Numero 1 - 1990

RATIO MATHEMATICA

Atti del Convegno di

Matematica Applicata all'Economia e all'Ingegneria

Pescara 26, 27, 28 Gennaio 1989

a cura di

Franco Eugeni e Mario Gionfriddo

Numero 1 - 1990

RATIO MATHEMATICA

Atti del Convegno di

Matematica Applicata all'Economia e all'Ingegneria

Pescara 26, 27, 28 Gennaio 1989

a cura di

Franco Eugeni e Mario Gionfriddo

Questo primo fascicolo di RATIO MATHEMATICA, assieme al secondo, contiene i lavori esposti al Primo Convegno Nazionale di Matematica Applicata all'Economia e all'Ingegneria, svoltosi a Pescara il 26,27,28 Gennaio 1989.

Non desideriamo commentare il contenuto scientifico del convegno, ma solo riportare le dichiarazioni di tre illustri partecipanti, dichiarazioni apparse su: L'Università D'Annunzio, Periodico d'informazione dell'Ateneo, anno IV, nn. 1-2, 1989.

Giovanni MELZI (Ordinario di Matematica Generale - Milano - Cattolica). Convegno riuscitissimo: è un giudizio senza riserve sugli esiti del Convegno, specialmente per quelli che avranno rilevanza dopo, nel seguito delle ricerche dei singoli partecipanti. Il momento del confronto, l'impegno a spiegare ai compagni di cordata lo stato dei tuoi studi sono occasioni di consolidamento di propositi, incoraggiamento a proseguire e, se ne è il caso, di ripensamento critico dei punti di partenza. L'esperienza più piacevole è quella della constatazione dell'esistenza di spinte concordi al di là di differenze apparentemente irriducibili. Credo di aver sentito più che osservato una spinta irresistibile verso il superamento delle barriere delle varie specializzazioni, che - quasi incredibile per i non addetti ai lavori - che, sono molte anche in un gruppo così numericamente ridotto di studiosi. Grazie Prof.Eugeni. E bravo !

Lorenzo PECCATI (Ordinario di Matematica Finanziaria - Torino). I progressi più significativi in numerosi campi di indagine scientifica registrati in questi ultimi anni sono sempre più osservati su temi di frontiera tra discipline diverse. Questo è vero soprattutto nella Matematica Applicata, ove almeno due sono i poli: la matematica e il dominio di applicazione. Il Convegno svoltosi in questi giorni è stato un'ottima occasione di confronto tra specialisti di arce differenti. L'interscambio tra associazioni scientifiche e gruppi di ricerca che nei fatti sono "compagni di strada" va iniziato, coltivato e sviluppato con grande pazienza: i risultati non mancheranno. Grazie dunque a ideatori ed organizzatori per quest'occasione stimolante.

Aniello RUSSO SPENA (Ordinario di Tecniche della Bonifica - L'aquila). La varietà dei temi trattati nelle relazioni generalie nelle comunicazioni su argomenti specifici, assieme alle approfondite discussioni che a queste sono seguite, hanno fornito l'opportunità a cultori di discipline apparentemente molto distanti tra loro di confermare, in maniera chiarissima, che le impostazioni di principio e metodologiche delle scienze applicate sono da considerarsi sostanzialmente comuni. Sotto questo aspetto il Convegno

organizzato dal Prof. Eugeni può considerasi perfettamente riuscito, e di questo dobbiamo essergli grati.

Circa Ratio Mathematica il nostro intento è semplicemente quello di creare una Rivista agile nei tempi di stampa e nella forma di Referee.

I singoli volumi saranno tematici e saranno decisi di volta in volta da curatori della rivista.

Franco Eugeni e Mario Gionfriddo.

Direttore responsabile
Prof. Franco Eugeni

(autorizzazione Num. 9/90 del 10.07.1990 del Tribunale di Pescara)

Fascicolo realizzato con il contributo del Dipartimento di Scienze e Storia dell'Architettura. Hanno collaborato alla realizzazione di questo fascicolo: il Prof. Antonio Maturo e gli Ing. Giuseppe Di Biase, Domenico Marconi e Giovanni Mataloni.

RATIO MATH. 1.
(1990), 1 - 14

Funzioni di Costo Minimo e di Ricavo Massimo come Coniugate Parziali della Funzione di Profitto e Conseguenze

Ilio Adorisio (*) e Luigia Berardi (**)
(*) Università "La Sapienza" - Roma
(**) Università degli studi di L'Aquila - Facoltà di Ingegneria

1. INTRODUZIONE

Richiamiamo, per completezza, alcune definizioni e teoremi di analisi convessa, che saranno utili nel seguito (cfr. [6]).

Data una funzione convessa $y = f(x)$, $x \in R^n$, $y \in R$, si definisce sua coniugata la funzione

$$f^{\wedge}(b) = \sup_x\{xb - f(x)\} = -\inf_x\{f(x) - xb\},$$

dove $x, b \in R^N$, ed xb è il prodotto interno.

Ricordiamo che una funzione convessa si dice **chiusa** se il suo epigrafo è chiuso, inoltre una funzione convessa ottenuta ponendo $y = \infty$, $\forall x \notin \text{dom } f$ è detta **propria**.

Sussistono le seguenti proprietà:

(a) La funzione $f^{\wedge}$ **coniugata** di una funzione convessa f è una funzione convessa **chiusa**, propria se e solo se f è **propria**. Inoltre $(\text{chius } f)^{\wedge} = f^{\wedge}$ ed $f^{\wedge\wedge} = \text{chius } f$.

(b) Il sottodifferenziale di una funzione convessa e quello della sua coniugata sono l'uno funzione inversa dell'altro.

(c) L'insieme delle direzioni di recessione $D = \{x+\lambda y \mid \lambda \geq 0\}$, $x \in \text{conv } C$ è il cono di recessione di C, denotato con O^+C.

(d) Un insieme non vuoto può essere individuato dai suoi iperpiani di sostegno. Sia S un qualsiasi sottoinsieme di R^n. Si definisce funzione di sostegno di S la funzione convessa, chiusa, propria, positivamente omogenea di grado 1, dell'argomento $b \in R^n$, $\delta^*(b \mid \text{conv } S) = \sup\{bx \mid x \in \text{conv } S\}$. Si ha allora la relazione duale $\text{conv } S = \{x \mid bx \leq \delta^*(b \mid \text{conv } S)\}$ con le ovvie semplificazioni se $S = C$ è convesso, ossia se l'insieme è convesso, la funzione di sostegno descrive l'insieme e non la sua estensione convessa.

(e) Dato un convesso C (eventualmente $C = \text{conv } S$) il dominio di definizione della funzione di sostegno $\delta^*(b \mid C)$ è un cono (eventualmente mancante dell'origine) che viene detto cono barriera e che può risultare non chiuso. Tuttavia vale la proprietà secondo la quale il polare del cono di recessione di C costituisce la chiusura del cono barriera.

(f) Il sottodifferenziale $\partial f(x)$ della funzione convessa $f(x)$ è un insieme convesso chiuso. La corrispondenza $\rho(x) = \partial f(x)$ è semicontinua dal di sopra.

(g) Il sottodifferenziale della funzione di sostegno di C, chiuso, non vuoto, è l'insieme, $\forall b$, dei punti, se esistono, dove la funzione lineare bx raggiunge il massimo; ossia è una faccia esposta di C. Se è $C = \text{conv } S$, allora non tutti i punti così individuati sono di massimo, ma solo quelli che appartengono alla intersezione tra la faccia esposta e l'insieme S.

(h) Si chiama polare del convesso C l'insieme C° di livello 1 della sua funzione di sostegno, ossia $C^\circ = \{b \mid \delta^*(b \mid C) \leq 1\} = \{b \mid bx \leq 1, \forall x \in C\}$. Se C è un convesso chiuso contenente l'origine il suo polare C° è un altro insieme chiuso, contenente l'origine ed è inoltre $(C^\circ)^\circ = C$. Esiste così una corrispondenza tra le faccie esposte di C e quelle di C°; queste ultime forniscono le direzioni dei vettori che sono massimizzanti per la corrispondente faccia esposta di C.

(i) Dato un convesso $C \neq \phi$, si definisce funzione di calibro la funzione convessa, positivamente omogenea di grado 1, data da $\gamma(x \mid C) = \inf\{\lambda \geq O \mid x \in C\}$. Se $O \in C$, l'insieme C è l'insieme di livello 1 della sua funzione di calibro e, nelle stesse condizioni, esiste una corrispondenza duale tra funzione di calibro e di sostegno, data dal fatto che la funzione di sostegno di C è la funzione di calibro di C°, mentre la funzione di calibro di C è la funzione di sostegno di C°.

Avvertiamo inoltre che per tutto quanto non esplicitamente richiamato nella nota, ovvero per approfondimenti ed esemplificazioni dei concetti usati si fa esplicito riferimento a [2].

Nel paragrafo 2 di questa nota riportiamo una sintesi delle applicazioni della dualità in analisi convessa nella teoria economica.

Nel paragrafo 3 sono riassunte le applicazioni nella teoria economica di una particolare dualità, quella esistente tra una funzione e la sua coniugata.

Nel paragrafo 4 vengono trattate le proprietà duali tra la funzione di *produzione e le funzioni di costo minimo o ricavo massimo.*

Infine, nel paragrafo 5, ci occupiamo di funzioni di produzione congiunta con insiemi di produzione non necessariamente convessi. Introduciamo il concetto di coniugata parziale di una funzione e stabiliamo relazioni duali tra la funzione di profitto e le funzioni di costo o ricavo. L'introduzione della funzione di costo generalizzata permette di dare una soluzione del classico **paradosso di Calais.**

2. SINTESI DELLE APPLICAZIONI NELLA TEORIA ECONOMICA DELLA DUALITA' IN ANALISI CONVESSA

Sintetizziamo ora quanto si rinviene in letteratura circa le applicazioni dei teoremi di analisi convessa richiamati nel paragrafo 1.

Sia $y = | q,z | \in R^{n+m}$ un vettore di produzione essendo $q = (q_1, ..., q_n)$, dove $q_i \geq 0$ sono gli n prodotti e $z = (z_1, z_2, ..., z_m)$ dove $z_i \leq 0$ gli m fattori. Supponiamo che l'insieme Y dei vettori y sia chiuso e non vuoto. L'insieme Y è un sottoinsieme del prodotto dell'ortante positivo o^+ dello spazio dei prodotti per l'ortante negativo o^- di quello dei fattori.

Allo scopo di semplificare le notazioni, seguendo la terminologia adottata in | 2 |, definiamo **frontiera superiore** di un convesso C l'insieme (se esiste) F^+C definito da:

$$F^+C = \{x \in \text{chius } C \mid bx = \delta^\wedge(x \mid C), \forall b > 0\} .$$

Si noti che, se C è superiormente limitato, esso ammette una frontiera superiore (non vale il viceversa).

Inoltre, definiamo **efficiente superiore** dell'insieme generico S l'insieme:

$$E^+S = \{x \in \text{chius } S \mid x \notin D_x, \forall x \in \text{chius } S\} ,$$

dove D_x è l'insieme dominato dal vettore x. L'efficiente superiore è l'insieme dei vettori appartenenti a chius S che non sono dominati da nessun vettore appartenente allo stesso insieme.

Se l'insieme è convesso è anche $F^+C = E^+C$.

Si noti che l'insieme conv Y che ammette un efficiente superiore, il cui cono

Nel paragrafo 3 sono riassunte le applicazioni nella teoria economica di una particolare dualità, quella esistente tra una funzione e la sua coniugata.

Nel paragrafo 4 vengono trattate le proprietà duali tra la funzione di *produzione e le funzioni di costo minimo o ricavo massimo.*

Infine, nel paragrafo 5, ci occupiamo di funzioni di produzione congiunta con insiemi di produzione non necessariamente convessi. Introduciamo il concetto di coniugata parziale di una funzione e stabiliamo relazioni duali tra la funzione di profitto e le funzioni di costo o ricavo. L'introduzione della funzione di costo generalizzata permette di dare una soluzione del classico **paradosso di Calais.**

2. SINTESI DELLE APPLICAZIONI NELLA TEORIA ECONOMICA DELLA DUALITA' IN ANALISI CONVESSA

Sintetizziamo ora quanto si rinviene in letteratura circa le applicazioni dei teoremi di analisi convessa richiamati nel paragrafo 1.

Sia $y = | q,z | \in R^{n+m}$ un vettore di produzione essendo $q = (q_1, ..., q_n)$, dove $q_i \geq 0$ sono gli n prodotti e $z = (z_1, z_2, ..., z_m)$ dove $z_i \leq 0$ gli m fattori. Supponiamo che l'insieme Y dei vettori y sia chiuso e non vuoto. L'insieme Y è un sottoinsieme del prodotto dell'ortante positivo o^+ dello spazio dei prodotti per l'ortante negativo o^- di quello dei fattori.

Allo scopo di semplificare le notazioni, seguendo la terminologia adottata in | 2 |, definiamo **frontiera superiore** di un convesso C l'insieme (se esiste) F^+C definito da:

$$F^+C = \{x \in \text{chius } C \mid bx = \delta^\wedge(x \mid C), \forall b > 0\} .$$

Si noti che, se C è superiormente limitato, esso ammette una frontiera superiore (non vale il viceversa).

Inoltre, definiamo **efficiente superiore** dell'insieme generico S l'insieme:

$$E^+S = \{x \in \text{chius } S \mid x \notin D_x, \forall x \in \text{chius } S\} ,$$

dove D_x è l'insieme dominato dal vettore x. L'efficiente superiore è l'insieme dei vettori appartenenti a chius S che non sono dominati da nessun vettore appartenente allo stesso insieme.

Se l'insieme è convesso è anche $F^+C = E^+C$.

Si noti che l'insieme conv Y che ammette un efficiente superiore, il cui cono

è l'espressione implicita di una funzione, parte della quale è la funzione di produzione, purché il dominio di definizione sia opportunamente delimitato.

Sussistono inoltre le relazioni:

$$y^\circ \in \partial \prod(p^\circ \mid \text{conv } Y) \Leftrightarrow \gamma(y^\circ \mid \text{conv } Y) = 1$$

$$p^\circ \in \partial\gamma(y^\circ \mid \text{conv } Y) \Leftrightarrow \prod(p^\circ \mid \text{conv } Y) = 1$$

che riassumono la dualità tra l'insieme di produzione ed il suo polare.

3. SINTESI DELL'APPLICAZIONE NELLA TEORIA ECONOMICA DELLA DUALITA' DEFINITA DALLA FUNZIONE CONIUGATA

Le nozioni richiamate in 1, applicate alla teoria della produzione consentono notoriamente di stabilire delle dualità tra funzione normalizzata di profitto e funzione di produzione. Ne richiamiamo gli aspetti essenziali.

Indichiamo con $x \geq 0$ i fattori produttivi in numero di n e con $q = f(x) > 0$ la funzione di produzione dell'unico prodotto q. In questo caso il massimo profitto è

$$\Pi(p,\bar{p}) = \sup_x\{pf(x) - \bar{p}x\}$$

dove p è il prezzo del prodotto e $\bar{p} \in R^n$ è il vettore dei prezzi dei fattori. Definiamo **profitto massimo normalizzato** $\Pi'(p')$ l'espressione

$$\Pi'(p') = \Pi(p,\bar{p})/p = \sup_x\{f(x) - p'x\} .$$

La funzione di profitto normalizzata è la coniugata di $-f(x)$. Segue che, se la funzione di produzione è concava, allora $\Pi'(p')$ è convessa e decrescente.

Inoltre, poiché il sottodifferenziale di una funzione convessa e quello della sua coniugata sono l'uno funzione inversa dell'altra, si ha che:

$$\bar{p} \in \partial f(x) \Leftrightarrow x \in -\partial \prod'(p') . \tag{3.1}$$

Chiaramente, se la funzione di produzione, oltre che concava, è differenziabile o poliedrica o omotetica ecc., si hanno tutte le conseguenze note sulla funzione di massimo profitto normalizzato.

Tali proprietà sono sfruttate econometricamente per risolvere il problema,

ritenuto più agevole, di risalire dalle proprietà delle funzioni di profitto alle proprietà dell'insieme Y delle possibilità tecniche di produzione.

Supponiamo che la funzione di produzione (generalmente quella di breve periodo) dipenda anche da parametri costanti, ossia che $q = f(x,w)$ dove w è il vettore dei parametri costanti, inoltre supponiamo che essa sia differenziabile due volte. In tal caso, applicando la trasformata di Legendre, si ottengono le condizioni di Hotelling, formulate nel 1932:

$$\nabla_w f = \nabla_w \Pi' . \tag{3.2}$$

Essendo

$$f(x)-\Pi'(p') = p'x ,$$

dalla (3.1) si ha l'ulteriore relazione duale:

$$f = \Pi' + p'\nabla_{p'}\Pi' \qquad \Pi' = f - x\nabla_x f .$$

La trasformata di Legendre consente una ulteriore applicazione al caso di produzione congiunta. Sia $H(y) = 0$ la funzione di produzione, nella quale $y = (q,z,x)$ ove $q \geq 0$ ha n componenti, $z = -x \leq 0$ ha m componenti ed $x > 0$ è un fattore non riproducibile. Per definizione, la funzione di produzione rappresenta il massimo ottenibile di ciascun fattore, assegnati tutti gli altri prodotti e tutti i fattori oppure, equivalentemente, il minimo di ciascun fattore, assegnati tutti gli altri fattori e tutti i prodotti. Perciò, se esplicitiamo la funzione di produzione, scrivendola nella forma:

$$x = F(q,z) ,$$

e supponiamo che F sia convessa, dividendo il profitto per il prezzo del fattore $(m+1)$-mo possiamo scrivere una nuova espressione del massimo profitto normalizzato come

$$\Pi'' = \sup_{qz}\{p_q q + p_z z - F(q,z)\} .$$

Quindi, ammessa la differenziabilità di F e supposto che il suo dominio di definizione si estenda al prodotto degli ortanti positivo e negativo interessati, si ottiene una generalizzazione del lemma di Hotelling, data dalla corrispondenza duale:

$$\nabla_q F = p_q \qquad \nabla_{p_q} \Pi'' = q$$

$$\nabla_z F = p_z \qquad \nabla_{p_z} \Pi'' = z$$

4. DUALITA', FUNZIONE DI PRODUZIONE, DI COSTO MINIMO E RICAVO MASSIMO

Riprendiamo in esame la funzione di produzione di una azienda con prodotto singolo $q = f(x)$ e sia f una qualunque funzione numerica continua o semicontinua dall'alto. Il costo minimo di produzione di q è:

$$C(q,p) = \inf_x \{px \mid f(x) \geq q\} .$$

La funzione di costo C(q,p) è positiva, positivamente omogenea di grado 1, concava, continua in p; non decrescente e semicontinua dal basso in q. Se esiste una funzione di costo che soddisfa alle condizioni elencate ed è differenziabile, allora, per la proprietà (g) enunciata in 1, si ottiene il lemma di Shepard:

$$x(p,q) = \nabla_p C(q,p) .$$

Tenuto conto che costo minimo è il minimo, per ogni q, di px sull'insieme di livello q di f(x), ossia $\{x \mid f(x) \geq q\}$, se la funzione di produzione è quasi concava, può essere dualmente ricostruita a partire dalla funzione di costo come frontiera dell'unione di tutti gli insiemi di livello 1 al variare di q.

Più in generale, considerando l'insieme di produzione Y come il grafico di una trasformazione, sia

$$Q = \rho(z) : R^m \to R^n$$

la corrispondenza che definisce come immagine l'insieme Q che chiamiamo di **trasformazione** e

$$Z = \rho^{-1}(q)$$

l'insieme di sostituzione.

La funzione di costo

$$C(q,p_z) = \delta^{\wedge}(p_z \mid \text{conv } Z)$$

coincide con la funzione di sostegno di Z(q). Essendo Z superiormente limitato, il dominio di definizione di C è l'intero ortante non negativo. Indichiamo con

$$\gamma'(z \mid \text{conv } Z(q)) = \gamma'(q,z)$$

la funzione di calibro di Z.

Le relazioni di dualità si sintetizzano in:

$$z^{\circ} \in \partial\, p_z\, C(q^{\circ},p_z^{\circ}) \Leftrightarrow \gamma'(q^{\circ},z^{\circ}) = 1$$

$$p_z^{\circ} \in \partial\gamma'(q^{\circ},z^{\circ}) \Leftrightarrow C(q^{\circ},p_z^{\circ}) = 1$$

Ovviamente sono minimizzanti per il costo solo i vettori z° che appartengono alla intersezione tra la faccia esposta di conv Z, individuata dal sottodifferenziale del costo, e l'insieme Z.

Si osservi che le funzioni C e γ' possiedono le seguenti caratteristiche duali: le proprietà di γ' rispetto a z sono identiche a quelle di C rispetto a p_z°; le proprietà di C rispetto a q sono reciproche delle proprietà di γ' rispetto a q.

Anche se la curva dei massimi ricavi non è usata in letteratura, essa merita di essere segnalata per la simmetria rispetto alla curva dei costi (minimi). Il ricavo R è la funzione:

$$R(z,p_q) = \delta^{\wedge}(p_q \mid \text{conv } Q)$$

positiva, positivamente omogenea di grado 1, convessa, continua in p_q, non crescente e semicontinua dall'alto. Ad essa si estendono le dualità con la funzione di calibro relativa all'insieme Q(z).

5. UNA TRATTAZIONE PIU' ESTESA DELLA DUALITA'

Nei paragrafi precedenti riteniamo di aver esposto l'essenziale delle applicazioni dei teoremi della dualità nella teoria della produzione.

Occorre tener presente che spesso in letteratura viene intesa come dualità una semplice corrispondenza. Le sole relazioni attinte alla teoria della dualità sono quelle tra funzioni di profitto (o di costo o di ricavo) e funzioni di calibro.

Le relazioni di dualità corrispondenti al coniugio delle funzioni convesse sono applicate solo in due casi di portata non generale (cfr. par.2).

In questo paragrafo daremo una relazione di dualità coniugata tra funzione di profitto e funzione di costo o di ricavo per il caso generale di produzione congiunta ed insieme anche non convesso.

Probabilmente, tali relazioni non sono state prese in considerazione sino ad ora in ragione del fatto che il grafico della funzione di profitto è un cono e, conseguentemente, la sua coniugata è nulla. Per superare tale ostacolo osserviamo che, se $f(x)$, $x=[u\ w]$ è una funzione convessa, avente le caratteristiche di una funzione di profitto, e si considera la sua intersezione con l'iperpiano $w=w_o=\text{cost.}$, allora la funzione $f(u,w_o)$ è una funzione convessa che ha una coniugata non identicamente nulla.

Definiamo pertanto come **coniugata parziale** della funzione $f(x)=f(u,w)$ l'operatore:

$$f_u\hat{}\,(b)=\sup_u\{bu-f(u,w)\}\,,$$

dove b è un vettore confrontabile con u.

Si riprenda in considerazione l'insieme di produzione Y. Proviamo il seguente

Teorema 5.1. Se Y è convesso, la funzione di costo (minimo) è la coniugata parziale rispetto a p_q della funzione di profitto.

Dimostrazione. Sia $\Pi(p_q,p_z)$ la funzione di profitto. La coniugata parziale:

$$\Pi\, p_q\hat{}\ = \sup p_q\,\{p_q q-\Pi(p_q,p_z)\}\,,$$

si ottiene per i valori ottimali q° tali che

$$q^\circ\in\partial\, p_q\,\Pi(p_q,p_z)\,.$$

Quindi:

$$\Pi_p\hat{}\,(p_q,p_z)\ =\ p_q{}^\circ q^\circ-(p_q{}^\circ q^\circ+p_z{}^\circ z^\circ)\ =\ C(q,p_z)\,.$$

La funzione di costo è una funzione convessa che ha rispetto a q le stesse proprietà che la funzione $\Pi(p_q,p_z)$, p_z = cost., ha rispetto a p_q.

Tenuto conto della corrispondenza inversa esistente tra le funzioni sottodifferenziali, si ricava:

$$p_q \in \partial_q C(q,p_z) \Leftrightarrow q^\circ \in \partial\, p_q\, \Pi(p_q,p_z)\,,$$

si trova cioè la regola per cui l'eguaglianza del prezzo dei fattori al costo marginale individua la produzione ottimale q°, con tutte le conseguenze dovute all'ipotesi di differenziabilità.

La corrispondenza $\partial_q C(q,p_z)$ è la **funzione dei costi marginali.** Essa è omogenea di grado 1 rispetto ai prezzi dei fattori.

La corrispondenza $\partial\, p_q \Pi(p_q,p_z)$ è la **funzione di offerta dell'impresa,** essa è l'inversa della funzione dei costi marginali.

Per la funzione di ricavo (massimo) si ha una proprietà analoga a quella espressa in 5.1 per la funzione di costo (minimo), infatti

Teorema 5.2. Se Y è convesso, la funzione di ricavo (massimo) R è la funzione opposta della coniugata parziale rispetto a p_z della funzione di profitto.

Dimostrazione. E' del tutto analoga a quella di 5.1.

Segue che

$$p_z \in \partial_z(-R(z,p_q)) \Leftrightarrow z^\circ \in \partial\, p_z \Pi(p_z,p_q)\,.$$

Si ha che la funzione R è concava. La corrispondenza $\partial_z(-R(z,p_q))$ è la **funzione dei ricavi marginali**; essa è omogenea di grado 1 rispetto ai prezzi dei prodotti.

La corrispondenza $\partial\, p_z \prod(p_z,p_q)$ è la **funzione di domanda dell'impresa;** essa è uguale all'opposta della funzione inversa dei ricavi marginali.

I teoremi 5.1 e 5.2 possono essere generalizzati ad insiemi di produzione non convessi, infatti si ha il

Teorema 5.3. Sia Y un insieme di produzione non convesso. Allora la coniugata parziale rispetto a p_q della funzione di profitto è la estensione convessa della funzione di costo minimo e l'opposta della coniugata parziale rispetto a p_z della funzione di profitto è la estensione convessa della funzione di ricavo massimo, ossia si ha:

$$\Pi\, p_q\,\hat{}\,(q,p_z) = \text{conv}\ C(q,p_z)\ ;$$

$$-\Pi\, p_z\,\hat{}\,(z,p_q) = \text{conv}\ R(z,p_q)\ .$$

Dimostrazione. Per la simmetria esistente tra le due relazioni dette nell'enunciato, è sufficiente dimostrare la prima eguaglianza.

Poniamo

$$C(q, p_z) = C(q \mid Y) \text{ (vera funzione di costo)}$$

$$C^{\circ}(q,p_z) := C(q \mid \text{conv } Y, p_z)\ ,$$

ove (cfr. | 2 |, pag. 36)

$$C(q \mid Y, p_z) \text{ se } (q,z)\in Y$$

$C(q \mid \text{conv } Y, p_z) =$

$$\hat{\text{i}}\inf\{\lambda_1 C(q_1) + \ldots + \lambda_m C(q_m) \mid \lambda_1 q_1 + \ldots + \lambda_m q_m = q \text{ se } q\in \text{conv } Y\text{-}Y\}\ .$$

Poiché la funzione di profitto è calcolata sempre su conv Y, per quanto detto nel caso di insiemi di produzione convessi, si ha che

$$\Pi\, p_q\,\hat{}\,(q,p_z) = C^{\circ}(q,p_z)\ .$$

Allora è sufficiente provare che

$$\text{conv } C(q \mid Y, p_z) = C^{\circ}(q,p_z) := C(q \mid \text{conv } Y, p_z)\ .$$

Per definizione, l'estensione convessa (di una qualsiasi funzione, e quindi anche) di $C(q \mid Y, p_z)$, è la funzione il cui epigrafo è l'estensione convessa dell'epigrafo di $C(q \mid Y, p_z)$.

Per definizione di epigrafo si ha

$$\text{epi } C(q \mid Y, p_z) = \{(q,z,\mu) \mid (q,z)\in Y, \mu \geq C(q,p_z)\}\ .$$

Denotiamo con A l'insieme seguente:

$$A := \text{conv epi } C(q \mid Y, p_z) =$$
$$= (q,z,\mu) = \lambda_1(q_1,z_1,\mu_1) + \ldots + \lambda_m(q_m,z_m,\mu_m)$$

con $(q_1,z_1,\mu_1) \in \text{epi } C(q \mid Y, p_z)$, i.e. $\mu_1 \geq C(q_1 \mid Y,p_z)$.

Denotiamo, inoltre, con B il seguente insieme:

$$B := \text{epi } C(q \mid Y, p_z) =$$
$$= \text{epi } C(q \mid Y, p_z) \cup \text{epi inf}\{\lambda_1 C(q_1) + \ldots + \lambda_m C(q_m)$$

con $q_i \in Y, \lambda_1 q_1 + \ldots + \lambda_m q_m = q$.

Per provare l'asserto è sufficiente provare che A = B.

L'eguaglianza A = B è banalmente verificata per qualsiasi punto di Y.

Supponiamo $(q_o,z_o,\mu_o) \in A$ con $(q_o,z_o) \notin Y$ e proviamo che $(q_o,z_o,\mu_o) \in B$. L'ipotesi implica che

$$q_o = \lambda_1 q_1 + \ldots + \lambda_m q_m$$

$$z_o = \lambda_1 z_1 + \ldots + \lambda_m z_m$$

$$\mu_o = \lambda_1 \mu_1 + \ldots + \lambda_m \mu_m$$

$$\mu_1 \geq C(q_i \mid Y,p_z)$$

Dalle prime due relazioni segue che $(q_o,z_o) \in \text{conv } Y$, inoltre si ha:

$$\mu_o = \lambda_1 \mu_1 + \ldots + \lambda m_\mu m_\geq$$
$$\geq \lambda_1 C(q_1 \mid Y,p_z) + \ldots + \lambda_m C(q_m \mid Y,p_z) \geq$$
$$\geq \inf\{\lambda_1 C(q_1 \mid Y,p_z) + \ldots + \lambda_m C(q_m \mid Y,p_z)$$

dunque $(q_o,z_o,\mu_o) \in B$.

Proviamo ora che ogni punto di B è anche in A.

Per i punti di epi $C(q \mid Y,p_z)$ l'asserto è chiaramente verificato. Consideriamo allora un punto $P \in B \setminus \text{epi } C(q \mid Y,p_z)$.

Ciò vuol dire che

$$\mu_o = \mu(P) \geq \inf\{\lambda_1 C(q_1 \mid Y,p_z) + \ldots + \lambda_m C(q_m \mid Y,p_z)\}.$$

Segue che

$$\mu_o = \lambda_1 C(q_1 \mid Y, p_z) + \ldots + \lambda_m C(q_m \mid Y, p_z);$$

allora, se $\mu_1 = C(q_i \mid Y, p_z)$, segue che

$$\mu_o = \lambda_{11} + \ldots + \lambda_{mm}, \text{ con } \mu_1 \geq C(q_i \mid Y, p_z).$$

Inoltre il punto (q_o, z_o, μ_o), ove

$q_o = \lambda_1 + \ldots + \lambda_m q_m$,
$z_o = \lambda_1 z_1 + \ldots + \lambda_m z_m$, è un punto di A.

Così l'asserto è completamente provato.

I risultati ottenuti consentono di estendere agli insiemi di produzione non convessi la regola ottimale: prezzo = costo marginale; inoltre tali risultati eliminano tutte le complicazioni connesse con il massimo profitto quando la funzione di costo è relativa ad una funzione di produzione quasi concava.

Illustriamo brevemente due delle tante difficoltà che vengono risolte attraverso la funzione di costo generalizzata.

(a) **Il paradosso di Calais** consiste nel seguente problema:

Ci sia una serie di traghetti che debbono servire una domanda passeggeri. L'applicazione della regola prezzo = costo marginale conduce alla seguente conseguenza: il primo passeggero ha un costo marginale pari a quello necessario per muovere il traghetto, se c è la capacità del traghetto, tutti gli altri c-1 passeggeri hanno un costo marginale nullo; il passeggero (c + 1)-mo ha di nuovo un costo marginale pari a quello necessario per muovere il traghetto, mentre quelli successivi zero, ... Il paradosso di Calais discende dall'applicazione della regola prezzo = costo marginale a questa situazione.

Se supponiamo, solo per semplicità, che tutti i traghetti abbiano costo identico, la funzione dei costi totali è una funzione a gradini, la cui estensione convessa si ottiene mediante una retta che congiunge gli spigoli inferiori dei gradini e la cui inclinazione è il costo per passeggero. Allora:

- Se vale l'ipotesi della teoria della produzione di domanda perfettamente elastica, avremo prezzo = costo medio

- Se, invece si cerca l'ottimo di efficienza, allora si ottiene un'offerta perfettamente elastica al costo medio, la quale determina le quantità da trasportare, come punti di intersezione con la funzione di domanda. Poiché tale punto appartiene all'intervallo tra due punti della funzione di costo, l'efficienza richiede che parta solo un numero di traghetti completamente

pieni (anche lasciando a terra passeggeri).

(b) Altro esempio è dato da una produzione puntiforme (con solo pochi punti). Considerando i costi medi relativi alle dioverse produzioni e la loro estensione convessa, si ottiene la funzione di costo generalizzata e quindi quella dei costi marginali, che, applicate con le precauzioni dette in precedenza, permettono di decidere la produzione.

SOMMARIO. Nella teoria della produzione è stato usato un complesso di proprietà duali, che vengono riassunte nel paragrafo 2. Inoltre, la dualità definita dalla coniugata di una funzione convessa viene sfruttata, sotto ipotesi restrittive (cfr. par.3), per stabilire corrispondenze tra funzioni di profitto e funzioni di produzione.

In questa nota introduciamo il concetto di coniugata parziale, onde ottenere una relazione duale tra funzione di profitto e funzioni di costo o ricavo, nel caso più generale di produzione congiunta, anche con insiemi di produzione non convessi. I risultati trovano applicazione nella spiegazione del noto Paradosso di Calais.

BIBLIOGRAFIA

| 1 | I: ADORISIO, **Principi di ottimizzazione non lineare**. Patron, Bologna, 1980.

| 2 | I. ADORISIO, **Ingegneria della produzione astratta**. CEDAM, Padova, 1986.

| 3 | A. A. V. V., **Consumer Theory**. Hand book of Math. Econom. vol. II, cap. 9-10-12, edited by Arrow & Intriligator, North Holland P.C., 1982.

| 4 | M. FUSS and Mc FADDEN, **Production economics: a dual approach to theory and applications**. North Holland P.C., Amsterdam-New York-Oxford, (1978).

| 5 | R. HOLMES, **A course on optimization and best approximation**. Lectures Notes 257, Springer-Verlag, Berlin-Heidelberg-New York, (1972).

| 6 | R. T. ROKAFELLER, **Convex Analysis**. Princeton University Press (1970).

RATIO MATH. 1.
(1990), 15 - 37

Il Problema della Protezione dell'Informazione, I: Cenni Storici e Metodi Statistici per la Decrittazione di Sistemi di Cifratura Classici

Emilio Ambrisi (*) e Franco Eugeni (**)

(*) Mathesis - via Vicenza 23 - Roma

(**) Dipartimento di Scienze e Storia dell'Architettura - Università di Pescara

1.- INTRODUZIONE: UN PO' DI STORIA

Una visione storica del problema è sempre di grande utilità per la comprensione dello stesso. In questa introduzione intendo dare una breve, spero efficace, panoramica sulla Crittologia.

La Crittologia può essere divisa in tre grandi branche:

- la **crittografia** o arte delle scritture segrete. In questo ambito il problema è nascondere un messaggio con dei procedimenti noti solo al mittente e al destinatario al fine di impedire che un personaggio estraneo alla comunicazione possa, senza esserne autorizzato, comprendere il messaggio.

I procedimenti per "cifrare" e "decifrare" i messaggi sono il segreto del codice.

- **l'autenticazione** è un ulteriore procedimento mediante il quale il ricevente ha una garanzia che il messaggio sia esattamente quello spedito proprio dal mittente, e che il testo sia autentico. Metodi di autenticazione più sofisticati sono i procedimenti di firma numerica, mediante essi il mittente non può disconoscere di aver inviato quel messaggio; inoltre il destinatario è in

grado di provare ad un terzo l'identità del mittente.

- la **crittoanalisi** è la metodologia di ricerca che mira alla ricostruzione, parziale e/o totale, dei sistemi di cifratura usati senza essere in possesso nè della loro architettura, nè delle norme d'impiego, nè delle chiavi usate. Le condizioni di lavoro precedentemente indicate sono le più difficili che si possono presentare.

L'uso delle scritture segrete è antichissimo. Erodoto (VII, 139) ci narra che un tale Demarato riuscì a informare i Lacedemoni del progetto di Serse di invadere la Grecia facendo pervenire loro un messaggio inciso su di una tavoletta, che era stata ricoperta con cera. Aulo Gellio (*Noct. att.*, XVII, 9) parla di un sistema simile, usato dai Cartaginesi, e descrive la *scytala* lacedemonica, della quale parla anche Plutarco. I caratteri venivano tracciati sopra una stretta striscia di pelle arrotolata attorno ad un bastone. Essi potevano essere letti solo da chi possedeva un bastone dello stesso diametro. Svetonio (*Caes.*, LVI) parla di un alfabeto convenzionale usato da Giulio Cesare, consistente nella sostituzione di ogni lettera con quella che la segue di un certo numero di posti nell'alfabeto normale.

Nel Medioevo non si ebbe una sostanziale evoluzione dei sistemi crittografici. Nel Rinascimento invece la crittografia ebbe notevole impulso; nuovi sistemi di cifratura furono ideati da Leon Battista Alberti, sul cui codice torneremo più avanti, da Giovan Battista Della Porta, celebre fisico napoletano (1540-1615), inventore della camera oscura, autore fra l'altro di un trattato *De furtivis literarum notis* (Napoli 1563), da Gerolamo Cardano, proprio lui: quello dell'equazione di terzo grado, medico e matematico (1501-1576), che, durante la sua sfortunata esistenza, trattò anche di argomenti crittografici in *De subtilitate* (Lione 1554). Fuori d'Italia troviamo il tedesco Tritemio (Johannes da Trittenheim, 1462-1516), autore della *Polygrafia* (Francoforte 1550) e della *Steganographia, hoc est ars per occultam scripturam animi sui voluntatem absentibus aperiendi* (Francoforte 1606-1622). Alcuni metodi di Tritemio sono riportati nel libro recente di Umberto Eco: Il pendolo di Focault. Il francese Blaise de Vigenère (1522-1596) autore di un *Traicté des chiffres ou secrètes manières d'escrire* (Parigi 1586) merita una descrizione a parte.

Il codice di Vigenère fu considerato "sicuro" per più di 200 anni. Fu un ufficiale prussiano ad ideare un test statistico (test di Kasiski) che distrusse il codice.

Nel sec. XVII fu attribuita sempre maggiore importanza alle scritture in cifra e le varie Nazioni adottarono sistemi di cifratura sempre più complessi.

Quindi, come è facilmente intuibile anche per i non addetti ai lavori, la

Crittologia nasce e prolifera come supporto per le comunicazioni militari. Con il passare dei secoli i metodi sono cambiati. I Crittografi naturalmente sono sempre a caccia di nuovi codici che i Crittoanalisti scoprono sistematicamente. E' interessante notare che in questa perenne caccia le invenzioni dalle più rudimentali alle più sofisticate giocano un importante ruolo.

A parte il cifrario di Giulio Cesare ricordato prima, va ricordato l'antico sistema persiano di trasmettere segnali accendendo fuochi su località elevate; simili sistemi di comunicazione furono usati dai greci, cartaginesi e romani, e addirittura fino ai tempi della guerra anglo-boera.

Si è ideato di tutto, alcuni scrivevano messaggi sulle foglie che servivano a bendare le piaghe purulente dello schiavo-corriere; durante le guerre persiane un messaggio fu impresso a fuoco sul cranio nudo di uno schiavo, al quale vennero poi fatti ricrescere i capelli.

Scipione l'Africano concepì un sistema di comunicazione recentemente molto usato dall'Unione Sovietica: inviare in altri paesi spie esperte travestite da domestici degli ambasciatori.

Nel sesto secolo, la rete informativa dell'Impero bizantino era divenuta uno dei fondamenti dello stato: agenti mercanti erano sparsi in tutto il paese con un sistema di import-export.

L'invenzione di alcuni dei più importanti sistemi di comunicazione viene fatta risalire ad Alessandro il Grande. Ad una certa distanza dal suo quartier generale, il Macedone aveva infatti costituito un vero e proprio ufficio di raccolta dati, basato sulle informazioni ottenute da agenti inviati nei paesi nemici. Costoro avevano anche il compito di spargere notizie false sulle intenzioni e le mosse di Alessandro, in modo da disorientare il nemico o indurlo a svelarsi. Insomma, un sistema simile a quello impiegato durante la 2^a guerra mondiale dall'ammiraglio americano Nimitz contro i giapponesi subito *prima della battaglia di Midway*.

