



Board of Studies Course Proposal

PROPOSED COURSE TITLE: Categories and quantum informatics

PROPOSER(S): Chris Heunen

DATE: 17 February 2016

SECTION 1 – CASE FOR SUPPORT

1a. Overall contribution to teaching portfolio

Category theory is an indispensable research tool in logic, semantics, and informatics in general. It also links informatics to various other areas, notably in mathematics. It is the kind of topic that takes some getting used to, and theoretical PhD students without exposure would often have had a much more efficient first year with prior exposure. Virtually all other serious research universities with MSc programmes offer courses involving category theory. Our current curriculum does not involve any category theory at all. The mathematics curriculum also does not include any taught courses in it, depriving students of opportunities. To illustrate the need: within LFCS, research students organise their own reading group on category theory to fill the gap.

Category theory is also the kind of topic that is learnt best when applied to another topic, to make it more concrete. The traditional applications are functional programming, logic, and mathematical topics such as algebraic topology and algebraic geometry. There is also a relatively novel application to quantum informatics, which has in fact grown to one of the largest current applications of category theory. The School has recently acquired expertise in this field in the form of the proposer, who has taught similar courses at the University of Oxford for the past four years. Introducing this course is a great opportunity to implement the motto that “research inspires teaching and teaching inspires research”.

1b. Target audience and expected demand

The course will appeal to MSc students interested in foundations of informatics, who are interested in conceptual structure of protocols rather than algorithmic and complexity-theoretic properties, and to those who are interested in quantum informatics and digital security. One overall aspect that will appeal to many students is the use of a graphical calculus that makes computations exceedingly easy.

The course will build things from the ground up, including the required background from quantum computing, and needs as prerequisites only UG1 linear algebra. It does require some maturity with abstraction, which is why it is proposed at MSc level. It only thematically overlaps with the current MSc course on Quantum Computing, and not in terms of techniques and results taught, which is why that course is not required as a prerequisite (but still advised to take concurrently to give students a more comprehensive overview).

A similar course at the University of Oxford, offered at a similar level, is taken yearly by around 10 students, out of a cohort of 40-50. Of course the curriculum and student interest there is different, but anticipated demand might therefore be estimated around 10-15 students.

1c. Relation to existing curriculum

This course contributes to the Computer Science MSc and Informatics MSc degree programmes, under the specialisms Theoretical Computer Science and perhaps Cyber Security & Privacy. It is thematically related to the MSc course Introduction to Quantum Computing, but they are not competitors, as there is no overlap in techniques and they are independent. Nevertheless students might be suggested to take both courses concurrently to get a more comprehensive overview. Therefore this course is probably best offered in 2nd semester, but this is not a strong constraint.

1d. Resources

Lectures (2 hours a week) will be provided by the proposer voluntarily, who is currently on a research fellowship and hence requires no resourcing. Because of the estimated class size, an interactive character is possible, and the part of the second lecture will be run as a tutorial, based on weekly exercise sheets. If demand turns out to be larger, officially resourced tutorials could be reconsidered in future. It would in future also be possible to have a guest lecture or two by dr. Ross Duncan from Strathclyde, and a practical session.

SECTION 2 – COURSE DESCRIPTOR

2a. Course Title: Categories and Quantum Informatics

2b. SCQF Credit Points: 20

SCQF Credit Level: 11

Normal Year Taken: 5/MSc

Also available in years: 4/5/MSc

2c. Subject Area and Specialism Classification:

Computer Science, specialist area Theoretical Computer Science

Appropriate/Important for the Following Degree Programmes:

Computer Science, Informatics

Timetabling Information:

Second semester, ideally, to avoid overlap with the independent course Introduction to Quantum Computing, which is expected to prove a popular combination.

2d. Summary Course Description:

Category theory is a powerful mathematical tool in logic and informatics, that has influenced the design of modern (functional and quantum) programming languages. It replaces concrete and often cumbersome set-theoretic encodings with more elegant abstractions that reveal the intrinsic structure underlying them. Category theory shines at easing complicated bookkeeping. In particular, a powerful graphical calculus lets us draw pictures instead of writing algebraic expressions. This technique is visually extremely insightful, yet completely rigorous. For example, correctness of protocols often comes down to whether a picture is connected or disconnected, whether there is information flow from one end to another. This course develops the basic ideas of category theory by applying them to quantum informatics. It investigates the conceptual reasons why quantum protocols and quantum computing work, rather than their algorithmic and complexity-theoretic aspects.

