Harvard Business Review
ITALIA
OTTOBRE 2019 N.10

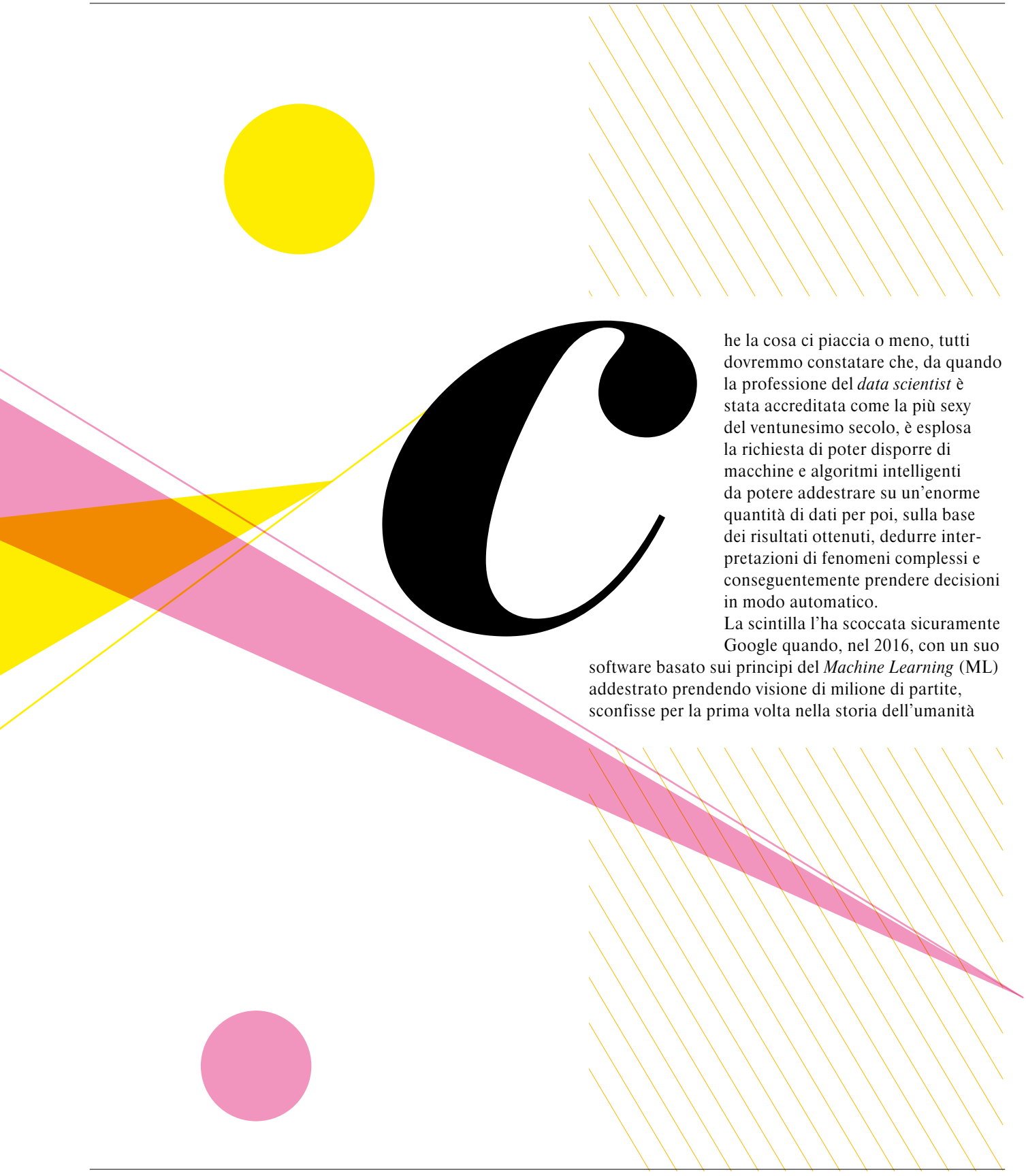
I limiti e le implicazioni di una predizione automatica

Cosa non aspettarsi dalle macchine e come aiutarle a prendere decisioni migliori.

