Università degli Studi di Genova
Inaugurazione dell'anno accademico 2016/2017

VIVA L'INFORMATICA!

Lectio magistralis del prof. Silvio Micali, docente presso il Laboratorio di informatica e intelligenza artificiale del MIT di Boston, USA

Ringrazio innanzitutto il Magnifico Rettore e il Prorettore Piana per il loro gentilissimo invito: è un privilegio augurare un proficuo Anno Accademico a tutti, al personale tecnico amministrativo, ai docenti, agli studenti, anzi, soprattutto agli studenti perché tutto questo è per voi. Devo dire quindi grazie all'Università di Genova e anche alla città di Genova che mi ha accolto a braccia aperte.

Un ciclo universitario, per chi c'è in mezzo e per chi lo sta per cominciare, è un periodo di formazione incredibile: per tutti noi, come umani, continuare a crescere e formarsi è il nostro destino, però diciamo che la formazione universitaria è forse quella che ci rimane per la vita e allora, visto che siamo in tema di ringraziamenti, desidererei appunto ringraziare a nome di tutti chi ci forma e soprattutto in questi corsi universitari; quindi un ringraziamento ai nostri maestri, sia quelli italiani, sia quelli stranieri, ai nostri compagni di corso, ai nostri colleghi e ai nostri studenti. E fra voi studenti quelli che poi diventeranno docenti sapranno senz'altro riconoscere quanto più si impara dai nostri studenti piuttosto che da noi e dai nostri stessi sforzi e dai nostri colleghi: in realtà la docenza ha un'importante funzione enzimatica per mettere davvero a frutto tutti quelli che sono i vostri talenti e il vostro desiderio di imparare. Grazie anche a quelli che ci ispirano da più lontano, perché come ha detto il Rettore, il mondo si sta internazionalizzando e quindi i nostri colleghi e i nostri collaboratori ormai vengono da tutte le parti. Insomma, grazie a tutti perché noi siamo chi siamo grazie a coloro che ci hanno influenzato: se siamo chi siamo, lo dobbiamo a loro.

E adesso passo all'augurio di "apprendimento" e "divertimento", che fanno rima perché in realtà vanno insieme: se non ci si diverte, non si riesce ad apprendere abbastanza profondamente; e anche tanti auguri di dedizione e di passione: io spero che voi troviate il vostro campo, quello che vi ispira e che davvero vi emoziona di più.

Per me questo campo è stato l'informatica: viva l'informatica! Debbo dire che io sono arrivato all'informatica attraverso, prima la fisica, e poi la matematica e devo dire mi sono proprio innamorato. Lo scorso secolo doveva essere quello dell'atomo ed è stato invece quello del computer e direi quasi che l'entrata nella storia umana del computer è forse tanto importante quanto quella del fuoco. La grande Carica di Balaklava è stato un evento a basso contenuto tecnologico: un assalto all'arma bianca, però forse è questa rappresentazione è forse la maniera migliore per trasmettere lei il senso del coraggio, dell'impeto e direi anche quasi dalla ferocia intellettuale con cui l'informatica continua a progredire; non soltanto a fare progredire il proprio campo, ma a dare una mano di collaborazione a tanti altri campi meravigliosi quali la matematica, la biologia, l'economia e la fisica. Debbo dire che, anche se spero che vogliate diventare informatici, qualunque siano i vostri progetti, i vostri sogni, se volete mettere nel vostro zainetto, prima in intraprendere il viaggio, qualche corso di informatica, vi assicuro che non soltanto non vi farà male, ma vi permetterà di andare anche più lontano nei vostri studi.

E adesso parliamo di scienza: il tipo di scienza di cui vorrei parlare si trova all'intersezione tra la matematica e l'informatica; e vorrei parlare di qualcosa che noi tutti conosciamo fin da piccoli e abbiamo sempre amato: le prove. Cominciamo dalle prove: non so qual è stata la vostra prima prova, ma la mia prima prova è stato il Primo Teorema di Conclusione dei Triangoli di Euclide che dice che se due triangoli hanno due lati e l'angolo incluso uguali, allora sono tutti uguali, infatti sono uguali anche gli altri due angoli e l'altro lato che non abbiamo mai misurato. Allora diciamo che, se mettiamo sul piatto della bilancia, partiamo da "poco" – due lati e un angolo – e da questo poco deduciamo che anche tutto il resto è uguale. Sembra un po' misterioso che da quel poco iniziale siamo arrivati ad avere così tanto. Qual è la conclusione? Pensandoci e ripensandoci, alla fine sono giunto alla conclusione che le prove sono molto pratiche e non ho mai cambiato idea perché tu stando al tavolino e