Course Description:

The course begins by introducing the idea behind category theory and the breadth of its scope. Why would it be a good idea to abstract away from specific hard-coded set-theoretic structures, and have compositional denotational semantics, in general? Illustrations from functional programming and categorical methods in logic are given.

We then focus more specifically on monoidal categories. Via lectures and self-study reading, the course teaches students the basics of dual objects in monoidal categories. Specific attention is paid to the graphical calculus, which makes the topic visually apparent. Via weekly exercise sheets, and their review incorporated into the contact hours, the student learns to graphically manipulate algebraic objects such as monoids and Frobenius structures. He/she will understand that this still allows perfectly rigorous proofs of correctness, and be able to see the information flow of a protocol that is often hidden behind superfluous details.

Throughout the course, the abstract material is linked to quantum informatics. We will categorically model notions typically thought to belong to quantum theory, such as entanglement, no-cloning, teleportation, and complementarity. But it will turn out some of these notions also make perfect sense in other settings. For example, the very same categorical description of quantum teleportation also describes classical encryption with a one-time pad. We identify characteristics of classical and quantum information, aiming to equip students to choose the right tools and techniques for future problems they may encounter.

Pre-Requisite Courses:

Introduction to Linear Algebra (MATH08057)

Co-Requisite Courses:

Introduction to Quantum Computing (INFR11099) is complementary to this course. Although the two are independent, it is suggested that students wishing to get a comprehensive overview take both.

Prohibited Combinations:

None

Other Requirements:

This course is open to all Informatics students including those on joint degrees. For external students where this course is not listed in your DPT, please seek special permission from the course organiser. Basic knowledge of linear algebra, vector spaces, and complex numbers will be assumed, as well as experience with mathematical abstraction. Undergraduates must have passed Introduction to Linear Algebra. Postgraduate or visiting students must have taken similar courses providing this background. No programming experience is required.

Available to Visiting Students: Yes

2e. Summary of Intended Learning Outcomes (MAXIMUM OF 5):

On completion of this course, the student will be able to:

1. Illustrate the idea behind and breadth of categorical semantics;
2. Apply and prove basic results about monoidal categories;
3. Fluently manipulate the graphical calculus for compact categories;
4. Model quantum protocols categorically and prove their correctness graphically;
5. Differentiate between categories modelling classical and quantum informatics.

Assessment Information

Written exam and one piece of coursework. The written exam will mostly test learning objectives 3, 4, and 5. The coursework will be similar to weekly exercise sheets, is due shortly after the course is halfway, and will mostly test learning objectives 1, 2, and 3.

Assessment Weightings:

Written Examination: 70%

Practical Examination: 0%

Coursework: 30%

Time spend on assignments:

Learning outcomes 1, 2, and 5 lend themselves best to longer ripening rather than time-limited exam settings. Therefore the coursework will weigh quite heavily.

Academic description:

This course gives an introduction to some topics in monoidal category theory, and shows how they can be used to model phenomena in quantum informatics. Everything will be built from the ground up, including the very notion of (monoidal) category, and the use of abstraction, compositionality, and generally categorical semantics. Specific topics include the graphical calculus for monoidal categories, dual objects, monoids, and Frobenius structures. Applications include entanglement, the quantum teleportation protocol, the no-cloning theorem, and the Deutsch-Jozsa algorithm.

Syllabus:

The course will follow the forthcoming book “Categories for Quantum Theory: An Introduction” by C. Heunen and J. Vicary, to be published by Oxford University Press, and/or lecture notes based there upon. Topics covered in 10 weeks:

- Abstract semantics, compositionality, categories
- Monoidal categories, coherence, symmetry, graphical calculus
- Scalars, daggers, entanglement, states
- Dual objects, quantum teleportation, information flow (2 weeks)
- Monoids and comonoids, cloning, products (2 weeks)
- Frobenius structures, normal forms, phases (2 weeks)
- Complementarity, Deutsch-Jozsa algorithm

Relevant QAA Computing Curriculum Sections:

Theoretical Computing, Developing Technologies

Graduate Attributes, Personal and Professional skills:

Generic Cognitive Skills:

- Obtain, organise, and use factual, theoretical, and/or hypothetical information in problem solving (level 6)
- Make generalisations and predictions (level 6)
- Present and evaluate arguments, information and ideas routine to the subject (level 7)
- Undertake critical analysis, evaluation and synthesis of ideas and concepts within the common understandings of the subject (level 8)

Reading List:

- “Categories for Quantum Theory: An Introduction” by C. Heunen and J. Vicary, to be published by Oxford University Press

Breakdown of Learning and Teaching Activities:

Lecture Hours: 15 hours

Seminar/Tutorial Hours: 5 hours

Supervise practical/Workshop/Studio hours: 0 hours

Summative assessment hours: 10 hours

Feedback/Feedforward hours: 1 hours

Directed Learning and Independent Learning hours: 64 hours

Total hours: 100 hours

Keywords:

category theory, quantum computing, semantics

Model answer:

(a) Associativity of \circ_M follows from associativity of \triangleleft . It follows from unitality of M that the identity $A \rightarrow A$ in \mathbf{C}_M is $\triangleleft \otimes \text{id}_A$.

(b) First assume the Frobenius law. That $f^{\dagger\dagger} = f$ follows from the Frobenius law and unitality. That $(g \circ_M f)^\dagger = f^\dagger \circ_T g^\dagger$ follows from the Frobenius law.

Conversely, suppose \mathbf{C}_M is a dagger category. Then

$$\left| \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \right| = \left(\left(\begin{array}{c} | \\ \bullet \\ | \end{array} \right) \right)^{\dagger\dagger} = \left(\begin{array}{c} \cup \\ \bullet \\ | \end{array} \right)^\dagger = \begin{array}{c} \bullet \\ | \\ \cup \\ \bullet \\ | \\ \bullet \end{array}$$

Postcomposing with \triangleleft gives the nondegenerate form of the Frobenius law.

(c) That they are well-defined functors follows from the Frobenius law and the monoid laws. That they preserve daggers follows from the Frobenius law.

(d) Straightforward unfolding of definition of dagger in \mathbf{C}_M .

3b. Sample coursework specification

The next page gives some information about *feedback structures*. Examine the constructions that are described, and prove all mathematical statements. Use examples to illustrate the aspects you are investigating, for instance drawn from **Rel** or **Hilb**. Make the most of opportunities to use a graphical calculus. You should aim to expand the information below into a comprehensive set of notes on feedback structures, suitable for anybody who has taken the Categorical Quantum Mechanics course. Feel free to include any additional observations on feedback structures you notice yourself that you can make precise.

Feedback Structures

A symmetric monoidal category is said to have a *feedback structure* when for any triple of objects A, B and X , a morphism $f: A \otimes X \rightarrow B \otimes X$ can be converted into a morphism $\Phi_{A,B}^X(f): A \rightarrow B$ in a well-controlled way. Intuitively, the idea is that the X part of the codomain of f has been ‘fed back’ into the X part of the domain of f . Feedback structures are required to satisfy the following axioms:

$$g \circ \Phi_{A,B}^X(f) \circ h = \Phi_{C,D}^X((g \otimes \text{id}_X) \circ f \circ (h \otimes \text{id}_X)) \quad (1)$$

$$\Phi_{X,X}^X(\sigma_{X,X}) = \text{id}_X \quad (2)$$

$$\Phi_{C \otimes A, C \otimes B}^X(\text{id}_C \otimes f) = \text{id}_C \otimes \Phi_{A,B}^X(f) \quad (3)$$

$$\Phi_{A,B}^X(\Phi_{A \otimes X, B \otimes X}^Y(f)) = \Phi_{A,B}^Y(\Phi_{A \otimes Y, B \otimes Y}^X((\text{id}_B \otimes \sigma_{Y,X}) \circ f \circ (\text{id}_A \otimes \sigma_{X,Y}))) \quad (4)$$

Any compact category allows a unique feedback structure.

An interesting way to construct a feedback structure is to start with a category with biproducts and a zero object, and use those as the monoidal product and unit. Intuitively, we can interpret a morphism $f: A \oplus X \rightarrow B \oplus X$ as a device that takes as input either an element of A or an element of X , and produces either an element of B or an element of X . Suppose we want to convert an element of A into an element of B . Then we could feed our element of A into the device, and repeatedly feed back in every element of X that is produced, until we obtain an element of B . Assuming certain infinite sums are well-defined in the category, this intuition leads to a formal construction of a feedback structure that satisfies the axioms above.

