (\!|q|\!))a$$

Multi-round semantics

$$[\![p]\!] \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP}))$$

$$[\![\omega]\!]_I \in \mathcal{M}(\mathrm{BP}) \to \mathcal{P}(\mathcal{M}(\mathrm{BP})), \text{ where } \omega = \pi_1 ⨟ \pi_2 ⨟ \ldots ⨟ \pi_k$$

$$[\![p]\!]a \triangleq \textstyle\bigcup_{\omega \in I(p)} [\![\omega]\!]_I a$$

$$[\![\epsilon]\!]_I a \triangleq \{a\}$$

$$[\![[t]r \blacktriangleright o]\!]_I a \triangleq \begin{cases} \{o \uplus a \backslash r\} & \text{if } r \subseteq a \text{ and } (\!|t|\!)a = \top \\ \emptyset & \text{otherwise} \end{cases}$$

$$[\![\pi_1 ⨟ \pi_2 ⨟ \ldots ⨟ \pi_k]\!]_I a \triangleq ([\![\pi_1]\!]_I \bullet [\![\pi_2 ⨟ \ldots ⨟ \pi_k]\!]_I)a$$

KA axioms

$(p+q)+r \equiv p+(q+r)$	KA-Plus-Assoc	$p ; 1 \equiv p$	KA-Seq-One
$p+q \equiv q+p$	KA-Plus-Comm	$1 ; p \equiv p$	KA-One-Seq
$p+0 \equiv p$	KA-Plus-Zero	$0 ; p \equiv 0$	KA-Zero-Seq
$p+p \equiv p$	KA-Plus-Idem	$p ; 0 \equiv 0$	KA-Seq-Zero
$(p;q);r \equiv p;(q;r)$	KA-Seq-Assoc	$1 + p ; p^\star \equiv p^\star$	KA-Unroll-L
$p;(q+r) \equiv p;q + p;r$	KA-Seq-Dist-L	$p ; r \leq r \Rightarrow p^\star ; r \leq r$	KA-Lfp-L
$(p+q);r \equiv p;r + q;r$	KA-Seq-Dist-R	$1 + p^\star ; p \equiv p^\star$	KA-Unroll-R
		$r ; p \leq r \Rightarrow r ; p^\star \leq r$	KA-Lfp-R

SKA axioms for $\parallel$

$(p \parallel q) \parallel r \equiv p \parallel (q \parallel r)$	SKA-Prl-Assoc	$p \parallel q \equiv q \parallel p$	SKA-Prl-Comm
$p \parallel (q+r) \equiv p \parallel q + p \parallel r$	SKA-Prl-Dist	$1 \parallel p \equiv p$	SKA-One-Prl
$; p) \parallel (y ; q) \equiv (x \parallel y) ; (p \parallel q)$	SKA-Prl-Seq	$0 \parallel p \equiv 0$	SKA-Zero-Prl

axioms for $\cdot$

$(p \cdot q) \cdot r \equiv p \cdot (q \cdot r)$	SKA-Ord-Assoc	$1 \cdot p \equiv p$	SKA-One-Ord
$p \cdot (q+r) \equiv p \cdot q + p \cdot r$	SKA-Ord-Dist-L	$p \cdot 1 \equiv p$	SKA-Ord-One
$(p+q) \cdot r \equiv p \cdot r + q \cdot r$	SKA-Ord-Dist-R	$0 \cdot p \equiv 0$	SKA-Zero-Ord
$; p) \cdot (y ; q) \equiv (x \cdot y) ; (p \cdot q)$	SKA-Ord-Seq	$p \cdot 0 \equiv 0$	SKA-Ord-Zero

ean axioms (in addition to monotone axioms)

$\mathbb{1} \uplus b \equiv \mathbb{1}$	Bool-One-U	$(t \wedge t') \uplus b \equiv t \uplus b \wedge t' \uplus b$	Bool-Conj-U-Dist
$b \wedge (b \uplus b') \equiv b$	Bool-Conj-Subset	$(t \vee t') \uplus b \equiv t \uplus b \vee t' \uplus b$	Bool-Disj-U-Dist
$b \vee b' \equiv b \cup b'$	Bool-Disj-U		

Network axioms

$[t]r \blacktriangleright o \cdot [t']r' \blacktriangleright o' \equiv [t \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Ord
$[t]r \blacktriangleright o \parallel [t']r' \blacktriangleright o' \equiv [(t \uplus r') \wedge (t' \uplus r)]\hat{r} \blacktriangleright \hat{o}$	if $\hat{r} = r \uplus r'$ and $\hat{o} = o \uplus o'$	Net-Prl

Single round axioms

$[\mathbb{1}]\emptyset \blacktriangleright \emptyset \equiv 1$	Sr-One	$(p \parallel p') \cdot (q \parallel q') \leq (p \cdot q) \parallel (p' \cdot q')$	Sr-Exc
$[\emptyset]r \blacktriangleright o \equiv 0$	Sr-Zero	$[b \wedge t]r \blacktriangleright o \equiv [(r \cup b) \wedge t]r \blacktriangleright o$	Sr-Can
		$[t]r \blacktriangleright o + [t']r \blacktriangleright o \equiv [t \vee t']r \blacktriangleright o$	Sr-Plus

