DIPARTIMENTO
DI INFORMATICA

SAPIENZA
UNIVERSITÀ DI ROMA

Percorso di eccellenza per laurea magistrale LM-18

Argomenti per i percorsi di eccellenza da scegliere per i bandi relativi all'a.a.2017-2018

Docente: Toni Mancini

Intelligenza Artificiale per la Medicina Personalizzata in Silico

Progettare un nuovo farmaco costa miliardi di Euro ed il relativo percorso di messa sul mercato è estremamente lungo (>10 anni) e pieno di ostacoli. E' molto frequente infatti che un farmaco che si comporta bene in laboratorio (in provetta, ovvero "in vitro", oppure su tessuti biologici isolati, ovvero "ex vivo") non superi i successivi stadi di verifica ("clinical trial") su animali e pazienti umani ("in vivo"). Tali stadi avanzati di verifica durano molti anni e sono estremamente costosi, dato che l'utilizzo di animali e pazienti umani impone una grande prudenza ed attenzione alla sicurezza delle cavie.

Il fallimento del progetto di un nuovo farmaco in una fase avanzata ("in vivo") implica una perdita economica ingente per gli attori coinvolti. Questo comporta una sempre maggiore prudenza, da parte delle case farmaceutiche, nell'avviare attività di ricerca per farmaci fortemente innovativi.

Una delle direzioni più rivoluzionarie della ricerca in medicina e farmacologia consiste nel definire ed utilizzare modelli matematici della fisiologia umana ("Virtual Physiological Human", VPH) per progettare e verificare nuovi farmaci e nuovi trattamenti clinici "in silico" (ovvero mediante simulazione al computer), prima di intraprendere costose, rischiose ed invasive sperimentazioni "in vivo" su animali ed esseri umani.

Obiettivo di un modello VPH è di catturare tutti i comportamenti biologicamente validi presenti in natura. Grazie all'uso combinato di misurazioni cliniche (ad es., esami del sangue) e di tecniche algoritmiche di Intelligenza Artificiale è possibile personalizzare tali modelli, affinché simulino il comportamento di un singolo (dato) individuo e la sua personale risposta ad un insieme di farmaci. Tale possibilità apre la porta al progetto (ancora "in silico") di terapie individualizzate ("personalised medicine"), ovvero che massimizzino le performance per un certo dato individuo e al contempo minimizzino rischio e gravità di effetti collaterali.

In conclusione, il successo della "in silico medicine" permetterà di raggiungere i seguenti obiettivi ad altissimo impatto tecnico, economico, sociale ed etico:

1. Una forte riduzione nell'uso di cavie animali e di volontari umani per la verifica di nuovi farmaci e protocolli clinici.
2. Una forte riduzione dei tempi di progetto e verifica di nuovi farmaci, con conseguente riduzione dei costi per i sistemi sanitari nazionali e, quindi, per i cittadini (attualmente la spesa in Sanità è di gran lunga la più onerosa per i bilanci degli stati europei) e il conseguente spostamento degli ingenti fondi così risparmiati nella ricerca di farmaci fortemente innovativi.
3. La possibilità di progettare trattamenti ottimali per ogni singolo paziente che massimizzino il risultato clinico su quel particolare paziente, al contempo minimizzando il rischio di effetti collaterali e la quantità di farmaco assunto.

Durante il percorso di eccellenza, lo studente imparerà metodologie e tecniche di Intelligenza Artificiale nell'ambito della "in silico medicine" per il progetto e la verifica di trattamenti farmacologici personalizzati, utilizzando opportuni modelli VPH.

Per maggiori informazioni, si veda: http://tmancini.di.uniroma1.it/index.php?page=teaching.eccellenza

***

Artificial Intelligence for Personalised In Silico Medicine

Designing a new pharmaceutical drug typically costs billions of Euros, and the entire path from research to market often takes many (>10) years, with several obstructions which often provoke failure of the entire process. In particular, often a drug which performs well in laboratory ("in vitro", or on isolated tissues, i.e. "ex vivo") fails the subsequent testing phases ("clinical trial") on animals and human patients ("in vivo"). Such advanced drug testing phases may last several years and often are extremely expensive, as the involvements of animals and human patients requires great care about safety and security.

