L'EVOLUZIONE DEL PENSIERO LOGICO: LE TEORIE ASSIOMATICHE E LA COMPLESSITÀ DEL MONDO ATTUALE IN ALCUNI ASPETTI DELLA COMUNICAZIONE

Franco EUGENI
Ordinario di Istituzioni di Matematica nell' Università di Teramo
Direttore Dipartimento di Metodi per l'Economia e il Territorio

Vincenzo DI MARCELLO
Professore IPSAA Teramo e Professore a contratto nell'Università di Teramo

... l'intuizione deve conservare il suo ufficio come complemento. Occorre insistere sulla parte che deve avere l'intuizione nell'insegnamento delle scienze (anche matematiche). Senza di essa le giovani menti non imparerebbero ad amarle soprattutto non diverrebbero mai capaci di applicarle.

J.H. POINCARÈ

1. INTRODUZIONE: SPUNTI DI LOGICA FORMALE

L'inderogabile necessità di conoscere, che è propria dello spirito umano, ha portato l'uomo a riflettere sul modo con cui egli ragiona; si è così convinto, dopo centenarie analisi, che le operazioni del suo pensiero obbediscono a regole ben determinate che formano la base e la guida di ogni investigazione o ricerca. All'insieme di tali regole si dà il nome di "logica" ed a quelle fra queste che sono indipendenti dall'oggetto particolare della singola ricerca si dà il nome di "logica formale".

È merito di Beltrand. Russell l'aver provato che, ad esempio, la matematica può essere basata soltanto sui principi della logica formale e sul postulato dell'infinito.

Spesso, nello sviluppo di una teoria, risulta opportuno, soprattutto per ragioni di semplicità, di usare un nuovo segno (simbolo o parola), o una nuova combinazione di segni al posto di un'altra combinazione il cui significato sia noto. Ognuna di tali convenzioni dicesi una definizione (esplicita). Non tutti i segni possono essere definiti; i primi segni che occorrono, cioè raffiguranti i concetti (idee, nozioni) dai quali si vuole iniziare una trattazione logica, non possono avere una definizione esplicita.

Tali segni, ed i concetti che essi indicano, si diranno "primitivi".

La scelta dei concetti primitivi è,"in certo qual modo", arbitraria. L'arte del creatore di una nuova teoria logico-formale sta nel comprendere cosa significhi .....*quel "in*

cui certo qual modo" .....Ad esempio può essere l'esperienza dell'intuito visivo a suggerire come formalizzare una teoria ed è questo il caso della geometria, nella quale il processo di formalizzazione corretta di tipo logico-formale è durato quasi duemila anni. Precisamente da Euclide ad Hilbert. Tuttavia il percorso può essere diverso e il desiderio di astrazione può essere utilizzato anche per trovare cosa può esserci di comune alla base di diversi ambiti di studio. Ritornando ai concetti primitivi è bene però che essi siano pochi e semplici, così da poterne dare brevemente e facilmente una descrizione che ne rilevi le proprietà primordiali, cioè le proprietà che si presentano all'inizio, nell'ordine logico della trattazione. L'attenzione, di cui è capace un essere umano, può portarlo a riconoscere se un oggetto è composto da altri oggetti (analisi), o se diversi oggetti hanno proprietà comuni(sintesi), ed, in quest'ultimo caso a (cercare) di concepire un ente ideale che riassume quelle sole proprietà (astrazione).

L'uomo assume capacità di giudizi che asseriscono o negano una proposizione. L'asserzione di una proposizione Q può essere conseguenza dell'asserzione di un'altra proposizione P.

Si dice allora che "Q è vera per deduzione da P" oppure che "P implica Q". All'interno di una teoria logico-formale riconosceremo assieme ai concetti primitivi l'elenco delle preposizioni base che li caratterizzano e l'insieme delle regole logiche che assegniamo per poter costruire le implicazioni e riconoscere così i giudizi corretti all'interno della teoria.

Si è spesso detto che in una teoria logico-formale un teorema è una affermazione, una implicazione "(I) implica (T)" non immediata dai postulati e la cui verifica è costituita da una catena di implicazioni:

"(I) implica P_1 ", "P_1 implica P_2", ..."P_{n-1} implica P_n ", "P_n implica (T)" mediante le quali la tesi (T) viene derivata all'ipotesi (I).

Oggi sempre più ci si chiede se:

a) È valida la deduzione anche se n è talmente grande che un singolo individuo non è in grado di comprendere l'intero processo?
(Esistono esempi come nel cosiddetto teorema delle15.000 pagine)[1].

b) Parte o tutte le implicazioni sono dedotte sperimentalmente da un elaboratore in una esperienza ripetibile non in tempi proibitivi (ad esempio molti mesi di lavoro macchina, e utilizzo di più computers e di molto personale) e a costi notevoli. (Esistono esempi come il teorema dei quattro colori e la non esistenza del piano di ordine dieci)[2].
I teoremi *"viziati dall'uso di tecniche elaborative esaustive"* sono detti tecno-remi.

---

[1] Si tratta della classificazione dei gruppi finiti sferodici. Il corpo di questa classificazione è costituito da un gruppo di note di vari autori avuti in vari tempi in circa 15.000 pagine.