Formal results

Definition 4.7 (Normal form of policies). A policy p is in normal form if it is a finite sum, s.t. every summand has a unique (r, o) pair with the corresponding t in canonical form w.r.t. r and $t \neq r$:

$$p = \sum [t] r \blacktriangleright o$$

Proposition 4.1 (Soundness and completeness). *Let p, q be single round policies. Then p and q are provably equivalent by the BellKAT axioms if and only if $(\!| p |\!) = (\!| q |\!)$.*

Theorem 4.2 (Soundness and completeness w.r.t. standard interpretation). *Policies p, q are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is, $I(p) = I(q)$ if and only if $\vdash p \equiv q$.*

Theorem 4.3 (Soundness of multi-round policies). *If policies $p, q \in \mathrm{P}$ are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is, $\vdash p \equiv q \implies [\![p]\!] = [\![q]\!]$.*

Formal results

Definition 4.7 (Normal form of policies). A policy p is in normal form if it is a finite sum, s.t. every summand has a unique (r, o) pair with the corresponding t in canonical form w.r.t. r and $t \neq r$:

$$p = \sum [t] r \blacktriangleright o$$

Proposition 4.1 (Soundness and completeness). *Let p, q be single round policies. Then p and q are provably equivalent by the BellKAT axioms if and only if $(\!| p |\!) = (\!| q |\!)$.*

Theorem 4.2 (Soundness and completeness w.r.t. standard interpretation). *Policies p, q are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is, $I(p) = I(q)$ if and only if $\vdash p \equiv q$.*

Theorem 4.3 (Soundness of multi-round policies). *If policies $p, q \in \mathrm{P}$ are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is, $\vdash p \equiv q \implies [\![p]\!] = [\![q]\!]$.*

Formal results

Definition 4.7 (Normal form of policies). A policy p is in normal form if it is a finite sum, s.t. every summand has a unique (r, o) pair with the corresponding t in canonical form w.r.t. r and $t \neq r$:

$$p = \sum [t] r \blacktriangleright o$$

$$\downarrow \downarrow$$

PROPOSITION 4.1 (SOUNDNESS AND COMPLETENESS). *Let p, q be single round policies. Then p and q are provably equivalent by the BellKAT axioms if and only if $(\!| p |\!) = (\!| q |\!)$.*

THEOREM 4.2 (SOUNDNESS AND COMPLETENESS W.R.T. STANDARD INTERPRETATION). *Policies p, q are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is, $I(p) = I(q)$ if and only if $\vdash p \equiv q$.*

THEOREM 4.3 (SOUNDNESS OF MULTI-ROUND POLICIES). *If policies $p, q \in \mathrm{P}$ are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is, $\vdash p \equiv q \Longrightarrow [\![p]\!] = [\![q]\!]$.*

Formal results

Definition 4.7 (Normal form of policies). A policy p is in normal form if it is a finite sum, s.t. every summand has a unique (r, o) pair with the corresponding t in canonical form w.r.t. r and $t \neq r$:

$$p = \sum [t] r \blacktriangleright o$$

$\downarrow \downarrow$

PROPOSITION 4.1 (SOUNDNESS AND COMPLETENESS). *Let p, q be single round policies. Then p and q are provably equivalent by the BellKAT axioms if and only if $(\!| p |\!) = (\!| q |\!)$.*

THEOREM 4.2 (SOUNDNESS AND COMPLETENESS W.R.T. STANDARD INTERPRETATION). *Policies p, q are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is, $I(p) = I(q)$ if and only if $\vdash p \equiv q$.*

THEOREM 4.3 (SOUNDNESS OF MULTI-ROUND POLICIES). *If policies $p, q \in \mathrm{P}$ are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is, $\vdash p \equiv q \Longrightarrow [\![p]\!] = [\![q]\!]$.*

Formal results

Definition 4.7 (Normal form of policies). A policy p is in normal form if it is a finite sum, s.t. every summand has a unique (r, o) pair with the corresponding t in canonical form w.r.t. r and $t \neq r$:

$$p = \sum [t] r \blacktriangleright o$$

$\downarrow\downarrow$

PROPOSITION 4.1 (SOUNDNESS AND COMPLETENESS). *Let p, q be single round policies. Then p and q are provably equivalent by the BellKAT axioms if and only if $⦇ p ⦈ = ⦇ q ⦈$.*

THEOREM 4.2 (SOUNDNESS AND COMPLETENESS W.R.T. STANDARD INTERPRETATION). *Policies p, q are equal under the standard interpretation if and only if they are provably equivalent using BellKAT's axioms. That is, $I(p) = I(q)$ if and only if $\vdash p \equiv q$.*

