Numero 6 - 1993

RATIO MATHEMATICA

Fascicolo dedicato alla Crittografia

a cura di

Franco Eugeni e Giovanni Moro

Comitato Scientifico

Luigia Berardi, *L'Aquila*
Albrecht Beutelspacher, *Giessen*
Franco Eugeni, *L'Aquila*
Mario Gionfrido, *Catania*
Michele Elia, *Torino*
Bruno Rizzi, *Roma*
Bal Khishau Dass, *Dehli*
Giovanni Moro, *Roma*

Numero 6 - 1993

RATIO MATHEMATICA

Fascicolo dedicato alla
Crittografia

a cura di

Franco Eugeni e Giovanni Moro

Comitato Scientifico

Luigia Berardi , *L' Aquila*

Aebacht Beutelspacher, *Giessen*

Franco Eugeni, *L' Aquila*

Mario Gionfrido, *Catania*

Michele Elia, *Torino*

Bruno Rizzi, *Roma*

Bal Khishau Dass, *Dehli*

Giovanni Moro, *Roma*

INDICE

A bound for codes correcting random and low-density closed-loop burst errors .
(L. Berardi e B.K. Dass) ..... pag. 1

Sul periodo delle matrici di permutazione .
(G. Campanini e A. Di Porto) .....pag. 6

Pseudorandom generators based on Lucas Sequences .
(A. Di Porto e W. Wolfowicz) .....pag. 15

I servizi crittografici delle Marine Britannica e Italiana.
(L. Donini) .....pag. 23

A Note on the Matrices of Maximum Order in GLH[k,p] and an Example of their Cryptographic Application.
(M. Elia) ....pag . 49

Osservazioni sulla distribuzione dei numeri primi dei tipi $(6n - 1)$ e $(6n + 1)$ - $n \geq 1$ intero.
(F. Eugeni e G. Moro) .....pag . 60

Note on cipher hypersystem
(S. Innamorati e F. Zuanni) .....pag . 74

Rappresentazione geometrica di parole.
(C. F. Manara) .....pag . 79

Su alcune strutture di spazio metrico con sostegno l'insieme delle variabili casuali associate a successioni di numeri a caso
(A. Maturo) .....pag . 84

A bound for codes correcting random and low-density closed-loop burst errors .

L. Berardi, Dip. di Ingegneria Elettrica, Università degli Studi dell'Aquila, Monteluco di Roio, I-67100, L'Aquila, Italy

B.K. Dass, Dep. of Mathematics, P.G.D.A.V.Collage (Univ. of Delhi), Nehru Nagar, New Delhi-110065, India

ABSTRACT

This paper presents a lower bound on the number of parity-check digits required for a linear code that corrects random errors and errors which are in the form of closed-loop low-density bursts.

INTRODUCTION

In some communication systems errors occur predominantly in the form of bursts. There are of course many situations in which errors occur in the form of a burst but not all digits inside the burst get corrupted, i.e. errors occur in the form of low-density bursts. In actual communication, while it is all important to consider correction of low-density bursts, care must be taken to correct at least up to a specific number of random errors no matter where they lie.

Most of the studies regarding the detection and correction of burst errors have been made with respect to what are called "open-loop burst" defined as:"An *open-loop burst* of length b is a vector whose only nonzero components are confined to b consecutive

[1] This work was carried out while the second author was Visiting Professor in L'Aquila (June-July, 1991) under C.N.R. grant.

positions, the first and the last of which are nonzero" [5].
There is another definition of the term *burst* which reads: "A *closed-loop burst* of length b, $2 \le b \le (n+1)/2$, is a vector $(a_1, a_2, \ldots, a_n)$ whenever there is an index i such that $1 \le i \le b-1$, $a_i \cdot a_{n-b+i+1} \neq 0$ and $a_{i+1} = a_{i+2} = \ldots = a_{n-b+1} = 0$ ".
This definition has also been found useful in certain communication systems though not much of the studies have been carried out with respect to it. Clearly, the definition of a closed-loop burst includes the definition of an open-loop burst, therefore, while considering the class of closed-loop bursts of length b or less, the set of open-loop bursts of length b or less is included in it.