[2] È facile provare che una qualsiasi carta geografica si può colorare con 5 colori in maniera che regioni contigue (non per un punto) sono colorati con colori differenti. Lo stesso problema non è risolvibile con tre colori. La domanda che per tanti anni non ha trovato risposta è se fossero sufficienti 4 colori. La prova è venuta, 4 colori bastano, ma la prova è essenzialmente dovuta ad un processo esaustivo di computer di tipo ripetibile. Anche la non esistenza del piano d'ordine 10 è stata provata con l'ausilio del computer.

Ritornando all'esame di una teoria logico-formale ritorniamo all'esame di quelle proposizioni base che caratterizzano i concetti primitivi. L'idea di fondo è per non dare luogo ad una "regressio in infinitum" si accetta l'idea che non tutte le proposizioni possono essere dimostrate. Le prime proposizioni che occorrono in una trattazione logica, quelle cioè che esprimono, come detto, le proprietà primordiali dei concetti primitivi non sono e non possono essere dimostrate. Le proposizioni che si asseriscono senza dimostrazione si dicono proposizioni primitive o postulati. Si dice anche che l'elenco delle preposizioni primitive costituiscono globalmente "la definizione implicita" dei concetti primitivi della teoria. Le proposizioni primitive devono essere compatibili e per il resto possono essere arbitrarie come i concetti primitivi. Dicendo che le proposizioni primitive devono essere compatibili si intende che fra le loro deduzioni non si trovi l'asserzione e la negazione simultanea di una stessa proposizione.

È curioso il fatto che fin dal medio evo, da quanto ci risulta dalla ricerca dei logici medioevali, ci risulta che ammettendo come vera sia una proposizione ***P*** che la sua negazione ***P*** da esse segue "come vera una qualsiasi preposizione". Si enuncia questo risultato nella formula

$$P \,\&\, P \rightarrow Q \text{ (qualsiasi)}$$
(teorema dello pseudo - scoto)

che generalmente si attribuisce a Scoto Eurigene, ma appare ben formulato dagli Scolastici:

ex falso sequitur quod libet e ripresa e "dimostrata da Hilbert.

Se è facile stabilire a priori la compatibilità di un sistema di proposizione base o assiomi della teoria è ben aperto il problema di sapere se nella teoria si potranno dedurre come vere due proposizioni A a A che sono l'una la negazione dell'altra. Questo problema detto della non contraddittorietà ha avuto il suo epilogo nel cosiddetto:

Teorema di Godel "Non è possibile dimostrare la non contraddittorietà di un sistema ipotetico –deduttivo con i mezzi offerti dal sistema stesso".

Questo "teorema esprime i limiti del pensiero assiomatico ed anche riafferma a nostro avviso la necessità di una strada non solo formale. Ritorneremo a questo argomento tra breve.

È anche bene che le proposizioni primitive siano indipendenti (sistema irriducibile), cioè siano tali che nessuna di esse possa dedursi dalle altre; ma tale condizione non è assolutamente necessaria per una trattazione logicamente rigorosa, ed anzi, talvolta, non è addirittura opportuna.

Il problema della indipendenza dei postulati ha condotto alla scoperta delle geometrie non euclidee.

Il matematico, filosofo, teologo Padre Girolomo Saccheni nel 1733 pubblicò il suo *Euclides ab omni naevo vindicatus* (Euclide liberato da ogni macchia) ove nel

tentativo di dimostrare il V postulato sulla scorta degli altri scopre "tra le righe" le nuove geometrie.

Il V Postulato (delle parallele) era infatti indipendente e la sua negazione conduceva a fenomeni in urto con l'intuito euclideo ma non illogici in quella geometria inutilità della esistenza e unicità delle parallele.

Un fenomeno analogo si è verificato nella logica.
L'assunto Aristotelico *tertium non datur* conduceva ad una visione bivalente della logica. Già in Occam si trovano ammissioni di aperture verso altre possibilità tanto che Occam si può considerare "il fondatore della Logica". Ma il Fondatore di nuove logiche è Lukasiewicz. Scrive il Lukasiewicz: Tutti i sistemi logici che si conoscono, dalla logica di Aristotele in poi, dalla logica formale tradizionale alla logica simbolica contemporanea, si basano sul principio secondo il quale ogni proposizione o è vera o è falsa. Questo principio è la base di tutta la logica finora conosciuta e che viene chiamata logica a due valori, cioè che ammette l'esistenza di due e soltanto due valori logici: vero e falso. Il principio di cui parla Lukasiewicz è il citato principio del terzo escluso (tertium non datur), principio su cui è fondata ogni dimostrazione per assurdo. Ammettere un tale principio equivale naturalmente ad ammettere che ogni proposizione possegga in sé, ed indipendentemente dalle nostre conoscenze, il carattere di vero o di falso. Questo aspetto non riveste naturalmente carattere di universalità, le proposizioni da usare in queste teorie (tra cui la matematica) sono i cosiddetti giudizi, nel senso aristotelico del termine.

2. UNO SGUARDO AL PROBLEMA DELLA COMUNICAZIONE

Alla base della conoscenza e della comunicazione è il linguaggio sia esso scritto o parlato. Sia che si parli di principi scientifici che di letteratura, di poesia o di arte credo che occorre tenere conto di due aspetti, direi fondamentali, del linguaggio: la permanenza e l'emergenza.