$\downarrow\downarrow$

THEOREM 4.3 (SOUNDNESS OF MULTI-ROUND POLICIES). *If policies $p, q \in \mathrm{P}$ are equivalent under BellKAT's axioms, then their denotational semantics coincide. That is, $\vdash p \equiv q \implies [\![p]\!] = [\![q]\!]$.*

Decidability

THEOREM 4.4. *If p and q are valid policies with respect to $\mathcal{N}_0 \subseteq \mathcal{N}$, then $[\![p]\!] =_{\mathcal{N}_0} [\![q]\!]$ is decidable.*

Decidability

THEOREM 4.4. *If p and q are valid policies with respect to $\mathcal{N}_0 \subseteq \mathcal{N}$, then $[\![p]\!] =_{\mathcal{N}_0} [\![q]\!]$ is decidable.*

Reachability property: Does protocol p always or never generate an entangled pair $A{\sim}E$

$$p; [1]\{\!\{A{\sim}E\}\!\} \blacktriangleright \{\!\{A{\sim}E\}\!\} \equiv_{\mathcal{N}_0} p \quad \text{or} \quad p; [\{\!\{A{\sim}E\}\!\}]\emptyset \blacktriangleright \emptyset \equiv_{\mathcal{N}_0} p$$

Decidability

> **Theorem 4.4.** *If p and q are valid policies with respect to $\mathcal{N}_0 \subseteq \mathcal{N}$, then $[\![p]\!] =_{\mathcal{N}_0} [\![q]\!]$ is decidable.*

Reachability property: Does protocol p always or never generate an entangled pair $A{\sim}E$

$$p; [1]\{\!\{A{\sim}E\}\!\} \blacktriangleright \{\!\{A{\sim}E\}\!\} \equiv_{\mathcal{N}_0} p \quad \text{or} \quad p; [\{\!\{A{\sim}E\}\!\}]\emptyset \blacktriangleright \emptyset \equiv_{\mathcal{N}_0} p$$

Verify more protocol properties with the BellKAT artifact!

Summary

- BellKAT – language to specify quantum networks based on a novel algebraic structure
- Soundness and completeness of BellKAT's axioms w.r.t. their corresponding semantics
- Decidability result for checking semantic equivalence of quantum network protocols
- Prototype tool for automated reasoning about protocols

Summary

- BellKAT – language to specify quantum networks based on a novel algebraic structure
- Soundness and completeness of BellKAT's axioms w.r.t. their corresponding semantics
- Decidability result for checking semantic equivalence of quantum network protocols
- Prototype tool for automated reasoning about protocols

THANK YOU!

Expressing failures

$$r \triangleright o + r \triangleright \emptyset \triangleq r \triangleright o + \mathsf{fail}\langle r \rangle$$

Bell pairs: consumed, produced and untouched

Expressing failures

$$r \triangleright o + r \triangleright \emptyset \triangleq r \triangleright o + \textsf{fail}\langle r \rangle$$

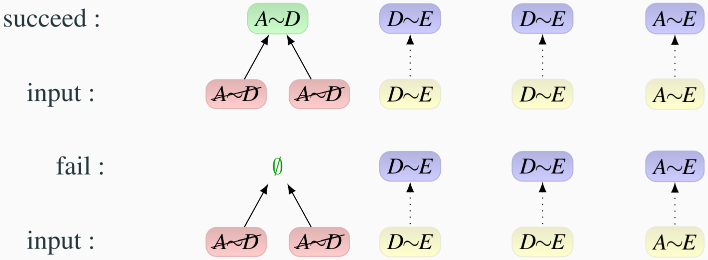
Distill $\{\!\{A{\sim}D, A{\sim}D\}\!\} \triangleright \{\!\{A{\sim}D\}\!\} + \{\!\{A{\sim}D, A{\sim}D\}\!\} \triangleright \emptyset$ on input $\{\!\{\underline{A{\sim}D}, \underline{A{\sim}D}, D{\sim}E, D{\sim}E, A{\sim}E\}\!\}$

Bell pairs: consumed, produced and untouched

Expressing failures

$$r \triangleright o + r \triangleright \emptyset \triangleq r \triangleright o + \mathsf{fail}\langle r \rangle$$

Distill $\{\!\{A{\sim}D, A{\sim}D\}\!\} \triangleright \{\!\{A{\sim}D\}\!\} + \{\!\{A{\sim}D, A{\sim}D\}\!\} \triangleright \emptyset$ on input $\{\!\{\underline{A{\sim}D}, \underline{A{\sim}D}, D{\sim}E, D{\sim}E, A{\sim}E\}\!\}$



Bell pairs: consumed, produced and untouched

Single round protocols

Parallel composition

$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$ acts on $\{\!\{A{\sim}R, B{\sim}R, B{\sim}R, B{\sim}R', C{\sim}R', A{\sim}B\}\!\}$

