Da Aristotele al computer.

Elio Giovannetti
Dipartimento di Informatica
Università degli Studi di Torino

1. Introduzione alla logica proposizionale: tavole di verità.
versione 07/02/2014

Copia delle slides ed eventualmente altro materiale:

http://www.di.unito.it/~elio/lezioni-liceo/

Il titolo (non il contenuto) si ispira ad una conferenza del 2011 di Tony Hoare, uno dei grandi padri fondatori dell'Informatica:
"Great Ideas of Computer Science From Aristotle to Euclid"

Introduzione

Una parola importante.

Un procedimento di calcolo è quello che noi oggi chiamiamo con una parola che ultimamente è diventata molto popolare:

Algoritmo

Da dove viene questa parola (etimologia)?

الخوارزمي

I M Z R AV K_h LA

al-Khvarismi

Matematico uzbeko-persiano , vissuto intorno all'anno 800 d.C, il cui libro "Calcoli con i numerali indiani" descriveva appunto gli algoritmi di calcolo per le operazioni aritmetiche con il sistema di numerazione indiano, cioè quelli che ancora oggi studiamo nella scuola elementare.

Un francobollo sovietico dell'Uzbekistan

fonte wikipedia

Mukhammed al'-Khorezmi

L'algoritmica moderna.

- l'*algoritmica*, ovvero la scienza degli algoritmi, è fin dagl'inizi dell'informatica una delle sue discipline centrali, ancora oggi attivo campo di ricerca.

Donald Knuth, padre dell'algoritmica moderna, autore dell'opera in più volumi
The Art of Computer Programming

Un complesso di edifici (a Sophia Antipolis, Antibes)

Che cos'è un algoritmo?

Un algoritmo è una procedura di calcolo ben definita che prende in ingresso un certo dato o insieme di dati, e genera in uscita un dato o insieme di dati costituente il risultato.

O anche:

Un algoritmo è una sequenza finita di istruzioni (comprendente eventualmente istruzioni di ripetizione, di decisione, ecc.) eseguendo la quale si ottiene, a partire dai dati in ingresso, il risultato in un numero finito di passi elementari.

Il procedimento di calcolo deve poter essere eseguito meccani-camente, senza alcuna creatività, senza "pensare".

I procedimenti di calcolo in colonna per le quattro operazioni, imparati alla scuola elementare, sono algoritmi.

Il procedimento effettuato dai computer di Google per trovare il percorso più corto o più veloce fra due località è un algoritmo.

Meccanica e macchine.

Proprio perché il calcolo deve essere meccanico, si presta ad essere eseguito con l'ausilio di strumenti inventati allo scopo, cioè con l'ausilio di una macchina (μηχανή).

Nota Bene

I greci e i romani non avevano la notazione posizionale dei numeri: come riuscivano a fare le operazioni aritmetiche?

Usavano uno strumento "meccanico": l'abaco!

Ricorda: *calculi* sono i ciottoli che si usano nell'abaco.

L'abaco è un antenato del pallottoliere.

Il pallottoliere era di uso comune ed intensivo, fino a non molti decenni fa, in Cina, Russia, e altri paesi.

Calcolare e ragionare

L'agorà greca:

- piazza del mercato - *forse si usava l'abaco?*
- luogo delle discussioni e deliberazioni politiche - *si sviluppano le arti della retorica e dell'argomentazione (come riuscire a convincere gli altri)*.

Dai modi di argomentare considerati corretti si estrassero delle forme comuni a ragionamenti su contenuti diversi (G. Longo): Le due argomentazioni:

- Socrate è uomo, tutti gli uomini sono mortali, quindi Socrate è mortale.
- Pericle è ateniese, tutti gli ateniesi sono greci, quindi Pericle è greco.

hanno la stessa forma: sono corrette in virtù della loro forma.

Il ragionamento è una forma di calcolo?

- Aristotele fu il primo (in Occidente) che si dedicò ad uno studio esplicito delle forme corrette di ragionamento.
- Anche il ragionamento corretto sembra caratterizzato dalla conformità a regole meccaniche, dunque meccanizzabile.
- È un caso che il termine

  λόγος (latino verbum, ratio)

  volesse dire sia *parola*, *ragione*, che *rapporto fra numeri*?
  In inglese il rapporto fra due quantità si dice ancora oggi *ratio*.
- Nel corso della storia è stata sempre presente la percezione di una analogia fra ragionamento e calcolo aritmetico, ed è quindi naturale che si sia sviluppata l'idea di una possibile riduzione del ragionamento a una qualche specie di calcolo ben definito: da cui, poi, ottenere una meccanizzazione del ragionamento.

Il ragionamento è una forma di calcolo?

Hobbes, a metà del '600:

"ragionare non è nient'altro che fare dei conti",

perché

"come gli studiosi di aritmetica insegnano ad addizionare e sottrarre coi numeri, e i geometri insegnano la stessa cosa con le linee, le figure, gli angoli [...], così i logici insegnano la stessa cosa con le conseguenze delle parole, sommando insieme due nomi per costruire una proposizione, e due proposizioni per costruire un sillogismo, e molti sillogismi per costruire una dimostrazione; ..."

Thomas Hobbes, 1588 -1679

Il ragionamento è una forma di calcolo?

Leibniz, 1677:

"Il est manifeste, que si l'on pouvoit trouver des caractères ou signes propres à exprimer toutes nos pensées aussi nettement et exactement que l'arithmétique exprime les nombres ou que l'analyse geométrique exprime les lignes, on pourroit faire en toutes les matières autant qu'elles sont sujettes au raisonnement tout ce qu'on peut faire en Arithmétique et en Géométrie."

Ancora Leibniz:

"Quo facto, quando orientur controversiae, non magis disputatione opus erit inter duos philosophos, quam inter duos computistas. Sufficiet enim calamos in manus sumere sedereque ad abacos, et sibi mutuo (accito si placet amico) dicere: calculemus!"

Gottfried Wilhelm von Leibnitz, 1646 -1716

Il ragionamento è una forma di calcolo?

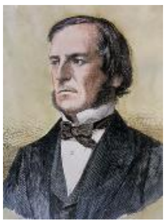
Dal Seicento all'Ottocento:

George Boole, The Laws of Thought (Le leggi del pensiero), Cork (Inghilterra), 1854.

È considerato il fondatore della logica proposizionale: il calcolo logico inventato da Boole può essere visto come un calcolo analogo a quelli aritmetici, fondato su una struttura matematica ben precisa che viene detta, in suo onore, algebra di Boole.

Ancora oggi, in tutti i linguaggi di programmazione ("tipati") esiste un tipo di dato che si chiama boolean, che è costituito da due elementi: true e false.

Affrontiamo lo studio di tale logica secondo gli approcci che sono oggi usuali.



George Boole, 1815 -1864

Verso la logica proposizionale

"Che cos' è la verità?" (Ponzio Pilato)

L'aggettivo "vero" e il sostantivo "verità", e i loro analoghi nelle altre lingue antiche e moderne, hanno molteplici significati.

- "vero" in italiano può significare, ad es., "autentico", cioè il contrario di "finto", "contraffatto":
  oro vero, amore vero, rolex vero, ecc.
- così "falso" può significare "finto", "contraffatto":
  falso oro, falso amore, rolex falso, ecc.
- "true" (vero) in inglese significa anche "fedele":
  But I'm always true to you, in my fashion (Ella Fitzgerald)
  (ma ti sono sempre fedele, a modo mio)
- "faux" (falso) in francese significa anche "sbagliato":
  le numéro de téléphone que tu m'as donné est faux
  (il numero di telefono che mi hai dato è sbagliato)

Logica: significato delle parole "vero" e "falso".

"True and False are attributes of speech, not of things.
And where speech is not, there is neither Truth or Falsehood."
Thomas Hobbes

Parole e cose: verità come corrispondenza coi fatti.

- La nozione di verità che interessa la logica è una proprietà di proposizioni o enunciati, cioè di particolari espressioni linguistiche, non una proprietà di "cose" in generale, se non nel senso che anche le frasi che diciamo o scriviamo sono "cose".
- Essa ha subito, nel corso della storia dall'antichità fino ai giorni nostri, numerose trasformazioni sia in filosofia che in logica, in matematica, e nelle scienze.
- Partiamo da una nozione di verità nel senso comune.
  Una proposizione (o enunciato, o asserzione) enuncia che nella realtà certe cose stanno in un certo modo:
  allora la proposizione si dice vera se nella realtà le cose stanno davvero (!) in quel modo, si dice falsa se nella realtà le cose non stanno in quel modo.
  Nella realtà le cose o stanno in quel modo oppure no, quindi una proposizione è o vera o falsa (principio di bivalenza).

Verità come corrispondenza, nella logica moderna.

- Nella logica del '900 la tradizionale nozione di verità come corrispondenza è stata ripresa dal logico Alfred Tarski:
  La proposizione "la neve è bianca" è vera
  se e solo se la neve è bianca, altrimenti è falsa.
  La proposizione "Paolo ama Francesca" è vera se e solo se Paolo ama Francesca, altrimenti è falsa.
  (Attenzione alle virgolette!)
  Il grande logico contemporaneo J.-Y. Girard l'ha chiamata "la piatta banalità della semantica(1) tarskiana".
- In realtà Tarski diede di tale nozione una definizione tecnica rigorosa per mezzo della teoria degli insiemi, e la semantica tarskiana è servita di base al grande sviluppo della logica matematica nel '900, in particolare di alcune sue aree.

(1) Nota: la semantica è la teoria del significato

Forme linguistiche e verità.

- Non tutte le espressioni linguistiche di senso compiuto sono proposizioni che enunciano che certe cose stanno in un certo modo, e per le quali quindi si può dire che sono vere o false.
- Ad esempio un ordine può essere giusto o ingiusto, eseguito o non eseguito, ma non è né vero né falso.
- Analogamente una promessa, un articolo di legge, ecc.
- In logica si chiama proposizione, o enunciato, un'espressione di cui abbia senso affermare che è vera o falsa (anche se poi magari non è noto se sia vera o falsa).
- Tuttavia, anche per "proposizioni" per cui parrebbe aver senso parlare di verità o falsità, la bivalenza può non essere ovvia.
- Ad esempio già presso i Greci si discuteva se per una proposizione con verbo al futuro, come "domani nevicherà", abbia senso dire (oggi) che è vera o falsa.

Altre culture, altri concetti?

- Secondo alcuni studiosi, nel pensiero di una grande civiltà quale quella cinese non vi è una nozione esattamente corrispondente a quella occidentale di verità.
- I Cinesi non avrebbero "l'ossessione occidentale per la (ricerca della) verità", sarebbero invece interessati a raggiungere la "saggezza", l'armonia con il mondo.
- Altri studiosi contestano l'affermazione di una radicale alterità della cultura cinese rispetto alle culture occidentali (vedasi ad esempio l'accesa polemica sviluppatosi anni fa in area francofona fra il filosofo e sinologo francese François Jullien e il sinologo svizzero Jean-François Billeter).
- La logica matematica e più in generale le scienze e le tecnologie moderne che oggi si studiano e si usano in Cina sono comunque le stesse che in tutto il mondo.

Logica proposizionale.

- Fin dai tempi di Aristotele, la logica è la scienza che cerca di stabilire quali siano le forme corrette di ragionamento, cioè come da certe assunzioni o premesse si possano ricavare delle conclusioni, in modo che se le premesse sono vere, le conclusioni siano sicuramente vere.
- La logica proposizionale studia le forme di ragionamento che non dipendono dai componenti interni delle proposizioni elementari, ma solo dal significato di particelle come la congiunzione "e", la disgiunzione "o", ecc., quando esse sono usate per connettere proposizioni elementari.
- La logica proposizionale quindi non analizza una proposizione elementare, ad es. "la neve è bianca", o "tutti i triangoli equilateri sono equiangoli", in termini di soggetto, predicato, complementi, ecc. ma la considera come un'espressione atomica (cioè indivisibile) che può essere vera o falsa.

La congiunzione.

- La congiunzione "e" in logica è intesa nel suo significato più di base, diversamente dalle lingue naturali in cui può avere diverse sfumature di significato, ad esempio indicare una successione temporale: "scrisse una lettera e la imbucò".
- La proposizione composta "la neve è bianca e tutti i triangoli equilateri sono equiangoli" è vera perché le proposizioni componenti "la neve è bianca" e " tutti i triangoli equilateri sono equiangoli" sono vere (attenzione alle virgolette!).
- Le proposizioni composte
  "Roma è la capitale d'Italia e Ivrea si trova in Lombardia"
  "Londra è la capitale d'Italia e Ivrea si trova in Piemonte"
  "Londra è la capitale d'Italia e Ivrea si trova in Lombardia"
  sono tutte false, perché una o entrambe le componenti di ciascuna di esse sono false. Invece:

"Roma è la capitale d'Italia e Ivrea si trova in Piemonte" è vera.

La congiunzione: notazione.

- Poiché la lingua universale della scienza e dell'informatica è l'inglese, la congiunzione viene spesso indicata con "and".
- Nel '900 in logica è stato introdotto il simbolo $\wedge$, che comunque leggiamo abitualmente and (almeno in Italia).
- In alcuni testi o contesti la congiunzione è denotata dal simbolo & ("e commerciale") o addirittura && (doppio "e commerciale").
- Attenzione: quale sia il simbolo per indicare la congiunzione logica è assolutamente irrilevante. L'importante è scegliere uno e usare sempre quello, senza mescolare notazioni diverse in uno stesso testo.
- Noi useremo la notazione $\wedge$, che è quella standard in logica.