Sharma and Dass [6] have given a lower bound over the number of parity-check digits for codes capable of correcting simultaneously random errors and low-density open-loop burst errors. In this paper, a lower bound over the number of parity-check digits for codes capable of correcting simultaneously random errors and low-density closed-loop burst errors has been derived.
In what follows, we shall confine ourselves to linear codes over GF(q) of length *n*. The weight of a vector is understood to be in the usual Hamming sense [3].

A LOWER BOUND

The following result presents a lower bound on the number of parity-check digits required for a linear code that corrects all random errors of weight m or less and all closed-loop bursts of length b or less with weight w or less. This result generalizes the well-known sphere-packing bound as well as results due to Campopiano [1], Dass and Muttoo [2], Muttoo and Tyagi [4].

THEOREM. The number of parity-check digits in an (n,k) linear code over GF(q) that corrects all combinations of m or fewer errors and all closed-loop bursts of length b or less with weight w or less, $1 \le m < w \le b < n/2$, is at least

$$\log_q \left[[1+(q-1)]^{(n,m)} + n \sum_{l=m+1}^{b} \sum_{j=m+1}^{w} \binom{l-2}{j-2} (q-1)^j \right] \qquad (1)$$

where

$$[1+x]^{(m,r)} = \begin{cases} 1 + \binom{m}{1} x + \ldots + \binom{m}{r} x^r, & 0 < r \leq m \\ 1, & r = 0 \\ 0, & r < 0 \end{cases} .$$

PROOF. Since the code is capable of correcting all errors of weight m and less, all n-tuples of weight m and less should be in different cosets of the standard array; their number, including the pattern of all zeros, is

$$[1 + (q-1)]^{(m,n)} \qquad (2)$$

Also, since the code corrects all those closed-loop bursts of length b or less which are of weight w or less, all such burst patterns must also be in different cosets except for those which are random errors of weight m or less. Since the closed-loop bursts of length m or less have weight m or less and hence are included in (2), we need only compute the number of closed-loop bursts of length m+1,m+2,...,b with weight greater than m but of weight less than or equal to w. The number of closed-loop bursts of length i (> m), i < n/2, with weight greater than m but of weight less than or equal to w is

$$n \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^j \qquad (3)$$

which gives the number of closed-loop bursts of length m+1, m+2, ...,b with weight greater than m but of weight less than or equal to w as

$$n \sum_{i=m+1}^{b} \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^j . \qquad (4)$$

Thus, the total number of errors to be corrected becomes

$$[1+(q-1)]^{(n,m)} + n \sum_{i=m+1}^{b} \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^j . \qquad (5)$$

Since there must be at least this number of cosets, and the total number of available cosets is q^{n-k}, therefore we must have

$$q^{n-k} \geq [1+(q-1)]^{(n,m)} + n \sum_{i=m+1}^{b} \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^j \qquad (6)$$

The theorem now follows by taking the logarithm on both the sides of (6) to the base q. □

Incidentally, it can be shown that the result applies to non-linear codes also.

DISCUSSION

For $m \geq w$, the second term in (5) vanishes and the bound reduces to Hamming's sphere-packing bound (cf. [5, Th. 4.5]).

For $w = b$, the lower bound on the number of parity-checks obtained in the theorem becomes

$$\log_q \left[[1+(q-1)]^{(n,m)} + n \sum_{i=m+1}^{b} \sum_{j=m+1}^{w} \binom{i-2}{j-2} (q-1)^j \right]$$

which coincides with a result due to Dass and Muttoo [2] obtained for a code that corrects random and closed-loop burst errors simultaneously.

Next, setting $m = 1$, the bound obtained in (1) reduces to

$$\log_q \left[[1+n(q-1)] + n \sum_{i=2}^{b} \sum_{j=2}^{w} \binom{i-2}{j-2} (q-1)^j \right] \qquad (1)$$

which coincides with a result due to Muttoo and Tyagi [4] obtained for a code that corrects low-density closed-loop burst errors.

