Theoretical Computer Science

@ Dipartimento di Informatica

Università di Verona

http://www.di.univr.it/

11 Aprile 2017

People

M.Paola Bonacina
Andrea Masini
Ugo Solitro

Logic

Alessandra Di Pierro
Andrea Masini

Mila Dalla Preda
Alessandra Di Pierro
Roberto Giacobazzi
Isabella Mastroeni
Massimo Merro
Roberto Segala
Nicola Fausto Spoto

Zsuzsanna Liptak
Roberto Posenato
Romeo Rizzi

Semantics

Formal Methods

Algorithms

Quantum Computing

Outline

Semantics

Provides rigorous foundations for

- Software Engineering (formal methods for analysis and verification)
- Programming Languages (concurrency, quantum and probabilistic λ-calculus)
- CPS, IoT, ...

Outline

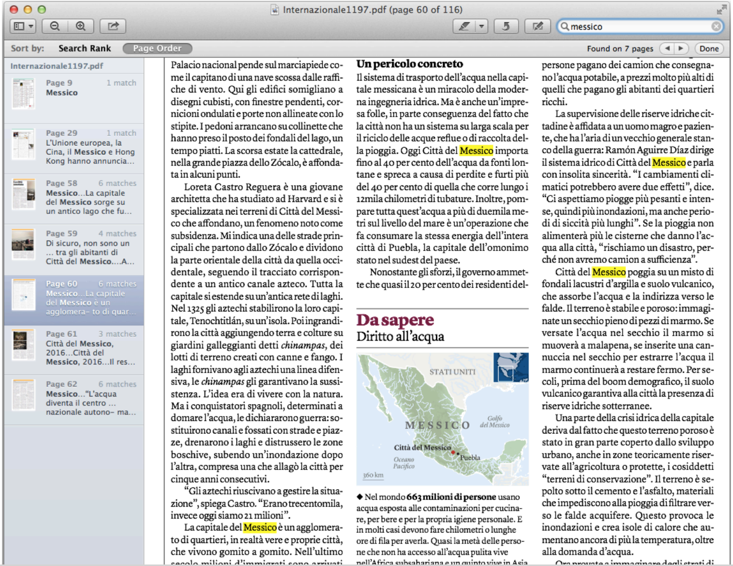
1. Semantics
2. Algorithms
3. Logic
4. Quantum Computing

Why study strings?

Text data (sequences of symbols)

- natural language (books, webpages, emails, . . .)
- biological sequence data (DNA sequences, protein sequences, . . .)
  All modern biological and medical research relies on sequence data!
- program code
- music
- time series
- multimedia streams
- any data that is stored in a file
- . . .

A Common Problem: Pattern Matching



Palacio nacional pende sul marciapiede come il capitano di una nave scossa dalle raffiche di vento. Qui gli edifici somigliano a disegni cubisti, con finestre pendenti, cornicioni ondulati e porte non allineate con lo stipite. I pedoni arrancano su collinette che hanno preso il posto dei fondali del lago, un tempo piatti. La scorsa estate la cattedrale, nella grande piazza dello Zócalo, è affondata in alcuni punti.

Loreta Castro Reguera è una giovane architetta che ha studiato ad Harvard e si è specializzata nei terreni di Città del Messico che affondano, un fenomeno noto come subsidenza. Mi indica una delle strade principali che partono dallo Zócalo e dividono la parte orientale della città da quella occidentale, seguendo il tracciato corrispondente a un antico canale azteco. Tutta la capitale si estende su un'antica rete di laghi. Nel 1325 gli aztechi stabilirono la loro capitale, Tenochtitlán, su un'isola. Poi ingrandirono la città aggiungendo terra e colture su giardini galleggianti detti *chinampas*, dei lotti di terreno creati con canne e fango. I laghi fornivano agli aztechi una linea difensiva, le *chinampas* gli garantivano la sussistenza. L'idea era di vivere con la natura. Ma i conquistatori spagnoli, determinati a domare l'acqua, le dichiararono guerra: sostituirono canali e fossati con strade e piazze, drenarono i laghi e distrussero le zone boschive, subendo un'inondazione dopo l'altra, compresa una che allagò la città per cinque anni consecutivi.

"Gli aztechi riuscivano a gestire la situazione", spiega Castro. "Erano trecentomila, invece oggi siamo 21 milioni".