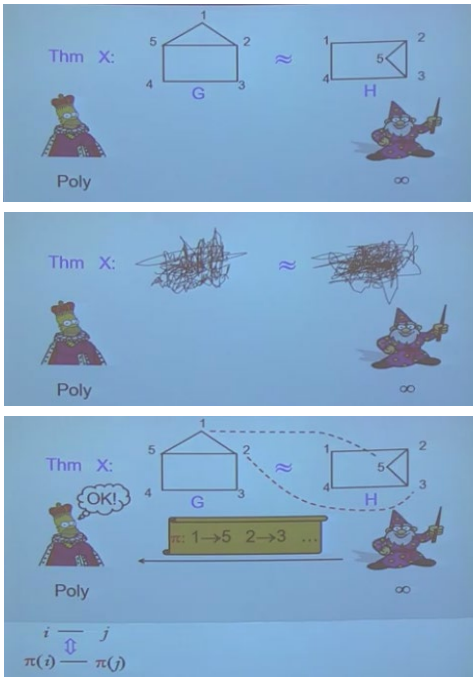
misurando soltanto qualcosa di locale, riesci a risparmiarti il viaggio dall'altra parte per andare a vedere se davvero gli altri angoli e gli altri lati sono uguali.

Dunque, le prove, almeno nella nostra tradizione, vengono dall'antica Grecia e diciamo che da 2500 anni questo concetto classico di prova continua ad evolversi fino ad arrivare a Gödel e Turing a metà del secolo scorso. Due personaggi straordinari: Gödel di stirpe tedesca, anche se era nato in Austria, è stato uno dei matematici più profondi, ma anche più tenaci della storia, era capace di seguire il filo dei suoi pensieri e immergersi nell'oceano da una parte e riemergere con la prova stretta tra i denti dall'altra parte, senza mai fermarsi. Un fenomeno incredibile. Altrettanto incredibile è l'inglese Alan Turing che aveva un approccio totalmente diverso, totalmente intuitivo: per lui risolvere i problemi di matematica e anche formalizzare il concetto di prova, è stato un processo di raffinamento elementare, rendere le cose sempre più semplici, tanto che alla fine il problema si risolve da sé, tanto che viene da chiedersi dove mai fosse stato questo problema, come raccogliere dei fiori un campo fiorito a primavera, una cosa miracolosa.
Questi due personaggi così diversi erano però pienamente in accordo con tutti i loro predecessori da 2500 anni che le prove sono degli oggetti sintattici: ricordiamoci, spero non con dolore, cosa sia una prova: è un elenco minuziosissimo di proposizioni del tipo "invoco l'assioma 1", "deduco la riga 2" e si continua a dedurre fino ad arrivare all'enunciato del teorema *Quod Erat Demonstrandum* (Q.E.D.) e ci si ferma. Nessuno si è mai posto il problema dell'efficienza della prova, perché la prova poteva essere tanto lungo quanto doveva essere, non è che ci sono problemi: i nostri antenati effettivamente avevano un orologio molto più lento del nostro, oggigiorno i tempi sono molto più incalzanti e cominciamo avere tutti quanti molta più fretta di quanto si avesse in passato.

Io ritengo che l'efficienza sia in realtà alla base del concetto di prova perché supponiamo che il lavoro necessario per verificare la prova di un teorema trovato da un altro sia lo stesso tempo di quello richiesto da colui che lo ha enunciato, allora il lavoro della prova diventa inutile perché è necessario ripercorrere gli stessi passi e, di conseguenza, sicuramente si giungerà alla medesima conclusione. Quindi, se vogliamo formalizzare davvero un sistema di prova, dobbiamo avere almeno due personaggi: il provatore, che è alacre e ha a disposizione un tempo infinito per la prova, e il verificatore, che è pigro e ha, in termini tecnici, un *polynomial time*, un tempo dato entro il quale deve essere convinto della prova. Allora il provatore scrive la prova e la dà al verificatore che si dichiara soddisfatto, ma allora quand'è che una prova è efficiente? Negli anni '70, quando gli informatici teorici stavano sviluppando questa nozione di efficienza, si afferma che la prova, per essere efficiente, deve avere due proprietà

1. Deve essere corta (certo, relativamente all'enunciato);
2. Deve essere veloce, facile da verificare.

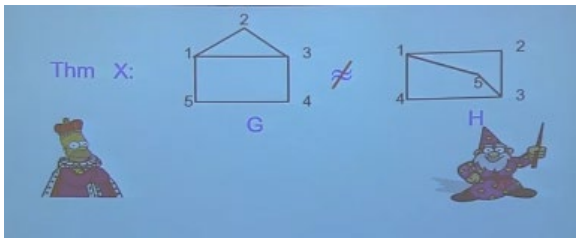
Vediamo un esempio di quella che era una prova efficiente fino agli anni Settanta.