$A{\sim}R$ $B{\sim}R$ $B{\sim}R$ $B{\sim}R'$ $C{\sim}R'$ $A{\sim}B$

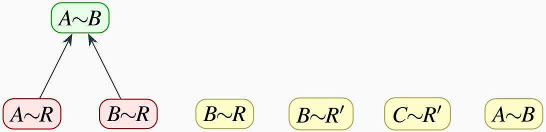
The order of basic actions is independent for this input multiset, thus:

$$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle = \mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$$

Input Bell pairs

Parallel composition

$\underline{\mathsf{sw}\langle A{\sim}B \,@\, R\rangle} \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$ acts on $\{\!\{\underline{A{\sim}R}, \underline{B{\sim}R}, B{\sim}R, B{\sim}R', C{\sim}R', A{\sim}B\}\!\}$



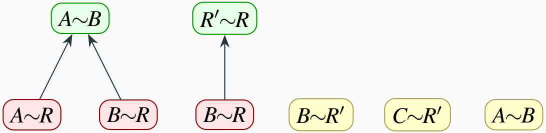
The order of basic actions is independent for this input multiset, thus:

$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle = \mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

Bell pairs: input and consumed, produced

Parallel composition

$\underline{\text{sw}\langle A{\sim}B \,@\, R\rangle \,||\, \text{tr}\langle B{\sim}R \rightarrow R'{\sim}R\rangle} \,||\, \text{sw}\langle B{\sim}C \,@\, R'\rangle$ acts on $\{\!\{\not{A{\sim}R}, \not{B{\sim}R}, \underline{B{\sim}R}, B{\sim}R', C{\sim}R', A{\sim}B\}\!\}$



The order of basic actions is independent for this input multiset, thus:

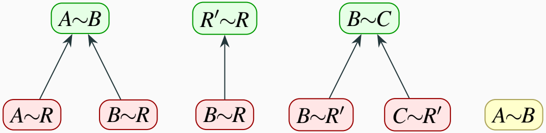
$\text{sw}\langle A{\sim}B \,@\, R\rangle \cdot \text{tr}\langle B{\sim}R \rightarrow R'{\sim}R\rangle \cdot \text{sw}\langle B{\sim}C \,@\, R'\rangle = \text{sw}\langle A{\sim}B \,@\, R\rangle \,||\, \text{tr}\langle B{\sim}R \rightarrow R'{\sim}R\rangle \,||\, \text{sw}\langle B{\sim}C \,@\, R'\rangle$

Bell pairs: input and consumed, produced

Single round protocols

Parallel composition

$\underline{\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \rightarrow R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle}$ acts on $\{\!\{\cancel{A{\sim}R}, \cancel{B{\sim}R}, \cancel{B{\sim}R}, \underline{B{\sim}R'}, \underline{C{\sim}R'}, A{\sim}B\}\!\}$



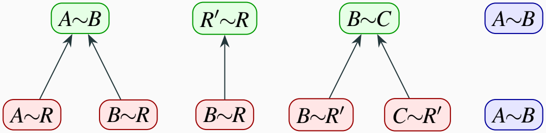
The order of basic actions is independent for this input multiset, thus:

$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \rightarrow R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle = \mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \rightarrow R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

Bell pairs: input and consumed, produced

Parallel composition

$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$ acts on $\{\!\{A{\sim}R, B{\sim}R, B{\sim}R, B{\sim}R', C{\sim}R', A{\sim}B\}\!\}$



The order of basic actions is independent for this input multiset, thus:

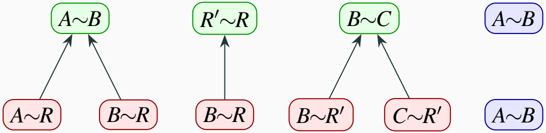
$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle = \mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

Bell pairs: consumed, produced and untouched

Single round protocols

Parallel composition

$\mathsf{sw}\langle A{\sim}B\,@\,R\rangle \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C\,@\,R'\rangle$ acts on $\{\!\{A{\sim}R, B{\sim}R, B{\sim}R, B{\sim}R', C{\sim}R', A{\sim}B\}\!\}$



The order of basic actions is independent for this input multiset, thus:

$$\mathsf{sw}\langle A{\sim}B\,@\,R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C\,@\,R'\rangle = \mathsf{sw}\langle A{\sim}B\,@\,R\rangle \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C\,@\,R'\rangle$$

Bell pairs: consumed, produced and untouched

Parallel composition vs. ordered composition

$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

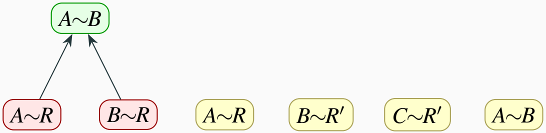
$A{\sim}R$ $B{\sim}R$ $A{\sim}R$ $B{\sim}R'$ $C{\sim}R'$ $A{\sim}B$

$\mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

Bell pairs: input and consumed, produced

Parallel composition vs. ordered composition

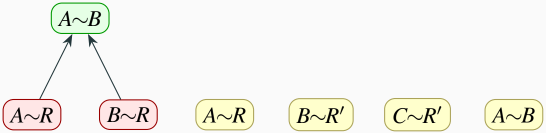
$\underline{\mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle} \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle$