Durante il Rinascimento, una rete fittissima di agenti copriva l'Europa: fra i più attivi erano quelli del Papato. Ma neanche il Papa poteva star tranquillo: il segretario di Adriano VI si dice fosse una spia dell'Imperatore Carlo V, al corrente di tutti i segreti del Papa e della sua corte.

Con la Riforma nasce così la "spia ideologica". Uomini e donne di ogni ceto sociale divennero traditori della loro patria per servire gli interessi di una delle due fazioni cristiane in lotta. Il miglior servizio di spionaggio dell'epoca era probabilmente quello spagnolo: l'agente principale di Filippo II era nientemeno che l'ambasciatore inglese a Parigi, Sir Edward Stafford, il quale fra l'altro riuscì a fornire agli spagnoli notizie sulla flotta di Sir Francis Drake, pronta a salpare contro l'Invincibile Armata. A questo punto però si inserì nel gioco Sir Francis Walshingham, che, raccolte le prove del tradimento di

Stafford, decise di sfruttarlo a suo vantaggio, così tramite Stafford si ottennero molteplici informazioni, ad esempio l'elenco preciso di tutte le spie spagnole in Inghilterra.

Padre Giuseppe, religioso al servizio del Cardinale Richelieu, fu famoso per la sua scuola di informatori. Essi trovarono pane per i loro denti solo con il servizio segreto inglese, guidato allora da Thurloe, abilissimo collaboratore di Cromwell.

Verso la fine del XVIII secolo il primato dell'organizzazione spionistica passa dall'Inghilterra alla Francia: Napoleone domina l'Europa, non solo con la potenza degli eserciti e con il genio strategico, ma anche con l'efficienza della sua rete di informatori. Tra questi il più grande di tutti, Karl Schulmeister.

Presentato da Savary a Napoleone con le parole "Ecco, Sire, un uomo tutto cervello e senza cuore, ai Vostri ordini", Schulmeister si accinse a quella che resta forse la più incredibile azione di spionaggio della storia: diventare capo del servizio di informazioni militari della coalizione avversa a Napoleone. Schulmeister si trasferì a Vienna ed offrì informazioni strategiche di grande importanza e *assolutamente vere.*

In meno di un anno, Schulmeister riuscì a farsi nominare capo del servizio di informazioni austriaco: da quel momento fu come se Napoleone stesso potesse esaminare i piani strategici del nemico.

Le vittorie di Ulm e di Austerlitz furono in gran parte dovute a Schulmeister, che non solo informava Napoleone delle mosse nemiche, ma forniva agli Alleati false indicazioni.

Nel 1900 la tecnica fa spietati passi avanti e i mezzi di comunicazione subiscono una vera e propria rivoluzione: la fotografia, il telegrafo, la radio, il telefono, l'aereo. Nascono i servizi militari organizzati. A volte forse anche più di uno per nazione. In Italia durante la 2^a guerra vi erano ad esempio i seguenti

Servizio Informazioni Militari (SIM) dell'Esercito

Servizio Informazioni Militari (SIS) della Marina

Servizio Informazioni Aeronautica (SIA) dell'Aeronautica

Centro di Controspionaggio Militare e Servizi Speciali (CCMSS) alle dipendenze del Ministro della Guerra

Organizzazione di Vigilanza e Repressione Antifascista (OVRA)

Chiusa l'era delle spie romantiche e degli avventurieri di genio, i nuovi personaggi saranno soprattutto colonnelli inglesi a riposo con l'hobby della decifrazione; giornalisti mondani affiliati da anni da qualche servizio segreto; taciturni camerieri turchi e scienziati atomici convinti che una potenza diversa dalla loro patria avrebbe fatto un uso più giusto dei terribili segreti di cui erano

effettivi di truppe, dati bellici o altre informazioni. Ecco un esempio di codice molto elementare.

Cliente = Alleato	Acquistare = Attaccare
Merce = Esercito nemico	Ditta = Divisione in soccorso
Interpellare = Comunicare a ...	Inviare = Far saltare

Per messaggi di questo tipo era necessario avere fantasia e tempo a disposizione. A causa della loro ingenuità essi apparivano subito come cifrati. Non erano così adatti per trasmettere informazioni di una certa importanza. E' bene che i messaggi cifrati sembrino veri. Messaggi convenzionali venivano alle volte inviati anche per mezzo di inserzioni nei giornali:

"Vendesi terreni per 10 ettari, 2 fabbricati, 823 bovini"

può essere benissimo un messaggio in cui 102823 è la chiave da usare per decifrare un successivo o precedente messaggio.

L'abilità consiste nel pensare il testo in modo da non destare il sospetto e da non richiamare l'attenzione dell'avversario.

Il mezzo più usato da quando esiste è stata la radio. Con essa è possibile inviare tempestivamente qualsiasi messaggio al proprio centro, da questo è possibile ricevere in ogni momento ordini e informazioni. Le trasmissioni avvenivano ad ore prestabilite ed iniziavano sempre con la sigla di una delle parti. Il dispaccio veniva trasmesso cifrato, con un sistema la cui chiave era conosciuta quasi sempre da un solo trasmettitore che, una volta raccolte le informazioni, le cifrava per affidarle all'agente incaricato di effettuare la trasmissione. Così questi inviava al centro una serie di numeri o lettere a lui stesso incomprensibili. Nel corso dell'emissione l'operatore inseriva il cosiddetto *parity check* che segnalava eventuali errori dovuti al canale e il *security check*, cioè un errore, una parola sbagliata sempre uguale, in modo che il centro avesse la certezza che l'agente stava trasmettendo liberamente. La radio presentava il grave inconveniente di poter essere individuata dalle stazioni di ascolto e di intercettazione avversari.

Come si è detto, i messaggi, prima di essere trasmessi, venivano tradotti "in cifra" secondo particolari metodi appositamente studiati.

I vari sistemi di cifratura possono a grandi linee raggrupparsi in tre categorie: sistemi *a trasposizione*, sistemi *a sostituzione* e sistemi *misti*. Nei primi la traduzione del linguaggio chiaro in linguaggio segreto ha luogo mediante una specie di anagramma degli elementi dei testi chiari; nei secondi mediante sostituzione degli elementi stessi con cifre crittografiche, cioè con segni convenzionali, o con gruppi di tali segni; nei terzi mediante entrambe le

operazioni, eseguite successivamente l'una dopo l'altra in un certo ordine.

I sistemi a sostituzione consistono nel mettere al posto di ogni lettera (o gruppo di lettere, o parole o frasi del testo) un'altra lettera (o numero, o gruppo di lettere o di numeri). La sostituzione letterale può essere *monoalfabetica* o *polialfabetica* secondo che ha luogo in base a un solo alfabeto cifrante o a più alfabeti cifranti, da adoperare in blocco, ma con una certa legge, di volta in volta, prestabilita.

Ad esempio il seguente messaggio: "**Appuntamento ora X....**" può essere così trasmesso:

BQQVMUBNFOUPPSPZ...

L'alfabeto usato in questo caso è un alfabeto slittato di un posto, nel quale la B ha preso il posto della A, la C della B, la D della C e così via.

Naturalmente l'alfabeto cifrante si può ottenere spostando di due, tre, quattro, anche ventisei posti l'alfabeto vero.

Un altro messaggio: "**giorno X ora Y In arrivo navi ed aerei alleati ...**" cifrato per trasposizione senza chiave diviene:

GIIE INEA OADT RRAI NREA OIRB XVEC OOID RNAE AALF YVLG

Esso si ottiene scrivendo su di un rettangolo il messaggio da inviare nel modo seguente:

GIORNOXORAY

INARRIVONAV

IEDAEREIALL

EATIABCDEFG

La cifratura può aver luogo per *lettere*, per *sillabe*, o per *gruppi* di un numero fisso di lettere (*poligrammi*), o per *frasi*, o in modo promiscuo. La maggior parte degli autori ripartisce i sistemi di cifratura nelle due categorie di sistemi letterali o di sistemi a repertorio. I primi consistono nella trasposizione e/o sostituzione delle lettere o di poligrammi. I secondi consistono invece nella sostituzione delle parole e delle frasi. Questa operazione può essere seguita da una seconda cifratura, o **sopracifratura**, per trasposizione e/o per sostituzione delle relative cifre crittografiche. I segni convenzionali che rappresentano gli elementi del linguaggio chiaro possono essere di qualsiasi genere, ma nei tempi moderni è frequente l'uso di segni adoperati nella corrispondenza telegrafica. Sono usati i segni della normale scrittura, e per lo

più si usano o sole cifre arabe o sole lettere e si formano gruppi di un numero fisso di elementi.

Molto comuni sono i sistemi a gruppi di cinque lettere o di cinque cifre arabe, ovvero di dieci lettere costituenti un insieme pronunciabile, tali essendo i massimi tassabili per una parola nelle comunicazioni telegrafiche internazionali.

La convenzione in base alla quale si eseguono le operazioni di sostituzione e di trasposizione è sovente rappresentata da una *chiave*, cioè da una serie di numeri o di lettere, il cui uso può spiegarsi mediante esempi.

ESEMPIO

Alfabeto chiaro	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	W	Z		
Alfabeto cifrato	g	i	n	e	p	r	o	a	b	c	d	f	h	l	m	q	s	t	u	v	w	z		
												g	i	n	o	p	r							

e salta

saltano

La parola "ginepro" formata da lettere tutte distinte è la chiave. Il metodo di cifratura è ovvio. Da notare che per il fatto che da s → a z ci sono troppe lettere fisse potrebbe essere conveniente cambiare la parola chiave.

La cifratura può anche essere eseguita mediante l'uso di griglie, cioè di poligoni di cartone o di altra materia ripartiti in caselle, delle quali un certo numero forate. Il tipo originario è la griglia quadrata, ideata dal Cardano, con la quale la cifratura ha luogo sovrapponendo quadrati di cartone forati in un certo modo convenuto. Il messaggio viene scritto nei fori della griglia appoggiata su di un foglio di carta quadrettata, ruotando il cartoncino in un modo stabilito quando tutte le fessure sono state riempite. Dopo aver tolto la griglia, si rilevano le lettere o colonna per colonna, sia in senso verticale che in senso orizzontale, oppure mediante l'aiuto di una "chiave" come nei casi precedenti.

1° quadrato					
	1				
2					
	3		5		
		4		6	
					7
				8	

2° q. ruotato di 90° ant.					
				7	
			6		8
		5			
			4		
1		3			
	2				

più si usano o sole cifre arabe o sole lettere e si formano gruppi di un numero fisso di elementi.

Molto comuni sono i sistemi a gruppi di cinque lettere o di cinque cifre arabe, ovvero di dieci lettere costituenti un insieme pronunciabile, tali essendo i massimi tassabili per una parola nelle comunicazioni telegrafiche internazionali.

La convenzione in base alla quale si eseguono le operazioni di sostituzione e di trasposizione è sovente rappresentata da una *chiave*, cioè da una serie di numeri o di lettere, il cui uso può spiegarsi mediante esempi.

ESEMPIO

Alfabeto chiaro	A	B	C	D	E	F	G	H	I	L	M		
Alfabeto cifrato	g	i	n	e	p	r	o	a	b	c	d		

e salta

	N	O	P	Q	R	S	T	U	V	W	Z		
	f	h	l	m	q	s	t	u	v	w	z		
	g	i	n	o	p	r							

saltano

La parola "ginepro" formata da lettere tutte distinte è la chiave. Il metodo di cifratura è ovvio. Da notare che per il fatto che da s → a z ci sono troppe lettere fisse potrebbe essere conveniente cambiare la parola chiave.

La cifratura può anche essere eseguita mediante l'uso di griglie, cioè di poligoni di cartone o di altra materia ripartiti in caselle, delle quali un certo numero forate. Il tipo originario è la griglia quadrata, ideata dal Cardano, con la quale la cifratura ha luogo sovrapponendo quadrati di cartone forati in un certo modo convenuto. Il messaggio viene scritto nei fori della griglia appoggiata su di un foglio di carta quadrettata, ruotando il cartoncino in un modo stabilito quando tutte le fessure sono state riempite. Dopo aver tolto la griglia, si rilevano le lettere o colonna per colonna, sia in senso verticale che in senso orizzontale, oppure mediante l'aiuto di una "chiave" come nei casi precedenti.

1^o quadrato					
	1				
2					
	3		5		
		4		6	
					7
				8	

2^o q. ruotato di 90^o ant.					
				7	
			6		8
		5			
			4		
1		3			
	2				

testo chiaro LA CRITTOGRAFIA E' INTERESSANTE

	L									E			N				
A									A		I	T					
	C		I					I					E		E		
		R		T					F					R		S	
					T	G		A									S
				O			R									A	

Gli spazi vuoti vengono riempiti ad esempio con lettere casuali.

Per eliminare in parte le ripetizioni che compaiono necessariamente in ogni crittogramma, specialmente nei testi molto lunghi, si ricorre alla sopracifratura, operazione che consiste nel cifrare di nuovo il testo ottenuto con la prima cifratura, magari cifrando parzialmente il testo o usando un cifrario tipo quello dell'Alberti, nel quale cambiare alfabeto è facile.

Naturalmente il destinatario per poter decifrare un crittogramma doveva compiere operazioni inverse a quelle eseguite dal mittente.

Da un punto di vista storico, possiamo dire che nel Medio Evo, per le condizioni politiche, i codici segreti vengono usati poco ed in genere solo per nascondere nomi di personaggi importanti.

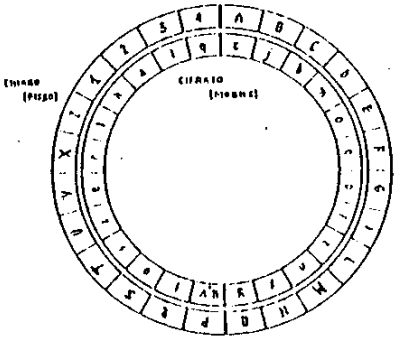
Verso la fine del Medio Evo, con l'inizio delle relazioni diplomatiche tra i vari stati, i codici segreti diventano una necessità.

Secondo ricerche storiche dovute a Meister (1902) l'uso sistematico dei codici segreti ebbe inizio nella Corte Papale, nelle Repubbliche e Signorie Italiane, a partire dal 1300 .

E' in questo periodo che la Crittografia ha una grossa evoluzione. Troviamo un cambiamento radicale, infatti nascono i primi codici segreti che non usano un solo alfabeto cifrante, ma molti alfabeti cifranti. Tali codici si chiamano codici polialfabetici.

Il primo codice polialfabetico è dovuto ad un illustre pensatore italiano: Leon Battista Alberti - architetto, urbanista, pedagogo, matematico e crittografo. E' suo, su commissione del segretario pontificio, Leonardo Dato, il primo codice polialfabetico della storia, messo a punto intorno al 1466.

Esso era costituito mediante due cerchi concentrici. Nel disco più esterno appare l'alfabeto in chiaro formato da 24 caselle, 20 delle quali contenenti lettere (mancano per ragioni di sicurezza crittografica, le lettere che si presentano con minore frequenza, cioè J, K, Y, W, Q, H) e le rimanenti quattro i numeri 1, 2, 3, 4.



Il disco interno contiene una permutazione di altre 24 lettere (manca la lettera w ed è u = v) formanti l'alfabeto cifrante. Esso può ruotare rispetto al primo disco.

Si fissa, prima di cominciare a criptare il messaggio, una lettera dell'alfabeto in chiaro detta indice del codice. Poiché c'è una corrispondenza biunivoca tra le caselle dei due dischi, allora alla lettera scelta come indice del codice, sia ad esempio F, corrisponde una ed una sola lettera del disco interno. Come prima lettera del testo cifrato si scrive la lettera corrispondente ad F e poi ogni lettera del messaggio viene sostituita con la corrispondente sempre del disco più interno. Supponiamo ora che dopo un certo numero di lettere (anche uno solo) si desideri cambiare alfabeto per rendere più difficile una possibile decrittazione. Si scelga allora uno dei numeri 1, 2, 3, 4 che sono a disposizione, ad esempio il numero 2, che va pensato come inserito nel testo in chiaro. A questo numero si sostituisce la lettera che gli corrisponde nella corrispondenza data dai due dischi. Fatto ciò, si ruota il disco finché la lettera corrispondente al numero scelto non si vada a situare esattamente sotto l'indice del codice, la lettera F nel nostro caso. Questa operazione cambia la biezione tra l'alfabeto in chiaro e quello cifrante quindi otteniamo un altro alfabeto, fino a che non decidiamo di fissare un nuovo numero e così via.

La tendenza del periodo è quella di costruire algoritmi per cifrare semplici. Troviamo altri codici polialfabetici (ricordiamo, ad esempio, quelli di G.Cardano e di Bellaso) e nasce l'uso della parola chiave principalmente per merito di un altro italiano, Giovan Battista Della Porta (1563), l'inventore della camera oscura. Con riferimento alla tavola Della Porta (pag. seguente) vediamo l'uso della parola chiave in quel codice .

Si comincia con il fissare una parola del tutto arbitraria ma contenente lettere tutte distinte (ciò perché ad ogni parola corrisponderà un diverso alfabeto); sia AMBRISEMLO (abbiamo tolto tre I). Si scrive tale parola sotto il messaggio un numero di volte tale da "coprire" il messaggio stesso, indi si usano le tavole come nel seguente esempio.

ESEMPIO.

Cosa ne facciamo della parola chiave? Ogni lettera di essa, *ad esempio* a, ci dice *quale alfabeto dobbiamo usare* per criptare la lettera del messaggio corrispondente. Nel caso generale quindi si deve dare una permutazione dell'alfabeto per ogni lettera della parola chiave. La costruzione di queste permutazioni costituisce il codice stesso. Come esempio vediamo il sistema Porta

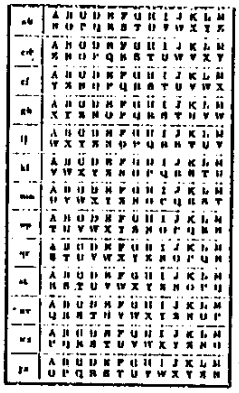


Tavola Della Porta

Nelle tavole di Della Porta le lettere minuscole scritte in testa danno il nome all'alfabeto di quella riga, che è ottenuto dividendo l'alfabeto in due parti di 13 lettere ognuna e stabilendo una biezione tra i due insiemi di 13 elementi. Allora se la lettera della parola chiave che stiamo considerando è una a oppure una b, *si cripta la lettera del testo corrispondente con l'alfabeto di nome* ab, e così via. Vediamo un esempio:

testo in chiaro: FRANCO EUGENI SPEDISCE UN TESTO SEGRETO

parola chiave : ambris emloam brisemlo am brise mloambr

testo cifrato : skniyk paoxap fknutlxx hg gwjcd lzzeygj

Per essere in grado di compilare i messaggi secondo i sistemi esposti, gli operatori devono conoscere sia le chiavi sia i sistemi di cifratura. Alle volte invece si sono usati codici cifranti, cioè fascicoli contenenti liste di cifre o di lettere da sostituire alle rispettive voci. Queste liste possono essere costituite da parole, frasi, o periodi, più frequentemente usati nei messaggi, con a fianco un gruppo cifrante, numerico o letterale, che può trasmettersi via telegrafo.

I sistemi monoalfabetici sono i più antichi; l'alfabeto cifrante è stabilito in un qualsiasi modo convenzionale e si può fare uso anche di *segni nulli*, nonché di *omofoni*, cioè di più segni rappresentanti la stessa lettera dell'alfabeto

normale, usabili indifferentemente.

I sistemi polialfabetici derivano tutti dalle tabelle ideate dall'Alberti, da Porta e da Tritemio.

Tritemio, citato ampiamente da Umberto Eco nel pendolo di Focault, usava rivestire i suoi molteplici codici, molti basati su peculiarità del latino, di misticismo. L'idea base fu quella di aggiungere molte parole in modo che il messaggio finale avesse senso compiuto. In Tritemio appare anche il **quadrato latino** 26x26 usato come tavola per cifrare e decifrare. Questo quadrato può essere visto come la tavola di addizione di Z_{26} qualora che sia

A = 0, B = 1, ..., Z = 25.

Un codice polialfabetico, che ha raggiunto maggiore notorietà, è quello dovuto al francese Blaise de Vigenère.

Egli nel 1586 pubblica il suo codice nel quale fa uso di una tavola quadrata, già introdotta dall'abate Tritemio e nota come tavola di Vigenère, sulla quale vi è veramente molto da dire. Il quadrato è passato alla storia come quadrato o *chiffre carré* del Vigenère. Esso è stato molto in voga, sino a epoca relativamente recente, per scopi militari e diplomatici.

	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Ogni riga della tavola è un alfabeto di Cesare, a cui diamo il nome della lettera posta a sinistra. Per criptare un messaggio si usano tanti alfabeti di Cesare quante sono le lettere della parola chiave.

ESEMPIO

Testo chiaro : IO SONO NATO A TERAMO

CHIAVE : te ramo tera m oteram

TESTO CIFRATO: bs jozc geko m hxvrma

La tavola è un quadrato latino cioè una matrice in ogni riga e colonna della quale vi è una permutazione della prima riga o colonna. Si tratta anche della tabella additiva delle classi resto modulo 26, quindi un esempio di gruppo finito. Il segreto di questo codice è tutto nella parola chiave. Quindi, il destinatario del messaggio (e si spera solo lui, oltre il mittente) conosce la parola chiave. Allora è in grado di decifrare il messaggio in arrivo usando il procedimento al contrario (ovvero la sottrazione modulo 26).

Per l'uso della suddetta tabella si adotta generalmente una chiave letterale consistente per lo più in una parola o in una frase, e la cifratura ha luogo sostituendo ogni lettera del testo chiaro con quella della colonna verticale, nel punto d'intersecazione delle colonne comincianti rispettivamente con la lettera da cifrare e con la corrispondente lettera della chiave, o viceversa.

Possono pure compilarsi tabelle per cifratura polialfabetica aventi per alfabeto base un alfabeto intervertito, che sia cioè una permutazione dell'alfabeto ordinario.

Sono stati ideati anche sistemi a rappresentazione numerica, nei quali gli alfabeti cifrati sono costituiti da numeri, ma essi non differiscono in maniera sostanziale, agli effetti del segreto crittografico, da quelli letterali.

I sistemi polialfabetici possono essere *a chiave fissa,* a chiave variabile, *a interruzione della chiave e autocifranti.* Nei sistemi a chiave variabile e in quelli a interruzione della chiave occorre stabilire per convenzione il modo in cui si deve segnalare al destinatario del messaggio il cambio o l'interruzione nell'uso della chiave. Nei sistemi autocifranti si adopera la chiave per le prime lettere del testo e si usa poi, come chiave, o lo stesso testo chiaro o il testo segreto ottenuto.

Può ricorrersi per la sostituzione polialfabetica all'uso di **macchine cifranti,** ciò che consente di eseguire rapidamente le operazioni di cifratura,

pure adoperando chiavi diverse e di notevole lunghezza. La cifratura per sostituzione può anche aver luogo per poligrammi, cioè per gruppi di un numero fisso di lettere, e per frazioni di lettere, cioè sostituendo le singole lettere del testo chiaro con gruppi di lettere o di cifre o di altri segni convenzionali, che si sottopongono poi a seconda cifratura. Potrebbe pure aver luogo per sillabe, ma i sistemi di questo tipo sono rarissimi e invero poco pratici. Le macchine cifranti moderne sono naturalmente i computer, ove tutto è veloce e dove la grande mole di lavoro non conta.

I sistemi *a repertorio*, che si ritengono ideati nel sec. XVII, sono di larghissimo uso nei tempi moderni, in quanto consentono maggior garanzia di sicurezza in confronto dei sistemi letterali e producono, d'altra parte, una notevole economia di spese telegrafiche. I repertorî, altrimenti chiamati codici, vocabolarî telegrafici, dizionarî cifrati, ecc., sono libri o anche programmi di computer contenenti un certo numero di voci, a ciascuna delle quali corrisponde un gruppo cifrante, composto generalmente di quattro o cinque lettere dell'alfabeto o cifre arabe.

3.- IL PROBLEMA DEI CRITTOANALISTI: INTERVENGONO GLI STATISTICI

Una simpatica storiella crittografica mostra come a volte non è bene fidarsi di piccole statistiche per dedurre.

Un intruso vuole carpire la parola d'ordine di un accampamento militare. Si nasconde dietro un cespuglio in prossimità dell'accesso e ascolta.

la sentinella domanda: dodici?
il 1° soldato risponde: sei! e passa;

la sentinella domanda: dieci?
il 2° soldato risponde: cinque! e passa;

la sentinella domanda: otto?
il 3° soldato risponde: quattro! e passa;

la sentinella domanda: sei?
il 4° soldato risponde: tre! e passa;

la sentinella domanda: quattro?

l'intruso risponde: due! e viene fulminato da un colpo di fucile perché per passare bisognava dire il numero delle lettere componenti il numero della domanda, quindi sette e non due!

La decrittazione dei crittogrammi è la traduzione di essi in linguaggio chiaro, eseguita da chi non sia a conoscenza dei cifrari e delle chiavi costituenti la base del segreto.

I metodi usati per decrittare i messaggi si basano su considerazioni statistiche, in particolare sulle caratteristiche di ciascuna lingua, cioè sul fatto che in ogni lingua le singole lettere, alcuni bigrammi e trigrammi e certe parole si ripetono più frequentemente di altre. Si chiama logoscopico il calcolo statistico delle parole, frasi e periodi che più frequentemente si riscontrano nel linguaggio. Il lavoro di decrittazione consiste in successive induzioni e deduzioni in merito al presumibile significato dei testi presi in esame e può essere agevolato da alcune circostanze favorevoli, quali il possesso di più testi cifrati relativi allo stesso testo chiaro, ma ottenuti con cifrari diversi, la conoscenza anche vaga del sistema di cifratura adottato, la conoscenza parziale o totale del testo chiaro corrispondente a qualche testo cifrato del quale si sia in possesso. Quindi cifrando un testo chiaro, se ad ogni lettera, o gruppo di lettere o parole si sostituisce un determinato segno, questo si ripeterà con la stessa frequenza del testo chiaro: cosicché alla lettera o alla cifra più frequentemente ripetuta nel testo cifrato, con ogni probabilità corrisponderà la lettera o la parola più frequente nel linguaggio chiaro.

Le basi linguistiche della decrittazione consistono nelle caratteristiche particolari di ciascuna lingua e cioè nelle sequenze percentuali delle lettere, dei bigrammi e trigrammi più comuni e di alcune parole, nelle sequenze percentuali delle lettere e di alcune parole tra di loro, nelle sequenze obbligate o molto probabili, in quelle escluse o assai poco probabili, nelle terminazioni più frequenti delle parole, ecc.. I dati caratteristici delle principali lingue sono contenuti in varie opere di crittografia.

Ad esempio nella lingua italiana il 45% delle lettere sono vocali e le sequenze con le quali si ripetono le varie lettere sono le seguenti:

A = 10,41 %	B = 0,95 %	C = 4,28 %
D = 3,82 %	E = 12,63 %	F = 0,75 %
G = 2,01 %	H = 1,10 %	I = 11,62 %
L = 6,61 %	M = 2,58 %	N = 6,49 %
O = 8,71 %	P = 3,26 %	Q = 0,57 %
R = 6,70 %	S = 6,04 %	T = 6,06 %
U = 3,04 %	V = 1,51 %	Z = 0,93 %

Nel seguente messaggio cifrato:

VSNHQ HPNFM HVHLA RQRQR VZUND LHQZN

si contano 5 H, 4 N, 4 Q, 3 R e 3 V alcune delle quali con ogni probabilità saranno vocali. Perciò quasi sicuramente la H corrisponderà alla "e".

Appare evidente che con ogni probabilità la prima parola, dato l'argomento di cui si tratta, sarà "spie" e quindi V = S e S = P. Perciò il crittogramma è stato ottenuto con un alfabeto spostato di tre posti. Una accurata verifica ci darà il seguente testo chiaro: **"Spie nemiche seguono nostri agenti".**

Bisogna però precisare che questi non sono che i metodi più semplici di decrittazione.

Ove non si conosca o presuma a quale sistema crittografico appartiene il metodo di cifratura, si deve anzitutto eseguire questa indagine, la quale spesso non presenta grandi difficoltà, avendo i varî sistemi tipici particolari caratteristiche. Non è raro tuttavia, e ciò avviene generalmente per i sistemi misti, che nel testo non si rilevino sufficienti indizî per la determinazione del sistema di cifratura; in questi casi il lavoro di crittoanalisi è, naturalmente, più difficile e può anche non portare, in mancanza di circostanze favorevoli, a un pratico risultato.

La decrittazione dei sistemi letterali a trasposizione si tenta mediante successive disposizioni e spostamenti delle lettere del testo cifrato, sino a quando non si riscontra qualche combinazione di lettere, parte di parola o parola, che valga a mettere sulla buona via.

Per i sistemi letterali a sostituzione monoalfabetica la decrittazione consiste nella ricostruzione dell'alfabeto cifrante.

Sia dato ad esempio il seguente crittogramma, che si presume riferirsi a un testo chiaro scritto in lingua italiana:

KSAJOHTQSVTKHXHJKTQPZJHQMTZFJATXS
ZQTJNNZTXJDTKHSXHFTPHMHEYSNZTDTE
TKKTETQEHKHJOHTQSILAASZHDTETQMSZS
QOJNJQJFSZHEJQJ

Il calcolo delle frequenze letterali dà il seguente risultato: 17 t; 13 h; 12 j; 10 q; 10 s; 8 z; 7 k; 6 e; 4 a; 4 n; 4 x; 3 d; 3 f; 3 m; 3 o; 2 p; 1 i; 1 l; 1 v; 1 y.

Il confronto delle suddette frequenze con quelle medie della lingua italiana (e 12,6%; i 11,6%; a 10,3%; o 8,7% ecc.) fa presumere che quattro delle lettere T, H, J, Q, S rappresentino le 4 vocali a, e, i, o; nel testo si riscontrano i

gruppi lo stesso posto; confrontando le frequenze suddette con quelle medie della lingua è possibile quasi sempre intuire il significato delle lettere più frequenti e formare in tal modo, in successivi tentativi, gruppi di lettere, parti di parole e parole, tenendo conto del presumibile contenuto del messaggio. Se gli alfabeti convenzionali sono disposti normalmente (tabella del Vigenère e simili) la conoscenza del significato di una lettera in un alfabeto ha per conseguenza quella del valore di tutte le altre lettere nello stesso alfabeto. Ciò non si verifica per i sistemi ad alfabeti intervertiti, nei quali però, se l'interversione è regolare, si ha l'equidistanza relativa delle varie lettere in tutti gli alfabeti e, conseguentemente, si deduce dal significato di una lettera in più alfabeti cifranti il valore che hanno in tutti questi alfabeti le lettere di cui si conosca il significato soltanto per uno di essi.

Per i sistemi a rappresentazione numerica, tanto monoalfabetici quanto polialfabetici, i metodi di decrittazione non sono diversi da quelli innanzi indicati per le rispettive categorie di sistemi a rappresentazione letterale.

La decrittazione dei sistemi a repertorio si tenta in base al confronto della frequenza dei gruppi cifranti con quella delle parole di uso più frequente nella lingua e cioè delle cosiddette parole vuote più importanti (articoli, verbi ausiliari, preposizioni, congiunzioni). La posizione di questi gruppi nel testo, il presumibile contenuto del messaggio, ed eventualmente la conoscenza, parziale o totale, di qualche testo chiaro corrispondente a un testo cifrato di cui si disponga, danno modo di intuire il significato di altri gruppi e di procedere nel lavoro di decrittazione.

La decrittazione dei repertorî ordinati e non sopracifrati è in linea di massima possibile, ove si disponga di testi aventi complessivamente una lunghezza opportuna, dato che la conoscenza o presunzione del significato di alcuni gruppi cifranti costituisce una guida di grande importanza. Circostanza particolarmente favorevole è l'esistenza di serie di gruppi che facciano pensare a una parola, generalmente nome proprio, cifrata mediante cifratura delle lettere o delle sillabe. Per esempio, se in un testo ottenuto con un repertorio di 10.000 voci che si ritenga in lingua italiana e in ordine normale, si riscontra una serie di gruppi come la seguente, si deve presumere che essa rappresenti un nome proprio e che i singoli gruppi corrispondano a una vocale o a una consonante secondo queste indicazioni:

3733	3409	7462	7462	0002	7462	4517
conson	vocale	conson.	conson.	vocale	conson.	vocale

Il gruppo 0002 è senza dubbio uguale ad a; i gruppi 3409 e 4517, data la distanza dall'inizio del cifrario e la loro distanza rispettiva equivalgono

presumibilmente ad e ed i; la consonante rappresentata da 3733 è molto probabilmente f. Il gruppo 7462 sarà presumibilmente corrispondente a p, r, s, ma, poiché delle tre ipotesi "Feppapi", "Ferrari", "Fessasi" la seconda è evidentemente la più probabile, può concludersi ritenendo 7462 = r. In tal modo si pongono dei punti di riferimento abbastanza attendibili per la ricostruzione del cifrario ed è agevole proseguire il lavoro di decrittazione, deducendo anzitutto, in base al calcolo delle frequenze, il significato delle parole vuote più importanti.

Per i repertorî paginati e sempre non sopracifrati si procede in maniera analoga, tenendo conto non soltanto delle frequenze dei singoli gruppi cifranti, ma anche di quelle complessive dei gruppi contenuti in ogni pagina.

Molto più difficile è la decrittazione dei repertorî intervertiti e non sopracifrati per la mancanza di qualsiasi ordine nella disposizione dei gruppi cifranti corrispondenti alle voci chiare; il lavoro, generalmente, può avere pratico risultato soltanto ove ricorra qualche circostanza favorevole o soccorra un'intuizione particolarmente felice, e comunque disponendo di un adeguato numero di messaggi cifrati.

Il problema della decrittazione dei sistemi a codice (intervertito o non) sopracifrato è di estrema complessità ed è anche piuttosto lungo descrivere casi particolari per farsi una idea. Comunque va detto che un tale problema è di fatto teoricamente impossibile se non vi sono sovrapposizioni nell'impiego del verme di sopracifratura. Se sovrapposizioni vi sono, si riesce ad eliminare la complicazione dovuta al verme lavorando sulle "differenze" fra i gruppi costituenti la differenza prima dei messaggi. Il "procedimento" usato è piuttosto complesso ed è praticamente impossibile descriverlo in questo lavoro.

Il problema è molto più complicato che nei codici di Cesare o comunque monoalfabetici. Si pensi che il codice di Vigenère è stato usato da vari eserciti resistendo ai vari "attacchi" che i crittoanalisti gli hanno dato per ben tre secoli. Nel 1863 un ufficiale prussiano, Kasiski, forza il codice di Vigenère con un metodo noto come test di Kasiski. Il test di Kasiski è basato sui seguenti punti:

- Il messaggio è sufficientemente lungo.
- Il primo passo è "trovare la lunghezza della parola chiave".
- Il secondo passo è "trovare le lettere della parola chiave".

Circa il primo passo iniziamo con il ricercare nel messaggio cifrato tutte le sequenze (cioè i gruppi) di tre o più lettere consecutive che si ripetono. E' molto probabile che a sequenze uguali del cifrato corrispondano sequenze

uguali del testo in chiaro. In ogni caso è questa una ipotesi di lavoro compatibile con la lunghezza del messaggio. Se così è vuol dire che le prime lettere di sequenze eguali sono state criptate con lo stesso alfabeto della tavola di Vigenère, analogamente le seconde, le terze, ... Da ciò segue che alle prime lettere delle sequenze uguali corrisponde la stessa lettera della parola chiave, analogamente alle seconde lettere e così via. Ma allora la distanza (= numero delle lettere) tra due sequenze uguali è un multiplo della lunghezza della parola chiave.

Quanto è lunga la parola chiave? Molto probabilmente la sua lunghezza è pari al M.C.D. delle distanze tra le sequenze uguali tra loro, che si ripetono.

Chiaramente una distanza "strana" tra due sequenze uguali, nel senso che non ha divisori comuni con le altre distanze, deve essere scartata; questo è il motivo per cui abbiamo detto "molto probabilmente la sua lunghezza ...". Ciò accade quando due sequenze uguali non corrispondono a due sequenze uguali del testo in chiaro.

Trovata la lunghezza d della parola chiave cerchiamo le lettere che la compongono. Notiamo che, nel testo cifrato, alla prima lettera, alla $(d+1)$-ma lettera, alla $(2d+1)$-ma lettera, ... corrisponde la stessa lettera della parola chiave e quindi tutte queste lettere sono state criptate con uno stesso codice di Cesare (cioè con una stessa riga del quadrato di Vigenère). Segue, ripetendo il ragionamento, che la seconda, la $(d+2)$-ma, la $(2d+2)$-ma riga sono anche loro crittografate usando uno stesso codice di Cesare. In definitiva ciascuna delle righe seguenti sono crittografate con una stessa lettera della parola chiave:

{I, $(d+1)$-ma, $(2d+1)$-ma, ...}

{II, $(d+2)$-ma, $(2d+2)$-ma, ...}

{III, $(d+3)$-ma, $(2d+3)$-ma, ...}

.....

.....

{d-ma, 2d-ma, 3d-ma, ...}

Le lettere di ognuno di questi insiemi sono state criptate con lo stesso codice di Cesare. Allora studiamo la frequenza delle lettere in ognuno di essi, con lo stesso metodo usato nei codici di Cesare. Scoperta una lettera, è noto il codice di Cesare usato, e quindi anche il nome dell'alfabeto (cioè la lettera che compare in testa), che ci dà la lettera della parola chiave. Allora il codice di Vigenère è forzato e quindi perde il suo interesse.

Dall'idea di Vigenère si ottiene un codice completamente sicuro, precisamente il codice di Vernam (1926). Questo è un codice del tipo di Vigenère nel quale si usa una parola chiave avente una lunghezza pari alla lunghezza del messaggio. Sembra che il telefono rosso, che fino a qualche anno fa esisteva tra la Casa Bianca e il Cremlino, facesse uso di un codice di Vernam per comunicare.

Per i sistemi crittografici, ben rari invero nei tempi moderni, in cui gli elementi del testo chiaro siano rappresentati con segni convenzionali diversi dalle lettere dell'alfabeto e dalle cifre arabe, la decrittazione si tenta in modi analoghi a quelli indicati per i sistemi a rappresentazione letterale o numerica, nei quali possono tramutarsi i sistemi suddetti, sostituendo con gruppi di lettere o di cifre i segni convenzionali speciali.

SOMMARIO.- Dalla crittografia, arte di costruire codici segreti, l'uomo ha costruito la crittoanalisi che è l'arte di scoprire il segreto dei codici. Nella crittoanalisi, intervengono metodi di tipo statistico e principalmente un modo di pensare logico-statistico. Molte di queste idee sono traducibili didatticamente, anche a livello Scuola Media inferiore come appare anche da un recente lavoro di L.Berardi, presentato al convegno dei nuclei didattici del C.N.R., tenutosi a L'Aquila nel 1989, nel quale si riferisce in relazione alla compiuta sperimentazione di alcune unità didattiche aventi come oggetto la crittografia.

RINGRAZIAMENTI

Gli Autori desiderano ringraziare vivamente l'Ammiraglio di squadra Giovanni MORO per gli utili consigli ed i colloqui avuti sugli argomenti trattati e per la cura con cui Egli ha riletto il nostro manoscritto, migliorandone la qualità.

BIBLIOGRAFIA

[1] C. Amè, Guerra segreta in Italia, Casini, Roma 1954.

[2] B. Baldessari, Aspetti probabilistici della crittografia, Atti 1o Simposio Nazionale su stato e prospettive della ricerca crittografica in Italia, Roma 30-31 Ottobre 1987.

[3] H. Becker e F.C. Piper, Cipher systems, Northwood Books, London 1982.

[4] L. Berardi, Some remarks about an electronic signature derived from a generalized RSA-code, J. of Information & Opti. Scien., in corso di stampa.

[5] L. Berardi e A. Beutelspacher, I buoni angeli custodi, ovvero i protettori di un messaggio, Archimede 2-3, 1988.

[6] L. Berardi e M. Di Fonso, Protezione delle informazioni su personal computer, Atti cit. in 2 .

[7] L. Berardi e F. Eugeni, Blocking sets e teoria dei giochi: origini e problematiche, (dedicato al Prof. Renato Nardini per il suo 70-mo compleanno), Atti Sem. Mat. Fis. Univ. Modena, 34, 1988.