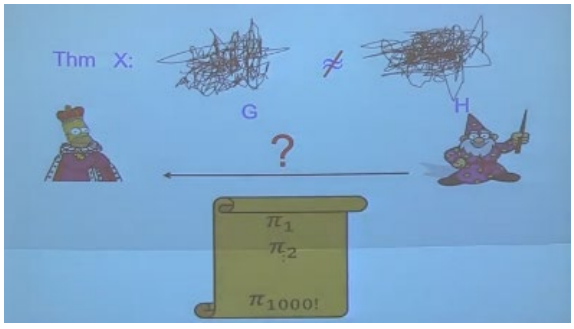


Ecco il Teorema di Hicks: questi due grafi G ed H sono gli stessi, in gergo tecnico sono isomorfi, però sono disegnati in maniera diversa. Si vede a occhio nudo, viene da dire che di certo non serve un teorema.
Prendiamo allora dei grafi un po' più complessi: adesso la risposta alla domanda se questi due grafi sono isomorfi non è chiara e allora cerchiamo di provarlo. Quindi facciamo in piccolo quello che dovremmo fare se questi due grafi fossero di migliaia e migliaia di nodi, archi, quindi di punti e linee.
Quand'è che sono due grafi sono diversi? Quando c'è una connessione biunivoca fra i vertici del primo grafo e il secondo: identifico il vertice 1 col numero 5, identifico il vertice 2 col numero 3 e poi stabilisco che se c'è una "strada" tra 1 e 2, ci deve essere una strada, un arco, fra 5 e 3. Quindi devo "indovinare" la corrispondenza tra i vertici di sinistra e i vertici di destra e poi voi verificherete che per ognuna di queste corrispondenze c'è una "strada" a sinistra *se e solo se* c'è una strada a destra. L'unica cosa che devo dimostrare è la corrispondenza, quindi la verifica è molto veloce.
In realtà, quello che vi ho fatto vedere, segretamente corrisponde a

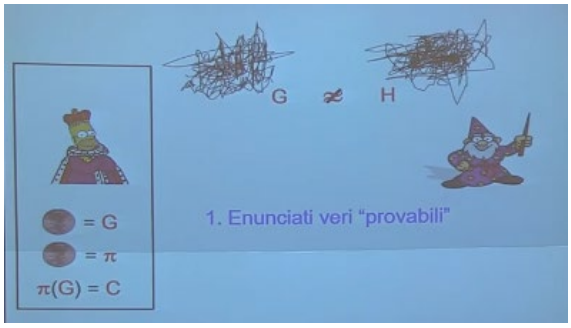
dimostrare che un'equazione ha uno 0, ha una soluzione e, come sapete, questo può essere difficile, però quando qualcuno ve la dà, verificarla è semplice. Quindi l'esistenza della soluzione ha una prova semplice, però supponete che vi dia un'equazione e vi dica "quest'equazione non ha soluzione"; a questo punto come la dimostro? Questo non è chiaro perché non posso andare a verificare tutte le soluzioni false visto che sono infinite. Quindi questo è molto più difficile da dimostrare; ancora più difficile è dire "ah sì, questa equazione ha soluzione: ne ha $2^{116}+17$". Come facciamo? Se anche le fornissi una per una – e non ci sarebbe il tempo, perché pure il sole si spegnerebbe in tutto il tempo che ci vuole per convogliare tutte queste soluzioni –, rimarrebbe sempre il dubbio che ci possa essere un'altra soluzione. Volendo, ci sarebbero anche altre complicazioni che però lasciamo perdere.
Quindi, in realtà anche se la nozione di classica di prova ci è stata utile per migliaia di anni, forse ci sono delle altre cose che noi dovremmo provare che non riusciamo a provare in modo classico; e allora che cosa dobbiamo fare? Dobbiamo cercare di allargare la nozione di prova.

La nozione che voglio proporvi è quella delle Prove Interattive. Cosa sono queste prove interattive? Sono delle prove impostate come giochi. Come tutti sappiamo, l'erario risparmierebbe un sacco di soldi se decidesse di lasciare perdere i problemi dell'università e della scuola e fornisse solo i libri dicendo "Eccovi i libri da studiare, arrivederci". Il costo della pubblica istruzione sarebbe pari al costo dei libri moltiplicato per il numero degli studenti: avremmo un grande risparmio, ma tutti noi sappiamo che quando siamo a tu per tu con un maestro, con un insegnante, in realtà apprendiamo molto più facilmente. Allora perché se noi come umani noi impariamo in questo modo, in maniera interattiva, quando poi formalizziamo la nozione di prova, la esponiamo in "maniera libresca"?