A late failure of the verification process for a new drug (for example, during the "in vivo" phase) implies a huge economic loss for the drug developers (for example, a pharmaceutical industry). This leads to the fact that pharma companies are often rather conservative in starting research activities on radically innovative drugs.

One of the most revolutionary research directions in medicine and pharmacology consists in defining and exploiting mathematical models of the human physiology ("Virtual Physiological Human", VPH) in order to design and verify safety and efficacy of new drugs and new treatment protocols "in silico" (i.e., by means of computer simulation), before starting expensive, risky and invasive "in vivo" clinical trials on animals and humans.

The main objective of a VPH model is to capture all biologically correct behaviours, that is all behaviours that could occur in nature. By combining clinical data on real patients (e.g., from blood samples) and sophisticated computational techniques from Artificial Intelligence, such models can be individualised in order to make them able to simulate the behaviour of any given patient and his/her personal reaction to a set of drugs. The possibility to individualise VPH models also allows "in silico" design of individualised pharmacological therapies, i.e., therapies that maximise their performance on a certain given human patient at the same time minimising expected risk and severity of negative side-effects.

Summing up: success of "in silico medicine" will lead to the following achievements with huge technical, economical, social and ethical impacts:

1. A great reduction in the number of animals and human volunteers in clinical trials for testing new drugs and treatments.
2. A great reduction in the duration and costs of new drug design and verification activities. This would also lead to a great reduction of the costs to be paid by national Public Health Systems and, as a consequence, by taxpayers (currently expenditures in Health is by far the highest item in national budgets), and, ultimately, in moving these enormous economic resources into research of radically innovative drugs.
3. The possibility to design optimal treatments for any single patient, which maximise the clinical outcome on that patient at the same time minimising risk and severity of side-effects as well as the quantity of drugs used.

During the Honour Programme, students will learn methods based on Artificial Intelligence in the context of "in silico medicine" in order to design and verify safety and efficacy of individualised treatment protocols, exploiting complex VPH models.

For more information, please refer to: http://tmancini.di.uniroma1.it/index.php?page=teaching.eccellenza

***

Docente: Roberto Navigli

Magistrale ita:

Titolo: Un viaggio nelle reti neurali per la comprensione del linguaggio naturale

Questo percorso consiste nello studio delle reti neurali fino alle più avanzate architetture di reti neurali al fine di sviluppare tecniche innovative per abilitare la comprensione automatica del linguaggio naturale (disambiguazione, traduzione automatica, ecc.). Dopo uno studio teorico, ai fini dell'implementazione si utilizzeranno i framework più diffusi, tra cui TensorFlow e Keras.

Magistrale EN:

Titolo: Neural networks for natural language understanding

This research path consists in the study of neural networks, including the most recent architectures, to develop innovative techniques that enable Natural Language Understanding (NLU, including: disambiguation, machine translation, etc.). The most popular frameworks, such as TensorFlow and Keras, will be used for practical implementation of existing and novel approaches to neural NLU.

***

Docente: Tiziana Calamoneri
Titolo: Algoritmi su Grafi per risolvere Problemi in Biologia

Molti problemi biologici possono essere risolti modellandoli come problemi su grafi.

Percorsi su questi argomenti consistono nello studio approfondito di uno di questi problemi e della sua modellizzazione su grafi.

Titolo: Algoritmi di Geometria Computazionale

La geometria computazionale è quel ramo dell'algoritmica che si occupa di risolvere efficientemente problemi geometrici in modo automatico.
Gli algoritmi di geometria computazionale richiedono tipicamente strutture dati abbastanza sofisticate.
Percorsi di questo tipo prevedono lo studio approfondito di algoritmi che risolvono problemi geometrici con particolare attenzione al loro costo computazionale.

MAGISTRALE INGLESE

Topic: Graph Algorithms to solve Problems in Biology

Some biological problems can be solved by modeling them as graph problems.
Studies in this context consist in deepening the known models and solutions.

Topic: Computational Geometry Algorithms

Computational geometry is the branch of Algorithmics dealing with efficient solution of geometric problems. Typically, computational geometry algorithms require sophisticated data structures.
Studies in this context consist in studying some notable examples of computational geometry algorithms with a particolar attention to their computational complexity.