Bell pairs: input and consumed, produced

Parallel composition vs. ordered composition

$\underline{\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle} \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

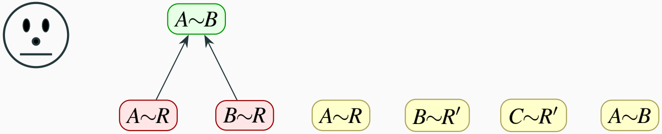


$\mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

Bell pairs: input and consumed, produced

Parallel composition vs. ordered composition

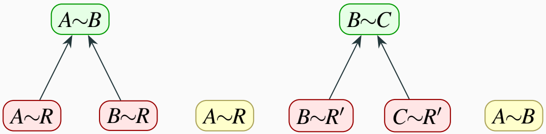
$\underline{\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle} \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$



Bell pairs: input and consumed, produced

Parallel composition vs. ordered composition

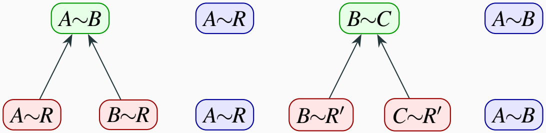
$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \rightarrow R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$



[2] Bell pairs: input and consumed, produced.

Parallel composition vs. ordered composition

$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

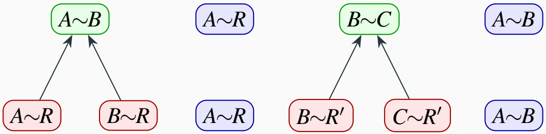


$\mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$

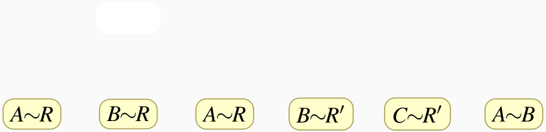
Bell pairs: consumed, produced and untouched

Parallel composition vs. ordered composition

$\mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle$



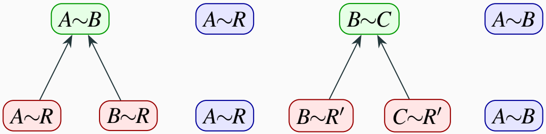
$\mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle$



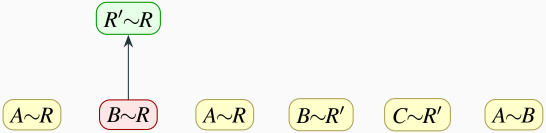
Bell pairs: consumed, produced and untouched

Parallel composition vs. ordered composition

$\underline{\mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle}$



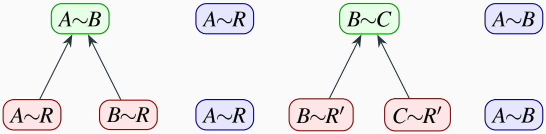
$\underline{\mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle} \cdot \mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle$



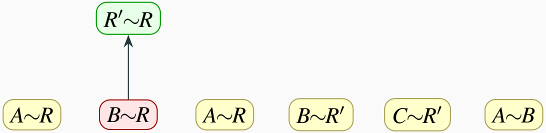
Bell pairs: consumed, produced and untouched

Parallel composition vs. ordered composition

$\underline{\mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle}$



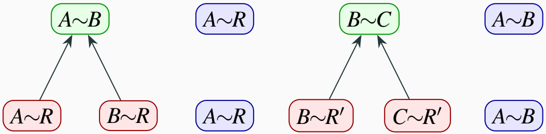
$\underline{\mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle} \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle$



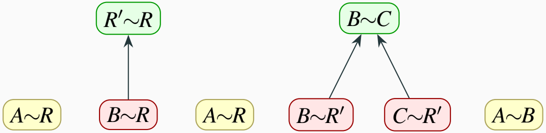
Bell pairs: consumed, produced and untouched

Parallel composition vs. ordered composition

$\mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle$



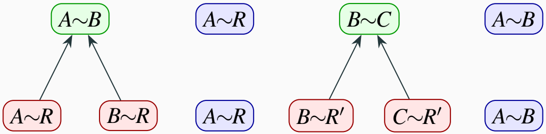
$\mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle A{\sim}B \mathbin{@} R\rangle \cdot \mathsf{sw}\langle B{\sim}C \mathbin{@} R'\rangle$



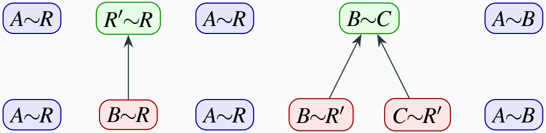
Bell pairs: consumed, produced and untouched