Tavole (o tabelle) di verità.

Usando delle lettere latine maiuscole per indicare proposizioni atomiche, e lettere greche per indicare proposizioni generiche, possiamo allora dire che la proposizione $\alpha \wedge \beta$ è vera se e solo se α è vera e β è vera, e in tutti gli altri casi è falsa.

Possiamo rappresentare tale banalità per mezzo di una tabella, dove F sta per falso (ingl. false) e T sta per vero (ingl. true):

α	β	$\alpha \wedge \beta$
F	F	F
F	T	F
T	F	F
T	T	T

Valori di verità e operatori logici.

- In quanto precede non vi è nulla che non sia ovvio. Facciamo tuttavia un altro piccolo passo.
- Consideriamo le abbreviazioni T ed F come due nuovi "valori", cioè come una nuova specie di "numeri", costituita da due soli elementi.
- Consideriamo il simbolo $\wedge$ come un simbolo di operazione di nuovo tipo, analogo agli operatori aritmetici ò e +: un operatore logico.
- Possiamo allora riscrivere la tabella precedente come una sorta di "tabelline" (o "tavola pitagorica") di nuovo tipo, per un insieme di due valori; invece di 2ò1 = 2, 2ò2 = 4, 2ò3 = 6, ecc.:

$$F \wedge F = F$$
$$F \wedge T = F$$
$$T \wedge F = F$$
$$T \wedge T = T$$

La "aritmetica" (o meglio, l'algebra) della logica.

Per accentuare l'analogia con l'aritmetica ordinaria, indichiamo il falso con 0 e il vero con 1, e indichiamo la congiunzione con il simbolo della moltiplicazione o prodotto. Le "tabelline" della congiunzione diventano allora:

0 ò 0 = 0
0 ò 1 = 0
1 ò 0 = 0
1 ò 1 = 1

che, tra l'altro, sono anche valide nell'aritmetica ordinaria!

Nei nostri computer il vero e il falso, così come le cifre 0 e 1, sono rappresentati da due livelli di voltaggio, alto e basso; i circuiti dell'unità logico-aritmetica sono in grado di eseguire tanto le operazioni aritmetiche che le operazioni logiche.

Linguaggi di programmazione e operazioni.

- In tutti i linguaggi di programmazione vi sono operatori aritmetici e logici, e simboli relazionali come <, >, =, ecc.
- Attenzione: nei linguaggi di programmazione i simboli <, >, = sono considerati anch'essi operatori come +, ò, ∧, di un tipo ancora diverso: sono operatori che prendono come operandi dei numeri, come + e ò, ma danno come risultato, invece di un numero, un valore di verità. Si ha così, ad esempio:

2 ò 3 → 6
2 > 3 → F
2 < 3 → T
2 = 3 → F
...

Così l'espressione 2 < 3 non è "sbagliata", è semplicemente un'espressione (proprio come 2+3) di cui possiamo calcolare il valore, e tale valore è false.

Che cos'è allora la verità?

- Benché quanto precede possa sembrare una serie di ovvietà, è importante notare il diverso "sguardo" che così si ottiene sulla nozione di verità.
- Il Vero e il Falso, da elevati e magari difficili concetti filosofici, diventano semplicemente due entità analoghe ai numeri, i "valori di verità" o "booleani" (dal logico George Boole), con i quali si possono fare operazioni simili a quelle aritmetiche.
- Con la nascita e lo sviluppo dei computer, i valori di verità e le operazioni con essi si materializzano in circuiti elettronici.
- Per un ingegnere elettronico intorno alla metà del '900, una "logica" non era una teoria filosofica o matematica, ma un chip, un circuito a transistori, che si comprava nei negozi di hardware (ferramenta).

Senso e significato.

- Grosso modo alla fine dell'Ottocento in filosofia e in logica compare la distinzione fra "senso" e "significato", o fra "connotazione" e "denotazione", in particolare nell'opera di Gottlob Frege, uno dei fondatori della logica moderna:

  G. Frege, "Über Sinn und Bedeutung", articolo del 1892.
- Un'espressione linguistica può denotare (cioè riferirsi a) un'entità del mondo: espressioni diverse, tuttavia, possono denotare una stessa entità attraverso differenti modi di concepirla, o di ottenerla.
- L'esempio classico è dato dalle due espressioni "stella del mattino" (o "Lucifero") e "stella della sera" (o "Vespero"). Entrambe le espressioni denotano il pianeta Venere, ma con due sensi o connotazioni differenti: la stella che scompare per ultima all'alba, o la prima stella che appare al tramonto.

Senso e significato.

- Altro esempio: le espressioni aritmetiche 5+3 e 4ò2 denotano entrambe il numero 8, ma in due sensi diversi.
- Oggi noi preferiamo dire che le due espressioni hanno entrambe come valore 8, o che "si riducono" a 8.
- Analogamente, l'espressione 3 < 5, come abbiamo visto, si riduce al valore di verità T, l'espressione 3 > 5 si riduce al valore di verità F.
- Possiamo allora dire, con Frege, che il significato di una proposizione è il suo valore di verità.
- Tutte le proposizioni vere hanno lo stesso significato, cioè il valore T, ma sensi diversi (il che sembra una definizione un po' bizzarra di significato, che tuttavia in seguito risulterà utile).
- Analogamente tutte le proposizioni false hanno uno stesso significato, il valore F.

Gli altri connettivi proposizionali

Connettivi proposizionali: la disgiunzione.

La disgiunzione "o" in logica è intesa in senso non esclusivo: le tre proposizioni sottostanti:

"Roma è la capitale d'Italia o Ivrea si trova in Lombardia"
"Londra è la capitale d'Italia o Ivrea si trova in Piemonte"
"Roma è la capitale d'Italia o Ivrea si trova in Piemonte"

sono tutte vere, perché in ognuna di esse una o entrambe le componenti sono vere.

Invece:

"Londra è la capitale d'Italia o Ivrea si trova in Lombardia"

è falsa perché entrambe le componenti sono false.

La disgiunzione viene indicata, a seconda dei contesti, con i simboli or, | , || , +, ∨.

La notazione standard in logica, che seguiremo, è ∨.

La tavola di verità per la disgiunzione.

La tavola di verità per la disgiunzione è quindi la seguente:

α	β	α ∨ β
F	F	F
F	T	T
T	F	T
T	T	T

Nella notazione "aritmetica" la disgiunzione è indicata con "+" e chiamata "somma logica". Le sue "tabelline" sono quindi:

0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 1

La negazione

Nella logica moderna la particella "non" (in ingl. "not") si usa solo per negare un'intera proposizione; non la si può usare per negare qualcosa che non sia una proposizione, ad esempio un attributo, o un complemento, ecc.

La negazione di un predicato o di un altro elemento sintattico nelle lingue naturali può essere di solito facilmente espresso mediante la negazione logica, ma occorre fare attenzione.

La particella "non" va quindi intesa intuitivamente come "non si dà il caso che", "non è vero (!) che", ecc.

La negazione viene indicata, a seconda dei contesti, con i simboli not, !, ~, Ė, o talvolta con la sopralineatura.

La notazione standard in logica, che seguiremo, è Ė, che si legge "not" all'inglese, o "non" all'italiana e alla francese.

La negazione: esempi nelle lingue naturali.

- La negata della proposizione "Paolo ama Francesca" è la proposizione "Paolo non ama Francesca", perché questa ha lo stesso senso di "non è vero che Paolo ama Francesca": in questo caso negando il verbo si nega l'intera proposizione.
- La negata della proposizione "tutti gli italiani sono disonesti" non è "tutti gli italiani non sono disonesti", che è una (brutta) frase equivalente a "nessun italiano è disonesto",
  bensì "non tutti gli italiani sono disonesti", che equivale a "non è vero che tutti gli italiani sono disonesti".
- A proposito della varietà e ambiguità delle lingue naturali, si noti che invece in francese la proposizione "tous les Italiens ne sont pas malhonnêtes" vuol proprio dire "non tutti gli italiani sono disonesti" !

Ma di questo genere di frasi ci occuperemo quando studieremo la logica dei predicati.

La tavola di verità per la negazione.

La tavola di verità per la negazione è quindi banale:

α	Ė α
F	T
T	F

Nella notazione "aritmetica" la negazione è spesso indicata con "¼", e la sua "tabellina" è semplicemente:

¼ 0 = 1
¼ 1 = 0

Con i tre "operatori booleani" *and*, *or*, e *not* si delinea quindi già una sorta di "algebra del pensiero".

Parentesizzazione e precedenza in aritmetica

In aritmetica, le espressioni contenenti più operatori sarebbero ambigue:

5 + 3 ò 7

L'ambiguità viene risolta, come sappiamo, tramite l'uso delle parentesi:

(5 + 3) ò 7 (= 56) è diverso da 5 + (3 ò 7) (= 26).

Poi si adotta la convenzione che il ò ha la precedenza sul +, e che quindi 5 + (3 ò 7) si può scrivere senza parentesi, mentre in (5 + 3) ò 7 le parentesi sono necessarie.

Nelle lingue naturali vi possono essere frasi corrette che sono ambigue, come "Luigi guarda la ragazza col binocolo" o "they are flying kites"; l'ambiguità è in genere risolta dal contesto.

Nei linguaggi logici, invece, l'ambiguità viene risolta come in aritmetica, per mezzo di parentesi e regole di precedenza.

Parentesizzazione e precedenza in logica

La frase italiana

Aldo scia e Leo prepara cena o Ada dorme

è ambigua; in logica la sua analoga viene disambiguata per mezzo di parentesi. La proposizione

(Aldo scia e Leo prepara cena) o Ada dorme

è diversa dalla proposizione

Aldo scia e (Leo prepara cena o Ada dorme)

Poi, come in aritmetica, si stabilisce che la congiunzione ha la precedenza sulla disgiunzione, e che quindi

Aldo scia e Leo prepara cena o Ada dorme

equivale a

(Aldo scia e Leo prepara cena) o Ada dorme

La congiunzione come il ò, la disgiunzione come il + !

Parentesizzazione e precedenza in logica

$(A\wedge B)\vee C$ è diverso da $A\wedge(B\vee C)$

Nella proposizione $(A\wedge B)\vee C$ le parentesi si possono anche omettere, ma non è vietato - soprattutto per i principianti - tenerle.

Anche per gli operatori logici $\wedge$ e $\vee$, come per quelli aritmetici ò e +, vale inoltre la proprietà associativa: così come

$(a + b) + c$ ha lo stesso valore di $a + (b + c)$

e quindi le parentesi possono essere omesse,

anche le proposizioni $(A\vee B)\vee C$ e $A\vee(B\vee C)$ ovviamente hanno lo stesso significato, e quindi le parentesi si possono omettere. La stessa cosa vale per l'operatore $\wedge$.

Le proposizioni scritte nella forma simbolica come qui sopra vengono anche dette formule logiche (proposizionali) o formule booleane, o, brevemente, formule.

Come si costruisce la tavola di verità di una formula composta.

Consideriamo ad es. la formula $A\vee(B\wedge C)$.
Per costruirne la tavola di verità dobbiamo esaminare tutte le possibili attribuzioni di valori di verità (in logica si dice piuttosto assegnazioni di valori di verità) alle componenti atomiche A, B, e C, e per ognuna di esse calcolare il valore risultante.

A	B	C	B ∧ C	A ∨ (B ∧ C)
F	F	F		
F	F	T		
F	T	F		
F	T	T		
T	F	F		
T	F	T		
T	T	F		
T	T	T		

Come si costruisce la tavola di verità di una formula composta.

Consideriamo ad es. la formula $A\vee(B\wedge C)$.
Per costruirne la tavola di verità dobbiamo esaminare tutte le possibili attribuzioni di valori di verità (in logica si dice piuttosto assegnazioni di valori di verità) alle componenti atomiche A, B, e C, e per ognuna di esse calcolare il valore risultante.

A	B	C	B ∧ C	A ∨ (B ∧ C)
F	F	F	F	
F	F	T	F	
F	T	F	F	
F	T	T	T	
T	F	F	F	
T	F	T	F	
T	T	F	F	
T	T	T	T	

Come si costruisce la tavola di verità di una formula composta.

Consideriamo ad es. la formula $A\vee(B\wedge C)$.
Per costruirne la tavola di verità dobbiamo esaminare tutte le possibili attribuzioni di valori di verità (in logica si dice piuttosto assegnazioni di valori di verità) alle componenti atomiche A, B, e C, e per ognuna di esse calcolare il valore risultante.

A	B	C	B ∧ C	A ∨ (B ∧ C)
F	F	F	F	F
F	F	T	F	F
F	T	F	F	F
F	T	T	T	T
T	F	F	F	T
T	F	T	F	T
T	T	F	F	T
T	T	T	T	T

Da quante righe è composta una tavola di verità?

Da quante righe è composta la tavola di verità di una formula contenente n formule atomiche distinte $A_1, A_2, \ldots A_n$?

(Nota: ognuno degli atomi può anche comparire più volte in una formula, ad es. A∧(B∨ Ė A)∧ … : quindi il numero n di atomi distinti può essere minore della lunghezza della formula).

La A_1 può essere falsa o vera: per ciascuno dei due valori la A_2 può a sua volta essere falsa o vera, quindi sono 2 ò 2 = 4 casi.