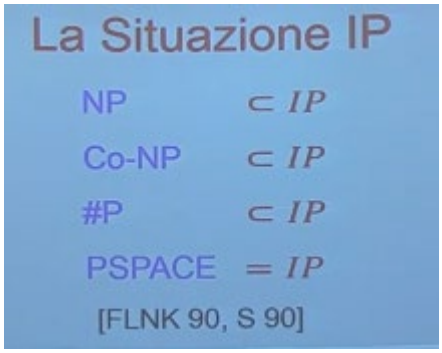
Allora cerchiamo di vedere come può essere convogliata una prova in modo interattivo attraverso un esempio. Voglio dimostrarvi che questi due grafi, che hanno entrambi 5 vertici e lo stesso numero di archi (di strade), non sono in realtà uguali. In questo caso si vede a occhio nudo, però come abbiamo visto in precedenza, non si potrebbe vedere a occhio nudo in altri casi. Per dimostrare che non sono uguali col metodo classico dovrei darvi tutte le possibili corrispondenze, che sono mille fattoriale (un numero stratosferico) e quindi non andremmo da nessuna parte; allora noi vorremmo dimostrare che gli enunciati veri sono provabili perché alla fine la prova consiste di due elementi: vogliamo che tutti i teoremi veri siano dimostrabili e vogliamo anche che nessun teorema falso sia dimostrabile. Tutto il resto è accessorio. Come si fa a dimostrare se questo grafo è davvero diverso dall'altro, a dimostrare che non è lo stesso? Ecco come si fa: il nostro re, che chiamiamo Artù (l'altro, il Mago Merlino, è il provatore) si chiude in una stanza in cui il mago non può vedere e in questa stanza prende una moneta per scegliere a caso tra i due grafici G e H. Supponiamo che scelga G; a questo punto lancia un'altra moneta e sceglie una permutazione dei vertici e cambia il grafo: applicando questa permutazione ottiene un terzo grafo C. Ricordate che, siccome ha soltanto cambiato i nomi dei vertici, per definizione C e G sono lo stesso grafo. A questo punto do il grafo C a Merlino, dicendogli: "tu mi dicevi che G e H non erano lo stesso grafo. Io ho permutato i vertici di uno di questi due. Il grafo C è il risultato della permutazione: di quale dei due grafi ho cambiato il nome?". Per il nostro mago questo problema è una bazzecola perché, avendo tempo infinito, riesce a capire che il grafo scelto prima della permutazione era G. Però il mago deve dimostrare anche che i teoremi falsi non si possono dimostrare. Quale sarebbe il teorema falso? Che Merlino ci dice che i due grafi non sono gli stessi quando



invece lo sono. In questo caso Merlino non è più il buon mago, ma un traditore che ci vuole ingannare, quindi bisogna proteggersi da questo potentissimo mago cattivo.

Questa volta allora il re si chiude di nuovo nella sua stanza, di nuovo lancia una moneta per scegliere fra G e H, sceglie una permutazione dei vertici, cambia di nuovo i nomi dei vertici e presenta il grafo C a Merlino. Questa volta Merlino dice che i grafi sono diversi (quando invece sono uguali) e il re chiede a quale dei due ha cambiato nome. A questo punto Merlino ha un vero problema perché siccome i due grafi sono davvero gli stessi, quando io ne prendo uno a caso e gli cambi il nome, questo, per la proprietà transitiva che tutti noi conosciamo, se G e H sono gli stessi, C è uguale sia a G sia a H. Quindi come fa il povero Merlino a capire a quale dei due grafi il re ha cambiato il nome? Appena apre bocca ha probabilità 1 probabilità su 2 di essere scoperto perché il grafo C è un grafo isomorfo sia G sia di H, sia che io abbia scelto G di partenza, sia che io abbia scelto H di partenza, quindi la probabilità di indovinare è esattamente 1/2; se lo rifacciamo, la probabilità di indovinare tutte e due le volte consecutive è un 1/4 e se la facessimo 300 volte sarebbe $1/2^{300}$. Perché insisto sul numero 300? Perché i miei colleghi fisici mi informano che tutte le particelle elementari dell'universo, molecole, atomi, fotoni, neutrini, tutte sono al massimo 2^{300}, quindi indovinare con questa probabilità è praticamente per noi umani 0.

Quindi eccovi una prova: desidero comunicarvi che in questo momento, nel 2016, abbiamo fatto dei progressi sull'isomorfismo dei grafi, ma non abbiamo trovato ancora una prova corta e veloce per dimostrare l'isomorfismo di due grafi. Però questa prova che ho appena delineato semplicemente a tutti voi è estremamente semplice, è estremamente veloce, prova esattamente tutto quello che è vero e non riesce a farci entrare niente che sia falso, quindi questo è un nuovo concetto di prova; e con questo nuovo concetto di prova – chiamiamole prove interattive – si riesce a dimostrare che un'equazione non ha soluzione, si riescono a contare e provare il numero esatto delle soluzioni e tante altre cose. Se riesce anche a contare e provare il numero esatto delle soluzioni e si riescono a fare tante altre cose.