Parallel composition vs. ordered composition

$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$



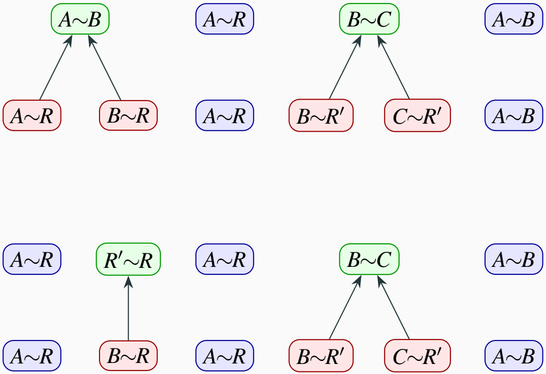
$\mathsf{tr}\langle B{\sim}R \to R'{\sim}R\rangle \cdot \mathsf{sw}\langle A{\sim}B \,@\, R\rangle \cdot \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$



Bell pairs: consumed, produced and untouched

Parallel composition vs. ordered composition

$\mathsf{sw}\langle A{\sim}B \,@\, R\rangle \parallel \mathsf{tr}\langle B{\sim}R \rightarrow R'{\sim}R\rangle \parallel \mathsf{sw}\langle B{\sim}C \,@\, R'\rangle$



Bell pairs: consumed, produced and untouched

Verification - properties with a classical analogoue

- *Reachability.* Will the execution of our protocol generate $A{\sim}C$?

Verification - properties with a classical analogoue

- *Reachability.* Will the execution of our protocol generate $A{\sim}C$?
- *Waypoint Correctness.* Does our protocol ever perform a swap at node B?

Verification - properties with a classical analogoue

- *Reachability.* Will the execution of our protocol generate $A{\sim}C$?
- *Waypoint Correctness.* Does our protocol ever perform a swap at node B?
- *Traffic (Protocol) Isolation.* Can we prove non-interference in a composition of Protocols I and II?

Verification - properties with a classical analogoue

- *Reachability.* Will the execution of our protocol generate $A{\sim}C$?
- *Waypoint Correctness.* Does our protocol ever perform a swap at node B?
- *Traffic (Protocol) Isolation.* Can we prove non-interference in a composition of Protocols I and II?
- *Compilation.* Can we ensure correct compilation to individual devices?

Verification - properties specific to quantum

- *Resource Utilization.* What is the number of required memory locations and communication qubits? For how many rounds must a Bell pair wait in the memory?

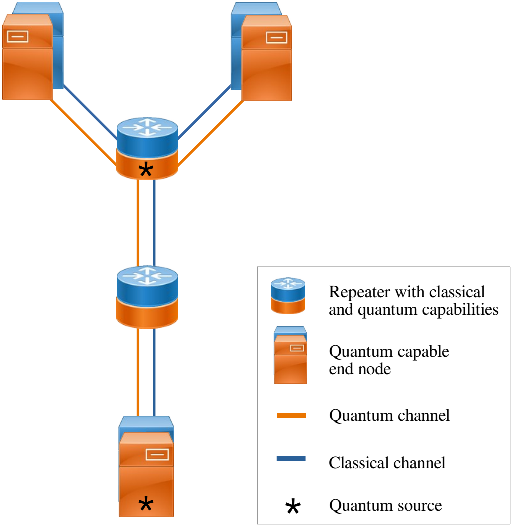
Verification - properties specific to quantum

- *Resource Utilization.* What is the number of required memory locations and communication qubits? For how many rounds must a Bell pair wait in the memory?
- *Quality of Service.* Do the generated Bell pairs have the required fidelity or capacity?

Verification - properties specific to quantum

- *Resource Utilization.* What is the number of required memory locations and communication qubits? For how many rounds must a Bell pair wait in the memory?
- *Quality of Service.* Do the generated Bell pairs have the required fidelity or capacity?
- *Compilation.* Can we minimize the number of accesses to the network global state?

Quantum network



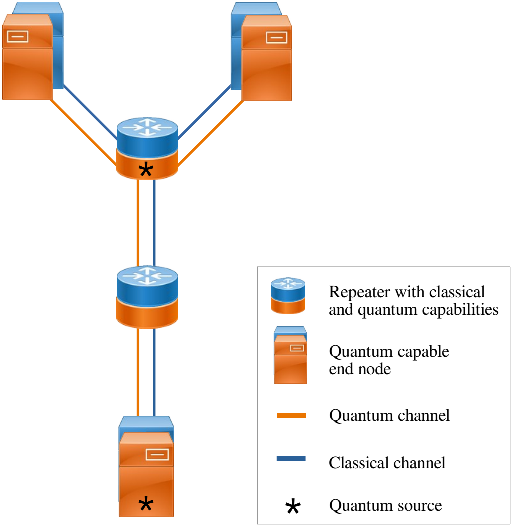
[1]

What/Key service: providing *communication services* to distributed quantum applications

How: end-to-end Bell pair distribution[2]

[1] [Kozlowski, Wehner NANOCOM 2019], [2] [RFC 9340 IRTF–QIRG 2023]

Quantum network



[1]