Any symmetric monoidal category \mathbf{C} with a feedback structure gives rise to a new category $\mathbf{K}(\mathbf{C})$ where:

- objects are pairs (A, B) of objects of \mathbf{C} ;
- morphisms $f: (A, B) \rightarrow (C, D)$ are morphisms $f: A \otimes D \rightarrow B \otimes C$ of \mathbf{C} ;
- composition of $f: (A, B) \rightarrow (C, D)$ and $g: (C, D) \rightarrow (E, F)$ is computed as

$$\Phi_{A \otimes F, B \otimes E}^C((\text{id}_B \otimes \sigma_{C,E}) \circ (f \otimes \text{id}_E) \circ (\text{id}_A \otimes (g \circ \sigma_{F,C}))).$$

In fact, this is a compact category.

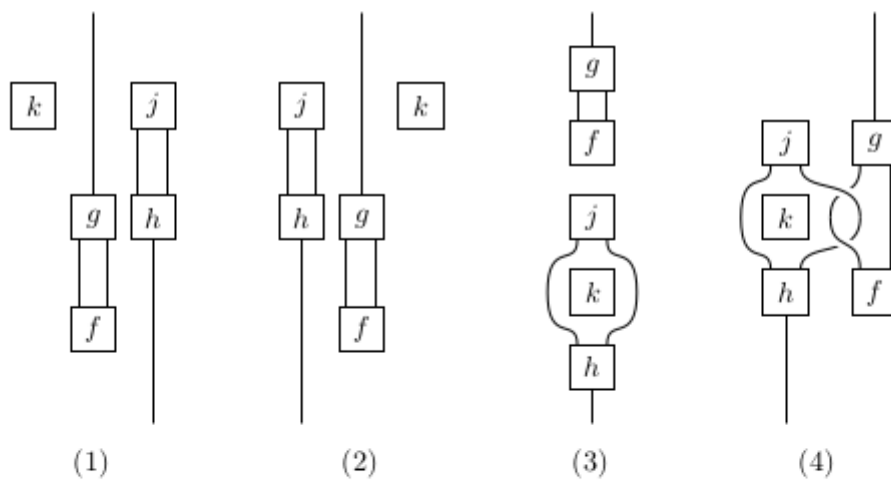
This has important implications for categorical models of quantum mechanics. If \mathbf{C} is a dagger compact category, then $\text{CP}(\mathbf{C})$, as defined in the lectures, embeds into $\mathbf{K}(\mathbf{C})$. This leads to a new way of defining $\text{CP}(\mathbf{C})$ for dagger symmetric monoidal categories that do not necessarily have duals for objects, including environment structures that enable one to disregard a subsystem by decoherence.

3c. Sample tutorial/lab sheet questions

Exercise 1.4.4. Convert the following algebraic equations into graphical language. Which would you expect to be true in any symmetric monoidal category?

- (a) $(g \otimes \text{id}) \circ \sigma \circ (f \otimes \text{id}) = (f \otimes \text{id}) \circ \sigma \circ (g \otimes \text{id})$ for $A \xrightarrow{f,g} A$.
- (b) $(f \otimes (g \circ h)) \circ k = (\text{id} \otimes f) \circ ((g \otimes h) \circ k)$, for $A \xrightarrow{k} B \otimes C$, $C \xrightarrow{h} B$ and $B \xrightarrow{f,g} B$.
- (c) $(\text{id} \otimes h) \circ g \circ (f \otimes \text{id}) = (\text{id} \otimes f) \circ g \circ (h \otimes \text{id})$, for $A \xrightarrow{f,h} A$ and $A \otimes A \xrightarrow{g} A \otimes A$.
- (d) $h \circ (\text{id} \otimes \lambda) \circ (\text{id} \otimes (f \otimes \text{id})) \circ (\text{id} \otimes \lambda^{-1}) \circ g = h \circ g \circ \lambda \circ (f \otimes \text{id}) \circ \lambda^{-1}$, for $A \xrightarrow{g} B \otimes C$, $I \xrightarrow{f} I$ and $B \otimes C \xrightarrow{h} D$.
- (e) $\rho_C \circ (\text{id} \otimes f) \circ \alpha_{C,A,B} \circ (\sigma_{A,C} \otimes \text{id}_B) = \lambda_C \circ (f \otimes \text{id}) \circ \alpha_{A,B,C}^{-1} \circ (\text{id} \otimes \sigma_{C,B}) \circ \alpha_{A,C,B}$ for $A \otimes B \xrightarrow{f} I$.

Exercise 1.4.5. Consider the following diagrams in the graphical calculus:



- (a) Which of the diagrams (1), (2) and (3) are equal as morphisms in a monoidal category?
- (b) Which of the diagrams (1), (2), (3) and (4) are equal as morphisms in a braided monoidal category?

