Il caso e la necessità[1]

Francesco Romani

Dipartimento di Informatica, Università di Pisa

1. Causalità, casualità, e pseudo-casualità

> Dio non gioca a dadi con l'universo, Egli è sottile ma non malizioso
> (A. Einstein).

Il gioco del biliardo è un gioco di precisione. Conoscendo esattamente l'intensità e la direzione del tiro, il movimento di tutte le palle *potrebbe* essere calcolato esattamente utilizzando le leggi della dinamica; il condizionale *corsivo* è da intendere "a meno degli inevitabili errori di misura e di calcolo". Il gioco della roulette è un gioco di azzardo puro. A gioco corretto, il risultato di ogni lancio è completamente imprevedibile e la probabilità di uscita di ognuno dei 37 numeri è esattamente 1/37.

Sia il biliardo che la roulette sono dispositivi meccanici, obbediscono alle stesse leggi fisiche, e in entrambi vi è l'intervento manuale di un operatore (il giocatore o il croupier). La differenza è che nel biliardo tutto è fatto per minimizzare gli effetti del caso: la superficie del tavolo è piana e orizzontale, il panno è liscio e le palle sono pesanti, rotonde e pulite. Nella roulette invece tutto massimizza gli effetti del caso: il piatto ruota e le losanghe servono a far rimbalzare la leggera pallina in modo imprevedibile.

Nella realtà, al livello macroscopico che cade sotto i nostri sensi, il caso è spesso un velo che impedisce una conoscenza deterministica; nella fisica classica gli approcci statistici sono una scorciatoia potentissima adottata quando le variabili in gioco sono troppe e non si conoscono le condizioni iniziali. In questo senso, una sequenza di numeri generati da una macchina usata per le estrazioni del Lotto e delle lotterie potrebbe essere prevista in via teorica se si conoscesse tutto il conoscibile sulla macchina e sulla posizione iniziale delle palline, ma in pratica il risultato è completamente imprevedibile ed è comunemente considerato casuale.

Nella meccanica quantistica, invece, l'approccio probabilistico è inevitabile e ogni tentativo di farne a meno è finora fallito. Era questo che dava fastidio ad Albert Einstein, che la considerò fino all'ultimo una teoria "incompleta". Una sequenza di numeri generata da un rivelatore di fenomeni microscopici come, ad esempio, le emissioni radioattive, è casuale anche da un punto di vista puramente teorico.

1 Lezione tenuta martedì 28 gennaio 2014, ore 11- Liceo Scientifico Barsanti e Matteucci, Via IV Novembre n. 151, Viareggio (LU)

Una sequenza di numeri è pseudo-casuale se è facilmente generabile con un programma e gode delle stesse proprietà statistiche di una sequenza casuale.

Questi sono, ad esempio, veri numeri del Lotto:
29 52 31 80 7 18 44 29 50 1 29 21 46 84 13 87 48 28 78 4 32 34 24 83 41 1 81 2 36 68 13 62 44 55 12 56 65 2 5 81 64 14 54 83 53 81 43 87 37 45 18 50 85 3 42 45 15 25 74 23 90 59 46 30 52 51 9 89 54 36 34 19 60 84 17 89 58 84 11 32 15 30 83 82 3 12 89 54 66 86 58 1 21 19 59 2 39 70 72 66 12 62 51 88 30 83 84 38 78 59 70 15 50 59 10 64 7 53 30 85 73 52 3 89 76 86 48 53 57 18 2 25 13 74 36 63 50 1 26 75 5 66 17 22 21 60 81 87 42 24 43 79 15 38 90
Questi, invece, sono numeri pseudo-casuali generati al computer:
74 75 2 27 28 2 7 60 73 41 3 60 22 41 68 19 64 47 13 2 76 3 41 49 63 85 73 65 37 42 23 27 3 55 36 46 87 29 78 90 52 65 82 30 58 65 22 4 84 89 2 10 6 28 26 69 24 37 68 56 63 32 37 22 57 45 81 42 86 70 46 55 35 56 75 65 82 68 30 37 81 39 63 46 71 42 53 44 90 72 39 7 75 26 16 39 32 49 12 37 46 50 53 85 75 22 83 48 90 47 43 12 33 62 16 69 82 14 58 22 57 85 59 38 8 72 20 4 73 60 30 26 29 39 62 78 16 63 13 59 62 21 47 58 17 20 86 3 65 69 22 44 13 75
La differenza tra le due sequenze sta nel fatto che non esiste alcun programma che possa generare la prima, a parte quello che la memorizza tutta e poi la stampa, mentre la seconda invece è prodotta da un programma abbastanza corto. In altre parole, per trasmettere a un amico un miliardo di numeri della prima sequenza io dovrei fare un miliardo di estrazioni, annotarne i risultati e spedire un file enorme, mentre nel secondo caso posso trasmettere solo un piccolo programma e il mio amico può calcolarsi quanti numeri vuole della seconda sequenza. A parte questa profonda differenza sulla possibilità di generarle, a posteriori le due sequenze sono *algoritmicamente indistinguibili*, nel senso che non esiste alcun procedimento che permetta di dire quale delle due è veramente casuale.