[8] L. Berardi e F. Eugeni, Strutture geometriche, crittografia e sistemi di sicurezza richiedenti un quorum, Atti cit. in 2 .

[9] L. Berardi e B. Rizzi, Generalizziamo il codice RSA e la funzione di Eulero, Atti cit. in 2 .

[10] A. Beutelspacher, Encyphered Geometry: some applications of Geometry to Cryptography, Annals of Discrete Math., 37, 1988.

[11] A. Beutelspacher, La scuola elementare della teoria dei codici, Quad. n. 1, suppl. did., Sem. Geom. Comb. Univ. de L'Aquila, 1983.

[12] A. Beutelspacher, Kriptologie, Wieweg-Sohn, 1987.

[13] O. Brugia, S. Improta e W. Wolfowicz, Segretezza e autenticazione nelle moderne reti di telecomunicazioni, Rel. Int. 2B 63385, Fondazione Ugo Bordoni, Roma 1985.

[14] O. Brugia, Sistemi crittografici a chiave pubblica, Quad. Scuola Super. "G. Reiss Romoli" n. 4673, 1985.

[15] N. Cera e A. Maturo, Generazione di numeri pseudo-casuali per mezzo di relazioni di ricorrenza sui campi di Galois, Fac. di Arch. Università di Pescara, 1981.

[16] M. Cerasoli, F. Eugeni e M. Protasi, Matematica discreta, Casa Editrice Zanichelli, in corso di stampa.

[17] Conti, Servizio segreto, De Luigi, Roma, 1945.

[18] D. E. Denning, Cryptography and data security, Addison-Wesley, 1983.

[19] W. Diffie e M.E. Hellman, New directions in cryptography, IEEE Trans. on Information Theory, vol. IT-22, n. 6, Nov. 1976.

[20] L. Gioppi, La crittografia diplomatica, militare e commerciale, Milano, 1897.

[21] M. Givierge, Course de cryptographie, Parigi, 1925.

[22] W. Heise e P. Quattrocchi, Informations und Codierung Theorie, Springer Verlag, Berlin-Heidelberg-New York-Tokio, 1983.

[23] M.E. Hellman, La crittografia a chiave pubblica, Le Scienze, 10, 1981.

[24] A. Ind, A history of modern espionage, Hodder & Stoughton, Londra, 1965.

[25] F.W. Kasiski, Die Geheimschriften und die Dechiffrirkunst, Berlino, 1863.

[26] A. Kerckhoffs, La cryptographie militaire, Parigi, 1883.

[27] A. Maturo, Messaggi cifrati per mezzo di numeri pseudo-casuali ottenuti a partire da successioni in algebre di supporto, Atti cit. in 2 .

[28] F. Mazzei, Sicurezza e riservatezza delle informazioni negli enti e nelle imprese, Franco Angeli Editore, Milano 1983.

[29] W.W. Peterson e E.J. Weldon, Error correcting codes, MIT Press, Cambridge, Massachussets, 1980.

[30] R.L. Rivest, A. Shamir e L. Adelman, A method of obtaining digital signatures and public key cryptosystem, Comm. of the ACM, vol. 21, n. 2, Febbraio 1978.

[31] A. Rizzi, On the sum (Modulo m) of two statistical variables, Boll. Union. Mat. Ital., 13, 1976.

[32] A. Rizzi, Generazione di simboli binari pseudo-casuali per mezzo di relazioni ricorrenti su campi di Galois, Statistica, 1982.

[33] A. Rizzi, Aspetti logici dell'analisi dei dati, Dipart. di Stat., Prob. e Stat. Appl. Univ. Roma "La Sapienza", n. 1, 1984.

[34] A. Rizzi, Alcune considerazioni sulle problematiche delle banche di dati, Dipart. di Stat., Prob. e Stat. Appl. Univ. Roma, 5, 1984.

[35] A. Rizzi, Alcune analisi statistiche della lingua italiana, Dipart. di Stat., Prob. e Stat. Appl. Univ. Roma, n. 6, 1984.

[36] A. Rizzi, Alcune considerazioni sulla crittografia, Conferenza di apertura al 1o Simposio Italiano su stato e prospettiva sulla ricerca crittografica in Italia, Atti cit. in 2.

[37] L. Sacco (Gen.), Manuale di crittografia, Litografia Covi, Roma 1947. Ristampa anastatica a cura della Scuola Superiore "G. Reiss Romoli", L'Aquila 1986.

[38] W. Schellenberg, Le memorie, Longanesi, 1960.

[39] R. Seth, Secret servants. The true story of Japanese espionage, Paperback, New York, 1968.

[40] A. Sgarro, Crittografia, Franco Muzzico Ed., Padova 1986.

[41] A. Shamir, How to share a secret, Comm. ACM, vol. 22, 1979.

[42] C.E. Shannon, A mathematical theory of communications, BSTJ 27, 1984.

[43] C.E. Shannon, Communication theory of secret systems, BSTJ 28, 1984.

[44] G. Tallini, Le geometrie di Galois e le loro applicazioni alla statistica e alla teoria della informazione, Rend. di Mat. Roma, 19, 1960.

[45] G. Tallini, Introduzione alla teoria dei Codici, Seminario Univ. L'Aquila, Febbraio 1979.

[46] P. Valerio, De la cryptographie, Parigi, 1893.

[47] G.S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphig communications, J. AIEE, 45, 1926.

[48] C.F. Vesin de' Romani, La cryptographie dévoilée, Parigi, 1857.

[49] M. Zanotti, Crittografia, Milano, 1928.

RATIO MATH. 1.
(1990), 39 - 50

Geometric Authentication Systems

Albrecht Beutelspacher(*) and Ute Rosenbaum(**)
(*) Universität Giessen-Mathematisches Institut-West Germany
(**) Siemens AG-Otto Hahn-Ring 6 - München-West Germany

1. INTRODUCTION

Suppose that Caesar wants to send a message M ("Ti amo") to Cleopatra. It is important that Cleopatra receives the message without any alteration. On the other hand, a bad guy X looks for his chance to alter M in his favour. In order to make the bad guy's life difficult, Caesar **authenticates** the message M.

For this, Caesar and Cleopatra have to agree on an authentication function f and a secret key K. The function f has M and K as its input, and the **authenticator** (also called **message authentication code**) f(M,K) as its output.

Now the procedure is as follows. Caesar sends the message M along with the authenticator A = f(M,K). Cleopatra receives a message, say M' and an "authenticator" A'. She computes $A^* = f(M',K)$. Only if $A^* = A'$ she accepts the received message as it stands.

What can a bad guy do? He wants to delete M and to insert another message M^* ("Ti odio"). Since he does not know the secret key K, he has no method to forge M, he can only try. But the bad guy's chances of success are not as bad as it may seem. Gilbert, MacWilliams and Sloane [9] have proved the following

Theorem. *Suppose that any authenticator has just one message. Assume furthermore that all messages and all keys occur with the same probability. Denote by k the total number of keys. Then, in any authentication system, the bad guy's chance of success is at least* $1/\sqrt{k}$.

An authentication system in which the bad guy's chance is exactly $1/\sqrt{k}$ is called **perfect.** In other words, in a perfect system the chance of success for a bad guy is as small as one can hope for. Gilbert, MacWilliams and Sloane [9] have constructed perfect authentication systems using projective planes (cf. sect. 2). These examples lack on the fact that there are very few messages (compared with the number of keys).

Apart from the above example, there are many other serious instances (in particular in the banking area), where authentication (and data integrity) is a necessity. So it is very important to have many good authentication systems available which enable the user to authenticate many messages. (See for instance [4] and [5].) The aim of this paper is to construct authentication systems, in particular those with 'many' messages. Some of our schemes are not perfect in a strong sense, but **essentially perfect.** By this we mean that the bad guy's chance of success is only $O(1/\sqrt{k})$. Our constructions are based on geometric structures, in particular finite projective spaces. Definitions and results can be found in [6] and [10].

In an other context, similar constructions can be found in [1]. Some of the results of this paper have shortly been described in [3].

2. Perfect systems allow only few messages

Throughout this paper we shall suppose that *any authenticator belongs to only one message.* Such systems are also called **cartesian.**

The aim of this section is to show that the example given in [8] is best possible in the sense that it has as many messages as possible.

The example (which we shall call **fundamental example**) is constructed as follows. Let P be a projective plane of order q. Fix a line l of P. Define the authentication system A as follows:

> The *messages* of A are the $q+1$ points on l,
>
> the *keys* of A are the q^2 points of P outside l,
>
> the *authenticator* belonging to message M and key K is the line of P through M and K.

It is easily shown (cf. also sect. 3) that A is a perfect system.

Consider now an arbitrary perfect authentication system A. Then the

number k of keys of A is a square number, say $k = k_1^2$ for a natural number k_1. We recall the following result (see [9], p.412).

2.1 Lemma. *Assume that* A *is a perfect authentication scheme with exactly* $k = k_1^2$ *keys. Then*

(i) *Every authenticator belongs to exactly* k_1 *keys.*

(ii) *Every message is on exactly* k_1 *authenticators.*

(iii) *Any two authenticators which belong to distinct messages have exactly one key in common.*

Now we are able to prove the following

2.2 Theorem. *Let* A *be a perfect authentication system with* $k = k_1^2$ *keys. Denote the number of messages by* m *and the number of authenticators by* a. *Then* $m \leq k_1 + 1$ *with equality if and only if* A *is the fundamental example.*

Proof. We define the incidence structure S in the following way.

The *points* of S are the messages and the keys of A,

the *lines* of S are the authenticators of A and a "special line" l.

The *incidence rules* are as follows. Any message is on the line l. A message M is on the authenticator A if there is a key K such that A is the authenticator of M under the key K. Similarly, a key K is on the authenticator A if there is a message M such that A authenticates M under the key K.

Then any two lines intersect in exactly one common point. [By our general hypothesis, any authenticator meets l uniquely. If two authenticators belong to different messages, then, by 2.1(iii), they have exactly one key in common. If they belong to the same message (but different keys), then they intersect in a unique message.] In other words, S is the dual of a "linear space". By a fundamental theorem due to de Bruijn and Erdös [7], the number b of lines of S is at least as big as the number v of points; equality holds if and only if S is a projective plane.

In our situation, this reads $a + 1 = b \leq v = k + m$. Since $a = k_1 \cdot m$ and $k = k_1^2$ it follows $k_1 . m + 1 \leq \kappa_1^2 + m$, hence

$$(k_1 - 1) \cdot m \leq k_1^2 - 1$$

Therefore $m \leq k_1 + 1$ with equality if and only if S is a projective plane.

Remark. Recently, in [12] perfect autentication schemes have been classified from a combinatorial point of view.

3. Geometric authentication systems

Definition. Let $\mathbf{P} = PG(d,q)$ be the finite projective space of dimension d and order q. Denote by **M** and **K** sets of (certain) s- and t-dimensional subspaces, respectively, with the property that any element of **K** is skew to any element of **M**.

We define the **geometric authentication system** $A = A(K, M)$ as follows:

The *keys* of A are the elements of **K**;

the *messages* are the elements of **M**;

the *authenticator* belonging to the key **K** and the message **M** is the subspace $<K,M>$ generated by **K** and **M**.

So, any authenticator is a subspace of dimension $s + t + 1$. We always denote by A the set of all authenticators, by k the total number of keys and by m the number of messages.

The maximal possible number of keys in an authenticator is computed in the following

3.1 Lemma. *Let* A *be a subspace of dimension* $s+t+1$ *and let* M *be an s-dimensional subspace of* A. *Then the number* a_t *of t-dimensional subspaces in* A *which are skew to* M *is* $q^{(s+1)(t+1)}$.

Proof. We proceed by induction on t.

If $t = 0$, then $\mathbf{P} = PG(s+1,q)$, and a_t is the number of points outside the hyperplane M of A. Hence $a_t = q^{s+1}$.

Now we assume that $t > 0$ and that the assertion is correct for t-1.

First we compute the number b_{t-1} of (t-1)-dimensional subspaces which are skew to M. Since any hyperplane contains exactly a_{t-1} of them and no distinct hyperplanes through M intersect in a (t-1)-dimensional subspace which is skew to M, we have

$$b_{t-1} = a_{t-1}(q^{s+t+1-s-1} + ... + 1) = a_{t-1}(q^t + ... + 1).$$

On the other hand, fix a (t-1)-dimensional subspace W skew to M. Through W there are $q^{s+t+1-(t-1)-1} + ... + 1$ subspaces of dimension t, $q^s + ... + 1$ of which are not skew to M. It follows

$$(q^t + ... + 1)a_t = a_{t-1}(q^t + ... + 1)q^{s+1},$$

so

$$a_t = a_{t-1}n^{s+1} = q^{(s+1)(t+1)}.$$

Now we define a very big class of geometric authentication systems.

Definition. Let W be a w-dimensional subspace of $\mathbf{P} = PG(d,q)$. Let M be a set of s-dimensional subspaces of W and denote by K the set of all t-dimensional subspaces of P skew to W.

Denote by $\mathbf{A} = A(d,w,s,t;M) = A(K,M)$ the corresponding geometric authentication system.

We shall compute the parameters of A and study the case when A is perfect.

3.2 Lemma. *Let* $\mathbf{A} = A(d,w,s,t;M)$ *be the above defined authentication system.*

(a) *The number of keys of* A *equals*

$$k_t = \frac{q^{(t+1)(w+1)} \cdot \theta_{d-w-1} \cdot ... \cdot \theta_{d-w-t-1}}{\theta_t \cdot ... \cdot \theta_0}$$

where $\theta_r = q^r + ... + q + 1$ *is the number of points in an r-dimensional projective space of order* q.

(b) *Any authenticator contains just one message and precisely* $q^{(s+1)(t+1)}$ *keys.*

Proof. (a) We proceed by induction on t.

For t = 0 we get

k_0 = number of points in P not in W = $q^{w+1}\cdot(q^{d-w-1}+\ldots+1)$.

Suppose now that the assertion is true for $t \geq 0$ and $d \geq w+t+2$. Consider the incidence structure whose points are t-dimensional subspaces skew to W and whose blocks are the $(t+1)$-dimensional subspaces skew to W. Double counting yields

$$k_{t+1}\cdot(q^{t+1}+\ldots+1) = k_t\cdot(q^{d-t-1}+\ldots+q^{w+1}).$$

Thus, the assertion follows.

(b) follows from the definition of A and in view of 3.1.

3.3 Theorem. *Suppose that* $A = A(d,w,s,t;M)$ *is a perfect authentication system. Then any two elements of* M *are disjoint. Moreover,* $w = 2s+1$ *and* $d = w+t+1 = 2s+t+2$.

Proof. Let M and M^* be two elements of M intersecting each other in a subspace of dimension $i \geq -1$.

The bad guy knows M and the corresponding valid authenticator A, which is a $(s+t+1)$-dimensional subspace through M. In order to obtain the valid authenticator for M^* he has to try all $(s+t+1)$-dimensional subspaces which are generated by M^* and a t-dimensional subspace T of A skew to M. The number of these subspaces can be computed using 3.1 as $q^{(s+1)(t+1)}/q^{(i+1)(t+1)} = q^{(s-i)(t+1)}$.

If A is perfect, then, by definition

$$k_t = q^{2(s-i)(t+1)}.$$

On the other hand, by 3.2 we have

$$k_t = q^{(t+1)(w+1)}\cdot f,$$

where $f \geq 1$ is the number of t-dimensional subspaces in a (d-w-1)-dimensional space. Therefore,

$$q^{2(s-i)(t+1)} = q^{(t+1)(w+1)}\cdot f \geq q^{(t+1)(w+1)},$$

so

$$2(s-i)(t+1) \geq (t+1)(w+1),$$

or

$$2s\text{-}2i \geq w+1 \geq 2s\text{-}i+1,$$

since $<M,M^*>$ is a subspace of W.

It follows that $i \leq -1$, so $i = -1$, which means that M and M^* are skew.

Moreover,

$$2(s+1) = 2(s\text{-}i) \geq w+1 \geq 2s+1+1,$$

and so $w = 2s+1$.

Finally, from

$$q^{2(s+1)(t+1)} = q^{2(s-i)(t+1)} = q^{(t+1)(2s+2)} \cdot f$$

it follows that $f = 1$. This means that the number of t-dimensional subspaces in a (d-w-1)-dimensional space equals 1, which implies $t = d\text{-}w\text{-}1$.

Remark. A particular important case of the above theorem is obtained when $s = 0$. We get the following example. The *messages* are the points on a line l in a $(t+2)$-dimensional projective space and the *keys* are the t-dimensional subspaces skew to l. If $t = 0$, we obtain again the fundamental example.

Another example of a geometric authentication system is obtained as follows.

Definition. Let **P** be a d-dimensional finite projective space of order q and fix a hyperplane **H** of **P**. We define the geometric authentication system $\mathbf{A_1} = \mathbf{A_1}(t,d)$ as follows:

The *messages* are the t-dimensional subspaces of **H** ($t \leq d\text{-}1$),

the *keys* are the points of **P-H.**

3.4 Theorem. *The authentication system* $\mathbf{A_1}(t,d)$ *is essentially perfect if and only if* $d = 2t+2$; *it is perfect if and only if* $d = 2, t = 0$.

Proof. In any case, the number of keys is $k = q^d$. Assume that the bad guy wants to forge an authenticated message. For this, we may assume that he has a valid authenticator A (which is a $(t+1)$-dimensional subspace of **P**), which intersects **H** in the message M. He wants to substitute M by the message M^*,

which is also a t-dimensional subspace of **H**. Since almost all t-dimensional subspaces of H are skew to M, we may assume for the moment that M and M^* are disjoint.

In the worst case, the bad guy is clever. He observes that he has not to check all keys, but only those which are points of A-H. Since there are only q^{t+1} such points, his chance of success is at least $1/(q^{t+1})$.

If our system is essentially perfect, we have therefore

$$O(1/\sqrt{q^d}) = O(1/q^{t+1}),$$

that is $d = 2t+2$.

Suppose now $d = 2t+2 > 2$. Then there are messages $M^* \neq M$ which intersect M in a subspace W of dimension $i \geq 0$. Then any hypothetical (but reasonable) authenticator A^* of M^* intersects A in a subspace of dimension $i+1$, the bad guy's chance of success is

$$1/q^{t-i} > 1/q^{t+1}.$$

So, the system is essentially perfect, not perfect in the strong sense.

Remark. The system $A_1(0,2)$ is exactly the fundamental example.

4. Partial spreads

Throughout this section, we denote by $\mathbf{P} = PG(d,q)$ the finite projective space of dimension d and order q. A **partial t-spread** of **P** is a set S of mutually skew t-dimensional subspaces of **P**. A **t-spread** of **P** is a partial t-spread S with the property that every point of **P** lies on (precisely) one element of S. It is well known that **P** has a t-spread if and only if $t+1$ divides $d+1$. Any t-spread in $PG(2t+1,q)$ has $q^{t+1}+1$ elements; a partial t-spread S of $PG(2t+1,q)$ has **deficiency** $\delta = q^{t+1}+1-|S|$. The set of points of **P** not covered by the partial t-spread S is denoted by D(S).

4.1 Theorem. *Let* S *be a partial t-spread of* $\mathbf{P} = PG(2t+1,q)$ *with* $|S| \geq 2$. *Define the authentication system* $\mathbf{A} = \mathbf{A}(S)$ *as follows:*

The **messages** *are the elements of* S;

the **keys** *are the points in* D(S);

the **authenticator** *for the message* M *under the key* K *is the* (t + 1)*-dimensional subspace* <M,K>.

If the deficiency δ of S *equals*

$$\delta = q^t + ... + q + 1,$$

then the number of messages is q^{t+1}-$q(q^{t-1} + ... + 1)$, *the total number of keys is* $(q^t + ... + 1)^2$ *and* A(S) *is essentially perfect.*

Proof. The number k of keys equals $k = \delta(q^t + ... + 1) = (q^t + ... + 1)^2$. On the other hand, any (t + 1)-dimensional subspace through an element of S has exactly δ points in common with D(S). So, the bad guy can forge a message with probability $1/\delta = 1/(q^t + ... + q + 1)$.

So, the assertion follows.

Remarks.

1. The case t = 1 is of particular interest. In the essentially perfect case, we have q^2-q messages, but only $(q + 1)^2$ keys. One example of such a system is obtained if a regulus is removed from a "regular spread" (alias an "elliptic congruence").

2. The authentication systems A(S) are only perfect if the order of P is 2. (Assume that A(S) is perfect. Then, by 2.1 (iii) any two distinct authenticators must intersect in a unique key. This means that any two (t + 1)-dimensional subspaces through distinct elements of S intersect each other in at most one point of D(S). Therefore any line joining two points of D(S) intersects at most one element of S. In other words, any such line contains at most one point of P(S), where P(S) denotes the set of points on the elements of S.

So, for a fixed point $Q \in D(S)$ we have

$q^{2t} + ... + q + 1$ = number of lines through $Q \geq |P(S)| = q^{2t+1} + ... + 1 - |D(S)|$,

therefore

$$|D(S)| \geq q^{2t+1}.$$

On the other hand, any line connecting two points on different elements on S contains at most one point of D(S). Since any point of P lies on such a line, it follows

$$| D(S) | \leq (q^t + \ldots + 1)^2.$$

Together it follows

$$q^{2t+1} \leq | D(S) | \leq (q^t + \ldots + 1)^2.$$

Consequently,

$$q^{2t+1}(q-1)^2 \leq (q^{t+1}-1)^2,$$

$$q^{2t+1}(q^2-3q+1) \leq -2q^{t+1}+1 < 0,$$

so $q = 2$.

5. The Lucky Bad Guy

In this last section we address the problem of the lucky bad guy. So far we considered our systems under the unspoken hypothesis that the same key was used only once. In other words, we assumed that a change of keys takes place after every message. Now we would like to discuss a more realistic situation in which there are several messages authenticated with the same key. Is there any security, if the bad guy knows two or more valid authenticators belonging to the same key? For most of the above discussed authentication schemes the answer is "no". (This is called a spoofing attack of order s [11]). For most of the above discussed authentication schemes the answer is "no". For instance, in the fundamental example two different authenticators determine the key uniquely.

Let us consider authentication systems in which all messages have the same number n of authenticators. Then the bad guy's chance of success is at least 1/n, since for his favourite message he simply has to choose one of the n authenticators at random. What we would like to have is that after the observation of s messages beloinging to the same key the chances of the bad guy become not better.

Under the same conditions for authentication system in [9] Fåk has shown the following:

Theoreme. *Suppose that any authenticator has just one message. Assume furthermore that all messages and all keys occur with the same probability. Denote by* k *the total number of keys. Then, in any authentication system, the bud guy's chance of succes for a spoofing attack of order* s *is at least* $1/k^{1/(s+1)}$.

For $s = 1$ this is the bound proven in [9].

An authentication system **A** in which this theoretical bound is hold is said to be **s-fold perfect.** In a s-fold perfect authentication system given any $i, 0 \leq i \leq s$ messages $m_1, ..., m_i$ authenticated by the same key, the bud guy's chance of successfully falsificating any messages $m \neq m_1, ..., m_i$ is only $1/k^{1/(s+1)}$.

A is called essentially **s-fold perfect,** if knowledge of any s authenticators belonging to the same key gives the bad guy a chance of success of $O(1/k^{1/(s+1)})$ for falsificating an authenticator of a message choosen at random out of the remaing messages.

We conclude by presenting the following authentication systems.

5.1 Theorem. *Let* $\mathbf{P} = PG(s+1,q)$ *be the* $(s+1)$*-dimensional projective space of order* q. *Fix a point* P_0 of **P**. *Define the following authentication system* **A.**

Messages are the $q^s + ... + q + 1$ lines of **P** through P_0,

keys are the q^{s+1} hyperplanes of **P** not through P_0,

the **authenticator** belonging to the message l and the key H is the point $l \cap H$. In other words, the authenticators are precisely the points $\neq P_0$ of **P**.

Then **A** is essentially s-fold perfect.

Proof. Suppose that the bad guy has observed $t \leq s$ messages $m_1, ..., m_t$ with corresponding authenticators $a_1, ..., a_t$. then the bad guy knows that the key hyperplane H interscts $< m_1, ..., m_t >$ in $< a_1, ..., a_t >$, which is a hyperplane of $< m_1, ..., m_t >$. therefore he knows that a message in $< m_1, ..., m_t >$ has as its authenticator the point $m \cap < a_1, ..., a_t >$. So, for those $\leq q^{t+1} + ... + q + 1$ messages the chance of falsificating is 1, whereas for any of the other $\geq q^s + ... + q^t$ messages the probability is only 1/q.

So, the mean probability of guessing the correct authenticator is $O(1/k^{1/(s+1)})$.

Hence **A** is essentially s-fold perfect.

5.2 Theorem. *Let* $\mathbf{P} = PG(s+1, q)$ *be the* $(s+1)$*-dimensional projective space of order* q. *Fix a point* P_0 of **P**. *Define the following authentication system* **A**.

> **Messages** *are lines of* **P** *throught* P_0 *which are in general position, that is, no* t *of them are contained in a common* (t-1)*-dimensional subspace* $(t \leq s+1)$
>
> **keys** are the q^{s+1} hyperplanes of **P** not through P_0,
>
> the **authenticator** belonging to the message l and the key H is the point $l \cap H$. In other words, the authenticators are precisely the points $\neq P_0$ of **P**.

Then **A** *is* s*-fold perfect.*

Proof.. It is clear that under the present hypotheses the situation described above cannot occur.

References

[1] A. Beutelspacher: Partial spreads in finite projective spaces and partial designs. Math. Z. 145 (1975), 211-229.

[2] A. Beutelspacher: Enciphered Geometry. Some Applications of Geometry to Cryptography. Annals of Discrete Math. 37 (1988), 59-68.

[3] A. Beutelspacher: Perfect and essentially perfect authentication systems. Extended abstract. Advances in Cryptology: Proceedings of EUROCRYPT 87 (Lecture Notes in Computer Science 304), D. Chaum and W.L. Price, Eds., Springer-Verlag 1988, 167-170.

[4] A. Beutelspacher: Kryptologie. Vieweg-Verlag, Braunschweig und Wiesbaden 1987.

[5] D.W. Davies and W.L. Price: Security for Computer Networks. John Wiley & Sons, 1984.

[6] P. Dembowski: Finite Geometries, Springer-Verlag, 1968.

[7] N.G. de Bruijn and P. Erdös: On a combinatorial problem. Indag. Math. 10 (1948), 421-423.

[8] V. Fåk: Repeated use of des which Detected Deception, IEEE Transactions in Information Theory, vol. IT-25, no. 2, pp. 233-234, March 1979.

[9] E.N. Gilbert, F.J. MacWilliams, N.J.A. Sloane: Codes which detect deception. Bell. Syst. Tech. J. 53 (1974), 405-424.

[10] J.W.P. Hirschfeld: Geometries over finite fields. Clarendon Press, Oxford 1979.

[11] J. L. Massey: Cryptography - A Selective Survey, Proc of Int. Tirrenia Workshop on Digital Communications, Tirrenia, Italy, Sept. 1985.

[12] de Soete, M. Vedder, K. Walker, M. : Cartesian Authentication schemes. To appear in Procedings of EUROCRYPT'89.

RATIO MATH. 1.
(1990), 51 - 59

Qualche Riflessione sull' Utilità Attesa

Erio Castagnoli
Istituto di Metodi Quantitativi, Università L. Bocconi di Milano

1. Il criterio dell'utilità attesa è certamente il più noto ed il più utilizzato tra quelli che consentono di dare un'ordine di preferenza, in particolare per finalità di scelta, a situazioni aleatorie.

Pur essendo giudicato un modo estremamente naturale di esprimere giudizi di prefernza, il criterio dell'utilità attesa non è certamente esente da critiche. Tra le molte che gli sono state mosse, la prima, a mio modo di vedere, è che esso sembra richiedere una funzione d'utilità con significato cardinale sulla cui esistenza sono sempre stato, a dir poco, scettico.

Negli ultimi mesi mi sono reso conto che è possibile dare una reinterpretazione dell'utilità attesa che non richiede il sacrificio intellettuale dell'utilità cardinale e che presenta qualche altro vantaggio. Mi sembra che questa rilettura, seppur molto semplice, direi quasi ovvia, sia nuova. Mi rendo conto che l'impostazione che presento qui apre parecchi problemi sui quali non ho potuto riflettere appieno e con calma. Su di essi tornerò in un prossimo futuro ma i primi risultati e le considerazioni più semplici già mi paiono interessanti.

2. Mi limiterò a considerare variabili aleatorie (v.a.) con supporto limitato $A=[a,b]\subseteq R$: ciò sia per semplicità analitica sia perchè ciò è sufficiente per ogni problema di interesse concreto anche lontano.

La cosiddetta utilità attesa di una v.a. X a valori in A è semplicemente definita come:

$$M(u(X)) = \int_A u(z)\, dF_x(z)$$

essendo u la funzione d'utilità cardinale prescelta e F_x la funzione di ripartizione (f.r.) di X. Donendo essere u crescente (in senso debole) su A, l'utilità attesa esiste per ogni v.a.

Nel seguito supporrò u continua a destra: se così non fosse si potrebbe ridefinirla nei punti di discontinuità facendo in modo che $u(x) = u(x^+)$.

Essendo una funzione d'utilità cardinale univocamente determinata a meno di una trasformazione lineare crescente, si può sempre fare in modo che $u(a) = 0$ e $u(b) = 1$, con il che u appare formalmente una f.r. di una v.a. a valori in A.

Rammento che, se X e Y sono due v.a. indipendenti a valori in A con f.r. F_X e F_Y :

$$Prob(X \geq Y) = \int_A F_Y(z)\, dF_X(z)$$

3. La proprietà sopra richiamata consente immediatamente di rileggere l'utilità attesa di una v.a. Detta infatti V la v.a. di f.r. $u(u = F_V)$, si può senz'altro scrivere:

$$M(u(X)) = Prob(X \geq V)$$

cioè l'utilità attesa di una v.a. appare come la probabilità che essa dia un valore non inferiore a tale V.

L'ordinamento instaurato in un insieme di v.a. dal criterio dell'utilità attesa può dunque essere riletto così: si stabilisce una v.a. V di riferimento e si calcola la probabilità che ogni v.a. dell'insieme sia non inferiore a V; l'ordinamento di preferenza determinato dall'utilità attesa è allora quello stesso indotto da tali probabilità.

In concreto tutto ciò può essere, almeno provvisoriamente, inteso come segue.

Supponiamo di dover scegliere un guadagno aleatorio (lotteria) in un insieme assegnato. Prima di tutto stabiliamo una v.a. che, per es., in base alla nostra esperienza ed alla nostra psicologia, riteniamo "normale" per tipo di situazione che stiamo indagando (oppure "equa", oppure "desiderabile", oppure "pericolosa": quale sia l'aggettivo con il quale materialmente denotarla è, per ora, irrilevante: l'unica cosa che importa è che la intendiamo come pietra di paragone).

$$M(u(X)) = \int_A u(z)\, dF_x(z)$$

essendo u la funzione d'utilità cardinale prescelta e F_x la funzione di ripartizione (f.r.) di X. Donendo essere u crescente (in senso debole) su A, l'utilità attesa esiste per ogni v.a.

Nel seguito supporrò u continua a destra: se così non fosse si potrebbe ridefinirla nei punti di discontinuità facendo in modo che $u(x) = u(x^+)$.

Essendo una funzione d'utilità cardinale univocamente determinata a meno di una trasformazione lineare crescente, si può sempre fare in modo che $u(a) = 0$ e $u(b) = 1$, con il che u appare formalmente una f.r. di una v.a. a valori in A.

Rammento che, se X e Y sono due v.a. indipendenti a valori in A con f.r. F_x e F_Y :

$$Prob(X \geq Y) = \int_A F_Y(z)\, dF_X(z)$$

3. La proprietà sopra richiamata consente immediatamente di rileggere l'utilità attesa di una v.a. Detta infatti V la v.a. di f.r. $u(u = F_v)$, si può senz'altro scrivere:

$$M(u(X)) = Prob(X \geq V)$$

cioè l'utilità attesa di una v.a. appare come la probabilità che essa dia un valore non inferiore a tale V.

L'ordinamento instaurato in un insieme di v.a. dal criterio dell'utilità attesa può dunque essere riletto così: si stabilisce una v.a. V di riferimento e si calcola la probabilità che ogni v.a. dell'insieme sia non inferiore a V; l'ordinamento di preferenza determinato dall'utilità attesa è allora quello stesso indotto da tali probabilità.

In concreto tutto ciò può essere, almeno provvisoriamente, inteso come segue.

Supponiamo di dover scegliere un guadagno aleatorio (lotteria) in un insieme assegnato. Prima di tutto stabiliamo una v.a. che, per es., in base alla nostra esperienza ed alla nostra psicologia, riteniamo "normale" per tipo di situazione che stiamo indagando (oppure "equa", oppure "desiderabile", oppure "pericolosa": quale sia l'aggettivo con il quale materialmente denotarla è, per ora, irrilevante: l'unica cosa che importa è che la intendiamo come pietra di paragone).

Questa v.a. rappresenta la nostra visione dell'ambiente nel quale siamo chiamati ad operare una scelta. I vari guadagni aleatori sono semplicemente comparati tra loro attraverso la probabilità che diano un risultato non peggiore di quello ottenuto dalla v.a. di riferimento. Per essere chiaro, non voglio sostenere che tale atteggiamento riscuota le mie incondizionate simpatie; sto solo affermando che il criterio dell'utilità attesa può essere riletto in tal senso, ovvero che la scelta di una funzione d'utilità equivale alla scelta di una v.a. di riferimento.

4. Ciò che precede consente di affermare che:

(i) L'utilità u(x) di un generico valore $x \in A$ è semplicemente:

$$u(x) = \text{Prob}(V \leq x)$$

cioè è la probabilità che, secondo la visione descritta da V, si sarebbe potuto ottenere un risultato inferiore o uguale a x.

Ciò mi sembra piuttosto sottoscrivibile.

Consideriamo un importo certo di denaro: Se mi si chede qualè il grado di soddisfazione che ne ritraggo, francamente non so che cosa rispondere: anzi ritengo proprio che, in questi termini, la domanda sia priva di senso.

Se invece colloco tale importo all'interno di un problema nel quale avrei potuto guadagnare un imprto aleatorio e sul quale manifesto un'opinione, mi sembra ragionevole rispondere che la mia soddisfazione è tanto più alta quanto più lo è la probabilità che avrei potuto guadagnare di meno, anzi, addirittura, mi sembra naturale misurare la soddisfazione attraverso tale probabilità.

(ii) La dominanza stocastica del prim'ordine può essere riletta in modo efficace .X domina Y se:

$$M(u(X)) \geq M(u(Y)) \text{ per ogni funzione crescente } u$$

cioè se:

$$\text{Prob}(X \geq V) \geq \text{Prob}(Y \geq V) \text{ per ogni v.a. } V$$

cioè se, qualunque sia la v.a. di riferimento, X ha miglior probabilità di Y di superare V.

Una qualunque dominanza stocastica può essere riletta negli stessi termini immaginando di restringere a una classe $\mathcal{V}$ le v.a. di riferimento:

$$\text{Prob}(X \geq V) \geq \text{Prob}(Y \geq V) \quad \forall V \in \mathcal{V}$$

(iii) Quando $u = F_v$ sia strettamente crescente e continua, il certo equivalente di una v.a.:

$$C(X) = u^{-1}(M(u(X)))$$

è il valore certo per il quale:

$$\text{Prob}(X \geq V) = \text{Prob}(C(X) \geq V)$$

cioè tale da avere la stessa probabilità di eccedere la v.a. di riferimento.

La cosa può farsi anche più in generale definendo:

$$u^{-1}(t) = \inf \{z: u(z) > t\}$$

(iv) Qualora V sia degenere nel solo valore k, il criterio dell'utilità attesa coincide con il criterio della probabilità di rovina:

$$M(u(X)) = \text{Prob}(X \geq k) = 1 - \text{Prob}(X < k)$$

5. Un punto critico della rilettura che propongo è ovviamente l'interpretazione da dare a V.

Mi sembra che le possibilità siano parecchie. Accenno a qualcuna.

(i) V potrebbe essere la v.a. che il decisore ritiene "equa", nel senso sostanziale che giudica indifferente acqistarla o cederla.

In questo senso può essere facilmente riletto l'esperimento mentale che conduce a fissare per punti una funzione d'utilità (e che ora può essere indifferentemente riletta come f.r.).

Ci si chiede qualè l'importo certo indifferente a una scommessa che, con probabilità 1/2, può far guadagnare a o b.

Detto x_1 tale importo, deve essere $u(x_1) = 1/2$. Si continua chiedendosi l'importo x_2 indifferente alla scommessa che, sempre con probabilità 1/2, può far guadagnare a o x_1: dev'essere $u(x_2) = 1/4$, e così via.

Nel seguito indicherò con a 1/2 b, a 1/2 x_1 le lotterie appena nominate.

Questa costruzione richede in sostanza l'indifferenza tra comprare e vendere una scommessa immaginando che, in ogni caso, vi sia un'asettica indifferenza tra importi certi e scommesse.

Ciò non sempre avviene in concreto, tanto più che un decisore affronta un problema o come compratore o come venditore e non da un punto di vista neutro.

La rilettura proposta consente di tener conto di tutto ciò. Infatti:

(ii) V potrebbe essere una v.a. "desiderabile" ovvero acquistabile.

Si può immaginare lo stesso esperimento mentale, indicando ora con x_1, x_2,, ecc... i prezzi massimi che si è disposti a pagare per acquistare le lotterie a 1/2 b, a 1/2 x_1, ecc...

(iii) V potrebbe essere una v.a. "indesiderabile" ovvero vendibile.

Ancora si può immaginare lo stesso esperimento mentale dove x_1, x_2, ecc... sono i prezzi minimi che si è disposti a ricevere per cedere le lotterie a 1/2 b, a 1/2 x_1, ecc...

In tal modo le decisioni di acquisto o di vendita di lotterie potrebbero condurre a ordinamenti anche molto diversi: psicologicamente si può immaginare un meccanismo di offerte di acquisto di vendita in busta chiusa per stabilire via via x_1, x_2, ecc...

In tal modo l'impostazione proposta consentirebbe di tener conto in modo semplice e naturale delle ovvie differenze che si riscontrano in concreto nei problemi nei quali si acquista o si cede rischio: per esempio comprare biglietti di lotterie e assicurarsi possono apparire inspiegabili se si accetta l'idea di utilità come livello di soddisfazione.

Consentirebbe anche di consacrare che il rischio può essere anche desiderabile: sicuramente lo è quando l'aletorietà non può che produrre miglioramenti rispetto alla situazione esistente.

(iv) V potrebbe essere una v.a. ritenuta "normale" o "di mercato".

In altre parole V potrebbe essere dotata di f.r. stimata o financo solo storicamente osservata nel mercato, ammesso che ve ne sia uno, nel quale si interviene (per es., rendimento dei titoli, quatazioni di valute estere, ecc...).

L'ipotesi di equilibrio metterebbe in moto le abituali teorie economiche per le quali i mercati sono, per loro natura, equi.

(v) V potrebbe essere la f.r. di un mercato parallelo o concorrenziale a quello nel quale si interviene. Con ciò si potrebbero stabilire "parità soggettive" tra mercati.

E' chiaro che, mutando l'intepretazione di V, mutano i valori di $M(u(X)) = Prob(X \geq V)$ e quindi, in definitiva, i giudizi: ciò mi sembra un pregio di flessibilità e di naturalezza che, d'altra parte, richiede un'attenta ed onesta riflessione del decisore sulla scelta di una particolare v.a. di riferimento.

Credo anche che, nella rilettura proposta, trovi una semplice collocazione l'"avversione al rischio". Essa non avrebbe più una posizione separata ma potrebbe, e dovrebbe, essere direttamente inglobata in V: la distribuzione di riferimento di un decisore prudente è diversa (in linea generale, nei casi (i) e (ii), puntualmente più elevata) da quella di un decisore imprudente.

6. Se consideriamo ora vettori aleatori, l'interpretazione data sopra presenta un ulteriore vantaggio. Supporrò ancora che i vettori aleatori abbiano un supporto limitato $A \subseteq R^n$ che si può sempre immaginare compatto.

E' noto che le seguenti proposizioni sono equivalenti per $n = 1$ ma non lo sono più per $n > 1$ (Marshall e Olkin (1979)):

(1) $Prob(X > Z) \geq Prob(Y > Z) \; \forall Z \in A$

(2) $Prob(X \leq Z) \leq Prob(Y \leq Z) \; \forall Z \in A$

(3) $M(u(X)) \geq M(u(Y))$ per ogni $u: A \to R$ crescente

(4) $g(X)$ domina secondo la dominanza stocastica del prim'ordine $g(Y)$ per ogni $g: A \to R$ crescente

(5) $Prob(X \in B) \geq Prob(Y \in B) \; \forall B \subseteq A$ con funzione indicatrice crescente.