***

Docente: Emanuele Rodolà

Topic: Geometric Deep Learning

Many practical problems in computer vision, graphics, pattern recognition, network analysis and neuroimaging deal with data living on non-flat domains such as graphs, 3D surfaces and volumes, as opposed to classical 2D images. Geometric deep learning is an emerging field aiming at extending the capabilities of successful deep learning models to deal with this kind of data, opening the doors to novel applications and unprecedented performance on several challenging tasks. This topic will explore all the way from the theoretical foundations to the computational and more applicative aspects of geometric deep learning in the areas of computer vision, graphics, network analysis and multiple other applicative sub-fields of computer science.

Topic: 3D Geometry Processing and Shape Analysis

The analysis and processing of 3D shapes arising in computer vision and graphics involve several tools, techniques, and mathematical formalisms pertaining to multiple branches of computer science and mathematics, including differential and spectral geometry, functional analysis, PDEs, optimization, graph analysis and related areas. This topic will explore theoretical, computational and applicative aspects of the analysis and processing of 3D geometric data, including but not limited to: discretization of geometric tools from the continuous domain to polygonal meshes and

point clouds, shape matching and similarity, processing of 3D point clouds, shape modeling, 2D-to-3D correspondence, shape synthesis, and simulation.

Topic: Computer Vision for Medical Imaging

Medicine and biological sciences have a strong tradition in the adoption of image-based techniques as a support for medical practice. Typical problems involve different modalities (CT scanning, MRI, X-ray, etc.) and include tasks of shape retrieval, segmentation, correspondence, similarity, and prediction in the context of intra-operative imaging, tumor detection, clinical trials, and drug design to name but a few. This topic will address the study, design and application of computer vision, machine learning, and pattern recognition techniques for typical medical imaging problems, and will explore novel techniques to tackle problems that have not (or cannot) so far been addressed with existing methodology.

Docente: Emanuele Rodolà

Titolo: Deep Learning geometrico

Molti problemi pratici in visione artificiale, grafica, pattern recognition, analisi di reti e neuroimaging prevedono lo studio di dati definiti su domini non-piani quali i grafi, le superfici 3D e i volumi, in netto contrasto a domini classici come le immagini 2D. Il deep learning geometrico è un campo emergente il cui obiettivo primario è l'estensione delle capacità dei modelli correnti di deep learning per poter gestire e manipolare dati di questo tipo, aprendo nuove possibilità, applicazioni e prestazioni senza precedenti in diversi problemi tradizionalmente considerati difficili. Questo argomento esplora i fondamenti teorici così come gli aspetti computazionali e più applicativi del geometric deep learning, nelle aree della visione artificiale, grafica, analisi di reti e molte altre sotto-aree applicative dell'informatica.

Titolo: Analisi ed elaborazione di geometria 3D

L'analisi e l'elaborazione di forme tridimensionali che emergono in visione artificiale e grafica coinvolgono a loro volta diversi strumenti, tecniche e formalismi matematici derivanti da branche differenti dell'informatica e della matematica, tra cui: geometria differenziale e spettrale, equazioni differenziali alle derivate parziali, analisi funzionale, ottimizzazione, analisi di grafi ed altre aree correlate. Questo argomento esplorerà gli aspetti teorici, computazionali e applicativi nell'analisi ed elaborazione di dati geometrici 3D, tra cui: discretizzazione di strumenti geometrici dal continuo a mesh poligonali, corrispondenza e similarità tra forme, elaborazione di nuvole di punti 3D, modellazione, corrispondenza tra 2D e 3D, sintesi e simulazione.

Titolo: Visione artificiale per imaging biomedico

Le scienze biologiche e mediche hanno una forte tradizione nell'adozione di tecniche basate su immagini come supporto alla pratica medica. Problemi tipici in questo campo prevedono l'uso di modalità multiple (scansioni TAC, risonanza magnetica, raggi X, ecc.) e includono obiettivi di rilevamento di forme, segmentazione, corrispondenza, similarità e predizione, in disparati contesti tra cui diagnostica per immagini intra-operatoria, rilevamento di tumori, test clinici, e progettazione di farmaci tra molti altri. Questo argomento verterà sullo studio, la progettazione e l'applicazione di tecniche di visione artificiale, machine learning e pattern recognition per problemi tipici nel campo dell'imaging biomedico; verranno inoltre esplorate nuove tecniche ed approcci per risolvere problemi che, al giorno d'oggi, non sono stati (o non possono essere) esplorati con le metodologie correnti.