Per ognuno di questi 4 casi A_3 può essere falsa o vera, quindi ci sono in tutto 4 ò 2 = 8 casi.

E così via: per n atomi distinti ci saranno 2^n casi (righe).

Attenzione: non confondere 2^n con n^2 !

n^2 è l'onesta funzione-quadrato, il cui valore si quadruplica quando la n si raddoppia;

2^n è la spaventosa funzione esponenziale, il cui valore si raddoppia quando la n aumenta di 1.

n	n^2		2^n	
10:	10^2	= 100	2^{10}	= 1024
20:	20^2	= 400	2^{20}	= 1.048.576
30:	30^2	= 900	2^{30}	] 10^9
100:	100^2	= 10.000	2^{100}	] 10^{30}
1000:	1000^2	= un milione	2^{1000}	] 10^{300}
. . .	. . .		. . .	

Il numero stimato di particelle elementari dell'universo è ¼ 10^{80}, 2^{1000} (cioè 10^{300}) è un numero inconcepibile …

Quattro slides da quelle del corso di

Algoritmi e Strutture Dati

Corso di Laurea in Informatica
Dipartimento di Informatica - Università di Torino
corso Svizzera 185
(Centro Piero della Francesca)

ingresso (giorni feriali) da *via Pessinetto 12*

Intermezzo: antica leggenda orientale.

Un giorno un re (o un bramino, o un califfo, ecc.) chiese ad un giovane (o all'inventore del gioco degli scacchi, o a un bramino, ecc.) che gli aveva reso un servizio (o salvato la vita, ecc.) che ricompensa volesse. La risposta fu:

" Dammi tanti chicchi di riso quanti se ne possono porre sulle caselle di una scacchiera ideale, mettendo un chicco sulla prima casella, due sulla la seconda, quattro sulla terza e così via raddoppiando ogni volta in numero di chicchi"

Il re accettò con entusiasmo, sembrandogli quella richiesta poca cosa. Ma se ne pentì ben presto …

… perché …

si può vedere con un facile calcolo che i chicchi di riso richiesto dal giovane (2^{64}-1) sarebbero sufficienti a tappezzare una strada larga circa 500 Km e lunga quanto la distanza dalla Terra alla Luna …, oppure a sommergere tutti i palazzi del centro di Torino.

ATTENZIONE !

Non confondere 2^n con n^2 !

n^2 $\begin{cases} \text{è una tranquilla funzione quadratica,} \\ \text{avente per grafico una parabola;} \\ \text{la sua crescita è considerata, in molti casi,} \\ \text{accettabile;} \end{cases}$

2^n $\begin{cases} \text{è una funzione esponenziale,} \\ \text{la sua crescita è spaventosamente rapida,} \\ \text{più di qualunque potenza !} \end{cases}$

ATTENZIONE !

Nel linguaggio giornalistico e nel linguaggio comune l'aggettivo "esponenziale" viene spesso usato con il significato di "che cresce rapidamente", a volte addirittura col significato di "molto grande" (ad es. una quantità esponenziale di …).
Nel linguaggio scientifico e nei linguaggi tecnici questo uso non è ammesso, è un gravissimo errore !

Chi all'esame dice "esponenziale" in questo senso, oppure dice esponenziale al posto di quadratico, o di lineare, ecc., rischia l'immediata bocciatura.

Fine delle slides prese dal corso di Algoritmi.

Nota terminologica

- Le funzioni che crescono come una potenza (con esponente costante) si dicono polinomiali.
- Le funzioni che crescono come (o di più) di un esponenziale si dicono appunto esponenziali (o iper-esponenziali).
- Esempi:

  x^2, $4x^3$, $3x^5 + 4x^2 + 6$ sono funzioni polinomiali di x

  2^x, 5^x, $5^x + x^2$, $5^x \cdot x^2$ sono funzioni esponenziali di x

La differenza fra polinomiale ed esponenziale è fondamentale!

Conseguenza logica
(canzone dei Matia Bazar? noo!)

Date una o più proposizioni come premesse o assunzioni, quali proposizioni possiamo ricavarne come conseguenze?

Un esempio super-banale: supponiamo che si voglia affermare che in un appartamento c'è sempre qualcuno, perché c'è Aldo che studia oppure c'è Leo che fa i compiti aiutato da Ada, o entrambe le cose. Supponiamo di descrivere tale situazione tramite la proposizione composta

Aldo studia o (Leo fa i compiti e Ada aiuta Leo)

Una delle conseguenze logiche di tale proposizione è

Aldo studia o Ada aiuta Leo

In forma simbolica: una conseguenza di $A\vee(B\wedge C)$ è $(A\vee C)$

(Altre conseguenze sono Aldo studia o Leo fa i compiti, (Aldo studia o Leo fa i compiti) e (Aldo studia o Ada aiuta Leo))

Verifica di conseguenze.

C'è un metodo (meccanico) per verificare se una formula è conseguenza di una data premessa, o di date premesse?

Basta applicare la ovvia definizione vista all'inizio:

Che cosa vuol dire che una proposizione (atomica o composta) τ è conseguenza logica di una proposizione σ o più in generale di un insieme di proposizioni $\sigma_1, \sigma_2, \ldots, \sigma_n$?

Vuol dire che se le premesse $\sigma_1, \sigma_2, \ldots, \sigma_n$ sono vere, allora la conclusione τ è necessariamente vera; per indicare in modo conciso tale fatto si scrive

$$\sigma_1, \sigma_2, \ldots, \sigma_n \models \tau$$

Allora basta costruire una tabella dei valori di verità e verificare se le attribuzioni di valori di verità alle componenti atomiche che rendono vere le premesse rendono vera la conclusione.

Vediamo alcuni esempi nelle slides seguenti.

Conseguenza logica e tavole di verità.

Iniziamo con un esempio con una sola premessa: vogliamo verificare se $(A\vee C)$ è conseguenza logica di $A\vee(B\wedge C)$.

Dobbiamo allora fare una tabella di tutte le possibili attribuzioni di valori di verità (*) alle componenti atomiche A, B, e C:

A	B	C	A ∨ (B ∧ C)	A ∨ C
F	F	F		
F	F	T		
F	T	F		
F	T	T		
T	F	F		
T	F	T		
T	T	F		
T	T	T		

(*) in logica si usa dire piuttosto *assegnazioni* di valori di verità.

Conseguenza logica e tavole di verità.

Poi, per ogni possibile assegnazione di valori di verità ad A,B,C, cioè per ogni riga della tabella, calcoliamo il valore di verità della premessa col metodo indicato prima (ricopiamo dalla slide 45, senza riportare la colonna intermedia):

A	B	C	A ∨ (B ∧ C)	A ∨ C
F	F	F	F	
F	F	T	F	
F	T	F	F	
F	T	T	T	
T	F	F	T	
T	F	T	T	
T	T	F	T	
T	T	T	T	

Conseguenza logica e tavole di verità.

Poi, per ogni possibile assegnazione di valori di verità ad A,B,C, cioè per ogni riga della tabella, calcoliamo con lo stesso metodo il valore di verità della conclusione (in questo caso particolare basta applicare la tavola della disgiunzione):

A	B	C	A ∨ (B ∧ C)	A ∨ C
F	F	F	F	F
F	F	T	F	T
F	T	F	F	F
F	T	T	T	T
T	F	F	T	T
T	F	T	T	T
T	T	F	T	T
T	T	T	T	T

Conseguenza logica e tavole di verità.

Infine, consideriamo tutte le righe nelle quali la premessa è vera, e controlliamo se in ognuna di esse è vera anche la conclusione:

A	B	C	A ∨ (B ∧ C)	A ∨ C
F	F	F	F	F
F	F	T	F	T
F	T	F	F	F
F	T	T	T	T
T	F	F	T	T
T	F	T	T	T
T	T	F	T	T
T	T	T	T	T

Conseguenza logica e tavole di verità.

Infine, consideriamo tutte le righe nelle quali la premessa è vera, e controlliamo se in ognuna di esse è vera anche la conclusione: sì, è proprio così!

(A∨C) è conseguenza logica di A∨(B∧C)

A	B	C	A ∨ (B ∧ C)	A ∨ C
F	F	F	F	F
F	F	T	F	T
F	T	F	F	F
F	T	T	T	T
T	F	F	T	T
T	F	T	T	T
T	T	F	T	T
T	T	T	T	T

Linguaggio e meta-linguaggio.

Abbiamo quindi verificato che A ∨ (B ∧ C) ⊨ A ∨ C

Attenzione: il simbolo ⊨ non è un simbolo del linguaggio logico, bensì un simbolo del meta-linguaggio con il quale noi parliamo del linguaggio logico! esso esprime una relazione fra formule del linguaggio, appunto la relazione di conseguenza logica fra un insieme di premesse e una conclusione!

Nella logica matematica, le proposizioni diventano degli enti matematici come i numeri o le figure geometriche, che quindi vengono studiati con metodi matematici.
"Logica matematica" non vuol dire (o non principalmente) "logica della matematica", bensì "matematica della logica"!
Naturalmente la matematica si fonda a sua volta sulla logica … ma nei discorsi sui fondamenti una certa circolarità è inevitabile!

Formule atomiche e formule generiche.

Ovviamente, nell'esempio visto, la relazione di conseguenza logica

A ∨ (B ∧ C) ⊨ A ∨ C

vale non solo per A, B, C formule atomiche, ma per formule generiche α, β, θ, che possono essere già formule composte di qualunque complessità:

α ∨ (β ∧ θ) ⊨ α ∨ θ

Nota: possiamo convenire di pronunciare il simbolo ⊨ in modo abbreviato come "da … (con)segue …".

Conseguenza logica di più premesse.

Il metodo si applica anche nel caso di più premesse.

Esempio elementare

Premesse.

1. Aldo ha una giacca rossa o Beatrice mente.
2. Aldo non ha una giacca rossa.
3. Beatrice non mente o Caio è l'assassino.

Una delle conseguenze che si possono ricavare è:

- Caio è l'assassino e Beatrice mente

Infatti, intuitivamente, dalle prime due proposizioni si ricava che Beatrice mente; da questo e dalla 3 si ricava appunto che Caio è l'assassino; ecc.

Formalizzazione del ragionamento.

Indichiamo ogni proposizione atomica con una lettera:

A = Aldo ha una giacca rossa
B = Beatrice mente
C = Caio è l'assassino.

Le tre premesse sono:

1. A∨B = Aldo ha una giacca rossa o Beatrice mente.
2. È A = Aldo non ha una giacca rossa.
3. È B∨C = Beatrice non mente o Caio è l'assassino.

La conseguenza che consideriamo è:

B∧C = Beatrice mente e Caio è l'assassino.

In modo più formale, scriviamo:

A∨B, È A, È B∨C ⊨ B∧C

Con il metodo delle tavole di verità controlliamo se è così.

Costruzione della tabella.

atomi — premesse — conclusione

A	B	C	Ė B	A∨B	Ė A	Ė B ∨ C	B ∧ C
F	F	F					
F	F	T					
F	T	F					
F	T	T					
T	F	F					
T	F	T					
T	T	F					
T	T	T					

Costruzione della tabella.

atomi — premesse — conclusione

A	B	C	Ė B	A∨B	Ė A	Ė B ∨ C	B ∧ C
F	F	F	T				
F	F	T	T				
F	T	F	F				
F	T	T	F				
T	F	F	T				
T	F	T	T				
T	T	F	F				
T	T	T	F				

Costruzione della tabella.

atomi — premesse — conclusione

A	B	C	Ė B	A∨B	Ė A	Ė B ∨ C	B ∧ C
F	F	F	T	F			
F	F	T	T	F			
F	T	F	F	T			
F	T	T	F	T			
T	F	F	T	T			
T	F	T	T	T			
T	T	F	F	T			
T	T	T	F	T			

Costruzione della tabella.

atomi — premesse — conclusione

A	B	C	Ė B	A∨B	Ė A	Ė B ∨ C	B ∧ C
F	F	F	T	F	T		
F	F	T	T	F	T		
F	T	F	F	T	T		
F	T	T	F	T	T		
T	F	F	T	T	F		
T	F	T	T	T	F		
T	T	F	F	T	F		
T	T	T	F	T	F		

Costruzione della tabella.

atomi — premesse — conclusione

A	B	C	Ė B	A∨B	Ė A	Ė B ∨ C	B ∧ C
F	F	F	T	F	T	T	
F	F	T	T	F	T	T	
F	T	F	F	T	T	F	
F	T	T	F	T	T	T	
T	F	F	T	T	F	T	
T	F	T	T	T	F	T	
T	T	F	F	T	F	F	
T	T	T	F	T	F	T	

Costruzione della tabella.

atomi — premesse — conclusione

A	B	C	Ė B	A∨B	Ė A	Ė B ∨ C	B ∧ C
F	F	F	T	F	T	T	F
F	F	T	T	F	T	T	F
F	T	F	F	T	T	F	F
F	T	T	F	T	T	T	T
T	F	F	T	T	F	T	F
T	F	T	T	T	F	T	F
T	T	F	F	T	F	F	F
T	T	T	F	T	F	T	T

Ora consideriamo tutti e soli i casi in cui le tre premesse sono tutte vere, cioè tutte e sole le righe in cui vi è T in tutte le premesse:

Costruzione della tabella.

atomi | premesse | conclusione

A	B	C	Ė B	A∨B	Ė A	Ė B ∨ C	B ∧ C
F	F	F	T	F	T	T	F
F	F	T	T	F	T	T	F
F	T	F	F	T	T	F	F
F	T	T	F	T	T	T	T
T	F	F	T	T	F	T	F
T	F	T	T	T	F	T	F
T	T	F	F	T	F	F	F
T	T	T	F	T	F	T	T

Ora consideriamo tutti e soli i casi in cui le tre premesse sono tutte vere, cioè tutte e sole le righe in cui vi è T in tutte le premesse: in questa tavola ce n'è una sola.