(In quel che precede "crescente" sta per crescente debolmente componente per componente; essendo u e g definite su un compatto si può sempre fare in modo che assumano valori tra 0 e 1).

Per $n > 1$ valgono le seguenti implicazioni:

$$\Rightarrow 2$$
$$5 \Leftrightarrow 4 \Leftrightarrow 3$$
$$\Rightarrow 1$$

E' particolarmente fastidioso che, nè dalla (1) nè dalla (2), segua la diseguaglianza (3) sulle utilità attese.

Valgoni però i due seguenti teoremi che consentono facilmente di vedere dove stia la radice del problema.

TEOREMA - $Prob(X > Z) \geq Prob(Y > Z) \; \forall Z \in A$ se e solo se $M(u(X)) \geq M(u(Y))$ per ogni f.r. u.

TEOREMA - Prob $(X \leq Z) \leq$ Prob $(Y \leq Z)$ $\forall Z \in A$ se e solo se $M(u(X)) \leq M(u(Y))$ per ogni funzione u che sia il complemento a uno di una f.r. (funzione di sopravvivenza).

Per maggiore chiarezza torno al caso $n = 1$: qui l'utilità di un valore certo x poteva essere riletta come la probabilità di registrare un esito non migliore di x: brevemente la probabilità che x si lascia alle spalle.

Ovviamente si poteva anche intendere l'utilità come il complemento a uno della probabilità di ottenere, secondo la distribuzione di riferimento, un valore migliore di x, cioè come il complemento a uno della probabilità che x si trova di fronte:

$$u(X) = \text{Prob}\,(V \leq X) = 1 - \text{Prob}\,(V > X)$$

Per $n > 1$, Prob $(V \leq X)$ e Prob $(V > X)$ non hanno più somma uno.

Secondo la rilettura proposta, esistono dunque due possibilità per attribuire utilità ad un $x \in A$:

$$u_i(x) = \text{Prob}(V \leq x)$$

$$u_a(x) = 1 - \text{Prob}(V > x)$$

che potremmo chiamare "utilità all'indietro" e "utilità in avanti": rispettivamente le probabilità che, secondo la distribuzione di riferimento, x si lascia alle spalle e il complemento a uno di quella che x si trova di fronte (se si preferesce si potrebbe chiamare $u_i(X)$ "utilità di X" e $1 - u_a(x) = \text{Prob}(V > x)$ "disutilità" o "rammarico").

Risulta ovviamente:

$$M(u_i(X)) = \text{Prob}(V \geq x)$$

$$M(u_a(X)) = 1 - \text{Prob}(X > V) = \text{Prob}(X \not< V)$$

Prendendo u_i, in forza del primo teorema, si ha:

$$3 \Leftrightarrow 2$$

mentre prendendo u_a si ha:

$$3 \Leftrightarrow 1$$

e si riottengono delle equivalenze, come nel caso scalare, tra disuguaglianze sulle f.r. o di sopravvivenza) e tra disuguaglianze su utilità attese.

7. In breve, nel caso $n > 1$, la non equivalenza delle cinque proposizioni era da ascrivere al fatto che $\leq$ rappresenta una relazione d'ordine parziale e non totale come per $n = 1$: l'inconveniente si supera ragionando in termini di $\geq$ e $\not\geq$ anzichè in termini di $\geq$ e $<$.

In altre parole quando si ragiona su $u_i(x) = \text{Prob}(V \leq x)$, la probabilità che x si lascia alle spalle, non si distingue più tra $\text{Prob}(V > X)$ e Prob(V non confrontabile con X), cioè tra probabilità che x si trova di fronte o "ai fianchi".

Viceversa, quando si ragiona su $1\text{-}u_a(u) = \text{Prob}(V > X)$, la probabilità che x si trova di fronte, non si distingue tra $\text{Prob}(V \leq x)$ e Prob(V non confrontabile con X), cioè tra la probabilità che x si lascia alle spalle o ai fianchi. E' chiaro che queste sono le due probabilità estreme e che, tra esse, altre meritano di essere studiate.

E' altrettanto chiaro che, quando il vettore aleatorio X sia sintetizzato in una v.a. g(X) con g: $A \to R$ crescente (tipicamente attraverso un sistema di prezzi), si dota A di un ordine totale che affina l'ordine instaurato da $\leq$ e quindi la doppia possibilità sparisce. In questo senso si può rileggere la proposizione (4) che chiede che si abbia dominanza stocastica del prim'ordine qualunque sia la funzione g di sintesi: qualora si scelga effettivamente una ben precisa g si ritorna nel caso scalare.

Le possibilità intermendie alle quali accennavo sopra possono allora essere viste come l'aver fissato una classe G di funzioni di g di sintesi che si vogliona ritenere ammissibili.

Su questi particolari mi riprometto di tornare in dettaglio in un lavoro successivo.

8. In conclusione mi sembra interessante far rilevare come la reinterpretazione qui vista dell'utilità attesa mostri come essa possa ritenersi fondata su un giudizio ordinale ($X \geq V$) e che l'utilità di un importo certo di denaro possa essere considerata una misura cardinale (essendo una probabilità) di un tale giudizio.

Attraverso questa rilettura dell'utilità attesa si può facilmente saldare la dominanza stocastica con la dominanza in probabilità e, in partcolare, con la dominanza stocastica di ordine zero (Castagnoli (1985)).

Anche l'utilità S.S.B. di Fisliburn può farsi rientrare in questa lettura.

BIBLIOGRAFIA

E. CASTAGNOLI (1985): "Some remarks on Stochastic Dominance", Riv. Mat. Appl. Sci. Ec. Soc., 7, pagg. 15-28.

A.W. MARSHALL, I. OLKIN (1979): "Inequalities", Academic Press, New York.

M. OTTAVIANI (1973): "Sulla relazione fra una impostazione della teoria dell'utilità e la probabilità di fallimento", Dipartimento di Ricerca Operativa e Scienze Statistiche dell'Università di Pisa.

RATIO MATH. 1.
(1990), 61 - 72

Interpretazione dei risultati di un campionamento statistico con approccio bayesiano: simulazione su calcolatore. ($)

Vittorio Colagrande (*) **Giuseppe Di Biase (**)**

(*) Istituto Tecnico Commerciale "Galiani", via Ricci 22 - Chieti

(**) Dipartimento di Scienze e Storia dell'Arch., viale Pindaro 42 - Pescara

1. INTRODUZIONE AL PROBLEMA

Uno dei problemi dell'inferenza statistica è quello di valutare l'effettiva operatività di ipotesi relative a caratteristiche numeriche incognite di una popolazione a seguito di esperimenti.

L'impostazione bayesiana dell'inferenza permette di utilizzare tutta l'informazione riguardo alle ipotesi in quanto tiene conto di una distribuzione di probabilità iniziale delle ipotesi stesse ed ottiene, a seguito di prove sperimentali, delle distribuzioni che sono sintesi del supporto sperimentale e delle conoscenze preliminari.

Se accade, come nell'esempio qui realizzato, che la distribuzione "a posteriori" ottenuta dopo le prove sperimentali, è dello stesso "tipo" di quella assunta all'inizio, l'effetto dell' "apprendimento dall'esperienza" si riflette sulla distribuzione dei parametri.

($) Lavoro eseguito con il contributo del C.N.R. (contratto n. 88.00307.01)

Nel seguito si presenta la risoluzione di un problema concreto di *verifica di ipotesi* nel campo della sicurezza delle costruzioni, simulando su calcolatore le prove sperimentali e il conseguente aggiornamento della distribuzione iniziale del parametro considerato.

Uno dei parametri essenziali nella valutazione della sicurezza delle costruzioni è la *resistenza caratteristica* del calcestruzzo.

La definizione del valore di tale grandezza è, però, affetta da notevoli fonti di aleatorietà ed incertezza, riconducibili essenzialmente alle seguenti:

a) *aleatorietà intrinseca,* legata alla variabilità spaziale delle caratteristiche meccaniche del materiale per effetto di alterazioni casuali intervenute durante la fattura originaria ed all'incompletezza delle indagini conoscitive preliminari;

b) *incertezza legata agli errori di misura.*

2. LA METODOLOGIA BAYESIANA

Sia X il numero aleatorio rappresentante la resistenza caratteristica del calcestruzzo.

Si attribuisce ad X distribuzione normale con valor medio incognito e varianza assegnata σ^2.

Sia Θ il numero aleatorio rappresentante il valor medio (incognito) di X.

Le "ipotesi" di cui ci proponiamo di calcolare la probabilità in seguito ad osservazioni statistiche sperimentali sono eventi che dipendono dalla distribuzione di Θ.

Seguendo l'approccio bayesiano, si assume per Θ una *distribuzione iniziale* che viene *"aggiornata"* più volte in base ai risultati di prove di schiacciamento su carote di materiale prelevato dalla struttura; le misure ottenute da tali prove sono determinazioni del numero aleatorio X.

Uno dei vantaggi derivanti dalla metodologia inferenziale di tipo bayesiano è che la *distribuzione iniziale* può essere definita in base ad informazioni sia di tipo qualitativo (manufatti simili situati nelle vicinanze) sia di tipo quantitativo (dati di progetto o risultati di provini presi all'epoca del getto).

È possibile, in molti casi, assumere per Θ una *distribuzione iniziale normale* con valor medio μ_o e scarto quadratico medio σ_o :

$$N_{\mu_o, \sigma_o}(\vartheta)$$

Sia $\mathbf{x} = (x_1, x_2, ..., x_n)$ il campione osservato e $\bar{x}$ la media campionaria:

$$\bar{x} = \sum_{i=1}^{n} \frac{x_i}{n}$$

Si dimostra (cfr. [8], [9]) che:

- la funzione di verosimiglianza del campione $\mathbf{x}$ condizionata a Θ è una distribuzione normale con varianza σ^2/n :

$$\alpha(x_1, x_2, ..., x_n / \vartheta) = \prod_{i=1}^{n} N_{\vartheta, \sigma}(x_i) = N_{\vartheta, \sigma/\sqrt{n}}(\bar{x})$$

– la distribuzione di probabilità "aggiornata" di ϑ condizionata al campione $\mathbf{x}$ (utilizzando il Teorema di Bayes) è ancora normale:

(1) $$\beta(\vartheta / x_1, x_2, ..., x_n) = N\mu_n, \sigma_n(\vartheta).$$

I parametri di tale distribuzione sono dati da:

$$\mu_n = \frac{\frac{\mu_0}{\sigma_0^2} + \frac{\bar{x}n}{\sigma^2}}{\frac{1}{\sigma_0^2} + \frac{n}{\sigma^2}} \quad ; \qquad \frac{1}{\sigma_n^2} = \frac{1}{\sigma_0^2} + \frac{n}{\sigma^2}$$

3. OSSERVAZIONI

Con il metodo descritto, la distribuzione iniziale attribuita al valor medio della resistenza caratteristica di progetto viene controllata tramite i risultati dei prelievi effettuati sul manufatto.

Combinando i dati preesistenti, che possono essere anche informazioni qualitative esprimenti il *grado di fiducia* personale sul valore della resistenza, con i dati aggiuntivi di tipo quantitativo e statistico, si riesce ad ottenere una distribuzione di probabilità più attendibile.

Come è naturale, il peso da attribuire al dato $\bar{x}$ dell'esperimento nella

valutazione del valor medio μ_n è tanto maggiore quanto più tale dato è relativo ad un numero aleatorio con distribuzione di probabilità poco dispersa e, analogamente, quanto più precisa è la determinazione iniziale del valor medio μ_o di $N_{\mu_o,\sigma_o}(\vartheta)$, tanto maggiore è il "peso" da attribuirgli.

All'aumentare della numerosità del campione, i dati osservati influenzano i parametri della distribuzione finale di Θ in modo sempre più preponderante rispetto alla distribuzione iniziale; precisamente *al crescere di n* la distribuzione finale di Θ tende a concentrarsi intorno al valore μ_n, con la corrispondente varianza σ_{n2} tendende a zero.

In conclusione, tenendo conto della forma della curva normale e dell'osservazione precedente, la (1) rende possibile nella pratica interpretare il numero μ_n come sintesi dell'intera distribuzione di Θ, per cui il numero μ_n individuato può rappresentare il valore da attribuire con maggior fiducia alla resistenza specifica del calcestruzzo.

4. SIMULAZIONE SU CALCOLATORE

Inizialmente si attribuisce a Θ una distribuzione normale introducendo in input i valori dei parametri caratteristici.

In base alla distribuzione inziale assunta per Θ siamo praticamente certi che i valori di tale variabile sono compresi fra due numeri reali a e b.. Per la loro determinazione si rimanda a [8].

Nel fare la simulazione abbiamo fissato un intervallo $(c, d) \supset (a, b)$ in modo da aumentare l'incertezza iniziale.

Il modo di procedere è il seguente:
si sceglie una distribuzione normale "vera" di X con scarto quadratico medio σ assegnato in input e valor medio:

$$\vartheta_r = (c+d)/2 + r\,(d-c)/6 \qquad (2)$$

essendo r un numero pseudocasuale con distribuzione normale standardizzata (cfr. [5]) estratto dal calcolatore.

La (2) si giustifica tenendo presente che ϑ_r è un valore della variabile Θ e che quasi certamente quest'ultima è compresa nell'intervallo (c, d) (cfr. [8]).

In tal modo viene simulata una possibile distribuzione di probabilità della resistenza caratteristica del calcestruzzo.

Le prove di schiacciamento di carote vengono simulate mediante

estrazione al calcolatore di successioni di numeri pseudocasuali con *distribuzione normale* di parametri ϑ_r e σ.

Si possono considerare, ad esempio, (come prescrivono le normative tecniche) tre campioni di numerosità quattro.

5. UN TENTATIVO DI DECISIONE

Due maniere significative di utilizzare i risultati ottenuti, allo scopo di arrivare a *decisioni statistiche*, sono le seguenti:

- determinare un intervallo di confidenza $[\vartheta_1, \vartheta_2]$ di Θ, tale, cioè, che:

$$\text{Prob}\,(\vartheta_1 \leq \Theta \leq \vartheta_2) = \gamma$$

essendo γ un valore assegnato in $(0, 1)$.

In sostanza, si vogliono ottenere due valori entro cui il valor medio della resistenza caratteristica del calcestruzzo è compresa con un certo livello di probabilità γ.

- Fissare un *valore di collasso* T e determinare la

$$\text{Prob}(\vartheta \leq T)$$

6. APPENDICE

Si allega un esperimento effettuato sul calcolatore ed il programma scritto in linguaggio Turbo Pascal ver. 5.0

```
Introdurre i parametri della distribuzione normale
iniziale del valor medio della resistenza caratteristica
del calcestruzzo:

     valor medio              mo = 280
     scarto quadratico medio  so = 40


Scarto quadratico medio della resistenza caratteristica
del calcestruzzo: 25
```

estrazione al calcolatore di successioni di numeri pseudocasuali con *distribuzione normale* di parametri ϑ_r e σ.

Si possono considerare, ad esempio, (come prescrivono le normative tecniche) tre campioni di numerosità quattro.

5. UN TENTATIVO DI DECISIONE

Due maniere significative di utilizzare i risultati ottenuti, allo scopo di arrivare a *decisioni statistiche*, sono le seguenti:

- determinare un intervallo di confidenza $[\vartheta_1, \vartheta_2]$ di Θ, tale, cioè, che:

$$\text{Prob}\,(\vartheta_1 \leq \Theta \leq \vartheta_2) = \gamma$$

essendo γ un valore assegnato in $(0, 1)$.

In sostanza, si vogliono ottenere due valori entro cui il valor medio della resistenza caratteristica del calcestruzzo è compresa con un certo livello di probabilità γ.

- Fissare un *valore di collasso* T e determinare la

$$\text{Prob}(\vartheta \leq T)$$

6. APPENDICE

Si allega un esperimento effettuato sul calcolatore ed il programma scritto in linguaggio Turbo Pascal ver. 5.0

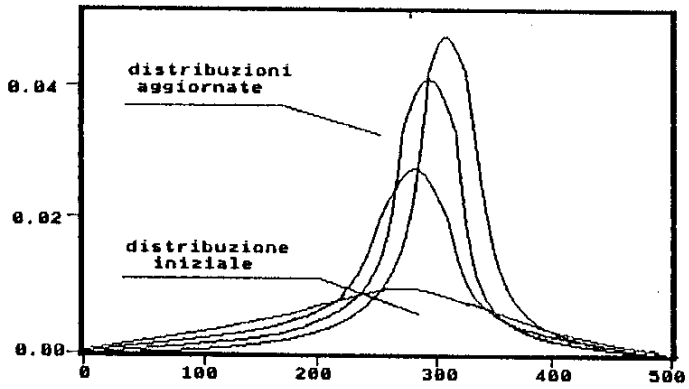
```
Introdurre i parametri della distribuzione normale
iniziale del valor medio della resistenza caratteristica
del calcestruzzo:

     valor medio              mo = 280
     scarto quadratico medio  su = 40

Scarto quadratico medio della resistenza caratteristica
del calcestruzzo: 25
```

```
Numerosità del campione  n = 4
   319   313   312   323

Numerosità del campione  n = 4
   317   328   318   317

Numerosità del campione  n = 4
   319   328   319   324

Introduci un livello di confidenza o un valore di collasso ?
Livello di confidenza : 0.95
```

Con i dati di input dell'esperimento, in seguito al campionamento, si ottengono i seguenti risultati:

	valor medio	scarto quadratico medio
1° campionamento	288	12
2° campionamento	303	9
3° campionamento	308	7

ed i seguenti grafici:



L'intervallo di confidenza ottenuto è il seguente:

$$\text{Prob}\ (303 \leq \Theta \leq 332) = 0.95$$

Program Inferenza_bayesiana;

```
{$N+}
{$IFDEF CPU87E+}
{$E-}
{$ELSE}
{$N+,E+}
{$ENDIF}

uses crt,graph,Integrat,radici;

const
  Num_Aleatorio = 'Resistenza Caratteristica del Calcestruzzo';
  Int = 100;
  rimp = 25;
  Interv = 3;
  xmin = 0;xmax = 20;ymin = -1;ymax = 1.5;
type
  reali = extended;

var
   a1,a2                          :Integer;
   a,b,sl,gamma,Ta,mr             :reali;
   m0,mN,s0,sN                    :reali;
   ALT,LARG                       :word;
   val_medio,scarto               :reali;
   sx,sy,k,incrx                  :reali;
   drivergraf,modograf,Errcodice  :Integer;
   fx,fy,hx,hy                    :Integer;
   flag                           :boolean;
   p                              :pointer;
   ch                             :char;


Function F(x,m,s:reali):reali;
begin
   F: = exp(-(x-m)*(x-m)/(2*s*s))/(s*sqrt(2*Pi));
end;


Procedure GRAFICA;
begin
   DriverGraf: = Detect;
   InitGraph(DriverGraf,ModoGraf,'');
   ErrCodice: = GraphResult;
   if Errcodicegrok then
     begin
       writeln('Errore grafica : ',GraphErrorMsg(Errcodice));
       writeln('Il programma abortisce...');Halt(1);
     end;
end;


Procedure PARAMETRI;
begin
   LARG: = GetMaxX;ALT: = GetMaxY;
   sx: = LARG/abs(xmax-xmin);
   sy: = ALT/abs(ymax-ymin);
   fx: = round(abs(xmin*sx));
   fy: = round(abs(ymin*sy));
   k: = 1;
   hx: = round(k*sx);hy: = round(k*sy);
   incrx: = 1/sx;
end;
```

```
Procedure ASSI;
var
 sinx,alty,desx,basy,i :integer;
 nu                    :string;
begin
   line(0,ALT-fy,LARG,ALT-fy);
   line(fx,0,fx,ALT);
   sinx:=fx;desx:=fx;
   alty:=fy;basy:=fy;
   i:=1;
   while (sinx0) or (desxARG) do
     begin
       sinx:=sinx-hx;
       desx:=desx+hx;
       line(sinx,ALT-fy-2,sinx,ALT-fy+2);
       line(desx,ALT-fy-2,desx,ALT-fy+2);
       str(25*i,nu);
       outtextxy(desx-7,ALT-fy+10,nu);
       i:=i+1
     end;
  i:=1;
  while  (alty0) or (basyALT) DO
     begin
       alty:=alty-hy;
       basy:=basy+hy;
       line(fx+3,ALT-alty,fx-3,ALT-alty);
       line(fx+3,ALT-basy,fx-3,ALT-basy);
       str(i/25:2:2,nu);
       outtextxy(fx+10,ALT-basy-3,nu);
       i:=i+1
     end;
end;

Procedure   TRACCIA_FUNZIONE(Val_medio,scarto:reali);
var
 px,py,pxprec,pyprec :integer;
 x,y                 :reali;
begin
   x:=xmin;
   pxprec:=round(x*sx/rimp)+fx;
   y:=rimp*F(x,Val_medio,scarto);
   pyprec:=round(y*sy)+fy;
   repeat
     y:=rimp*F(x,Val_medio,scarto);
     px:=round(x*sx/rimp)+fx;
     py:=round(y*sy)+fy;
     putpixel(px,ALT-py,15);
     line(pxprec,ALT-pyprec,px,ALT-py);
     x:=x+rimp*incrx;
     pxprec:=px;pyprec:=py;
  until xrimp*xmax
end;

Procedure   MEMORIZZA_GRAFICO(x1,y1,x2,y2:word;var punt:pointer);
var
   lunghezza :word;
begin
   lunghezza:=Imagesize(x1,y1,x2,y2);
   getmem(punt,lunghezza);
   getimage(x1,y1,x2,y2,punt^);
end;
```

```
Procedure    RICHIAMA_GRAFICO(x1,y1,x2,y2:word;var punt:pointer);
var
  lunghezza :word;
begin
   Putimage(x1,y1,punt^,1);
   lunghezza: = imagesize(x1,y1,x2,y2);
   freemem(punt,lunghezza);
   p: = nil
end;


Procedure    FIN_TESTO;
begin
   window(0,0,20,20);
   RestoreCrtMode;
end;


Function    RAN1: reali;
var
  t:reali;
begin
   t: = (a1*32749 + 3) mod 32749;
   a1: = trunc(t);
   Ran1: = abs(t/32749)
end;


Function    RAN2: reali;
var
   t:reali;
begin
   t: = (a2*10001 + 3) mod 17417;
   a2: = trunc(t);
   Ran2: = abs(t/17417)
end;


Function    SCELTARAN: reali;
var
   f:reali;
begin
   f: = Ran2;
   if f0.5 then SceltaRan: = Ran1
           else  begin Randomize;SceltaRan: = Random end
end;


Procedure    RULLA;
var
   i  :integer;
   sc:reali;
begin
   a1: = 1;a2: = 203;
   for i: = 1 to 10 do sc: = SCELTARAN
end;


Function    CASNORM:reali;
var
   somma,sc:reali;
   i              :integer;
begin
   somma: = 0;
   for i: = 1 to 12 do
     begin
        sc: = SCELTARAN;
```

```
        somma: = somma + sc
      end;
   CASNORM: = (somma-6)/12
end;


Procedure    PAR_INIZ;
var
  ch:char;
begin
    clrscr;
    gotoxy(1,3);
    write('Introdurre i parametri della distribuzione normale iniziale del');
    gotoxy(1,5);write('valor medio della ',Num_Aleatorio,' : ');
    gotoxy(10,8);write('valor medio          m0 = ');read(m0);
    gotoxy(10,10);write('scarto quadratico medio  s0 = ');read(s0);
    gotoxy(1,13);
    write('Scarto Quadratico Medio di ',Num_Aleatorio,' : ');
    read(si);
    repeat
      gotoxy(1,24);write('Vuole introdurre un "Livello di confidenza"  o ',
                         'un Valore di collasso ? (L/V) ');
      ch: = readkey;ch: = upcase(ch)
    until ch in ['L','V'];
    gotoxy(1,15);
    if ch = 'L'then begin
                      write('Livello di confidenza  : ');readln(gamma);flag: = true
                    end
              else  begin
                      write('Valore di collasso : ');readln(Ta);flag: = false
                    end;
    a: = m0-interv*s0;b: = m0 + interv*s0;
end;


Procedure    SCELTA;
var
    c,d,sc,cas :reali;
begin
    RULLA;
    sc: = SCELTARAN;c: = int*sc + a-int;
    sc: = SCELTARAN;d: = int*sc + b;
    cas: = CASNORM;
    mr: = (d-c)*cas/6 + (d + c)/2;
end;


Procedure    CAMPIONE;
var
    cas,x,media,va:reali;
    N,I                :integer;
begin
     clrscr;
     gotoxy(3,3);write('Numerosit del campione  N = ');readln(N);
     writeln;
     media: = 0;
     for I: = 1 to N do
       begin
          cas: = CASNORM;
          x: = si*cas + mr;
         write(x:8:2);
         delay(300);
         media: = media + x/N
       end;
    readln;
    sn: = 1/(s0*s0) + N/(si*si);
```

```
   mn: = (m0/(s0*s0) + N*media/(si*si))/sn;
   sn: = 1/sqrt(sn);
   m0: = mn;s0: = sn;
end;

Procedure   INTERVALLO;
var
   epsi:reall;
begin
   epsi: = sn*soluz4((gamma + 1)/2);gotoxy(10,10);
   write('Intervallo di confidenza  :  (',mn-epsi:3:3,' , ',mn + epsi:3:3,' )')
end;


Procedure   COLLASSO;
var
   Prob:reall;
begin
   Prob: = simpson(-50,(Ta-mn)/sn);
   gotoxy(5,10);writeln('La probabilità che la ',Num_Aleatorio);
   gotoxy(5,12);write('sia insufficiente  : ');write(Prob:3:3)
end;


Procedure   TASTO;
begin
   outtextxy(0,alt-10,' ESC per finire ');
   ch: = readkey;ch: = upcase(ch)
end;


{Programma  Principale}

begin
   clrscr;textcolor(15);
   PAR_INIZ;
   SCELTA;
   GRAFICA;
   PARAMETRI;
   ASSI;
   TRACCIA_FUNZIONE(m0,s0);
   readln;
   repeat
     MEMORIZZA_GRAFICO(0,0,larg,alt,p);
     FIN_TESTO;
     CAMPIONE;
     GRAFICA;
     RICHIAMA_GRAFICO(0,0,larg,alt,p);
     TRACCIA_FUNZIONE(m0,s0);
     TASTO
   until ch = chr(27);
   RestoreCrtMode;
   if flag then INTERVALLO else COLLASSO;
   repeat until keypressed
end.
```

Il programma utilizza due unit:
integrat, una cui function (chiamata simpson) è utilizzata nella procedura COLLASSO per calcolare con il metodo di Simpson l'integrale tra $-\infty$ e $\frac{T-\mu_n}{\sigma_n}$ della funzione:

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$$

radici, una cui function (chiamata soluz4) è utilizzata nella procedura COLLASSO per il calcolo approssimato delle radici dell' equazione che si ricava imponendo che $\text{Prob}(\vartheta_1 \leq \Theta \leq \vartheta_2) = \gamma$.

Di tali **unit** si omette, per brevità, il listato.

BIBLIOGRAFIA

[1] N. CERA - A. MATURO (1990) Analisi della bontà di alcuni generatori di numeri pseudocasuali per la cifratura di messaggi e la simulazione. Ratio Math. 2, in corso di stampa.

[2] M. CIAMPOLI (1989) Reability Evaluation of Existing Structures: Updating Techniques to account for Experimental Data. Atti della International conference on "Monitoring, Snerveillance and Predective Maintenance of Plants and Structures", Taormina, 16-18 Ottobre 1989, in corso di stampa.

[3] V. COLAGRANDE - G. DI BIASE (1990) Simulazione su calcolatore di alcuni esempi di applicazione del Teorema di Bayes, accettato sul Periodico di Matematiche, in corso di stampa.

[4] A.MATURO (1990) Numeri Pseudocasuali. Libreria dell'Università, Pescara.

[5] L.PICCINATO-N.PINTACUDA (1985) Probabilità e Statistica. Quaderni C.N.R.

[6] H.SCHILD (1988) Turbo Pascal 4.0. Programmazione avanzata. Mc.Graw-Hill.

[7] R.SCOZZAVAVA (1988) Probabilità soggettiva e grandi rischi. Archimede N.40.

[8] R.SCOZZAFAVA (1981) Introduzione alla probabilità e alla statistica. Ed. Veschi, Roma.

[9] R.SCOZZAFAVA (1989) La probabilità soggettiva e le sue applicazioni. Ed. Masson, Milano.

Ringraziamo sentitamente il Prof. Romano Scozzafava per l'incoraggiamento e gli utili suggerimenti fornitici.

Il programma utilizza due unit:
integrat, una cui function (chiamata simpson) è utilizzata nella procedura COLLASSO per calcolare con il metodo di Simpson l'integrale tra $-\infty$ e $\frac{T-\mu_n}{\sigma_n}$ della funzione:

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$$

radici, una cui function (chiamata soluz4) è utilizzata nella procedura COLLASSO per il calcolo approssimato delle radici dell' equazione che si ricava imponendo che $\text{Prob}(\vartheta_1 \leq \Theta \leq \vartheta_2) = \gamma$.

Di tali **unit** si omette, per brevità, il listato.

BIBLIOGRAFIA

[1] N. CERA - A. MATURO (1990) Analisi della bontà di alcuni generatori di numeri pseudocasuali per la cifratura di messaggi e la simulazione. Ratio Math. 2, in corso di stampa.

[2] M. CIAMPOLI (1989) Reability Evaluation of Existing Structures: Updating Techniques to account for Experimental Data. Atti della International conference on "Monitoring, Snerveillance and Predective Maintenance of Plants and Structures", Taormina, 16-18 Ottobre 1989, in corso di stampa.

[3] V. COLAGRANDE - G. DI BIASE (1990) Simulazione su calcolatore di alcuni esempi di applicazione del Teorema di Bayes, accettato sul Periodico di Matematiche, in corso di stampa.

[4] A.MATURO (1990) Numeri Pseudocasuali. Libreria dell'Università, Pescara.

[5] L.PICCINATO-N.PINTACUDA (1985) Probabilità e Statistica. Quaderni C.N.R.

[6] H.SCHILD (1988) Turbo Pascal 4.0. Programmazione avanzata. Mc.Graw-Hill.

[7] R.SCOZZAVAVA (1988) Probabilità soggettiva e grandi rischi. Archimede N.40.

[8] R.SCOZZAFAVA (1981) Introduzione alla probabilità e alla statistica. Ed. Veschi, Roma.

[9] R.SCOZZAFAVA (1989) La probabilità soggettiva e le sue applicazioni. Ed. Masson, Milano.

Ringraziamo sentitamente il Prof. Romano Scozzafava per l'incoraggiamento e gli utili suggerimenti fornitici.

RATIO MATH. 1.
(1990), 73 - 81

Studio analitico di un modello matematico per le strutture in muratura.

Giuseppe Di Biase* **- Antonio Maturo***
(*) Dipartimento di Scienze e Storia dell'Arch., viale Pindaro 42 - Pescara

1. Introduzione

In [1] e in [6] viene presentato un metodo per la determinazione dello stato di tensione e di deformazione nelle murature considerate come materiale non resistente a trazione e sottoposte ad azioni sismiche.

Il problema viene rappresentato da un modello matematico del tipo

$$M\delta'' + K\delta = -Ma \tag{1.0}$$

dove M e K sono matrici quadrate di ordine n, dette rispettivamente, matrici d'**inerzia** e di **rigidezza**, δ è un vettore di ordine n, detto degli spostamenti ed a è un vettore di ordine n, detto delle **accelerazioni del terreno**.

Le matrici M e K soddisfano alle seguenti condizioni:

(1) sono simmetriche;

(2) la M è definita positiva.

Il sistema (1.0) è risolto per mezzo del metodo delle differenze finite.

In questo lavoro mostriamo vari altri metodi per lo studio analitico del modello matematico rappresentato dal seguente sistema di equazioni differenziali:

$$M\delta'' + H\delta' + K\delta = -Ma \tag{1.1}$$

che costituisce una generalizzazione del modello studiato nei lavori citati in [1] e [6].

Nella (1.1) H è una matrice quadrata di ordine n, detta di **smorzamento.**

Per $H=0$ si ottiene la (1.0), che corrisponde all'ipotesi di assenza di smorzamento.

2. Metodo della funzione esponenziale.

Poniamo $y_1 = \delta$, $y_2 = \delta'$ e premoltiplichiamo ambo i membri della (1.1) per M^{-1}. Il sistema (1.1) si riduce al sistema del 1° ordine, in 2n incognite;

$$(2.1) \qquad \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}' + \begin{bmatrix} 0 & -I_n \\ M^{-1}K & M^{-1}H \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 0 \\ -a \end{bmatrix}$$

Poniamo:

$$Y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \quad , \quad A = \begin{bmatrix} 0 & -I_n \\ M^{-1}K & M^{-1}H \end{bmatrix}$$

$$B = \begin{bmatrix} 0 \\ -a \end{bmatrix} \quad , \quad Y_0 = \begin{bmatrix} \delta(0) \\ \delta'(0) \end{bmatrix}$$

e supponiamo che A sia non singolare.

Il sistema (2.1) assume la forma:

$$(2.2) \qquad Y' + AY = B$$

e quindi (cfr.[2]) la sua soluzione soddisfacente la condizione iniziale $Y(0) = Y_0$ è data dalla formula:

$$(2.3) \qquad Y = e^{-tA}Y_0 + e^{-tA}\int_0^t e^{uA}B(u)\,du$$

dove, per ogni numero reale t, per definizione è:

$$e^{tA} = \sum_{k=0}^{+\infty} \frac{(tA)^k}{k!} \tag{2.4}$$

Nella pratica, si presentano notevoli difficoltà nel calcolo della (2.4) a meno che la matrice A non soddisfi a particolari condizioni. Una di esse è, ad esempio, l'esistenza di 2n autovettori linearmente indipendenti di A. In tal caso, infatti, detta S la matrice che ha per colonne tali autovettori e posto $\Lambda = \text{diag}(\lambda_1, \lambda_2, ..., \lambda_{2n})$, indicato con $\text{diag}(\lambda_1, \lambda_2, ..., \lambda_{2n})$ la matrice diagonale dei corrispondenti autovalori, si ottiene:

$$A = S\ diag\,(\lambda_1, \lambda_2, \dots, \lambda_{2n})\ S^{-1} \tag{2.5}$$

e quindi, per ogni $k \in N_1$,

$$A^k = S\ diag\,(\lambda_1^k, \lambda_2^k, \dots, \lambda_{2n}^k)\ S^{-1} \tag{2.6}$$

Allora, tenuto conto della (2.4) e dello sviluppo in serie della funzione esponenziale, risulta:

$$e^{tA} = S\ diag\,(e^{t\lambda_1}, e^{t\lambda_2}, \dots, e^{t\lambda_{2n}})\ S^{-1} \tag{2.7}$$

La condizione dell'esistenza di 2n autovalori linearmente indipendenti di una matrice A è in genere dedotta dalla simmetria di A. Purtroppo, nel nostro problema, la A è simmetrica se e solo se sono verificate contemporaneamente le condizioni:

$$M^{-1}K = -I_n; \qquad M^{-1}H \text{ è simmetrica,} \tag{2.8}$$

ciò che, in generale, non avviene.

3. Metodo della trasformata di Laplace.

Consideriamo, per ogni funzione f definita in $[0, +\infty)$ e sommabile in ogni intervallo $[0,a]$, $\forall\ a \in \Re$ l'integrale:

$$(3.1) \qquad F(p) = \int_0^{+\infty} e^{-pt} f(t)\, dt$$

con p numero complesso.

Se esiste almeno un $p_o \in C$ tale che esiste finito l'integrale $F(p_o)$, la f(t) si dice L-trasformabile.

Allora si può verificare che (cfr.[9]) esiste un numero reale α, detto **ascissa di convergenza**, tale che l'integrale (3.1) esiste finito per $Re\,(p) > \alpha$ e non esiste finito per $Re\,(p) < \alpha$.

Inoltre la F(p) è una funzione olomorfa nel semipiano $Re(p) > \alpha$, detto **semipiano di convergenza.**

Se la f(t) è L-trasformabile allora la F(p), definita nel semipiano di convergenza, si dice trasformata di Laplace della f(t) e si indica con L[f(t)].

Supponiamo che, per le funzioni che consideriamo, siano soddisfatte le condizioni di esistenza della trasformata e della trasformata inversa. Dal sistema (1.1), prendendo le trasformate di ambo i membri, si ottiene:

$$(3.2) \qquad ML[\delta''] + HL[\delta'] + KL[\delta] = -ML(a),$$

da cui, per la nota formula

$$(3.3) \qquad L[f''(t)] = pL[f(t)] - f(0^+),$$

si ottiene:

$$(3.4) \quad M[p^2 L[\delta] - p\delta(0) - \delta'(0)] + H[pL[\delta] - \delta(0)] + KL(\delta) = -ML(a),$$

ossia

$$(3.5) \quad [p^2 M + pH + K]\, L[\delta] = (pM + H)\delta(0) + M\delta'(0) - ML[a].$$

Si ha quindi:

$$(3.6) \quad L[\delta] = (p^2 M + pH + K)^{-1} [(pM + H)\delta(0) + M\delta'(0) - ML(a)]$$

da cui si ottiene δ come trasformata inversa del 2° membro.

Una delle maggiori difficoltà nel calcolo della (3.6) consiste nella determinazione dell'inversa di $p^2 M + pH + H$.

Il problema si semplifica se vale la seguente condizione:

(I_o) $M^{-1}H$ e $M^{-1}K$ hanno uno stesso insieme di n autovettori linearmente indipendenti.

Ciò è certamente verificato nell'ipotesi considerata nei lavori [1] e [6], in cui $H=0$, di assenza di smorzamento e nell'ipotesi $H=hM$ (smorzamento proporzionale all'inerzia) o $H=rK$ (smorzamento proporzionale alla rigidezza).

Infatti, se vale la (I_o), detti $x_1, x_2, ..., x_n$ gli autovettori indipendenti delle matrici $M^{-1}H$ e $M^{-1}K$, indichiamo con h_i e μ_i i rispettivi autovalori delle due matrici associati ad uno stesso x_i. Se S è la matrice che ha per colonne gli x_i risulta:

$$M^{-1}H = S\ diag(h_1, h_2, \dots, h_n)\ S^{-1}$$

$$M^{-1}K = S\ diag(\mu_1, \mu_2, \dots, \mu_n)\ S^{-1}$$

e quindi

$$(p^2M + pH + K)^{-1} = [p^2 I_n + pS\ diag(h_1, h_2, \dots, h_n)\ S^{-1} + S\ diag(\mu_1, \mu_2, \dots, \mu_n)\ S^{-1}]^{-1} M^{-1},$$

da cui

$$(p^2M + pH + K)^{-1} = S\ diag\left[\frac{1}{p^2 + ph_1 + \mu_1}, \dots, \frac{1}{p^2 + ph_n + \mu_\nu}\right] S^{-1} M^{-1}$$

Posto allora:

$$\Lambda = diag\left[\frac{1}{p^2 + ph_1 + \mu_1}, \dots, \frac{1}{p^2 + ph_n + \mu_\nu}\right],$$

dalla (3.6) si ottiene:

$$(3.7)\ \delta = SL^{-1}[p\Lambda]S^{-1}\delta(0) + SL^{-1}[\Lambda]S^{-1}[M^{-1}H\delta(0) + \delta'(0)] - SL^{-1}[\Lambda S^{-1}L[a]]$$

Il calcolo di $L^{-1}[p\Lambda]$ e $L^{-1}[\Lambda]$ si riduce a quello noto delle espressioni, per $i=1,2,...,n$:

$$L^{-1}\left[\frac{p}{p^2 + p\,h_i + \mu_i}\right], \qquad L^{-1}\left[\frac{1}{p^2 + p\,h_i + \mu_i}\right].$$

Come per il metodo della funzione esponenziale può sorgere qualche difficoltà nella determinazione degli autovalori h_i e μ_i dovute al fatto che le matrici $M^{-1}H$ e $M^{-1}K$ non sono, in generale, simmetriche.

4. Metodo della bidiagonalizzazione

Le difficoltà che si presentano nei due metodi precedenti possono essere superate utilizzando la teoria della bidiagonalizzazione ed opportune trasformazioni di coordinate in $\Re^n$.

Poichè M è simmetrica e definita positiva, esiste una matrice V, non singolare di ordine n, tale che:

$$V^t M V = I_n, \tag{4.1}$$

dove V^t è la trasposta di V.