Lastly, for $m = 1$ and $w = b$, the bound obtained in (1), as expected becomes

$$\log_q \left[1 + n(q-1)\, q^{b-1} \right] ,$$

which was proved by Campopiano [1].

REFERENCES

[1] C.N.CAMPOPIANO, Bounds on Burst-Error-Correcting Codes, *IEEE Trans.*, IT,pp.257-259,1962.

[2] B.K.DASS and S.K.MUTTOO, Codes Correcting Random and Closed Loop Bursts, *Bull.Cal.Math.Soc.* (to appear).

[3] R.W.HAMMING, Error Detecting and Error Correcting Codes, *Bell Syst.Tech.J.*,Vol.29,pp.147-160,1950.

[4] S.K.MUTTOO and V.K.TYAGI, Bounds for Codes Correcting Low-Density Closed-Loop Bursts, Communicated.

[5] W.W.PETERSON and E.J.WELDON Jr.,*Error-Correcting Codes*, MIT Press, Mass.,1972.

[6] B.D.SHARMA and B.K.DASS, On Linear Codes Correcting Random and Low-Density Burst Errors, *Linear Algebra and its Applications*, Vol.16, No.1, pp.5-18,1977.

Sul periodo delle matrici di permutazione

G. Campanini - A. Di Porto
Fondazione Ugo Bordoni, Roma, Italia

Introduzione

Dopo un breve richiamo alla definizione di *matrici di permutazione* e ad alcune loro proprietà, si affronta lo studio del *periodo* delle suddette matrici. In particolare si analizza il massimo periodo ammissibile e si fornisce il numero delle matrici aventi un prefissato periodo T.

Matrici di permutazione

Sia n un intero positivo. Consideriamo l'insieme $\mathcal{M}(n, \mathbb{Z}_2)$ delle matrici quadrate di ordine n i cui elementi, a_{ij} $(i, j = 1, 2,..., n)$, appartengono al campo di Galois $GF(2)=\mathbb{Z}_2=\{0,1\}$. Per ogni matrice $A \in \mathcal{M}(n,\mathbb{Z}_2)$ indichiamo con $|A_{(1)}|$ il numero degli elementi a_{ij} il cui valore sia 1, $0 \le |A_{(1)}| \le n^2$.

Prendiamo adesso in considerazione il sottoinsieme $\mathcal{G}_{(n)}$ di $\mathcal{M}(n, \mathbb{Z}_2)$ così definito:

$$\mathcal{G}_{(n)} = \{A : |A_{(1)}| = n ;\ a_{sk} = 1 \Rightarrow a_{ik} = 0, \forall i \neq s \ \ \& \ \ a_{sj} = 0, \forall j \neq k \}.$$

Nel seguito indicheremo con le lettere A, B, C le matrici, dette anche *matrici di permutazione* [1], appartenenti all'insieme $\mathcal{G}_{(n)}$, e con le lettere a_{ij}, b_{ij}, c_{ij}, $(i, j = 1, 2,..., n)$, i rispettivi elementi; la notazione $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ indica, quindi, una matrice definita dai suoi elementi.

Si osservi che le matrici di $\mathcal{G}_{(n)}$ sono tutte *non singolari*, ovvero a *determinante non nullo*, poiché, per ogni A in $\mathcal{G}_{(n)}$, un solo *prodotto associato* ad A è diverso da zero ed è uguale a ± 1 [2].

Proposizione 1: L'insieme $\mathcal{G}_{(n)}$ dotato dell'operazione prodotto righe per colonne è un *gruppo non commutativo* [3].