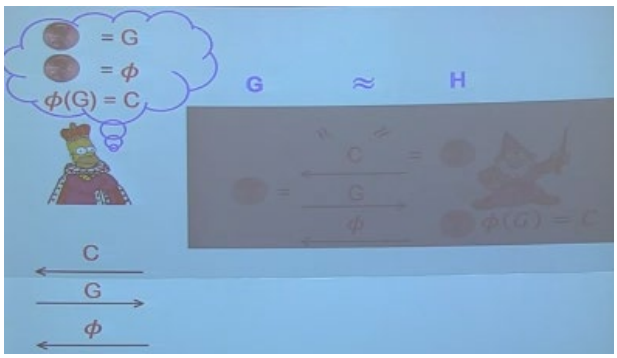
Cosa abbiamo guadagnato con questo nuovo concetto di prova? Tutti abbiamo sentito parlare del famoso cloud computing, ma cloud computing è un nome sbagliato perché noi dalla nuvola non ci facciamo dare le computazioni che ci servono, noi abbiamo *cloud storage*: noi prendiamo i nostri dati e li mettiamo sulla nuvola e quando li vogliamo usare, diciamo alla nuvola "mi dai il dato numero 3?" e la nuvola ce lo restituisce. Il cloud computing è una cosa diversa: supponiamo che il re voglia trovare la funzione f(x), il risultato di una computazione molto molto molto lunga che non può realizzare col suo laptop. In questo caso lo chiede alla nuvola dove sono collegati megacomputer in grado di risolvere complicati problemi computazionali. Il problema, però, è difficile, tanto che persino la nuvola ci mette un mesetto e dopo tutti i calcoli dice al Re "Sire, il risultato di f(x) è 27. Ecco 50 mila euro di fattura per i miei servizi, grazie della Vostra fiducia". E il re chiederebbe "perché dovrei pagati 50mila euro? Come faccio a sapere se il valore che mi hai dato è giusto? Prima di pagare vorrei sapere anche quello". In realtà con queste prove interattive, mentre il tempo di trovare la soluzione del teorema, il tempo di trovare la computazione, può essere lunghissimo noi siamo capaci con un'interazione estremamente rapida e veloce di convincere che la verità è quella e quindi questo crea un mercato della computazione. Oggi come oggi direi che la computazione, la capacità computazionale ha forse più valore anche del petrolio perché noi viviamo di computazione.

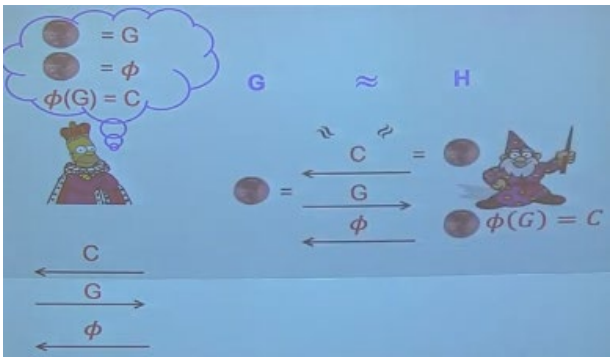
Quindi le prove sono molto pratiche, appena cambiamo un poco il sistema di prova, apriamo addirittura un nuovo mercato. In realtà, io ritengo che, come tutte le cose fondamentali, il concetto di prova è un gigante addormentato e che man mano che noi lo svegliamo, saltano fuori un sacco di altre cose. E vorrei condividere con voi almeno un'ultima di queste: per esempio, poniamoci la domanda "quanta conoscenza è necessaria per la verificabilità di una prova?" perché certamente ce ne deve essere parecchia. E anche una domanda un pochino più impegnata "Che cos'è la conoscenza?". Ma perché fermarci lì, ci sono anche domande ancora più difficili come "C'è vita dopo la morte?". Quindi, che cos'è la conoscenza? È un argomento difficilissimo, lo hanno affrontato Artistotele, Kant, Husserl, non è un problema che si risolve in due secondi. Fortunatamente le domande cambiano: supponiamo che io ho un grave, in questo caso è una chiavetta da computer, e io lo faccio cadere, lo lascio andare. Questo grave cade. Qual è la domanda? Un aristotelico, quando vede questo

fenomeno, si pone anche lui la domanda "che succede?", ma la sua domanda era "dove vuole andare?". Una volta che la domanda è quella, tutta la teoria dei luoghi naturali, cioè che chi ha più terra vuol andare verso la terra, chi è più leggero vuole andare verso il cielo, ha tutto senso; lo stesso fenomeno, 1500 anni dopo, lo testa Galileo Galilei dalla Torre di Pisa, ma la sua domanda è cambiata: lui non vuole più sapere dove vogliono andare questi gravi, bensì come cadono. E una volta che la domanda è cambiata, le cose cambiano e riesce a ricostruire tutto. E per fortuna che le domande cambiano, diversamente staremmo sempre a rimuginare le stesse cose. Quindi non chiediamoci "cosa sia la conoscenza", ma almeno per oggi, per i prossimi cinque minuti, cosa la conoscenza *non* sia.

Vorrei darvi un concetto di prova e dimostrarvi che è possibile trasmettere la verità e nient'altro che la verità, dimostrare che un teorema è vero, senza che voi riusciate a sapere perché è vero, cioè di scollare la verificabilità dalla informazione, cose che andavano invece sempre insieme. L'editto della conoscenza ha due assiomi: 1) La computazione efficiente è gratis; 2) Le stringhe casuali sono gratis. Partiamo dal primo e supponiamo vi incontri per la strada e vi dica: "sentite, vi faccio una proposta: io ho un intero x nella mano sinistra, un intero x nella mano destra e se voi mi date mille euro io vi vendo il prodotto di questi due interi.". Voi ci stareste? Sicuramente no, perché sappiamo già moltiplicare. Benissimo, siamo d'accordo sul primo assioma. Passiamo al secondo (le stringhe casuali sono gratis). Supponiamo che vi faccia un'altra proposta: se voi mi date mille euro, io vi do una stringa di mille bit casuali. Anche in questo non me li dareste perché lanciando mille volte una moneta posso costruirmi i miei mille bit casuali senza spendere niente, non ho bisogno di qualcun altro per farlo. A questo punto abbiamo tutti gli elementi per riconoscere queste prove a conoscenza zero perché in realtà se quello che faccio da me non è conoscenza, se quello che è facile da computare non è conoscenza, questa deve provenire soltanto da quello che mi richiede molta computazione, che non potrei fare da solo. Teniamo a mente quanto detto all'inizio, cioè che il modo di dimostrare che due grafi sono gli stessi è di indovinare la corrispondenza e definirla: questo metodo dà *troppa conoscenza*, perché non soltanto questo dimostra che i due grafici sono gli stessi, ma dimostra anche *perché* sono gli stessi, mi dà tutta l'informazione possibile. Cerchiamo allora una prova alternativa, sempre interattiva.