Infatti, siano $m_1, m_2, ..., m_n$ gli autovalori di M e $x_1, x_2, ..., x_n$ i corrispondenti autovettori, che si possono asssumere di norma unitaria e a due a due ortogonali.

La matrice Q che ha per colonne i vettori $x_1, x_2, ..., x_n$ è allora ortogonale.

Segue quindi che:

$$Q^t M Q = Q^{-1} M Q = \text{diag}\,(m_1, m_2, ..., m_n). \tag{4.2}$$

Posto:

$$D = diag\left(\frac{1}{\sqrt{m_1}}, \frac{1}{\sqrt{m_2}}, \ldots, \frac{1}{\sqrt{m_n}}\right), \tag{4.3}$$

segue che:

$$(QD)^t M (Q D) = I_n \tag{4.4}$$

e quindi, posto $V = Q D$, si ottiene la (4.1).

Premoltiplicando ambo i membri della (1.1) per V^t ed eseguendo il cambio di variabile:

$$\delta = V Y, \tag{4.5}$$

con $Y \in \Re^n$, la (1.2) diventa:

$$Y'' + A_1 Y' + A_2 Y = B, \tag{4.6}$$

con $A_1 = V^t H V$, $A_2 = V^t K V$, $B = - V^t M a$.

Le matrici A_1 e A_2 sono simmetriche e ciò facilita la soluzione della (4.6) con il metodo della funzione esponenziale o con quello della trasformata di Laplace.

Vogliamo però mostrare come, sotto condizioni abbastanza generali su A_1 e A_2, si può studiare il modello matematico in maniera molto semplice e da un punto di vista estremamente significativo.

Assumiamo la seguente ipotesi:

(J_o) A_1 e A_2 hanno lo stesso insieme di n autovettori linearmente indipendenti.

La (J_o) ammette, come casi particolari, molte situazioni di notevole importanza fisica, quali ad esempio le seguenti, con h, r, s, t numeri reali e p, q numeri interi:

(1) $H = 0$ (assenza di smorzamento);

(2) $H = h M$ (smorzamento proporzionale all'inerzia);

(3) $H = r K$ (smorzamento proporzionale alla rigidezza);

(4) $A_1 = s (A_2)^p$;

(5) $A_2 = t (A_1)^q$.

Ammesso che valga la (J_o), sia P una matrice che ha per colonne gli autovettori linearmente indipendenti di A_1 e A_2.

Poniamo:

$$D_1 = \text{diag}\,(h_1, h_2, ..., h_n), \quad D_2 = \text{diag}\,(\mu_1, \mu_2, ..., \mu_n). \tag{4.7}$$

Premoltiplicando la (4.6) per P^{-1} si ottiene:

$$(4.8) \qquad P^{-1} Y'' + P^{-1} A_1 Y' + P^{-1} A_2 Y = P^{-1} B.$$

Effettuiamo il cambiamento di variabile

$$(4.9) \qquad Y = P Z,$$

con $Z \in \Re^n$. Poichè:

$$(4.10) \qquad P^{-1} A_1 P = D_1, \qquad P^{-1} A_2 P = D_2,$$

dalla (4.8) si ottiene:

$$(4.11) \qquad Z'' + D_1 Z' + D_2 Z = P^{-1} B.$$

Il sistema (4.11) è formato da n equazioni differenziali ciascuna con una sola incognita. In forma estesa, posto

$$(4.12) \qquad P^{-1} B = \begin{bmatrix} b_1 \\ b_2 \\ . \\ . \\ b_n \end{bmatrix}$$

esso si scrive:

$$(4.13) \qquad \begin{cases} z''_1 + h_1 z'_1 + \mu_1 z_1 = b_1 \\ z''_2 + h_2 z'_2 + \mu_2 z_2 = b_2 \\ \quad \ldots\ldots \ldots\ldots \ldots\ldots \\ \quad \ldots\ldots \ldots\ldots \ldots\ldots \\ z''_n + h_n z'_n + \mu_n z_n = b_n. \end{cases}$$

Calcolato Z, dalle (4.6) e (4.9) si ottiene:

$$(4.14) \qquad \delta = V P Z.$$

Le (4.13) e (4.14) permettono di studiare facilmente il modo di variare delle soluzioni al variare del vettore $P^{-1} B$ dei termini noti o dei coefficienti h_i e μ_i.

Poichè

$$(4.15) \qquad P^{-1} B = - P^{-1} V^{-1} a,$$

se a ha come componenti delle funzioni periodiche moltiplicate per funzioni esponenziali è possibile applicare ad ogni singola equazione del sistema (4.13) la teoria delle oscillazioni forzate di un oscillatore semplice e quindi, in particolare, trovare le condizioni per la risonanza del sistema.

BIBLIOGRAFIA

[1] C.A.Anselmi,L.Fino: **Un modello matematico per le strutture in muratura** - VI Congresso ICOMOS, 1981

[2] T.M. Apostol: **Calcolo II** - Boringhieri, 1982

[3] J.H.Argyris: **Finite element linear and non linear analysis, methods and general purpose programs** - Stresa, 1975

[4] F.Ayres: **Matrici** - Etas, 1974

[5] D.M.Biggs: **Introduction to structural dynamics** - New York, 1964

[6] M.D'Anselmo, A.De Leonardis, A.Fusilli: **Strutture in muratura in campo dinamico** - Atti del Sesto Congresso Internazionale sulle murature in mattoni, Roma 1982

[7] G.Di Biase, A.Maturo: **Algoritmi e programmi per la risoluzione numerica di un modello matematico per le strutture in muratura** - Ratio Math 2, in corso di stampa

[8] F.Eugeni: **Alcune proprietà delle trasformazioni conformi** - Atti del Seminario Matematico e Fisico dell'Università di Modena, vol.II, 1967

[9] D.Greco: **Complementi di analisi** - Liguori, Napoli, 1967

[10] H.Haut: **Programmi di matematica e statistica in basic** - Jackson, 1982

[11] S.Lipschutz: **Algebra lineare** - Etas, 1975

[12] J.C.Mason: **Basic matrix methods** - Butterworths, 1984

[13] A.Maturo: **Metodi matematici per l'analisi statistica dei dati** - Montefeltro, Urbino, 1981

[14] A.Maturo: **Argomenti di matematica applicata, vol.I** - Montefeltro, Urbino, 1983

[15] E.Pessa, B.Rizzi: **Relazioni di ricorrenza ed equazioni differenziali** - Periodico di Matematiche n.2-3, 1987

[16] E.Pessa, B.Rizzi: **L'integrazione per serie delle equazioni differenziali ordinarie: aspetti e problemi** - Periodico di Matematiche n.4, 1986

[17] P.Pozzati: **Teoria e tecnica delle costruzioni** - Utet, 1982

[18] G. e M.Romano: **Sul calcolo delle strutture ad arco non resistenti a trazione** - Istituto di Scienza delle Costruzioni Facoltà Ingeneria, Napoli, 1979

[19] H.Sandy: **Discrete methods in some linear dynamic problems** - Symposium on Discrete methods in Ingeneering, Milano, 1974

[20] L.Santoboni: **La trasformata di Laplace in alcune operazioni finanziarie** - Quaderni di Statistica e Matematica Applicata Facoltà Economia e Commercio, Perugia, 1981

[21] C.B.Saw: **Finite element analysis of masonry walls on beams** - Symposium on Discrete methods in Engineering, Milano, 1974

[22] O.C.Zienkiewicz: **The finite elements method in engineering science** - London, 1971

RATIO MATH. 1.
(1990), 83 - 101

Un'Indagine sull'Uso dei Sistemi di Lettura (Codici a Barre) nel Settore del Commercio

Giovanni Ippoliti, Domenico Marconi, Giovanni Mataloni
Dipartimento di Scienze e Storia dell'Arch., viale Pindaro, 42 - Pescara

1. INTRODUZIONE

L'Era moderna può essere definita in molti modi: Era Atomica, Era dei Computers, Era Industriale, etc. ma, senza dubbio, l'appellativo più confacente al nostro *status vivendi* è quello di società dei consumi. Infatti nella maggior parte dei paesi industrializzati, ed anche in quelli in via di sviluppo, il benessere in espansione ha portato ad un generale incremento del tenore di vita tale da far concretizzare un uniforme livellamento in alto dell'economia familiare. Questo fenomeno, in ultima analisi, ha fatto sentire i suoi effetti *in primis* per ciò che concerne l'aspetto consumistico della società, il che ha comportato, già verso la fine degli anni sessanta e negli Stati Uniti per prima (e non poteva non essere il Paese consumistico per eccellenza ad essere il primo), la creazione di una vasta gamma di tecniche atte a migliorare la gestione industriale e commerciale, il controllo e la movimentazione, l'organizzazione e la movimentazione delle varie fasi nonché la razionalizzazione della movimentazione di cose e persone.

Una tra le più importanti di queste tecniche, se non la più importante, è rappresentata dai CODICI A BARRE.

2. ORIGINI E SVILUPPO DEI CODICI A BARRE

Il codice a barre vede la sua genesi nella necessità della lettura automatica dei caratteri rappresentati, attraverso un procedimento di lettura ottica e di decodifica elettronica.

Le origini del BAR-CODE risalgono al 1949. I primi studi sulla possibilità che un codice a caratteri stampati sulle confezioni dei prodotti di largo consumo possa essere decodificato da un sistema ottico, evitando così la creazione di lunghe file alle casse dei vari supermercati, risalgono al 1960.

L'elaborazione del primo codice adattabile ai prodotti di consumo, denominato UPC (Universal Products Coding) è dovuta agli americani Mc Enroe e Jones, nel 1971, ma le prime applicazioni si ebbero solo a partire dal 1973.

Il sistema Americano prese successivamente piede anche in Europa, attraverso la creazione di un sistema di identificazione e catalogazione dei vari prodotti, il cosiddetto CODICE EAN (European Article Number, o numero europeo dell'articolo). Questo codice sta a rappresentare in un certo senso la "carta d'identità" di ciascun prodotto, sia confezionato nel nostro Paese, sia importato. In seguito all'introduzione di tale sistema, avvenuta nel 1977, all'interno di ogni Paese aderente all'accordo, è stato poi creato un organo ufficiale con il compito precipuo di attribuire ai vari prodotti i relativi numeri di codice. Per quel che riguarda il mercato italiano, l'Istituto responsabile di tale ufficio, nato nel 1979, sull'iniziativa delle maggiori imprese italiane, è l'INDICOD che ha la sua sede in Milano.

Per dare un'idea della grande diffusione che i codici hanno avuto, si riportano alcune delle cifre più significative circa l'incremento del suo uso nei vari Paesi: negli USA nel 1983 la percentuale dei prodotti codificati era del 95%, in Germania dell'84%, in Belgio ed in Inghilterra del 72%, in Francia del 70%. In Italia il grande boom è avvenuto a partire dal 1973 con il 70%.

Il metodo di adesione al sistema Europeo è molto semplice e comporta il pagamento, da parte delle aziende che lo richiedono, di una quota proporzionale al fatturato dichiarato, per riceverne in cambio tutti i consigli e le agevolazioni per ciò che concerne l'uso appropriato dei codici sulle confezioni degli articoli. Per questo motivo viene realizzata una speciale pellicola: il *film master*. Nell'ambito nazionale i produttori di film master, che vengono realizzati mediante computers, sono in numero di sette: BANCOLINI, CPS, DATA FLASH, EURORIDEL, IPIERRE, SIGEM e CODEX.

3. APPLICAZIONI DEI CODICI A BARRE

Le applicazioni dei codici a barre sono innumerevoli. Il settore in cui sono stati applicati in maggior misura è quello del conteggio e della movimentazione magazzino e vendite che si realizza marcando gli articoli con il codice prodotto e tradotto in codice a barre sulla confezione che viene stampata in produzione. Al momento dell'ingresso nel magazzino alla vendita nei supermercati, il codice viene letto, decodificato ed inviato ad un elaboratore il quale provvede a movimentare il magazzino, ad effettuare eventuali elaborazioni relative a movimenti contabili e a far stampare alla stampante di cassa un elenco dettagliato degli articoli venduti con il relativo prezzo e quantità.

Viene inoltre applicato per la gestione ordini dei rappresentanti del catalogo di vendita. Il rappresentante viene dotato di un computer portatile con lettore ottico di codici a barre. Il sistema viene anche applicato per lo smistamento automatico dei prodotti sia nei magazzini che alla distribuzione. Infatti un lettore scanner a raggio laser legge il codice dell'articolo che si trova su di un nastro trasportatore principale. Il riconoscimento di questo attiva poi gli espulsori relativi ai vari nastri trasportatori secondari, collocati a 90° rispetto a quello principale.

Un ulteriore utilizzo del bar-code sta nell'applicazione per il riconoscimento del personale e per attivare gli ingressi ad aree riservate e/o effettuare il riconoscimento. Il personale, o il visitatore, viene dotato di una tessera plastificata con su stampato il codice a barre ed eventualmente la propria fotografia; a seconda del codice letto e memorizzato da un elaboratore, possono essere adottate tutte le procedure che si desiderano: aprire una o più barriere, prendere nota dell'ora di ingresso o di uscita del personale, stampare uno scontrino fiscale. Un esempio significativo su questa falsariga può essere rappresentato dalla gestione delle presenze del personale o del passaggio degli utenti di uno ski-lift. Nell'automazione industriale vengono etichettati i vari elementi da assemblare, in modo da poter essere riconosciuti per il montaggio automatico; oppure vengono targati i carrelli che trasportano materiali, onde rilevarli durante il percorso ed alle stazioni di montaggio.

Altre applicazioni prevedono la lettura dei dosimetri di radiazioni; la loro assegnazione al personale e la relativa analisi per *targare* le varie provette con i campioni da analizzare.

Altro caso è l'utilizzo pratico dei codici a barre sulle buste dello sviluppo fotografico al fine del riconoscimento del negozio dal quale sono state inviate le pellicole, facilitando così le fasi di smistamento e di invio delle foto,

3. APPLICAZIONI DEI CODICI A BARRE

Le applicazioni dei codici a barre sono innumerevoli. Il settore in cui sono stati applicati in maggior misura è quello del conteggio e della movimentazione magazzino e vendite che si realizza marcando gli articoli con il codice prodotto e tradotto in codice a barre sulla confezione che viene stampata in produzione. Al momento dell'ingresso nel magazzino alla vendita nei supermercati, il codice viene letto, decodificato ed inviato ad un elaboratore il quale provvede a movimentare il magazzino, ad effettuare eventuali elaborazioni relative a movimenti contabili e a far stampare alla stampante di cassa un elenco dettagliato degli articoli venduti con il relativo prezzo e quantità.

Viene inoltre applicato per la gestione ordini dei rappresentanti del catalogo di vendita. Il rappresentante viene dotato di un computer portatile con lettore ottico di codici a barre. Il sistema viene anche applicato per lo smistamento automatico dei prodotti sia nei magazzini che alla distribuzione. Infatti un lettore scanner a raggio laser legge il codice dell'articolo che si trova su di un nastro trasportatore principale. Il riconoscimento di questo attiva poi gli espulsori relativi ai vari nastri trasportatori secondari, collocati a 90° rispetto a quello principale.

Un ulteriore utilizzo del bar-code sta nell'applicazione per il riconoscimento del personale e per attivare gli ingressi ad aree riservate e/o effettuare il riconoscimento. Il personale, o il visitatore, viene dotato di una tessera plastificata con su stampato il codice a barre ed eventualmente la propria fotografia; a seconda del codice letto e memorizzato da un elaboratore, possono essere adottate tutte le procedure che si desiderano: aprire una o più barriere, prendere nota dell'ora di ingresso o di uscita del personale, stampare uno scontrino fiscale. Un esempio significativo su questa falsariga può essere rappresentato dalla gestione delle presenze del personale o del passaggio degli utenti di uno ski-lift. Nell'automazione industriale vengono etichettati i vari elementi da assemblare, in modo da poter essere riconosciuti per il montaggio automatico; oppure vengono targati i carrelli che trasportano materiali, onde rilevarli durante il percorso ed alle stazioni di montaggio.

Altre applicazioni prevedono la lettura dei dosimetri di radiazioni; la loro assegnazione al personale e la relativa analisi per *targare* le varie provette con i campioni da analizzare.

Altro caso è l'utilizzo pratico dei codici a barre sulle buste dello sviluppo fotografico al fine del riconoscimento del negozio dal quale sono state inviate le pellicole, facilitando così le fasi di smistamento e di invio delle foto,

fatturazione e contabilizzazione. Un'ennesima, ma non ultima, applicazione del bar-code può essere la gestione del noleggio delle videocassette, o dei libri e tante altre, praticamente tutte quelle dove occorre leggere e gestire un codice in modo automatico e molto più celere dell'uso della tastiera.

A testimonianza dell'importanza e della multifunzionalità di un tale tipo di codice, diamo qui un elenco di ulteriori applicazioni del codice a barre:

a) Sistemi di controllo d'accesso: ski-pass, parcheggi, presenze, ingressi riservati, gestione automatica delle paghe;

b) Costruzioni aeronautiche - meccaniche - elettroniche: riconoscimento delle attrezzature e dei materiali in fase di montaggio, gestione delle commesse di lavorazioni, collaudi e controllo di qualità;

c) Farmaceutica: riconoscimento, gestione, magazzinaggio, riordino;

d) Industrie in genere: movimentazioni e riconoscimento delle apparecchiature di trasporto per la gestione e l'ottimizzazione dei percorsi, controllo fasi di processo ed avanzamento in catene di montaggio, controllo ed avanzamento di lavori su isole, gestione scorte;

e) Magazzinaggio: riconoscimento e gestione;

f) Banche: controlli di sicurezza, gestione di documenti;

g) Centri trasfusionali e di analisi: analisi e identificazione;

h) Gestione contabile: riconoscimento, acquisizione, controllo dati, documenti;

i) Finanziaria: carte di credito, carte di acquisto;

l) Centri di raccolta agricoli: raccolta dei conferenti;

m) Editoria-giornali e riviste: controllo automatico distribuzione e resti;

n) Aeroporti: biglietterie, gestione, destinazione bagagli;

o) Campeggi: gestione ed automazione ingresso/uscita auto;

p) Uffici postali: smistamento automatico dei plichi;

q) Robotica: apparecchiature automatiche ed elettroniche, programmazione delle apparecchiature;

r) Ospedali: identificazione pazienti, registrazione analisi, gestione dati documentali, magazzini;

s) Biblioteche - videoteche - noleggio in genere: gestione giacenze, gestione prestiti e resi, gestione contabile.

4. VANTAGGI E COMPARAZIONE DEI CODICI A BARRE RISPETTO AD ALTRI SISTEMI.

L'adozione dei codici a barre porta con sè una serie di vantaggi che possiamo così schematizzare:

a) vantaggi per la produzione, visti come miglioramenti gestionali;

b) vantaggi per la distribuzione nel miglioramento della ricezione delle merci, delle consegne ai punti di vendita;

c) vantaggi nella movimentazione delle merci per l'eliminazione della marcatura dei singoli pezzi, vantaggi per l'impossibilità di errori umani nella fase di prezzatura. Inoltre non è possibile alcun caso di frode da parte degli acquirenti nel caso dello scambio di etichette, di rimarcatura di merci già esposte, nel caso di variazioni dei prezzi;

d) vantaggi nella gestione ed amministrazione delle attività commerciali grazie alla disponibilità di notizie dettagliate sulle vendite.

Il codice a barre può garantire la rilevazione dei fenomeni legati alle vendite con maggior celerità e precisione di qualsiasi altro metodo. Infatti:

1) rispetto all'operatore manuale da tastiera, i codici a barre sono vincenti in termini di semplicità, accuratezza e sicurezza;

2) rispetto al sistema a schede perforate, il codice a barre elimina i problemi di applicazione, distacco e collezionamento. Ha costi ridotti di apparecchiature e materiali ed elimina i problemi di sicurezza in quanto con il suo uso vengono di molto ridotte le perdite;

3) nei confronti del sistema magnetico, il bar-code ha un costo notevolmente inferiore, è di più semplice manipolazione ed è insensibile ad eventi di cancellazione dell'informazione, cosa questa addirittura indispensabile in condizioni di esercizio gravoso, quali campi magnetici e elettrici, ambienti e situazioni con apporto di materiali abrasivi e polverosi;

4) in confronto ai sistemi OCR, i lettori di codici a barre sono meno complicati, meno costosi, meno delicati e meno sensibili ad eventuali imperfezioni della stampa e, nelle applicazioni manuali, alla manualità dell'operatore essendo nei codici a barre l'informazione del carattere ridondante rispetto a tutta l'altezza della barra del codice.

5. IL CODICE DEI CODICI

Il principio di funzionamento di un codice a barre è apparentemente molto semplice in quanto non è altro che una sequenza di strisce nere e bianche che, una volta decodificate, corrispondono ad una successione di caratteri corrispondenti ad un'informazione ben precisa. In realtà, però, le variazioni possibili di questo schema sono molteplici ed in effetti esistono vari tipi di codifiche. Il motivo dell'esistenza di questa molteplicità risiede nel tipo di funzione che il codice deve assolvere. I codici possono essere di lunghezza fissa o variabile; sono dotati di barre di *start* e *stop* di modulo fisso, caratteristiche per ogni codice e posto all'inizio ed alla fine dello stesso. Il sistema di codificazione può inoltre essere dotato di *check digit*. Tale carattere viene anch'esso espresso in barre ed è posto generalmente alla fine delle barre di codifica e prima delle barre di stop. Il sistema che effettua la lettura e la decodifica, interpreta e calcola il check digit affinché soddisfi l'algoritmo di verifica del codice, per dare validità allo stesso. Il codice può generalmente anche essere letto in maniera bidirezionale. Ecco allora quali sono i codici a barre più usati in tutto il Globo:

CODIFICA INTERNAZIONALE								
CODICE	LUNGH.	TIPO	NC	BC	LM	LC	CBS	CD
Ean 13	fissa 13	numer.	10	7	2.6	2.1	si	o
Upc A	fissa 12	numer.	10	7	2.4	2.1	si	o
Ean 8	fissa 8	numer.	10	7	2.9	2.1	si	o
Codice 39	variabile	alfan.	43	9	4.56	3.9	si	o
Upc E	fissa 6	numer.	10	7	3.0	2.1	si	o
2/5 interl.	variabile	numer.	10	5	2.7	2.4	si	opt
2/5 indust.	variabile	numer.	10	5	4.4	3.9	no	opt
Code 11	variabile	numer.	11	5	2.85	2.4	si	o
Codabar	variabile	numer.	16	7	2.35	2.0	si	n
Msi	variabile	numer.	10	4	3.8	3.6	no	o

NC = numer. caratt. codificati
BC = bit per carattere
LM = lungh. media caratt. in mm
LC = lungh. caratt. in mm.
CBS = codifica in barre e spazi
CD = check digit
o = obbligatorio
opt = opzionale; n = non usato

5. IL CODICE DEI CODICI

Il principio di funzionamento di un codice a barre è apparentemente molto semplice in quanto non è altro che una sequenza di strisce nere e bianche che, una volta decodificate, corrispondono ad una successione di caratteri corrispondenti ad un'informazione ben precisa. In realtà, però, le variazioni possibili di questo schema sono molteplici ed in effetti esistono vari tipi di codifiche. Il motivo dell'esistenza di questa molteplicità risiede nel tipo di funzione che il codice deve assolvere. I codici possono essere di lunghezza fissa o variabile; sono dotati di barre di *start* e *stop* di modulo fisso, caratteristiche per ogni codice e posto all'inizio ed alla fine dello stesso. Il sistema di codificazione può inoltre essere dotato di *check digit*. Tale carattere viene anch'esso espresso in barre ed è posto generalmente alla fine delle barre di codifica e prima delle barre di stop. Il sistema che effettua la lettura e la decodifica, interpreta e calcola il check digit affinché soddisfi l'algoritmo di verifica del codice, per dare validità allo stesso. Il codice può generalmente anche essere letto in maniera bidirezionale. Ecco allora quali sono i codici a barre più usati in tutto il Globo:

CODIFICA INTERNAZIONALE								
CODICE	LUNGH.	TIPO	NC	BC	LM	LC	CBS	CD
Ean 13	fissa 13	numer.	10	7	2.6	2.1	si	o
Upc A	fissa 12	numer.	10	7	2.4	2.1	si	o
Ean 8	fissa 8	numer.	10	7	2.9	2.1	si	o
Codice 39	variabile	alfan.	43	9	4.56	3.9	si	o
Upc E	fissa 6	numer.	10	7	3.0	2.1	si	o
2/5 interl.	variabile	numer.	10	5	2.7	2.4	si	opt
2/5 indust.	variabile	numer.	10	5	4.4	3.9	no	opt
Code 11	variabile	numer.	11	5	2.85	2.4	si	o
Codabar	variabile	numer.	16	7	2.35	2.0	si	n
Msi	variabile	numer.	10	4	3.8	3.6	no	o

NC = numer. caratt. codificati
BC = bit per carattere
LM = lungh. media caratt. in mm
LC = lungh. caratt. in mm.
CBS = codifica in barre e spazi
CD = check digit
o = obbligatorio
opt = opzionale; n = non usato

5.1.1 Il codice 2/5

Il codice più semplice e di più largo uso, soprattutto in campo industriale, è il CODICE 2/5 (2 su 5); o, meglio, la famiglia dei 2/5, in quanto esistono diversi *sottocodici* di esso. I più usati sono l'*interleaved* e l'*industrial*; entrambi sono costituiti da 5 elementi, barre o spazi, di cui i sottili (1 unità), sono 4 ed i grossi (3 unità), sono 2. Gli elementi sottili rappresentano lo "0", mentre i grossi l'"1". Mentre nell'interleaved sia le barre che gli spazi contengono l'informazione, nell'industrial ogni barra ed ogni carattere sono separati da uno spazio unitario non significativo, in quanto non contiene alcuna informazione (vedere TAB. 1).

5.1.2 Il codice alfanumerico 39

Tale codice è simile al precedente ma più ricco di elementi per il fatto che in esso non si rappresentano soltanto i numeri, ma anche le lettere dell'alfabeto. Infatti, oltre ad avere codifica alfanumerica, possiede 7 caratteri speciali ed è, di conseguenza, più versatile degli altri codici. Consta di 9 elementi di cui 3 sono di doppia unità ed è costituito da 5 barre e 4 spazi. L'unico svantaggio di tale codice è la lunghezza; infatti ogni carattere per la sua stampa, richiede 6.6 mm. e l'insieme di tutti gli elementi, occupa lo spazio di ben 6 cm. (vedere TAB. 2).

5.1.3 Il codice UPC

Il codice UPC è in uso negli USA, in Canada e nel Regno Unito; si distingue in due diversi tipi:

a) UPC versione A

b) UPC versione E

Mantiene la stessa codifica dell'EAN (di cui tratteremo in seguito), salvo che per le barre laterali di controllo per l'UPC E (vedere TAB. 3 e TAB. 7).

5.1.4 Il codice 11

Questo codice è bidirezionale, numerico e di lunghezza variabile; è inoltre provvisto di *check digit*. La sua codifica prevede sia barre che spazi. Le barre e gli spazi unitari (sottili), valgono "0". Le barre e gli spazi di 2 unità (grossi), valgono "1". Esistono barre di *start* e di *stop* del codice. I vari caratteri sono separati da spazi unitari (vedere TAB. 4).

5.1.5 Il CODABAR

Si tratta di un codice bidirezionale sviluppato da Pitney Bowes. Oltre alle 10 cifre della numerazione, tale codice è costituito da altri 14 caratteri speciali, formati in parte da lettere ed in parte da simboli o segni di interpretazione. Anche per questo codice, come per il codice 39, lo svantaggio è la bassa intensità di informazione (5.5 mm. per carattere). Ogni elemento è separato dall'altro da uno spazio non significativo. Non è presente nel codice il *check digit*, in quanto ciascun carattere è dotato di un bit di controllo interno (vedere TAB. 5).

5.1.6 Il codice MSI

Anche in questo caso si tratta di un codice bidirezionale numerico; le barre di *start* corrispondono ad una barra grossa, le barre di *stop* a due barre sottili. Ogni cifra è rappresentata da 4 barre. Lo spazio che separa le barre non è significativo. Onde evitare errori, in quanto questo codice non è ridondante, è indispensabile dotarlo di *check digit*, meglio se doppio (vedere TAB. 6).

5.1.7 Il codice EAN

Il codice EAN (European Articles Numbering), è strutturato in due formati: l'EAN 13 e l'EAN 8, ma il primo è di gran lunga il più usato. All'inizio del 1977, dopo anni di lavoro e di studio a livello internazionale, i

rappresentanti delle industrie di beni di consumo e della distribuzione di 12 Paesi Europei (Repubblica Federale di Germania, Francia, Svizzera, Inghilterra, Austria, Svezia, Danimarca, Olanda, Belgio, Norvegia, Finlandia e Italia) sottoscrissero, a Bruxelles, un accordo per un sistema comune di identificazione automatica dei prodotti, attraverso codici e simboli. Questo sistema, denominato appunto EAN, era stato studiato per essere compatibile con quello Americano (UPC). Nell'EAN, ad ogni prodotto messo in commercio viene destinato un numero di codice che individua univocamente il prodotto su base nazionale. Tale numero, impresso dal produttore sulla confezione, ha due rappresentazioni; una decimale ed una binaria. La prima è costituita da una serie di barre scure su fondo chiaro, di larghezza variabile. Il codice attribuito ad ogni prodotto è unico ed è composto da 13 cifre e da una corrispondente rappresentazione grafica consistente in un simbolo a barre chiare, destinato alla lettura ottica. Infatti l'introduzione dei codici a barre è legata alla possibilità di decodificarlo per mezzo di un lettore ottico a luce laser (*scanner*). Il sistema EAN è biunivoco, il che significa che ogni prodotto viene identificato da un solo codice e che ad ogni codice corrisponde un solo prodotto, in tutti i Paesi dell'accordo. Il sistema in codice viene rappresentato per mezzo delle cifre da 0 a 9 ed è leggibile in entrambe le direzioni (*bidirezionalità*). Le 13 cifre del codice sono così destinate: le prime due indicano la nazione di produzione; esse sono attribuite dall'Associazione Internazionale. Eccone alcuni esempi:

TABELLA CODIFICA NAZIONALITA'

CODICE	*DEFINIZIONE*
00-09	UPC e CANADA
20-29	in store use
30-37	FRANCIA
40-43	GERMANIA
49	GIAPPONE
50	REGNO UNITO
54	BELGIO
57	DANIMARCA
64	FINLANDIA
70	NORVEGIA
73	SVEZIA
76	SVIZZERA
80-81-82-83	ITALIA

84	SPAGNA
87	OLANDA
90-91	AUSTRIA
93	AUSTRALIA

Il gruppo delle cinque cifre successive si riferiscono al produttore od al distributore e vengono attribuite dall'Istituto Internazionale; per l'Italia è l'INDICOD. Le cinque cifre seguenti, indicano il tipo di prodotto ed il relativo prezzo. Esse vengono attribuite dal produttore o dal distributore. L'ultima cifra è una cifra di controllo (*check digit*).

Ogni carattere occupa una striscia prestabilita costituita da 7 strisce più piccole (*moduli*) della stessa larghezza. Il codice è caratterizzato, lateralmente e centralmente, dalle barre di controllo, costituite rispettivamente da 3 e 5 moduli. In totale abbiamo 95 moduli, visto che i vari caratteri sono accostati senza segni intermedi. L'insieme di più moduli adiacenti, dello stesso colore, costituisce una barra.

La caratteristica del codice EAN è che ogni cifra risulta essere costituita da due barre scure e due chiare alternate, di grandezza diversa. Un altro segno particolare che contraddistingue l'EAN è che la codifica delle varie cifre varia sia nella parte destra che nella parte sinistra del codice. Infatti esso è diviso in due sezioni, delimitate alle estremità ed al centro da tre coppie di barre sottili. La prima sezione (sinistra) è codificata sia in codifica di tipo A che in quella di tipo B. La seconda sezione (destra) è codificata in codifica di tipo C.

Tali classi di codifiche (tipo A, B, C) non sono indipendenti. Infatti la classe A è complementare della classe C, cioè ogni barra chiara è trasformata in una barra scura e viceversa. Invece la classe B è simmetrica rispetto alla C.

Una peculiarità di tale disposizione è che ogni segno della classe A ha un numero dispari di moduli scuri, mentre le altre due classi ne possiedono un numero pari. Ciò si deve al fatto che lo scanner è in grado di riconoscere se la lettura avviene da destra o da sinistra dato che la prima cifra del codice è sempre scritta nella forma A (numero dispari di moduli scuri), mentre l'ultima è codificata nella forma C (numero pari di moduli scuri).

Il motivo per cui si hanno le tre diverse classi è dovuto alla necessità di rendere compatibile l'EAN con gli altri sistemi.

5.2 Calcolo del check digit per il codice EAN

Si scelgono due numeri interi (*pesi*) r ed s tali che r sia maggiore o uguale ad 1 ed s sia maggiore o uguale a 9. Ora, ad ogni confezione viene assegnato un numero di 13 cifre: b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12}, b_{13}. Le possibili combinazioni che si possono ottenere da tali 13 cifre sono 10^{13} visto che 10 sono i caratteri possibili per ogni cifra.

La condizione del codice EAN è che tra le 10^{13} combinazioni possibili, le ammissibili sono quelle tali che il numero:

$$x = r(b_1+b_3+b_5+b_7+b_9+b_{11})+s(b_2+b_4+b_6+b_8+b_{10}+b_{12})$$

(cioè il numero formato dalla somma del numero r moltiplicato per la sommatoria dei caratteri in posizione dispari, più il numero s moltiplicato per la sommatoria dei valori dei caratteri in posizione pari) sia multiplo di 10.

Sostituendo nel codice una cifra con un'altra, l'errore può essere rilevato. Se ad esempio sostituiamo la cifra b con d il numero x varierà assumendo un valore x' tale che $(x-x') = r(b-d)$. Se il numero r non è multiplo di 2 o di 5, la differenza (x-x') non può mai essere multiplo di 10 visto che tale differenza varia tra 0 e 9. Dunque (x-x') sarà multiplo di 10 a patto che (b_1-d_1) sia uguale a 2, 4, 5, 8; quindi l'errore di sostituzione di una cifra potrà essere rivelata a condizione che si scelgano i numeri r ed s tra i seguenti: 1, 3, 7, 9. Comunque di solito, per semplicità, vengono dati ad r ed s i valori: $r = 1$ ed $s = 3$.

Per la determinazione del *check digit* si procede come segue: si sommano i caratteri in posizione dispari ed il risultato ottenuto lo si moltiplica per $r = 1$. Si ripete poi lo stesso procedimento per i caratteri in posizione pari moltiplicandoli, però, per $s = 3$. Si sommano indi i totali delle due operazioni; se il risultato ottenuto è un multiplo di 10, il carattere di controllo (*check digit*) è proprio il numero 10, altrimenti sarà pari al numero p che si ottiene sottraendo dal numero 10 la cifra delle unità (vedere TAB. 7).

Esempio

$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8\ b_9\ b_{10}\ b_{11}\ b_{12}\ b_{13}$
4 9 0 1 7 8 0 0 7 4 1 7 4

somma $(b_1+b_3+b_5+b_7+b_9+b_{11})\cdot 1 = 19$
somma $(b_2+b_4+b_6+b_8+b_{10}+b_{12})\cdot 3 = 87$
somma totale = 106

CHECK DIGIT = (10-6) = 4

Le cifre b_1 e b_2 corrispondono al codice della SONY CORPORATION TOKYO. Le cifre b_8, b_9, b_{10}, b_{11} e b_{12} corrispondono al tipo di articolo ed al relativo costo: CASSETTA HF 46 TYPE 1 lire 4000. Il *check digit* non è in grado di rilevare l'errore quando si tratta dello scambio di due cifre consecutive. Se, ad esempio, la parola:

$$b_1\, b_2\, b_3\, b_4\, b_5\, b_6\, b_7\, b_8\, b_9\, b_{10}\, b_{11}\, b_{12}\, b_{13}$$

viene letta come

$$b_1\, b_2\, b_3\, b_4\, b_6\, b_5\, b_7\, b_8\, b_9\, b_{10}\, b_{11}\, b_{12}\, b_{13}$$

indicando con x" il numero così ottenuto, la differenza tra i numeri x ed x" soddisfa la relazione:

$$(x\text{-}x'') = (r\text{-}s)\cdot b_5 + (s\text{-}r)\cdot b_6 = (r\text{-}s)\cdot(b_5\text{-}b_6)\,.$$

Poiché r ed s sono sempre numeri dispari, la loro differenza sarà sempre un numero pari, quindi se $(b_5\text{-}b_6)$ è uguale a ± 5, la cifra di controllo sarà comunque un multiplo di 10 ed in tal maniera non è possibile rilevare l'errore commesso dallo *scanner*. Tale caso non ha comunque gravi conseguenze, data l'alta improbabilità che questo errore si verifichi, con l'uso di scanner elettronici e stampanti. Un metodo molto più semplice per il calcolo del *check digit* è quello usato nel caso del codice **ISBN (INTERNATIONAL STANDARD BOOK NUMBER)**, utilizzato per i libri e nelle biblioteche pubbliche. In questa codifica, il codice è costituito da 10 cifre ed è così composto:

b_1	$b_2\, b_3$	$b_4\, b_5\, b_6\, b_7\, b_8\, b_9$	b_{10}
cod. nazione	cod. editore	cod. libro	cod. contr.

La condizione di questo codice per il check digit è che il numero:

$$q = 10\cdot b_1 + 9\cdot b_2 + 8\cdot b_3 + 7\cdot b_4 + 6\cdot b_5 + 5\cdot b_6 + 4\cdot b_7 + 3\cdot b_8 + 2\cdot b_9 + 1\cdot b_{10}$$

sia un multiplo di 11. In questo caso non si presentano problemi relativi alla rilevazione di errori, visto che 11 è un numero primo.

6. QUALE CODICE ADOTTARE

Il codice EAN risulta ormai il più diffuso già come marcatura dei prodotti all'origine in quanto si è imposto come standard. Si può adottare la codifica già presente in EAN qualora la maggioranza dei prodotti giunga già codificata dato che questa è biunivoca a livello internazionale. Per i prodotti non codificati, come ad esempio per il riconoscimento dei prodotti da banco nei quali va codificato solo il prezzo da leggere in automatico, si mette il campo *codice produttore* a 0, il prezzo si codifica nel campo *codice prodotto*. Spetta poi al software dell'elaboratore che riceve i codici il riconoscimento e la gestione di tali accorgimenti.

In campo numerico il codice da preferire, che assomma i maggiori pregi, è senza dubbio il 2/5 Interleaved. Questo codice, oltre alla elevata compattazione dei caratteri, può essere stampato anche da stampanti ad aghi di non elevata qualità mantenendo una buona possibilità di lettura.

Mentre i codici EAN/UPC necessitano di una elevata qualità di stampa ed hanno una codifica ormai obsoleta, per quanto riguarda la codifica alfanumerica, il codice 39 risulta il più versatile e, di conseguenza, il più diffuso.