(cfr. F. Eugeni, D.Eugeni, questa opera)

"L'emergenza è una filosofia o una tecnica che si presenta, si vede o si usa per la prima volt; appare evidente che un linguaggio totalmente costruito di emergenze sarebbe incomprensibile, dunque ogni linguaggio ha una quantità di permanenze e di emergenze. Un qualsiasi discorso è di interesse, ovvero esteticamente e contenutisticamente interessante, quando in esso si ravvisino giusti eauilibri tra emergenze e permanenze. Le permanenze da sole, almeno per l'esperto o iniziato, dando luogo a discorsi scontati o il che è lo stesso psicologicamente noiosi. Un moderno calcolatore elettronico si può assimilare ad un genio senza emergenze, potendo compiere in modo perfetto e sovraumano esattamente le operazioni per cui è predisposto. Il calcolatore tuttavia è incapace di formulare qualunque "progetto", sia pure in sen-

so lato, tale capacità progettuale, rimanendo uno dei più solidi veicoli di comunicazione significativa. Non sempre nella storia il linguaggio "emergente" di alcuni personaggi si è rilevato comprensivo nel suo tempo. I geni i ogni campo, sono apparsi talvolta strani e folli profeti..."

È interessante l'osservazione del graffiante George Bernard Shaw nel suo avviso di "sana pazzia", ovvero come noi diciamo relativo all'emergenza". L'avviso recita: *Il saggio adatta se stesso al mondo. Il pazzo pretende di adattare il mondo a se stesso. Perciò il progredire del mondo è opera dei pazzi.*

Ancora da (F. Eugeni, D. Eugeni, op. cit.).

"Ci vuole del coraggio ma anche dell'intuito per fare delle previsioni, ma allorquando si usi un linguaggio totalmente emergente si è tacciati facilmente da folli ed eretici. Al contrario applicare un "sicuro linguaggio totalmente permanente porta a dei paradossi come costruire cerimoniali in ogni campo ossessivamente sempre uguali fino addirittura a concepire perfino l'arte ripetibile con esattezza.

L'arte priva di emergenze (squallida opera di libri assemblati da un computer o quadri prodotti in serie), è una illusione che presenta analogia con il "sogno di Leibniz". Leibniz si era forse ispirato all'esoterico Raimondo Lullo e al famoso sconosciuto (da Don Abbondio) Carneade che li ha preceduti nell'idea. Il loro sogno era la costruzione di un linguaggio, nel quale le deduzioni scaturissero meccanicamente dalle premesse, cioè un linguaggio totalmente privo di emergenze, un calcolatore ante litteram".

A proposito di Raimondo Lullo di Majorca (filosofo spagnolo 1235 – 1315), si racconta che fosse un giovane bellissimo, ma in odore di zolfo per le sue pratiche alchemiche. Fu precursore della Logica Matematica, la sua Teoria esercitò grande influsso su Leibniz. Infatti Lullo aspira a costruire un procedimento meccanico che permetta di ottenere le deduzioni a partire da principi dati. Questa finalità viene ricordata come "il sogno di Leibniz" e della sua ricerca di un simbolismo adeguato "characteristica universalis" per un "calculus ratiocinator"[3].

Una costruzione della Matematica senza emergenze si può trovare nella intera opera dei Boubakisti, movimento che negli anni '30 arriva dalla Francia. Per essi: "si fa ma senza anima, come un calcolatore, e quindi senza arte".

Nicolas BOURBAKI non è mai esistito! Lo pseudonimo è di un gruppo di Matematici francesi ed americani che in una monumentale opera di 30 volumi ricostruiscono in modo completamente razionale tutta la Matematica.

---

[3] Ci piace collegare questo pensatore con il vecchio CARNEADE (150 a.C.) il chi era costui di Don Abbondio, uno dei primi a comprendere che in una teoria razionale non si può tutto definire e tutto dimostrare poiché ciò darebbe luogo ad un processo di regressum in infinitum. Ciò prelude alle idee dei Logici de XX secolo ed alle loro idee sul concetto di sistema razionale cosi come appare nelle opere di Rudolph Carnap e Beltrand Russell.

A quanto detto si può collegare l'idea di Benedetto CROCE (1866-1952) che parte sostanzialmente dall'idealismo di Fichte (1762- 1814) ed Hegel (1779 -1831) e passando attraverso il positivismo conduce a quella corrente che è stata detta del neo- idealismo. Il Croce distingue due forme teoriche come presenti nella conoscenza: l'intuizione (che non è esattamente quella che abbiamo chiamato emergenza, ma sta forse per creatività progettuale nel complesso) che da luogo all'arte e i concetti che costituiscono la parte filosofica. Croce riconosce due forme di elaborazione pratica o se vogliamo due metodiche della conoscenza: la formazione di *pseudoconcetti empirici* e classificatori (concetti, non universali tipici delle Scienze Naturali) e la formazione di *pseudoconcetti astratti* numerativi e misurativi (universali, non concreti come quelli delle Matematiche[4]. La sintesi della visione razionale della Matematica e della Logica è nella frase provocatrice di Beltrand Russell: "La Matematica è quella disciplina nella quale non si sa di che cosa si parla astrattezza dei concetti di base) e nella quale non si sa se quello che si dice sia vero o falso ("vero" significa solo, nelle teorie razionali, "deducibile dalle premesse").