Costruzione della tabella.

atomi | premesse | conclusione

A	B	C	Ė B	A∨B	Ė A	Ė B ∨ C	B ∧ C
F	F	F	T	F	T	T	F
F	F	T	T	F	T	T	F
F	T	F	F	T	T	F	F
F	T	T	F	T	T	T	T
T	F	F	T	T	F	T	F
T	F	T	T	T	F	T	F
T	T	F	F	T	F	F	F
T	T	T	F	T	F	T	T

Andiamo allora a vedere in tale riga il valore della conclusione: è anch'esso T. Quindi la conclusione è conseguenza logica delle premesse.

Virgola e congiunzione.

Abbiamo dunque stabilito, in modo puramente meccanico, una relazione di conseguenza logica tra formule:

A∨B, Ė A, Ė B ∨C ⊨ B∧C

Si osservi, guardando la tavola di verità, che poiché contano solo le righe in cui tutte le premesse sono vere, è come se le premesse fossero tutte in congiunzione (AND) fra di loro.
La virgola è cioè una sorta di meta-congiunzione, e si ha

$\alpha_1, \alpha_2, \ldots, \alpha_n \models \beta$ se e solo se $\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n \models \beta$

Esercizio: un altro esempio.

Un altro esempio super-banale: dalla premessa

Aldo scia e (Leo prepara cena o Ada dorme)

si ha come conseguenza logica la proposizione

(Aldo scia e Leo prepara cena) o (Aldo scia e Ada dorme)

Cioè da $A\wedge(B\vee C)$ si ha come conseguenza $(A\wedge B)\vee(A\wedge C)$:

$$A\wedge(B\vee C) \models (A\wedge B)\vee(A\wedge C)$$

Verifichiamolo meccanicamente con il metodo appena visto.

Costruzione della tabella.

Per ogni assegnazione di valori di verità ad A,B,C, cioè per ogni riga della tabella, calcoliamo il valore di verità della premessa (facciamo il calcolo a mente, omettendo le colonne intermedie):

A	B	C	A ∧ (B ∨ C)	(A∧B) ∨ (A∧C)
F	F	F		
F	F	T		
F	T	F		
F	T	T		
T	F	F		
T	F	T		
T	T	F		
T	T	T		

Costruzione della tabella.

Per ogni assegnazione di valori di verità ad A,B,C, cioè per ogni riga della tabella, calcoliamo il valore di verità della premessa (facciamo il calcolo a mente, omettendo le colonne intermedie):

A	B	C	A ∧ (B ∨ C)	(A∧B) ∨ (A∧C)
F	F	F	F	
F	F	T	F	
F	T	F	F	
F	T	T	F	
T	F	F	F	
T	F	T	T	
T	T	F	T	
T	T	T	T	

Costruzione della tabella.

Per ogni assegnazione di valori di verità ad A,B,C, cioè per ogni riga della tabella, calcoliamo il valore di verità della conclusione (facciamo il calcolo a mente, omettendo le colonne intermedie):

A	B	C	A ∧ (B ∨ C)	(A∧B) ∨ (A∧C)
F	F	F	F	F
F	F	T	F	F
F	T	F	F	F
F	T	T	F	F
T	F	F	F	F
T	F	T	T	T
T	T	F	T	T
T	T	T	T	T

Diversamente dagli esempi prec., qui le righe in cui la premessa è vera e la conclusione è vera sono esattamente le stesse!

Equivalenza logica

Nell'ultimo esempio, a differenza dei precedenti, scambiando i ruoli di premessa e conclusione vale ancora la relazione di conseguenza logica; si ha cioè non solo

$$A \wedge (B \vee C) \models (A \wedge B) \vee (A \wedge C)$$

ma anche

$$(A \wedge B) \vee (A \wedge C) \models A \wedge (B \vee C)$$

Due proposizioni che sono ciascuna conseguenza dell'altra si dicono logicamente equivalenti fra loro.

Per indicare l'equivalenza logica usiamo il simbolo ø .

Scriviamo quindi $A \wedge (B \vee C)$ ø $(A \wedge B) \vee (A \wedge C)$.

L'equivalenza logica è analoga all'uguaglianza aritmetica; se usiamo i simboli ò e + rispettivamente per ∧ e ∨, otteniamo:

$$A \text{ ò } (B + C) \text{ ø } (A \text{ ò } B) + (A \text{ ò } C)$$

È la proprietà distributiva del prodotto rispetto alla somma!

Un'altra proprietà distributiva.

Si può facilmente vedere che vale anche l'equivalenza:

$$A \vee (B \wedge C) \text{ ø } (A \vee B) \wedge (A \vee C)$$

che scritta con i simboli aritmetici è:

$$A + (B \text{ ò } C) \text{ ø } (A + B) \text{ ò } (A + C)$$

Nella logica booleana vale anche la proprietà distributiva della somma (logica) rispetto al prodotto (logico), che invece non vale in aritmetica.

Ovviamente anche le proprietà di cui sopra valgono non solo per formule atomiche A, B, C, ma per formule generiche σ, τ, φ:

$$\sigma \wedge (\tau \vee \varphi) \text{ ø } (\sigma \wedge \tau) \vee (\sigma \wedge \varphi)$$

$$\sigma \vee (\tau \wedge \varphi) \text{ ø } (\sigma \vee \tau) \wedge (\sigma \vee \varphi)$$

Altri connettivi

- Si possono definire altri connettivi, semplicemente prendendo come definizioni tavole di verità diverse.
- In questo modo si possono definire connettivi bizzarri, oppure connettivi utili, come la disgiunzione esclusiva (in inglese exclusive or), corrispondente al latino aut … aut … .
- Viene indicata di solito col simbolo XOR, oppure ă, o anche ⊻.
- Esercizio: scrivere la tavola di verità che definisce ă.

α	β	α ă β

Altri connettivi

- Si possono definire altri connettivi, semplicemente prendendo come definizioni tavole di verità diverse.
- In questo modo si possono definire connettivi bizzarri, oppure utili, come la disgiunzione esclusiva (in inglese exclusive or), corrispondente al latino aut … aut … .
- Viene indicata di solito col simbolo XOR, oppure ă, o anche ⊻.
- Esercizio: scrivere la tavola di verità che definisce ă.

α	β	α ă β
F	F	F
F	T	T
T	F	T
T	T	F

Formule soddisfacibili, valide, contraddittorie.

Le tavole di verità considerate finora hanno nelle colonne dei risultati sia dei T che degli F; cioè in generale una formula può essere vera o falsa a seconda delle assegnazioni di valori di verità alle formule atomiche componenti.

Ad esempio $(A \vee B) \wedge (A \vee C)$ è, come abbiamo visto, vera in alcuni casi, falsa in altri.

Ci può essere qualche formula che risulta vera in tutti i casi, e qualche altra formula che risulta falsa in tutti i casi?

Esempi primordiali:

A	ĖA	A ∨ ĖA
F	T	T
T	F	T

A	ĖA	A ∧ ĖA
F	T	F
T	F	F

Formule soddisfacibili, valide, contraddittorie.

- Una formula che risulta vera per qualunque assegnazione di valori di verità si dice valida. Una formula valida viene anche detta tautologia.
  Esempio: A ∨ Ė A è una tautologia (*"tertium non datur"*)
- Una formula che risulta falsa per qualunque assegnazione di valori di verità si dice contraddittoria, o incoerente o (con un brutto ma diffuso inglesismo) inconsistente. Come è naturale, una formula contraddittoria viene anche detta contraddizione!
  Esempio: A ∧ Ė A è l'esempio primigenio di contraddizione.
- Una formula che risulta vera per almeno una assegnazione di valori di verità (ed eventualmente falsa per altre assegnazioni) si dice soddisfacibile, o coerente, o (con brutto ma diffuso inglesismo) consistente.

Formule soddisfacibili, valide, contraddittorie.

Quindi:

Una tautologia è un particolare genere di formula soddisfacibile.

Una formula è soddisfacibile se e solo se non è contraddittoria.

"non soddisfacibile" equivale dunque a "contraddittoria"

Una tautologia è vera (o una contraddizione è falsa) in virtù della sua forma, indipendentemente dalla verità o falsità (e quindi dal significato, dall'*interpretazione*) delle loro componenti atomiche.

Una tautologia o una contraddizione è necessariamente una proposizione composta: la verità o falsità di una proposizione atomica, come "Lea dorme" oppure "la neve è bianca", dipende dalla realtà cui la formula si riferisce, cioè dalla *interpretazione* della formula stessa.

Tautologie, contraddizioni, e negazione.

Poiché una tautologia è una formula che nella sua colonna ha tutti T, la negata di una tautologia ha nella sua colonna tutti F, ed è quindi una contraddizione; ovviamente vale il viceversa: la negata di una contraddizione è una tautologia.

Esempio

A	B	A ∨ ĖB ∨ (ĖA ∧ B)	Ė(A ∨ ĖB ∨ (ĖA ∧ B))
F	F		
F	T		
T	F		
T	T		

La formula **A** ∨ Ė**B** ∨ (Ė**A** ∧ **B**) è una … .

Esempio

A	B	A ∨ ĖB ∨ (ĖA ∧ B)	Ė(A ∨ ĖB ∨ (ĖA ∧ B))
F	F	T	
F	T	T	
T	F	T	
T	T	T	

La formula **A** ∨ Ė**B** ∨ (Ė**A** ∧ **B**) è una tautologia.

Esempio

A	B	A ∨ ĖB ∨ (ĖA ∧ B)	Ė(A ∨ ĖB ∨ (ĖA ∧ B))
F	F	T	F
F	T	T	F
T	F	T	F
T	T	T	F

La formula **A** ∨ Ė**B** ∨ (Ė**A** ∧ **B**) è una tautologia.
La formula Ė (**A** ∨ Ė**B** ∨ (Ė**A** ∧ **B**)) è una contraddizione.

Tabella riassuntiva

contraddittoria ≡ non soddisfacibile
cioè
soddisfacibile ≡ non contraddittoria

Una formula è o contraddittoria o soddisfacibile.
Una formula soddisfacibile può essere o no una tautologia.

Connessione con la negazione
σ è contraddittoria ≡ $\neg\sigma$ è una tautologia;
σ è una tautologia ≡ $\neg\sigma$ è contraddittoria

Tautologie

Ricordando che la scrittura

$$\sigma_1, \sigma_2, \ldots, \sigma_n \models \tau$$

vuol dire:
in tutti i casi in cui $\sigma_1, \sigma_2, \ldots, \sigma_n$ sono contemporaneamente vere, τ è vera,
per indicare che τ è una tautologia, cioè è vera in tutti i casi, cioè per tutte le possibili assegnazioni di valori di verità, senza condizioni, è naturale scrivere

$$\models \tau$$

senza premesse.
Una tautologia è, per così dire, una conseguenza logica di un insieme di premesse vuoto.

Contraddizioni

A	$\neg$A	...	A $\wedge$ $\neg$A	C
F	T	...	F	...
T	F	...	F	...
...	...	...	F	...

La proposizione C è conseguenza di $A \wedge \neg A$ se in tutti i casi in cui $A \wedge \neg A$ è vera, anche C è vera. Ma $A \wedge \neg A$ non è vera in nessun caso, quindi la condizione affinché C sia conseguenza di $A \wedge \neg A$ è banalmente soddisfatta: la premessa non pone alcun vincolo!
Da una formula contraddittoria si ha come conseguenza logica qualsiasi formula:

$$\sigma \wedge \neg\sigma \models \tau \quad \text{(ex falso quodlibet)}$$

Esempio umoristico standard

Se 1 = 2, io sono il Papa.

Dimostrazione:
il Papa e io siamo 2;
ma 2 = 1, quindi il Papa e io siamo 1;
dunque io sono il Papa.

Una tavola di verità per la conseguenza logica?

Osserviamo che anche la relazione di conseguenza logica può essere caratterizzata da una particolare tavola di verità.
Riprendiamo infatti il primo esempio (vedi slide seguente).

Il primo esempio.

A	B	C	A ∨ (B ∧ C)	A ∨ C
F	F	F	F	F
F	F	T	F	T
F	T	F	F	F
F	T	T	T	T
T	F	F	T	T
T	F	T	T	T
T	T	F	T	T
T	T	T	T	T

Concentriamoci sulle due ultime colonne: in esse compaiono solo tre tipi di righe:

premessa	conclusione
F	F
F	T
T	T

Una tavola di verità per la conseguenza logica?

Osserviamo ancora che l'unico caso in cui una conclusione non è conseguenza logica di una premessa (ed è quindi una conclusione "illogica") è quando vi è qualche caso in cui la premessa è vera e la conclusione è falsa: cioè quando nella tavola di verità compare la riga:

premessa	conclusione
T	F

Quando invece la premessa è falsa, la verità o falsità della conclusione non ha importanza. La pseudo-tavola di verità per la conseguenza logica sarebbe allora:

α	β	$\alpha \models \beta$
F	F	T
F	T	T
T	F	F
T	T	T

Una tavola di verità per la conseguenza logica?