Ecco i due grafi, ecco il trovatore e il verificatore; il verificatore fa una cosa: visto che i due grafi G e H sono uguali, sceglie casualmente, fra tutti i grafi del mondo, uno che sia uguale a entrambi e lo chiama C e lo manda al che il re. Il re lancia una moneta e chiede al mago, visto che afferma che il grafo C è uguale a entrambi, di dimostrargli che è uguale a G. A questo punto il mago, fra tutte le corrispondenze di vertici fra G e C ne sceglie una a caso e la dà al re. Il re è convinto: gli enunciati veri sono "provabili", se lui facesse questo gioco più e più volte il re sarebbe sempre soddisfatto. Però dobbiamo anche dimostrare che gli enunciati falsi non sono provabili. Vorrei omettere questa dimostrazione, ma la accenno soltanto. Se due grafi non sono gli stessi, C non è lo uguale ad almeno uno dei due, quindi se il re chiede di avere a caso la corrispondenza tra il grafo che ha scelto lui e un altro che non uguale, purtroppo questa non c'è. Perché questa prova è alternativa? Non è chiaro che questa prova trasmetta meno conoscenza perché alla fine il re non sapeva la corrispondenza tra C e G e questa è stata data dal mago, ma questa corrispondenza deve dimostrare che non ha nessuna conoscenza ulteriore. Perché? Supponiamo che il mago non ci sia e il re sia da solo perché, ricordate, tutto ciò che faccio da solo non ha valenza di conoscenza, è conoscenza zero. Cosa fa il re nella sua testa, senza mago e senza aiuto da nessuno? Può lanciare una moneta e scegliere tra uno dei due grafi (lo fa e sceglie G). Può lanciare di nuovo la moneta e per rinominare a caso i vertici del grafo che ha scelto. Può applicare questa questo cambiamento di nomi, applicarlo al grafo G e ottenere il grafo C. A questo punto, prende un pezzo di carta e una penna e scrive C con una freccia da destra a sinistra e sotto scrive G con una freccia da sinistra a destra e, infine, il *renaming* da destra a sinistra.





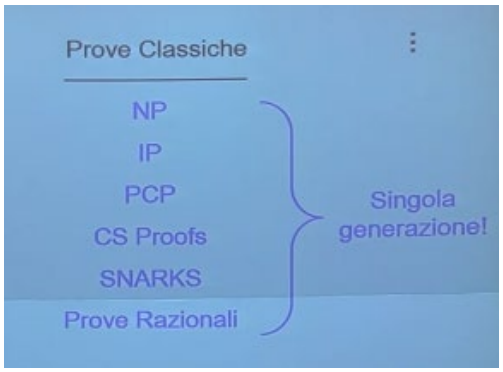
Adesso confrontiamo questa prova con quella che avrebbe ottenuto dal mago se il mago fosse esistito. La prima parte di questa conversazione è la selezione di un grafo a caso, sia a sinistra, sia a destra. Il secondo step è un bit a caso che è lo stesso sia a destra, sia a sinistra; infine, la terza parte che cos'è? È un cambiamento a caso dei nomi sia a sinistra, sia a destra. Praticamente, se io sapessi che i due grafi sono gli stessi, la conversazione che mi dimostra che i due grafi sono gli stessi me la posso rifare nella mia testa tale e quale.

Quindi, mentre questa prova mi dimostra che i due casi sono uguali, non mi dimostra nient'altro: dovrei matematicamente fare qualche altro passaggio, ma soprassediamo. Alla fine, quello che voglio dire è questo: come ci sono arrivato io a questa tipo dimostrazione? Attraverso la stessa l'esperienza che tutti voi, tutti noi come umani abbiamo avuto. E qual è questa esperienza fondamentale? Che, a un certo punto della nostra vita, nasce il pensiero se il mondo esterno esiste oppure no. Ci siamo passati tutti, ci sono passato pure io e a un certo punto mi sono convinto (avevo circa 15 o 16 anni) che il mondo non esistesse e che fosse tutto un prodotto della mia immaginazione. Però, coerentemente, siccome il mondo non esisteva, mi sono rifiutato di andare a scuola. Passa un altro e mi rifiuto di togliermi il pigiama perché se tanto il mondo non esiste, posso fare quello che voglio. Ovviamente mia madre si è preoccupata e mi chiede cosa stia succedendo. "il mondo non esiste", al che mi risponde "ma cosa stai dicendo? Io esisto, sono qui e ti sto parlando", ma io le rispondo che lei è un prodotto della mia immaginazione e che io le sto lasciando dire quello che voglio sentirmi dire. Insomma, come si vede, è un pochettino la stessa cosa: questo è il veicolo per dimostrare che la quantità di conoscenza, non solo può essere ridotta, ma addirittura eliminata e possiamo avere la verità totalmente separata dall'informazione. E questo addirittura è un teorema che afferma che "tutto il provabile è provabile a conoscenza zero".