Exercise 1.4.8. Recall that an entangled state of objects A and B is a state of $A \otimes B$ that is not a product state.

(a) Which of these states of $\mathbb{C}^2 \otimes \mathbb{C}^2$ in **Hilb** are entangled?

$$\begin{aligned} & \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ & \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle) \\ & \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle) \\ & \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \end{aligned}$$

(b) Which of these states of $\{0, 1\} \otimes \{0, 1\}$ in **Rel** are entangled?

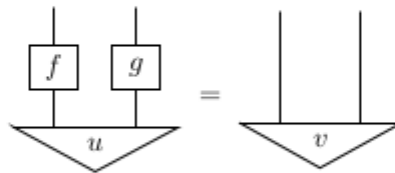
$$\{(0, 0), (0, 1)\}$$

$$\{(0, 0), (0, 1), (1, 0)\}$$

$$\{(0, 1), (1, 0)\}$$

$$\{(0, 0), (0, 1), (1, 0), (1, 1)\}$$

Exercise 1.4.9. We say that two joint states $I \xrightarrow{u,v} A \otimes B$ are *locally equivalent*, written $u \sim v$, if there exist invertible maps $A \xrightarrow{f} A$, $B \xrightarrow{g} B$ such that



(a) Show that \sim is an equivalence relation.

(b) Find all isomorphisms $\{0, 1\} \rightarrow \{0, 1\}$ in **Rel**.

(c) Write out all 16 states of the object $\{0, 1\} \times \{0, 1\}$ in **Rel**.

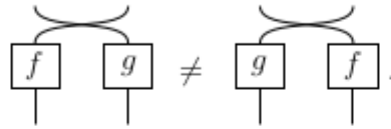
(d) Use your answer to (b) to group the states of (c) into locally equivalent families.

How many families are there? Which of these are entangled?

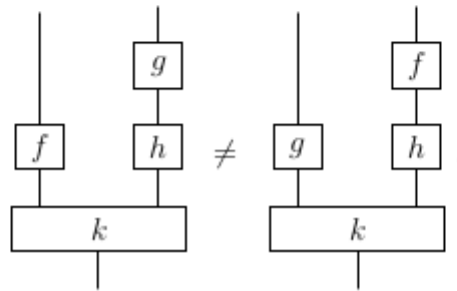
Model answers:

Exercise 0.0.4. Recall that the swap map is natural.

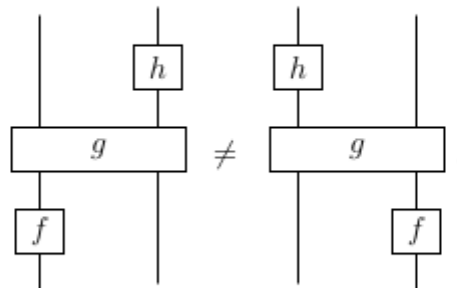
- (a) Taking $A = \{0, 1\}$, $f = \text{id}_A$ and $g(0) = 1$ and $g(1) = 0$ in (Set, \times) shows that



- (b) Taking $A = C = \{a\}$, $B = \{0, 1\}$, $k(a) = (0, a)$, $f = \text{id}_B$, and $g(0) = 1$ and $g(1) = 0$ in (Set, \times) shows that



- (c) Taking $A = \{0, 1\}$, $f = \text{id}_A$, $g = \text{id}_{A \times A}$ and $h(0) = 1$ and $h(1) = 0$ in (Set, \times) shows that



- (d) This equation holds in any monoidal category, because both sides expand

Exercise 0.0.8. Recall that an entangled state of objects A and B is a state of $A \otimes B$ that is not a product state.

(a) The first and fourth are product states:

$$\begin{aligned}\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) &= \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right), \\ \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) &= \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right).\end{aligned}$$

In general, because $|0\rangle$ and $|1\rangle$ form an orthonormal basis, any product state takes the form $(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + cd|11\rangle$ for some $a, b, c, d \in \mathbb{C}$. For the second and third states, there is no

solution to the ensuing system of linear equations, so these two states are entangled.

(b) The first and fourth are product states:

$$\begin{aligned}\{(0, 0), (0, 1)\} &= \{0\} \times \{0, 1\}, \\ \{(0, 0), (0, 1), (1, 0), (1, 1)\} &= \{0, 1\} \times \{0, 1\}.\end{aligned}$$

In general, if $S \subseteq \{0, 1\} \times \{0, 1\}$ is a product state, then it must be the product of $\{x \mid \exists y: (x, y) \in S\}$ and $\{y \mid \exists x: (x, y) \in S\}$. The second and third states do not satisfy this, and are hence entangled.

