

API

Brevi commenti sulla ricerca in corso
e sulle applicazioni dell'informatica
teorica

Automati e model checking

- Gli FSA sono alla base del *model checking*
 - Tecnica per verificare automaticamente le proprietà di correttezza di sistemi a stati finiti
 - Proprietà specificate in logica
 - Per le formule di logica temporale, Clarke, Emerson e Sifakis sono stati insigniti del prestigioso Turing Award nel 2007 per il loro lavoro sul model checking

Specifiche

- Tecniche di dimostrazione automatica di teoremi per garantire certe condizioni
- Tecnica di base: asserzioni (disponibili in tutti i linguaggi moderni)
- Esempi di linguaggi e strumenti di specifica ad hoc:
 - **Java Modeling Language (JML)**, con pre- e postcondizioni e invarianti, secondo il paradigma del design by contract.
 - **Code contracts** (design-by-contract programming per .NET)
- Esempio di strumenti di verifica:
 - **ESC/Java2** ("Extended Static Checker for Java") e i suoi successori (OpenJML)

Altre applicazioni

- Teoria della complessità un po' ovunque
 - Decidibilità di problemi (non solo l'arresto, ma letteralmente migliaia di problemi)
 - Riduzioni da/verso altri problemi
- Connessione stretta tra automi, grammatiche e compilatori
- Importanza delle strutture dati (autoevidente)

Turing award

- Compilatori: Perlis (1966), Cocke (1987), Allen (2006)
- Algoritmi: Dijkstra (1972), Knuth (1974), Hopcroft&Tarjan (1986), Aho&Ullman (2020)
- Grammatiche: Backus (1977), Naur (2005)
- Specifica/verifica: Hoare (1980), Pnueli (1996), Clarke&Emerson&Sifakis (2007)
- Complessità e computabilità: Rabin&Scott (1976), Cook (1982), Karp (1985), Hartmanis&Stearn (1993), Blum (1995), Chi-Chih Yao (2000), Valiant (2008), Micali&Goldwasser (2012), Hellman&Diffie (2015), Wigderson (2023)

Millennium Problems

- P vs NP (introdotto da S. Cook nel 1971)
 - E' uno dei 7 “Millennium problems” del Clay Mathematics Institute
 - <https://www.claymath.org/millennium/p-vs-np/>
 - Formalmente: la classe dei problemi risolvibili in tempo polinomiale con una TM deterministica è la stessa della classe di problemi risolvibili in tempo polinomiale con una TM non deterministica?
- (Molto) informalmente: la classe dei problemi facili da risolvere e dei problemi facili da verificare sono equivalenti?

Folklore e stranezze

- Recentemente: centenario di Turing (2012)
- Biografia interessante...
 - Test di Turing, macchina di Turing, ...
 - Ma anche: lavoro a Bletchley Park durante la seconda guerra mondiale per infrangere il codice della macchina Enigma, arresto, trattamento ormonale (che gli provocò impotenza e ginecomastia), morte dovuta ad avvelenamento (suicidio?), ...
- Rappresentato al cinema:
 - Enigma (2001), di M. Apted, con D. Scott e K. Winslet (in modo molto vago e parziale)
 - The imitation game (2014), di M. Tyldum, con B. Cumberbatch e K. Knightley
- Scuse del governo (una storia infinita):
 - Petizione per scuse postume a Turing (2011)
 - ... richiesta respinta (2012)
 - ... introduzione di un disegno di legge per il perdono del reato (2013)
 - ... perdono divenuto definitivo per intervento della regina sotto la prerogativa reale della grazia

Folklore e stranezze (continua...)

- Altra biografia interessante...
 - Kurt Gödel
 - Entro i 25 anni dimostrò i suoi due teoremi di incompletezza, che risolsero (negativamente) secoli di dibattiti sul potere della logica matematica
 - Sviluppò gravi sintomi paranoici quando il filosofo Moritz Schlick fu assassinato da uno dei suoi studenti
 - Durante la seconda guerra mondiale lasciò Vienna per Princeton, dove strinse un'amicizia con Einstein
 - Fece domanda per la cittadinanza americana e, nel colloquio tentò di dimostrare che la costituzione americana era logicamente inconsistente e poteva portare alla dittatura...
 - Diventò ossessionato dall'idea di essere avvelenato e mangiava solo cibo preparato dalla moglie. Quando questa fu ricoverata per 6 mesi, si lasciò morire d'inedia
- Raramente rappresentato nei film:
 - I.Q. (1994), di F. Schepisi, con T. Robbins, M. Ryan, e W. Matthau
- Altri risultati fondamentali:
 - Dimostrò che l'assioma della scelta (AC) non può essere confutato nell'insiemistica comunemente accettata (ZF)
 - Dimostrò che l'ipotesi del continuo (CH) non può essere confutata in ZFC (cioè ZF+AC)
 - (Paul Cohen dimostrò che CH non può essere neanche dimostrato, cioè è indipendente)
 - Sviluppò una «prova» ontologica dell'esistenza di dio...
 - Apparato di assiomi di logica modale che distinguono ogni proprietà in positiva o negativa. Dio è definito come un ente con tutte e sole le proprietà positive... poiché l'esistenza necessaria è una proprietà positiva, allora in ogni mondo possibile c'è un (oggetto simile a) dio... collasso modale... inconsistenza... dimostrazione automatica

Letture consigliata

- Le biografie dei protagonisti del sogno di Leibniz sono mirabilmente descritte da Martin Davis nel libro:
 - «Il calcolatore universale. Da Leibniz a Turing»
(Adelphi, 2^a edizione, 2012)

Sul mercato del lavoro

- Vorreste lavorare per una grande azienda il cui cardine sia l'analisi di grandi quantità di dati?
- Non vi chiederanno banalmente di elencare 3 punti forti e 3 punti deboli del vostro CV...
- Invece vi chiederanno di:
 - **formalizzare e risolvere**, al volo, problemi non banali (tipicamente **NP-difficili**)
 - Fornire euristiche adeguate
 - Determinare **complessità asintotica** e soluzioni alternative per casi semplici