***

Docente: Daniele Venturi

Title: Non-malleable codes.

Description: Non-malleable codes encode a given message in such a way that mauling attempts with a codeword (within a certain class of allowed tampering functions) have the effect that decoding a modified codeword yields either the original message or a completely unrelated value. Such codes are interesting on their own right, but also have several applications to cryptography.

During this honor program the student will try to tackle open research questions in this context, e.g. studying the relationship between different flavors of non-malleable codes, constructing new codes for larger tampering families, and exploring new cryptographic applications.

References:
http://eprint.iacr.org/2014/173
http://eprint.iacr.org/2013/702

Title: Codici non malleabili.

Descrizione: I codici non malleabili codificano un dato messaggio in modo che ogni tentativo di malleare una parola di codice (usando funzioni in una certa classe di modifiche disponibili) ha l'effetto che la decodifica di una parola di codice modificata ritorna il messaggio originale o un valore completamente scorrelato. Studiare tali codici è interessante per se, ma ha anche diverse applicazioni in crittografia.

Durante questo percorso di eccellenza, lo studente proverà ad affrontare problemi aperti di ricerca in questo contesto, ad esempio studiare la relazione tra diverse sfumature di codici non malleabili, costruire nuovi codici per famiglie difunzioni più grandi, ed esplorare nuove applicazioni crittografiche.

Riferimenti:
http://eprint.iacr.org/2014/173
http://eprint.iacr.org/2013/702

Title: Leakage and Tamper Resilient Cryptography.

Description: The security of modern cryptographic algorithms is typically analyzed under the assumption that an adversary has neither partial knowledge nor she can modify the underlying secrets. Unfortunately, several realistic attacks (so called leakage and tampering attacks) do not obey this assumption, which creates a gap between theoretical cryptography and the real word.

During this honor program, the student will design new cryptographic primitives with provable guarantees against leakage and tampering attacks.

References:
http://eprint.iacr.org/2015/517
http://eprint.iacr.org/2016/529

Title: Crittografia resistente agli attacchi collaterali.

Descrizione: La sicurezza delle primitive crittografiche moderne è tipicamente analizzata sotto l'assunzione che l'attaccante non ha informazione né può modificare i segreti sottostanti. Sfortunatamente, molti attacchi reali (così detti attacchi collaterali) non obbediscono a questa assunzione, il che crea un gap tra la crittografia teorica ed il mondo reale.

In questo percorso di eccellenza, lo studente progetterà nuovi schemi crittografici con sicurezza dimostrabile contro gli attacchi collaterali.

Riferimenti:
http://eprint.iacr.org/2015/517
http://eprint.iacr.org/2016/529

***

Docente: Enrico Tronci
Titolo: Model Based System Engineering

Uno degli aspetti più critici e costosi nella progettazione di sistemi cyberphysical (che cioè coinvolgono, software, hardware e comunicazione) sono quelli legati alla validazione dei requisiti a livello di sistema ed alla verifica del design del sistema stesso.

L'approccio moderno a tali problematiche si basa sull'uso di modelli matematici (Model Based System Engineering, MBSE) per definire la dinamica delle varie componenti del sistema e sull'uso della "Hardware In the Loop Simulation" (HILS) per condurre le attività di verifica e validazione.

L'obiettivo del presente percorso di eccellenza è di far acquisire allo studente familiarità con le tecniche avanzate in questo settore sia da un punto di vista metodologico sia da un punto di vista progettuale.

Title: Model Based System Engineering

Requirements validation and system verification are among the most critical and

expensive steps in the design of Cyber-Physical systems, that is of systems comprising software, hardware and communication components.

The modern approach to V&V (Verification and Validation) rests on the use of mathematical models (Model Based System Engineering, MBSE) to define the dynamics of the system to be verified and on the use of "Hardware In the Loop Simulation" (HILS) to carry out V&V activities using a simulator running the system model.

The goal of the proposed activity is to expose the student to state-of-the-art methods and tools for MBSE for Cyber-Physical systems, both from a methodological as well as practical point of views.