2. Il Lotto (ovvero *la madre dei fessi è sempre incinta*)

Il gioco del Lotto e le lotterie sono stati introdotti per migliorare le finanze statali, non solo in Italia e non solo in tempi recenti: anche Giacomo Casanova organizzò lotterie per il Re di Francia. Una semplice analisi del regolamento mostra che il Lotto è un gioco non equilibrato in cui il banco (lo Stato) guadagna sempre. Anche la Roulette è un gioco non equilibrato, per la presenza dello zero, ma in confronto giocare al Lotto è molto più svantaggioso. L'unico modo *razionale* (sic!) per vincere al Lotto è aspettare che la buonanima di un parente defunto ci appaia in sogno e ci dia qualche numero buono.

È abbastanza diffusa l'ingenua credenza che lo studio dei risultati passati possa portare qualche informazione sui risultati futuri e in particolare che una strategia di gioco basata sui ritardi abbia qualche speranza di guadagno. Purtroppo, una semplice analisi della tecnologia fisica con cui sono effettuate le estrazioni mostra senza ombra di dubbio che, imbrogli a parte, le estrazioni sono indipendenti e che quindi in nessun modo il passato può influenzare il futuro. Tutte le strategie di gioco hanno la stessa speranza di vincita qualunque sia il numero giocato (non fa differenza giocare sempre gli stessi numeri o cambiarli ogni volta). Questo è banalmente ovvio, se si pensa che i numeri sono solo nomi accidentali e che il gioco è invariante per permutazione. In altre parole, le proprietà meccaniche e statistiche del gioco non dipendono (né potrebbero dipendere in alcun modo) dai numeri scritti sui foglietti all'interno delle palline.

3. La legge dei grandi numeri e il Teorema centrale dei limiti

Consideriamo una sequenza illimitata di variabili casuali indipendenti, tutte con la stessa distribuzione, in particolare con la stessa media μ e la stessa varianza σ^2. Un semplice esempio è dato da una serie di lanci di monete "non truccate" a cui si attribuisce il valore 0 se esce *testa* e il valore 1 se esce *croce*. La *Legge debole dei grandi numeri* (LDGN) è un teorema di Calcolo delle Probabilità che afferma che il valore medio di n estrazioni tende al valore aspettato μ. Più precisamente, per qualunque $\varepsilon>0$ prefissato piccolo a piacere, se si indica con S_n la somma dei primi n risultati (nell'esempio di cui sopra il numero delle croci su n lanci), allora:

$$\lim_{n \to \infty} \Pr\left(\frac{S_n}{n} - \mu < \varepsilon\right) = 1$$

Applicato al Lotto, ciò significa che il rapporto tra le uscite e le estrazioni di ogni numero tende a 5/90 = 1/18 quando il numero delle estrazioni tende all'infinito.

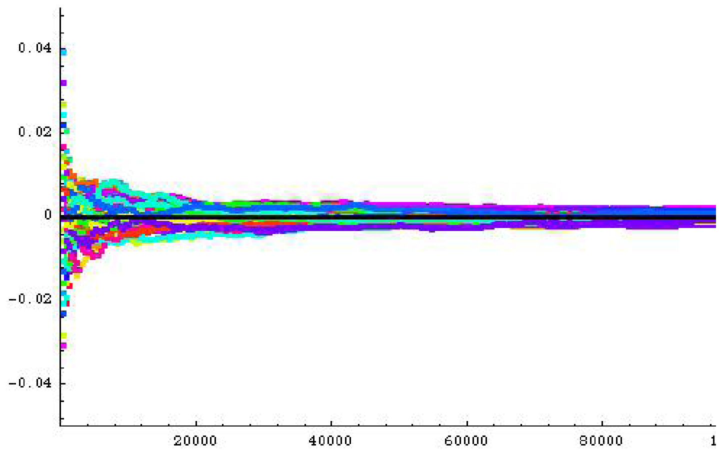

Figura 1. Differenza tra il rapporto uscite/estrazioni e la media teorica 1/18 per i 90 numeri del lotto su 200000 estrazioni. Secondo la LDGN, il valore tende a zero al crescere di n