3. IL PARADIGMA DELL'ABDUZIONE COME EMERGENZA DI CREAZIONE

Il sogno di Leibniz di trovare gli elementi semplici della conoscenza furono riprese dal Lambert. L'idea di sostituire il linguaggio ordinario con un più perfetto linguaggio formale è presente in logici matematici inglesi del secolo XIX quali A. De Morgan (1806-1876), G. Boole (1815-1864), C.S. Peirce (1839- 1914).

Taluni autori, tra i quali Eco e Gisburg, ad esempio, hanno evidenziato una connessione tra Peirce, figura mitica, reale e di *misteriosa grandezza* con *l'indecifrabile essere virtuale* che risponde al nome di Sherlock Holmes, creazione letteraria di Sir Artur Conan Doyle, ma che ha assunto un ruolo di personaggio virtuale reale. Conan Doyle nel 1888 creò il suo personaggio Sherlock Holmes e gli diete forte caratteristiche abduttive. Schiacciato dal suo personaggio fu costretto a "farlo morire" nel 1891 e poi a risuscitarlo nel 1894 a furor di popolo. Oggi non sono pochi i Club Sherlock Holmes che negano una reale esistenza di Doyle, giocano a credere che Holmes sia stato un reale personaggio. È così un personaggio dotato di "forte emergenza" addirittura uccide sia pure virtualmente il suo creatore, sia pure emergente ma in dose minore..

---

[4] Ancora secondo Croce i concetti matematici non hanno una realtà concreta. Un pensiero che nulla abbia di reale non sarebbe un concetto, ma una funzione concettuale. Un triangolo non serve né alla fantasia né al pensiero ma al misuratore di un campo. Secondo il Croce dunque la Matematica andrebbe respinta dal mondo dell'arte e della filosofia per essere relegata nella sfera delle \attività pratiche. Tuttavia il Croce finisce per ammettere la Matematica nel pensiero teoretico in quanto presente nella storia dell'uomo.

La "esperable uberty" (o auspicabile valore di produzione) di peirciana memoria deriva dai tre tipi canonici di ragionamento, per la precisione: deduzione, induzione e abduzione. È l'ubertà, cioè la produttività, di quest'ultimo tipo di ragionamento che, afferma Peirce, si accresce. La deduzione, secondo Peirce dipende dalla fiducia che abbiamo nella nostra abilità di analisi del significato dei segni. L'induzione, invece, dipende dalla fiducia che l'esperienza non verrà mutata. L'abduzione, ancora dipende dalla nostra speranza di indovinare, ovvero di raccogliere adeguate informazioni che lo permettono.

In occasione del centenario di Edgard Allan Poe (1809-1849), nel 1911, Sir Arthur Conan Doyle presiedette una cena commemorativa a Londra. Fu lui che trasmise a Sherlock Holmes, fra gli altri aspetti caratteristici del Dupin, l'investigatore di Poe, quella astuta abilità, quell'affascinante illusione semiotica di decodificare e scoprire i più nascosti pensieri degli altri, interpretando i loro muti dialoghi interiori, i movimenti della faccia e degli occhi, i vari segni verbali, quanto si leggeva da ogni particolare visibile ed intuibile. Nel 1908 Peirce, riferendosi a un'osservazione di Poe in il delitto della Rue Morgue ("Mi sembra che questo mistero sia considerato insolubile per la stessa ragione che invece dovrebbe farlo considerare di facile soluzione ...") disse che "*quei problemi che a prima vista sembrano del tutto insolubili ricevono proprio in quella circostanza le chiavi che più dolcemente vi si adattano*".

I diversi elementi di un'ipotesi sono nella nostra mente ancor prima che noi stessi ne diventiamo cascienti. L'idea di mettere insieme quello che prima non avremmo mai sognato di mettere insieme è la luce che fa da faro alla nuova suggestione.

Peirce descrive la formazione di un'ipotesi come "un atto di insight", di interiorizzazione per indicare quella "suggestione abduttiva" che viene a noi "come un lampo di luce". La sola differenza tra un giudizio percettivo e un'inferenza abduttiva è che il primo, a differenza della seconda, non è soggetto a un'analisi logica.

Immaginate due matematici al lavoro, stanno lavorando su una nuova idea. Cosa fanno? In primo luogo costruiscono esempi – devono farsi una idea di ciò che succede – raccolgono indizi. Poi il processo abduttivo prende corpo, si fa una ipotesi, si tenta una dimostrazione, la prova riesce, il gioco è fatto. La prova non riesce, si trova un contro esempio, nuove informazioni si ottengono su ciò che non è. Come afferma anche Pierce, nel metodo scientifico l'abduzione è propedeutica sia all'induzione, intesa come prova sperimentale della ipotesi, che alla deduzione. L'abduzione si presenta come un istinto che utilizza percezioni inconsce e connessioni tra aspetti diversi delle informazioni possedute; sembra essere l'unico tipo di argomento che generi nuove idee. Il giudizio percettivo sarebbe invece un caso limite di abduzione con "poche informazioni". Non è certo che Pierce abbia personalmente conosciuto Sir Arthur Conan Doyle e né che abbia letto qualche racconto di Sherlock Holmes. È abbastanza verosimile che Pierce, in qualche modo ha sentito parlare delle prime storie di Sherlock Holmes; il primo racconto (A Study in Scarlet) fu

pubblicato negli Stati Uniti nel 1888; e nel 1890 The Sign of Four fu pubblicato su Lippincott's Magazine. Va solo osservato che Doyle nel 1894, quando Pierce trascorse circa due mesi con i suoi colleghi americani, era ben noto in tutti gli Stati Uniti.