What/Key service: providing *communication services* to distributed quantum applications

How: end-to-end Bell pair distribution[2]

secure communication

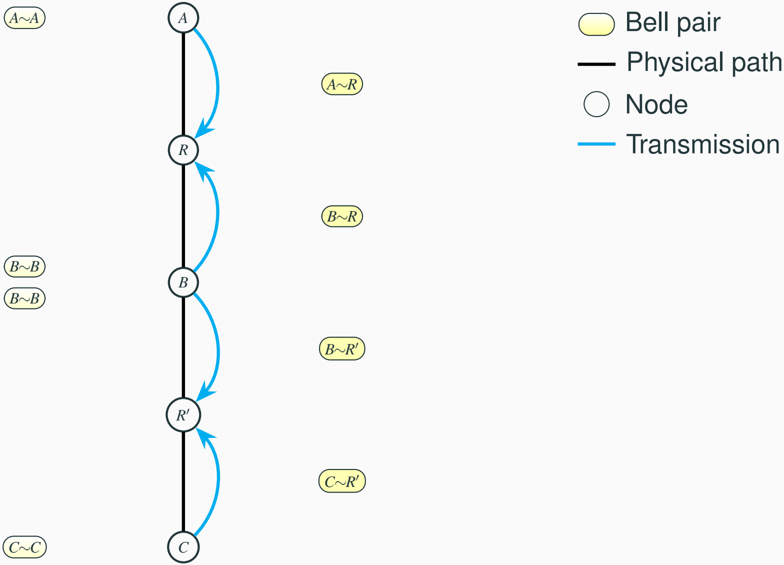
secure quantum computing in the cloud

clock synchronization
password identification
position verification

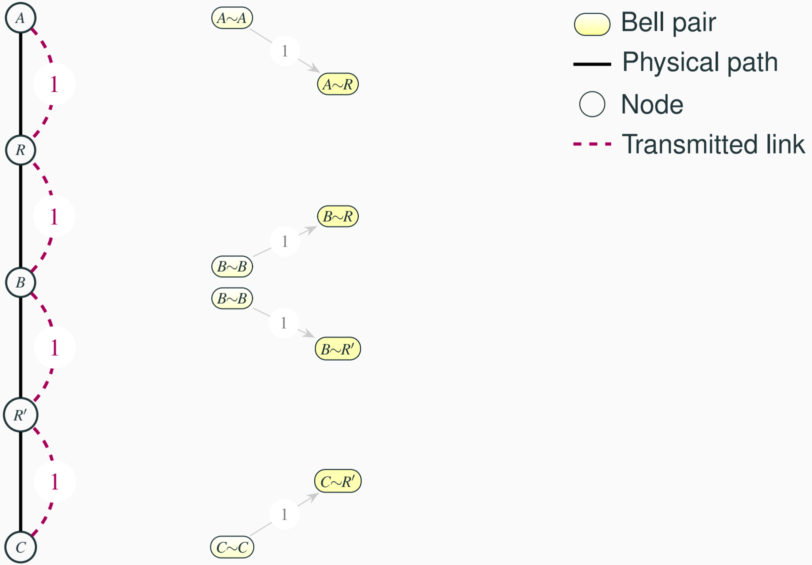
quantum computing clusters

[1][Kozlowski, Wehner NANOCOM 2019], [2][RFC 9340 IRTF–QIRG 2023]