ALLEGATI

TAB. 1 CODIFICA DEI CODICI 2/5 INTERLEAVED E 2/5 INDUSTRIAL

Carattere	Barre/spazi
1	G S S S G
2	S G S S G
3	G G S S S
4	S S G S G
5	G S G S S
6	S G G S S
7	S S S G G
8	G S S G S
9	S G S G S
0	S S G G S
	B S B S
Barre di guardia sinistra	S S S S
Barre di guardia destra	G S S

S = 0 Elemento sottile (barra o spazio)
G = 1 Elemento grosso (barra o spazio)
B = barra - S = spazio

Carattere	Barre/spazi
0	00110
1	10001
2	01001
3	11000
4	00101
5	10100
6	01100
7	00011
8	10010
9	01010

TAB. 2 CODIFICA DEL CODICE 39

Carattere	BS BS BS BS B
0	000110100
1	100100001
2	001100001
3	101100000
4	000110001
5	100110000
6	001110000
7	000100101
8	100100100
9	001100100
A	100001001
B	001001001
C	101001000
D	000011001
E	100011000
F	001011000
G	000001101
H	100001100
I	001001100
J	000011100
K	100000011
L	001000011
M	101000010

N	000010011
O	100010010
P	001010010
Q	000000111
R	100000110
S	001000110
T	000010110
U	110000001
V	011000001
W	111000000
X	010010001
Y	110010000
Z	011010000
-	010000101
.	110000100
Spazio	011000100
$	010101000
/	010100010
+	010001010
%	000101010
*	010010100

TAB. 3 TIPO DI CODIFICA NEL CODICE UPC E

Check digit	
0	A A A B B B
1	A A B A B B
2	A A B B A B
3	A A B B B A
4	A B A A B B
5	A B B A A B
6	A B B B A A
7	A B A B A B
8	A B A B B A
9	A B B A B A

TAB. 4 CODIFICA DEL CODICE 11

Carattere	Codifica BS BS B
0	00001
1	10001
2	01001
3	11000
4	00101
5	10100
6	01100
7	00011
8	10010
9	10000
./-	01000
Barre di guardia laterali	00110

B = Barra - S = Spazio
Barra/spazio larghi = 1
Barra/spazio sottili = 0

TAB. 5 CODIFICA DEL CODICE CODABAR

Carattere	BS BS BS B
0	0000011
1	0000110
2	0001001
3	1100000
4	0010010
5	1000010
6	0100001
7	0100100
8	0110000
9	1001000
-	0001100
$	0011000
:	1000100
/	1010001
.	1010100

+	0010101
Barre di guardia laterali	0011010

B = Barra - S = Spazio

TAB. 6 CODIFICA DEL CODICE MSI

Carattere	Codifica binaria	Codice
0	USS USS USS USS	0000
1	USS USS USS DS	0001
2	USS USS DS USS	0010
3	USS USS DS DS	0011
4	USS DS USS USS	0100
5	USS DS USS DS	0101
6	USS DS DS USS	0110
7	USS DS DS DS	0111
8	DS USS USS USS	1000
9	DS USS USS DS	1001
Barra di guardia sx. DS		1
Barra di guardia dx. USS USS		00

U = Barra unitaria - D = Barra doppia
S = Spazio unitario
USS = 0 - DS = 1

TAB. 7 CODIFICA DEI CODICI EAN 13 - EAN 8 - UPC A - UPC E

Carattere	Gruppo A	Gruppo B	Gruppo C
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000

7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Spazio unitario = 0
Barra unitaria = 1

TIPO DI CODIFICA USATA (EAN - UPC A)

13esimo digit	7 6 5 4 3 2
0	A A A A A A
1	A A B A B B
2	A A B B A B
3	A A B B B A
4	A B A A B B
5	A B B A A B
6	A B B B A A
7	A B A B A B
8	A B A B B A
9	A B B A B A

Barre di guardia 101 (EAN - UPC)
Barre centrali 01010 (EAN - UPC A)
Barre di guardia dx. 010101 (UPC E)

CODICI DI IDENTIFIC. DI ALCUNE INDUSTRIE PRODUTTRICI

Industria	Codice
SONY	01780
CASIO	71850
PARMALAT	02580
DASH	01090
MARS ITALIA	11100
GALBANI	00430

RATIO MATH. 1.
(1990), 103 - 119

Numeri pseudocasuali ottenuti a partire da successioni in algebre finite su Z_m.

Antonio MATURO
Dipartimento di Scienze e Storia dell'Architettura, Viale Pindaro, 42 - Pescara

Introduzione

Lo studio comparato di vari metodi di generazione di numeri pseudocasuali mi ha spinto a prendere in considerazione alcune caratteristiche comuni ai vari generatori ed a studiare la possibilità di elaborare una teoria generale alla quale possano ricondursi gran parte dei vari metodi di generazione.

I vantaggi di una tale teoria sarebbero notevoli. Si potrebbero conoscere a priori una serie di proprietà matematiche e statistiche di una vasta classe G di generatori, individuandole per analogia e con procedimenti di generalizzazione e astrazione a partire da quelle dei generatori più noti. Questi ultimi potrebbero essere visti come elementi dell'insieme G aventi, oltre alle proprietà a priori, particolari caratteristiche.

In quest'ottica si potrebbero individuare, in G, nuovi generatori particolarmente significativi, ad esempio cercando la sottoclasse di quelli che godono di proprietà assegnate, in dipendenza di certi requisiti o vincoli che si vogliono siano rispettati nei procedimenti di simulazione.

Nel presente lavoro propongo un inquadramento della teoria generale, deducendo da essa criteri per lo studio di alcune sottoclassi di G.

2. Definizioni fondamentali e criteri per la costruzione di successioni di numeri pseudocasuali

Siano $(Z_m, +, \cdot)$ l'anello degli interi modulo m, $(S, \oplus, \otimes)$ un anello commutativo unitario e $\cdot$ una operazione esterna in S avente Z_m come dominio degli operatori.

Utilizziamo, in seguito, con abuso di notazione, i simboli Z_m e S per indicare non solo i sostegni dei corrispondenti anelli ma anche gli anelli stessi. Indichiamo con lettere latine gli elementi di S e con lettere greche quelli di Z_m.

Per semplicità di notazione, e quando ciò non dia luogo ad quivoci, sarà spesso utilizzata la notazione moltiplicativa usuale per le operazioni $\cdot$, $\cdot$ e $\otimes$ e quella additiva usuale per le $+$ e $\oplus$.

Allo scopo di costruire successioni di numeri pseudocasuali introduco le seguenti definizioni.

Definizione 2.1 Diciamo che S è *un'algebra di supporto di dimensione* n su Z_m, se sono soddisfatte le seguenti proprietà

(P1) S è, rispetto all'operazione esterna $\cdot$, un' algebra su Z_m;

(P2) esiste, in S, una base *B* formata da n elementi a cui appartiene l'unità u di S;

(P3) esiste, in S, un elemento x tale che gli elementi di B coincidono, tranne al più l'ordine, con le potenze $x^0 = u, x, x^2, ..., x^{n-1}$;

(P4) l'elemento x è invertibile rispetto a $\otimes$.

Dalla definizione 2.1 si deducono i seguenti

Corollario 2.1.1 Il numero di elementi di S è m^n.

Corollario 2.1.2. Gli elementi $\alpha \cdot u$, con $\alpha \in Z_m$, formano, rispetto a $\oplus$ e $\otimes$ un sottoanello di S isomorfo a Z_m.

Corollario 2.1.3. Se $n \geq 2$, allora $x \in B$ e $x \neq u$.

Definizione 2.2. Chiamiamo *funzione di supporto* una funzione $\psi : S \to Z_m$, dove S è un'algebra di supporto su Z.

In questo lavoro si assumerà l'ipotesi "lineare omogenea"

(LO) la ψ è un epimorfismo fra le strutture $(S, \oplus, *)$ e $(Z_m, +, \cdot)$, dove, al pari di $*$, anche $\cdot$ è vista come operazione esterna con dominio di operatori Z_m.

Sia $\alpha \in Z_m$. Allora α è una classe di residui modulo m e si può determinare il minimo intero non negativo $r(\alpha)$ tale che $r(\alpha) \in \alpha$:

Definizione 2.3. Chiamiamo *funzione ausiliaria di primo tipo,* la

$$\chi : \alpha \in Z_m \to r(\alpha)/m \in [0,1) \tag{2.1}$$

Sia h un intero positivo fissato. Data la h-pla $\alpha = (\alpha_1, \alpha_2, \ldots \alpha_h)$ di elementi di Z_m, indichiamo con $n(\underline{\alpha})$ il numero razionale che, nel sistema di numerazione in base m, si esprime nella forma $0 . r(\alpha_1) r(\alpha_2) \ldots r(\alpha_h)$

Definizione 2.4 Chiamiamo *funzione ausiliaria di secondo tipo* la

$$\omega : \underline{\alpha} \in (Z_m)^h \to n(\underline{\alpha}) \in [0,1) \tag{2.2}$$

La funzione $\chi o \psi$ fa corrispondere a successioni di elementi di S successioni di numeri razionali nell'intervallo [0,1). Esse, se soddisfano a opportuni tests statistici si possono ritenere pseudocasuali.

Se $\Psi = (\psi_1, \psi_2, \ldots, \psi_h)$ è una h-pla di funzioni di supporto,anche la ω o ψ fa corrispondere a successioni di elementi di S successioni di numeri razionali nell'intervallo [0,1).

Si può ritenere che l'uso della (2.1) è opportuno per m molto elevato (ad esempio dell'ordine di 10^{10}), mentre l'uso della (2.2), con h tale da rendere m^h abbastanza grande, lo è per m piccolo. Ad esempio può essere usata per $m = 2$ o per $m = 10$.

Notiamo che, per $h = 1$, la (2.2) si riduce alla (2.1).

Si potrebbero introdurre anche altri tipi di funzioni ausiliarie. In questo lavoro però ci si limiterà a considerare esclusivamente le χ e ω. Ciò non è restrittivo , in quanto i risultati ottenuti sono quasi tutti indipendenti dalla scelta della funzione ausiliaria.

3. Caratterizzazione delle algebre di supporto

Supponiamo che S sia un'algebra su Z_m soddisfacente le (P1) e (P2), con

base $B = \{x_0 = u, x_1, \ldots, x_{n-1}\}$.

Ogni $x \in S$ è esprimibile, in una sola maniera, nella forma:

$$x = \sum_{i=0}^{n-1} \alpha_i x_i \tag{3.1}$$

con opportuni $\alpha_i \in Z_m$.

Se x_r e x_t sono due elementi qualsiasi della base esistono, allora, in Z_m, degli elementi γ_{sti} tali che:

$$x_s \cdot x_t = \sum_{i=0}^{n-1} \gamma_{sti} x_i \tag{3.2}$$

Al variare di s,t,i si ottengono n^3 elementi γ_{sti}, detti *costanti di struttura dell'algebra,* dai quali è possibile determinare ogni prodotto $x \cdot y$ con x e y scelti arbitrariamente in S.

Infatti, se

$$x = \sum_{i=0}^{n-1} \alpha_i x_i \quad , \quad y = \sum_{i=0}^{n-1} \beta_i x_i \ , \tag{3.3}$$

risulta:

$$x \cdot y = \sum_{s=0}^{n-1} \alpha_s x_s \cdot \sum_{t=0}^{n-1} \beta_t x_t = \sum_{s=0}^{n-1} \sum_{t=0}^{n-1} \alpha_s x_s \beta_t x_t$$

e, per la (3.2),

$$x \cdot y = \sum_{i=0}^{n-1} \left(\sum_{s=0}^{n-1} \sum_{t=0}^{n-1} \alpha_s \gamma_{sti} \beta_t \right) x_i \tag{3.4}$$

Le grandezze γ_{sti} non sono indipendenti.

Le relazioni di associatività $(x_r x_s)x_t = x_r(x_s x_t)$ implicano che, per ogni scelta degli indici i, r, s, t, da 0 a n-1 valgono le formule

$$\sum_{j=0}^{n-1} \gamma_{rsj} \gamma_{jti} = \sum_{j=0}^{n-1} \gamma_{rji} \gamma_{stj} \ . \tag{3.5}$$

Le relazioni di commutatività $x_r \bullet x_s = x_s \bullet x_r$ implicano che, per ogni scelta di s,t,i, risulta:

$$\gamma_{sti} = \gamma_{tsi} \tag{3.6}$$

Il fatto che $x_o = u$ implica, infine, che, per ogni scelta di s e i, si ha:

$$\gamma_{osi} = \gamma_{soi} = \begin{cases} 0 & per\ s \neq i \\ 1 & per\ s = i \end{cases} \tag{3.7}$$

Le (3.5), (3.6),(3.7) caratterizzano la struttura moltiplicativa delle algebre soddisfacenti le (P1) e (P2).

Infatti, sia S un modulo su Z_m rispetto all'addizione $\oplus$ in S e all'operazione esterna $\cdot$ e sia $B = \{x_o, x_1, ..., x_{n-1}\}$ una sua base.

Si può dimostrare il seguente

Teorema 3.1 Assegnati gli elementi γ_{sti} di Z_m, con s,t,i appartenenti a $\{0, 1, ..., n-1\}$, soddisfacenti le (3.5), la (3.4) definisce, in S, una moltiplicazione $\Diamond$ tale che $(S, +, \Diamond, \cdot)$ è un algebra su Z_m.

Tale algebra è commutativa se vale la (3.6). E' unitaria con $x_o = u$ se vale la (3.7).

Supponiamo ora che l'algebra S sia di supporto e che gli elementi di B siano ordinati in modo che $x_s = x^s$ per $s \in \{0, 1, ..., n-1\}$. Per $n \geq 2$ è $x_1 = x$ e la (P3) equivale alle relazioni $x_1 \bullet x_s = x_{s+1}$, per $0 \leq s < n-1$, ossia alle:

$$\gamma_{1si} = \gamma_{s1i} = \begin{cases} 0 & per\ i \neq s+1 \\ 1 & per\ i = s+1 \end{cases} . \tag{3.8}$$

Poichè B è una base , esistono e sono univocamente determinati, degli elementi $\beta_o, \beta_1, ..., \beta_{n-1}$ di Z_m tali che:

$$x^n = \sum_{i=0}^{n-1} \beta_i x_i = \sum_{i=0}^{n-1} \beta_i x^i \tag{3.9}$$

La (3.9) si può scrivere

$$x\,(x^{n-1} - \sum_{i=1}^{n-1} \beta_i x^{i-1}) = \beta_0 u \tag{3.10}$$

da cui segue che, se β_0 è invertibile in Z_m, risulta:

$$x \cdot (\beta_0^{-1} x^{n-1} - \beta_0^{-1} \sum_{i=1}^{n-1} \beta_i x^{i-1}) = u . \tag{3.11}$$

La (P4) è allora soddisfatta se risulta

$$\beta_0 \text{ è invertibile in } Z_m. \tag{3.12}$$

Supponiamo che sia $n \geq 2$. Poichè $x = x_1$, ponendo $y = x_{n-1}$, dalla (3.4) si deduce

$$x^n = \sum_{i=0}^{n-1} \gamma_{1n-1i} x_i \tag{3.13}$$

e, poichè B è una base, seguono le uguaglianze

$$\beta_i = \gamma_{1\,n-1\,i}, \quad \forall i \in \{0, ..., n-1\} \tag{3.14}$$

$$x^{n+k} = \sum_{i=0}^{n-1} \beta_i x^{i+k} . \tag{3.15}$$

Poichè, per ogni coppia (x_s,x_t) di elementi di B, risulta $x_s \cdot x_t = x^s \cdot x^t = x^{s+t}$, la (3.15) implica, ragionando per ricorrenza su k, che le γ_{sti} sono tutte determinate a partire dagli n valori β_i.

Chiamiamo i β_i *costanti caratteristiche* dell'algebra di supporto S.

Osserviamo che dalla (3.15) si deduce la

$$x^k = \beta_0^{-1} x^{n+k} - \sum_{i=1}^{n-1} \beta_0^{-1} \beta_i x^{i+k} \tag{3.16}$$

particolarmente utile per k negativo, in quanto ci permette di ottenere, per ricorrenza, le potenze negative di x in funzione degli elementi della base.

4. Modelli isomorfi con sostegno Z_m^n

Consideriamo l'insieme $V = Z_m^n$ delle n-ple di elementi di Z_m. Introduciamo, in V, una addizione $\oplus$ e una moltiplicazione $\cdot$ di un elemento di V per un elemento di Z_m, ponendo, per $x = (\alpha_0, \alpha_1, ...\alpha_{n-1})$, $y = (\beta_0, \beta, ..., \beta_{n-1})$ in V e ω in Z_m,

$$x \oplus y = (\alpha_0+\beta_0, \alpha_1+\beta_1, ..., \alpha_{n-1}+\beta_{n-1}), \tag{4.1}$$

$$\omega \cdot x = (\omega \alpha_0, \omega \alpha_1, ..., \omega \alpha_{n-1}). \tag{4.2}$$

Rispetto alle operazioni così definite, V è un modulo su Z_m. Esso possiede basi formate da n elementi. Sia $A = \{y_0, y_1, ..., y_{n-1}\}$ una di tali basi.

Sia S una algebra su Z_m soddisfacente le (P1) e (P2) e sia $B = \{x_0, x_1, ..., x_{n-1}\}$ una sua base con $x_0 = u$.

L'applicazione

$$\varphi : \sum_{i=0}^{n-1} \alpha_i x_i \in S \rightarrow \sum_{i=0}^{n-1} \alpha_i y_i \in V \tag{4.3}$$

è un isomorfismo fra S, considerato con la sua struttura di Z_m- modulo, e V.

Si può introdurre, in V, una struttura moltiplicativa ponendo, per definizione,

$$x \cdot y = \varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y)), \quad \forall \ x, y \in V. \tag{4.4}$$

In tal modo V, rispetto alle operazioni ivi definite, soddisfa le (P1) e (P2).

Ciò può essere verificato, anche a prescindere dalle proprietà dell'isoformismo φ, dall'esame delle costanti dei struttura.

Infatti la (4.4) equivale all'affermazione che, se $x = \sum_{i=0}^{n-1} \alpha_i y_i$, $y = \sum_{i=0}^{n-1} \beta_i y_i$ e le γ_{sti} sono le costanti di struttura dell'algebra S, allora

$$x \cdot y = \sum_{i=0}^{n-1} \left(\sum_{s=0}^{n-1} \sum_{t=0}^{n-1} \alpha_s \gamma_{sti} \beta_t \right) y_i \tag{4.5}$$

Le (3.5), (3.6), (3.7), valide per le ipotesi su S, e il teorema 3.1 assicurano allora che V è un' algebra su Z_m soddisfacente le (P1) e (P2) e tale che $y_o = u$.

Vale il seguente

Teorema 4.1. Se S è un'algebra su Z_m soddisfacente le (P1) e (P2), definendo in V una moltiplicazione $\bullet$, per mezzo delle (4.3), (4.4), o in maniera equivalente della (4.5), V assume la struttura di algebra su Z_m isomorfa ad S ed avente le stesse costanti di struttura.

Supponiamo ora che S sia un'algebra di supporto.

Sia x l'elemento di S soddisfacente le (P3) e (P4) e ammettiamo che gli elementi di B siano ordinati in modo che $x_i = x$, per $i = 0, 1, ..., n-1$. Introdotto l'isomorfismo φ, sia $y = \varphi(x)$. Dalla (4.4) o dalla (3.8) si vede subito che $y_i = y$, che la (3.9) equivale alla

$$y^n = \sum_{i=0}^{n-1} \beta_i y^i \tag{4.6}$$

e che la invertibilità di x implica quella di y.

Le considerazioni svolte si possono riassumere enunciando il seguente

Teorema 4.2 Sia S un'algebra di supporto di dimensione n su Z_m, avente le costanti caratteristiche β_i e sia $y = \varphi(x)$. La (4.6) e le condizioni $y_i = y^i$ definiscono, in V, una struttura moltiplicativa rispetto alla quale V è un algebra di supporto su Z_m di dimensione n isomorfa, tramite la φ, ad S.

Come vedremo in seguito, fissati in Z_m gli elementi β_i in modo tale che β_0 sia invertibile, esiste (ed è unica a meno di isomorfismi) un'algebra di supporto S che ha le β_i come costanti caratteristiche.

Di conseguenza vale il seguente

Teorema 4.3 Fissata, nel modulo V su Z_m, la base $A = \{y_o, y_1, .., y_{n-1}\}$ e fissati, in Z_m, gli elementi $\beta_0, \beta_1, .., \beta_{n-1}$ tali che β_0 sia invertibile, esiste, ed è univocamente definita, una moltiplicazione $\bullet$ in V tale che, rispetto ad essa, V è un'algebra di supporto di dimensione n su Z_m ed inoltre

(M1) $y_0 = u$ e, per $n \geq 2$, $y_i = y_{1i}$;

(M2) vale la (4.6)

5. Esempi di costruzione di successioni di numeri pseudocasuali a partire da algebre con sostegno V

Sia $V = Z_m^n$ il modulo su Z_m definito nel paragrafo precedente e sia $B = \{x_0, x_1, .., x_{n-1}\}$ una base qualsiasi di V.

Per il teorema 4.3, fissati in Z_m degli elementi $\beta_0, \beta_1, .. \beta_{n-1}$, sono determinati degli elementi γ_{sti} soddisfacenti le (3.5), (3.6), (3.7), (3.8), (3.12) e, per $n \geq 2$, la (3.14).

La (3.4) definisce, allora, una moltiplicazione rispetto alla quale V ha la struttura di algebra di supporto.

In essa $x_0 = u$ e, per le (3.8), $x_i = (x_1)^i$. Poniamo, come al solito, $x = x_1$.

Sia ψ una funzione di supporto (LO).

Molti generatori di numeri pseudocasuali possono essere ottenuti come casi particolari del seguente procedimento

(G1) si considera, in Z_m, la asuccessione di termine generale $y_k = \psi(x^k)$, con $n \in N_0$;

(G2) si trasforma, per mezzo di una funzione ausiliaria, la successione ottenuta in una, $\{z_k\}_{k \in N0}$ di numeri razionali nell'intervallo [0,1).

Prescindiamo, per il momento, dalla funzione ausiliaria e chiamiamo, con abuso di linguaggio, non essendo ancora state verificate le proprietà statistiche e non trattandosi di elementi di [0,1), successione di numeri pseudocasuali la $\{z_k\}_{k \in N0}$

Cominciamo con l'esaminare il caso in cui B è la base usuale, ossia, per ogni i, x_{i-1} ha la componente i-sima uguale a 1 e le altre tutte nulle.

In tal caso vale il seguente

Teorema 5.1 Data la matrice, di ordine n,

$$A = \begin{bmatrix} 0 & 0 & \dots & 0 & \beta_0 \\ 1 & 0 & \dots & 0 & \beta_1 \\ . & . & \dots & . & . \\ 0 & 0 & \dots & 1 & \beta_{n-1} \end{bmatrix}, \tag{5.1}$$

le potenze di x soddisfano alla relazione ricorrente

$$x^{k+1} = A\, x^k \quad , \text{ per ogni } k \in Z. \tag{5.2}$$

Dimostrazione. E'immediato verificare che la (5.2) è valida per $0 \leq k \leq n-1$. Ammesso che essa valga per $0 \leq k \leq h$, con un fissato $h \geq n-1$, risulta, per la (3.15),

$$(5.3)\quad x^{h+2} = \sum_{i=0}^{n-1} \beta_i x^{i+h+2-n} = A \sum_{i=0}^{n-1} \beta_i x^{i+h+1-n} = A x^{h+1}$$

per cui essa vale anche per $k = h+1$. In base al principio di induzione matematica la (5.3) è allora valida per ogni $k \in N_0$.

La relazione (5.3) si può anche scrivere, dato che A è invertibile, poichè tale è β_0,

$$(5.4)\qquad x^k = A^{-1} x^{k+1} \quad , \text{ per ogni } k \in Z.$$

Essa è valida per ogni $k \in N_0$.

Ammesso che valga per $0 \geq k \geq h$, con un fissato $h \leq 0$, risulta, per la (3.16),

$$(5.5)\qquad x^{h-1} = \beta_0^{-1} x^{n+h-1} - \sum_{i=1}^{n-1} \beta_0^{-1} \beta_i x^{i+h-1} =$$

$$= A^{-1}(\beta_0^{-1} x^{n+h} - \sum_{i=1}^{n-1} \beta_0^{-1} \beta_i x^{i+h}) = A^{-1} x^h \ ,$$

per cui essa è valida anche per $k = h-1$. In base al principio di induzione matematica la (5.2) è allora valida anche per valori negativi di k.

Dal teorema 5.2 si ottengono i seguenti

Corollario 5.1.1 Le potenze di x soddisfano alla relazione

$$(5.6)\qquad x^k = A^k x_0$$

ossia, detto a_{ij}^k l'elemento generico della matrice A^k,

$$(5.7) \qquad x^k = \begin{bmatrix} a_{11}^k \\ a_{21}^k \\ \cdots \\ \cdots \\ \cdots \\ a_{n-1}^k \end{bmatrix}$$

Dimostrazione. La (5.6) è vera per $k=0$. Se essa è vera per $k=h>0$ risulta $x^{h+1}=Ax^h=A(A^hx_0)=A^{h+1}x_0$ e quindi è vera anche per $k=h+1$. Se essa è vera per $k=-h<0$ risulta $x^{-h-1}=A^{-1}(x^{-h})=A^{-1}(A^{-h}x_0)=A^{-h-1}x_0$ e quindi è vera anche per $k=-h-1$.

Corollario 5.1.2 La successione di termine generale y_k soddisfa alla relazione

$$(5.8) \qquad y_k = \psi_0 A^k x_0 ,$$

dove y_0 è il vettore riga $[\psi(x_0), \psi(x_1), ..., \psi(x_{n-1})]$, ossia alla:

$$(5.9) \qquad y_\kappa = \psi(x_0)a_{11}^k + \psi(x_1)a_{21}^k + ... + \psi(x_{n-1})a_{n1}^k .$$

Dimostrazione. Se B è una qualsiasi matrice di ordine n e $v=[v_0, v_1, ..., v_{n-1}]'$ è un qualsiasi elemento di V, risulta, per le proprietà di linearità di ψ,

$$(5.10) \qquad \psi(Bv) = \psi_0 Bv$$

La (5.6) implica allora la (5.8) e la (5.7) implica la (5.9).

Esempi notevoli di funzioni di supporto (LO) sono:

(S1) $\forall z \in V$, $\psi(z) = z_i$ (i-sima componente di z) ;

(S2) $\forall z \in V$, $\psi(z) = \sum_{i=1}^{n} z_i$;

(S3) $\forall z \in V$, $\psi(z) = \sum_{i=1}^{n} \alpha_i z_i$, con $\alpha_i \in Z_m$ e tali che almeno uno di essi sia invertibile.

La (S3) include, come casi particolari, i primi due.

La espressione di y_k si riduce, nei tre casi considerati, rispettivamente alle

(5.11.1) $$y_k = a_{i1}^k ,$$

(5.11.2) $$y_k = \sum_{i=1}^{n} a_{i1}^k ,$$

(5.11.3) $$y_k = \sum_{i=1}^{n} \alpha_i \, a_{i1}^k \ .$$

Consideriamo ora il caso in cui la base $B = \{x_0, x_1, ..., x_{n-1}\}$ non sia quella usuale. Sia $F = \{z_0, z_1, ..., z_{n-1}\}$ e sia B la matrice avente come colonne i vettori $x_0, x_1, ..., x_{n-1}$.

Se v è un qualsiasi elemento di V e v^* è il vettore delle sue coordinate rispetto alla base B risulta

(5.12) $$v = B v^*, \quad v^* = B^{-1} v$$

Sia le potenze di $v \in V$ che le relazioni fra esse come la (4.6) non dipendono dal sistema di riferimento scelto.

Usando come sistema di riferimento la base B i vettori $x_0, x_1, ..., x_{n-1}$ hanno come vettori delle coordinate quelli della base usuale per cui dalla (5.2) segue

(5.13) $$x^{k+1\,*} = A \, x^{k\,*}$$

Allora, per la (5.12), risulta

(5.14) $$x^{k+1} = B A B^{-1} x^k \ .$$

Posto $A^* = B A B^{-1}$, le (5.6) e (5.8) sono, in tal caso, sostituite rispettivamente dalle

(5.15) $$x^k = A^{*k} x_0 ,$$

(5.16) $$y_k = \psi_0 A^{*k} x_0 \ .$$

Presentiamo un esempio di algebra su V che, pur soddisfacendo le (P1) e (P2), non è di supporto .

Si assuma, in V, la base B in modo che sia $x_0 = (1, 1, ..., 1)$ e, per $i \neq 0$, x_i uguale al vettore $(i+1)$-simo della base usuale.

Definiamo, in V, una moltiplicazione ponendo, per $x = (\alpha_0, \alpha_1, ..., \alpha_{n-1})$ e $y = (\beta_0, \beta_1, ..., \beta_{n-1})$,

$$x\,y = (\alpha_0\beta_0,\ \alpha_1\beta_1,\ \ldots,\ \alpha_{n-1}\ \beta_{n-1}) \tag{5.17}$$

Si può facilmente dimostrare che la moltiplicazione (5.17) gode della *proprietà associativa e di quella distributiva rispetto all'addizione in V ed* inoltre che valgono, rispetto al complesso delle operazioni, i vari assiomi di un'algebra. Il fatto che, rispetto alla (5.17), V è un'algebra si può anche vedere mostrando che le costanti di struttura verificano le (3.5).

Infatti la (5.17) implica le

$$x_s\,x_t = \begin{cases} x_t \ \textit{per}\ \ s = 0\ \textit{oppure}\ s = t \\ x_s \ \textit{per}\ \ t = 0 \\ 0 \ \textit{negli altri casi} \end{cases} \tag{5.18}$$

per cui

$$\gamma_{sti} = \begin{cases} 1 \ \textit{per}\ \ s = 0\ e\ i = t\ . \\ \quad \textit{oppure per}\ t = 0\ e\ \ i = s\ \ \textit{oppure per}\ \ s = t = i\ . \\ 0 \ \textit{negli altri casi} \end{cases} \tag{5.19}$$

Le formule (3.5) si riducono a

$$\gamma_{rsr}\ \gamma_{rti}\ + \gamma_{rss}\ \gamma_{sti}\ = \gamma_{rsi}\ \gamma_{sts}\ + \gamma_{rti}\ \gamma_{stt}\ .$$

Considerando tutti i possibili valori di r,s,t,i, tenendo conto della (5.19) si vede che le (3.5) sono soddisfatte. Allora, in base al teorema 3.1, V e un'algebra.

Se $x = (\beta_o, \beta_1, \ldots, \beta_{n-1})$, la (3.1) si riduce a

$$x = \beta_0\ x_0\ +\ \sum_{i=1}^{n-1}\ (\beta_i\ -\ \beta_o)\,x_i$$

e viceversa, se $x = \sum_{i=0}^{n-1}\ \alpha_i\ x_i$, risulta

$$x\ = (\alpha_0\,,\ \alpha_1\ +\ \alpha_0,\ \ldots,\ \alpha_{n-1}\ +\ \alpha_0).$$

Si puo osservare che, per $n > 1$, la (5.17) implica che $x_1 y = \beta_1\, x_1$ e, in particolare, $x_{12} = x_1$. Segue che x_1, essendo diverso dall'unità, non è invertibile e, per $n > 2$, nessun x può soddisfare alla(P3).

L'algebra costruita non è di supporto per nessun $n > 1$.

6. Algebre di supporto di dimensione 1 o 2 e successioni di numeri pseudocasuali ottenute da esse

Consideriamo le algebre di supporto di dimensione 1. Per il teorema 4.2 non si viene meno alla generalità ponendo $S = V = Z_m$.

Un'algebra di supporto di dimensione 1 viene allora costruita introducendo una opportuna moltiplicazione in Z_m considerato come modulo su Z_m.

In base al corollario 2.1.2, tale moltiplicazione non può che identificarsi con quella ordinaria in Z_m.

Poichè,in tal modo, sono soddisfatti gli assiomi (P1), (P2), (P3), (P4), segue che esiste un'unica algebra di supporto di dimensione 1 su Z_m, avente la base $B = \{x_0 = 1\}$ e l'unica costante di struttura $\gamma_{000} = 1$.

Se x è un elemento invertibile di Z_m e $\beta_0 = x$, la (3.9) si riduce alla

$$x = \beta_0 x_0 = \beta_0 x^0 \tag{6.1}$$

e le (3.15) e (3.16) si riducono, rispettivamente, alle

$$x^{k+1} = \beta_0 x^k \; ; \quad x^k = \beta_0^{-1} x^{k+1} \; . \tag{6.2}$$

Se ψ è una funzione di supporto (LO) risulta, allora

$$\psi(x) = \beta_0 \psi(1) \quad , \quad \psi(x^{k+1}) = \beta_0 \psi(x^k) \; . \tag{6.3}$$

Poniamo $\psi(x^k) = y_k \quad , \quad \beta_0 = a \quad , \quad \psi(1) = y_0$.

Le (6.3) si riducono alla relazione ricorrente, in Z_m,

$$y_{k+1} = a y_k \; , \; \textit{con} \; y_0 \; \textit{assegnato.} \tag{6.4}$$

Alla successione $\{x^k\}_{k \in N0}$ delle potenze di x corrisponde tramite la ψ, la successione (6.4) ossia il generatore moltiplicativo con moltiplicatore $r(a)$ e seme $r(y_0)$.

Si noti come il fatto che β_0 sia invertibile si traduce nella classica condizione $(r(a), m) = 1$.

Poichè ψ è un epimorfismo fra gruppi additivi aventi una moltiplicazione esterna con dominio di operatori Z_m, per ogni $y \in Z_m$ deve esistere un $z \in Z_m$ tale che $\psi(z) = z\,\psi(1) = y$. Ciò avviene se e solo se $\psi(1)$ è invertibile. Questo fatto, in riferimento al generatore moltiplicativo, si traduce nell'altra classica condizione $(r(y_0),m) = 1$.

Consideriamo ora le algebre di supporto di dimensione 2.

Sempre per il teorema 4.2, si può prendere $S = V = Z_{m2}$ e costruire un'algebra introducendo una opportuna moltiplicazione in V considerato come modulo su Z_m.

Sia $A = \{x_0, x_1\}$ una base di V e imponiamo le condizioni

$$(6.5) \qquad \begin{cases} x_0 x_0 = x_0 \\ x_0 x_1 = x_1 x_0 = x_1 \\ x_1 x_1 = \beta_0 x_0 + \beta_1 x_1 \end{cases}$$

con β_0 invertibile in Z_m.

Esse si traducono nel fatto che le matrici γ_{sti}, con i fissato, delle costanti di struttura sono

$$[\gamma_{st0}] = \begin{bmatrix} 1 & 0 \\ 0 & \beta_0 \end{bmatrix}, \qquad [\gamma_{st1}] = \begin{bmatrix} 0 & 1 \\ 1 & \beta_1 \end{bmatrix}.$$

Si può facilmente dimostrare che tali costanti soddisfano le (3.5),(3.6), (3.7), (3.8), (3.12), per cui definiscono un'algebra di supporto, in cui $x_0 = u$.

Se $y = \delta_0 x_0 + \delta_1 x_1$ e $z = \gamma_0 x_0 + \gamma_1 x_2$, in base alla (3.4) risulta

$$(6.6) \qquad y \cdot z = \sum_{i=0}^{1} \Big(\sum_{s=0}^{1} \sum_{t=0}^{1} \delta_s \gamma_t \gamma_{sti} \Big) x_i ,$$

ossia, per le (6.5),

$$(6.7) \quad y \cdot z = (\delta_0 \gamma_0 + \delta_1 \gamma_1 \beta_1) x_0 + (\delta_1 \gamma_0 + \delta_0 \gamma_1 + \delta_1 \gamma_1 \beta_1) x_1$$

Poniamo $x_1 = x$. L'ultima delle (6.5) si può scrivere

$$(6.8) \qquad x^2 = \beta_0 x^0 + \beta_1 x$$

ed è un caso particolare della (3.9).

Le (3.15) e (3.16) si scrivono, rispettivamente

$$x^{k+2} = \beta_0 x^k + \beta_1 x^{k+1} , \tag{6.9}$$

$$x^k = \beta_0^{-1} x^{k+1} - \beta_0^{-1} \beta_1 x^{k+1} . \tag{6.10}$$

Sia ψ una funzione di supporto (LO). Risulta, per le (6.8) e (6.9),

$$\psi(x^{k+2}) = \beta_0 \psi(x^k) + \beta_1 \psi(x^{k+1}) . \tag{6.11}$$

Poniamo

$$\psi(x^k) = y^k , \quad \beta_0 = a_0 , \quad \beta_1 = a_1 . \tag{6.12}$$

Le (6.11) si riducono alla relazione ricorrente, in Z_m,

$$y_{k+2} = a_0 y_0 + a_1 y_{k+1} , \quad \textit{con } y_0 \textit{ e } y_1 \textit{ assegnati} . \tag{6.13}$$

Alla successione $\{x^k\}_{k \in No}$ delle potenze di x corrsponde la successione ottenuta dalla (6.13), ossia dal generatore lineare omogeneo del 2º ordine.

Per $r(a_0) = r(a_1)$, $r(y_0) = 0$, $r(y_1) = 1$ esso fornisce la classica successione di Fibonacci modulo m.

Il fatto che ψ sia un epimorfismo implica che, per ogni $y \in Z_m$, esistono α_0 e α_1 tali che

$$\alpha_0 y_0 + \alpha_1 y_1 = y , \tag{6.14}$$

ossia che l'ideale in Z_m generato da y_0 e y_1 coincide con Z_m. Ciò avviene o se almeno uno fra y_0 e y_1 è invertibile, oppure se non esistono divisori dello zero che dividano sia y_0 che y_1.

Infatti la (6.14) ammette soluzioni se e solo se ammette soluzioni intere $r(\alpha_0)$, $r(\alpha_1)$, k l'equazione

$$r(\alpha_0) r(y_0) + r(\alpha_1) r(y_1) + km = r(y) , \tag{6.15}$$

ossia se e solo se

(6.16) $D(r(y_0), r(y_1), m) = D(r(y_0), r(y_2), m, r(y))$.

Se uno fra y_0 e y_1 è invertibile oppure non esistono divisori dello zero che dividano sia y_0 che y_1 risulta $D(r(y_0), r(y_1), m) = 1$ e quindi la (6.16) è soddisfatta. Se, invece, esiste un divisore dello zero δ che divide sia y_0 che y_1 allora la (6.16) ammette soluzioni solo se δ divide anche y. Non ammette soluzioni se, ad esempio, y è invertibile, dato che, in tal caso, $D(r(y), m) = 1$.

BIBLIOGRAFIA

(1) G.Ascoli **Lezioni di Algebra**. Editrice Tirrenia. Torino. 1965

(2) A.C. Arvillas and D.G. Matitsas **Partitioning the period of a class of m-sequences and application to pseudorandom number generation**. Journal of the Association for Computing Machinery. Vol 25. 1978

(3) M. Curzio **Lezioni di Algebra**. Liguori Editore Napoli. 1967

(4) I: Glazman-Y. Liubitch **Analyse linèare dans le espaces de dimensions finies**. Editions Mir Moscou. 1974

(5) S.W. Golomb **Shift register sequences**. Holden-Dsy, Inc. London. 1965

(6) D.E. Knuth **The art of computer programming**. Vol 2. Seminumerical Algorithms. Addison-Wesley. London. 1969

(7) T.G: Lewis and W.H. Payne **Generalized feedback shift register pseudorandom number algorithm**. Journal of the Association for Computing Machinery. Vol 20. 1973

(8) A. Maturo **Numeri pseudocasuali**. Montefeltro Edizioni Urbino. 1982

(9) A. Maturo N.Cera ***Confronto fra alcuni generatori di numeri pseudocasuali***. Ratio Math. 2, in corso di stampa.

(10) A. Maturo N. Cera **Generazione di numeri pseudocasuali per mezzo di relazioni di ricorrenze su campi di Galois**. Periodico di Matematiche, in corso di stampa.

(11) W.W. Peterson-E.J. Weldon **Error-correcting codes**. Massachusetts Institute of Technology Press. Cambridge. 1972

(12) I.S. Reed and R. Turn **A generalization of shift register sequences generators**. Journal of the Association for Computing machinery. Vol 16. 1969

(13) A. Rizzi **Su un metodo per la generazione di sequenze di simboli binari pseudo-casuali**. Metron. Vol XXIX. 1971

(14) A. Rizzi **Generazione di simboli binari pseudocasuali mediante polinomi primitivi**. Statistica. 1982

(15) C.S. Smith **Multiplicative pseudo-random number generators with prime modulus**. Journal of the Association for Computing Machinery. Vol 18. 1971

(16) R.C. Tausworthe. **Random numbers generated by linear recurrence modulo two**. Mathematics of Computation 19. 1965

(17) J.P.R. Tootil-W.D. Robinson and A.G. Adams **The runs up and down performance of Tausworthe pseudorandom number generators**. Journal of Association for Computing Machinery. Vol 18. 1971

(18) G. Zappa-R. Permutti **Gruppi, corpi, equazioni**. Feltrinelli. 1972

(19) N. Zierlir **Linear recurring sequences**. J Soc. Industr. Appl. Math. Vol 7. 1959

RATIO MATH. 1.
(1990), 121 - 132

Analisi Critttografica e Ricerca Scientifica

Giovanni Moro

1. PREMESSE

Prima di entrare nel vivo dell'argomento mi sembra opportuno qualche cenno, anche se fugace, sulla "Crittografia", l'arte- scienza che, fin dalle sue origini, ha avuto due obiettivi non solo ben distinti, ma addirittura antitetici:

- uno, quello della tutela del segreto delle comunicazioni, mediante la loro cifratura;
- l'altro, quello della penetrazione (illegale) del segreto delle comunicazioni, a mezzo decrittazione.

L'attività di studio e ricerca, che è alla base dei tentativi di decrittazione dei messaggi cifrati, va sotto il nome ormai universalmente noto di "Analisi Crittografica" o "Criptoanalisi".

LA CRIPTOANALISI.