Ma non è meglio avere sempre anche informazione? Cominciamo a parlare di qualcosa di molto pratico, ovvero le parole d'ordine, quelle che ci permettono di accedere ai nostri file oppure sono quelle che servivano al cavaliere medievale per entrare nel castello. Il problema di questa parola d'ordine qual è? Che non soltanto la conosce il castellano, ma anche il nemico che è nascosto nel fossato del castello. Una volta che l'ha carpita, si presenta lui con la parola d'ordine ed entra. C'è anche un secondo problema: inevitabilmente il castellano deve sapere la parola d'ordine e inevitabilmente usa la stessa parola d'ordine per una serie di altre attività. Quindi il castellano si può presentare direttamente la mia banca e con la stessa parola d'ordine prelevare una certa quantità di denaro. Questi sono i problemi della parola d'ordine e non sono risolvibili perché la parola d'ordine deve essere conosciuta da due persone e la seconda persona che la conosce può impersonale il titolare.

Supponiamo invece che, al posto della parola d'ordine, per entrare nel castello, facciamo una prova a conoscenza zero: in pratica si tratta di dire alla mia banca/castello/computer: "questo numero intero è il prodotto di due grandi numeri primi che ho scelto a caso e so solo io: chiunque ti dimostri interattivamente e in modo estremamente veloce che questo numero è il prodotto di due numeri primi, può accedere, perché non può essere altri che me.". Questo perché funziona? Perché essendo a conoscenza zero, non trasmette, non permette a nessuno di impersonarmi, perché nessuno sa dimostrare la cosa, si può solo sapere che è vero che quel numero è il prodotto di due primi, ma non si può dimostrare a nessuno. È una prova caratterizzata da Perfetta Segretezza, Non Impersonabilità e Completa Negabilità.

Morale della favola: le prove sono molto pratiche. Oggi come oggi, a vostra insaputa, questi sistemi sono quelli che permettono, nelle applicazioni più sicure, di identificarvi in maniera sicura.



Le prove classiche le abbiamo viste, sono NP, poi abbiamo parlato un poco di IP, ma ce ne sono anche tante altre e la cosa straordinaria è che questa evoluzione del concetto di prova è rimasto statico per 2500 anni e ha avuto un'accelerazione straordinaria e in una singola generazione è cambiato tutto. Noi come umani abbiamo spesso eretto ai cieli architetture meravigliose (e l'architettura della prova non è meno bella, almeno se siete matematici), però per costruire queste nostre architetture ci abbiamo messo più e più generazioni, la gente si tassava per fare soltanto le fondamenta di qualcosa che non avrebbe mai visto: tanto di cappello ai nostri antenati. Quello che è incredibile in questo mondo è che questa cattedrale (quella della prova) sia stata edificate soltanto in 25 anni, che è un fatto straordinario e io non posso che dire quanto sono eccitato e orgoglioso di avere partecipato a questo sforzo.

Concludendo, amore, prove e guerra hanno qualcosa in comune: sono delle attività cui si deve dedicare tutto sé stesso, non una parte perché è qualcosa cui teniamo così che siamo disposti a fare tutto per ottenere un successo in questi campi. Quando parliamo di noi stessi, certamente il nostro intelletto è importante, ma anche le nostre emozioni sono vitali per il successo finale, così come la nostra storia personale e anche il nostro senso dell'estetica. Le prove sono "quintessenzialmente" umane: ormai il linguaggio sappiamo che anche specie "meno evolute" e ce l'hanno, ma non le prove no. Ed esse sono quel magico ponte tra razionalità e realtà per il quale tutto ciò che è vero nella nostra testa, chissà perché, quando poi lo andiamo a testare è vero anche fuori. E direi che, come umanità, saranno ancora più utile perché i problemi del mondo continuano ad essere sempre più complessi e per mettere in equilibrio il nostro pianeta avremmo bisogno di un meccanismo così complesso che se non riusciamo a provarlo prima di innestarlo, non che va da nessuna parte. Quindi, in sostanza, le prove sono secondo me il nostro passato il nostro presente e il nostro futuro.

