Category Theory in Communication, Cryptography, & Security

Peter M. Hines

Y.C.C.S.A

Univ. York

The purpose of the talk ...

1. An elementary introduction to (some) category theory

   [Disclaimer : it is a very large subject !]

2. Motivation : why should it be of interest in S.C.C. ?

   - Motivation by example – elementary tools.
   - Unexpected structural connections.
   - Simplifying seemingly complex structures.

Established category theorists may find the first half rather straightforward!

The big question

Before we get into definitions & details ...

Question :

Why should CCS researchers put in the effort of learning about category theory?

Some motivation

Answer 1(a) : It has – at least partially – already happened.

The *quantum world* is further along this track – at least, in terms of widespread acceptance – than the classical world.

> "A categorical semantics for quantum protocols"
> — S. Abramsky & B. Coecke (2004)

Categorical / graphical tools for describing & reasoning about protocols such as *quantum key distribution*, *teleportation*, etc., based on category theory originally developed for models of formal logic.

The utility: Replacing complex Hilbert space calculations by simple diagrammatic manipulation.

Some motivation

Answer 1(b) : It has – at least partially – already happened.

Similar tools are found the *classical world*.

> *"Category Theory Applied to Information Flow for Computer Security"*
> *– C. O'Halloran (Oxford Uni. D.Phil. Thesis)*

Colin O'Halloran :

- Currently founding director of DrisQ

  > *"assuring the behaviour of systems and software for the UK government"*

- Formerly of QinetiQ (U.K. Gov. Research Lab.s).

Some more motivation

Answer 1(c) : It has – at least partially – already happened.

More recently :

- "Chasing diagrams in cryptography" – D. Pavlovic (2014) Diagram-chasing is a key categorical technique for replacing *equational* by *diagrammatic* manipulations.

  – a key theme of the Univ. Hawaii cryptography & security group.

- Well-received computer packages & systems, designed along purely categorical lines, with all trace of this hidden from the end-user.
- University courses that include category-theoretic content without using that name ...

Some motivation

Answer 2 : To make thing simpler(!)
Category theory frequently expresses *equations* as *pictures*.

Algebraic manipulations are replaced by *diagram-chasing*.

(This was by necessity: symbol-pushing proofs in category theory can be ridiculously long & unwieldy.)

Two distinct but related methods:

1. String diagrams (originally from physics – Penrose diagrams, &c.),
2. Commuting diagrams (original to category theory).

Even more motivation

Answer 3 : Unexpected & surprising connections
We occasionally find fundamental structures from the foundations of category theory in other fields.

C.C.S. is no exception. We need to ask :

1. Is there some deep reason why?
2. Is there any practical utility to making such an observation?

The topic of the second half of the talk

Category Theory – the original motivation

- A formalism for reasoning about the 'large-scale' properties of mathematical structures.
- Introduced in 1940s by S. Eilenberg & S. MacLane, in the context of *algebraic topology*.
- Significant precursors include the von Neumann - Gödel - Bernay theory of proper classes.

The canonical textbook:

Categories for the Working Mathematician

— Saunders MacLane (1971)

Working through this is not easy, without a fair grasp of algebraic topology and related areas ...

Towards formal definitions ..

We might consider the categories of all **groups**, or all **rings**, or all **spaces**, or even all **sets**, etc., and study their properties and relationships with each other.

A category consist of **objects** and **arrows** :

Objects All mathematical structures of a certain kind.

Arrows Structure-preserving mappings between objects.

Composition Arrows may be composed ...

The definition ...

A **category** $\mathcal{C}$ consists of

- A **proper class** of objects, $Ob(\mathcal{C})$.
- For all objects $A, B \in Ob(\mathcal{C})$, a **set** of arrows $\mathcal{C}(A, B)$.

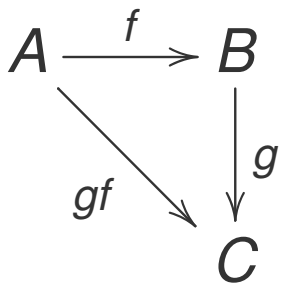
We will work diagrammatically:

An arrow $f \in \mathcal{C}(A, B)$ is drawn as

$$A \xrightarrow{f} B$$

The axioms ...

- Matching arrows can be composed



- Composition is associative

$$h(gf) = (hg)f$$

- There is an identity 1_A at each object A

A straightforward consequence ..

The set $\mathcal{C}(A, A)$ of arrows from an object to itself is a monoid.

The intuition

Many categories are of the following form:

Objects All mathematical structures of a certain type.

Arrows Structure-preserving mappings between objects.

Identities Doing nothing is certainly structure-preserving!

These are 'large categories'

Category theory as a 'big-picture' view of mathematics.

Mathematical structures as categories

- **Monoid**
  - (Objects:) *all monoids*.
  - (Arrows:) *homomorphisms*.
- **Hilb**
  - (Objects:) *all Hilbert spaces*.
  - (Arrows:) *bounded linear maps*.
- **Top**
  - (Objects:) *all topological spaces*.
  - (Arrows:) *continuous maps*.
- **Set**
  - (Objects:) *all sets*.
  - (Arrows:) *functions between sets*.

The underlying philosophy

The area of study is **not** the structures in question

It is the structure-preserving maps between them!

In particular

We do not discuss *elements* or *subsets* of an object.

This is not set theory!

Maps between categories

A **functor** $\Gamma : \mathcal{C} \to \mathcal{D}$ is a structure-preserving map between categories:

$$A \xrightarrow{\quad f \quad} B \qquad \text{in category } \mathcal{C}$$

$$\Gamma \Downarrow$$

$$\Gamma(A) \xrightarrow{\quad \Gamma(f) \quad} \Gamma(B) \qquad \text{in category } \mathcal{D}$$

Functors preserve *composition* and *identities*.

We can discuss the category of all categories ...

From the large to the small

At the other extreme, we have **small categories**.

- A *monoid* is itself a category, with only one object.
- A *partially ordered set* is a category:
  - Objects are elements of the poset.
  - There is a unique arrow $a \to b$ iff $a \leqslant b$.

Curious fact:

Many interesting structures are themselves particularly significant kinds of categories.

From the abstract to the concrete – tools from category theory

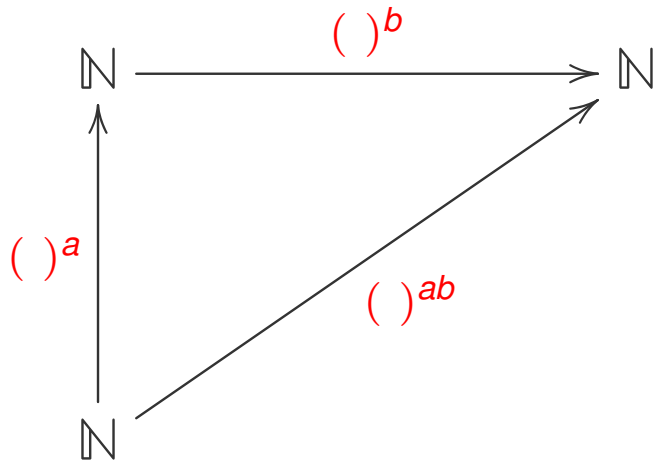
Diagrams in category theory

A **diagram** is a directed graph, whose *vertices* are labeled by *objects*, and whose *edges* are labeled by *arrows* between these objects.

Diagrams in categories

Identities and equations are traditionally expressed graphically.

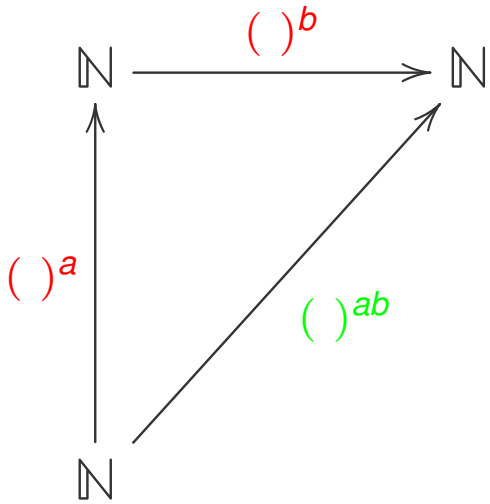
A **diagram** in the category **Set**

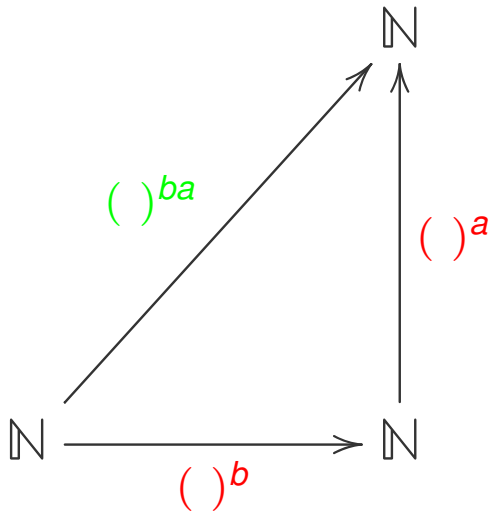


A diagram **commutes** when all paths with the same source / target describe the same arrow.

The art of diagram-chasing

Commuting diagrams can be **pasted** *along a common edge.*

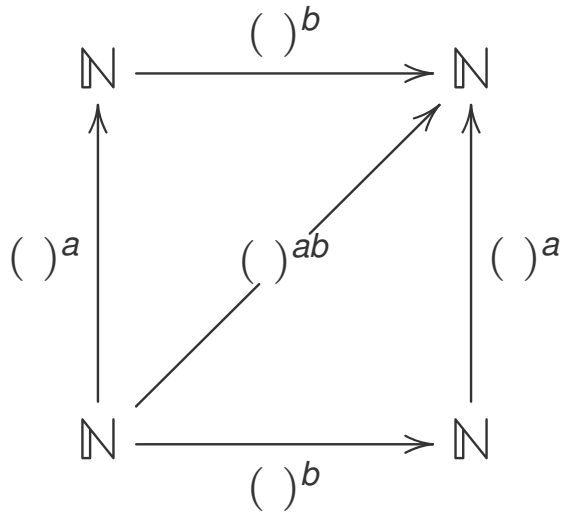




Both the above diagrams commute . . .

The art of diagram-chasing

Commuting diagrams can be **pasted** *along a common edge, to give another commuting diagram.*



Building up commuting diagrams is easy – deciding whether a given diagram commutes may be harder ... how hard?

A passing observation!

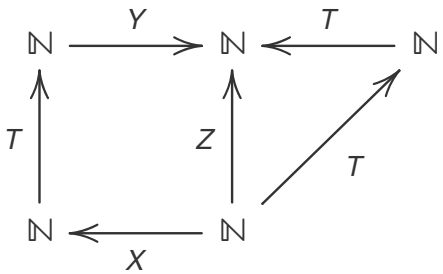
The **word problem** for a monoid is a special case of **deciding commutativity**.

Some simple arithmetic bijections ...

$$X(n) = \begin{cases} n & n \,(mod\ 2) = 0 \\ 2n-1 & n \,(mod\ 4) = 1 \\ n+2 & n \,(mod\ 8) = 3 \\ \frac{n-1}{2} & n \,(mod\ 8) = 7 \end{cases} \qquad Y(n) = \begin{cases} 2n & n \,(mod\ 4) = 0 \\ n+2 & n \,(mod\ 8) = 2 \\ \frac{n+1}{2} & n \,(mod\ 8) = 6 \\ n & n \,(mod\ 2) = 1 \end{cases}$$

$$Z(n) = \begin{cases} 4n & n \,(mod\ 2) = 0 \\ n+2 & n \,(mod\ 4) = 1 \\ \frac{n+1}{2} & n \,(mod\ 8) = 3 \\ \frac{n-3}{4} & n \,(mod\ 8) = 7 \end{cases} \qquad T(n) = \begin{cases} 2n & n \,(mod\ 2) = 0 \\ n+1 & n \,(mod\ 4) = 1 \\ \frac{n-1}{2} & n \,(mod\ 4) = 3 \end{cases}$$

This diagram commutes:



How difficult is **deciding commutativity** for **arbitrary** diagrams over $\{X, Y, Z, T\}$?