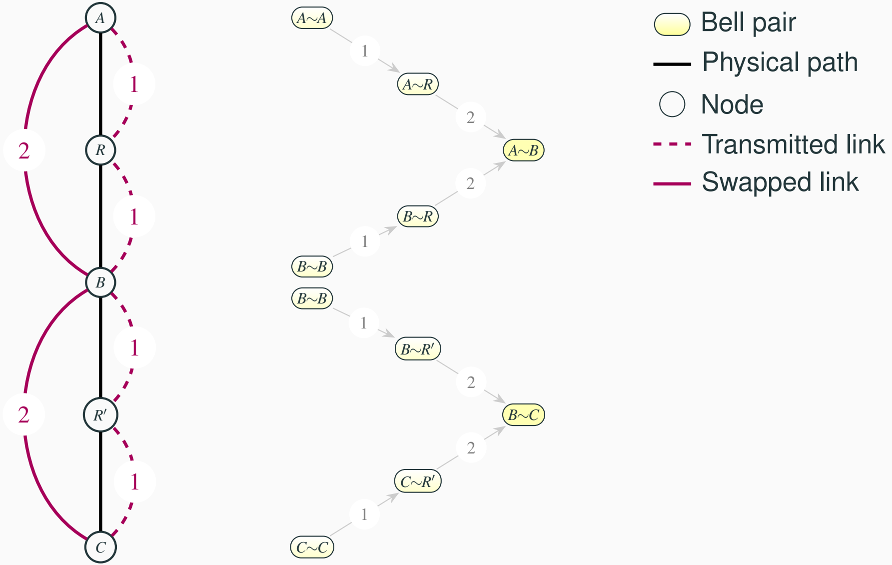
Bell pair generation: Protocol I



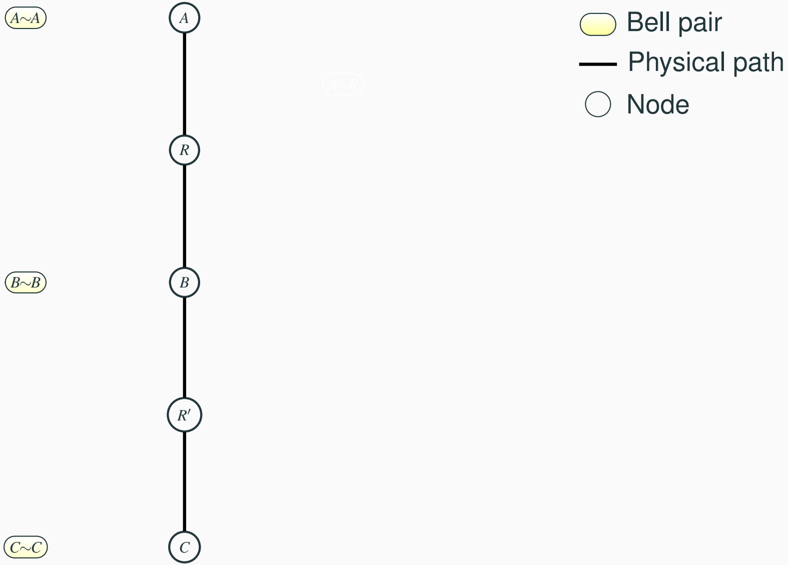
Bell pair generation: Protocol I, round 1



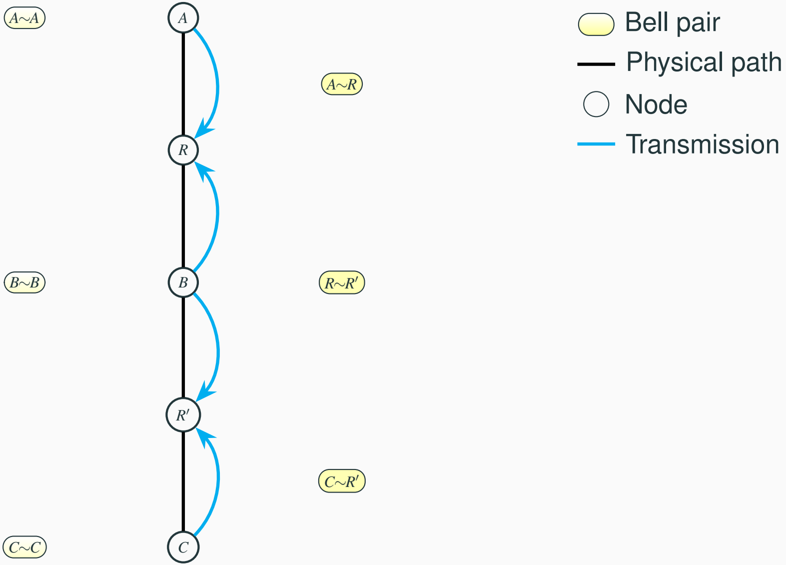
Bell pair generation: Protocol I, round 2



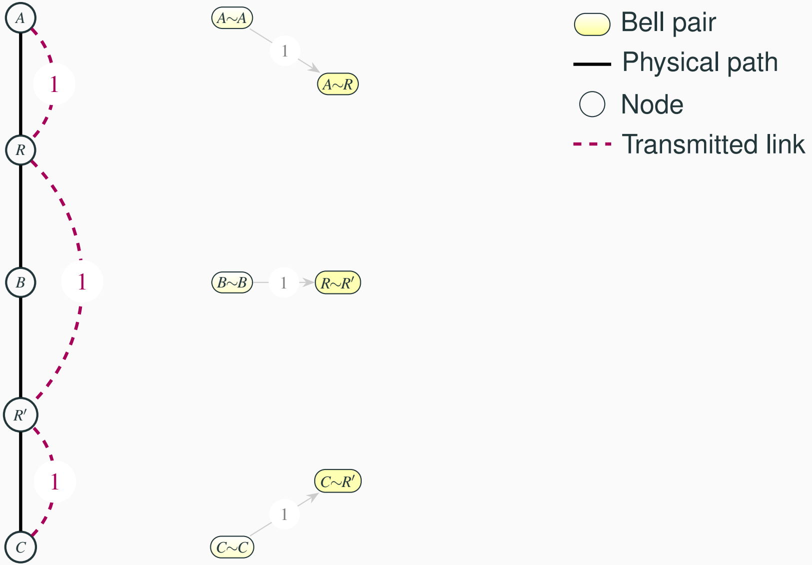
Bell pair generation: Protocol II



Bell pair generation: Protocol II



Bell pair generation: Protocol II, round 1



Bell pair generation: Protocol II, round 2