***

Docente: Novella Bartolini

1. Network tomography (ITA)

Quando un guasto si sviluppa e si propaga in una rete di telecomunicazione, specialmente in caso di disastri e attacchi su larga scala, prima di pianificare interventi di riparazione e riconfigurazione, e` necessario conoscere la posizione e l'estensione dei guasti.

Questa informazione generalmente e` disponibile solo in modo parziale o probabilistico attraverso misure indirette che evidenziano la degradazione della qualita` del servizio offerto dalla rete.

La network tomography permette di inferire lo stato di nodi interni della rete correlando informazioni derivanti da misurazioni end-to-end prese da alcune posizioni strategiche, attraverso opportuni percorsi di monitoraggio.

In questo percorso di studio si svilupperanno nuovi algoritmi per massimizzare l'identificabilita` dei guasti, minimizzando il numero di monitor o di percorsi di monitoraggio nella rete.

Si studieranno inoltre i limiti teorici delle suddette tecniche in diversi domini applicativi e topologie di rete.

1. Network tomography (ENG)

After a failure (possibly at large scale) propagates in a communication network, it is of primary importance to be able to perform a fast and efficient damage assessment. This is preliminary to any recovery intervention.

Performance degradation of the network services is the primary symptom of existing failures. Nevertheless this gives only a partial or probabilistic view of the damages.

Network tomography provides a series of measurement and analytical techniques which allow to infer the state of individual internal nodes and links of a network, by analyzing the outcome of end-to-end measurements taken from strategic positions and paths along the network.

We plan to study existing algorithms and to develop new approaches to maximize failure identifiability, while minimizing the monitoring effort in terms of number of monitors and of monitoring paths.

Finally we will study the theoretical bounds of the proposed techniques in several application domains and different network topologies.

2. Uso di dispositivi mobili (sensori terrestri e droni) per il monitoraggio di ambienti critici (ITA).

Facendo riferimento a scenari geografici critici, soggetti a disastri naturali, come cataclismi, o a incidenti, come fughe di gas, radioattivita`, incendi, studieremo algoritmi per il dispiegamento e il coordinamento autonomo di squadre di droni e di sensori mobili terrestri.

Tra gli scenari di applicazione considereremo in particolare l monitoraggio di zone soggette a catastrofi naturali per ausilio nelle operazioni di salvataggio di uomini e animali, e quello del monitoraggio di agenti patogeni in aree agricole a bassa accessibilita`, in paesi in via di sviluppo.

2. Networks of aerial and terrestrial vehicles for critical environment monitoring. (ENG)

Autonomous squads of drones and terrestrial mobile sensors are a fundamental tool for disaster and critical environment monitoring. Earthquakes, flooding, chemical plumes are just few of the many examples where automated squads of monitoring devices could provide a fast and safe monitoring intervention.
We will study algorithms and protocols to enable autonomous deployment and monitoring of these networks.

We will consider two types of applicative scenarios posigin different challenges in terms of quality of service. In particular, we will consider the case of monitoring a land in the aftermath of a natural disaster, and the case of monitoring the spread of plant diseases in low accessiblility lands, such as farms in developing countries.

***

Docente: Alessandro Panconesi
Tipologia: laurea magistrale in informatica, sino a tre studenti
Argomento: Machine Learning vs Consistency
In molte applicazioni del ML, ad esempio clustering o feature selection, l'input cambia nel tempo e si vuole mantenere il più a lungo possibile una buona soluzione (consistency). Scopo del progetto è esplorare la possibilità di sviluppare algoritmi efficienti che mantengano una soluzione approssimata man mano che l'input cambia e che necessitino di un numero minimo di un numero minimo di ricomputazioni della soluzione stessa.

Docente: Alessandro Panconesi
Tipologia: master degree in computer science, up to three students
Argomento: Machine Learning vs Consistency
In several applications of machine learning, for instance clustering and feature selection, the input is constantly changing over time and one would like to maintain as long as possible a good solution (consistency). The goal of the project is to explore the possibility of devising algorithms that maintain a good solution as the input changes, and such that good solutions need to be recomputed as small a number of times as possible.