An algebraic approach to secret sharing

It is entirely natural to express the algebraic core of protocols as commuting diagrams.

Commuting Action Key Exchange (CAKE)

- A general family of key exchange (secret sharing) protocols.
- Introduced in 2004 by V. Shpilrain & G. Zapata
- Includes many interesting protocols as special cases

We will look at the monoid-theoretic version:

Example 3, Section 3 of *Combinatorial Group Theory and Public Key Cryptography* S.-Z. (2004).

CAKE – sharing protocol

Alice and Bob will come to share a secret element of a monoid $\mathcal{M}$.

1. Alice and Bob both have large **key pools** $A, B \subseteq \mathcal{M}$ that satisfy

$$ab = ba \;\; \forall \; a \in A, \;\; b \in B.$$

2. A fixed public **root element** $\gamma \in \mathcal{M}$ is chosen.
3. Alice chooses her **private key**, $(\alpha_1, \alpha_2) \in A \times A$, and publicly broadcasts $\alpha_1 \gamma \alpha_2 \in \mathcal{M}$
4. Bob chooses his **private key**,$(\beta_1, \beta_2) \in B \times B$, and publicly broadcasts $\beta_1 \gamma \beta_2 \in \mathcal{M}$.
5. Alice computes $\alpha_1 \beta_1 \gamma \beta_2 \alpha_2$ and Bob computes $\beta_1 \alpha_1 \gamma \alpha_2 \beta_2$.

By the point-wise commutativity of $A, B \subseteq \mathcal{M}$, these are equal, giving Alice and Bob's **shared secret** σ as

$$\sigma \;\; = \;\; \alpha_1 \beta_1 \gamma \beta_2 \alpha_2 \;\; = \;\; \beta_1 \alpha_1 \gamma \alpha_2 \beta_2$$

In a clearer form!

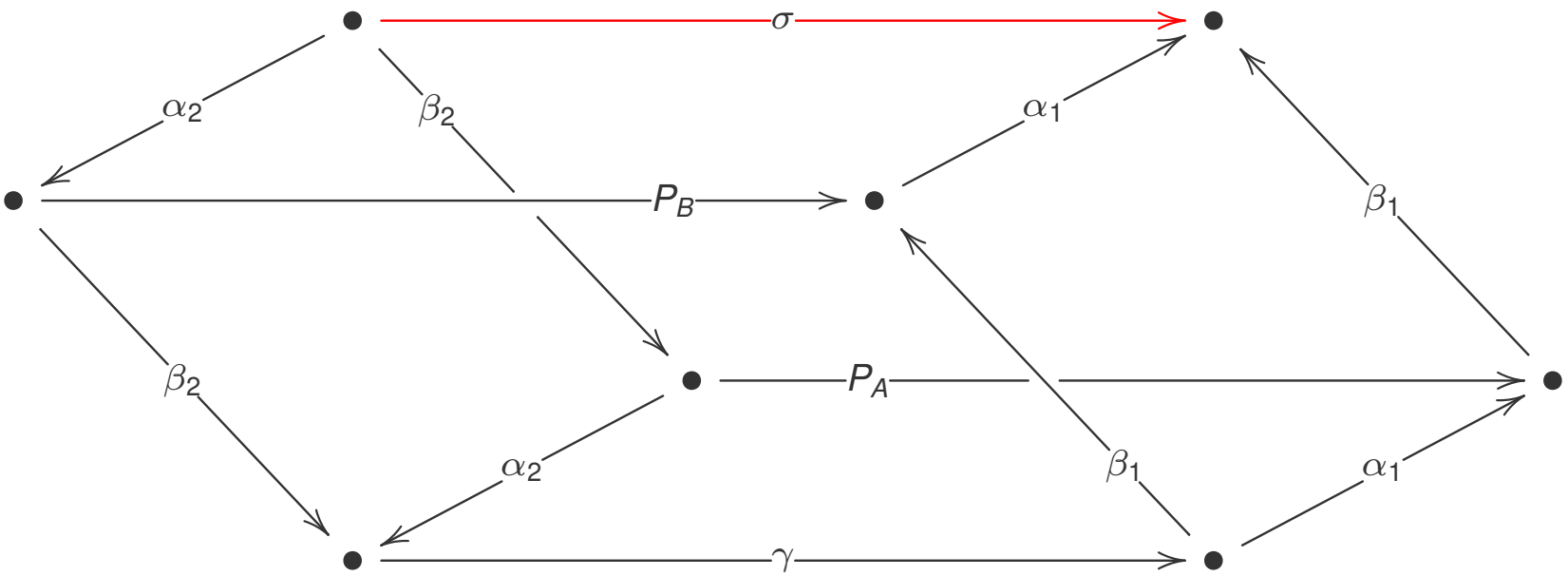
The algebraic data:

Alice	**Public**	**Bob**
	Public root γ	
Selects private $\alpha_1, \alpha_2 \in A$		Selects private $\beta_1, \beta_2 \in B$
Sends $\alpha_1 \gamma \alpha_2$	$P_A \longrightarrow$	
	$P_B \longleftarrow$	Sends $\beta_1 \gamma \beta_2$
Computes: $\alpha_1 P_B \alpha_2$	*By commutativity, these are equal.*	Computes: $\beta_1 P_A \beta_2$

CAKE as a commuting diagram over a monoid

The required arrows are:

1. The root γ
2. Alice & Bob's private keys, (α_1, α_2) and (β_1, β_2)
3. Alice & Bob's public announcements, P_A and P_B
4. Their shared secret σ



A very general technique

We may draw the algebraic core of numerous other protocols in the same manner

The usual story ...

Three participants $\{Alice, Bob, Carol\}$ will come to share a secret.

Start with a (public) prime p and **root** $g \in \mathbb{Z}_p$.

- *Alice*, *Bob*, and *Carol* have private keys $a, b, c \in \mathbb{Z}_p$.
- They will construct the shared secret $g^{abc} = g^{bca} = g^{cab}$.
- All three of them are required, to construct this.
- The usual evesdropper *Eve* can see all communication.

Tripartite Diffie-Hellman

Based on the **public root** g, and their **private keys** a, b, c,

1. Alice computes g^a and announces the result to Bob.
2. Bob computes g^b and announces the result to Carol.
3. Carol computes g^c and announces the result to Alice.

Tripartite Diffie-Hellman, Round II

Based on the messages they receive,

1. Alice computes $(g^c)^a = g^{ca}$ and announces the result to Bob.
2. Bob computes $(g^a)^b = g^{ab}$ and announces the result to Carol.
3. Carol computes $(g^b)^c = g^{bc}$ and announces the result to Alice.

Tripartite Diffie-Hellman, Round III

They are now able to compute the shared secret.

1. Alice computes $\left(g^{bc}\right)^{a} = g^{abc}$.
2. Bob computes $\left(g^{ca}\right)^{b} = g^{abc}$
3. Carol computes $\left(g^{ab}\right)^{c} = g^{abc}$.

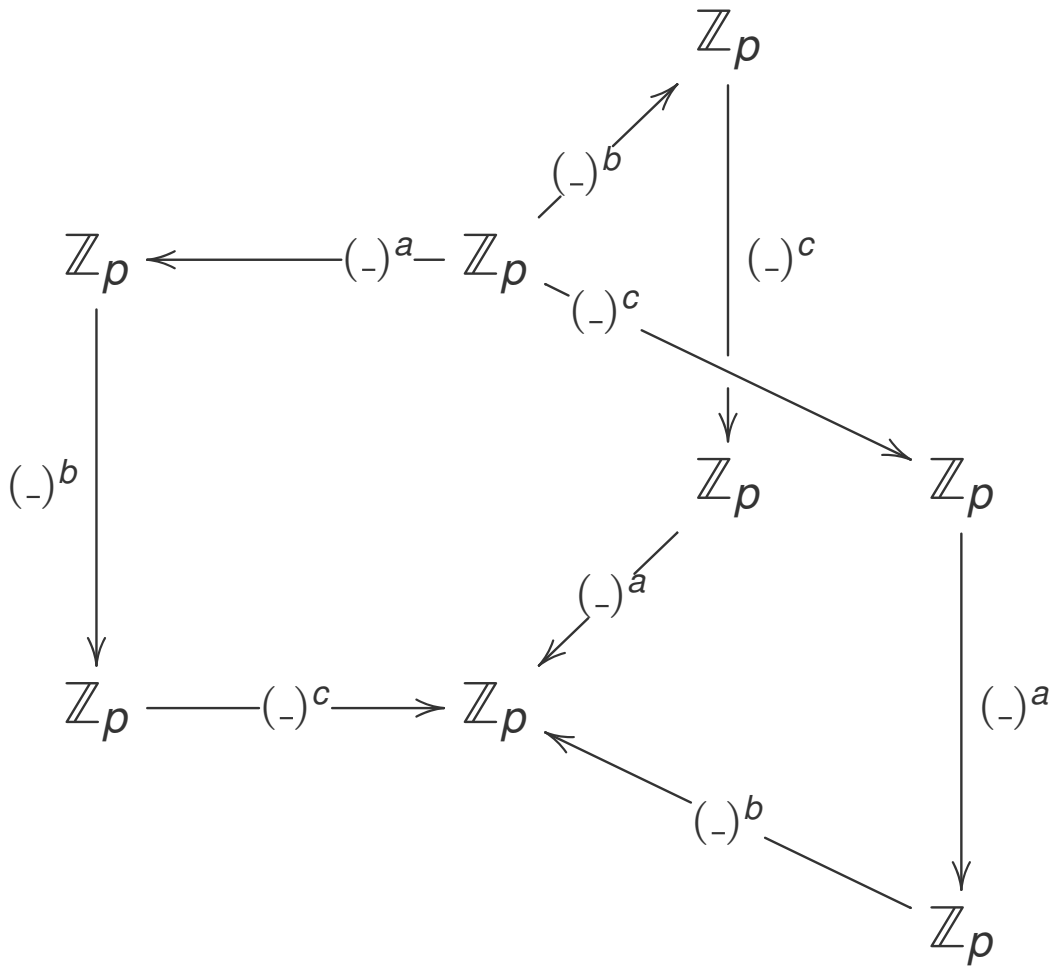
The underlying category

The action takes place in a small subcategory of **Set**:

- **Objects:** $\mathbb{Z}_p$ and $\{*\}$
- **Arrows:**
  1. *modular exponentiation* $(\ )^x : \mathbb{Z}_p \to \mathbb{Z}_p$, for all $x = 0 \ldots p-1$
  2. *selecting an element* $[x] : \{\star\} \to \mathbb{Z}_p$, where $[x](\star) = x \in \mathbb{Z}_p$