La capitale del Messico è un agglomerato di quartieri, in realtà vere e proprie città, che vivono gomito a gomito. Nell'ultimo secolo milioni d'immigrati sono arrivati

Un pericolo concreto

Il sistema di trasporto dell'acqua nella capitale messicana è un miracolo della moderna ingegneria idrica. Ma è anche un'impresa folle, in parte conseguenza del fatto che la città non ha un sistema su larga scala per il riciclo delle acque reflue o di raccolta della pioggia. Oggi Città del Messico importa fino al 40 per cento dell'acqua da fonti lontane e spreca a causa di perdite e furti più del 40 per cento di quella che corre lungo i 12mila chilometri di tubature. Inoltre, pompare tutta quest'acqua a più di duemila metri sul livello del mare è un'operazione che fa consumare la stessa energia dell'intera città di Puebla, la capitale dell'omonimo stato nel sudest del paese.

Nonostante gli sforzi, il governo ammette che quasi il 20 per cento dei residenti del-

Da sapere

Diritto all'acqua

STATI UNITI
MESSICO
Golfo del Messico
Città del Messico
Puebla
Oceano Pacifico
360 km

◆ Nel mondo **663 milioni di persone** usano acqua esposta alle contaminazioni per cucinare, per bere e per la propria igiene personale. E in molti casi devono fare chilometri o lunghe ore di fila per averla. Quasi la metà delle persone che non ha accesso all'acqua pulita vive nell'Africa subsahariana e un quinto vive in Asia

persone pagano dei camion che consegnano l'acqua potabile, a prezzi molto più alti di quelli che pagano gli abitanti dei quartieri ricchi.

La supervisione delle riserve idriche cittadine è affidata a un uomo magro e paziente, che ha l'aria di un vecchio generale stanco della guerra: Ramón Aguirre Díaz dirige il sistema idrico di Città del Messico e parla con insolita sincerità. "I cambiamenti climatici potrebbero avere due effetti", dice. "Ci aspettiamo piogge più pesanti e intense, quindi più inondazioni, ma anche periodi di siccità più lunghi". Se la pioggia non alimenterà più le cisterne che danno l'acqua alla città, "rischiamo un disastro, perché non avremo camion a sufficienza".

Città del Messico poggia su un misto di fondali lacustri d'argilla e suolo vulcanico, che assorbe l'acqua e la indirizza verso le falde. Il terreno è stabile e poroso: immaginate un secchio pieno di pezzi di marmo. Se versate l'acqua nel secchio il marmo si muoverà a malapena, se inserite una cannuccia nel secchio per estrarre l'acqua il marmo continuerà a restare fermo. Per secoli, prima del boom demografico, il suolo vulcanico garantiva alla città la presenza di riserve idriche sotterranee.

Una parte della crisi idrica della capitale deriva dal fatto che questo terreno poroso è stato in gran parte coperto dallo sviluppo urbano, anche in zone teoricamente riservate all'agricoltura o protette, i cosiddetti "terreni di conservazione". Il terreno è sepolto sotto il cemento e l'asfalto, materiali che impediscono alla pioggia di filtrare verso le falde acquifere. Questo provoca le inondazioni e crea isole di calore che aumentano ancora di più la temperatura, oltre alla domanda d'acqua.

Jumbled Pattern Matching

In one variant, we are looking for all permutations (“jumbles”) of the pattern:

`messico, sesicom, ocsimec, ...`

Parikh vector $p(t)$: $p(aabacc) = (3, 2, 1)$

Jumbled Pattern Matching

Given strings s (the text) and t (the pattern).

Find all occurrences of substrings u of s s.t. $p(u) = p(t)$.