Docente: Emanuele Panizzi

Titolo: Lo smartphone in automobile

Questo percorso consiste nello studio dei principali problemi aperti di transportation (es. smart parking, jam absorption, lane determination, collision avoidance, maintenance and alerting) e delle possibili soluzioni che utilizzano lo smartphone in automobile o nei mezzi pesanti.
Verrà progettato un prototipo di applicazione mobile che sfrutti appieno i sensori dello smartphone, le possibilità di comunicazione e la potenza di calcolo, per realizzare interfacce altamente usabili.

Title: Smartphone in transportation
This topic consists in the study of the main open problems in transportation (e.g. smart parking, jam absorption, lane determination, collision avoidance, maintenance and alerting) and their possible smartphone-based solution in the car or in trucks. The student will design a prototype of mobile application that exploits smartphone sensors, communication and computation capabilities in order to create highly usable interfaces.

***

Docente: Igor Melatti

Algoritmi e tool per le Smart Cities e le Smart Grids
Percorso di eccellenza per laurea triennale e magistrale

Una delle sfide del prossimo futuro consiste nello sfruttare la sempre maggiore quantità di informazioni sul consumo energetico degli utenti residenziali al fine di ottenere una sensibile riduzione dei costi da parte delle cosiddette "utility" (ad es. nel caso italiano Acea, Enel etc.). Tale riduzione dei costi permette di abbassare la bolletta agli utenti residenziali stessi, che quindi grazie a ciò possono accettare di buon grado le installazioni del necessario software (i tool che si vogliono sviluppare in questo percorso di eccellenza) e hardware (batterie, sensori, microcomputer dedicati, etc). Per facilitare tale accettazione da parte degli utenti, è anche necessario che la privacy dei dati degli utenti sia assicurata (ad esempio, se sono disponibili i dati per ogni singolo elettrodomestico, tali dati potranno essere comunicati all'utility solo in forma aggregata). Infine, la riduzione dei costi deve riguardare non solo l'aspetto meramente economico "immediato", ma anche l'aspetto ambientale, riducendo ad esempio le emissioni di CO_2 necessarie per produrre energia. E' inoltre possibile indagare lo sviluppo di software che interagisca solamente con la casa

stessa, senza necessità di interazione con l'utility.
Questo percorso di eccellenza si propone quindi di insegnare a progettare algoritmi (tipicamente basati su tecniche di model checking) che raggiungano tale scopo, e a realizzare tool che implementino effettivamente questi algoritmi.

Algorithms and tools for Smart Cities and Smart Grids
Honour Programme for Bachelor and Master Programmes in Computer Science

One of the main challenges for our society's future is to exploit the ever increasing information about residential users electrical consumption, in order to cut electrical energy costs payed by utilities (such as Distributed System Operators and energy retailers). In turn, utilities will lower down residential users energy bills, in order to justify installation of the needed software (which is actually what we will develop in this honour programme) and hardware (batteries, sensors, dedicated microcomputers, etc; we will use existing hardware). In order to have residential users actually accepting the new setting, it is also necessary to guarantee their privacy (e.g., if in a smart home all appliances are able to communicate their energy consumption, then such data must be communicated to utilities only in an aggregated form). Finally, costs reduction must involve not only the economic saving, but also the environmental aspect, e.g., by provably reducing CO2 emissions. We also want to design and implement software which only works inside a single house, without communicating with the utility at all.

Summing up, this honour programme will teach how to devise, design and effectively implement new algorithms (typically based on model checking techniques) achieving the above described goals.

***

Docenti: Bottoni, Gorla, Labella, Parisi Presicce
Titolo: Computazioni distribuite e consistenza