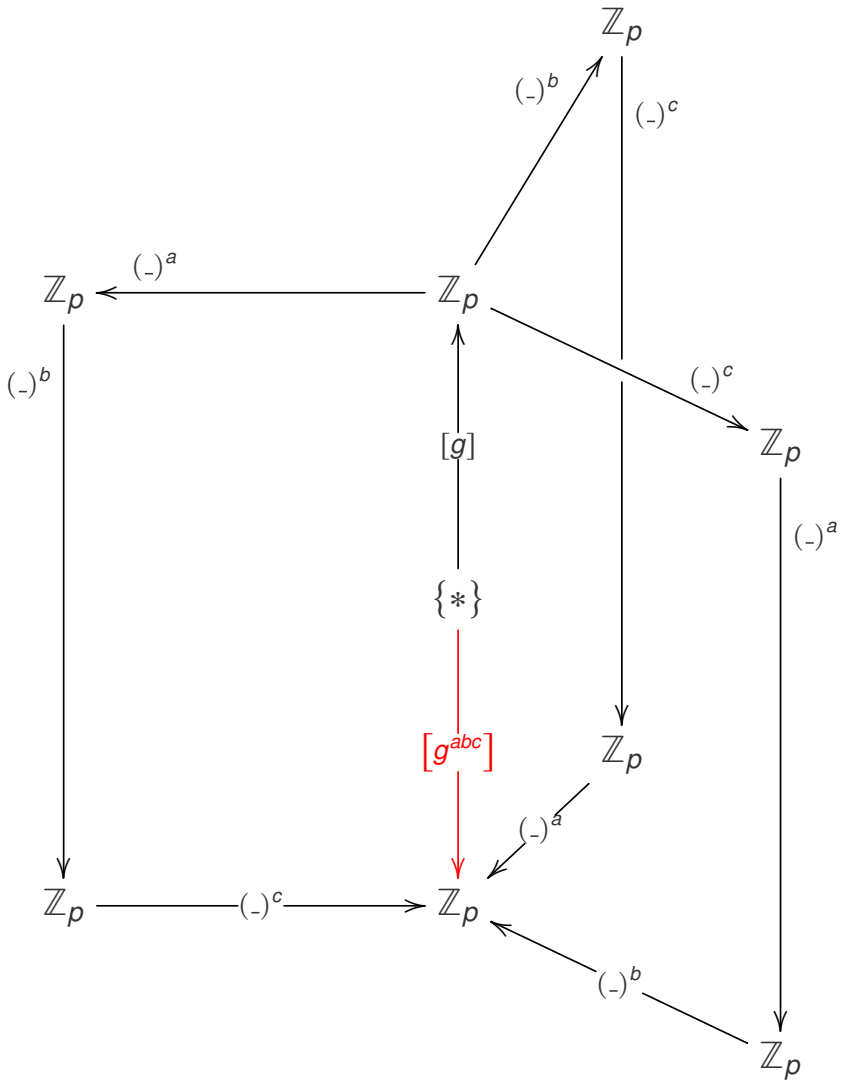
The core identity

The basic identity is $(((\_)^a)^b)^c = (((\_)^b)^c)^a = (((\_)^c)^a)^b$



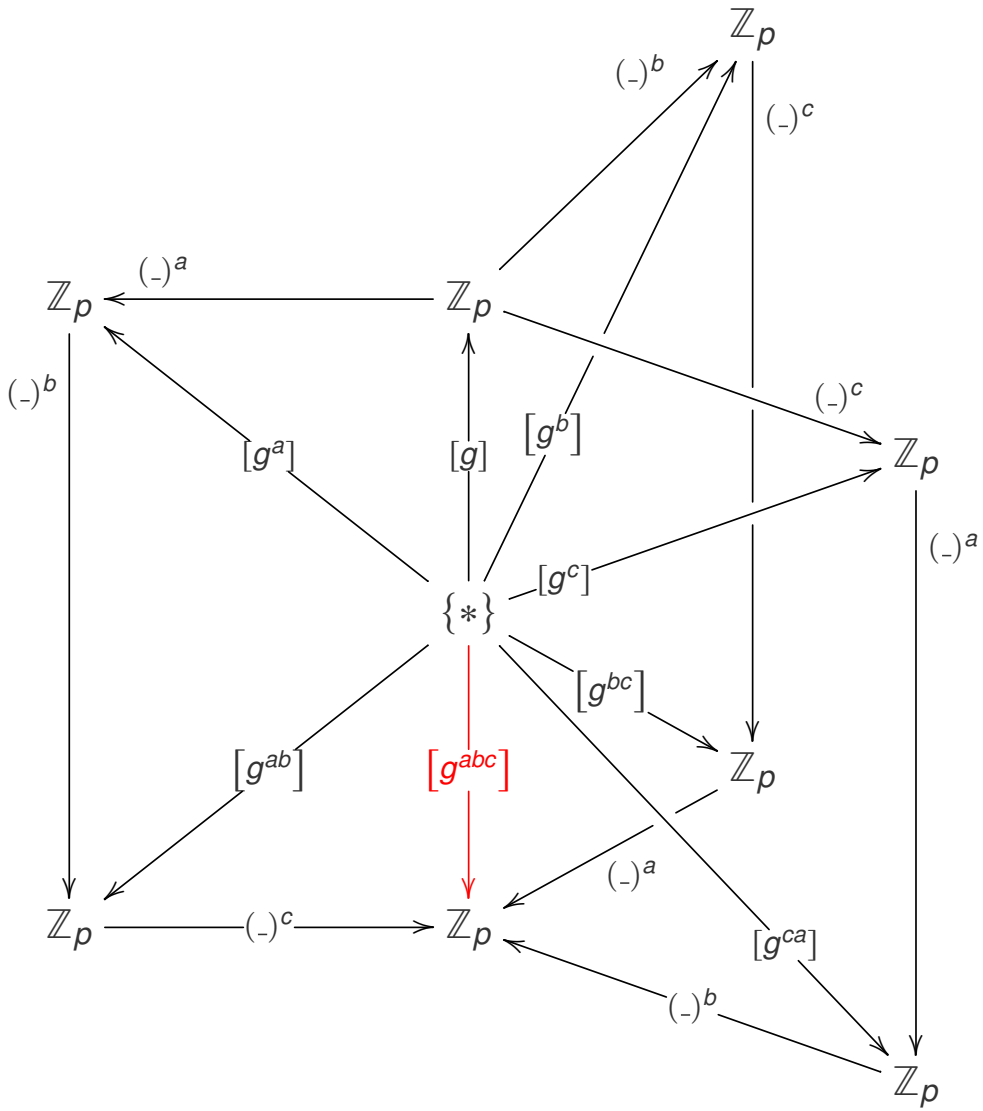
Adding in the root element

We require these equalities *applied to the root* $g \in \mathbb{Z}$.



What announcements are made?

The elements $g^a, g^b, g^c, g^{ab}, g^{bc}, g^{ca}$ are all announced:



Based on experiments(!)

With a bit of practice ...

turning algebraic identities into diagrams becomes straightforward.

Taking things further ...

Four participants (+ eavesdropper)

$$\{ \mathit{Alice}, \mathit{Bob}, \mathit{Carol}, \mathit{Dave} \} \cup \{ \mathit{Eve} \}$$

Each participant has a private key $\{ a, b, c, d \} \subseteq \mathbb{Z}_p$.

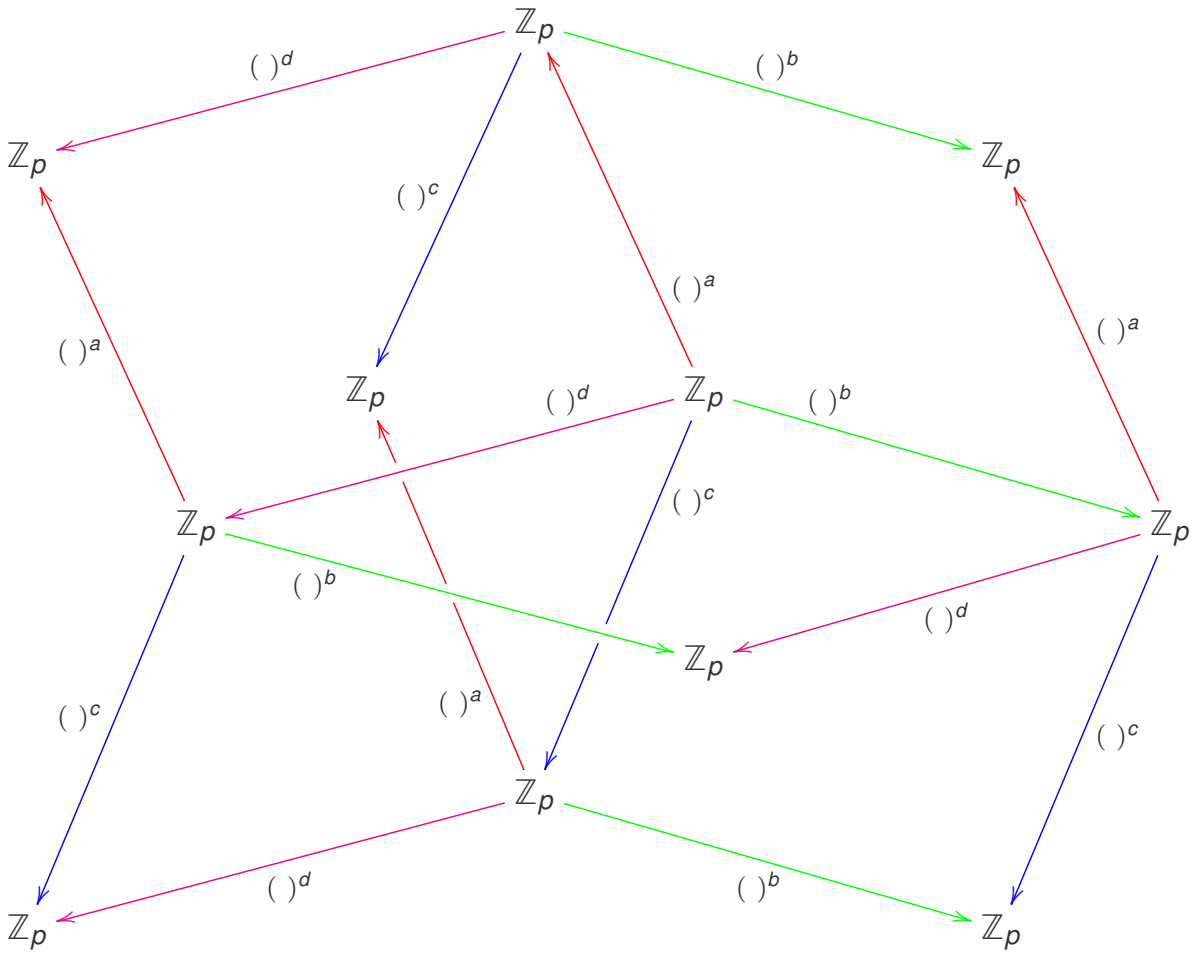
These allow them to perform their secret operations:

$$(\,)^a, (\,)^b, (\,)^c, (\,)^d : \mathbb{Z}_p \to \mathbb{Z}_p$$

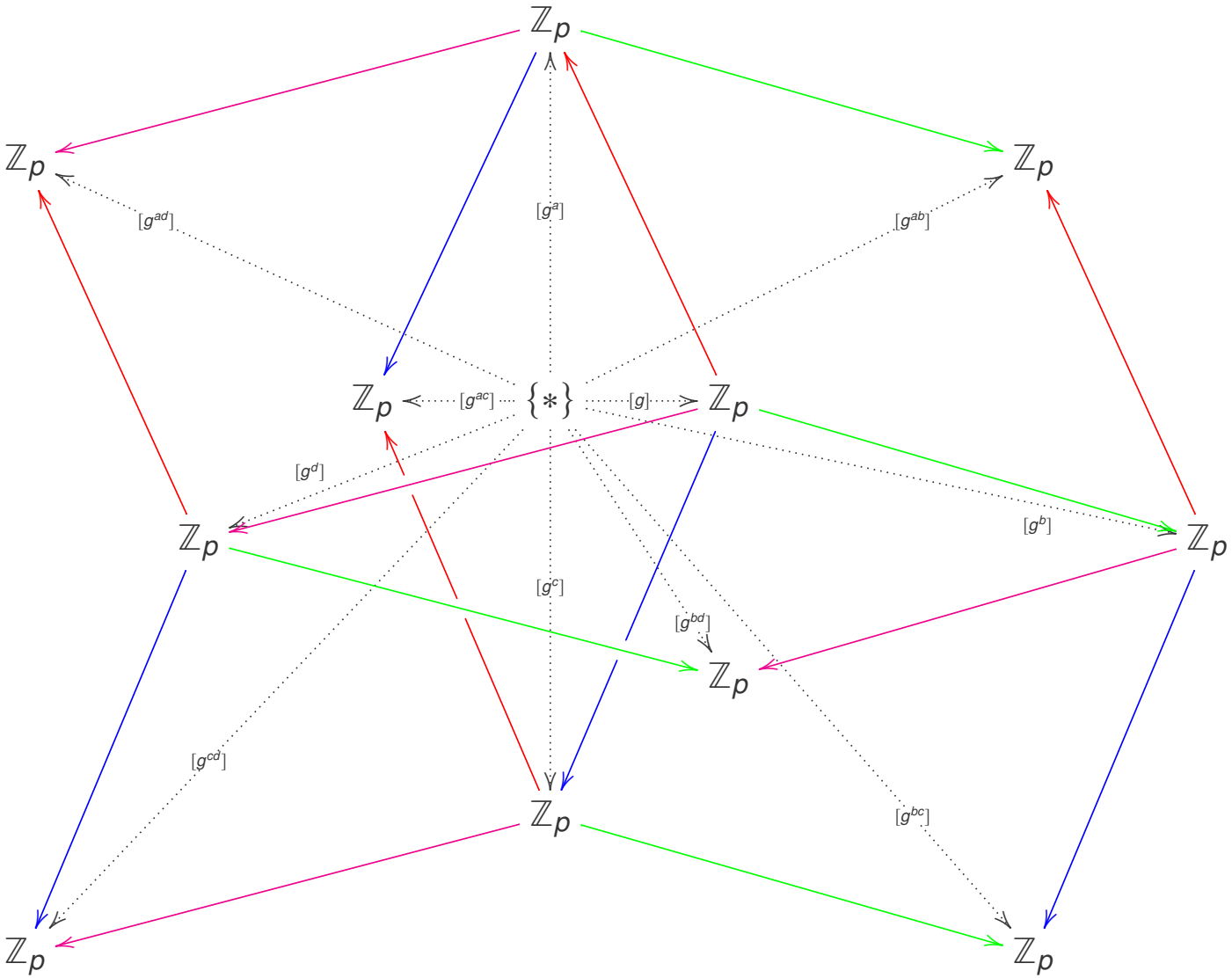
Starting from some root $g \in \mathbb{Z}_p$, each pair of participants computes a shared secret:

$$g^{ab}, g^{ac}, g^{ad}, g^{bc}, g^{bd}, g^{cd}$$

The underlying algebraic relations :



Adding in public announcements :



A very category-theoretic question :

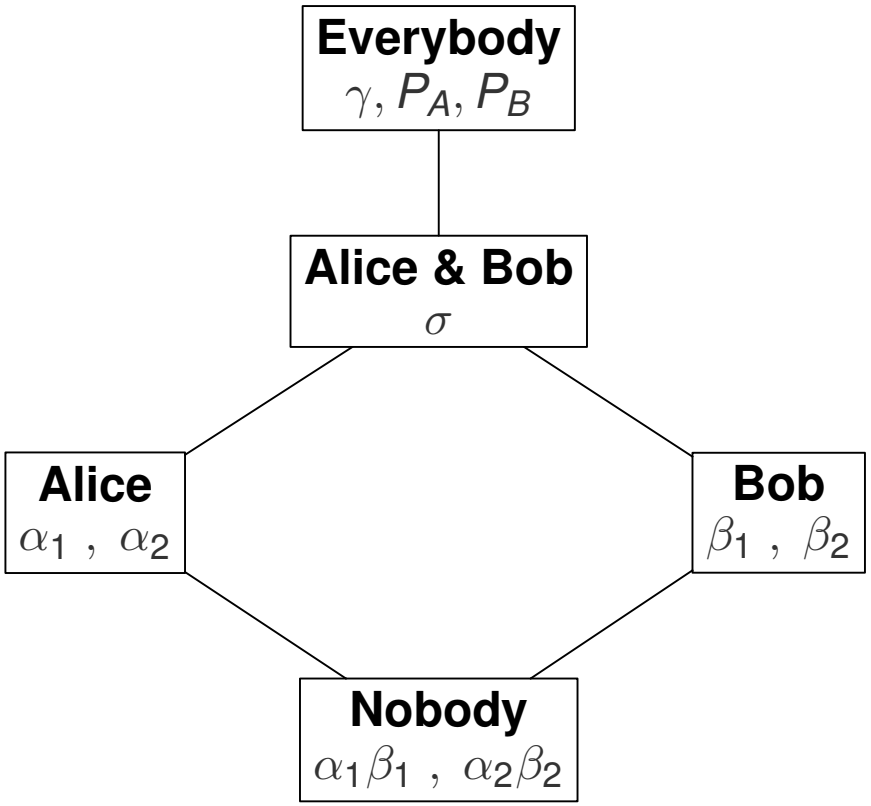
We can draw (pretty?) pictures for the algebra behind a wide range of communication protocols.

Question: Do they have anything in common
– is there any structure they *all* share?

Knowns and unknowns in semigroup CAKE

The participants: { Alice, Bob, Eve }.

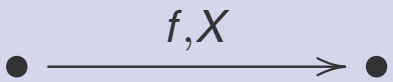
The epistemic data:



Combining algebraic & epistemic data

Introducing epistemic data to diagrams

- Form the subset-lattice of participants.
- Label each edge in the diagram by an element of this lattice:

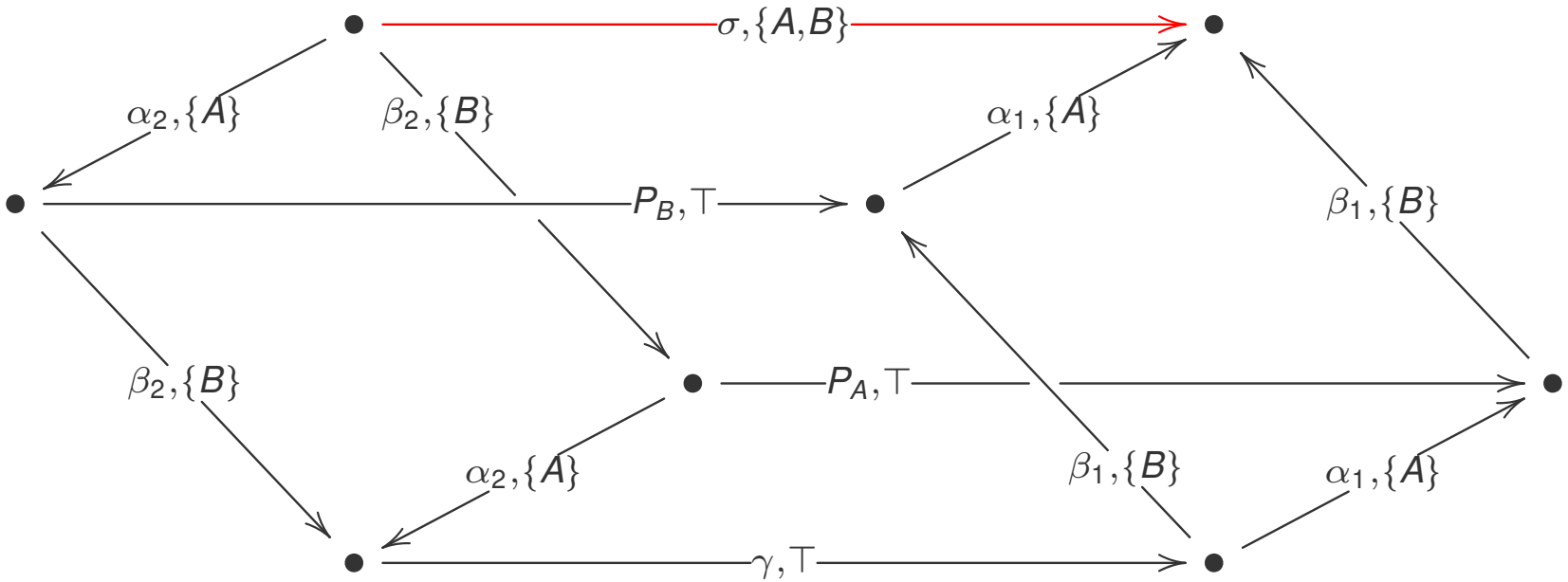


$X \subseteq \{Alice, Bob, Eve\}$ consists of participants who

  - know the value of f, or (more accurately)
  - are able to perform the operation f.

CAKE, in summary

The **Algebraic-Epistemic diagram** for semigroup-CAKE:



Commuting diagrams??

Treating $2^{\{A,B,E\}}, \cap$ as a monoid:

Question: Is this diagram for CAKE a commuting diagram over the product category $\mathcal{M} \times 2^{\{A,B,E\}}$?

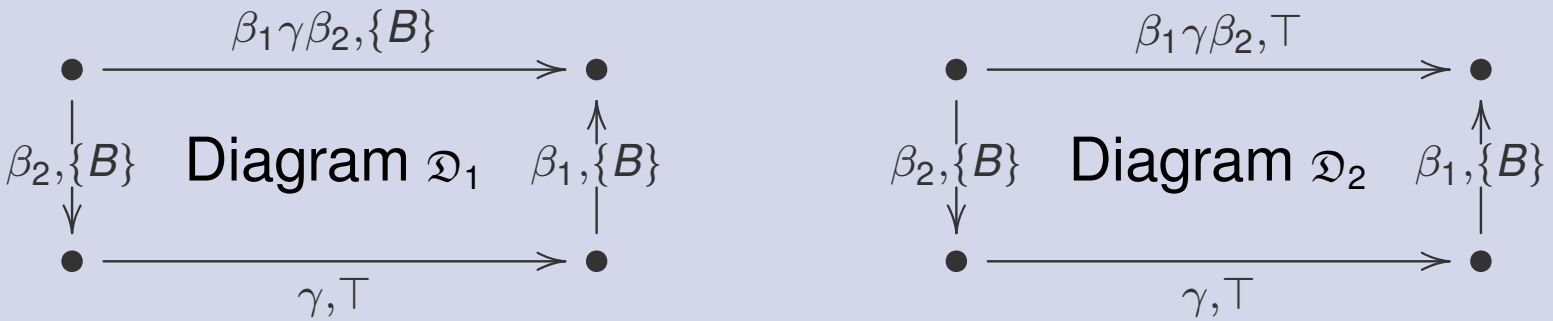
Answer: No!

Turning a bug into a feature: *The reasons why / points at which it fails to commute are highly significant.*

1. Announcements / information sharing by participants.
2. Different routes to calculating the same value.

Failure of commutativity & public announcements

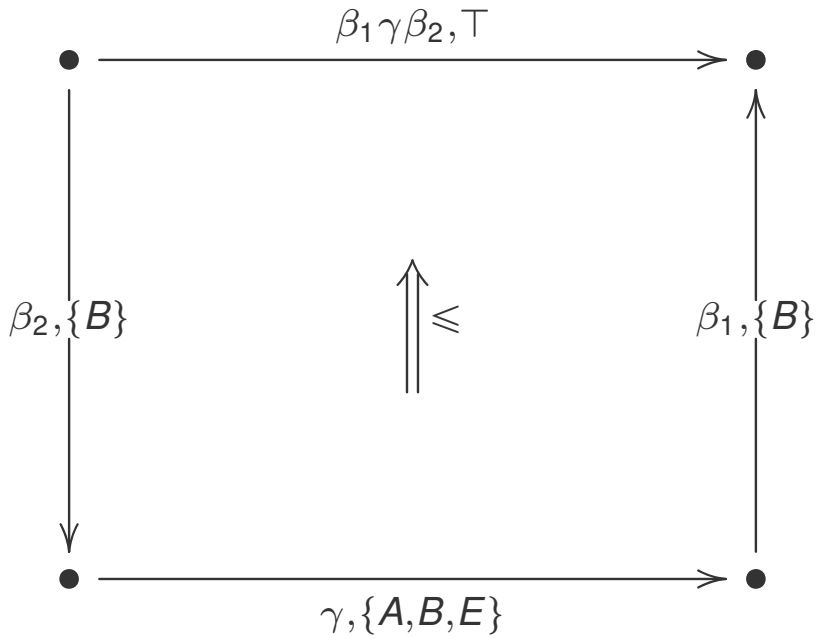
Diagram 1 commutes, Diagram 2 is a slice of CAKE.