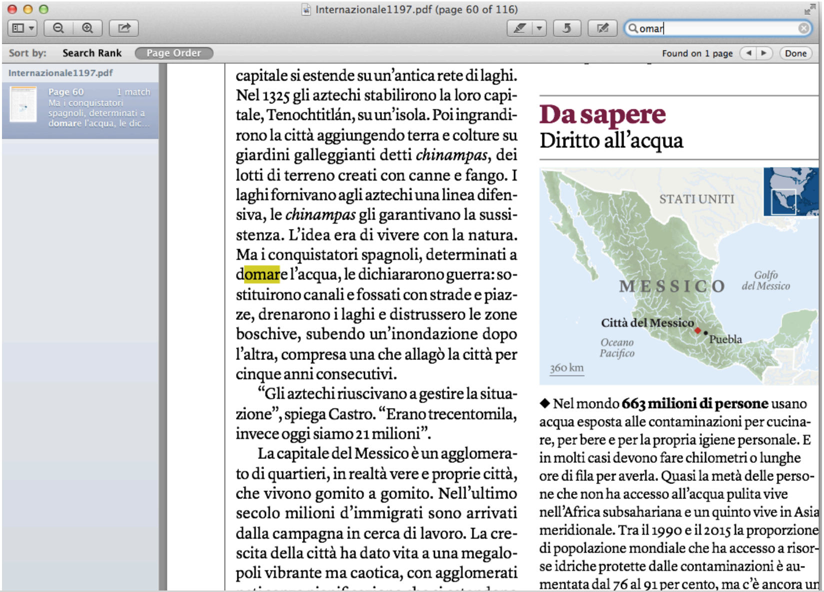
Ex.: $\Sigma = \{a, b, c\}$, query $t = aabacc$

b b a c a c c a b a b b a b c c a a a c

Goal

Find efficient algorithms for this problem! (applications in Comp. Biol.)

Find all jumbled matches of `roma`: `amro`, `omar`, `ramo`, ...



Prefix normal words

In the context of JPM (jumbled pattern matching) for binary strings the following definition turns out to be useful:

Definition

A binary word s is a prefix normal word (w.r.t. 1) if no substring has more 1's than the prefix of the same length.

Example

$$s = 1010011011000111 0010 \quad NO$$

$$s' = 1110100101100101 0010 \quad YES$$

Where you can learn more about this

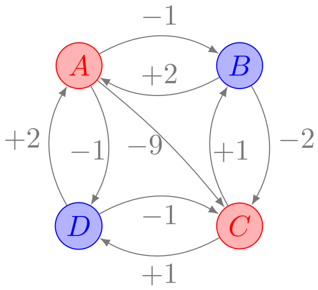
Master in Medical bioinformatics

"Computational Analysis of Genomic Sequences"

(= "Computational methods for textual big data"
= "Metodi di analisi testuale per big data")

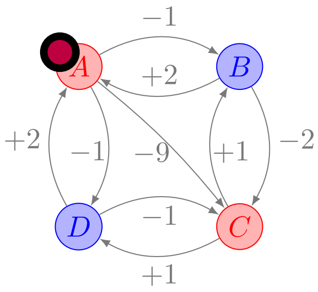
Zsuzsanna Liptak

Mean Payoff Games



- A *Mean-Payoff Game* (MPG) is a two-player game played on an *arena* $\Gamma = \langle V, E, w, (V_{\texttt{Max}}, V_{\texttt{Min}})\rangle$.
- $G^{\Gamma} = \langle V, E, w\rangle$ is a finite weighted directed graph whose nodes are partitioned in two classes, $V_{\texttt{Max}}$ and $V_{\texttt{Min}}$.
- Every node has at least one outgoing edge.
- Weights are integers, i.e., $w : E \to \mathbf{Z}$.
- Nodes in V_p, where $p \in \{\texttt{Max}, \texttt{Min}\}$, are those under control of Player p.

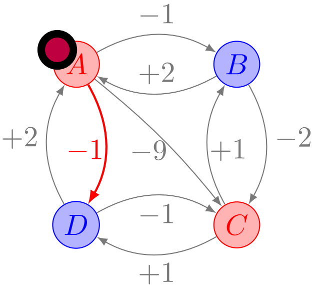
Mean Payoff Games: play example



- Each match starts with a pebble placed at some node $v \in V_{\mathtt{Max}} \cup V_{\mathtt{Min}}$.
- Here $v = A \in V_{\mathtt{Max}}$, the nodes controlled by Player $\mathtt{Max}$.

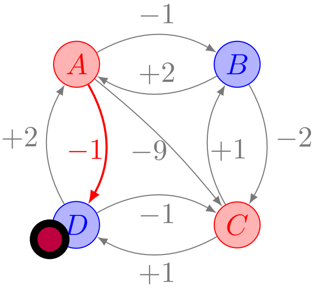
  Player $\mathtt{Max}$ chooses an $e \in E$ exiting v and moves the pebble along e.