AUTORI

Giuseppe Cappiello
Università di Bologna

Marco Roccetti
Università di Bologna



Che la cosa ci piaccia o meno, tutti dovremmo constatare che, da quando la professione del *data scientist* è stata accreditata come la più sexy del ventunesimo secolo, è esplosa la richiesta di poter disporre di macchine e algoritmi intelligenti da potere addestrare su un'enorme quantità di dati per poi, sulla base dei risultati ottenuti, dedurre interpretazioni di fenomeni complessi e conseguentemente prendere decisioni in modo automatico.

La scintilla l'ha scoccata sicuramente Google quando, nel 2016, con un suo software basato sui principi del *Machine Learning* (ML) addestrato prendendo visione di milione di partite, sconfisse per la prima volta nella storia dell'umanità

il campione umano del più complesso gioco da tavolo conosciuto: il GO.
Tuttavia, le scoperte scientifiche alla base di questo movimento, ancorché in parte già note da decine di anni, si sono tramutate solo recentemente in algoritmi e procedure effettivamente praticabili per due motivi prevalenti. Il primo: l'umanità, in tutte le sue componenti, ha contribuito al grande gioco della trasformazione di tutti i dati che la riguardano in un formato digitale. Senza la presenza di abbondanti quantità di dati digitali con cui addestrare le macchine, la rivoluzione in atto non sarebbe potuta accadere. Bisogna anche dare atto ai pochi ricercatori di avere continuato a sviluppare studi nell'ambito degli algoritmi per il ML. Nel 2018, Yoshua Bengio, Geoffrey Hinton e Yann LeCun, tre dei maggiori esperti del settore, sono stati insigniti del più prestigioso premio internazionale nell'ambito delle scienze informatiche: il Turing Award.
Ciò premesso, nostra opinione è che la strada sia ancora lunga prima di vedere una macchina o un algoritmo (in questo articolo i due termini saranno trattati senza distinzioni) capaci di prendere decisioni che siano paragonabili a quelle che prenderebbero uomini saggi in circostanze dubbie o comunque delicate; come quelle che la realtà ci presenta. Tra l'altro, senza fare errori. O facendone in quantità, o modalità, tali che l'umanità li consideri *accettabili*, o *perdonabili* o almeno *spiegabili*, come spesso avviene quando gli errori sono compiuti da esseri umani.
Per presentare le nostre idee in materia, non vorremmo tuttavia fare ricorso a modelli di natura filosofica. Per questo esistono già apposite teorie (si legga, tra i tanti, Floridi, dell'Oxford Internet Institute). Non vorremmo, cioè, fare l'errore di iniziare con disquisizioni di livello filosofico, per esempio su che cosa sia realmente una decisione: una scelta con assunzione di responsabilità. Queste trattazioni competono ad altri. Vorremmo, invece, partire dalle basi, e queste ci insegnano che il *machine learning* è una procedura al tempo stesso semplice e delicata, in cui alla fine si chiede a una macchina di classificare un oggetto mai visto prima. È bianco o è nero? È un cane o è un gatto? Il tutto sulla base del fatto che a quella macchina, in una qualche forma digitalizzata, sono stati precedentemente mostrati tantissimi esempi di oggetti bianchi e neri e di gatti e di cani. Un mero classificatore, dunque, che per giunta restituisce le sue classificazioni in stretti termini probabilistici. Con un valore di probabilità associato alla previsione. Alcuni semplificano: niente più che Bayes più Shannon più Occam. A questo punto, il nostro pane consiste nel dedicarci a questioni "tecniche" tanto importanti quanto insolute, seppure assai indagate e comunque incontrovertibili nella loro essenza. Queste questioni sono lì, ci sfidano, ma noi stiamo evitando di guardarle in faccia.

I DATI NON BASTANO (ANCORA)