Dimostrazione : L'operazione definita in $\mathcal{G}_{(n)}$ è l'usuale *prodotto righe per colonne tra matrici* [2]. Tale operazione è binaria [3] e definita su tutto $\mathcal{G}_{(n)}$. Infatti è immediato verificare che, comunque si prendano A e B in $\mathcal{G}_{(n)}$, risulta

Lavoro eseguito nell'ambito della Convenzione in atto tra l'Amministrazione delle Poste e delle Telecomunicazioni e la Fondazione Ugo Bordoni

$$A \times B = C \in \mathcal{G}_{(n)} \quad ,$$

e quindi:

- l'*insieme* $\mathcal{G}_{(n)}$ *è chiuso* rispetto all'operazione su esso definita;
- la *legge associativa* è rispettata in $\mathcal{G}_{(n)}$, poiché $\mathcal{G}_{(n)}$ è un s. i. dell'insieme $\mathcal{M}(n, \mathbb{R})$ delle matrici quadrate di ordine n a elementi reali [3];
- la matrice $I \in \mathcal{G}_{(n)}$ che ha tutti gli elementi non nulli sulla diagonale principale è l'unico *elemento neutro* rispetto al prodotto tra matrici sopra definito;
- per ogni $A = (a_{ij}) \in \mathcal{G}_{(n)}$ la matrice $A^{-1} = (a'_{ij}) \in \mathcal{G}_{(n)}$ i cui elementi sono tali che

$$a'_{sh} = 1 \quad \text{se} \quad a_{hs} = 1 \quad ,$$

è la *matrice inversa* di A e risulta

$$A^{-1} \times A = A \times A^{-1} = I \quad .$$

Si noti che, tenendo conto del fatto che le matrici di $\mathcal{G}_{(n)}$ sono *non singolari*, la definizione sopra data di A^{-1} coincide con l'usuale definizione di matrice inversa, inoltre è sempre $A^{-1} = \overline{A}$, dove con $\overline{A}$ si indica la *matrice trasposta* di A [2].

Si osservi, infine, che il gruppo $\mathcal{G}_{(n)}$ *non è commutativo*, per $n > 2$. Ad esempio, per $n = 4$, si considerino le matrici A e B definite rispettivamente dai seguenti elementi

$$A : a_{12} = a_{23} = a_{31} = a_{44} = 1$$

$$B : b_{13} = b_{24} = b_{31} = b_{42} = 1 \quad ,$$

risulta allora

$$C = A \times B \neq B \times A = C' \quad ,$$

si ha, infatti, $c_{14} = 1$ e $c'_{11} = 1$.◆

Inoltre, il gruppo $\mathcal{G}_{(n)}$ è isomorfo al *gruppo totale* $\mathcal{S}_n$(*) *delle sostituzioni* su n elementi ; di conseguenza l'*ordine* (o *cardinalità*) di $\mathcal{G}_{(n)}$ [3] è finito ed è uguale a $n!$.

Relazione d'equivalenza associata a una matrice di $\mathcal{G}_{(n)}$

Al fine di caratterizzare il *periodo* di un elemento di $\mathcal{G}_{(n)}$, risulta utile ricordare la definizione generale di *periodo di un elemento di un gruppo* .

(*) $\mathcal{S}_n$ è detto anche *gruppo simmetrico* di grado n [1].

Un elemento x di un gruppo ha periodo e finito(**) se risulta:

$$x^e = u \quad ; \quad x^h \neq u \quad , \quad 0 < h < e,$$

dove u indica l'unità del gruppo.

Per il gruppo $\mathcal{G}_{(n)}$ valgono inoltre le seguenti proposizioni:

Proposizione 2 : $\mathcal{G}_{(n)}$ non è un gruppo ciclico.
Proposizione 3 : Ogni elemento di $\mathcal{G}_{(n)}$ ha periodo finito.
Proposizione 4 : Se $A \in \mathcal{G}_{(n)}$ ha periodo e allora

$$A^s = I \Rightarrow s \equiv 0 \pmod{e} \; ; \quad A^s = A^r \Rightarrow s \equiv r \pmod{e},$$

e, inoltre, l'insieme

$$\mathcal{A} = \{A, A^2, \ldots, A^e = I\}$$

è sottogruppo ciclico di $\mathcal{G}_{(n)}$; $\mathcal{A}$ è quindi commutativo e viene brevemente indicato con il nome di *gruppo generato da* A [3].