Molti (con superficialità, ignoranza o malafede) sostengono che la LDGN implichi che al crescere del numero delle estrazioni il numero delle teste tende a pareggiare il numero delle croci e si appellano quindi a una qualche legge empirica che favorisca le uscite meno frequenti in passato. Ciò non è affatto vero, la LDGN non afferma che lo scarto S_n-μn tende a zero per n che tende all'infinito. Per avere qualche informazione sul comportamento dello scarto bisogna scomodare un teorema più complesso, dal nome ambiguo: il *Central Limit Theorem*[2] (CLT). In base al CLT con la stessa notazione di cui sopra si può affermare che per ogni x reale vale:

$$\lim_{n \to \infty} \Pr\left(S_n - \mu n \le x\sigma\sqrt{n}\right) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt$$

Il termine al secondo membro è praticamente 1 per $x>3$, quindi, il numero di uscite effettivo si avvicina al numero di uscite teorico con un errore che va come la radice di n. In altre parole (e meno rigorosamente) si può dire che la grandezza $\frac{S_n - \mu n}{\sigma\sqrt{n}}$ tende a una gaussiana di media 0 e varianza 1. Lo scarto, quindi, può andare all'infinito (sorpresa!) ma non più velocemente della radice di n, e quest'ultimo fatto permette di ricavare facilmente la LDGN in quanto $\frac{\sqrt{n}}{n}$ tende a zero per n che tende all'infinito.

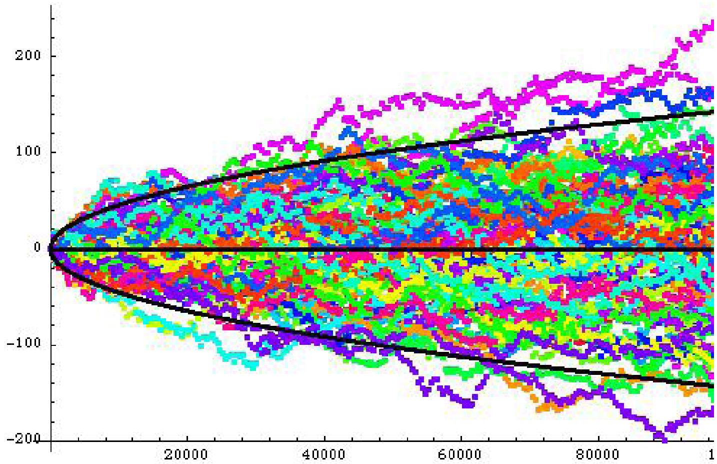

Figura 2. Differenza tra il numero delle uscite e il valore atteso n/18 per i 90 numeri del lotto su 200000 estrazioni. Secondo il CLT, il valore può crescere come la radice di n. Questa figura mostra in modo evidente l'assurdità delle farneticazioni dei ritardisti: chi usa la Legge dei Grandi Numeri per giustificare la teoria dei ritardi è un ignorante oppure un truffatore

4. Entropia e bit

In Termodinamica l'**entropia** rappresenta una misura del disordine di un sistema e costituisce uno dei concetti fondamentali della fisica. Se un sistema riceve una quantità di calore Δq a una temperatura assoluta T, questo causa un aumento $\Delta S = \Delta q / T$ dell'entropia del sistema. Il *Secondo Principio della Termodinamica* afferma informalmente che

> In un sistema isolato l'entropia non può diminuire.

Si può dare anche una formulazione statistica dell'entropia:

> In un sistema le cui componenti hanno distribuzione di energia w_n vale:

2 L'inglese *Central Limit Theorem* si può tradurre sia *Teorema centrale dei limiti* che *Teorema del limite centrale*, ma il nome è stato introdotto, in tedesco, da Georg Pólya nel 1920 nel lavoro *Über den zentralen Grenzwertsatz der Wahrscheinlichkeitsrechnung und das Momentenproblem* e questa citazione risolve senza dubbi l'ambiguità linguistica.

$$S = -\sum_n w_n \log w_n$$

La definizione statistica formalizza quello che è il vero concetto che sta dietro l'entropia. Se ho due cestini vuoti e li riempio di palline lanciando ogni volta una moneta per scegliere il cestino da riempire è estremamente improbabile che dopo migliaia di lanci un cesto sia vuoto e l'altro pieno. Se al posto delle palline metto molecole di gas, anche se il loro moto è casuale è praticamente impossibile che tutte quante si concentrino in angolo della stanza in cui mi trovo lasciandomi morire asfissiato. È con considerazioni simili che si dimostra che le leggi della Fisica Statistica, per *n* molto grande, producono le leggi deterministiche della Termodinamica classica.