Il procedimento per stabilire se una formula τ è conseguenza di una formula σ può infatti essere riformulato nel modo seguente:

- costruisci la tavola di verità per σ;
- costruisci la tavola di verità per τ;
- a partire da queste, costruisci la "tavola di verità" per $\sigma \models \tau$ (in pratica, dalla colonna di σ e da quella di τ, usando la tavola di $\models$ della slide precedente, costruisci la colonna di $\sigma \models \tau$);
- se in tutte le righe di tale colonna c'è T, allora vale la proprietà che $\sigma \models \tau$, cioè che τ è conseguenza logica di σ.

Dunque si ha $\sigma \models \tau$ se e solo se nella "tavola di verità" la colonna di $\sigma \models \tau$ ha T in tutte le righe.

Ma abbiamo visto che una tavola di verità può essere usata per definire un connettivo; allora la relazione metalinguistica di conseguenza logica è un connettivo?

La conseguenza logica non è un connettivo!

Si noti che il simbolo $\models$, essendo un simbolo metalinguistico che indica una relazione tra formule del linguaggio, non può comparire in espressioni annidate: non avrebbe alcun senso scrivere

$$\rho \models (\sigma \models \tau)$$

che si leggerebbe:

la formula ρ ha come conseguenza logica il fatto che
la formula σ ha come conseguenza logica la formula τ.

La frase in italiano informale è sensata, ma si ricordi che:

- la nozione di conseguenza logica è definita come una relazione tra formule del linguaggio logico;
- invece la frase-conclusione $\sigma \models \tau$ non è una formula del linguaggio logico, bensì una proposizione del metalinguaggio!

Si sta confondendo linguaggio con metalinguaggio!

Linguaggio e metalinguaggio

Nella frase in lingua naturale:

la formula ρ ha come conseguenza logica il fatto che
la formula σ ha come conseguenza logica la formula τ.

l'espressione "conseguenza logica" scritta in rosso denota una ben precisa relazione fra formule del linguaggio;

l'espressione "conseguenza logica" scritta in blu indica invece la relazione intuitiva di conseguenza logica …

Ma un momento! La nozione rigorosa di "conseguenza logica" non è semplicemente la precisazione della nozione intuitiva?

Allora basterebbe considerare la scrittura $\rho \models (\sigma \models \tau)$ come una scrittura in cui il simbolo $\models$ blu è diverso dal $\models$ rosso.

Il $\models$ blu sarebbe quindi una sorta di meta-meta-conseguenza. Ma allora potrei poi avere un livello meta-meta-meta …. e così via all'infinito, come nella barzelletta: "Turtles all the way down"

Un nuovo connettivo: la freccia o implicazione.

Ma possiamo introdurre un nuovo connettivo, definito proprio come il connettivo la cui tavola di verità è la pseudo-tavola della conseguenza logica:

la relazione metalinguistica di conseguenza logica può essere "internalizzata" nel linguaggio:

cioè possiamo introdurre nel linguaggio logico un connettivo che esprime, all'interno del linguaggio, una nozione riguardante il linguaggio stesso (cioè la relazione di conseguenza tra formule del linguaggio)!

È il connettivo-implicazione, che indichiamo con il simbolo ì , che si legge "implica", oppure "se … allora …".

La tavola di verità dell'implicazione

La tavola di verità che definisce il connettivo freccia è dunque:

σ	τ	σ ì τ
F	F	T
F	T	T
T	F	F
T	T	T

La tavola di verità della freccia, se presentata isolatamente, può generare perplessità nei principianti. In particolare sembra bizzarra la seconda riga:

σ	τ	σ ì τ
F	T	T

secondo la quale una proposizione come
"se Torino è in Lombardia, Bologna è in Emilia" risulta vera.

Implicazione e intuizione

Occorre però ricordare che la logica proposizionale non riguarda il senso e quindi la verità delle proposizioni atomiche, ma solo la relazione di conseguenza logica fra formule.

Dire che la proposizione "Bologna è in Emilia " è vera, come abbiamo fatto nell'esempio, può essere fuorviante, perché tale verità è una verità di fatto, cioè che dipende dalla realtà a cui riferiamo la proposizione, ma non riguarda la logica; ad esempio se con il nome Bologna intendo riferirmi a un mio conoscente torinese che ha quel cognome, la proposizione precedente è falsa.

La vera motivazione della riga F ì T = T è che essa è quella giusta affinché, come abbiamo visto, il connettivo ì rifletta esattamente la relazione di conseguenza logica ⊨ (e la sua proprietà che "ex falso quodlibet").

Implicazione e intuizione

Può inoltre lasciare perplessi il fatto che la premessa o alcune delle premesse possano non avere alcuna connessione con la la conclusione, ad esempio:

A, Ė A∨B, C, D∧ E ⊨ B

le premesse C e D∧ E non sono rilevanti per stabilire che B è conseguenza logica delle premesse.

Ma anche in una teoria stabilita da un certo insieme di assiomi (ad es. la geometria euclidea) vogliamo poter dire che i teoremi della teoria sono conseguenza logica degli assiomi, anche se la verità di qualche teorema non dipende da quella di tutti gli assiomi, ma solo di alcuni.

In particolare una tautologia, che è vera in tutti i casi, è conseguenza logica di qualunque insieme (anche vuoto, come si è visto) di premesse.

Implicazioni annidate.

A differenza del simbolo ⊨, la freccia ì è un connettivo proposizionale che fa parte del linguaggio logico, proprio come ∧, ∨, Ė, ecc., e quindi - come quelli - può essere annidato a piacere: la scrittura

ρ ì (σ ì τ)

è quindi perfettamente legittima, è una formula del linguaggio, che si può leggere ad esempio, alternando la lettura "se-allora" con la lettura "implica" per rendere l'italiano più comprensibile:

se ρ, allora σ implica τ,

oppure ρ implica che se σ allora τ

oppure anche: ρ implica che σ implica τ

ecc.

Implicazione e conseguenza logica.

Dunque si ha σ ⊨ τ, dove σ e τ sono due formule (atomiche o composte), se e solo se la formula σ ì τ è vera in tutti i casi, cioè è una tautologia, o proposizione (logicamente) valida:

⊨ σ ì τ

Si ha quindi la proprietà che

⊨ σ ì τ se e solo se σ ⊨ τ

La formula σ ì τ esprime all'interno del linguaggio il fatto che dalla formula σ si ottiene, tramite le tavole di verità, come conseguenza logica τ. Questo "gioco" fra linguaggio e metalinguaggio è, come vedremo, una caratteristica, in forme diverse, della logica standard, messa oggi in questione da alcuni logici (J.Y.G.)

Esempio: avevamo trovato che:

A ∨ (B ∧ C) ⊨ A ∨ C

allora si ha: ⊨ A ∨ (B ∧ C) ì A ∨ C

cioè la proposizione A ∨ (B ∧ C) ì A ∨ C è una tautologia.

Conseguenza logica, freccia, tautologia.

Ricordando, dalla slide 75, che

$\sigma_1, \sigma_2, \dots, \sigma_n \models \tau$ se e solo se $\sigma_1 \wedge \sigma_2 \wedge \dots \wedge \sigma_n \models \tau$

abbiamo allora che:

$\sigma_1, \sigma_2, \dots, \sigma_n \models \tau$ se e solo se $\models \sigma_1 \wedge \sigma_2 \wedge \dots \wedge \sigma_n$ ì τ

Cioè: una formula è conseguenza di un insieme di formule se e solo se la formula che esprime all'interno del linguaggio logico stesso tale relazione fra formule è una tautologia.

La cosa non deve stupire troppo: anche in geometria euclidea, ad esempio, assumendo che un triangolo ABC sia equilatero, si dimostra è equiangolo, e poi si scrive come teorema:

Se un triangolo è equilatero, allora è equiangolo.

La corrispondenza con la pratica matematica sarà ancora più chiara quando parleremo dei sistemi deduttivi.

Riassumendo

Si ha

$\sigma_1, \sigma_2, \dots, \sigma_n \models \tau$

se e solo se $\models \sigma_1 \wedge \sigma_2 \wedge \dots \wedge \sigma_n$ ì τ

La relazione di conseguenza logica fra un insieme di premesse ed una conclusione si traduce in una tautologia, in cui la congiunzione delle premesse implica la conclusione.

Implicazione e tautologia: un esempio.

Costruiamo la tavola di verità per A ∨ (B ∧ C) ì A ∨ C, semplicemente aggiungendo alla tavola di slide 50 una colonna, corrispondente all'introduzione del connettivo ì :

A	B	C	A ∨ (B ∧ C)	A ∨ C	A ∨ (B ∧ C) ì A ∨ C
F	F	F	F	F	
F	F	T	F	T	
F	T	F	F	F	
F	T	T	T	T	
T	F	F	T	T	
T	F	T	T	T	
T	T	F	T	T	
T	T	T	T	T	

L'ultima colonna ha tutti T, la formula è una tautologia!

Implicazione e tautologia: un esempio.

Costruiamo la tavola di verità per A ∨ (B ∧ C) ì A ∨ C, semplicemente aggiungendo alla tavola di slide 50 una colonna, corrispondente all'introduzione del connettivo ì :

A	B	C	A ∨ (B ∧ C)	A ∨ C	A ∨ (B ∧ C) ì A ∨ C
F	F	F	F	F	T
F	F	T	F	T	T
F	T	F	F	F	T
F	T	T	T	T	T
T	F	F	T	T	T
T	F	T	T	T	T
T	T	F	T	T	T
T	T	T	T	T	T

L'ultima colonna ha tutti T, la formula è una tautologia!

Esempio

Avevamo visto che dalle premesse:

1. A∨B = Aldo ha una giacca rossa o Beatrice mente.
2. Ė A = Aldo non ha una giacca rossa.
3. Ė B∨C = Beatrice non mente o Caio è l'assassino.

una conseguenza logica è:

B∧C = Beatrice mente e Caio è l'assassino.

Allora la proposizione

(A∨B) ∧ Ė A ∧ (Ė B∨C) ì (B∧C)

cioè:

"se Aldo ha una giacca rossa o Beatrice mente, e Aldo non ha una giacca rossa, e Beatrice non mente o Caio è l'assassino, allora Beatrice mente e Caio è l'assassino"

è una tautologia.

Altri ben noti esempi di conseguenza logica o freccia.

Modus ponens

versione "semantica": α, α ì β ⊨ β

versione sintattica: ⊨ α ∧ (α ì β) ì β

Modus tollens

versione "semantica": Ė β, α ì β ⊨ Ė α

versione sintattica: ⊨ Ė β ∧ (α ì β) ì Ė α

Esercizio: verificare per mezzo delle tavole di verità.

Esempio

Definiamo le seguenti proposizioni atomiche:

A = Ada legge
B = il babbo è felice

Modus ponens

Assumiamo come premesse le proposizioni:

1. A ì B cioè: se Ada legge, allora il babbo è felice
2. A cioè: Ada legge

una conseguenza logica è B, cioè il babbo è felice

Modus tollens

Se invece assumiamo come premesse le proposizioni:

1. A ì B cioè: se Ada legge, allora il babbo è felice
2. Ė B cioè: il babbo non è felice

una conseguenza logica è Ė A, cioè Ada non legge.

La doppia implicazione.

È comodo introdurre anche il connettivo "doppia implicazione":

Scriviamo α ↔ β come abbreviazione di (α → β) ∧ (β → α) .

Come si vede immediatamente, la doppia implicazione riflette all'interno del linguaggio la nozione di equivalenza logica (che è meta-linguistica), cioè:

⊨ α ↔ β se e solo se α ø β

Esercizio facile: scrivere la tavola di verità per il connettivo é .

α	β	α é β
F	F	T
F	T	F
T	F	F
T	T	T

Il gioco fra la negazione e gli altri connettivi.

Come portare la negazione all'interno di una formula: leggi di de Morgan.

A quale proposizione equivale la proposizione Ė(A ∧ B) ?

Esempio: non [è vero che] (Ada studia e Lea dorme)

Qualcuno risponderà: Ada non studia e Lea non dorme.

Sbagliato!

Affinché non sia vero che Ada studia e Lea dorme, basta che una delle due componenti sia falsa, cioè che Ada non studi o Lea non dorma (o che succedano entrambe le cose!)