Riguardo il paradigma indiziario è parere di molti che una sua origine è rintracciabile nalle pieghe delle fiabe e precisamente in una novella orientale, che apparve forse per la prima volta, in Occidente, in una raccolta di Sercambi, in cui si parla... di tre fratelli che interpretando/comprendendo una vasta serie di indizi riescono a fornire una descrizione di un animale che essi non hanno visto. Successivamente, sulla metà del Cinquecento, riapparve a Venezia in una raccolta di novelle, piuttosto ampia, con il titolo Peregrinaggio. L'opera era presentata come una traduzione dal persiano, traduzione curata da tale Cristoforo Armeno. Si narra dei tre giovani figliuoli del re Serendippo. Il libro ebbe molte ristampe e venne tradotto non solo in tedesco ma anche nelle principali lingue europee. Il successo anche popolare della storia dei tre fratelli/figli di Seredippo fu tanto e tale che venne coniato il neologismo *"serendipity"* ad indicare il paradigma delle *"scoperte impreviste, fatte grazie al caso e alla intelligenza"* – cioè di fatto le emergenze." (Horace Walpole -1754).

Anche Voltaire, pochi anni prima, nel terzo capitolo di Zadig, aveva scritto una ripresentazione della novella del Peregrinaggio, Nella riscrittura di Voltaire il cammello originale si era sdoppiato in divenuto si era trasformato in una cagna e un cavallo. Il saggio Zadig, *"specialista in abduzioni ante litteram"* descriveva minutamente gli animali decifrandone le tracce sul terreno. Venne condotto dinanzi ai giudici e accusato. Si discolpò raccontanto ad alta voce il processo mentale che lo aveva portato ad "abdurre" il ritratto degli animali che mai aveva visto:

"All'epoca di Re Moabdar c'era in Babilonia un giovane di nome Zadig, di buona indole nativa rafforzata dall'educazione". Non stiamo ad entrare nei dettagli del suo carattere generoso "...quando mangi da mangiare ai cani, anche se dovessero morderti..." non parleremo delle sue ricchezze, della sua scienza, del suo amore per Semira, delle sue nozze con la leggera Azora, ripudiata dopo un mese, ma dell'episodio del cane e del cavallo.

Un giorno passeggiando vide correrglì incontro l'eunuco della Regina che con vari ufficiali cercavano il cane della Regina e il Cavallo del Re.

"Giovanotto, non avete visto il cane della Regine – chiese l'eunuco – È una cagna, non un cane. È una cagnetta spagnola minuscola che ha fatto da poco i cuccioli, zoppica dal piede anteriore sinistro e ha le orecchie assai lunghe – rispose Zadig – l'avete allora vista? – disse l'eunuco – No – rispose Zadig – non ho mai saputo che la Regina avesse un cane".

Anche il capocaccia gli chiese se avesse visto il cavallo, "È il cavallo che galoppa meglio, è alto cinque piedi, ha zoccoli piccolissimi, ha la coda lunga tre metri e mezzo, le borchie del morso sono d'oro a 23 carati, i ferri sono d'argento di undici

denari – disse Zadig – quale strada ha preso chiese il capocaccia – non l'ho visto – rispose ancora Zadig".

Finì davanti al grande desterham (Giudice-tesoriere) che lo condannò allo knut (staffile di nerbi di bue con punte di metallo) e alla deportazione in Siberia. Ma il cavallo e la cagna furono ritrovati e gli fecero pagare quattrocnto once di ammenda per aver detto di non aver visto ciò che aveva, secondo i giudici visto, allora Zadig diede spiegazioni.

"Vidi sulla sabbia le impronte di un animale – raccontò Zadig – e capii facilmente che erano le orme d'un piccolo cane. Dai solchi lunghi e leggeri rimasti impressi sui minimi rilevi della sabbia proprio tra le tracce lasciate dalle zampe compresi che si trattava d'una cagna con le mammelle penzoloni, quindi doveva aver figliato da pochi giorn... Riguardo al cavallo... ho scorto le tracce dei ferri sui viottoli tutte ad eguale distanza: un cavallo che galoppa in modo perfetto... il morso deve essere d'oro, strisciò infatti contro una pietra ...osservando i segni sui ciottoli di altra specie ho ritenuto che i ferri erano d'argento..." I giudici ammirarono la profondità del discernimento, tutti parlarono bene di Zadig, anche il Re, ma i giudici trattennero trecentonovantotto once per le spese e gli uscieri chiesero la mancia.

Ecco in queste storie, in queste favole l'origine dell'abduzione e dell'emergenza, l'embrione del serendipity. Nella screndipity è anche l'embrione della patologia chirurgica e non solo chirurgica, i metodi di riconoscimento di opere d'arte alla Morelli, i paradigmi indiziari per le ricostruzioni storiche alla Ginsburg ovvero le brillanti indicazioni che da Peirce a Umberto Eco ci lasciano pensare per... indovinare - diranno subito i miei piccoli lettori... ed invece no, avete sbagliato per abdurre alla Conan Doyle, alla Sherlock Holmes secondo metodi e modi che al di la della apparente futilità spiegano i motivi, apparentemente incosci, della straordinaria fortuna del romanzo poliziesco. Su questo filone s'impernia un modello conoscitivo che è nello stesso tempo antichissimo e moderno. Dalla sua essere antico, quasi senza memoria si è detto. Per la sua modernità, citeremo qunto segue:

... Oggi basta vedere l'impronta di un piede forcuto per concludere che l'animale che ha lasciato impronta era un ruminante, e questa conclusione è altrettanto certa di qualunque conclusione della fisica o della morale. Basta quest'orma per dare all'osservatore la forma dei denti, la forma delle mascelle, la forma delle vertebre, la forma di tutte le ossa delle gambe, delle cosce, delle spalle e del bacino dell'animale che è appena passato: si tratta di un segno più sicuro di tutti quelli di Zadig.....(elogio di Cuvier della scienza paleontologica).