La criptoanalisi è la scienza composita che, partendo da messaggi cifrati con sistemi di cifratura dei quali può anche non essere noto nulla, si prefigge, in linea di massima, di raggiungere, nell'ordine, i seguenti obiettivi:

(1) determinare l'architettura del sistema di cifratura impiegato, individuandone i "parametri" fondamentali, o di base, che lo governano sul piano operativo;

(2) ricostruire le leggi, se ve ne sono di determinabili, alle quali fa capo la "variazione" dei "parametri base", che, con la loro evoluzione temporale,

dovrebbero assicurare l'impervietà del sistema di cifratura;

(3) ricostruire le "chiavi" dei singoli messaggi;

(4) decrittare i messaggi, possibilmente in tempo utile per poterli sfruttare operativamente;

(5) acquisire una "conoscenza" tanto approfondita del sistema studiato, che consenta di individuare la "filosofia" che è a monte del sistema stesso.

Se questo risultato è raggiunto, in caso di "varianti" sia funzionali che operative al sistema di cifratura, si possono più facilmente individuare le eventuali linee preferenziali di studio-ricerca da seguire per risolvere i problemi che le "varianti" apportate creano.

I moderni sistemi di cifratura, in linea di massima, sono ormai talmente complessi e sofisticati che il loro studio non può essere effettuato da singoli, anche se molto preparati. E' necessario impiegare teams composti da persone di varia estrazione culturale e scientifica; oltre ai "crittografi" più o meno classici che dovrebbero fungere anche da analisti di sistema, è necessario, secondo le varie necessità che si possono presentare, impiegare anche: statistici, matematici, spesso specializzati in teoria dei numeri; eletronici; linguisti; programmatori; tecnici delle trasmissioni.

L'impiego di sistemi di elaborazione elettronica di adeguata potenza è dato per scontato.

I dati ricavati dalla "Criptoanalisi" sono di grandissima utilità anche per la ideazione, progettazione, realizzazione dei moderni sistemi di cifratura elettronici che, oltre che efficienti, devono essere sicuri.

La "Criptoanalisi" deve quindi essere una attività di studio- ricerca non considerata a sè stante, ma inquadrata nel più ampio contesto della "Crittografia", intesa nel suo più ampio significato.

CRIPTOANALISI E RICERCA SCIENTIFICA

Normalmete si pensa alla "Crittografia" come ad una scienza tributaria di altre scienze, ma non anche come ad una scienza autonoma, che possa essere di ausilio alle altre.

La mia esperienza quarantennale di lavoro in tale campo, mi porta a ritenere questo modo di pensare non valido in assoluto. Cercherò di dimostrare la correttezza di questo mio convincimeto:

(1) Illustrando, anche se solo a grandi linee, la "logica" che è alla base del lavoro crittografico, facendo vedere come l'"Analisi Crittografica", considerata nei suoi aspetti generali, non sia altro che ricerca scientifica, talvolta pura.

(2) Riportando, come pratico esempio di applicazione dei principi di cui

sopra, i risultati da me ottenuti studiando da "crittografo" l'equazione a numeri interi: $M^2 = N^2 - P^2$.

2. CENNI SULL'"ANALISI CRITTOGRAFICA"

L'"Analisi crittografica", in sintesi, si sviluppa attraverso le seguenti fasi successive, fra di loro strettamente collegate da legami di retroazione, a quasi tutti i livelli.

(1) Si assume una base numerica, su modulo/i opportuno/i , con la quale tradurre in numeri i dati oggetto di studio. Si ricavano "blocchi" di "numeri", che costituiscono la base per le successive fasi di sviluppo delle ricerche.

(2) Sui "blocchi" di "numeri" così trovati, considerati singolarmente e, o opportunamente raggruppati, si va alla ricerca di "fenomeni", di natura generalmente "logico-matematica", che escono, "ragionevolmente", al di fuori della fascia della "casualità".

(3) Si cerca di dare una interpretazione "logico-matematica" ai fenomeni "non casuali" rilevati, facendo, se necessario, ipotesi "attendibili". Si verifica l'attendibilità delle eventuali ipotesi fatte.

(4) Si cerca di inserire e coordinare in un unico "modello logico-funzionale", i singoli "fenomeni" rilevati e le eventuali "ipotesi", che gli stessi hanno originato.

(5) Si procede all'esame critico (sperimentale, quando necessario) del "modello" trovato ed alla verifica finale della sua validità.

(6) Si applica il "modello finale" al caso studiato.

Il lavoro, quando necessario, procede per approssimazioni successive.

Nello sviluppo delle singole fasi dello studio è spesso, per non dire quasi sempre, specialmente nei problemi molto complessi, necessario ritornare nelle "fasi" precedenti per apportare correzioni alle interpretazioni date dai "fenomeni" rilevati e, o alle "ipotesi logiche", o di altro tipo, che si sono fatte.

Nel caso di "ricostruzione" di sistemi di cifratura, il "modello" ricavato può essere "fittizio" e, o "reale".

Se si esaminano le "fasi" attraverso le quali si sviluppa la "criptoanalisi", sembra di poter pervenire alla conclusione che segue.

L'"analisi crittografica" non è altro che un "metodo" di "ricerca scientifica" pura, che si può applicare anche in campi, che ben poco, per quel che può

sembrare, hanno a che fare con la "crittografia".

La cosa non deve stupire più di tanto, perchè, in ultima analisi, l'"analisi crittografica" e la "ricerca pura", hanno come obiettivo finale comune la ricerca di "informazioni", nei casi in cui esistano, indipendantemente dalla loro natura e dal fatto che siano, o meno, determinabili.

3. RADICI DELL'EQUAZIONE $M^2 = N^2-P^2$, PER: M, N, P INTERI.

3.1 PREMESSE.

Per l'equazione:

$$M^2 = N^2 - P^2 = (P + Z)^2-P^2 \tag{1}$$

(M, N, P, Z interi), *con "procedimenti" di lavoro "crittografico"*, sono stati trovati i seguenti tre metodi per calcolarne le infinite radici.

(I)

$$\begin{cases} M = \{2^{(1+r)}GZ + Z^2\}; \; N = \{2^{(1+r)}GZ + 2^{(1+2r)}G^2\}; \\ P = \{2^{(1+r)}GZ + 2^{(1+2r)}G^2\} \end{cases} \tag{2}$$

ove: $Z \geq 1$, intero dispari qualsiasi; G intero dispari ($\lesseqgtr 0$), primo con Z, qualsiasi; $r \geq 0$, intero qualsiasi. *La (1) è verificata per qualsiasi terna di valori di M, N, P definita da un "blocco" di valori qualsiasi di Z; G; r.*

(II) *L'equazione:*

$$M^2 = \{(M^2 + Z^2) / 2Z\}^2 - \{(M^2-Z^2) / 2Z\}^2 \tag{3}$$

ammette soluzione:

- *per:* $Z = 1$, per qualsiasi valore intero di $M \geq 3$, dispari;
- *per:* $Z = 2$, per qualsiasi valore intero di $M \geq 4$, *pari.*

(III) *Ricostruendo sistematicamente, a catena*, nell'ambito di un prefissato valore qualsiasi di Z, *i valori, crescenti, degli: M- N-P, omologhi nelle rispettive successioni, costituenti le infinite terne soluzioni della (1)*, caratterizzate dal

prescelto valore di Z.

Come terna di partenza, terna numero 1, è stata scelta la:

$$M^2 = N^2 - P^2 = Z^2-(0)^2 \tag{4}$$

Omesso un approfondimento dei casi (1) e (2), passiamo al caso (III).

3.2 CASO (III).

La ricostruzione (calcolo), a catena, dei termini omologhi delle tre successioni degli M, N, P, noti i quali sono determinate le infinite terne M, N, P soluzioni della (1), si può effettuare tenendo presenti:

(a) Il seguente schema:

M	$M_1 = Z$	$M_2 - M_3$ -		M_s	successione M crescenti
	D_1M	$D_1M - D_1M$ -			successione 1^e Differenze M
N	$N_1 = Z$	$N_2 - N_3$ -		N_s	successione N crescenti
	D_1N	$D_1N - D_1N_2$ -			successione 1^e Differenze N
	D_2N	D_2N -			successione 2^e Differenze N
P	$P_1 = 0$	$P_2 - P_3$ -		P_s	successione P crescenti

(5)

Ove:

$S \geq 1$, intero qualsiasi;

$D_1M = \{M_{(s+1)}-M_s\}$ = costante - 1^e Differenze succ. M;

$D_1N = \{M_{(s+1)}-N_s\}$ - 1^e Differenze succ. N;

$D_2N = \{D_1N_{(s+1)}-D_1N_s\}$ = costante - 2^e Differenze succ. N.

Dal quadro (5) risulta chiaramente come, partendo da:

$-M_1 = Z$ e D_1M, mediante somme successive a catena, da sinistra a destra, si possono ricostruire tutti i termini della successione degli M.

$-N_1 = Z$, D_1N_1 e D_2N, mediante somme successive a catena, sempre da sinistra a destra, si possono ricostruire tutti i termini e della successione ausiliaria dei D_1N e di quella degli N.

I valori dei P_s sono dati da: $(N_s - Z)$.

Z è noto perchè il suo valore viene prefissato in partenza: gli altri elementi base per lo sviluppo del procedimento, e cioè: M_1- D_1M-N_1-D_1N_1-D_2N sono calcolabili con le:

(b) Seguenti formule:

	Z			
	$(2H+1)^2$	$\{(2K)^2:2\}$	$(2H_1+1)$	$(2K_1)$
	$H \geq 0$	$K \geq 1$	$H_1 \geq 1$	$K_1 \geq 2$
M_1	$(2H+1)^2 = Z$	$\{(2K)^2:2\} = Z$	$(2H_1+1) = Z$	$(2K_1) = Z$
D_1M	$2(2H+1)$	$2K$	$2(2H_1+1) = 2Z$	$(2K_1) = Z$
N_1	$(2H+1)^2 = Z$	$\{(2K)^2:2\} = Z$	$(2H_1+1) = Z$	$(2K_1) = Z$
D_1N_1	$2(2H+1)+2$	$(2K+1)$	$4(2H_1+1) = 4Z$	$3K_1$
D_2N	4	2	$4(2H_1+1) = 4Z$	$(2K_1) = Z$
P_s	$(N_s$-$Z)$	$(N_s$-$Z)$	$(N_s$-$Z)$	$(N_s$-$Z)$

(6)

Nelle quali:

H, intero qualsiasi;
K, intero qualsiasi;
H_1, intero per cui $(2H_1+1)$ diverso $(2H+1)^2$;
K_1, intero per cui $(2K_1)$ diverso $\{(2K)^2:2\}$.

La configurazione caratteristica delle formule di cui sopra, suggerisce l'idea di considerare, per l'insieme dei valori di Z, i seguenti quattro sottoinsiemi caratteristici:

- $S_z(2H+1)^2$-$S_z(1)$: sottoinsieme dei valori di Z, dei quadrati dei numeri dispari.
- $S_z\{(2K)^2:2\}$-$S_z(2)$: sottoinsieme dei valori di Z, delle metà dei quadrati dei numeri pari.
- $S_z(2H_1+1)$-$S_z(3)$: sottoinsieme dei valori di Z, dei numeri dispari, esclusi i quadrati.
- $S_z(2K_1)$-$S_z(4)$: sottoinsieme dei valori di Z, dei numeri pari, escluse le metà dei quadrati dei pari.

3.3 PROPRIETA' DI MAGGIOR INTERESSE DELLE SOLUZIONI DELLA (1)

Nell'allegato 1, sono riportati, a titolo di esempio, raggruppati in funzione di Z, blocchi di valori di M - N - P costituenti terne di interi soluzioni della (1), determinate con il "procedimento" di cui al caso (III).

Definite come soluzioni "primitive", quelle che possono essere ricavate "esclusivamente" come soluzioni della (1):

- applicando uno qualsiasi dei metodi sopra visti;
- e che presentano valori di P - "pari";

l'unico dei quattro sottoinsiemi dei valori di Z, che contiene anche soluzioni "*primitive*" è $S_z(1)$.

Considerando le soluzioni della (1) raggruppate in funzione di: $S_z(1)$ - $S_z(2)$ - $S_z(3)$ - $S_z(4)$, si rileva quanto di seguito specificato, per ciascuno dei quattro sottoinsiemi citati.

a) *Sottoinsieme* $S_z(1)$.
$H = 0$ - $Z = 1$: *tutte le soluzioni sono "primitive"*.
$H \geq 1$ - $Z = (2H+1)^2$. Se:

$$(7) \qquad \begin{cases} (M_1)^2 = (P_1+1)^2 - (P_1)^2 \\ (M_2)^2 = (P_2+1)^2 - (P_2)^2 \end{cases} \qquad M_1 < M_2$$

sono soluzioni, del gruppo $Z = 1$; si ha che gli: M_3 - N_3 - P_3 dati da:

$$(8) \qquad \begin{cases} M_3 = M_1 M_2 \\ N_3 = (P_2+1) + P_1 = ((M_2)^2 + (M1)^2)/2 = (N2) + (P_1) \\ P_3 = (P_2) - (P_1) = ((M_2)^2 - (M_1)^2)/2 \end{cases}$$

sono soluzioni della (1), del gruppo $Z = (M_1)^2 = (2P_1 + 1)$.
(9) *Regola di derivazione* A.

Le soluzioni nelle quali M - N - P sono tra loro "non" - "primi", oltre che con la (9), sono sicavabili ("derivabili") anche da opportune soluzioni (terne M - N - P), che chiameremo soluzioni "base", moltiplicate per opportune costanti.
(10) *Regola di derivazione* B.

Nei quadri $S_z(1)$ dell'Allegato 1 vicino a ciascuna terna "derivata" sono indicate le relative regole: A - B di "derivazione".

"A", è seguito da due numeri, che indicano i numeri d'ordine delle due terne "base" - entrambe del gruppo di soluzioni $Z = 1$ - che danno origine alla terna "derivata".

"B", è seguita da tre numeri che indicano nell'ordine:

- valore di Z al quale appartiene la terna base;
- numero d'ordine, in tale gruppo di soluzioni, della terna "base";
- valore della costante moltiplicativa degli M - N - P della terna "base" che sono serviti per ricavare la terna "derivata".

Da rilevare, come già detto in altro punto, che per $S_z(1)$, qualsiasi sia il valore di Z, tutti i valori di P sono "pari".

b) Sottoinsieme $S_z(2)$

Le soluzioni sono tutte "derivate".

Le regole di "derivazione", applicando le quali, a seconda dei casi, si ricavano le varie terne di M - N - P soluzioni della (1) sono le seguenti tre:

(a) Si scambiano di posto i valori di M e P, mantenedo fisso quelo di N, di una soluzione di $S_z(1)$.

(11) *Regola di derivazione* C.

(b) Si moltiplicano per 2 i valori degli M - M - P di una soluzione di $S_z(1)$.

(12) *Regola di derivazione* D.

(c) Si moltiplicano per 4 i valori degli M - N - P di una soluzione di $S_z(2)$, stesso.

(13) *Regola di derivazione* E.

Nei quadri di $S_z(2)$, dell'allegato1, vicino a ciascune terna soluzione, sono indicate le relative regole: C - D - E, di derivazione.

C, è seguito da due numeri, che indicano nell'ordine:

- valore di Z, al quale appartiene la terna "base";
- numero d'ordine, in tale gruppo di soluzioni, della terna "base";

che sono serviti per ricavare la terna "derivata".

Tali due elementi sono riportati anche dopo D ed E, in tali casi sono poi seguito da un terzo: la costante moltiplicativa.

c) Sottoinsieme $S_z(3)$

Le soluzioni sono tutte "derivate".

Regola impiegata: si moltiplicano per $Z=(2H_1+1)$ i valori di M - N - P della soluzione omologa - terna "base" - di $Z=1$.

(14) *Regola di derivazione* F.

Nel quadro, dell'allegato 1 di S_z (3), accanto ad F è riportata la costante

moltiplicativa.

d) Sottoinsieme $S_z(4)$

Le soluzioni sono tutte "derivate".

Regola impiegata: si moltiplicano per K_1 i valori di M - N - P della soluzione omologa - terna "base" - di $Z=2$.

(15) *Regola di derivazione* G.

Nel quadro, dell'allegato 1, di S_z (4), accanto a G è riportata la costante moltiplicativa.

3.4 Vedere, nell'allegato 2, un "procedimeto", diverso da quelli già sopra descritti, per ricavare le terne di: M - N - P soluzioni della (1) - caso $Z=(N-P)=1$.

ALLEGATO 1

ESEMPI DI RISULTATI OTTENUTI CON L'APPLICAZIONE DELLE: (5) - (6) PER LA RICOSTRUZIONE A CATENA DELLE SOLUZIONI DELLA (1).

1. *Sottoinsieme* S_z (1)

$H=0; Z=1$				$H=1; Z=3^2=9$			REGOLE		
S	M	N	P	M	N	P	A	B	S
1	1	1	0	9	9	0	2-2	1-1-9	1
2	3	5	4	15	17	8	2-3	-	2
3	5	13	12	21	29	20	2-4	-	3
4	7	25	24	27	45	36	2-5	1-2-9	4
5	9	41	40	33	65	56	2-6	-	5
6	11	61	60	39	89	80	2-7	-	6
7	13	85	84	45	117	108	2-8	1-3-9	7
8	15	115	112	51	149	140	2-9	-	8
9	17	145	144	57	185	176	2-10	-	9
10	19	181	180	63	225	216	2-11	1-4-9	10

NOTE

(1) I valori di: M_s - N_s - P_s, costituenti la S^a terna soluzione della (1) - per $Z=(2H+1)^2$, $H\geq 0$ qualsiasi - si possono calcolare anche applicando le seguenti tre formule:

(16) $M_s=(2H+1)\{2(H+S)-1\}$; $N_s=\{(2H+S)^2+(S-1)^2\}$; $P_s=2(S-1)(2H+S)$

(2) I "guadri", intestati a: $Z=(2H+1)^2$ - per $H \geq 1$ - delle terne: M - N - P soluzioni della (1), si possono ricavare applicando la regola di "derivazione" - A (vedere (9)), facendo giocare la terna $S=(H+1)$, successivamente con le terne:

(17) $S_{\bullet}=(H+1)\text{-}(H+2)\text{-}(H+3)\text{-}(H+4)\text{-}\ldots$

del gruppo di soluzioni di $Z=1$ -$(H=0)$.

2. Sottoinsieme S_z (2)

K = 1

Z = 2 REGOLE

S	M	N	P	C	D
1	2	2	0	-	1-1-2
2	4	5	3	1-2	-
3	6	10	8	-	1-2-2
4	8	17	15	9-2	-
5	10	26	24	-	1-3-2
6	12	37	35	25-2	-
7	14	50	48	-	1-4-2
8	16	65	63	49-2	-
9	18	82	80	-	1-5-2

K = 2

Z = 8 REGOLE

M	N	P	C	E	S
8	8	0	-	2-1-4	1
12	13	5	1-3	-	2
16	20	12	-	2-2-4	3
20	29	21	9-3	-	4
24	40	32	-	2-3-4	5
28	53	45	25-3	-	6
32	68	60	-	2-4-4	7
36	85	77	49-3	-	8
40	104	96	-	2-5-4	9
44	125	117	81-3	-	10

3. Sottoinsieme $S_z(3)$

$H_1 = 1$

$Z = 3$ R.

S	M	N	P	F
1	3	3	0	3
2	9	15	12	3
3	15	39	36	3
4	21	75	72	3
5	27	123	120	3
6	..	...	...	3

4. Sottoinsieme $S_z(4)$

$K_1 = 2$

R. $Z = 4$

G	M	N	P	S
2	4	4	0	1
2	8	10	6	2
2	12	20	16	3
2	16	34	30	4
2	20	52	48	5
2	..	..	..	6

ALLEGATO 2

Schema di calcolo delle terne: M, N, P (interi) soluzioni della $M^2 = N^2 - P^2$, per $Z = (N - P) = 1$, partendo dalla successione: 0^2, 1^2, 2^2, 3^2, 4^2, ...

$\{(n+1)^2 - n^2\}$ n^2 $[(n+1)^2 + n^2]$ $\{[(n+1)^2 + n^2] - 1\}$

$\{M\}$ $[N]$ $\{P\}$

1	1	0	1	0	1
2	3	1	5	4	2
3	5	4	13	12	3
4	7	9	25	24	4
5	9	16	41	40	5
6	11	25	61	60	6
7	13	36	85	84	7
8	15	49	113	112	8
9	17	64	145	144	9
10	19	81	181	180	10
11	21	100	221	220	11
12	23	121	265	264	12
13	25	144	313	312	13
14	27	169	365	364	14
15	..	196	...	...	15
..	..	...	...	...	..

n = 0, 1, 2, 3, 4, 5, ..., ecc., ...

SOMMARIO. Viene illustrata la possibilità che la tecnica di lavoro legata all'"Analisi crittografica", sia impiegabile in campi della ricerca, che, poco, sembrano avere in comune con la "Crittografia". Come esempio di realizzazione di tale possibilità vengono presentati i risultati ottenuti nello studio dell'equazione a numeri interi: $M^2 = N^2 - P^2$

RATIO MATH. 1.
(1990), 133 - 138

Di Tassi e di Tasse

Lorenzo Peccati
Università degli studi di Torino e Università "L.Bocconi" di Milano

0. INTRODUZIONE

L'uso di un metodo ([1]), proposto dallo scrivente, per lo svolgimento di interessanti analisi finanziarie sia di singole operazioni, sia di portafogli di operazioni, conduce a cercare sotto quali condizioni la messa in conto delle imposte non alteri troppo la struttura dell'insieme dei tassi interni di un'operazione finanziaria.

Nel n. 1 il problema sarà impostato, nel n. 2 si forniscono semplici condizioni sufficienti affinché l'eccessiva alterazione non avvenga. Nel n. 3 si indicano alcune direzioni di approfondimento promettenti.

1. IL PROBLEMA

Si consideri un'operazione finanziaria (o.f. nel seguito) con funzione cumulativa dei flussi L: $R_+ \to R$ essendo R_+ l'insieme dei numeri reali non negativi. L(t) denota così la somma algebrica dei flussi con scadenza non oltre t. È naturale ([2]) assumere L a variazione limitata su R_+, cosicché si possa pensarla come differenza tra le due funzioni cumulative delle entrate e delle uscite. Assumerò in tutto questo lavoro che su R_+ L sia monotona non decrescente. Altre ipotesi saranno $L(0) = -1$ e $L(+\infty) < +\infty$.

Il Discounted Cash-Flow per tale o.f. è:

$$G(\delta) = -1 + \int_0^{+\infty} exp(\delta t)\, dL(t)$$

intendendo l'integrale nel senso di T.J. Stieltjes. La funzione $\Gamma(\delta)$ sarà definita per $\delta > \delta_o$. Assumerò $\delta = -\infty$. È evidente che da $G(0) = L(+\infty) > 0$ e da $G(+\infty) = -1$ discende l'esistenza di almeno un tasso interno δ^* per l'o.f. La monotonia di G ne garantisce l'unicità.

Tutto questo "prima delle tasse". L'effetto dell'impostazione fiscale può essere modellizato, almeno in prima battuta, come segue. Sia $A: R_+ \to R$ la funzione con il seguente significato: A(t) è la parte del costo iniziale (unitario per semplicità) "deducibile" entro t. Assumerò A monotona non decrescente, con $A(+\infty) \leq 1$. Suppongo, altresì che l'"imponibile" sia sempre non negativo, ossia che la funzione differenza $N = L\text{-}A: R_+ \to R$, ovviamente a variazione limitata, sia monotona non decrescente. L'"imponibile" in t è allora dN(t). Su tale "imponibile" viene calcolata l'imposta $\lambda\, dN(t)$. Tale prelievo è materialmente effettuato h(t) unità di tempo più tardi (assumerò dunque $h(t) \geq 0$ anche se in concreto può interessare h di segno qualunque a causa del giuoco degli acconti).

Il valore scontato in 0 dei versamenti a titolo d'imposta sarà:

$$\lambda\, I(\delta) = \lambda \int_0^{+\infty} \exp\left(-\delta\,(t+h)\right)\, dN(t)$$

ove I(t) è il valore scontato in 0 a tasso δ degli "imponibili" relativi all'operazione in esame.

Il DCF "dopo le tasse" riesce allora:

$$\Gamma(\delta) = G(\delta) - \lambda I(\delta)$$

Grossolanamente si può descrivere l'effetto delle imposte dicendo che abbassano i valori di Γ rispetto a G e pertanto la radice δ^* diventa $\delta^{**} < \delta^*$. Tale tasso δ^{**} è proprio quello che serve per l'applicazione del metodo proposto dallo scrivente ([3]).

In realtà il problema non è così semplice perché il passaggio da G a Γ altera la struttura dell'insieme dei tassi interni per l'o.f.. Si può, per esempio, elementarmente provare ([4]) che se gli ultimi flussi dell'o.f. "dopo le tasse" sono imposte allora anche se G ammette, come nel nostro caso, una sola radice δ^* e se, sperabilmente, le imposte non si portano via tutto il profitto, allora Γ ne ammmette almeno due, la minore delle quali, δ_o, è negativa. L'interpretazione di δ_o è piuttosto evidente: l'o.f. "dopo le tasse" acquista un segmento terminale con natura di finanziamento il cui tasso si riflette in δ_o. Di ciò ci si può

convincere studiando il DCF di un'operazione modificata ove si sostituiscono ai valori L(t) i valori $1 + L(t)$.

Dal punto di vista che m'interessa in questa sede la radice δ_0 non provoca alcun fastidio, nel senso che δ^{**} è il tasso da utilizzare per lo svolgimento dell'analisi economico-finanziaria citata. Altro paio di maniche se tra 0 e δ^* cadesse più di una radice di Γ. Che questo possa accadere per i livelli di λ sufficientemente elevati non può, per quanto so, essere escluso. Intendo fornire condizoni sufficienti acciocché questo non accada, ossia, affinchè $\Gamma(\delta) = G(\delta)-\lambda I(\delta)$ possegga un solo zero δ^{**} tale che $0 \leq \delta^{**} \leq \delta^*$. Per $\lambda = 0$ questo è banalmente garantito, interessa dunque studiare il problema per $0 < \delta^{**} \leq \delta^*$. Sarà naturale cercare limitazioni superiori per λ affinché sia garantita tale unicità. Altre interessanti limitazioni potranno venire dalla richiesta che i pagamenti delle imposte non siano troppo lontani nel tempo dalle epoche di conseguimento dei redditi che le determinano.

2. CONDIZIONI SUFFICIENTI

Da:

$$G(\delta) = -1 + \int_0^{+\infty} exp(-\delta t)\, dL(t)$$

si trae con facili calcoli che su ogni intervallo $(\eta, +\infty)$, con $\eta > 0$, G è differenziabile e riesce:

$$G'(\delta) = -\int_0^{+\infty} t\ exp(-\delta t)\, dL(t)$$

Sarà, come già osservato, $G'(\delta) < 0\ \forall\ \delta \in (0, +\infty)$.

Analogamente si ottiene:

$$G''(\delta) = \int_0^{+\infty} t^2\ exp(-\delta t)\, dL(t)$$

Risulta, nelle nostre ipotesi, $G''(\delta) > 0$. E, già dalla negatività di $G'(\delta)$ scende esistenza ed unicità di δ^*.

Da:

$$I(\delta) = \int_0^{+\infty} \exp\left(-\delta\,(t + h(t))\right)\, dN(t)$$

si ha facilmente:

$$I'(\delta) = -\int_0^{+\infty} (t + h(t)) \exp\left(-\delta\,(t + h(t))\right)\, dN(t)$$

$$I''(\delta) = -\int_0^{+\infty} (t + h(t))^2 \exp\left(-\delta\,(t + h(t))\right)\, dN(t)$$

Se ne trae $I'(\delta) < 0$, $I''(\delta) > 0$.

Una prima semplice condizione sufficiente per l'unicità di δ^{**} in $(0,\delta^{*})$ è la negatività di $\Gamma'(\delta)$ su tale intervallo.

Poiché: $\Gamma'(\delta) = G'(\delta) - \lambda I'(\delta)$, osservato che, con riferimento all'intervallo da 0 a δ^{*}, la funzione G' è minima in δ^{*} e la funzione I' è massima in 0, $\Gamma'(\delta) < 0$ sull'intervallo rilevante se:

$$G'(\delta^{*}) - \lambda I'(0) \leq 0$$

ossia se:

$$\lambda \leq \lambda^{*} = G'(\delta^{*}) / I'(0)$$

È ben noto che $G'(\delta^{*})$ coincide con $\Delta_L(\delta^{*})$, la duration a tasso δ^{*} del cash-flow in entrata dell'impiego. Si ha poi:

$$I'(0) = -\int_0^{+\infty} (t + h(t))\, dN(t)$$

e per il confine superiore λ^{*} per λ vale la rappresentazione

$$\lambda^{*} = \frac{\Delta_L(\delta^{*})}{\int_0^{+\infty} (t + h(t))\, dN(t)}$$

Il denominatore può scriversi anche come prodotto della scadenza media aritmetica τ delle imposte moltiplicata per l'imponibile totale. Tale scadenza media aritmetica è ponderata con gli imponibili (o, che è lo stesso, con le imposte):

$$\int_0^{+\infty} (t + h(t))\, dN(t) = \tau\, (N(+\infty)) - (N(0)) = \tau\, N(+\infty)$$

La condizione trovata è sicuramente semplice, ma potrebbe essere troppo restrittiva. Essa, infatti, impegna l'andamento di Γ su tutto l'intervallo $(0,\delta^*)$. Si ottiene una condizione meno esosa chedendo che in ogni radice δ^{**} in tale intervallo riesca $\Gamma'(\delta^{**}) < 0$.

Da $G'(\delta^{**})-\lambda I(\delta^{**}) < 0$, atteso che $G(\delta^{**})-\lambda I(\delta^{**}) = 0$, si ottiene, rammentato quanto sappiamo sui segni di G e I:

$$D \ln G(\delta^{**}) < D \ln I(\delta^{**})$$

ove D indica derivazione rispetto al tasso. Quest'ultima condizione può essere riscritta in maniera interessante in termini di durate medie finanziarie dei ricavi provenienti dall'operazione principale e di flussi di cassa da imposte.

Basta osservare che:

$$D \ln G(\delta) = G'(\delta) / G(\delta) = -\Delta_L(\delta)(1 + G(\delta)) / G(\delta)$$

e che:

$$D \ln I(\delta) = -\Delta_I(\delta)$$

ove $\Delta_I(\delta)$ è la duration a tasso δ del cash-flow delle imposte.

La condizione di negatività di Γ in ogni punto δ^{**} ove sia anche $\Gamma(\delta^{**}) = 0$, si riduce a:

$$\Delta_I(\delta^{**}) < \Delta_L(\delta^{**})(1 + G(\delta^{**})) / G(\delta^{**})$$

di interpretazione finanziaria estremamente facile. Se la prima condizione data garantiva l'unicità di δ^{**} chiedendo che le imposte non fossero troppo alte, questa chiede che non siano troppo differite nel tempo.

Da quest'ultima condizione si possono trarre criteri di semplici applicazioni minorando il secondo membro e maggiorando il primo. Una

minorazione per il secondo membro può ottenersi osservando che $\Delta_L(\delta^{**})$ non può essere inferiore a $\Delta_L(\delta^*)$ e che l'altro fattore supera certamente $1/G(0) = 1/L(+\infty)$. Osservato altresì che il primo membro della disuguaglianza è maggiorato dalla scadenza media aritmetica delle entrate $z = \int_0^{+\infty} t\,dN(t)/N(+\infty)$, *basta che:*

$$z < \Delta_L(\delta^*)/L(+\infty)$$

Quest'ultima condizione appare invero di agevole controllo.

3. ULTERIORI DIREZIONI DI RICERCA

Appare di un certo interesse considerare profili L che ben descrivono operazioni finanziarie concrete, funzioni di ritardo (o anticipo, a causa degli acconti) h e controllare attraverso le due condizioni indicate, o altre ancora, se sia per essi garantita l'unicità del tasso interno positivo "dopo le tasse".

NOTE

([1]) Peccati (1987), Cerquetti (1988), Peccati (1989), Peccati (1990).

([2]) Si veda Castagnoli, Peccati (1973).

([3]) Peccati (1989)., Peccati (1990).

([4]) Castagnoli (1983)

BIBLIOGRAFIA

E. CASTAGNOLI, L.PECCATI (1973): 'Alcune osservazioni sulla classificazione degli investimenti'. Giornale degli Economisti e Annali di Economia.

E. CASTAGNOLI (1983): 'Di tassi e di tasse'. Notiziario Economico Bresciano.

A .CERQUETTI (1988): 'Tassi medi di rendimento di obblogazioni singole e in portafoglio'. Pubblicazioni dell'Istituto di Matematica, Un. degli studi "G.D'Annunzio", Fac. di Econ. e Comm., Chieti.

L .PECCATI (1987): 'DCF e risultati di periodo'. Atti dell'XI Convegno AMASES, Torino-Aosta.

L .PECCATI (1989): 'La misurazione del rendimento medio di un portafoglio', in corso di stampa.

L. PECCATI (1990): 'Valutazioni finanziarie analitiche e sintetiche', in corso di stampa nei "Quaderni della Rivista Milanese di Economia".

RATIO MATH. 1.
(1990), 139-161

SULLA INTEGRAZIONE DELLA EQUAZIONE SEMPLIFICATA DEL MOTO VARIO DI UNA FALDA FREATICA.

Aniello Russo Spena e Maria Teresa Todisco

Dipartimento di Ingegneria delle Strutture, delle Acque e del Terreno
Università di L'Aquila

1. - INTRODUZIONE.

Per caratterizzare il regime idraulico di una falda acquifera, usualmente, vengono assunte le variazioni cui sono soggette, in ciascun luogo, le quote della superficie libera (o di quella piezometrica) della falda stessa.

Tuttavia, nelle situazioni più frequenti, stabilire per via diretta le connessioni tra tali quote e i fattori che ne determinano le variazioni è praticamente impossibile poichè, in genere, non si riesce a precisare in modo sicuro, sia l'entità e le modalità degli afflussi alla falda, sia le minute condizioni fisico-geologiche dell'ammasso sede della circolazione idrica.

Di fronte a queste difficoltà, gli studi di carattere generico sulle falde vengono limitati alla ricerca, per semplice raffronto, delle connessioni tra il regime dei livelli della falda e quello degli afflussi di maggiore importanza e più facilmente osservabili (piogge e irrigazioni).

Per questa via si giunge, effettivamente, a porre in evidenza le manifestazioni globali dei caratteri fondamentali dei regimi delle falde e, in particolare, il loro "potere regolatore" [1].

Quando però sia necessario prevedere gli effetti indotti sul regime delle falde da opere particolari (opere di ravvenamento o di captazione, ad esempio), non è sufficiente limitarsi ad individuare i legami di connessione poco sopra richiamati: in questi casi, infatti, è necessario valutare la efficacia, la estensione e la prontezza di risposta del sistema filtrante al particolare provvedimento adottato.

Tale valutazione, quando le velocità in gioco sono sufficientemente piccole, una volta definito il sistema liquido-mezzo poroso, può essere conseguita basandosi sulla relazione lineare di Darcy:

$$\vec{v} = k \nabla \varphi \tag{1}$$

In essa, $\vec{v}$ e k rappresentano rispettivamente, la velocità (apparente) di filtrazione e la conducibilità idraulica [1] ; φ è una funzione scalare detta potenziale del campo del vettore $\vec{v}$ e, al pari di questo, è definito anche nei punti interni alla struttura solida del sistema.

Per un mezzo poroso saturo, interessato dal flusso di un liquido omogeneo pesante, il potenziale φ è costituito dalla somma del potenziale gravitazionale φ_g e del potenziale delle pressioni φ_p: espresso in termini di energia per unità di peso, esso assume le dimensioni di una lunghezza e viene a coincidere con il carico piezometrico apparente $(z + p/\gamma)$.

Nei punti interni al dominio spaziale Ω occupato dal liquido (incomprimibile) in moto molto lento, la (1), unitamente alla equazione di continuità:

$$\nabla \cdot \vec{v} = 0 \tag{2}$$

(scritta per un mezzo poroso caratterizzato da microstruttura geometrica interna rigida), fornisce

$$\nabla^2 \varphi = 0 \tag{3}$$

[1] Se il mezzo poroso è isotropo, k è uno scalare; in presenza di anisotropia, k è un tensore doppio simmetrico e il vettore $\vec{v}$ è dato dal prodotto del tensore k per il vettore $\nabla\varphi$ [6]. Nel seguito verranno considerati solo mezzi porosi isotropi.

La (3) indica che i moti dei liquidi filtranti rientrano nella vasta categoria dei fenomeni retti dalla equazione di Laplace e che la determinazione delle caratteristiche dinamiche (velocità e pressioni) nei diversi punti del dominio può essere ricondotta alla determinazione del potenziale φ compatibile con le condizioni vigenti sul contorno del dominio stesso.

Per individuare, dunque, un'unica soluzione della (3) è necessario associare ad essa le condizioni imposte lungo il contorno dell'ammasso filtrante.

In regime stazionario sulla parte di contorno costituita da linee di flusso, queste ultime si riducono a porre uguali a zero le componenti normali delle velocità (ovvero, equivalentemente, ad annullare la derivata normale di φ); lungo le superfici limite attraverso cui si perfeziona l'alimentazione del sistema, il potenziale φ deve assumere valore costante; lungo la superficie di sbocco, infine, occorre tener conto del fenomeno denominato dal De Marchi [3],[9] "sorgente sospesa".

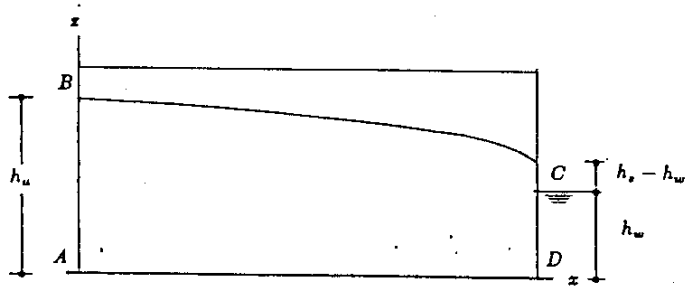


Fig.1 - *Moto stazionario di filtrazione.*

Con riferimento al caso di moto stazionario di filtrazione nel piano (x, z) - fig.1 - di una falda freatica delimitata inferiormente da un piano impermeabile orizzontale e da fronti estremi (di alimentazione e di sbocco) verticali, con i simboli di figura, le condizioni al contorno richiamate sono espresse analiticamente dalle seguenti relazioni:

· lungo il paramento di imbocco AB, per il tratto di altezza h_a:

$$\varphi = h_a \qquad ovvero: \qquad p = \gamma(h_a - z) \tag{4a}$$

· lungo il paramento di sbocco DC, per il tratto di altezza h_w:

$$\varphi = h_w \qquad ovvero: \qquad p = \gamma(h_w - z) \tag{4b}$$

e, per il tratto $(h_s - h_w)$ sede della sorgente sospesa:

$$\varphi = z \qquad ovvero: \qquad p = 0 \tag{4c}$$

· lungo la linea di fondo (orizzontale) AD:

$$\frac{\partial \varphi}{\partial z} = 0 \qquad ovvero: \qquad \frac{\partial p}{\partial z} = -\gamma \tag{4d}$$

Più complessa è la condizione da imporre sulla superficie libera della falda: la sua posizione, infatti, non è nota a priori sicchè sarà necessario preliminarmente individuare ulteriori condizioni indipendenti atte a determinarla. Queste vengono definite, in genere, prescindendo dalla presenza della cosidetta "frangia capillare" (immaginando cioè che un netto contorno separi lo spazio occupato dal liquido in movimento da quello soprastante), e ammettendo che, in ogni punto di tale contorno (coincidente peraltro con una linea di flusso, essendo il moto permanente), la pressione relativa sia nulla e che, in nessun punto esso possa essere attraversato da fluido.

Nel caso che si esamina (falda freatica poggiante su un letto impermeabile orizzontale) la prima condizione dà:

$$p = 0 \qquad ovvero: \qquad \varphi = h(x) \tag{4e}$$

(essendo $h(x)$ la quota del generico punto della superficie libera misurata a partire dal piano orizzontale impermeabile di sostegno della falda); la seconda condizione si traduce invece [8] nella:

$$\frac{\partial p}{\partial z} = -\gamma sen^2(nx) \tag{4f}$$

ovvero, equivalentemente, nella:

$$\frac{\partial p}{\partial x} = -\gamma sen(nx)cos(nx) \tag{4g}$$

avendo denotato con n la normale " esterna " (orientata, cioè, verso l'esterno del dominio occupato dal liquido in movimento) in ogni punto della linea libera.