Vale anche il viceversa: se Ada non studia o Lea non dorme allora non è vero che Ada studia e Lea dorme. Insomma:

Ė(A ∧ B) ø ĖA ∨ ĖB

Nella notazione "aritmetica":

¼(A ò B) = ¼ A + ¼ B

Verificare la legge di de Morgan tramite le tavole

A	B	A ∧ B	Ė (A ∧ B)	Ė A	Ė B	ĖA ∨ ĖB
F	F					
F	T					
T	F					
T	T					

Verificare la legge di de Morgan tramite le tavole

A	B	A ∧ B	Ė (A ∧ B)	Ė A	Ė B	ĖA ∨ ĖB
F	F	F				
F	T	F				
T	F	F				
T	T	T				

Verificare la legge di de Morgan tramite le tavole

A	B	A ∧ B	Ė (A ∧ B)	Ė A	Ė B	ĖA ∨ ĖB
F	F	F	T			
F	T	F	T			
T	F	F	T			
T	T	T	F			

Verificare la legge di de Morgan tramite le tavole

A	B	A ∧ B	Ė (A ∧ B)	Ė A	Ė B	ĖA ∨ ĖB
F	F	F	T	T		
F	T	F	T	T		
T	F	F	T	F		
T	T	T	F	F		

Verificare la legge di de Morgan tramite le tavole

A	B	A ∧ B	Ė (A ∧ B)	Ė A	Ė B	ĖA ∨ ĖB
F	F	F	T	T	T	
F	T	F	T	T	F	
T	F	F	T	F	T	
T	T	T	F	F	F	

Verificare la legge di de Morgan tramite le tavole

A	B	A ∧ B	Ė (A ∧ B)	Ė A	Ė B	ĖA ∨ ĖB
F	F	F	T	T	T	T
F	T	F	T	T	F	T
T	F	F	T	F	T	T
T	T	T	F	F	F	F

Verificare la legge di de Morgan tramite le tavole

A	B	A ∧ B	Ė (A ∧ B)	Ė A	Ė B	ĖA ∨ ĖB
F	F	F	T	T	T	T
F	T	F	T	T	F	T
T	F	F	T	F	T	T
T	T	T	F	F	F	F

Le due colonne corrispondenti rispettivamente alle formule Ė(A ∧ B) e ĖA ∨ ĖB sono uguali, quindi le due formule sono logicamente equivalenti.

L'altra legge di de Morgan

Per la negazione della disgiunzione vale una legge simmetrica della precedente:

non [è vero che] (Ada studia o Lea dorme)

è equivalente a

Ada non studia e Lea non dorme.

Le due leggi di de Morgan per la negazione sono quindi:

Ė (α ∧ β) ø Ė α ∨ Ė β
Ė (α ∨ β) ø Ė α ∧ Ė β

In un certo senso, la negazione trasforma la congiunzione nella disgiunzione e viceversa.

Esercizio: si verifichi tramite la tavola di verità la seconda legge di de Morgan.

Augustus de Morgan

Madras (India),1806 - Londra,1871

Figlio di un ufficiale inglese residente in India ma rientrato in Inghilterra sette mesi dopo la sua nascita. Vita interessante ed infelice, vedi wikipedia.

Altre equivalenze logiche notevoli

La doppia negazione è un'affermazione:

Ė Ė α ø α

L'implicazione equivale ad una disgiunzione, poiché α implica β se e solo se α è falso oppure β è vero:

α ì β ø Ė α ∨ β

La negata di un'implicazione è quindi una congiunzione, poiché α non implica β se e solo se α è vero e β è falso:

Ė (α ì β) ø α ∧ Ė β

Se α implica β, allora non α implica non β, e viceversa:

(α ì β) ø (Ė β ì Ė α)
(contrapositio)

Esercizio: si verifichino le equivalenze tramite le tavole di verità.

Esempi di *contrapositio*

"se c'è il sole, allora Ada va a sciare"

è logicamente equivalente a

"se Ada non va a sciare, allora non c'è il sole"

"se due rette formano con una trasversale angoli corrispondenti uguali, sono parallele"

è logicamente equivalente a

"se due rette non sono parallele, allora non formano con una trasversale angoli corrispondenti uguali"

Non servono tanti connettivi … ne bastano due …

Osserva: si ha, ad esempio

(1) α ∨ β ø Ė(Ė α ∧ Ė β)

infatti è Ė(Ė α ∧ Ė β) ø Ė Ė α ∨ Ė Ė β ø α ∨ β

Allora si può assumere la (1) come definizione di α∨ β: cioè considerare α ∧ β come abbreviazione di Ė(Ė α ∨ Ė β).

La proposizione "Ada studia o Bea studia" deve allora essere considerata come abbreviazione della proposizione

"non accade che Ada non studia e Bea non studia"
o "non è vero che né Ada studia né Bea studia"

La coppia di connettivi ∧, Ė è sufficiente ad esprimere tutti gli altri: cioè ogni altro connettivo è definibile per mezzo di ∧ e Ė .

Alternativamente, anche la coppia ∨, Ė permette di definire tutti gli altri, e così pure la coppia ì , Ė .
Insomma, bastano la negazione e un solo altro connettivo.

… anzi, ne basta uno!

Consideriamo il connettivo definito dalla tavola qui sotto, detto Sheffer stroke oppure nand (cioè "not and"), equivalente appunto alla negazione della congiunzione, e indicato spesso in logica con il simbolo "|" (barra verticale) :

α	β	α | β
F	F	T
F	T	T
T	F	T
T	T	F

Si può constatare facilmente che tutti gli altri connettivi sono definibili per mezzo di esso (esercizio: verificare!):

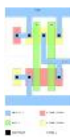
Ė α ø α | α, α ∧ β ø (α | β) | (α | β), α ∨ β ø (α | α) | (β | β)

α ì β ø α | (β | β)

Logica ed elettronica.

Ovviamente esprimere tutte le formule solo per mezzo del nand non è molto comodo ...

L'interesse di questa riducibilità a un solo connettivo sta nella sua utilizzabilità per la fabbricazione di circuiti elettronici che realizzino formule booleane, i cosiddetti circuiti logici combinatori, che sono componenti essenziali dei computer e di ogni genere di dispositivi: grazie infatti alla suddetta proprietà, qualunque circuito logico si può realizzare utilizzando un solo tipo di componente elementare, il nand gate (porta nand), prodotto ad es. in tecnologia CMOS.



Altri esempi.

Come si definirebbe la congiunzione per mezzo della freccia?

Si ha: α ∧ β ø Ė (α ì Ė β)

Sarebbe come dire che:

"Ada studia e Bea studia" è un'abbreviazione per:

"non accade che se Ada studia allora Bea non studia"

che non è un modo intuitivo di esprimere la congiunzione ...
Vien da dire: e se Ada non studia? ma allora l'implicazione interna è vera, quindi la sua negazione è falsa …
Meglio lasciar perdere le "traduzioni" in lingua naturale …

Nota: vedremo che nella logica intuizionista, che è una logica importante per l'informatica, non fondata sulla nozione di verità (bensì su quella di "dimostrazione"), tale interdefinibilità degli operatori logici non sussiste più.

La freccia come disgiunzione.

In realtà, conviene piuttosto assumere come connettivi primitivi la negazione, la disgiunzione e la congiunzione, le cui tavole di verità sono le più intuitive, e considerare l'implicazione come abbreviazione di una disgiunzione, cioè

α ì β come abbreviazione di Ė α ∨ β

il che è molto semplice e facile da ricordare:

α ì β "vuol dire" che o α non è vero, e allora non importa se β è vero o falso, oppure, se α è vero, allora è vero anche β.

Altre equivalenze logiche relative all'implicazione

α ì (β ì θ) ø (α ∧ β) ì θ

Dire che α implica che se β allora θ equivale a dire che "α e β" implica θ.

Esempio:

"se c'è il sole, allora se la seggiovia funziona Ada va a sciare"

è logicamente equivalente a

"se c'è il sole e la seggiovia funziona, Ada va a sciare"

Più in generale:

α_1 ì (α_2 ì (… (α_n ì θ) ø ($\alpha_1 \wedge \alpha_2 \wedge$ … α_n) ì θ

"se c'è il sole, allora, se la seggiovia funziona, se non fa freddo Ada va a sciare" è logicamente equivalente a

"se c'è il sole e la seggiovia funziona e non fa freddo, allora Ada va a sciare"

Tautologie contenenti l'implicazione

α ì α ogni formula implica se stessa (banale!)

α ì (β ì α)
se una formula è vera, allora è implicata da qualunque formula

Ė α ì (α ì β)
se una formula è falsa, allora essa implica qualunque formula

(α ì (β ∧ Ė β))) é Ė α
una formula implica una contraddizione se e solo se è falsa.

ecc.

Visione insiemistica

Se consideriamo le proposizioni come insiemi di elementi di un qualche universo U, dove una proposizione A è l 'insieme degli elementi di U che godono di una proprietà A, si ha la seguente corrispondenza fra connettivi proposizionali e operazioni insie-mistiche:

congiunzione	= intersezione	∩
disgiunzione	= unione	∪
negazione	= complemento	

La relazione di conseguenza logica corrisponde all'inclusione.

Vedi figure disegnate alla lavagna.

Forme normali

Sono delle particolari "forme" di proposizioni composte.

Forma normale congiuntiva (conjunctive normal form, cnf)

È una formula costituita da una congiunzione di disgiunzioni di atomi, semplici o negati. Ad esempio:

(A∨Ė B∨C) ∧ B ∧ (Ė C∨D) ∧ ... ∧ (Ė A∨D ∨ Ė F∨ Ė G)

Si noti che la negazione può comparire solo applicata ad atomi: non si può avere, ad es. Ė (B∨C).

Forma normale disgiuntiva (disjunctive normal form, dnf)

È una formula costituita da una disgiunzione di congiunzioni di atomi, semplici o negati. Ad esempio:

(A ∧ Ė B ∧ C) ∨ B ∨ (Ė C ∧ D) ∨ ... ∨ (Ė A ∧ D ∧ Ė F ∧ Ė G)

Si noti che la negazione può comparire solo applicata ad atomi: non si può avere, ad es. Ė (B ∧ C).

Forme normali

Si può dimostrare che una qualunque formula booleana si può trasformare sia in una forma normale congiuntiva che in una forma normale disgiuntiva logicamente equivalenti ad essa.

Esempio:

¬((A ∨ ¬B) ì C) ì (D ∧ ¬E) ricorda: α ì β ø Ė α ∨ β
¬¬((A ∨ ¬B) ì C) ∨ (D ∧ ¬E)
((A ∨ ¬B) ì C) ∨ (D ∧ ¬E) ricorda: α ì β ø Ė α ∨ β
(¬(A ∨ ¬B) ∨ C) ∨ (D ∧ ¬E) ricorda de Morgan
((¬A ∧ B) ∨ C) ∨ (D ∧ ¬E)
(¬A ∧ B) ∨ C ∨ (D ∧ ¬E) (dnf)
...
(¬A ∨ C ∨ D) ∧ (¬A ∨ C ∨ ¬E) ∧ (B ∨ C ∨ D) ∧ (B ∨ C ∨ ¬E) (cnf)

Analogia con l'algebra:
l'espressione (a+b)(c+d) ha forma normale ac+ad+bc+bd

Digressione su logica e lingua naturale.

Attenzione agli errori logici!

L'implicazione non si può invertire!

Da σ ì τ non si ha come conseguenza τ ì σ !

Esempio.

Da Se Joe è un cavallo, allora Joe ha la coda.

non si può ottenere come conseguenza:

Se Joe ha la coda, allora Joe è un cavallo.

Eppure questo ragionamento errato viene spesso fatto nei discorsi politici, nei discorsi da bar, ecc.
Al più si può fare la *congettura* che Joe sia un cavallo, sapendo che può rivelarsi errata, perché magari è un asino ...

Attenzione agli errori logici!

L'implicazione non si può invertire!

Da σ ì τ non si ha come conseguenza τ ì σ !

Esempio.

Da Se Joe è un cavallo, allora Joe ha la coda.

non si può ottenere come conseguenza:

~~Se Joe ha la coda, allora Joe è un cavallo.~~

Eppure questo ragionamento errato viene spesso fatto nei discorsi politici, nei discorsi da bar, ecc.

Al più si può fare la *congettura* che Joe sia un cavallo, sapendo che può rivelarsi errata, perché magari è un asino ....

Attenzione agli errori logici!

La negazione non è distributiva sull'implicazione!

Da σ ì τ non si ha come conseguenza Ė σ ì Ė τ !

Esempio.

Da Se Joe è un cavallo, allora Joe ha la coda.

non si può ottenere come conseguenza:

~~Se Joe non è un cavallo, allora Joe non ha la coda.~~

perché, anche qui, Joe potrebbe essere un asino con la coda.

È invece corretta, come abbiamo visto, la

Contrapositio

Da σ ì τ si ha come conseguenza Ė τ ì Ė σ !

In un certo senso: la negazione cambia verso alla freccia.

Da Se Joe è un cavallo, allora Joe ha la coda.

si ha come conseguenza:

Se Joe non ha la coda, allora Joe non è un cavallo.

L'ambiguità delle lingue naturali: se.

Nelle lingue naturali, il significato delle parole e delle frasi è spesso molteplice, ricco di sfumature, non perfettamente determinato.

1) "Se c'è bel tempo, Ada va a sciare."

Che cosa fa Ada se non c'è bel tempo?

Può darsi che vada lo stesso a sciare!

2) "Ada va a sciare se c'è bel tempo."

La frase 2 ha lo stesso significato della 1 ?

3) "Ada va a sciare solo se c'è bel tempo."

Nel linguaggio comune, le frasi 2 e 3 hanno quasi lo stesso significato, diverso da quello della 1.

Nell'uso ordinario della lingua il significato della congiunzione "se" è ambiguo, e assume sfumature diverse a seconda del contesto e della posizione nella frase.

Solo se.

Dire "Ada scia solo se è bel tempo" vuol dire che

se Ada scia, deve esserci bel tempo, se no non scierebbe.

Quindi dire "Ada scia solo se è bel tempo"

equivale a dire "se Ada scia, allora è bel tempo".

