



## Descrierea disciplinelor din Grup G

### Geometria computațională

Geometria computațională se ocupă cu studiul algoritmilor ce pot fi definiți sub o formă geometrică.

Cele două ramuri importante sunt geometria algoritmică și modelarea geometrică. Scopul geometriei algoritmice este dezvoltarea algoritmilor eficienți și a structurilor de date necesare rezolvării problemelor definite prin intermediul obiectelor geometrice (puncte, linii, poligoane). Exemple includ calcularea înfășurătorii convexe, diagramelor Voronoi, triangularizărilor Delaunay; găsirea drumului minim, a celor mai apropiate puncte, a intersecției linie-segment, ray-casting, căutarea într-un domeniu definit, cel mai apropiat vecin și multe alte probleme care apar în o varietate de domenii, nu neapărat geometrice la origine.

Modelarea geometrică se ocupă cu modelarea prin suprafețe și curbe. Cele mai importante obiecte sunt curbele și suprafețele parametrice și sunt folosite în aplicații de inginerie pe calculator.

Cursul se folosește de trei metode de predare: prezentarea teoriei de către profesor; prezentări ale studenților la curs, bazate pe articole de cercetare de ultimă oră și dezvoltarea de către studenți a unui proiect, pornind de la teme propuse, proiecte în dezvoltare sau o nouă idee pe care pot să o propună chiar ei.

### Tehnici de Comunicare și Scriere Tehnică

Cursul de Tehnici de Comunicare și Scriere Tehnică prezintă o serie de tehnici de comunicare în scris și în persoană. Se porneste de la studiul audienței, se continuă cu realizarea unui plan de elaborare a documentelor, și apoi se detaliază etapele necesare realizării unei documentații științifice. Se schitează principiile și regulile general valabile în scrierea tehnică, de la utilizarea cuvintelor, a propozițiilor, a paragrafelor și secțiunilor, la cea a listelor, tabelelor și graficelor. Se continuă cu prezentarea unor tipuri de documentație specifice: manuale, rapoarte de laborator, postere științifice, sau propuneri de proiecte de cercetare. Se discută importanța deosebită a editării textului obținut cu verificări ale calității, ortografiei și punctuației. Cursul se încheie cu prezentarea etapelor de elaborare ale unei prezentări tehnice, și anume: documentarea prezentării, stabilirea unei metode de prezentare adecvate, realizarea tehnică propriu-zisă și în



final prezenta scenica. In cadrul acestui curs, studentii trebuie sa realizeze un document tehnic de calitate si sa sustina o prezentare individuala.

## **Categorii si Computer Science**

Cursul “Categorii si Computer Science” urmareste familiarizarea studentilor atat cu aparatul de baza conceptual al teoriei categoriilor, dar si cu tehnicile și metodele necesare abordarii anumitor tipuri de probleme ce apar frecvent in informatica, in special cele care implica considerații structurale si functionale. Continutul tematic al cursului este urmatorul: 1) Categorii, functori si transformari naturale. 2) Constructii universale. 3) Tipuri de date, algebre si inductie structurala. 4) Monade. Cursul are la bază notiuni de logica propozitionala elementara, de teoria multimilor si de matematica discreta asimilate la cursurile de Matematică 1 si Matematică 2.

## **Complemente de matematică**

Cursul “Complemente de matematică” este orientat către prezentarea unor metode matematice esențiale pentru studenții de la master (diverse discipline) interesați în rezolvarea problemelor de optimizare.

O parte a cursului prezintă metode de optimizare cu variabile numere reale reprezentând instrumente de larg interes în inginerie: programare liniară; strategii alternative de rezolvare a programelor liniare; probleme de optimizare în rețele; elemente de teoria optimizării convexe cu restricții; probleme de optimizare numerică neliniară (fără restricții și cu restricții); metode de penalizare pentru minimizarea cu restricții. Se explicitează relații de bază existente între teoria grafurilor și optimizare.

A doua parte a acestui curs este orientată către prezentarea unor conexiuni dintre logică și optimizarea discretă. Se introduc noțiuni de bază de logică matematică și relația lor cu optimizarea: calcul propozițional; calcul cu predicate; consistență și satisfiabilitate; forme normale de formule; lema de interpolare a lui Craig; mulțimi complete de conectori logici; logică clauzală și rezoluție; testarea satisfiabilității prin algoritmi în timp polinomial; satisfiabilitatea teoriilor clauzale și optimizare discretă.

## **Criptografie**

Cursul de “*Criptografie*” își propune să prezinte, din punct de vedere teoretic și practic, tehnicile și metodele criptografice necesare asigurării securității informației din perspectiva confidențialității, integrității, autenticității și nonrepudierii informației. Cursul abordează ambele



domenii ale criptologiei: criptografia (proiectarea de sisteme) și criptanaliza (spargerea sistemelor). Astfel, sunt abordate, din ambele perspective, **sistemele clasice de cifrare** (sisteme ce utilizează, de regulă, substituții, simple sau digrafice, precum și transpoziții), **sistemele criptografice asimetrice** (sisteme ce își bazează securitatea pe dificultatea rezolvării anumitor probleme computaționale, cum ar fi spre exemplu factorizarea numerelor mari (RSA), problema logaritmului discret (ElGamal), curbele eliptice), precum și **sistemele criptografice simetrice** (sisteme pentru care este realizată o estimare a nivelului de securitate prin raportarea la cantitatea minimă necesară de informație pentru efectuarea unei căutări a cheii mai rapidă decât căutarea exhaustivă). Totodată, sunt prezentate tehnici și protocoale criptografice destinate managementului cheilor criptografice, cum ar fi, spre exemplu, infrastructurile cu chei publice (PKI).

## **Type systems and functional programming**

Functional programming. Untyped Lambda Calculus. Recursion and fixed-point combinators. Operational semantics as a language specification tool. Typed Lambda Calculus. The "type system" concept. Particular monomorphic types: Boolean, natural numbers, product. Recursive types: lists. Parameterized polymorphism. System F. Type reconstruction: unification, principal types, typing rules. The Fw system. Particular problems: types, classes and functors in Haskell.

## **Security of eHealth Systems**

The course presents the main concepts of eHealth systems, the security of eHealth systems, and standards for interoperability of eHealth applications.

The first part of the course introduces fundamental topics: eHealth terminology and eHealth application types, eHealth standards, interoperability and security issues.

The second part presents the most important standards used for eHealth applications, i.e. ISO/IEEE 11073 and the HL7 family of standards, and introduces a hands-on security analysis of IEEE 11073 and HL7 message protocols, types of attacks on eHealth systems, medical data privacy, sensitive data access control policies and protection methods (e.g. data encryption, biometric authentication, role/attribute policies).

See the course syllabus: [Security of eHealth Systems](#)



Universitatea POLITEHNICA  
din București



Facultatea de AUTOMATICĂ  
și CALCULATOARE

## **Introducere în Quantum Computing**

Acest curs prezintă o introducere în domeniul informației cuantice și al calculului cuantic, fiind structurat în 4 părți: Elemente de mecanică cuantică, Informație cuantică, Circuite cuantice și Algoritmi cuantici.