Fin dalla fine dell' Ottocento si ebbe conoscenza di questi processi. Si pensi che perfino il grande Thomas Huxley in un famoso ciclo di Conferenze inneggianti alla dottrina Darwiniana ebbe a parlare del cosiddetto *"metodo di Zadig"* per indicare il proceesso indiziario quale metodo di indagine comune a vari campi quali l'archeologia, l'arte, l'astronomia,la criminologia, la fisica, la geologia, la matematica, la medicina, la paleontologia, la patologia, la storia e...scusate se è poco.

4. LA PROTEZIONE DELL'INFORMAZIONE E LA MATEMATICA

Dalla logica finale alla logica del mondo reale il passo è complesso. Noi ci addentreremo ora ad un campo poco conosciuto la cui evoluzione è andata di pari passo con quello della logica. Al campo della protezione dell'informazione i logici hanno sempre dato e da esso hanno sempre attinto.

Basti uno per tutti: Charles Dodson in arte Lewis Carrol (cfr. Le Scienze, 50, 1972). Era un logico ed è stato un importante crittoanalista. Non ripercorreremmo l'aspetto storico rimandando per questo a testi specializzati e all'articolo di F. Eugeni e D. Eugeni, op. cit. presente in questo volume.

La protezione dell'informazione, oggi. In questi campi di studio convergono molte parti di discipline classiche, quali Algebra classica e moderna, Analisi algebrica ed infinitesimale, Geometria algebrica, Geometrie di Galois, Calcolo delle Probabilità, Statistica e Teoria dei Giochi e delle decisioni, ma anche la Teoria dei Numeri e tutto l'intero settore della Matematica Discreta. Queste discipline si intrecciano un modo mirabile negli aspetti più disparati rivelando inaspettati crittomorfismi, insolite e feconde analogie teoriche, sporadicità di fenomeni, solo raramente dominabili con l'uso di un elaboratore. Nulla è più sbagliato della erronea credenza che in un universo finito *"tutto si può contare"* come si sono accorti matematici del livello di Eulero fin dal 1700, quando iniziarono a scontrarsi con il finito. È certo che l'avvento dei Computer e la possibilità di effettuare verifiche su "piccoli, ma non piccolissimi, numeri" ci è stata veramente di grosso aiuto ma non più di tanto. La Matematica Discreta è legata poi a tutta una serie di problemi applicati che nascono allora che ci si ponga nella situazione di volere /dovere "gestire un sistema di trasmissione e/o trasformazione della informazione", anzi la Matematica Discreta appare come la matematica più adatta per operare in questo settore.

Il problema del proteggere l'informazione e il relativo uso di Codici opportuni era ben presente in tempi molto antichi – come ci narra Svetonio. Risale alla guerra contro la Gallia uno dei primi codici segreti importanti. Si ha un notevole sviluppo presso le corti papali al tempo di Leon Battista Alberti, che era un cultore di Matematica Discreta e Crittografia. Ritroviamo in questo settore nomi inattesi e insospettabili.

Oggi occorre tenere in conto la profonda rivoluzione che l'Elettronica e l'Informatica hanno provocato nel trattamento dell'Informazione. Ad esempio in tutte le transazioni finanziarie del mondo di oggi si deve tenere presente che il denaro e quindi ogni interscambio finanziario, è considerato, e quindi trattato, come una informazione. Precisamente esso è l'informazione del credito reale o presunto che la società riconosce ad un individuo o ad un gruppo di individui formanti una società o gruppo finanziario. Una volta si pagava in oro, la bontà dell'oro si saggiava con i denti e le transazioni avvenivano a stendi mano. Oggi le transazioni finanziarie si intrecciano a velocità della luce all'interno dei canali pubblici che sono i cavi telefo-

nici e le reti di computers. Ma il problema della riservatezza o privacy e della manipolazione delle informazioni è oggi più importante e più delicata di ieri.

È noto che dalla metà del 1800 la nascita delle società per azioni, l'obbligatorietà della conservazione di certe scritture contabili, la trasparenza dei bilanci d'azienda e della contabilità di stato condussero le Aziende e le varie Amministrazioni a disporre di un enorme mole di informazioni riguardanti privati cittadini, Imprese Commerciali ed Enti dello Stato e del parastato. Una conseguenza inevitabile è stato il commercio delle informazioni, lo spionaggio industriale, l'uso e la manipolazione di informazioni alle quali non si è autorizzati ad accedere, contraffazione di posta e denaro elettronico. Si pensi soltanto ai rischi che si possono correre se un "bandito elettronico" acceda a reti o archivi quali quelli di Banche, Enti assicurativi, di Società ovvero di Enti governativi.