Ada scia ì è Bel tempo

A solo se B equivale a se A, allora B cioè A ì B

Invece "Ada scia se è bel tempo" viene di solito considerato, nel linguaggio della matematica, diversamente dall'italiano naturale, come equivalente a "se è bel tempo, allora Ada scia".

Cioè, per i matematici,

A se B equivale a se B, allora A cioè B ì A

Se e solo se.

Quindi la comune espressione del linguaggio matematico

A se e solo se B, spesso abbreviata in A sse B,

in inglese "A if and only if B", spesso abbreviata in "A iff B",

equivale a: se A allora B, e se B allora A

cioè alla doppia implicazione (che corrisponde, nel linguaggio logico, all'equivalenza logica fra proposizioni del linguaggio):

A ↔ B

A ø B

Esempio: Ada scia se e solo se è bel tempo.

Ovviamente "A sse B" è lo stesso che "B sse A":

È bel tempo se e solo se Ada scia!

Ma …

Vi sono tuttavia dei contesti, ad esempio le definizioni, in cui anche nel linguaggio matematico (non logico) una frase della forma "A se B" è intesa proprio nel senso di "A se e solo se B".

Esempi: Un insieme ordinato si dice denso se, comunque presi due elementi ... ecc.

Un triangolo si dice equilatero se …

Ovviamente, un insieme è denso, o un triangolo è equilatero, se e solo se soddisfa alla condizione enunciata nella rispettiva definizione !

Tuttavia nelle definizioni il "solo se" viene spesso omesso, cioè lasciato implicito.

D'altra parte, la maggior parte dei matematici non sono direttamente dei logici matematici …

Fine della digressione.

La logica (proposizionale, e non solo) vista attraverso la "lente computazionale".

Difficoltà di calcolo.

Come abbiamo visto, i problemi di stabilire:

- se una formula è conseguenza logica di un'altra (o più in generale di un insieme di formule) o no;
- se una formula è valida (cioè è una tautologia) o no;
- se una formula è soddisfacibile o no;

sono fra loro connessi:

stabilire se una formula è conseguenza di certe altre equivale a stabilire se una formula (contenente la freccia) è una tautologia, cioè se la sua negata non è soddisfacibile, ecc.

Si risolvono tutti costruendo la tavola (o le tavole) di verità della formula (o delle formule) per cui ci si pone la domanda, ed esaminando poi tali tavole. I procedimenti, come abbiamo visto, sono del tutto meccanici e noiosi: sono algoritmi semplici la cui esecuzione può essere affidata ad un computer. O no?

Difficoltà di calcolo: osservazioni generali.

È evidente che il tempo necessario per stabilire se una formula è contraddittoria, o soddisfacibile, o tautologica, è (nel caso peggiore) proporzionale al numero di righe della tavola di verità della formula.

Ma abbiamo visto che la tavola di una formula contenente n formule atomiche distinte ha 2^n casi (righe), e che il valore di 2^n cresce con rapidità spaventosa al crescere di n.

Poiché ad es. 2^{1000}] 10^{300}, nemmeno il più potente computer presente o futuro sarebbe in grado di eseguire l'algoritmo per una formula con 1000 componenti atomiche !

(e 1000 non è un numero troppo grande, in certe applicazioni ingegneristiche).

Soddisfacibilità: tempo di calcolo.

Ricorda: una formula si dice soddisfacibile se c'è una assegnazione di valori di verità (alle componenti atomiche della formula) che rende la formula vera, altrimenti si dice contraddittoria.

Allora il modo intuitivo più efficiente per determinare se una formula è soddisfacibile oppure contraddittoria consiste nel calcolare la tavola di verità della formula riga per riga (invece che colonna per colonna, come - per ragioni didattiche - nelle slides precedenti).

Cioè per ciascuna combinazione di valori degli atomi (riga) si calcola il valore della formula, e ci si ferma appena si trova una combinazione di valori per cui il risultato è true.

Se si è fortunati (caso migliore) una (o la) combinazione buona la si trova subito, se si è sfortunati la si trova in una delle ultime righe; se la formula è contraddittoria, per saperlo occorre aver calcolato tutti i casi.

Trovare è difficile, verificare è facile.

Mediamente, si può assumere che una combinazione "buona" si trovi a circa metà della tavola: il numero di righe da calcolare sarà quindi circa $2^n/2$, se n è il numero di atomi distinti.

Il tempo di calcolo è quindi, nel caso peggiore e nel caso medio, proporzionale a $L \cdot 2^n$, dove L è la "lunghezza" della formula; al crescere di n il tempo cresce in modo esponenziale rispetto a n; se consideriamo i casi in cui il numero di atomi distinti è circa proporzionale alla lunghezza L della formula, il tempo di calcolo cresce in modo esponenziale rispetto a L.

Al contrario, se supponiamo di conoscere già magicamente una soluzione, cioè una combinazione di valori che rende vera la formula, per verificare che la combinazione è proprio "giusta" basta calcolare il valore della formula per quei valori, il che si fa in un tempo proporzionale alla lunghezza L della formula.

Forme particolari.

In casi particolari si possono adottare algoritmi polinomiali: ad esempio, se la formula è una forma normale disgiuntiva, cioè una disgiunzione di congiunzioni di atomi (negati o no), come

A ∧ Ė B ∧ Ė A ∨ Ė B ∧ Ė D ∧ B ∧ F ∨ B∧D ∧ Ė E ∨ ...

basta percorrere la formula (ad esempio da sinistra a destra) e appena si trova una congiunzione che non contiene un atomo e il suo negato (nell'esempio la terza) si sa che la formula è soddisfacibile.

Per una formula booleana di forma generica, tuttavia, non sono noti algoritmi radicalmente diversi da quello del "provarle tutte", che quindi richiede un tempo esponenziale.

Ma un momento! Abbiamo detto che qualunque formula si può trasformare in forma normale disgiuntiva: allora basta fare la trasformazione, e poi la soluzione è facile! Dove sta l'inghippo? Pensateci!

Forme particolari

Per forme normali congiuntive in cui ogni disgiunzione sia costituita di non più di 2 atomi, come

(A∨Ė B) ∧ B ∧ (Ė C∨D) ∧ (E∨ F) ∧ ... ∧ (Ė A∨ Ė F)

(il cosiddetto problema 2-SAT), c'è un algoritmo risolvente il cui tempo di calcolo cresce solo polinomialmente al crescere della lunghezza della formula: anche in questo caso, infatti, si può risolvere il problema senza costruire la tavola di verità.

Però già per forme normali congiuntive in cui ogni disgiunzione possa essere costituita da non più di 3 atomi (il cosiddetto problema 3-SAT) non si conoscono algoritmi polinomiali.

Il problema 3-SAT è difficile come il problema SAT generico.

Problemi simili.

Vi sono molti problemi per i quali trovare la soluzione positiva, se esiste, è difficile, verificare che una soluzione proposta è davvero una soluzione è facile:

- scomposizione in fattori: scomporre in fattori primi un numero molto grande è difficile (bisogna "provarli tutti"); verificare che una scomposizione è corretta è facile, basta fare il prodotto;
- cammino hamiltoniano: trovare un cammino in un grafo (ad es. una rete stradale) che tocchi tutti i nodi del grafo (le località della rete) senza passare due volte dalla stessa località è difficile; se si ha il cammino hamiltoniano, verificarlo è facile;
- problema del commesso viaggiatore: data una lista di città e per ciascuna coppia di città la loro distanza, trovare un percorso che visiti tutte le città una volta sola ritornando al punto di partenza e la cui lunghezza totale sia inferiore a un valore prefissato è difficile; la verifica è facile.

Classi di problemi: P ed NP.

- classe P: informalmente, è la classe dei problemi che possono essere risolti "facilmente", cioè in tempo polinomiale, cioè che non cresce esponenzialmente con la dimensione dell'input;
- classe NP: informalmente, è la classe dei problemi per i quali, se viene fornita una soluzione, controllare se tale soluzione è corretta è facile (si può fare in un tempo non esponenziale).

La classe NP ovviamente contiene la classe P, perché se si sa risolvere facilmente un problema, a maggior ragione si sa controllare facilmente se la soluzione è corretta.

Vi sono tuttavia molti problemi, come quelli elencati nella slide precedente, per i quali la verifica della soluzione è facile (cioè sono problemi NP), ma per i quali nessuno è riuscito finora a inventare un algoritmo non esponenziale per trovare la soluzione. Si sospetta quindi fortemente che tali problemi siano in NP ma non in P. Tuttavia ...

Un problema da un milione di dollari

Benché nessuno sia finora riuscito a trovare per tali problemi algoritmi polinomiali, nessuno è riuscito a dimostrare che tali algoritmi efficienti non possono esistere, e che quindi la classe NP non coincide con la classe P, ma è davvero più grande.

Il problema è dunque: trovare tali algoritmi, oppure dimostrare che non possono esistere.

P = NP o P ≠ NP ?

È uno dei 7 grandi
Problemi Matematici del Millennio (Millennium Prize Problems) compresi nella lista redatta dal Clay Institute of Mathematics, che per la risoluzione di ognuno di essi ha messo in palio un milione di dollari.

Buona fortuna!

Le formule famose di Homer Simpson

P = NP ?

formula di Eulero

e$^{i®}$ +1 = 0

Tutte le volte che di un problema è facile verificare se una soluzione proposta è corretta, tale soluzione è anche facile da trovare?

Come cercare un ago in un pagliaio.

NP è una classe di problemi che si risolvono con una ricerca esaustiva in uno spazio enorme di possibili combinazioni di elementi.

Il problema P vs. NP è: si possono risolvere questi problemi senza effettuare la ricerca, bensì sfruttando qualche finora ignota proprietà della soluzione?

Servirebbe una potente calamita per estrarre l'ago dal pagliaio senza cercarlo!

Precisazione: problemi di decisione.

Chiamiamo "problema di decisione" un problema consistente nello stabilire se un certo dato o insieme di dati ha una certa proprietà oppure no.

Ossia è un problema la cui risposta è si o no (vero o falso).

Esempi:

- data una formula logica: è una tautologia o no?
- data una formula logica: è soddisfacibile o contraddittoria?
- dato un numero naturale: è un numero primo o composto?
- dato un numero naturale: ha un fattore primo < di un dato k?
- dato un insieme di numeri naturali: si può dividere in due parti tali che la somma degli elementi di una parte sia uguale alla somma degli elementi dell'altra?
- dato un grafo: c'è un cammino hamiltoniano o no?
- ecc.

Allora, più precisamente:

- classe P: è la classe dei problemi di decisione per i quali la risposta è facile, cioè può essere trovata in tempo polinomiale, cioè che non cresce esponenzialmente con la dimensione dell'input;
- classe NP: è la classe dei problemi di decisione per i quali la correttezza della risposta SI è facile da verificare: cioè per i quali, se viene fornito il dato o i dati che permettono la risposta SI (ad es. la riga della tavola, o i fattori primi del numero, ecc.) la verifica della correttezza della risposta si può fare in tempo polinomiale;
  esempio: il problema della soddisfacibilità booleana;
- classe co-NP: è la classe complementare di NP, cioè la classe dei problemi di decisione per i quali è facile da verificare la correttezza della risposta NO;
  esempio: stabilire se una formula booleana è una tautologia.

Nota terminologica

NP sta per Nondeterministico Polinomiale.

NP è infatti la classe dei problemi che si risolverebbero in tempo polinomiale se ogni volta che si deve scegliere quale strada seguire (ad esempio quale riga di una tavola di verità calcolare):

- un "oracolo" indicasse la scelta giusta;
- oppure, equivalentemente, se quando si devono effettuare n calcoli indipendenti fra loro (ad es. quelli delle n righe di una tavola di verità), si potessero creare n cloni della CPU (unità centrale di calcolo del computer) che effettuano i calcoli in parallelo;
  nel caso delle tavole di verità ciò evidentemente richiederebbe una crescita esponenziale del numero delle CPU.

NP e co-NP

Si dimostra facilmente che se fosse NP = P, allora sarebbe anche co-NP = P. Se ci fosse un modo "facile" per stabilire se una formula è soddisfacibile, ci sarebbe anche un modo "facile" per stabilire se una formula è una tautologia, cioè la lunghezza della dimostrazione che una formula è una tautologia crescerebbe in modo polinomiale rispetto alla lunghezza della formula: formule "corte" avrebbero sempre dimostrazioni "corte".

Problemi NP-completi.

Nella classe dei problemi NP vi sono numerosi problemi, e fra questi la soddisfacibilità booleana, tali che, se si disponesse di un algoritmo efficiente (cioè polinomiale) per risolvere uno di essi, un tale algoritmo potrebbe essere sfruttato per risolvere in modo efficiente tutti i problemi NP.

I problemi di questo tipo vengono detti NP-completi e sono i problemi più difficili all'interno della classe dei problemi NP.

Altri problemi NP-completi sono:

- il problema del commesso viaggiatore;
- il problema della colorazione dei nodi di un grafo usando un numero massimo prefissato di colori in modo che nessun nodo abbia lo stesso colore di un suo vicino;
- il problema di scomporre un numero in fattori primi;
- il sudoku di dimensione arbitraria.

Dimostrare contro verificare.

Vedremo, studiando la logica predicativa del prim'ordine (che è quella in cui si esprimono normalmente le teorie matematiche), che il problema di stabilire se un enunciato matematico è dimostrabile è un problema insolubile.