Qui finisce la parte scientifica, però essendo questo all'inizio dell'Anno Accademico ed essendo io un docente, ho deciso di dare qualche consiglio agli studenti perché un docente che all'inizio dell'Anno Accademico non dà consigli, tastategli il polso perché è morto.
Tra i vari dei consigli il numero uno è la collaborazione: la ricerca, la scienza è un processo collettivo non è una torta che se ne prendo una fetta io, a voi ne spetta di meno. La collaborazione è sempre superiore alla competizione ed è anche molto più divertente, quindi il mio consiglio sarebbe quello di collaborare quanto più potete.
Il secondo riguarda Fiducia e Dubbio: la fiducia è indubbiamente necessaria per intraprendere una qualunque attività di ricerca, però anche il dubbio ha una funzione fondamentale perché se noi ci prefiggiamo gli obiettivi e siamo totalmente fiduciosi di poterli raggiungere, non ci spingiamo abbastanza, in realtà facciamo molto meno che quello che avremmo dovuto fare. Quindi fiducia e dubbio insieme
Poi la fortuna: mai vergognarsi della fortuna perché senza la fortuna niente di importante è mai successo è mai avverrà. Gli antichi romani, che pure erano inorgogliti dai loro successi, hanno eretto a Palestrina un tempio monumentale, un'intera montagna trasformato a tempio: quello della Fortuna Primigenia. La fortuna ha molti aspetti: uno è quello del tempismo, avere la fortuna di lavorare al problema giusto al momento giusto; l'altro è quello dell'ignoranza perché quando si sanno troppe cose, trovare l'ago nel pagliaio è piuttosto difficile, mentre se siamo fortunati di saperne poche, forse tra poche pagliuzze l'ago riusciamo a trovarlo; e l'altra è la miopia perché se potessimo sin dall'inizio guardare in faccia il problema che vogliamo risolvere, ce ne andremmo da un'altra parte, scapperemmo, quindi non avere il senso della proporzione, della difficoltà che ci attende, è una grandissima fortuna. Quindi il mio consiglio, ragazzi siate fortunati!
Però ci sono due altri consigli: uno è la testardaggine, io sono testardo con un mulo e sono orgoglioso di esserlo. Per esempio, queste questo lavoro di cui vi ho parlato, fatto con la mia collega Shafi Goldwasser, l'hanno chiamato "Proofs of untrusted oracles" ed eravamo sicuri di questo successo, certi che sarebbe stato accettato. Invece viene rigettato; però siccome noi ci credevamo, lo abbiamo ripresentato, con un titolo diverso, così da sviare le commissioni di esame. Nuovamente viene rigettato. Allora ci abbiamo riprovato ancora e ancora viene rigettato. A questo punto abbiamo cooptato un altro collega secondo il quale c'era un problema di scrittura:

abbiamo totalmente cambiato l'introduzione che è diventata: "la comunicazione è uno strumento per trasferire conoscenza. Tradizionalmente, lo scopo è trasferire quanta più conoscenza è possibile quanto più efficientemente possibile. Quando tutti i partecipanti sono buoni amici non c'è da curarsi se trasferiamo più conoscenza dal dovuto. La situazione in un protocollo crittografico è ben diversa". Che bella prosa!... non ha funzionato. Alla fine, siamo riusciti a pubblicarlo, quindi il mio consiglio, ragazzi, è: perseverate! Se vi sentite che siete nel giusto, non date retta a nessuno e continuate nella vostra strada.
Un altro punto importante riguarda le limitazioni; ci siamo passati tutti da studenti: "io vorrei fare delle cose, però mi sento limitato. Come faccio?". In realtà, le nostre limitazioni sono la nostra forza, tanto è vero che un'ottima strategia è autolimitarci per renderci più forti. Forse l'esempio più calzante è quello di Hernán Cortés che nel 1519, con pochissimi uomini, sbarca nel Messico – un territorio immenso, un paese sconosciuto, un paese in armi – e per prima cosa, cosa fa? Affonda le navi con cui era partito, quindi limitandosi, rendendosi più forte e guadagnandosi un impero. Tanto per rimanere in patria, il povero Dante doveva scrivere un poema un po' complicato in cui descriveva la crisi di mezza età di un uomo che decide di spogliarsi delle passioni terrene, fino a rendersi degno dell'incontro mistico con Dio. E tutto come lo scrive? Si è autolimitato: l'ha scritto in dialetto e parlando nel dialetto fiorentino di allora, si è reso universale. Quindi avvantaggiatevi delle vostre limitazioni.
C'è poi l'ispirazione. Diceva Tolstoj: "se vuoi essere universale, parla del tuo villaggio e ti capiranno tutti". Io vi dico che non c'è bisogno di parlare del villaggio perché se parlate del ventricolo sinistro è più che sufficiente: il percorso di trovarsi è un percorso tortuoso, però troverete delle persone che vi assisteranno in questo processo di auto-scoprimento.

Quindi non lasciatevi impressionare: il cammino da fare è molto lungo e spesso e volentieri pensiamo che le nostre gambe non ce la facciano, però, diciamoci la verità, abbiamo niente di meglio da fare e di capire chi siamo davvero e che cosa vogliamo da questo mondo? Io non credo, quindi accettiamo con gioia il nostro destino, facciamo i bagagli e mettiamoci in cammino passo dopo passo con fiducia, con speranza e soprattutto con buona fortuna.

Buon Anno Accademico a tutti.