Ci si potrebbe appropriare quindi non solo di denaro ma anche di informazioni su movimenti contabili, situazioni fiscali, piani di produzione e sviluppo, movimenti personali di managers ed informazioni personali sugli stessi anche dedotti da archivi ospedalieri. Infine un operatore finanziario potrebbe disconoscere l'ordine elettronico di un cliente e viceversa.

Un rimedio è certamente quello di disporre di buoni prodotti crittografici. La crittografia, che oggi si presenta ben più sofisticata che non ieri quando il suo uso era riservato al solo ambito militare, è oggi una disciplina nella quale si osserva un grosso fermento.

5. LE GEOMETRIE FINITE E IL PROBLEMA DELLA AUTENTICAZIONE

L'aritmetica di base nella Crittografia è costruita dall'algebra dei campi Campi di Galois, specie binari.

Se occorre inviare un messaggio, che non debba essere intercettato e decrittato da personaggi non autorizzati, si può ottenere un alto grado di protezione, certificabile probabilisticamente. Si possono ottenere risultati notevoli solo utilizzando la Teoria dei Numeri e l'algebra dei Campi di Galois.

Un problema di grande importanza è quello *dell'autenticazione di un messaggio.*

Al di là del fatto che un messaggio sia o meno coperto, nella sua leggibilità diretta, da un prodotto crittografico, occorre una garanzia al ricevente di sicurezza dell'identità, altamente probabile del mittente, e al mittente occorre una garanzia altrettanto altamente probabile che il mittente abbia ricevuto il messaggio e lo abbia ricevuto integro da manipolazioni. Inoltre entrambi devono essere in grado di provare questo ad un terzo. I migliori risultati in questo campo sono stati ottenuti utilizzando le geometrie proiettive sui campi di Galois.

Sia M un messaggio crittografato o no, e sia K una chiave concordata tra mittente e destinatario, quindi una chiave privata. Un autenticatore è un algoritmo f che

applicato alla coppia messaggio - chiave produce un oggetto A = f(M. K), detto appunto autenticatore. Il mittente invia al destinatario la coppia (M, A). Il destinatario ricevere una coppia (M*, A*) che può essere realmente la coppia (M, A) inviata ma può essere anche una coppia manipolata da un terzo. Come può fare il ricevente ad accorgersi della manipolazione?

Il ricevente, conoscendo la chiave K e l'algoritmo f costruisce il valore f (M*, K), se tale valore coincide con A*, ricevuto con M*, il ricevente accetta il messaggio M* come autentico, altrimenti lo rifiuta.

La domanda che si pone è quella di conoscere la probabilità che un intruso indovini una coppia (M*, A*), senza conoscere la chiave K, compatibile con l'algoritmo f, cioè tale che A* = f (M*, K).

La risposta è fornita dall'ormai classico

TEOREMA DI GILBERT-MC WILLIAMS - SLOANE (1975)

Se i messaggi e le chiavi sono tutti egualmente possibili, allora la probabilità P che il sistema sia sicuro è maggiore o eguale all'inverso del numero delle chiavi.

I sistemi per i quali P è proprio l'inverso del numero delle chiavi si dicono *perfetti*, quelli per cui P è dell'ordine di grandezza dell'inverso del numero delle chiavi si dicono *essenzialmente perfetti.*

Esempi di sistemi di autenticazione perfetti ed essenzialmente perfetti sono stati costruiti utilizzando le Geometrie di Galois. Esempi vecchi e d esempi nuovi saranno presentati durante il convegno.

Con queste aritmetiche convivono delle geometrie precisamente le geometrie finite.

Iniziamo con il definire un piano affine sopra un campo di Galois GF(q). I "punti" del piano sono le coppie ordinate (x,y) di elementi di GF(q). Per definire le "rette" consideriamo, come in geometria analitica, il luogo dei punti del piano le cui coordinate sono soluzioni di una equazione lineare di GF(q) del tipo: ax+by+c = 0 con a, b non entrambi nulli. Se a è non nullo, al variare di y in GF(q) esattamente in q modi, si ottengono i corrispondenti valori di x, e cioè q punti (x = a' (-bh-c), y = h) della retta. È possibile anche trovare il punto comune di due rette risolvendo i corrispondenti sistemi, anche con il metodo di Cramer. Infatti tutta la teoria delle matrici e dei sistemi lineari, come ben noto, sussiste del tutto inalterata sopra un qualsiasi campo. Un piano affine ha q^2 punti (si pensi al numero delle coppie (x,y)), ogni classe di parallelismo ha q rette e quindi avendosi q+1 direzioni per un punto (q rette incidenti una data e la parallela), ci sono in totale q^2+q rette nell'intero piano. Un piano affine di Galois viene universalmente denotato con il simbolo AG(2,q), dove 2 è sinonimo di dimensione 2.

È ora il momento di definire un piano proiettivo di Galois. Utilizzeremo la vecchia idea delle coordinate omogenee. Un piano proiettivo su un campo di Galois

d'ordine q, in simboli PG(2,q), è l'insieme di tutte le possibili terne ordinate (x,y,t), con x,y,t elementi di un campo di Galois, tali che:
a) le terne sono composte da elementi non tutti nulli;
b) terne proporzionali si riguardano come identiche.

Dunque i "punti" sono queste terne, se t non è nullo il punto si dice proprio ed ad esso si attribuiscono coordinate "cartesiane - affini" X=x/t, Y=y/t,in accordo con il fatto che terne proporzionali sono lo "stesso punto". Se t=0, il punto (a,b,0) si chiama improprio ed ad esso si associano tutte le rette affini del tipo bX-aY+c=0.