Mean Payoff Games: play example



- Each match starts with a pebble placed at some node $v \in V_{\mathtt{Max}} \cup V_{\mathtt{Min}}$.
- Here $v = A \in V_{\mathtt{Max}}$, the nodes controlled by Player Max.
- Player Max chooses an arc $e \in E$ exiting v and moves the pebble along e.

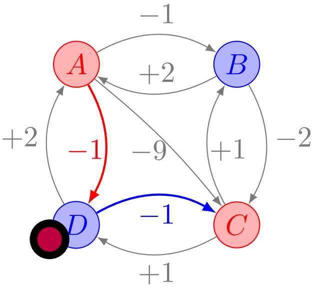
Mean Payoff Games: play example



- When the pebble is in a node $v \in V_p$, the turn is to Player p.
- Here $v = D \in V_{\texttt{Min}}$, the nodes controlled by Player `Min`.

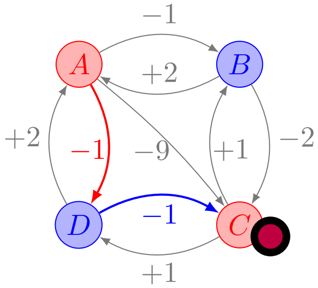
  Player `Min` chooses an $e \in E$ exiting v and moves the pebble along e.

Mean Payoff Games: play example



- When the pebble is in a node $v \in V_p$, the turn is to Player p.
- Here $v = D \in V_{\texttt{Min}}$, the nodes controlled by Player `Min`.
- Player `Min` chooses an arc $e \in E$ exiting v and moves the pebble along e.

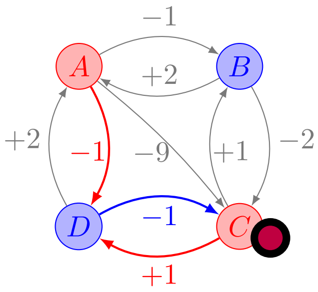
Mean Payoff Games: play example



- When the pebble is in a node $v \in V_p$, the turn is to Player p.
- Here $v = C \in V_{\mathtt{Max}}$, the nodes controlled by Player `Max`.

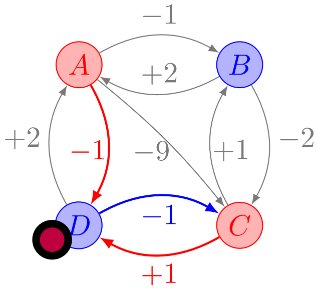
  Player `Max` chooses an $e \in E$ exiting v and moves the pebble along e.

Mean Payoff Games: play example



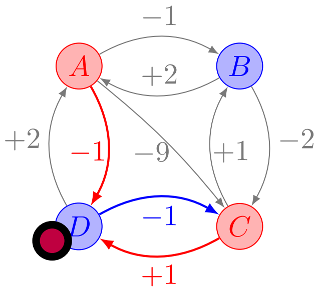
- When the pebble is in a node $v \in V_p$, the turn is to Player p.
- Here $v = C \in V_{\texttt{Max}}$, the nodes controlled by Player `Max`.
- Player `Max` chooses an arc $e \in E$ exiting v and moves the pebble along e.

Mean Payoff Games: play example



- The two players move the pebble until a cycle $\mathcal{C}$ is eventually closed.
- The sequence of encountered nodes, i.e., $\pi = v_0 v_1 \cdots v_n \cdots = ADCD$ is a named a *play*.
- In this case, the cycle is $\mathcal{C} = DCD$.

Mean Payoff Games: play example



- In order to play well, Player Max wants to:

$$\texttt{maximize} \text{ the average weight } \frac{w(\mathcal{C})}{|\mathcal{C}|} \text{ of that cycle.}$$

- and Player Min wants to minimize the average weight of that cycle $\mathcal{C}$.

Algorithms and Complexity for:

1. Games on Finite Graphs (Games for Formal Verification) [*Grädel, 2002*]
2. Temporal Constraint Networks (Temporal Planning and Scheduling) [*Dechter, 1991*]

Announcement

On **Wed. 19 April**, *Dr. Giorgio Audrito* (University of Torino) will give a seminar on Parity Games.