1. In **diagram 1**, Bob computes $\beta_2\gamma\beta_1$, and *keeps quiet*.
2. In **diagram 2**, Bob computes $\beta_2\gamma\beta_1$, and *tells the whole world the result*.

Public announcements as 2-categorical data

Announcements appear as *inequalities*:

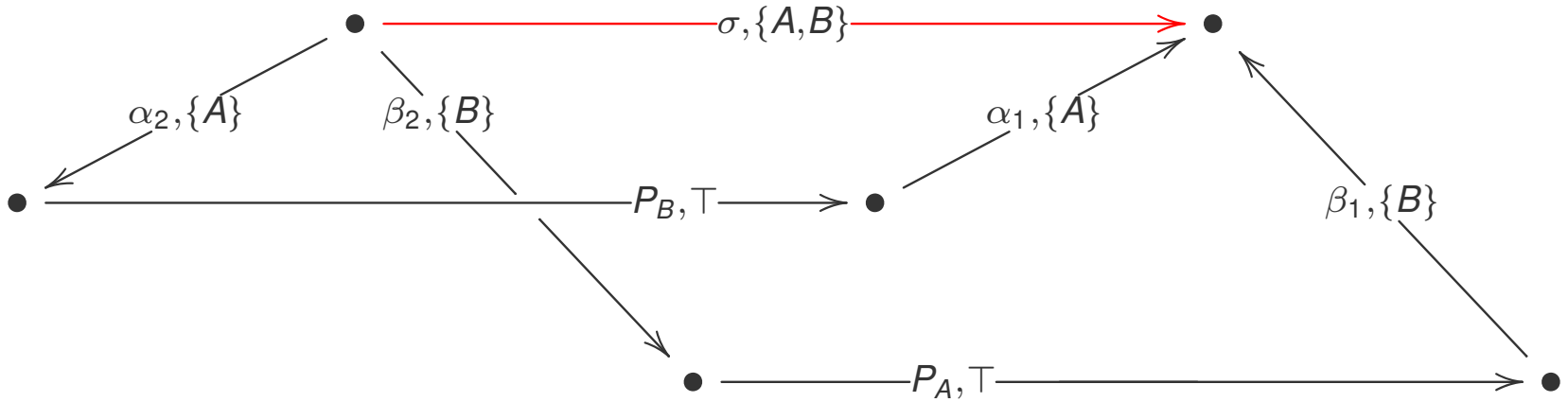


From a category-theory viewpoint ...

A **very standard** notion: 2-categories have *arrows between arrows*, drawn diagrammatically as "2-cells".

Non-trivial two-cells without public announcements

Another slice of CAKE :



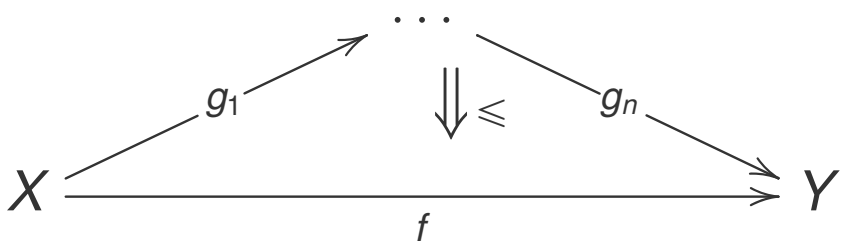
We have non-identity 2-cells, but no announcements.

Here, non-trivial 2-cells correspond to *Alice and Bob's distinct routes to calculating the shared secret*.

A simple definition ...

A diagram $\mathfrak{D}$ satisfies the **edge-path condition (EPC)** when:

Given **an edge and a path** between the nodes X and Y, we have the following 2-cell:



Algebraically,

$$g_n g_{n-1} \cdots g_1 \leqslant f$$

Interpreting the edge-path condition

We claim this as a generic ‘correctness criterion’ for protocols.

In existing protocols ...

We always find this to be the case.

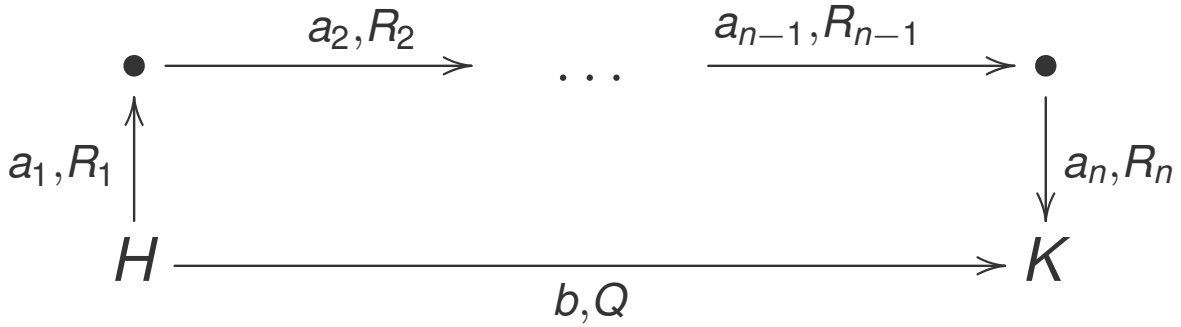
If it fails, then either:

1. We have failed to account for the results of some announcement,
2. We have missed some route to calculating a secret value,
3. There is the possibility of *deadlock*.

This is about information flow: nothing at all to do with the difficult of solving problems!

The edge-path condition: who knows what?

Consider a fragment of the A-E diagram for some protocol:



The edge-path condition states that

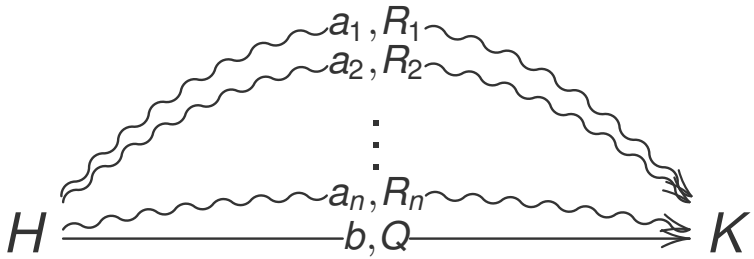
$$b = a_n \ldots a_1 \quad \text{and} \quad \bigcap_{j=1}^{n} R_j \subseteq Q$$

Quite simply:

Every individual $x \in \bigcap_{j=1}^{n} R_j$ knows every operation $\{a_j\}_{j=1..n}$ and therefore also knows their composite $a_n \ldots a_1$.

No participant left behind

Consider a fragment of an A-E diagram for some protocol with a **single edge** and **multiple paths** from node H to node K.



The edge-path condition states that $R_j \subseteq Q$ for all $j = 1..n$.

Again, a simple interpretation:

The members of $R_1, R_2, \ldots, R_n$ are all able to calculate (perform) b, albeit in different ways. Therefore, the set of participants who can perform b must contain each R_j.

A worked example

Tripartite Diffie-Hellman key exchange

The usual story ...

Three participants $\{Alice, Bob, Carol\}$ will come to share a secret.

Start with a (public) prime p and **root** $g \in \mathbb{Z}_p$.

- *Alice*, *Bob*, and *Carol* have private keys $a, b, c \in \mathbb{Z}_p$.
- They will construct the shared secret $g^{abc} = g^{bca} = g^{cab}$.
- All three of them are required, to construct this.
- The usual evesdropper *Eve* can see all communication.

Tripartite Diffie-Hellman, Round I

Based on the **public root** g, and their **private keys** a, b, c,

1. Alice computes g^a and announces the result to Bob.
2. Bob computes g^b and announces the result to Carol.
3. Carol computes g^c and announces the result to Alice.

Tripartite Diffie-Hellman, Round II

Based on the messages they receive,

1. Alice computes $(g^c)^a = g^{ca}$ and announces the result to Bob.
2. Bob computes $(g^a)^b = g^{ab}$ and announces the result to Carol.
3. Carol computes $(g^b)^c = g^{bc}$ and announces the result to Alice.

Tripartite Diffie-Hellman, Round III

They are now able to compute the shared secret.

1. Alice computes $\left(g^{bc}\right)^{a} = g^{abc}$.
2. Bob computes $\left(g^{ca}\right)^{b} = g^{abc}$
3. Carol computes $\left(g^{ab}\right)^{c} = g^{abc}$.

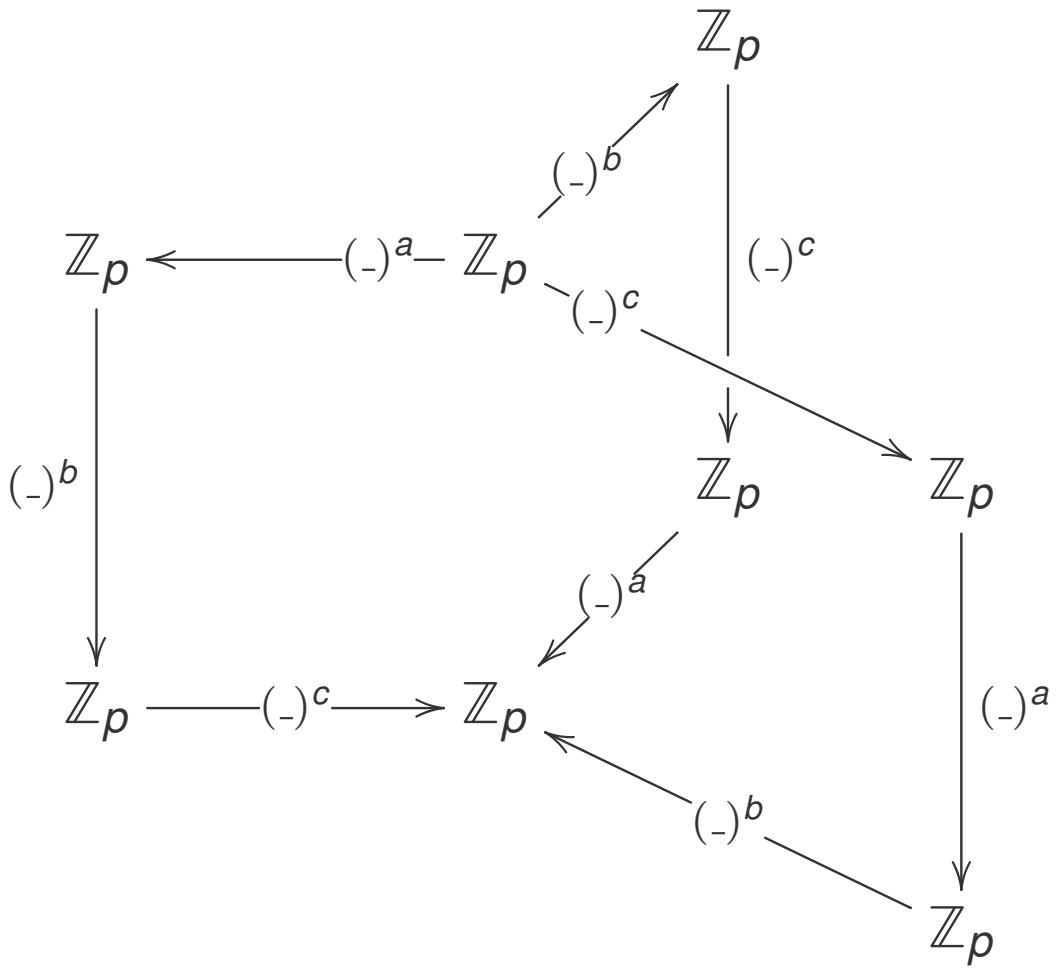
The underlying category

The action takes place in a small subcategory of **Set**:

- **Objects:** $\mathbb{Z}_p$ and $\{*\}$
- **Arrows:**
  1. *modular exponentiation* $(\ )^x : \mathbb{Z}_p \to \mathbb{Z}_p$, for all $x = 0 \ldots p-1$
  2. *selecting an element* $[x] : \{\star\} \to \mathbb{Z}_p$, where $[x](\star) = x \in \mathbb{Z}_p$

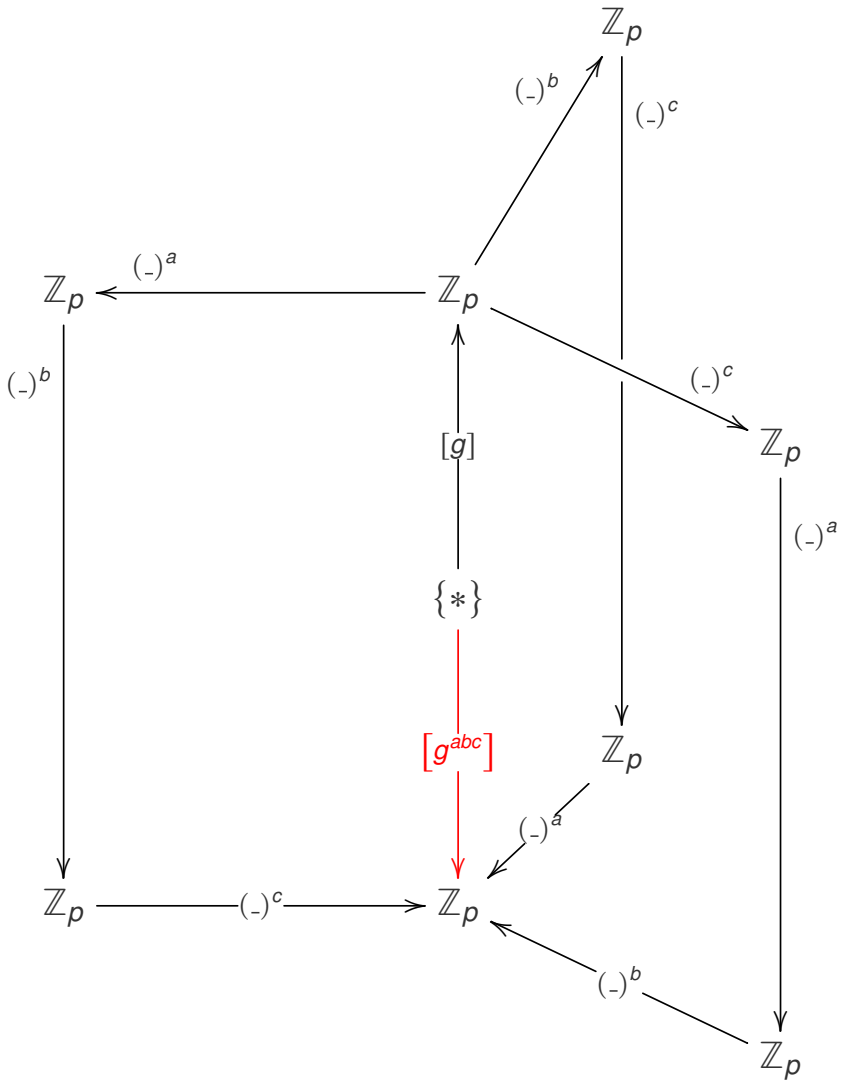
The core identity

The basic identity is $(((\_)^a)^b)^c = (((\_)^b)^c)^a = (((\_)^c)^a)^b$



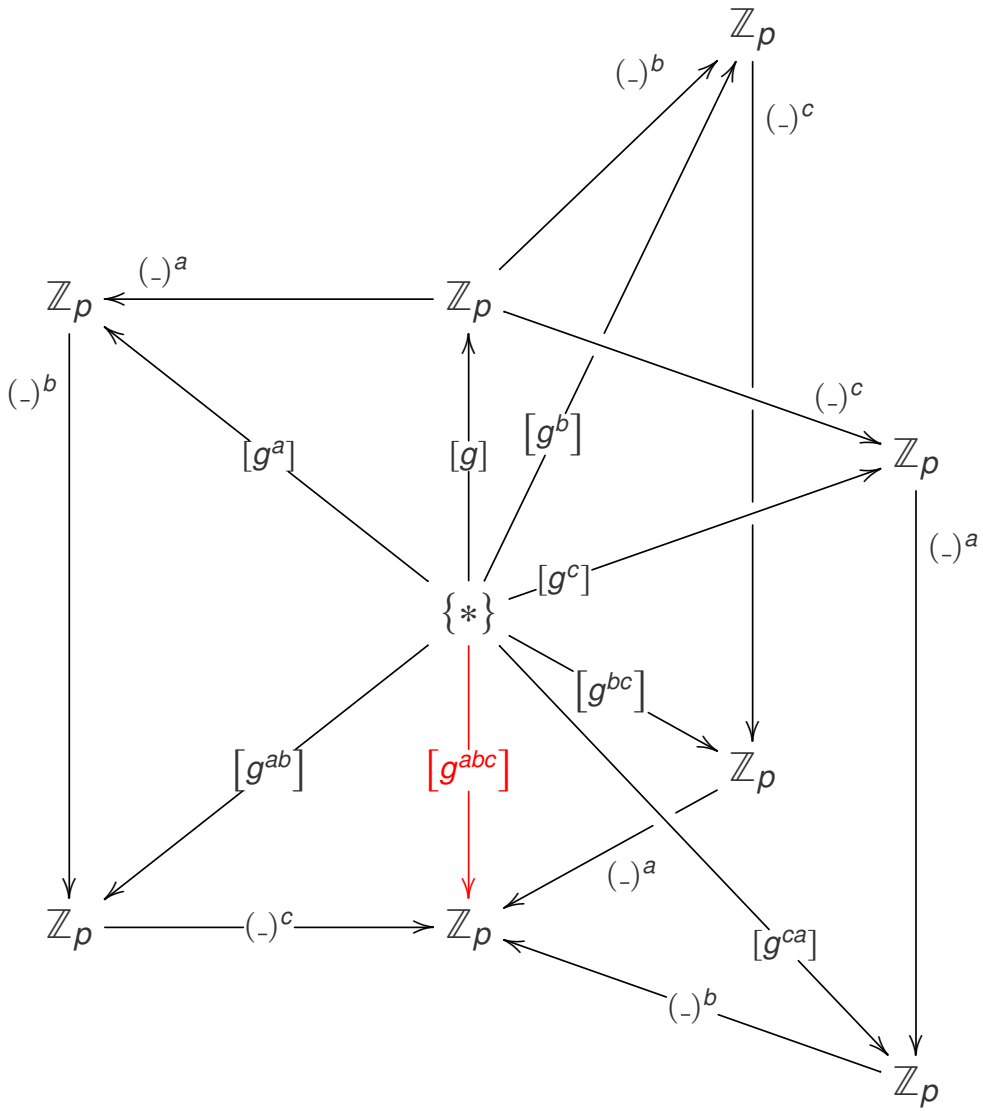
Adding in the root element

We require these equalities *applied to the root* $g \in \mathbb{Z}$.



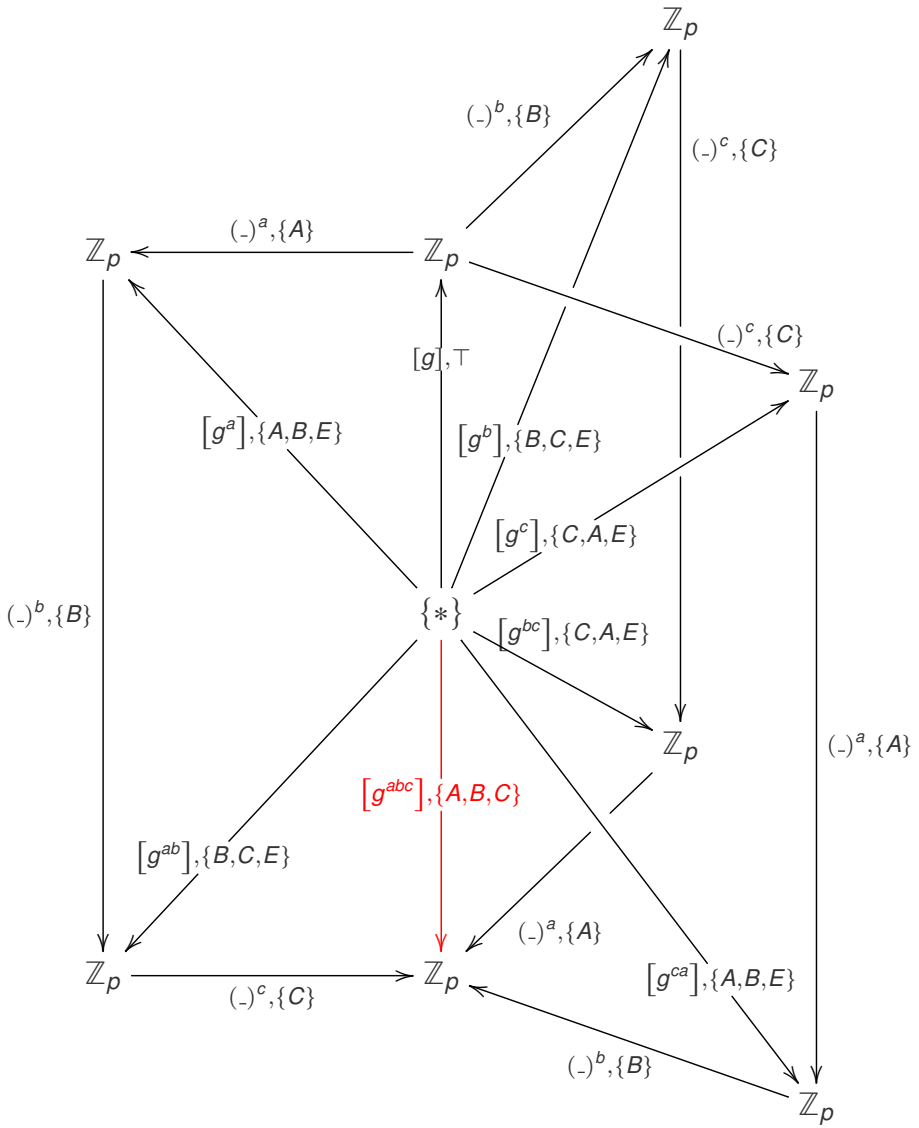
What announcements are made?

The elements $g^a, g^b, g^c, g^{ab}, g^{bc}, g^{ca}$ are all announced:



Who knows what?

Adding in the epistemic data:



Does this help??

Simple diagram-chasing makes it easy to answer some questions:

Question Can we vary the order of computations / announcements?

Answer Yes, quite a bit!

Question Does it matter if any of the participants (apart from Eve) are evesdropping?

Answer No, not at all!

Question What does Eve need to know, to find the shared secret?

Answer *Any of the private keys will do*!

We can also ***compare approaches*** to the same problem.

Another approach ...

How else may *Alice*, *Bob*, and *Carol* communicate privately?