In Informatica, l'incertezza nel risultato di un esperimento con un numero finito di possibili risultati ciascuno con probabilità p_1, p_2, ..., p_i, ... vale:

$$H = -\sum_i p_i \log_2 p_i$$

Questa quantità si misura in bit e viene detta *Entropia dell'esperimento* [3]. La formula, simile a quella usata in fisica statistica, si può derivare da alcuni semplici e ragionevoli assiomi sul contenuto informativo di un esperimento stocastico. Brillouin in [1] ha dimostrato che ogni esperimento che porta a un aumento dell'informazione costa un aumento maggiore di entropia termodinamica, ne consegue che ogni conoscenza che può portare ordine si paga con un disordine fisico non minore.

Un importante corollario del secondo principio della Termodinamica è il seguente:

> Se in un sistema isolato l'entropia termodinamica aumenta, il processo è irreversibile.

Le leggi della dinamica sono simmetriche rispetto al tempo. Se, ad esempio, guardiamo il filmato di uno scontro di due palle su di un biliardo, non è possibile stabilire se il filmato è proiettato in modo corretto o all'inverso.

D'altra parte lo scorrere del tempo è sinonimo di irreversibilità e le leggi della probabilità ci vengono in aiuto per stabilire la freccia del tempo in caso di eventi complessi. Nell'esempio del biliardo se il film mostra una palla che ne colpisce molte altre disposte in modo regolare è banale individuare la corretta sequenza temporale.

In generale la Termodinamica ci viene in aiuto per stabilire la direzione della freccia del tempo.

- Il calore passa sempre da un corpo caldo a uno freddo, ma non viceversa.
- Il moto si trasforma spontaneamente in calore, ma non viceversa. Nessuno ha mai visto una ruota che si mette in moto da sola perché si sta raffreddando.
- Se fai bollire un acquario ottieni una zuppa di pesce, ma raffreddando la zuppa di pesce non ritorni ad avere l'acquario.

Si può avere inoltre *irreversibilità per perdita di informazione*: ogni qual volta una certa quantità di informazione viene distrutta il processo è irreversibile. Inoltre, per i legami tra le due entropie, la distruzione di informazione è un processo che costa energia e produce aumento di entropia termodinamica.

Esiste infine l'*irreversibilità per l'osservazione microscopica*. In meccanica quantistica un'osservazione altera permanentemente lo stato del sistema (all'apertura della scatola il gatto di Schrödinger si rivela tutto vivo o tutto morto).

4. L'evoluzione

Il secondo principio della termodinamica viene spesso interpretato come una tendenza naturale al disordine. In realtà, all'interno di sistemi non isolati o in parti di sistemi chiusi lontane dall'equilibrio nulla impedisce il verificarsi di fenomeni di auto-organizzazione. Chi scrive è uno di questi fenomeni (non nel senso che sono bravo a tenere le penne in ordine). Nei casi in cui si può fare una analisi precisa, si vede che l'organizzazione locale avviene sempre a spese dell'entropia termodinamica globale.

L'evoluzione è un fatto (come la terra rotonda, anche se c'è chi dubita anche di questo). L'evoluzione biologica darwiniana aumenta l'ordine a spese dell'entropia termodinamica (aumento locale - perdita globale). Si dice che l'evoluzione biologica si mantiene al margine del caos. Secondo Dawkins [2], il motore dell'evoluzione non è la sopravvivenza degli individui, dei gruppi o delle specie ma di quegli insiemi di informazione che (semplificando) egli chiama geni e che possono durare milioni di anni. Nessuna visione teleologica ma solo un dato di fatto matematico, quasi una tautologia: *i replicanti capaci di sopravvivere meglio e più a lungo, replicano più degli altri!* Quella che si propaga e sopravvive è quindi l'informazione, i sistemi auto-organizzati, gli individui e le specie hanno invece una durata limitata nel tempo.

BIBLIOGRAFIA

[1] Brillouin, L., Science and Information Theory, Academic Press, 1962. (ristampa Dover, 2004)

[2] Dawkins, D., Il gene egoista, Mondadori, 2009.

[3] Shannon C.E., A Mathematical Theory of Communication, Bell system Technical Journal, 1948.