Partiamo dalla prima: conta di più una teoria ben strutturata o una grande abbondanza di dati? Iniziamo da un esempio semplice, ma conosciuto. Nel 2009 alcuni colleghi pubblicarono su *Science* l'esito di un esperimento condotto con uno di questi algoritmi intelligenti. Guidato da una qualche strategia di apprendimento di tipo evoluzionistico, dopo avere esaminato una quantità esorbitante di dati relativi a un pendolo in movimento, fu in grado, senza possedere alcuna conoscenza pregressa di fisica, cinematica e geometria, di dedurre leggi fisico-matematico complesse, come gli Hamiltoniani, i Lagrangiani e altre leggi di conservazione fisica, inclusa quella del momento. Il gioco è fatto? Dopo secoli di scienza basata, a partire da Galileo e Newton, sulla relazione tra l'immaginazione di una teoria e il suo confronto con l'osservazione della realtà, possiamo buttare via tutto ciò? Possiamo sostituirla con un super algoritmo, un *Master Algorithm*, come alcuni lo chiamano, che *surfando* tra i dati di un universo completamente digitalizzato farà scienza per noi che dunque metteremo in soffitta ipotesi e modelli, congetture ed esperimenti?
Non sappiamo dire se tutto ciò sia bello o terrificante.
Per certo, però, sappiamo che quanto sopra detto non è ancora vero, o comunque non realizzabile oggi. Quello che sta emergendo, infatti, da numerosi studi, inclusi i nostri, è che sicuramente l'AI, i Big Data, il ML, nelle sue forme più *hot* quali il *deep*, faranno sicuramente parte di questa importantissima partita, ma non saranno gli unici giocatori. Si evidenzia, infatti, che talora "più dati non fanno migliori predizioni". In meteorologia, uno degli ambiti più praticati dagli euforici dei dati, è noto che le migliori

previsioni si ottengono tramite un bilanciamento corretto tra il *quantitative modeling* (uso automatico dei dati) e le interpretazioni fornite da riflessioni di tipo concettuale che solo i grandi esperti della materia sanno offrire. In ambiti più delicati, quali la medicina, la questione rimane nei termini suddetti. Se si vuole, ancora più esacerbata, nella necessità di trovare un equilibrio tra un'analisi quantitativa e una interpretazione che tenga conto di fattori umani difficilmente modellabili. Citando un collega, con parole che suonano meglio in inglese: "*Big data always need a big theory*".

DIMENSIONI PROBLEMATICHE

Passiamo ora a un secondo punto, composto di due domande. La prima: quanto può essere precisa una predizione fatta da una macchina? Non vorremmo annoiare con inutile matematica, anche se ribadiamo al lettore la natura probabilistica del sistema, ma rimane un risultato indiscusso il fatto che la precisione di una tale predizione dipende strettamente dalle dimensioni del problema posto. Detto semplice: volete previsioni accuratissime usando solo dati e algoritmi intelligenti? Bene, certo, si può fare, ma scegliete un problema molto semplice, che coinvolga poche dimensioni e con poche variabili. La seconda domanda. Ma se tutto il gioco consiste nel proporre a un algoritmo intelligente un insieme di esempi positivi e negativi da fargli apprendere, a partire da cui esso poi proporrà interpretazioni e farà previsioni, con che criterio questo insieme di esempi viene costruito? Siamo sicuri che la maniera con cui noi umani catturiamo i dati di un fenomeno sia così netta e pulita, non includa errori, impurità, distrazioni? Quale lettore esperto di quale processo aziendale potrebbe ignorare quanto sia il rumore che accompagna i dati che produciamo e, conseguentemente, accetterebbe di fornirlo alla macchina unitamente ai dati con cui è stato raccolto, con il rischio che essa impari ciò che non dovrebbe o che la confonda? E il fenomeno dell'hacking? Chi ci garantisce che un altro *man/machine in the middle* non stia inquinando i dati che poi diverranno la teoria su cui baseremo le decisioni?
Ulteriormente, una domanda che i teorici del ML si sono posti, e spesso se la pongono anche coloro che il ML lo praticano, è: quale è l'insieme *minimo* di esempi che dobbiamo mostrare a una macchina affinché impari ciò che le serve? Questione non irrilevante, essendo la nostra vita, come quelle delle aziende, ispirata se possibile a criteri di risparmio di risorse. Purtroppo, ciò che di *meglio* si sa in quest'ambito è che questo tema si correla a uno dei paradossi scoperti dal famoso filoso-matematico Kurt Godel. Ovvero, il problema pare indecidibile. Cioè, allo stato,

non sappiamo rispondere alla domanda: o il problema è semplice, o sapere a priori con quanti dati addestrare efficacemente uno di questi algoritmi non è dato.

QUALE OTTIMO?