Per quel che riguarda le proposizioni 2, 3 si tenga rispettivamente presente che $\mathcal{G}_{(n)}$ è non commutativo e che $\mathcal{G}_{(n)}$ è un gruppo finito; per la proposizione 4 si ricordino le definizioni di periodicità di un elemento e di gruppo ciclico [3].◆

Indichiamo con $a_{ij}^{(t)}$ gli elementi della matrice A^t (potenza t-esima di $A \in \mathcal{G}_{(n)}$). Fissata una qualunque riga di A, e sia essa la i-esima, definiamo *periodo della riga i-esima* di A il più piccolo esponente $t > 0$ tale che $a_{ii}^{(t)} = 1$.

Al fine di chiarire la precedente definizione mostriamo un esempio in $\mathcal{G}_{(6)}$.

Esempio 1 : Sia $A \in \mathcal{G}_{(6)}$ definita dai seguenti elementi

$$A : a_{13} = a_{25} = a_{34} = a_{41} = a_{52} = a_{66} = 1,$$

la riga 6 ha periodo 1;

$$A^2 : a_{14}^{(2)} = a_{22}^{(2)} = a_{31}^{(2)} = a_{43}^{(2)} = a_{55}^{(2)} = a_{66}^{(2)} = 1,$$

le righe 2 e 5 hanno periodo 2;

$$A^3 : a_{11}^{(3)} = a_{25}^{(3)} = a_{33}^{(3)} = a_{44}^{(3)} = a_{52}^{(3)} = a_{66}^{(3)} = 1,$$

le righe 1, 3 e 4 hanno periodo 3.
È immediato vedere che il periodo di A è uguale a 6.

(**) In letteratura sono spesso usate le parole *ordine* ed *esponente* come sinonimi di periodo finito.

Proposizione 5: Fissata una qualunque matrice $A \in \mathcal{G}_{(n)}$ ad essa è associata una *relazione d'equivalenza* (indicata con il simbolo $\approx$) tra le sue righe, così definita: la riga i-esima è equivalente alla riga j-esima se e solo se $a_{ij}^{(r)} = 1$ per qualche intero $r \neq 0$, ovvero, indicando le righe di A con il loro indice

$$i \approx j \iff \exists\, r \gtrless 0 \text{ tale che } a_{ij}^{(r)} = 1.$$

Dimostrazione: La relazione così definita tra le righe di A è una relazione d'equivalenza [3]. Infatti, essa

- è *riflessiva*, $i \approx i$, poiché $a_{ii}^{(t)} = 1$, dove t è il periodo della riga i;
- è *simmetrica*, $i \approx j \iff j \approx i$, poiché, tenendo conto dell'uguaglianza $(a_{hk}^{(-r)}) = A^{-r} = \overline{A}^{r}$, si hanno le seguenti successive implicazioni
$$i \approx j \Rightarrow a_{ij}^{(r)} = 1 \Rightarrow a_{ji}^{(-r)} = 1 \Rightarrow j \approx i;$$
- è *transitiva*, $i \approx j$ e $j \approx k \Rightarrow i \approx k$, poiché
$$i \approx j \Rightarrow a_{ij}^{(r)} = 1. \text{ e } j \approx k \Rightarrow a_{jk}^{(s)} = 1,$$
e le due ultime uguaglianze implicano
$$a_{ik}^{(r+s)} = 1 \Rightarrow i \approx k. \quad \blacklozenge$$

Dalla proposizione 5 possiamo dedurre le seguenti proposizioni:

Proposizione 6: Data una matrice di permutazione $A \in \mathcal{G}_{(n)}$, essa definisce una relazione d'equivalenza che induce una partizione nell'insieme delle righe di A in sottoinsiemi disgiunti ovvero in *classi d'equivalenza* (***).

Proposizione 7: Data una matrice di permutazione $A \in \mathcal{G}_{(n)}$, il periodo massimo ammissibile di una riga di A è uguale a n.