In condizioni di moto vario il potenziale φ è funzione anche del tempo sicchè la sua determinazione, in ogni istante $t > t_0$ (con

t_0 istante da cui si inizia a contare il tempo) e in ogni punto del campo, richiede che siano definiti i confini geometrici del dominio Ω - e, in particolare, della linea libera - nonchè le condizioni cui deve soddisfare φ su tali confini.

Tali condizioni possono essere definite agevolmente, in base a considerazioni fisiche analoghe a quelle esposte per il caso stazionario, sulle superfici impermeabili ed equipotenziali; sulla linea libera invece - la cui posizione varia continuamente nel tempo e non coincide pertanto con una linea di flusso - la $(4f)$ - o la $(4g)$ - andranno sostituite con la relazione (dedotta mediante l'equazione di continuità [12]):

$$\frac{\epsilon}{k}\frac{\partial h}{\partial t} = \frac{\partial \varphi}{\partial x}\frac{\partial h}{\partial x} - \frac{\partial \varphi}{\partial z} \qquad (4h)$$

che rappresenta la equazione differenziale del moto della superficie libera della falda; in essa ϵ denota la porosità del mezzo assunta costante in Ω e indipendente dal tempo.

Soluzioni rigorose e complete per via analitica della (3), con le condizioni al contorno (e iniziali, per regime non stazionario) descritte, nella maggior parte dei casi di interesse applicativo, sono praticamente da escludere: si presenta, di conseguenza, come inevitabile il ricorso a metodi di calcolo approssimati basati, ordinariamente, sulla discretizzazione della equazione di campo o del dominio fisico.

Nell'applicazione di questi metodi, sia in regime stazionario che vario, la definizione della posizione della superficie libera della falda potrà essere determinata per approssimazioni successive [7].

Una semplificazione consistente del problema può essere ottenuta quando le variazioni di φ lungo la verticale sono modestissime (e conseguentemente modestissimo è il valore della componente verticale della velocità in ogni punto di Ω) e si possono considerare praticamente indipendenti dalla quota del punto considerato le componenti orizzontali della velocità di filtrazione (ipotesi di Dupuit-Forchheimer).

Con queste assunzioni la posizione:

$$\varphi(x, z, t) = h(x, t) \qquad (5)$$

riuscendo valida non solo sulla superficie libera ma in tutti i punti del dominio Ω, consente di ricondurre il problema alla determinazione della sola funzione $h(x, t)$.

Infatti, dalla (3), si ha:

$$\int_0^{h(x,t)} \frac{\partial^2 \varphi}{\partial z^2} dz = -\int_0^{h(x,t)} \frac{\partial^2 \varphi}{\partial x^2} dz$$

ma:

$$\int_0^{h(x,t)} \frac{\partial^2 \varphi}{\partial z^2} dz = \frac{\partial \varphi}{\partial z} \quad ; \quad \int_0^{h(x,t)} \frac{\partial^2 \varphi}{\partial x^2} dz = h \frac{\partial^2 h}{\partial x^2}$$

onde:

$$\frac{\partial \varphi}{\partial z} = -h \frac{\partial^2 h}{\partial x^2} \tag{6}$$

Introdotta la (6) nella (4h) otteniamo, in definitiva:

$$\frac{\epsilon}{k} \frac{\partial h}{\partial t} = \frac{\partial}{\partial x} \left(h \frac{\partial h}{\partial x} \right) \tag{7}$$

La (7) rappresenta non solo la condizione da imporre sulla superficie libera della falda bensì, come anticipato, anche l'equazione differenziale alle derivate parziali che descrive il processo di moto vario allo studio; essa può essere facilmente generalizzata per il caso di moto vario di una falda freatica poggiante su un piano impermeabile inclinato dell'angolo α sull'orizzontale (fig.2).

Posto infatti:

$$\varphi(x, z, t) = z_f(x) + h(x; t) \tag{8}$$

(essendo $z_f(x)$ la quota del generico punto appartenente al piano di sostegno e $h(x,t)$ la quota del pelo libero della falda misurata verticalmente a partire dallo stesso piano) dalla (3) discende

$$\int_{z_f}^{z_f+h} \frac{\partial^2 \varphi}{\partial z^2} dz = -\int_{z_f}^{z_f+h} \frac{\partial^2 \varphi}{\partial x^2} dz$$

e quindi:

$$\frac{\partial \varphi}{\partial z} = -h \frac{\partial^2 h}{\partial x^2} \tag{9}$$

Introdotta la (9) nella (4h), posto $i_f = -\frac{dz_f}{dx}$, si ha:

$$\frac{\epsilon}{k} \frac{\partial h}{\partial t} = \frac{\partial}{\partial x} \left(h \frac{\partial h}{\partial x} \right) - i_f \frac{\partial h}{\partial x} \tag{10}$$

La (10) è la nota equazione di Boussinesq [2]: essa implica che le sezioni trasversali della falda possono essere considerate piane e che i filetti liquidi, in cui è possibile scomporre la massa fluida in movimento, sono sensibilmente paralleli alla retta di fondo.

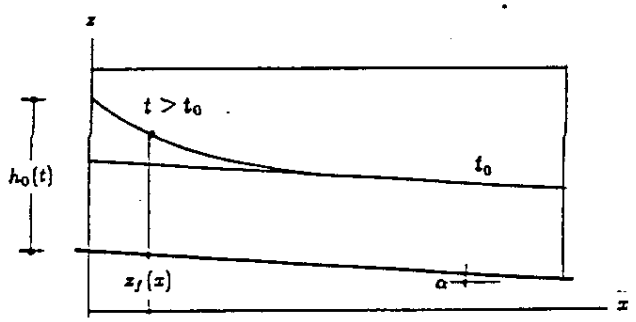


Fig.2 -*Falda su piano di sostegno inclinato.*

Per valori della pendenza $i_f \neq 0$, lo spessore effettivo della falda, misurato secondo la normale al fondo stesso, differisce dal valore di h misurato secondo la verticale della quantità $\Delta h = h\sqrt{1 - i_f^2}$; lo scostamento percentuale $\Delta h/h$ assume valori dell'ordine di 0.001 quando $i_f = 4.5\%$ e valori dello 1% quando i_f è pari al 14% [4]: pendenza questa non frequente nelle situazioni pratiche.

Ciò comporta, come ulteriore semplificazione, la possibilità di considerare le sezioni trasversali della falda, oltre che piane, verticali e di esprimere la portata q, in un generico istante e in una generica sezione trasversale, nella forma [2] :

$$q = -kh\left(\frac{\partial h}{\partial x} - i_f\right) \qquad (10a)$$

Alla (10) conviene dare una forma diversa, più comoda ai fini dell'esame e della discussione di alcuni fenomeni cui faremo cenno

[2] Nella (10a) la quantità $i_f - \partial h/\partial x$ rappresenta la "cadente piezometrica": essa, per piccoli valori di i_f, coincide con l'inclinazione della superficie freatica sull'orizzontale.

nel seguito: posto, allo scopo, genericamente in essa:

$$D(h) = \frac{k}{\epsilon}h \qquad ; \qquad K(h) = i_f \frac{k}{\epsilon}h \tag{11a}$$

e osservato che:

$$\frac{dK(h)}{dh} = i_f \frac{k}{\epsilon} = C_0 \tag{11b}$$

la (10) viene formalmente a coincidere con la "equazione della diffusione":

$$\frac{\partial h}{\partial t} = \frac{\partial}{\partial x}\left[D(h)\frac{\partial h}{\partial x}\right] - C_0 \frac{\partial h}{\partial x} \tag{12}$$

a sua volta, completamente analoga alla "equazione della conduzione termica" [3] .

La (12) è un'equazione differenziale, quasi lineare, di tipo parabolico - con coefficiente $D(h)$ funzione lineare di h e coefficiente $C_0 = i_f k/\epsilon$ costante per il caso di processi di filtrazione in mezzi porosi saturi - la cui soluzione, per fissate condizioni iniziali e al contorno, può essere ottenuta solo con l'ausilio del calcolo numerico.

Le condizioni iniziali (all'istante t_0 assunto come origine dei tempi) per la funzione $h(x,t)$ vengono usualmente assegnate nella forma:

$$h(x,t_0) = f(x)$$

con $x\epsilon[0,l]$ e $f(x)$ funzione nota generalmente continua; le condizioni agli estremi $x = 0$ e $x = l$, ordinariamente, vengono assegnate in relazione ai regimi temporali ivi imposti alla funzione $h(x,t)$, o alla sua derivata, o alla relazione tra la funzione stessa e la sua derivata. Naturalmente agli estremi del dominio possono prevedersi combinazioni diverse di queste condizioni sicchè, anche limitando ad esse lo studio dei processi di moto vario retti dalla (12), il numero di casi di esaminare diviene notevolmente grande.

Le condizioni richiamate si riferiscono a domini "limitati" di lunghezza l; quando l assume valori tali che gli effetti indotti dalle condizioni imposte ad un estremo (per esempio l'estremo $x = 0$) non si risentono in misura apprezzabile - almeno per tutti gli istanti t compresi nell'intervallo di tempo durante il quale si studia il processo

[3] Allorchè il coefficiente k non è costante ma, come avviene nei processi di filtrazione nei mezzi non saturi, è funzione della pressione della fase liquida, il termine C_0 diviene funzione di h.

di moto - nelle zone in cui la funzione h è determinata dalle sole condizioni iniziali, sarà lecito supporre il dominio "illimitato da un lato" ed ammettere che la variabile spaziale possa assumere tutti i valori $x\epsilon[0,\infty[$.

Questa situazione rappresenta un caso "degenere" dei problemi ai limiti; un altro caso degenere, di notevole portata applicativa, si ha quando possono essere trascurate, ai fini dello studio, le condizioni iniziali ("problemi ai limiti senza condizioni iniziali"): questa circostanza si verifica ogni volta che l'istante t in corrispondenza del quale interessa conoscere la funzione $h(x,t)$ è tanto lontano da quella iniziale t_0 da poter ritenere che la distribuzione delle h sia determinata dalle sole condizioni al contorno.

Per superare gli ostacoli analitici che si frappongono alla soluzione in termini finiti della (12), basterà sostituire in essa, alla funzione $D(h)$ un valore D_0 costante opportunamente scelto: con tale posizione, infatti, essa si semplifica nella equazione linearizzata (a coefficienti costanti):

$$\frac{\partial h}{\partial t} = D_0 \frac{\partial^2 h}{\partial x^2} - C_0 \frac{\partial h}{\partial x} \tag{13}$$

ovvero, nel caso di falda poggiante su piano di sostegno orizzontale ($i_f = 0$ e quindi $C_0 = 0$), nella

$$\frac{\partial h}{\partial t} = D_0 \frac{\partial^2 h}{\partial x^2} \tag{14}$$

per le cui soluzioni è possibile avvalersi di metodi noti nel campo della fisica matematica.

E' evidente che la (13) e la (14) sono aderenti alla realtà del fenomeno di moto vario che si studia solo se possono ritenersi verificate le ipotesi poste a base del procedimento di linearizzazione: quando ciò non avviene, le approssimazioni introdotte possono conferire ai risultati dei calcoli significato di semplice orientamento. Tuttavia, anche per questi casi, le soluzioni analitiche delle (13) e (14) si presentano come un mezzo prezioso - e, sovente, insostituibile - per la messa a punto di procedimenti numerici e per il controllo delle relative soluzioni.

2. - PROCEDIMENTI DI CALCOLO.

I procedimenti di calcolo per la risoluzione delle equazioni richiamate, quando la $h(x,t)$ è definita nel dominio limitato $x\epsilon[0,l]$, sono sufficientemente noti; per domini illimitati da un lato - $x\epsilon[0,\infty[$ - o per domini illimitati da entrambi i lati - $x\epsilon]-\infty,+\infty[$ -, tali schemi di risoluzione devono essere opportunamente modificati anche in relazione alle condizioni iniziali e al contorno assegnate.

Per inquadrare questi schemi è comodo riferirsi al caso semplice di una falda freatica (*fig.3*) in quiete entro un ammasso poroso omogeneo ed isotropo nei riguardi della conducibilità k, poggiante su un piano di sostegno impermeabile, orizzontale, limitato da un lato da una parete verticale permeabile per tutta l'altezza (" fronte di alimentazione").

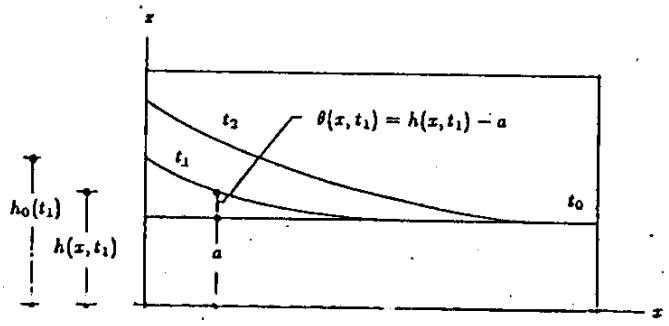


Fig.3 - *Andamento a carattere qualitativo dei profili superficiali della falda in istanti diversi.*

Si riferisca il sistema ad una coppia di assi cartesiani ortogonali avente l'asse x orizzontale e l'asse z verticale e diretto verso l'alto; la lunghezza dell'ammasso sia indefinita nel campo delle ascisse x positive; si indichi altresì con "a" lo spessore iniziale della falda e si assuma infine unitaria la larghezza dello strato permeabile nella direzione perpendicolare al piano x,z.

Si supponga ora che, nel sistema così definito e all'istante $t_0 = 0$ assunto come origine dei tempi, in corrispondenza del fronte di alimentazione $(x = 0)$ venga immessa una portata q costante.

In tale situazione, al trascorrere del tempo, il livello idrico all'ascissa $x = 0$ si innalza progressivamente e, contemporaneamente, il

profilo superficiale si solleva e tende asintoticamente al profilo orizzontale della falda.

Nella *fig.*3, a titolo d'esempio, sono riportati i profili di pelo libero della falda nei due istanti t_1 e t_2 successivi; dalla stessa figura è immediato evincere la condizione iniziale:

$$h(x,0) = h_0 = a \tag{15}$$

e la condizione all'ascissa $x \to \infty$, $\forall t > 0$:

$$h(\infty,t) = a \tag{16}$$

Più complessa è la condizione da imporre all'ascissa $x = 0$: qui infatti, è assegnato il valore della portata q immessa: a norma della legge di Darcy, tenuto conto delle ipotesi di Dupuit-Forchheimer, tale portata, è data da:

$$q(0,t) = -kh(0,t)\left(\frac{\partial h}{\partial x}\right)_{x=0} \tag{17}$$

La (17) è non lineare; tuttavia, se nello spirito delle approssimazioni fino ad ora adottate, si ammette che i sopraelevamenti $\theta = [h(x,t) - a]$ del pelo libero siano in ogni istante t e per ogni x (e in particolare per $x = 0$) piccoli in confronto ad a, posto $q_0 = q(0,t)$,sarà lecito approssimare la (17) con la:

$$q_0 = -ka\left(\frac{\partial h}{\partial x}\right)_0 \tag{18}$$

Con questa posizione il problema si riporta a trovare una funzione $h(x,t)$ tale che la sua derivata nella direzione della normale al contorno $x = 0$ si riduca, ivi, ad una funzione (in particolare, ad una costante) assegnata (problema di Neumann).

Un semplice artificio consente peraltro di ricondurre il problema posto alla determinazione di una nuova funzione nel dominio $[0,\infty[$ che, al contorno $x = 0$ assume un valore prefissato (problema di Dirichlet).

Infatti, se si derivano il primo e secondo membro della (14) rispetto a x, tenuto conto della approssimazione $q(x,t) = -ka\partial h/\partial x$, con passaggi immediati si deduce:

$$\frac{\partial q}{\partial t} = D_0 \frac{\partial^2 q}{\partial x^2} \tag{19}$$

Per essa le condizioni iniziali e al contorno si scrivono:

$$q(x,0) = 0 \tag{20}$$

$$q(\infty,t) = 0 \tag{21}$$

$$q(0,t) = q_0 \tag{22}$$

La soluzione della (19) con le (20), (21) e (22), può essere trovata agevolmente avvalendosi del cambiamento di variabile (trasformazione di Boltzmann):

$$\xi = \frac{x}{\sqrt{t}} \tag{23}$$

Infatti, introdotta la (23) nella (19), questa si trasforma nella equazione differenziale ordinaria, del secondo ordine, omogenea a coefficienti variabili:

$$\frac{d^2q}{d\xi^2} + \frac{\xi}{2D_0}\frac{dq}{d\xi} = 0 \tag{24}$$

che con le condizioni iniziali e al contorno, a loro volta specializzate nelle:

$$q(\xi = 0) = q_0$$

$$q(\xi \to \infty) = 0$$

ammette l'integrale particolare:

$$q(\xi) = q_0 erfc\frac{\xi}{2\sqrt{D_0}} \tag{25}$$

in cui $erfc(\cdot)$ è la funzione complementare di Gauss.

La (25), scritta in termini di x e t diviene:

$$q(x,t) = q_0 erfc\frac{x}{2\sqrt{D_0 t}} \tag{26}$$

ovvero, quando la condizione in $x = 0$ è fissata all'istante $t_0 \neq 0$:

$$q(x,t) = q_0 erfc\frac{x}{2\sqrt{D_0(t-t_0)}} \tag{27}$$

Quest'ultima, tenuto conto che è anche : $q(x,t) = -ka\partial h/\partial x$ consente la determinazione della funzione cercata $h(x,t)$. Indicata, infatti, al solito, con $\theta(x,t)$ la differenza $h(x,t) - a$, risulta:

$$\theta(x,t) = 2\sqrt{D_0 t}\frac{q_0}{ka} ierfc\frac{x}{2\sqrt{D_0 t}} \tag{28}$$

dove

$$ierfc\frac{x}{2\sqrt{D_0 t}} = \int_{\frac{x}{2\sqrt{D_0 t}}}^{\infty} erfc\alpha d\alpha = \frac{1}{\sqrt{\pi}} e^{-\alpha^2} - \alpha erfc\alpha$$

è l'integrale della funzione complementare degli errori.

Della soluzione (26) ci si può avvalere anche per la ricerca dell'andamento della funzione $h(x,t)$ determinata dall'immissione, in $x = 0$, di una portata $q(0,t)$ variabile in modo generico con il tempo.

Per illustrare le modalità della sua utilizzazione è conveniente riferirsi al caso in cui la funzione $q(0,t)$, in $x = 0$, abbia l'andamento di un "impulso rettangolare", ossia:

$$q(0,t) = \begin{cases} 0 & \text{per } t < t_0 \\ q_0 & \text{per } t_0 \leq t_1 \\ 0 & \text{per } t > t_1 \end{cases}$$

Posto, per semplicità di scrittura:

$$g(x, t - t_0) = erfc\frac{x}{2\sqrt{D_0(t - t_0)}}$$

tenuto conto della (27) risulta, $\forall t \geq t_1$:

$$q(x,t) = q_0 \left[g(x, t - t_0) - g(x, t - t_1)\right] \tag{29}$$

e

$$\theta(x,t) = 2\sqrt{D_0}\frac{q_0}{ka}\left[\sqrt{t - t_0} ierfc\alpha_0 - \sqrt{t - t_1} ierfc\alpha_1\right] \tag{30}$$

Allorchè la $q(0,t)$ è assegnata in forma generica, sarà lecito scomporla nella seguente serie di impulsi rettangolari:

$$q(0,t) = \begin{cases} q_0 & \text{per } t_0 < t \leq t_1 \\ q_1 & \text{per } t_1 < t \leq t_2 \\ \vdots & \\ q_{n-1} & \text{per } t_{n-1} < t \leq t_n \end{cases}$$

sicchè, in analogia a quanto esposto per il caso di un impulso rettangolare unico, si ha, per il primo impulso:

$$q(x,t) = q_0 \left[g(x,t-t_0) - g(x,t-t_1)\right]$$

per il secondo impulso:

$$q(x,t) = q_0 \left[g(x,t-t_0) - g(x,t-t_1)\right] + q_1 \left[g(x,t-t_1) - g(x,t-t_2)\right]$$

e quindi, generalizzando:

$$q(x,t) = \sum_{i=0}^{n-2} q_i \left[g(x,t-t_i) - g(x,t-t_{i+1})\right] \tag{31}$$

da cui, infine:

$$\theta(x,t) = \frac{2}{ka} \sum_{i=0}^{n-1} \sqrt{D_0} q_i \left[\sqrt{t-t_i}\, ierfc\alpha_i - \sqrt{t-t_{i+1}}\, ierfc\alpha_{i+1}\right] \tag{32}$$

Il procedimento descritto può essere generalizzato per lo studio dei processi di moto retti dalla (13).

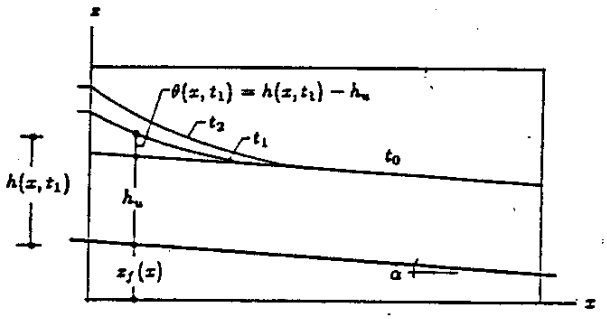


Fig.4 - *Andamento a carattere qualitativo dei profili superficiali della falda in istanti diversi.*

A tale scopo si prenda in esame, per fissare le idee, il caso semplice di una falda freatica (*fig.*4) in moto uniforme (caratterizzato

da altezza idrica h_u e portata q_u costanti) entro un ammasso poroso omogeneo ed isotropo nei riguardi della conducibilità k, poggiante su un piano di sostegno impermeabile, inclinato di i_f sull'orizzontale, limitato da un lato da un fronte di alimentazione".

Si riferisca il sistema ad una coppia di assi cartesiani ortogonali avente l'asse x orizzontale e l'asse z verticale e diretto verso l'alto; la lunghezza dell'ammasso sia indefinita nel campo delle ascisse x positive.

Si assuma infine unitaria la larghezza dello strato permeabile nella direzione perpendicolare al piano x, z

Con riferimento ai simboli riportati in figura è immediato evincere la condizione iniziale:

$$h(x,0) = h_u \tag{33}$$

e la condizione all'ascissa $x \to \infty$, $\forall t > 0$:

$$h(\infty,t) = h_u \tag{34}$$

All'ascissa $x = 0$ è assegnato il valore della portata q_0 immessa: a norma della legge di Darcy, tenuto conto delle ipotesi di Dupuit-Forchheimer, tale portata è data da:

$$q(0,t) = kh(0,t)\left(i_f - \frac{\partial h}{\partial x}\right)_{x=0}$$

ovvero, nello spirito delle approssimazioni fino ad ora adottate, da:

$$q_0 = kh_u\left(i_f - \frac{\partial h}{\partial x}\right)_{x=0} \tag{35}$$

In perfetta analogia a come operato per il caso di falda orizzontale, la (13) si trasforma nella:

$$\frac{\partial q}{\partial t} = D_0\frac{\partial^2 q}{\partial x^2} - C_0\frac{\partial q}{\partial x} \tag{36}$$

per la quale le condizioni iniziali e al contorno si scrivono:

$$q(x,0) = q_u \tag{37}$$

$$q(\infty, t) = q_u \tag{38}$$

$$q(0, t) = q_0 \tag{39}$$

Per la risoluzione della (36) con le (37), (38) e (39) poniamo:

$$q(x,t) = w(x,t) exp\left[\frac{C_0 x}{2D_0} - \frac{C_0^2 t}{4D_0}\right] \tag{40}$$

in cui $w(x,t)$ è funzione incognita da determinare.

In base ad essa la (36) si riduce all'equazione differenziale lineare a coefficienti costanti di tipo parabolico:

$$\frac{\partial w}{\partial t} = D_0 \frac{\partial^2 w}{\partial x^2} \tag{41}$$

mentre le condizioni iniziali e al contorno fissate per la $q(x,t)$ risultano modificate. In particolare, la condizione iniziale, sarà espressa da :

$$w(x,0) = C_0 exp\left(-\frac{C_0 x}{2D_0}\right) = f(x) \tag{42}$$

la condizione all'estremo $x \to \infty$, - espressa dalla (38) - e quella all'estremo $x = 0$ - espressa dalla (39) - , diventeranno rispettivamente, $\forall t > 0$:

$$w(\infty, t) = 0 \tag{43}$$

$$w(0,t) = q_0\, exp\left(\frac{C_0^2 t}{4D_0}\right) = p(t) \tag{44}$$

La (44) mostra che, la condizione per la $w(x,t)$ all'estremo $x = 0$ diviene funzione del tempo anche quando il valore q_0 che figura nella (39) è costante.

La soluzione dell'equazione lineare (41), con le condizioni (42), (43) e (44) potrà essere ricercata spezzando la funzione incognita nella somma:

$$w(x,t) = w_1(x,t) + w_2(x,t) \tag{45}$$

in cui $w_1(x,t)$ è soluzione della:

$$\frac{\partial w_1}{\partial t} = D_0 \frac{\partial^2 w_1}{\partial x^2} \tag{46}$$

soggetta alle condizioni:

$$w_1(x,0) = f(x) \tag{47}$$

$$w_1(0,t) = 0 \quad ; \quad w_1(\infty,t) = 0 \tag{48}$$

mentre la $w_2(x,t)$ è soluzione della

$$\frac{\partial w_2}{\partial t} = D_0 \frac{\partial^2 w_2}{\partial x^2} \tag{49}$$

soggetta alle condizioni:

$$w_2(x,0) = 0 \tag{50}$$

$$w_2(0,t) = p(t) \quad ; \quad w_2(\infty,t) = 0 \tag{51}$$

La soluzione della (46) con le condizioni iniziali e al contorno assegnate, è nota [5],[11] ed è fornita dall'integrale:

$$w_1(x,t) = \frac{1}{2\sqrt{\pi D_0 t}} \int_0^\infty \left(e^{-\frac{(x-\xi)^2}{4D_0 t}} - e^{-\frac{(x+\xi)^2}{4D_0 t}} \right) f(\xi)\, d\xi \tag{52}$$

La soluzione della (49) è invece, come già mostrato, fornita da:

$$w_2(x,t) = \sum_{i=0}^{n-2} p\left[g(x,t-t_i) - g(x,t-t_{i+1})\right] + p_{n-1}\, g(x,t_n - t_{n-1}) \tag{53}$$

(in cui $g(x,t-t_i) = erfc(x/(2\sqrt{D_0(t-t_i)}))$) ottenuta schematizzando la $p(t)$ con la funzione a gradini:

$$p(t) = \begin{cases} p_0 & \text{per } t_0 < t \le t_1 = t_0 + \Delta t \\ p_1 & \text{per } t_1 < t \le t_2 = t_1 + \Delta t \\ \vdots & \\ p_{n-1} & \text{per } t_{n-1} < t \le t_n = t_{n-1} + \Delta t \end{cases}$$

dove si è indicato, al solito, con $\Delta t = (t_n - t_0)/n$ - essendo n il numero di parti in cui è diviso l'intervallo $(t_n - t_0)$ - l'ampiezza del gradino.

Tenuto conto della posizione (57) si ha:

$$w(x,t) = \frac{1}{2\sqrt{\pi D_0 t}} \int_0^\infty \left(e^{-\frac{(x-\xi)^2}{4D_0 t}} - e^{-\frac{(x+\xi)^2}{4D_0 t}} \right) f(\xi)\, d\xi +$$

$$+ \sum_{i=0}^{n-2} p_i \left[g(x, t-t_i) - g(x, t-t_{i+1}) \right] + p_{n-1} g(x, t_n - t_{n-1}) \quad (54)$$

Questa, in base alla (40), consente la definizione della $q(x,t)$, da cui si risale per integrazione alla $h(x,t)$.

Naturalmente nulla muta nel procedimento descritto se l'ammasso filtrante si estende indefinitamente nella direzione delle x negative: basterà, in tal caso, introdurre nelle relazioni trovate la trasformazione di variabili $x_1 = -x$.

3. - ESEMPI DI APPLICAZIONI E CONCLUSIONI.

La (54) è stata applicata [4] per lo studio delle situazioni illustrate nelle figg.5a,b, c,d.

Nella fig.5a. in particolare, sono diagrammati i valori assunti dalla funzione $\theta(x,t)$ - relativi ad una falda freatica defluente entro un ammasso poroso caratterizzato dai coefficienti $k = 3.6m/ora$ e $\epsilon = 0.15$, che poggia su un piano di sostegno impermeabile declive nel senso del moto ($i_f = .004$) e indefinitamente esteso nel dominio $x\epsilon[0,\infty[$ - per effetto della immissione della portata costante $q_0 = 3.6m^3/ora/m$ in corrispondenza del fronte di alimentazione posto all'ascissa $x = 0$.

In condizioni di regime la falda è sede di un moto uniforme di portata $q_u = ki_f h_u = 1.44m^3/ora/m$ e altezza $h_u = 100m$.

Dall'esame della fig.5a si rileva che, in ogni istante $t > 0$, la $\partial\theta/\partial x$ è sempre negativa, e tende a zero per $x \to \infty$; corrispondentemente l'altezza h è sempre maggiore dell'altezza di moto uniforme e tende ad essa per $x \to \infty$: ciò indica che, in ogni sezione della falda, in regime di moto vario, defluisce una portata - sempre superiore a quella corrispondente al regime di moto uniforme - che

[4] Nei calcoli è stato scelto, per D_0 il valore kh_u/ϵ.

tende ad assumere il valore q_u all'ascissa $x \to \infty$ ove $\partial\theta/\partial x \to 0$ e $\partial h/\partial x \to i_f$.

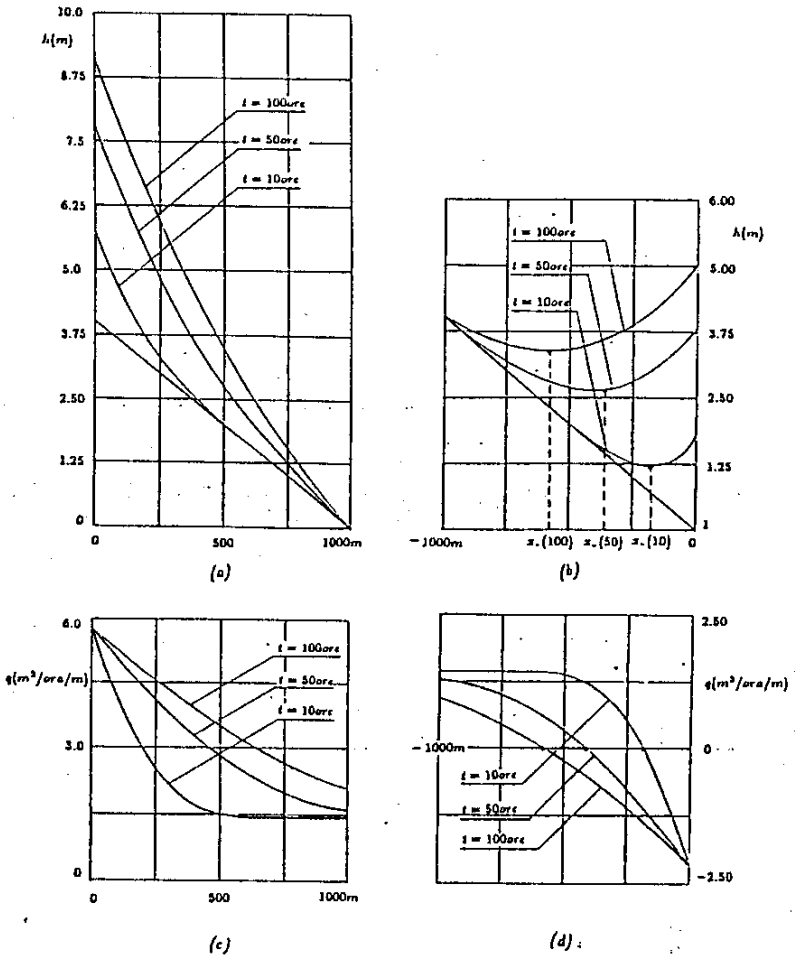


Fig.5- *(a,b) -Escursioni del profilo superficiale della falda in istanti successivi per immissione di portata costante all'ascissa x=0.*
(c,d) - Valori della portata q(x) in istanti successivi.

Quest'ultima circostanza è posta espressivamente in evidenza

nella fig.5c dove sono riportati i valori assunti dalla portata lungo la direzione del moto, durante la fase di ravvenamento.

Nella fig.5b sono invece illustrate le situazioni che vengono a determinarsi nella stessa falda quando questa si estende nel dominio $]-\infty, 0]$ ed è alimentata dalla portata $q_0 = 3.6m^3/ora/m$ all'ascissa $x = 0$.

Da essa si evince che che la $\partial\theta/\partial x$ a monte del fronte di alimentazione è positiva e, almeno per il caso che si esamina, in prossimità di detto fronte risulta maggiore di i_f: ciò sta ad indicare la esistenza di un moto retrogrado rispetto a quello corrispondente alle condizioni di moto uniforme; procedendo verso monte la $\partial\theta/\partial x$ diminuisce fino ad assumere il valore $\partial\theta/\partial x = i_f$ nella sezione di ascissa x_* dove la portata q della falda si annulla; a monte di x_* il moto è diretto verso valle ($i_f > \partial\theta/\partial x$) e la portata q, corrispondentemente, cresce fino ad assumere il valore q_u all'ascissa $x \to -\infty$ in cui è $\partial\theta/\partial x \to 0$ e $\partial h/\partial x \to i_f$.

Anche queste circostanze risultano chiaramente evidenziate nella fig.6b dove sono riportati i valori della $q(x)$ in diversi istanti $t > 0$.

La validità dei risultati ottenuti può essere accertata confrontando i profili istantanei della falda dedotti per via teorica con quelli ottenuti sperimentalmente su modelli di filtri realizzati con una apparecchiatura alla "Hele-Shaw", che si presta particolarmente bene per lo studio dei moti vari nelle falde [10].

Il dispositivo sperimentale, in dotazione presso il Dipartimento di Ingegneria delle Strutture, delle Acque e del Terreno della Università di L'Aquila, consiste essenzialmente di quattro vetri a specchio a facce perfettamente piane e trasparenti che delimitano tre intercapedini parallele e verticali, ciascuna di spessore costante.

La presenza delle due intercapedini laterali evita che, durante le prove, si verifichino apprezzabili deformazioni dei vetri che delimitano la intercapedine centrale costituente il "campo di misura".

Quale liquido filtrante viene impiegato olio minerale non additivato di viscosità tale che il regime del moto si mantenga regolare anche in intercapedini il cui spessore consente di ridurre a entità trascurabile l'influenza delle forze capillari.

Nel corso di ogni prova si procede alla registrazione fotografica

dei profili assunti dal contorno superiore della falda in istanti successivi.

Prove sull'apparecchiatura descritta sono attualmente in corso. A titolo di esempio nella $fig.6a$ sono consegnati i risultati relativi al caso di moto vario indotto in una falda freatica - caratterizzata da coefficiente k=0.867 cm/s e $\epsilon = 1$, poggiante su un piano impermeabile inclinato di $i_f = 0.03511$ sull'orizzontale,inizialmente animata di moto uniforme ($h_u = 16cm$) - quando questa viene alimentata, in corrispondenza del fronte di alimentazione, con una portata q_0 variabile con legge assegnata ($fig.6b$).

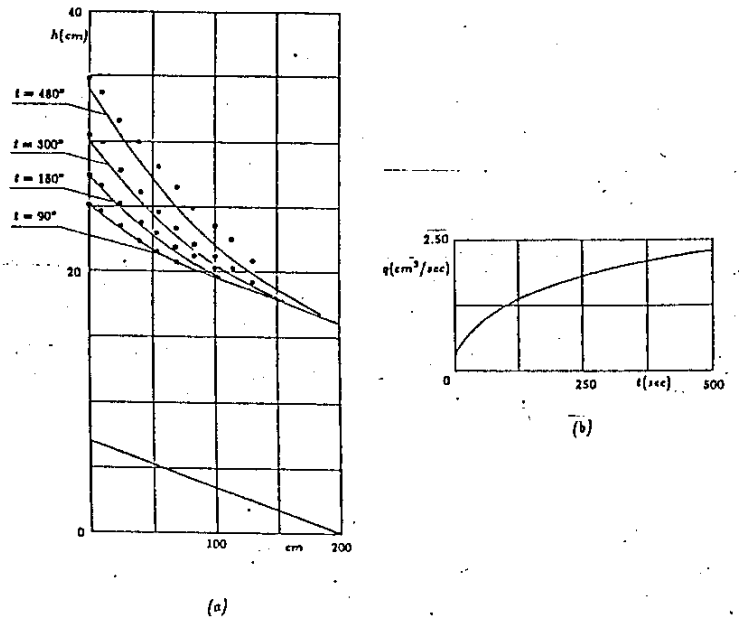


Fig.6 - *(a) Profili superficiali relativi ad istanti successivi.*
(b) Valori della portata q all'ascissa x=0 in istanti successivi.

Nella figura sono riportati i profili teorici (linea a tratto con-

tinuo) e i punti sperimentali (contrassegnati con un cerchietto annerito).

Dall'esame dei risultati sperimentali si rileva che, per valori dell'altezza $h(0,t)$ della falda in corrispondenza del fronte di alimentazione minori di $1.45h_u$ gli scarti tra i valori teorici e quelli sperimentali raggiungono al più l'ordine del 2.5%.

Gli scarti via via più accentuati che si evidenziano a maggiori valori di $h(0,t)$ derivano, in larga misura, dal contemporaneo venir meno sia delle ipotesi di Dupuit-Forchheimer che della validità delle approssimazioni poste a base del procedimento di linearizzazione della (12) e della condizione (17): in particolare, per $h(0,t) = 1.73h_u$, lo scarto all'ascissa $x = 0$ risulta dell'ordine del 6%.

Almeno per il campo dei valori indagati, dunque, il procedimento esposto può essere giudicato di concreta utilità anche per valutazioni quantitative circa la efficacia, la estensione e la prontezza di risposta del sistema filtrante ad interventi di ravvenamento di falde.

SOMMARIO.- Viene esaminato il fenomeno di moto vario che si instaura in una falda freatica per effetto della immissione, con modalità assegnate, di volumi idrici in una trincea che interessa tutto lo spessore della falda fino al piano impermeabile di sostegno.

Vengono dedotte soluzioni analitiche dell'equazione linearizzata del moto gradualmente vario la cui validità viene accertata confrontando i profili istantanei della falda dedotti per via teorica con quelli ottenuti sperimentalmente su modelli di filtri realizzati con apparecchiature alla "Hele-Shaw".

BIBLIOGRAFIA

[1] Arredi F., Costruzioni e impianti idraulici , Vol.I, Principato Ed.,1947.

[2] Boussinesq M.J., Essai sur la theorie des eaux courantes, Mem.Acad.Sci., 1877.

[3] De Marchi G., Idraulica, Hoeply Ed..

[4] De Marchi G., Sul cambiamento di regime di una corrente lineare a pelo libero in un alveo di sezione costante, L'Energia Elettrica, Vol.XXVII, 1950.

[5] Eckert E.R.G., Analysis of heat and mass transfer, McGraw-Hill International Book Company.

[6] Marchi E., Rubatta A., Meccanica dei fluidi, UTET.

[7] Noseda G., Applicazione del metodo di "relaxation", a un caso di moto vario di filtrazione, Atti del Convegno di Idraulica e Costruzioni Idrauliche, Palermo,

1961.

[8] Remson I., Hornemberg G.M., Moltz F.I. Numerical Methods in Subsurface Hydrology, J.Wiley and S.in.

[9] Russo Spena Andrea, Su alcune caratteristiche del fenomeno di sbocco da falde freatiche, Atti dell'Istituto di Idraulica e Costruzioni Idrauliche, Napoli,1956.

[10] Russo Spena Andrea, Moti filtranti a superficie libera in presenza di capillarità, L'Energia Elettrica, n.12, 1954.

[11] Russo Spena A., Processi di moto vario di correnti a superficie libera, Appunti delle lezioni del Corso di Tecnica della bonifica, L'Aquila, 1987.

[12] Schneebely G., Hydraulique Souterraine, Eyrolles ed. Paris.

Indice del fascicolo

Finito di stampare il 18.07.1990 presso il
Dipartimento di Scienze e Storia dell'Architettura
della Facoltà di Architettura
dell'Università "G. D'Annunzio" di Chieti.

L'uso della testata è stato concesso dal prof. Franco Eugeni.