Definiamo le "rette" come l'insieme dei punti le cui coordinate omogenee sono soluzione di una equazione del tipo:

$$ax + by + ct = 0,\ a, b, c \text{ non tutti nulli.}$$

Se a, b sono nulli si ha la retta impropria t=0,che è il luogo dei punti impropri ovvero delle q+1 direzioni del piano affine. Se a, b non sono entrambi nulli, si ha sulla retta il punto (b,-a,0) e tutti i q punti della retta affine aX+bY+c=0. In totale dunque una retta proiettiva ha q+1 punti: precisamente i q punti della retta affine sottogiacente ed in più il punto improprio. Ci sono q+1 rette per un punto ci sono q2+q+1 punti nel piano ed altrettante rette.

È utile esercizio rappresentare tutte le rette di AG(2,3) e di PG(2,3) e confrontarle ed associarle nel modo naturale. Per il lettore interessato un esame dettagliato di AG(2,3),detto piano di Sarrus, può trovarsi in Cerasoli, Eugeni e Protasi.

Con AG(r, q) indicheremo l'insieme delle r- ple ordinate di elementi di GF(q). In AG(r,q) si chiama sotto spazio h- dimensionale l'insieme dei punti che sono soluzione di un sistema lineare non omogeneo costituito da r- h equazioni indipendenti. In altre parole si traduce ad uno spazio affine finito quanto usualmente si adotta per uno spazio r- dimensionale sui reali, nozione di vettore e di prodotto interno incluso. La nozione di norma e di distanza indotte dal prodotto interno usualmente non vengono introdotte.

In modo del tutto analogo con il simbolo PG(r, q) si indica l'insieme delle (r+1)-ple ordinate di elementi non tutti nulli e definiti a meno di un fattore. Un sottospazio h-dimensionale è rappresentato da r-h equazioni indipendenti.

BIBLIOGRAFIA

[1] E. AMBRISI-F. EUGENI, Il problema della protezione della informazione, I: cenni storici e metodi statistici per la decrittazione, Ratio Math. 1 (1990), 15-37.

[2] L. BERZOLARI, G. VIVANTI, D. GIGLI (a cura di), Enciclopedia delle Matematiche Elementari e Complementi, Editore Ulrico Hoepli Milano, 1979.

[3] A. BEUTELSPACHER-F. EUGENI, Geometrie Finite e crittosistemi: stato dell'arte e problematiche, Atti del II Simposio Nazionale su: "Stato e prospettive della ricerca crittografica in Italia" a cura della Fondazione Bordoni, Roma, 1989.

[4] G. BOOLE, L'analisi Matematica della Logica, Serie scientifica Universale Bollati Boringhieri, Torino 1993.

[5] C.B. BOYER, Storia della Matematica, Oscar Mondadori, Milano 1990.

[6] M. CERASOLI, F. EUGENI, M. PROTASI, Elementi di Matematica Discreta, Zanichelli, Bologna 1988.

[7] C. CUNDARI, F. EUGENI, L. CARNEVALI, La geometria dell'Illuminismo: I grandi protagonisti di una esplosione culturale, Quaestio N.= (La rivista del disegno), (1998), 23-55.

[8] K. DEVLIN, Dove va la Matematica, Bollati Boringhieri, Torino 1994.

[9] U. ECO, T. A. SEBEOK (A cura di), il Segno dei tre: Holmes, Dupin, Perce, Studi Bompiani, Milano 1983.

[10] O.D. EDWARDS, The quest for Sherlock Holmes, Penguin Books, 1983.

[11] F. EUGENI, Combinatorics and Cryptography, Testo di una Conferenza generale tenuta a: International Conference "COMBINATORICS '90", Gaeta 1990.

[12] F. EUGENI, Le due rivoluzioni matematiche del secolo: da Bourbaki alla Matematica del discreto, Per.di Mat. I (1992), 3-21. (dedicato al Prof. C. Eugeni nel suo 80.mo compleanno).

[13] F. EUGENI-B.K.DASS, How to share secrets: the idea of threshold games, Journal of Information & Optimization Sciences, 12 (1991), 451-458.

[14] F.EUGENI, S.INNAMORATI, Esploriamo la geometria combinatoria, Bollettino dei docenti di matematica, (Canon Ticino), 35 (1997), 45-55.

[15] F. EUGENI, D.,EUGENI, Salvator Dali conosceva l'ipercubo? ovvero uscire da un cubo senza attraversare la facce prima dei diciotto anni, Atti Convegno "Il metodo storico nell'insegnamento della Matematica" – Ripattoni (Teramo), 1998.

[16] F. EUGENI, D. EUGENI, Matematica e scienza applicata tra oriente ed occidente e i prodromi della moderna teoria dell'informazione, in questo volume, (2000).

[17] S. GUERRA, E. SOLITO, I diciassette scalini, Casa Editrice "Il Torchio", Roma, 1998.

[18] S. INNAMORATI, Storia e metodologia dei fuzzy sets, Atti Convegno "Il metodo storico nell'insegnamento della Matematica" – Ripattoni (Teramo), 1998.

[19] VOLTAIRE, Zadig e altri racconti filosofici, Feltrinelli, Milano, 1994.