

Plano de Ensino - Atividades Remotas Emergenciais - 2021/1

Código	DCC XXX (A definir)
Disciplina	<i>Quantitative Information Flow</i> (Fluxo de Informação Quantitativo)
Turma	Pós-Graduação + Graduação
Professor	Mário Sérgio Alvim

Pré-requisitos: Conhecimento prévio em matemática discreta (conjuntos, funções, métodos de demonstração elementares) e probabilidade discreta (probabilidade simples, condicional, valor esperado).

Língua: O curso será **ministrado na língua inglesa**.

Objetivos: Introduzir o(a) aluno(a) a uma abordagem científica rigorosa sobre o problema de fluxo de informação quantitativo, capacitando-o(a) a modelar e quantificar como a informação flui ao ser processada por sistemas computacionais.

Ementa: Revisão de probabilidade discreta e inferência Bayesiana. Modelagem de incerteza e métricas de informação. Conceito e propriedades fundamentais de canais de informação, de fluxo de informação e de robustez de canais. Modelagem de problemas de segurança.

Programa

Obs:

- As aulas síncronas (*on-line, live lectures*) se darão de modo interativo, sendo gravadas e disponibilizadas para acesso posterior.
- Os exames (*remote exams*) ocorrerão de modo assíncrono.
- As apresentações de seminários se darão em reuniões interativas síncronas (*on-line, live interactive meetings*).

Lecture	Date	Topic	Notes
---	May-18	<i>Welcome to new students.</i>	
01	May-20	<i>Introduction: An overview of Quantitative Information Flow</i>	On-line, live lecture
02	May-25	<i>Review of discrete probability</i>	On-line, live lecture
03	May-27	<i>Modeling secrets / On g-vulnerability</i>	On-line, live lecture
04	Jun-01	<i>On g-vulnerability</i>	On-line, live lecture
---	Jun-03	<i>Holiday: Corpus Christi</i>	
05	Jun-08	<i>On g-vulnerability</i>	On-line, live lecture
06	Jun-10	<i>Channels</i>	On-line, live

			lecture
07	Jun-15	<i>Channels</i>	On-line, live lecture
08	Jun-17	<i>Posterior vulnerabilty and leakage</i>	On-line, live lecture
09	Jun-22	<i>Posterior vulnerabilty and leakage</i>	On-line, live lecture
10	Jun-24	<i>Posterior vulnerabilty and leakage</i>	On-line, live lecture
11	Jun-29	<i>Spare class / Review</i>	On-line, live interactive meeting
12	Jul-01	<i>First exam</i>	Remote exam
13	Jul-06	<i>Robustness / Capacity</i>	On-line, live lecture
14	Jul-08	<i>Capacity</i>	On-line, live lecture
15	Jul-13	<i>Composition of channels</i>	On-line, live lecture
16	Jul-15	<i>Refinement</i>	On-line, live lecture
17	Jul-20	<i>Refinement</i>	On-line, live lecture
18	Jul-22	<i>The Dalenius perspective</i>	On-line, live lecture
19	Jul-27	<i>Axiomatics</i>	On-line, live lecture
20	Jul-29	<i>The geometry of hypers, gain and losses</i>	On-line, live lecture
21	Aug-03	<i>Applications: The Crowds Protocol</i>	On-line, live lecture
22	Aug-05	<i>Advanced topics: Differential privacy</i>	On-line, live lecture
23	Aug-10	<i>Advanced topics: Differential privacy</i>	On-line, live lecture
24	Aug-12	<i>Spare class / Review</i>	On-line, live interactive meeting
25	Aug-17	<i>Second exam</i>	Remote exam
26	Aug-19	<i>Seminars</i>	On-line, live interactive meeting
27	Aug-24	<i>Seminars</i>	On-line, live interactive meeting
28	Aug-26	<i>Seminars</i>	On-line, live interactive meeting
29	Aug-31	<i>Seminars</i>	On-line, live interactive meeting
30	Sep-02	<i>Make-up exam</i>	Remote exam

Bibliografia

The Science of Quantitative Information Flow.

Mário. S. Alvim, Konstantinos Chatzikokolakis, Annabelle McIver, Carroll Morgan, Catuscia Palamidessi, Geoffrey Smith.
Springer International Publishing (2020).

Material de apoio

Página da disciplina (slides e outro material didático).

Moodle (comunicação com estudantes).

Microsoft Teams (aulas e encontros interativos online).

Avaliações

1	Primeiro exame remoto assíncrono	25 pontos	2021-Jul-01
2	Segundo exame remoto assíncrono	25 pontos	2021-Ago-17
3	Seminário final	30 pontos	2021-Ago-19 a 31
4	Listas de exercícios feitas em casa	20 pontos	Ao longo do semestre