Computazioni distribuite, quali quelle necessarie a mantenere registri distribuiti (*distributed ledger*) come permessi dalle tecnologie basate su *blockchain*, presentano tipicamente il problema di garantire la consistenza degli stati locali, o analogamente delle viste locali sullo stato globale, dei nodi (o agenti) coinvolti nella computazione, in modo che, anche nel caso alcune computazioni locali non siano immediatamente integrate nello stato globale, il sistema complessivo possa convergere a una soluzione condivisa. In particolare la ricerca su Conflict-free Replicated Data Types (CRDTs) ha posto le basi per definire tipi di dato, le cui manipolazioni siano fondamentalmente additive, in modo da consentire in ogni momento di proseguire la computazione fino a raggiungere un consenso sullo stato finale [SPBZ11a].
Attraverso queste tecniche si ottengono garanzie di eventual consistency, cioè di potere completare una computazione in modo che tutti i nodi siano in accordo sullo stato finale. Ciò ha messo in luce alcune insufficienze connesse alla garanzia di eventual consistency, e ha portato a proporre una nozione di strong consistency, in cui ogni stato stabile è sicuro, cioè tutte le transazioni riportate nel ledger sono legali, con alta probabilità [GKL15].
In questo percorso di eccellenza lo studente analizzerà la letteratura esistente, prenderà dimestichezza con le tecnologie utilizzate in questo campo e realizzerà un progetto

riguardante le garanzie di eventual consistency e strong consistency sul raggiungimento di stati comuni per CRDT.

Title: *Distributed computations and consistency*
Distributed computations, such as those required to maintain distributed ledgers as permitted by blockchain-based technologies, typically present the problem of ensuring the consistency of local states, or similarly of local views on the global state, of the nodes (or agents) involved in the computation, so that even if some local computations are not immediately integrated into the global state, the overall system can converge to a shared solution. In particular, the search on Conflict-free Replicated Data Types (CRDTs) has set a framework for defining data types, whose manipulations are fundamentally additive, so as to allow at any time to continue the computation until reaching a consensus on the final state. [SPBZ11a].
Through these techniques, guarantees are obtained of eventual consistency, i.e. agents are able to complete a computation so that they all agree on the final state. This has highlighted some shortcomings related to the guarantee of eventual consistency, and has led to the proposal of a notion of strong consistency, in which every stable state is secure, i.e. all the transactions reported in the ledger are legal, with high probability [GKL15].
In this path of excellence, the student will analyze existing literature, will become familiar with the technologies used in this field and will carry out a project regarding guarantees of eventual consistency and strong consistency on the achievement of common states for CRDTs.

[GKL15] Christian Decker, Jochen Seidel, and Roger Wattenhofer. 2016. Bitcoin meets strong consist-ency. In *Proc. ICDCN '16*). ACM, Article 13, DOI:https://doi.org/10.1145/2833312.2833321

[GKL15] Garay J., Kiayias A., Leonardos N. (2015) The Bitcoin Backbone Protocol: Analysis and Applications. In: Oswald E., Fischlin M. (eds) *Advances in Cryptology - EUROCRYPT 2015*. EUROCRYPT 2015. Lecture Notes in Computer Science, vol 9057. Springer, Berlin, Heidelberg

[SPBZ11a] Shapiro M., Preguiça N., Baquero C., Zawirski M. (2011) Conflict-Free Replicated Data Types. In: Défago X., Petit F., Villain V. (eds) *Proc. SSS 2011*. Lecture Notes in Computer Science, vol 6976. Springer, Berlin, Heidelberg

***

Docente: Nicola Galesi
Magistrale [at most 2]
From Complexity Theory to Logic and back.

The activity's goals is to understand the relations between lower bounds in Complexity Theory and lower bounds in Proof Complexity.
The work will consist in understanding precisely a technique to prove lower bounds for the complexity of proving theorems in
a specific proof system using known lower bounds for models of computations.

Dalla Teoria della Complessità alla Logica e viceversa.
L'obiettivo dell'attività é quello di di capire le relazioni tra risultati di limitatezza in Teoria della Complessità e Complessità delle Dimostrazioni.

Il lavoro consiste nel comprendere precisamente una tecnica per dimostrare un limite inferiore per la complessità delle dimostrazioni di un teorema
in un sistema di dimostrazione concreto usando risultati di limitatezza per modelli di calcolo.

***

Docenti Dottorato (Chiara Petrioli e Nicola Galesi)
Titolo: Sapersi muoversi nella mondo della Ricerca e Innovazione

Finalità (per la commissione di CAD): Un percorso di eccellenza super partes e ortogonale a tutti gli altri (fatto con la con la collaborazione di tutti i gruppi di ricerca), che dovrebbe essere parte di ogni percorso di eccellenza (e non esclusivo) al fine di educare i nostri migliori studenti di magistrale (potenziali studenti di PhD) a riconoscere qualità nella Ricerca e Innovazione
e a sapersi muovere nelle decisioni che li riguardano sul mondo delle ricerca.