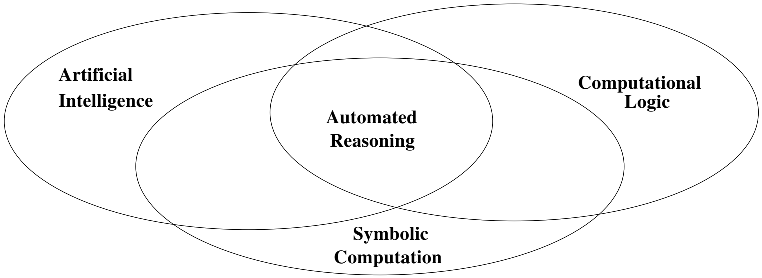
Outline

Machine Intelligence

"... The study is to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves."

(From John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon, Proposal for the Dartmouth Conference on AI, 1955)

Automated Reasoning



- Precisely described: symbols
- Symbolic reasoning: Logico-deductive, Probabilistic ...

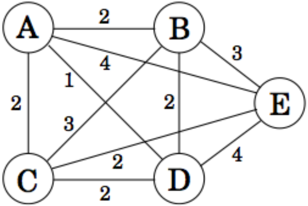
Logico-deductive Reasoning

- Theorem Proving, Constraint Solving or Model Finding: Inference and Search
- $\mathcal{T} \models \varphi$, $y \simeq x \vee y \simeq z$, $\mathcal{T}$-model of φ, $x^2 + y^2 \leq 1 \vee xy > 1$, $\neg L_1 \vee Q_2 \ldots \vee Q_k$, explain, learn, backjump, $a \sqsubseteq b$, $f \vee \neg e \vee \neg b$, conflict, $\mathcal{T} = \bigcup_{i=1}^{n} \mathcal{T}_i$, resolution, linear arithmetic, $\simeq$, SAT, expansion, contraction, bit-vectors, ...
- Logic: a Machine Language
- Applications: Verification, Natural Language, Computer Mathematics, Education, ...

Outline

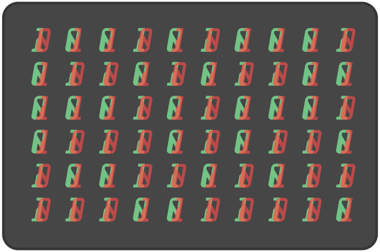
The Quest for Quantum Computers

There exist problems so complex, so inscrutable, that to solve them would take current computers more time than the current age of the universe—or even longer.



Quantum Computers

Will we ever be able to defeat exponentiality?



Qantum Computer

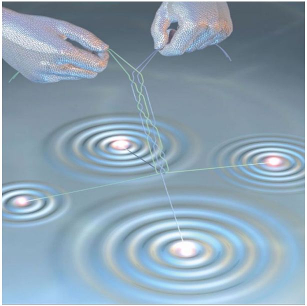
Factorisation $\Rightarrow$ ~~RSA~~

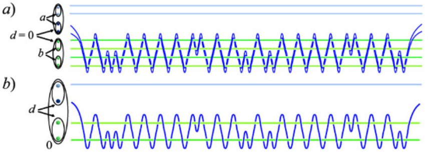
The D-Wave System

Optimisation problems $\Rightarrow$ Machine Learning

The Quest for Topological Quantum Computers

Processors working according to the rules of quantum mechanics are extremely delicate objects. TQC is a scheme to perform quantum computation in a way that is naturally immune from errors. This is because operations are carried out by *braiding* particles.



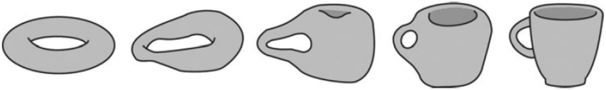


$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{pmatrix} \qquad \begin{pmatrix}-1&0\\0&-1\end{pmatrix}$$

New algorithmic techniques, new hints for Quantum Machine Learning.

Topology

Topology is the part of geometry which survives deformation/perturbation.



Topological properties of quantum systems are robust to perturbation/deformation.

Anyons

Frank Wilczek, Nobel prize in Physics 2004, coined the word **anyons** for the physical particles with such a topological behaviour.

Do anyons exist, outside of theorists' imaginations?

Conclusion

In Frank Wilczek' words

Everything not forbidden is compulsory.

Nature, in her abundance, provides materials to embody all theoretically consistent possibilities. Trusting in that principle, I strive to exercise what Richard Feynman called “imagination in a straitjacket”.