As before, assume:

- Prime p,
- Public Root $g \in \mathbb{Z}_p$
- Private keys $a, b, c \in \mathbb{Z}_p$

Every pair will compute a *distinct* shared secret.

$$\textit{Alice} - - \textit{Bob} \quad \textit{Bob} - - \textit{Carol} \quad \textit{Carol} - - \textit{Alice}$$

Pairwise three-party Diffie-Hellman

- *Alice*, *Bob*, and *Carol* compute

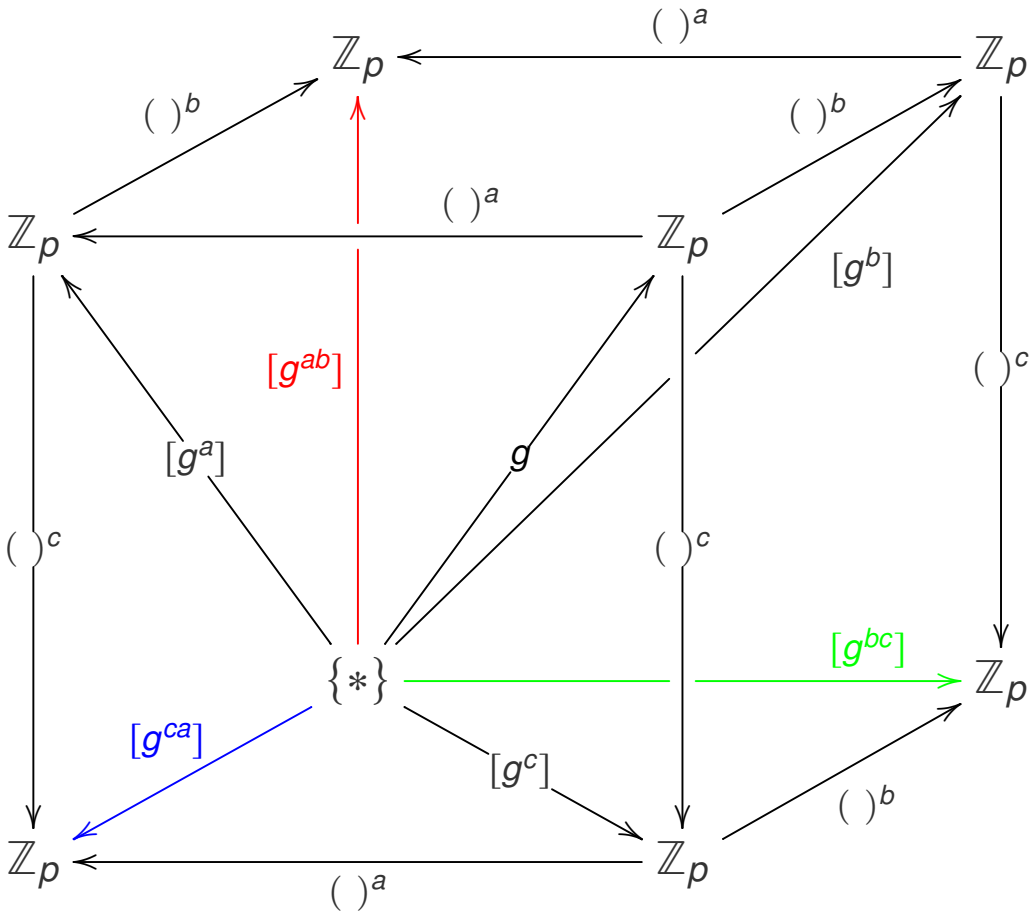
$$g^a \quad \text{and} \quad g^b \quad \text{and} \quad g^c$$

  respectively. They publicly announce their results.
- They each compute a *pair* of shared secrets:

Alice	computes	g^{ba} and g^{ca}
Bob	computes	g^{cb} and g^{ab}
Carol	computes	g^{ac} and g^{bc}

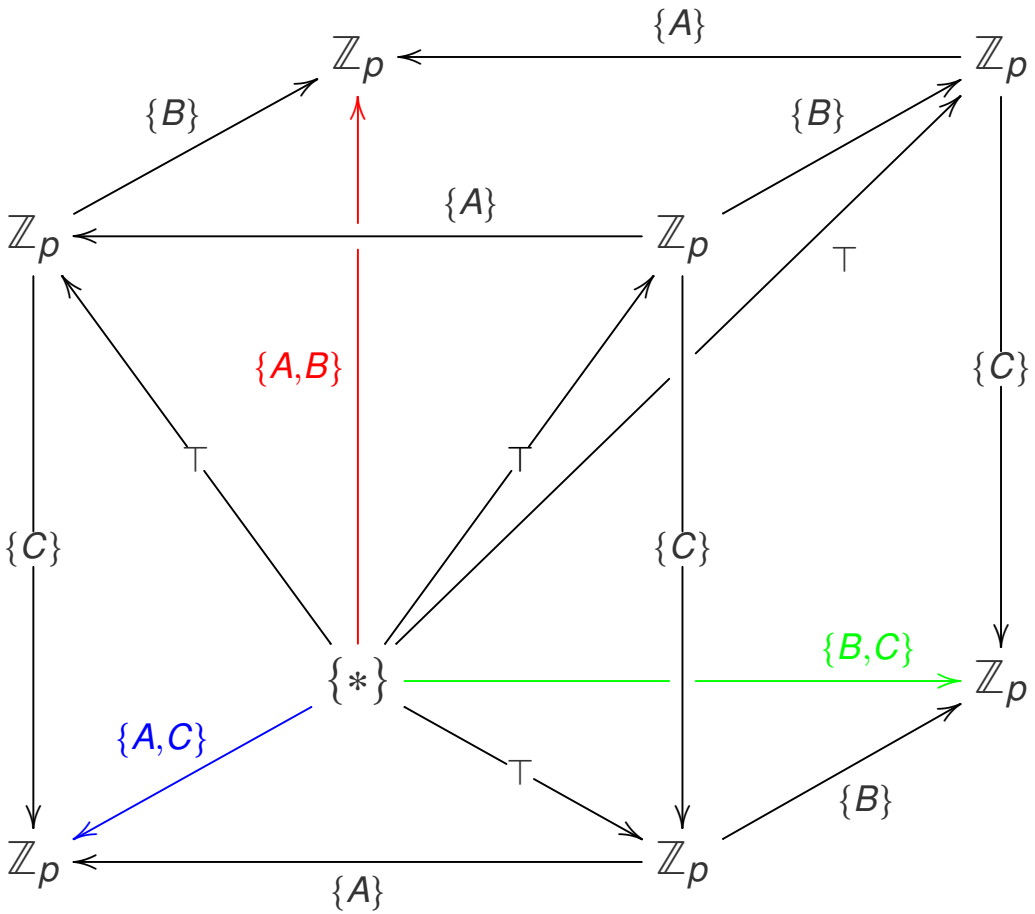
A-E diagram for 3-way secret sharing

The (commuting) algebraic labelling:



A-E diagram for 3-way secret sharing

The (EPC satisfying) lattice labelling:



Comparing this approach ...

Again, by simple diagram-chasing:

Question Can any additional information be announced?

Answer No, not without compromising the protocol!

Question What happens if Eve discovers (say) Bob's secret key?

Answer She can discover two out of the three shared secrets.

Question Is this the same as tripartite Diffie-Hellman?

Answer *No, definitely not!*

Can we go further??

Drawing diagrams gives a *visual representation* of algebraic relationships, epistemic knowledge, and information flow.

We can use 'diagram-chasing' techniques to answer questions about information flow.

This is using **tools from category theory** rather than **category theory itself**.

Back to CAKE

Recall the CAKE protocol

This is a *general recipe* for producing public key protocols.

Security depends entirely on the *choice of monoid*.

In fact, any structure with an associative composition will do.

We could use a more general category!

An interesting first choice ...

CAKE was first proposed in:

Combinatorial group theory and public key cryptography (2004)

General proposals for cryptosystems based on algebraic structures.

A concrete protocol was given in:

Thompson's group and Public Key Cryptography (2004)

The underlying structure was Thompson's group $\mathcal{F}$.

Defining Thompson's $\mathcal{F}$

Thompson's group was originally given as a group of piece-wise linear maps on $[0, 1]$.

It is well-known as:

1. A counterexample to conjectures
2. A key player in unresolved problems in group theory.

The 'standard infinite' group presentation:

$$\mathcal{F} = \langle x_0, x_1, x_2, \ldots \; : \; x_i^{-1} x_j x_i = x_{j+1} \; \forall \; i < j \rangle$$

The elements $\{x_0, x_1\}$ generate the whole group, but the required relators are then more complex.

Any particular reasons?

From TFA

"This group has several properties that make it *particularly fit for cryptographic purposes*."

- No non-abelian quotients.
- 'almost-linear' word problem.
- " ... resembles the **factorization problem** at the heart of the R.S.A. cryptosystem."

A practical reason ...

Group-based cryptosystems are susceptible

to **length-based cryptanalysis** *(— pioneered by Shamir).*

This works best with groups that are

'close to being free' – **Folklore**

Thompson's group $\mathcal{F}$ is *'as far from free as possible'*.

Any additional relators cause a collapse to an abelian group.

This is an ex-protocol

This Folklore is incorrect:

- The S-U Protocol for Thompson's Group F is always breakable **Matucci** (2006)
- Length-based cryptanalysis: the case of Thompson's group **Ruinsky, Shamir, Tsaban** (2007)

  "We conjecture that any protocol based on $\mathcal{F}$ is likely to be insecure."

Can this really have anything to do with category theory ??

Back to basics ...

Some simple, yet fundamental category theory

Important operations on categories

We often consider categories with **extra structure**.
A fundamental one is a **tensor**:

$$\_ \otimes \_ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$

This acts as:

$$A \xrightarrow{\quad f \quad} B$$

$$X \xrightarrow{\quad g \quad} Y$$

Important operations on categories

We often consider categories with **extra structure**.
A fundamental one is a **tensor**:

$$\_ \otimes \_ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$$

This acts as:

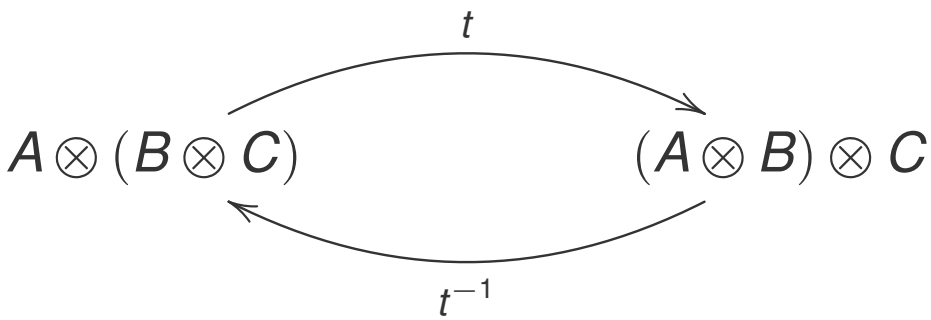
$$A \otimes X \xrightarrow{f \otimes g} B \otimes Y$$

Examples again ...

- **Cartesian product** of Sets / functions
- **Tensor product** of Vector spaces / linear maps
- **Disjoint union** of Sets / relations
- **Tensor product** of Abelian groups / homomorphisms
- **Direct sum** of Hilbert spaces / bounded linear maps
- **...**

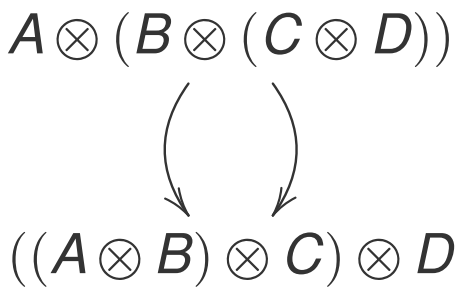
Any axioms ?

- **Associativity** up to isomorphism



- A **coherence condition**

  The two ways of re-arranging four objects



  are the same.

Bad news for LISP programmers ...