Siamo infine arrivati al terzo e decisivo punto. Quando noi umani prendiamo una decisione, crediamo di fare il meglio. Non discutiamo qui il meglio per chi o per cosa. La questione è che ognuno di noi pratica una sua nozione di meglio. Il quale coincide, anche se un po' il gioco di parole dovrebbe farci riflettere, con quello che i matematici chiamano l'*ottimo*. In altri termini, quando decidiamo, siamo vicini a eseguire un processo simile a quello compiuto dai matematici che massimizzano una funzione. Ora, ritornando alle macchine che apprendono: siamo sicuri di volere l'ottimo anche nelle previsioni di una macchina? La domanda non sia intesa provocatoriamente. Se ci avete seguito finora, già avete gli strumenti per pensare insieme a noi che tale ottimo, se richiesto alla sola deduzione automatica, potrebbe non essere facilmente raggiungibile. Non solo, immaginiamo pure un algoritmo capace di fare previsioni, con un valore di correttezza probabilistico anche esageratamente alto, il 99,9999%, e domandiamoci, però, cosa succederebbe se si avverasse lo 0,0001 delle probabilità e si verificasse un incidente. Per esempio, automobilistico, con un morto, come già è successo. Vogliamo fingere di ignorare le reazioni che si scatenerebbero? Non vorremmo nessuno dimenticasse la natura dell'umanità. Sappiamo perdonare a noi stessi errori gravissimi, e in grande quantità, ma non siamo altrettanto tolleranti con gli errori di altre entità: persone, robot, macchine o algoritmi che siano.

INVERTIRE LA LOGICA

Ma allora esiste una soluzione a tutto ciò? Certamente: una combinazione di *human* e *machine intelligence*. Che non pretenda il 100% del lavoro, e dell'accuratezza nella previsione, dalla macchina, ma che coinvolga anche le competenze umane. Spieghiamolo, per rendere tutto più comprensibile, con un esempio preso dalla medicina.
Esistono già numerosi sistemi di previsione automatica per analisi mammografiche. Tali sistemi non hanno mai raggiunto elevati livelli di impiego, proprio per la delicatezza di affidare una diagnosi così importante a una componente non umana, ma anche per la oggettiva limitatezza dei livelli di accuratezza. Dal punto di vista medico, il problema più rilevante è l'identificazione delle lesioni ad alta probabilità di natura maligna, ciò per la complessa semeiotica radiologica che le caratterizza. A complicare lo scenario, contribuisce la variabilità di densità del tessuto mammario e la frequente presenza di lesioni non caratterizzabili con il solo *imaging*, e che restituiscono predizioni falsamente positive.
Tuttavia, se si pensa al processo di *screening* nella sua vera essenza, ciò che si pretende è di massimizzare la *sensibilità*, in modo da non perdere nessun caso potenzialmente letale (vogliamo il 100% della certezza di diagnosi su chi è malato). A questo punto basterebbe *invertire la logica*. Usare il *deep learning* non per identificare con alta probabilità (cosa improbabile) le lesioni pericolose, ma sfruttarlo per consentire di ottimizzare il *valore predittivo negativo* della lettura. In altri termini, finalizzarne l'uso allo scopo di identificare gli esami sicuramente negativi (cosa fattibile con alta probabilità). Lo sviluppo di un approccio a due passaggi (primo screening mammografico a lettura automatica per escludere, diciamo il 70% dei casi che sono evidentemente e fortunatamente negativi, e successivo studio dei soli pazienti con esami non negativi mediante metodica avanzata) potrebbe costituire un modello particolarmente utile di economia sanitaria, sicuramente applicabile in tempi rapidi al versante assistenziale e non solo.

Indicazioni bibliografiche

M. Schmidt & H. Lipson, "Distilling free-form natural laws from experimental data", *Science*, 324, 2009.

L. Floridi, *The Fourth Revolution. How the infosphere is reshaping human reality*, Oxford University Press, 2014.

H. Hosni & A. Vulpiani, *Forecasting in the light of Big Data*, *https://arvix.org/abs1705.11186. 2017.*

M. Buchanan, "The limits of machine prediction", *Nature Physics*, Vol. 15., 2019.

S. Ben David, P. Hrubes, S. Moran, A. Shpilka & A Yehudayoff, *Nature Mach. Intell.*, 1, 2019.

M. Roccetti, G. Delnevo, L. Casini & G. Cappiello, "Is bigger always better? A controversial journey to the center of machine learning design, with uses and misuses of big data for predicting water meter failures", *Journal of Big Data*, 2019.

GIUSEPPE CAPPIELLO e **MARCO ROCCETTI**, Alma Mater Studiorum, Università di Bologna.