Invece il problema di stabilire se un enunciato matematico è dimostrabile con una dimostrazione più corta di una data lunghezza n è risolubile, per mezzo un metodo banale.

Infatti, dato uno qualunque dei grandi problemi insoluti della matematica, ad esempio quello di dimostrare la congettura di Goldbach, basta generare tutte le possibili dimostrazioni corrette di lunghezza minore di n (ad es. tutte quelle composte da non più di 1 milione di simboli, equivalente a circa 350 pagine), e controllare se fra di esse vi è la dimostrazione dell'enunciato cui si è interessati! Ma con tale metodo non basterebbe un tempo pari all'età dell'universo per avere la risposta!

Dimostrare contro verificare

Non stupisce quindi sapere che il problema di stabilire se un enunciato matematico è dimostrabile con una dimostrazione più corta di una data lunghezza n è un problema NP-completo.

Se per caso fosse NP = P, ciò vorrebbe dire che una macchina potrebbe fornire la risposta in un tempo ragionevole: la creatività dei matematici potrebbe quindi essere sostituita dalle macchine. I matematici non sarebbero più necessari … non più di quanto sia oggi necessario saper fare a mano le quattro operazioni (ci sono le calcolatrici) o calcolare una derivata o un integrale di funzione elementare: raffinati sistemi software lo fanno per voi …

Ma nessuno crede che sia NP = P !

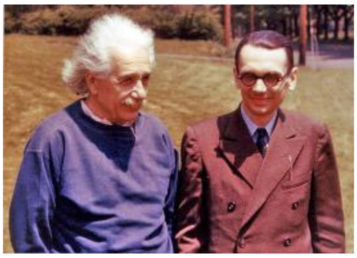
Alla fine degli anni '80, viene trovata a Princeton una sorprendente lettera del 1956 di Gödel a von Neumann.

"[…] Die Frage ist, wie rasch $\varphi(n)$ für eine optimale Maschine wächst. […] Wenn es wirklich eine Maschine mit $\varphi(n)$ ¼ $k \cdot n$ (oder auch nur $k \cdot n^2$) gäbe, hätte das Folgerungen von der grössten Tragweite. Es würde nämlich offenbar bedeuten, dass man trotz der Unlösbarkeit des Entscheidungsproblems die Denkarbeit des Mathematikers bei ja-oder-nein Fragen vollständig durch Maschinen ersetzen könnte."

"… La questione è: quanto rapidamente cresce $\varphi(n)$ per una macchina ottimale? […] Se ci fosse davvero una macchina con $\varphi(n)$ ¼ $k \cdot n$ (o anche solo $k \cdot n^2$), […] il lavoro intellettuale del matematico sulle questioni "si o no" potrebbe essere completamente sostituito da macchine"

Gödel nel 1956 aveva già individuato il problema P =? NP, poi introdotto formalmente da Cook, Levin, Karp nel 1971 !

Tre giganti della prima metà del '900: Albert Einstein, Kurt Gödel, John von Neumann



Ulm (Germania) 1879	Brno 1906 (Impero Asburgico)	Budapest, 1903
Princeton (USA) 1955	Princeton (USA) 1978	Washington, 1957

Tre giganti di oggi: Cook, Levin, and Karp

Stephen Cook, 1939, Buffalo (USA)

Leonid Levin, 1948, Dnepropetrovsk, Ucraina, Unione Sovietica

Richard Karp, 1935, Boston (USA).

L'importanza del sudoku …

Allora, per risolvere il problema P = NP o P ≠ NP ? basta concentrarsi su un singolo problema NP-completo, e:

- o trovare un algoritmo polinomiale che lo risolve;
- oppure (più probabilmente) dimostrare che un tale algoritmo non può esistere.

Esempio: chi trovasse un algoritmo in grado di risolvere rapidamente (cioè in tempo polinomiale) un qualsiasi sudoku di qualunque dimensione, sarebbe in grado di risolvere rapidamente, utilizzando tale algoritmo, i problemi del commesso viaggiatore, della scomposizione in fattori … e sarebbe quindi in grado di violare tutti i sistemi di sicurezza di banche, governi, …, che dipendono, in ultima analisi, dalla difficoltà della scomposizione in fattori.

L'importanza del sudoku

Anzi, come si è accennato, lo scopritore potrebbe sfruttare il suo algoritmo per risolvere tutti gli altri grandi problemi insoluti della matematica, come gli altri sei problemi dell'Istituto Clay, e vincere così non 1 ma 7 milioni di dollari!

Purtroppo, però, come abbiamo visto, si pensa che un tale algoritmo non esista … Ci sarà ancora e sempre bisogno dei matematici e più in generale della creatività umana.

Scomposizione in fattori e test di primalità

- Il problema della scomposizione in fattori è NP (ma non si sa se sia NP-completo: si pensa che non lo sia).
- Il problema di scomporre un numero composto (grande) nei suoi fattori primi è quindi difficile.
- Dato un numero composto e dati i suoi fattori primi, verificare che la scomposizione è corretta è facilissimo (basta fare la moltiplicazione).
- Su tale asimmetria fra "trovare" e "verificare" si basano tutti gli algoritmi di crittografia oggi usati.
- Invece il problema di stabilire se un numero è primo oppure composto, ma senza necessariamente trovarne i fattori, è un problema per cui nel 2002 è stato trovato da tre ricercatori dell'Indian Institute of Technology di Kanpur un algoritmo polinomiale, basato sulla una nota caratterizzazione della primalità: n è primo se e solo se per $x < n$ è $(x^{n-1} = 1) \bmod n$.

Scomposizione in fattori e computazione quantistica.

Nel 1994 il matematico americano Peter Shor dell'MIT ha ideato un algoritmo di calcolo quantistico che permette di risolvere il problema della scomposizione in fattori in tempo polinomiale, con una probabilità di errore che si può rendere piccola quanto si vuole.

Pertanto, se e quando si costruiranno effettivamente dei computer quantistici, tutti gli attuali sistemi di sicurezza informatici basati sulla cosiddetta crittografia a chiave pubblica diventeranno vulnerabili e perciò inutilizzabili (banche, governi, commercio elettronico, posta elettronica, ecc.)

Ma i ricercatori sono già da tempo al lavoro per mettere a punto sistemi alternativi, di crittografia quantistica!

Ricorda il problema della scomposizione in fattori è NP, ma si crede che non sia NP-completo.

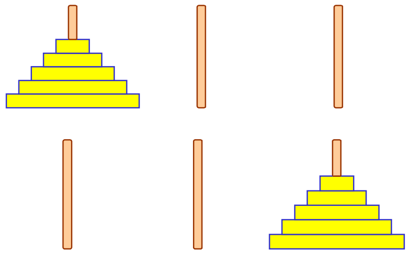
Pertanto, anche se e quando i computer quantistici saranno davvero costruiti, l'algoritmo di Shor non permetterebbe di risolvere efficientemente tutti i problemi NP.

La maggior parte dei ricercatori ritiene che neppure i computer quantistici siano in grado di risolvere i problemi NP-completi in tempo polinomiale, anzi che nessuna tecnologia sia in grado di farlo.

Ancora una volta, sembra che la matematica e la creatività umana rimangano insostituibili …

Ci sono anche problemi non NP !

Ci sono anche problemi per i quali invece si è dimostrato che un algoritmo polinomiale non può esistere: un esempio tipico è il gioco delle torri di Hanoi, in cui la soluzione stessa consiste di un numero di mosse che cresce esponenzialmente con il numero dei dischi.



Ci sono anche problemi non NP: il gioco degli scacchi

- Il bianco muove per primo: esiste una strategia in grado di vincere contro qualunque strategia avversaria? oppure ci sono strategie avversarie contro le quali il bianco può al massimo pareggiare?
- Una soluzione del problema richiederebbe l'esame di tutte le possibili partite di scacchi, che sono un numero finito ma inconcepibilmente grande.
- Ma anche per controllare se una proposta di soluzione è corretta bisognerebbe controllare tutte le possibili partite, anzi, come nel caso delle Torri di Hanoi, la soluzione è essa stessa costituita da un numero inconcepibile di partite!

EXP è più grande di NP

- Ci sono cioè dei problemi, come le Torri di Hanoi o la strategia vincente per il gioco degli scacchi, nei quali anche solo controllare che la soluzione sia corretta richiede un tempo che cresce esponenzialmente con la dimensione dell'input.
- Si tratta quindi di problemi per la cui soluzione non esistono algoritmi efficienti, e sappiamo (si è dimostrato) che non ne possono esistere. Sono i problemi cosiddetti intrattabili: risolubili in teoria, ma non risolubili in pratica, né ora né in futuro, se non per input di dimensione molto piccola (ad es. le Torri di Hanoi con un numero di dischi abbastanza piccolo).
- Come abbiamo detto, si sospetta fortemente che anche i problemi NP siano così, ma nessuno è ancora riuscito a dimostrarlo!

Un gioco di parole …

Nel linguaggio matematico-scientifico anche delle lingue latine si è diffuso l'inglesismo "provare" nel senso di "dimostrare", e "prova" nel senso di "dimostrazione", nonché (anche nel linguaggio comune) l'uso degli avverbi derivati da aggettivi con funzione di predicato, come in

"chiaramente si è sbagliato" per "è chiaro che si è sbagliato", ecc.

Potremmo allora dire che i problemi NP sono problemi

proBabilmente intrattabili ma non proVabilmente intrattabili.

In spagnolo, dove la B e la V si pronunciano nello stesso modo, l'introduzione dell'inglesismo fonderebbe i due avverbi in uno:

probablemente intratable !

In realtà "probablemente" vuol solo dire "probabilmente" (credo), benché "probable" voglia dire sia "probabile" che "dimostrabile"!

Conclusione e proseguimento degli incontri.

Abbiamo visto come la logica proposizionale assomiglia ad una aritmetica con due valori, dotata di operazioni analoghe alle operazioni aritmetiche, ma che obbediscono a leggi un po' diverse.

Abbiamo definito la nozione di conseguenza logica e abbiamo visto che le tavole di verità sono uno strumento che permette di calcolare in modo puramente meccanico conseguenze logiche, equivalenze, ecc.

Nelle prossime lezioni introdurremo un metodo radicalmente diverso per effettuare dei ragionamenti: quello dei sistemi di inferenza o sistemi deduttivi.

Vedremo che per la logica proposizionale si può introdurre un sistema deduttivo che risulta equivalente al metodo delle tavole di verità. Estenderemo poi tale sistema alla logica dei predicati, per la quale le tavole di verità non si possono usare.

Appendice (quasi) filosofica.

Linguaggio e metalinguaggio, sintassi e semantica: qualche estratto da

J-Y. Girard, Le fantôme de la transparence, 2010

Jean-Yves Girard

La logique moderne a imaginé, à la fin du XIXe siècle, un univers de référence a priori ; ainsi Frege a-t-il expliqué que le sens (implicite) d'une proposition réfère à une dénotation (explicite). L'espace des dénotations constitue la sémantique, un mot de novlangue : en effet, l'activité sémantique consiste, la plupart du temps, à obscurcir le sens. Ce que l'on comprendra facilement :

le sens d'une proposition est contenu dans son énoncé, alors que la dénotation vit on ne sait trop où, dans un paradis thomiste à jamais inaccessible. […]

L'explication achoppe sur l'impossibilité d'établir un rapport autre que fantasmatique entre le sens et sa dénotation : quoi que l'on fasse, on ne quitte jamais le domaine du raisonnement et on est en droit de se demander si l'espace sémantique existe réellement.

Jean-Yves Girard

Dans l'entre-deux-guerres, les logiciens polonais (Łukasiewicz, Tarski) ont récrit le paradigme sémantique avec une obstination réductionniste étrangère à l'ébauche frégéenne. […]
Tarski devait passer en revue les primitives logiques et "donner" leur sémantique : celle de la conjonction est une conjonction, celle de la disjonction une disjonction . . .
Ce qui nous ramène au Diafoirus de Molière : l'opium fait dormir à cause de sa *vertu dormitive*.
Pour éviter le reproche de lapalissade, les disciples de Tarski ont fait de la dénotation de la conjonction une méta-conjonction.
Encore un gros mot de lâché, car qu'est ce qu'une méta-conjonction ? Elle réfère, on le pressent, à une méta-méta-conjonction.
Comme dans cette blague de physiciens : le monde repose sur une tortue, qui repose sur autre tortue qui repose … finalement, il y a des tortues "all the way down". […] Oubliant qu'une idiotie ne gagne rien à être répétée, et encore moins transfiniment.

Jean-Yves Girard, nota a pie' pagina:

"Fuite en avant adoubée par le chosisme-léninisme ; ainsi A. Badiou, dans son concept de modèle (Maspéro, 1969) nous apprend-il que vrai et faux réfèrent à vri et fax. Renversant !"

Qui Girard si riferisce con sarcasmo al noto filosofo marxista francese Alain Badiou e a un suo libro del 1969:

"The concept of a model: an introduction to the materialist epistemology of mathematics".

In questo vecchio testo Badiou in effetti dà una presentazione abbastanza tradizionale della logica matematica, con la sua semantica basata sull'insiemistica, e ad una prima occhiata la parte tecnica non sembra nemmeno così male, a parte la trovata di inventarsi i nomi vri e fax per evidenziarne l'assenza di un significato naturale pre-esistente.

Ma oggi Girard mette in discussione proprio la distinzione sintassi/semantica, con un lavoro tecnico tutt'altro che facile.