A significant special case ...

It is easier to work with **strict associativity**

$$A \otimes B \otimes C \xleftarrow{1_{X \otimes Y \otimes Z}} A \otimes B \otimes C$$

Probably the most famous theorem in category theory (1970)

MacLane's (coherence) Theorem: Every category with a tensor is equivalent[1] to one with a strict tensor.

[1] The precise meaning of 'equivalent' is *very subtle.*

That which is canonical (!)

Two notions that are **core** to

- MacLane's theorem
- Coherence
- Foundations of category theory

A canonical arrow:

An arrow built up using *identities*, *associators*, and *the tensor*.

A canonical diagram:

A diagram where every arrow is canonical.

Two pieces of folklore ...

Folklore (Computer Scientists ...)

All canonical diagrams commute

Folklore (Mathematicians ...)

Categories where not all all canonical diagrams commute may exist, but are pathological, and to be avoided.

Slightly more recently ...

Another result on coherence & associativity:

Journal of Homotopy PMH (2016)

A tensor on a monoid is **strictly associative**

if and only if

it is **degenerate**.

"Degenerate" $\Longrightarrow$ the monoid is abelian, and tensor & composition are the same operation.

An interesting observation ...

The homology of Thompson's group $\mathcal{F}$ — K. Brown (2006)

There exists an injective group homomorphism

$$\mu : \mathcal{F} \times \mathcal{F} \to \mathcal{F}$$

that is associative up to a fixed element $x_0 \in \mathcal{F}$.

Perhaps unsurprisingly ...

This operation is a categorical tensor.

The same operation occurs as:

Inverse semigroup theory (PMH, M.V. Lawson 1998)

Pure category theory (PMH 2000)

Formal logic (J-Y Girard 1989)

Perhaps more surprisingly ...

In any monoid with a (non-degenerate) tensor

- The canonical arrows form a group.
- This group is *always* Thompson's $\mathcal{F}$.
- The generators of the standard infinitary presentation are:

$$t\ ,\ 1 \otimes t\ ,\ 1 \otimes (1 \otimes t)\ ,\ 1 \otimes (1 \otimes (1 \otimes t))\ ,\ \ldots$$

We may describe $\mathcal{F}$ as:

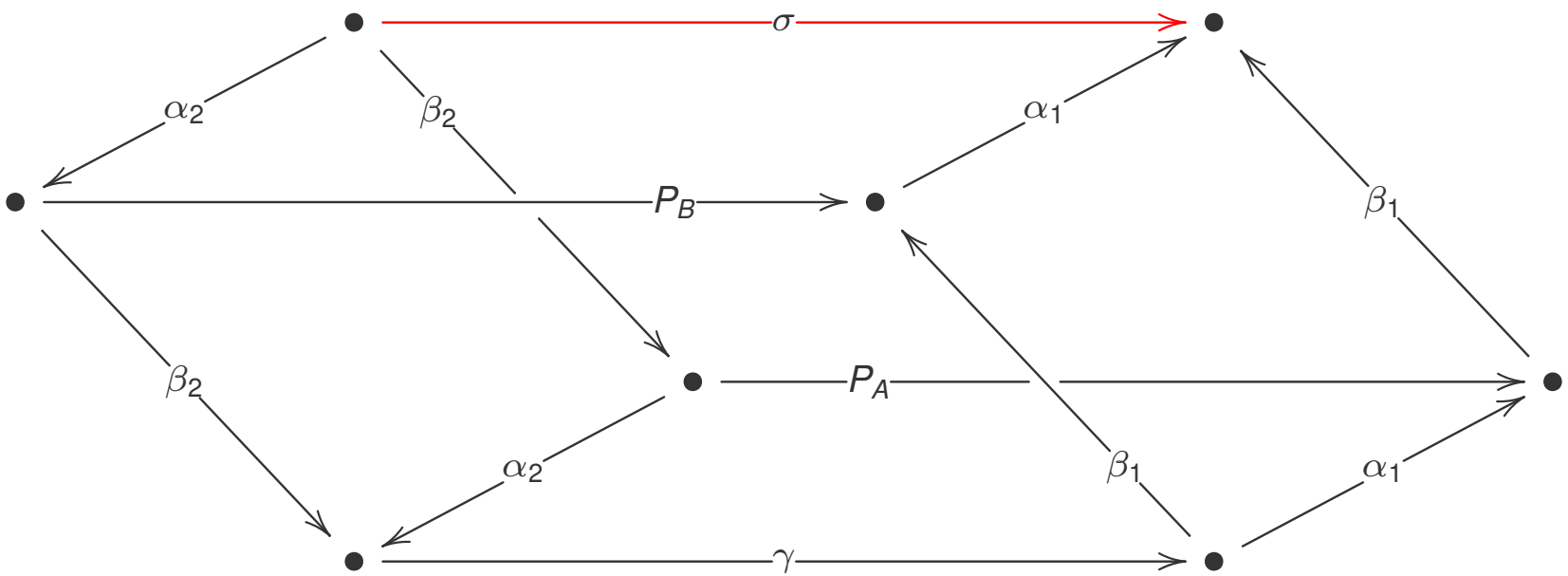
The free monogenic monoid-with-tensor.

Some prehistory ...

- **R. McKenzie, R. Thompson** (1971): Close connection between Thompson's group $\mathcal{F}$, and associativity laws
- **PMH, MVL** (1998) A class of associativity isomorphisms via inverse semigroup theory.
- **M. V. Lawson** (2004) These associativity isomorphisms form a copy of $\mathcal{F}$.
- **P. Dehornoy** (2005) 'The only [non-trivial] relations in this presentation of $\mathcal{F}$ correspond to the well-known MacLane-Stasheff pentagon.'
- **M. Brinn** (2005) 'the resemblance of the usual coherence theorems with Thompson's group $\mathcal{F}$'.
- **M. Fiore, T. Leinster** (2010) Thompson's group $\mathcal{F}$ is the symmetry group of an idempotent U in the free strict monoidal category generated by U.

In terms of protocols

The Shpilrain-Ushakov protocol is a *commuting canonical diagram*



Transplanting ideas between fields

What do we get, for free?

Simple consequences (I)

Thompson's $\mathcal{F}$ has no non-abelian quotients

Identifying distinct associators

$\equiv$

defining a strictly associative tensor.

(The allegedly desirable property for CAKE).

Simple consequences (II)

Numerous self-embedding properties

The self-embeddings:

$$\mathcal{F} \hookrightarrow 1 \otimes \mathcal{F} \quad , \quad \mathcal{F} \hookrightarrow \mathcal{F} \otimes 1$$

can be iterated (and bracketing matters!)

This gives a method of building, & perhaps characterising, *large commuting subsets*.

(As needed for Alice & Bob's key pools).

Simple consequences (III)

A decision procedure for commutativity of diagrams

Commutativity of canonical diagrams can be decided in linear time, using *Robinson's unification algorithm*.

A very special case being the word problem for $\mathcal{F}$.

Simple consequences (IV)

An infinite family of arithmetic representations of $\mathcal{F}$

Every partition of $\mathbb{N}$ into two infinite subsets determines a distinct tensor on the symmetric group of $\mathbb{N}$. (PMH 1998)

This gives various modular arithmetic representations of $\mathcal{F}$.

One example among (uncountably) many:

Let us divide $\mathbb{N}$ into the **even** and **odd** subsets: $\mathbb{N} = 2\mathbb{N} \cup 2\mathbb{N} + 1$.

Simple consequences (IV) cont.d

We have a tensor:

$$(f \otimes g)(n) = \begin{cases} 2.f\left(\frac{n}{2}\right) & n \text{ even}, \\ 2.g\left(\frac{n-1}{2}\right) + 1 & n \text{ odd}. \end{cases}$$

The associator t, together with $1 \otimes t$, generates a copy of $\mathbb{F}$.

Recall our simple arithmetic functions ...
$t(n) = \begin{cases} 2n & n\,(mod\ 2) = 0 \\ n+1 & n\,(mod\ 4) = 1 \\ \frac{n-1}{2} & n\,(mod\ 4) = 3 \end{cases}$ $\quad (1 \otimes t)(n) = \begin{cases} n & n\,(mod\ 2) = 0 \\ 2n-1 & n\,(mod\ 4) = 1 \\ n+2 & n\,(mod\ 8) = 3 \\ \frac{n-1}{2} & n\,(mod\ 8) = 7 \end{cases}$
Deciding commutativity of a diagram over these primitives is a linear-time task

More generally, we can partition $\mathbb{N}$ as $\{n\,(mod\ p) = q\}$ and $\{n\,(mod\ p) \neq q\}$

Simple consequences (V)

Using **identical** category theory, in a different setting:

Another infinite family of arithmetic representations of $\mathcal{F}$

Every bijection $\Psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ determines a distinct tensor on the symmetric group of $\mathbb{N}$. (PMH 1998)

These are slightly more complex:

$$\Psi(x, y) = 2^{x+1}y + 2^x - 1$$

We still derive families of arithmetic representations of $\mathcal{F}$.

Fortunately(!) none of these, contrary to Shpilrain-Ushakov, seem related to R.S.A.

We can say a lot about a dead protocol ...

Is there any *current* point to studying category theory?

From the large to the small ... (I)

Considering important properties of **large categories**,

in the setting of **small categories** (monoids, &c):

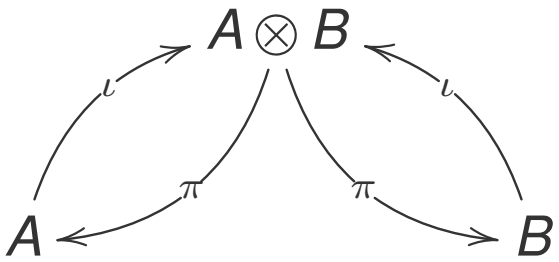
- Canonical arrows for symmetric tensors:

$$A \otimes (B \otimes C) \;\cong\; (A \otimes B) \otimes C \;\text{ and }\; A \otimes B \;\cong\; B \otimes A$$

- Thompson's group $\mathcal{V}$ (M. Fiore, M. Campos 2013)

From the large to the small ... (II)

- Canonical arrows for projections / inclusions:



- Nivat & Perrot's polycyclic monoids (PMH 2001)

From the large to the small ... (III)

- Canonical arrows for Cartesian Closure (currying of functions on sets):

$$Arrows(X \times Y \to Z) \equiv Arrows(X \to Arrows(Y \to Z))$$

- Untyped lambda calculus & hence

  universal computability (Lambek & Scott 1986)

From the large to the small ... (IV)

- Canonical arrows for associativity, commutativity & fixed points:

$$X \otimes Y \cong Y \otimes X$$

$$X \otimes (Y \otimes Z) \cong (X \otimes Y) \otimes Z$$

$$X \otimes R_X \cong R_X$$

$$L_X \otimes X \cong L_X$$

- The *mapping group* $\mathfrak{M}_{\mathcal{C}}$ of homeomorphisms on Cantor space.
- Restrictions of these (e.g. commutativity & fixed points only ...)

  — many interesting structures, e.g. Grigorchuk's group $\mathfrak{G}$.

From the large to the small ... (V)

- Canonical arrows for distributivity:

$$X \otimes (Y \oplus Z) \cong (X \otimes Y) \oplus (X \otimes Z)$$

- This is the difficult one!
- Known to have connections to Shor's QM factorisation algorithm:

  "Quantum speed-up & categorical distributivity" – (PMH 2013)

- No single explicit algebraic description.
- Done *implicitly* in J.-Y. Girard's logical models (1989,1992)

  — unfortunately, the jump from implicit to explicit is rather large!

What we really really want ...

We need a *systematic method* of moving from:

theories of ‘coherence’ for large categories

all the way down to

what these look like as *single* algebraic structures.

Volunteers to read through early drafts of a monograph are welcome!