Exercise 0.0.9. Two joint states are locally equivalent when then can be transformed into one another using only uncorrelated local operations. So if two joint states possess a different ‘amount of correlation’, they will not be locally equivalent.

- (a) Taking $f = g = \text{id}$ shows that $u \sim u$. If $u \sim v$ because $v = (f \otimes g) \circ u$, then also $(f^{-1} \otimes g^{-1}) \circ v = u$, whence $v \sim u$. Finally, if $u \sim v$ and $v \sim w$ because $v = (f \otimes g) \circ u$ and $w = (k \otimes h) \circ v$, then $w = ((k \circ f) \otimes (h \circ g)) \circ u$ by the interchange law, so that $u \sim w$.
- (b) Isomorphisms in Rel are the graphs of bijections: $\{(0, 0), (1, 1)\}$ and $\{(0, 1), (1, 0)\}$ are the only isomorphisms $\{0, 1\} \rightarrow \{0, 1\}$.
- (c) States of $\{0, 1\} \times \{0, 1\}$ are its subsets.
- (d) Simply starting with one state we haven’t classified yet, and generating all possible locally equivalent ones by pre- and/or postcomposing with all bijections, we find the following 7 local equivalence classes.

$$\begin{aligned}\emptyset \\ \{(0, 0)\} \sim \{(0, 1)\} \sim \{(1, 0)\} \sim \{(1, 1)\} \\ \{(0, 0), (0, 1)\} \sim \{(1, 0), (1, 1)\} \\ \{(0, 0), (1, 0)\} \sim \{(0, 1), (1, 1)\} \\ \{(0, 0), (1, 1)\} \sim \{(0, 1), (1, 0)\} \\ \{(0, 0), (0, 1), (1, 0)\} \sim \{(0, 0), (0, 1), (1, 1)\} \sim \{(0, 0), (1, 0), (1, 1)\} \sim \{(0, 1), (1, 0), (1, 1)\} \\ \{(0, 0), (0, 1), (1, 0), (1, 1)\}\end{aligned}$$

Notice that local equivalence respects cardinality (but states of the same cardinality need not be locally equivalent).

3d. Any other relevant materials

Optional material for possible practical and/or interested students:

- “Basic Category Theory” by Tom Leinster, Cambridge University Press
- Quantomatic proof assistant: <https://sites.google.com/site/quantomatic/>
- Globular proof assistant: <http://globular.science/>

SECTION 4 - COURSE MANAGEMENT

4a. Course information and publicity

Introductory video. Course description, both official and extracted from this document. Lecture notes, and complete set of exercises. A full set of lecture slides is also available, but due to the interactive character, I plan *not* to release these at the start of the academic year, but rather adapt and publish them as the course progresses.

4b. Feedback

Feedback from the students:

There will be “pre-assessment” questionnaire to gauge prior knowledge, experience, and expectations from the course. The course will have an interactive character, and the students are free at any point to ask for explanations. Part of every second lecture will be run as a tutorial, reviewing exercise sheets.

Feedback to the students:

Part of every second lecture will be run as a tutorial, reviewing exercise sheets. This gives students opportunity to compare answers with each other, and will also include students working through exercises on the board, thus giving them feedback. The coursework will be marked within two weeks. Part of a the lecture after that will be dedicated to discussions and matters arising. As is standard in Informatics, individual feedback will not be provided on the written exam. The lecturer will produce brief notes on what was done well or badly, common mistakes, and points of note.

4c. Management of teaching delivery

Lecturer will give lectures, including the tutorial-like sessions, as well as mark the coursework and written exam.

SECTION 5 - COMMENTS

5a. Year Organiser Comments

Year 4 organiser (Mary Cryan):

"Not an expert in this area of theory but it might have too much content for one of our 10-point courses. It seems there is too much "stuff" in there getting delivered in the 15 lectures. Maybe a good idea to compare to "Intro to Theoretical Computer Science" (which is level 10, 3rd year, like ADS)"

After this feedback the proposal was consolidated to reduce the delivered content.

"The students here tend to avoid the abstract courses ...you might get a few from Physics to join"

There might be some interest from Mathematics students as well.

Year 5 organiser (Mashesh Marina):

pending

MSc organiser (Paul Jackson):

pending

5b. BoS Academic Secretary (Alan Smail):

"A well-motivated and presented proposal"