Titolo: Sapersi muoversi nella mondo della Ricerca e Innovazione
Lo studente potrà scegliere in modo flessibile tutte o alcune tra le seguenti attività:
- Incontri finalizzati alla comprensione della propria attitudine alla ricerca, del come sviluppare il talento per lavorare in R&D e della rete die eccellenza della ricerca internazinale .
- Meeting con PI's di progetti internazionali del dipartimento: Come sfruttare le proprie idee e capacità di innovazione per ottenere finanziamenti per la ricerca.
- Partecipazione a seminari su argomenti avanzati di ricerca e mini-corsi aperti solo a studenti di dottorato.
- Partecipazione attiva a Laboratori di Problem Solving di vari gruppi di ricerca disponibili.
- Partecipazione aperta a seminari sulla ricerca attuale nel dipartimento organizzati dai diversi gruppi di ricerca

Title: Understanding Research and Innovations:
The student will be able to flexibly select all or part of these activities:
- What are the needed skills, which talents to develop to work in R&D, where is innovation developed in the world
- Problem Solving Lab (with at least 3 different topic areas)
- Possible participation to CS Colloquium and to Advanced mini course on breakthrough topics in CS typically opened only to PhD students
- Which innovations happens here? Seminar on research currently on going in the department.
- How to fund and exploit your ideas: true and fakes in the information you're exposed to, opportunities and challenges if you become an innovator. This activity will involve meetings with PIs of projects, external experts from highly innovative industries and experts of exploitation and valorization of innovations.

***

Docente: Lorenzo Carlucci

Ramsey Theory and Computability

The study of the effective (or computable) content of combinatorial principles is an active area of research at the crossroads of combinatorics, computability and logic. The focus is on theorems from Ramsey Theory, which have applications in many computer science contexts (e.g., program termination).
This honor program introduces the student to the main techniques and results in the field in order to tackle open problems of various difficulty.

Teoria di Ramsey e Calcolabilità

Lo studio del contenuto effettivo (o calcolabile) di principii combinatori è una vivace area di ricerca all'intersezione tra combinatoria, calcolabilità e logica. Il focus è su teoremi della Teoria di Ramsey, che trovano applicazioni in diverse aree dell'informatica (e.g., nella terminazione dei programmi). Questo percorso di eccellenza introduce lo studente alle tecniche e ai risultati principali del campo nella prospettiva di affrontare problemi aperti di varia difficoltà.

***

Docente: Luigi Vincenzo Mancini

Per studenti della laurea magistrale in Informatica. Percorso di eccellenza magistrale
Argomento: Blockchain Technologies
Studio della struttura blockchain e delle applicazioni che rende possibili, quali le monete virtuali (Bitcoin e derivati) e smart contracts (Ethereum). Analisi di possibili estensioni future e nuove applicazioni che possono beneficiare dell'uso di blockchain.

Topic: Blockchain Technologies
Study the structure of blockchain and its applications, such as Virtual currencies (Bitcoin and derivatives) and smart contracts (e.g., Ethereum). Analysis of possible future extensions and new applications that can benefit from the use of blockchain.

Argomento: Secure Machine Learning
Studio di tecniche di machine learning, come neural networks e deep learning, dal punto di vista della sicurezza di queste ultime. Moderne applicazioni si basano sull'uso di tecniche di machine learning applicate anche a dati sensibili: dati medici, clinici, foto, registrazioni audio e video. Come e' possibile progettare reti neurali privacy-preserving che siano accurate, ma allo stesso tempo sicure? Ovvero che siano resistenti a manipolazioni esterne e riescano a preservare la privacy dei dati di training?

Topic: Secure Machine Learning
Study of machine learning techniques such as neural networks and deep learning, from the point of view of their security and privacy. Today, modern applications based on the use of machine learning techniques are applied also to sensitive data, such as: medical data, clinical, photos, audio and video recordings. How can you design neural networks privacy-preserving that are accurate and at the same time prevent the leak of sensitive data contained in the training data set? How can you design neural networks that are resistant to external manipulation, and are able to preserve the data privacy?