Proposizione 8: Data una matrice di permutazione $A \in \mathcal{G}_{(n)}$, le righe di A appartenenti ad una stessa classe di equivalenza $\mathbf{c}$ hanno tutte lo stesso periodo, quest'ultimo è uguale al numero degli elementi contenuti in $\mathbf{c}$. Siano $\mathbf{c}_{n_s}$, $(s = 1, 2,\ldots,r)$ le classi di equivalenza della partizione indotta da A; n_s indica il periodo e il numero delle righe fra loro equivalenti contenute in $\mathbf{c}_{n_s}$ e si ha:

$$1 \leq r \leq n \;;\; \sum_{s=1}^{r} n_s = n \;;\; 0 < n_1 \leq n_2 \leq \ldots \leq n_r \leq n \;.$$

(***) La definizione di classe d'equivalenza definita da una matrice di permutazione non differisce, "mutatis mutandis", dalla definizione di *orbita di un elemento* $s \in S = \{1, 2,\ldots, n\}$ sotto l'azione di una permutazione $\sigma \in \mathcal{S}_n$, dove $\mathcal{S}_n$ è il gruppo simmetrico di grado n [1].

Prima di proseguire nella trattazione illustriamo quanto detto con un esempio:

Esempio 2 : Sia $A \in \mathcal{G}_{(8)}$ definita dai seguenti elementi

$$A : a_{13}= a_{22}= a_{35}= a_{46}= a_{51}= a_{64}= a_{78}= a_{87}= 1,$$

le classi d'equivalenza associate alla matrice di permutazione A sono le seguenti:

$$\mathbf{c}_{n_1} = \{2\} \ ; \ \mathbf{c}_{n_2} = \{4, 6\} \ ; \ \mathbf{c}_{n_3} = \{7, 8\} \ ; \ \mathbf{c}_{n_4} = \{1, 3, 5\}.$$

Periodo delle matrici di permutazione

Da quanto esposto in precedenza (in particolare dalla proposizione 8), si possono enunciare le due seguenti proposizioni:

Proposizione 9: Data una matrice di permutazione $A \in \mathcal{G}_{(n)}$ essa definisce una relazione d'equivalenza tra le sue righe; il periodo T di $A \in \mathcal{G}_{(n)}$ è allora uguale al minimo comune multiplo (mcm) tra le cardinalità delle classi disgiunte associate alla relazione di equivalenza indotta da A: $T = \text{mcm}\ (n_1, n_2,\ldots,n_r)$.

Proposizione 10: I periodi ammissibili sono quegli interi T tali che:

$$T = \prod_{i=1}^{\infty} p_i^{\alpha^i} \qquad \text{con la condizione} \qquad \sum_{\substack{i=1 \\ i\,:\,\alpha^i > 0}}^{\infty} p_i^{\alpha^i} \le n$$

dove p_i rappresenta l'i-esimo primo, essendo $p_1 = 2$.

Inoltre, per ogni periodo ammissibile, esiste almeno una matrice di permutazione avente quel fissato periodo. Si presenta quindi il problema di calcolare il numero di matrici $A \in \mathcal{G}_{(n)}$ aventi un fissato periodo T, dato un intero n maggiore di 1.

Sia T un periodo ammissibile per gli elementi di $\mathcal{G}_{(n)}$, allora avremo una o più *partizioni* [4] di n tali che il mcm tra i suoi addendi sia proprio T. Data una qualunque di tali partizioni,

$$(1) \qquad n = a +\ldots+ a + b +\ldots+ b +\ldots+c +\ldots+ c$$

con $k \ge 1$ addendi a, $h \ge 1$ addendi b e così via, $a > b >\ldots> c$, essa può essere associata a tutte quelle matrici $A \in \mathcal{G}_{(n)}$ che definiscono una relazione di equivalenza tra le loro righe che induce una partizione in k classi di equivalenza ciascuna di cardinalità a, in h classi di equivalenza ciascuna di cardinalità b, e così via; diremo allora che tutte queste matrici hanno la stessa *struttura ciclica* [1].

Dalla proposizione 9 è immediato concludere che le matrici aventi la stessa struttura ciclica hanno tutte lo stesso periodo T, mentre non si può affermare che tutte le matrici aventi lo stesso periodo T abbiano la stessa struttura ciclica.

Si noti che il numero delle strutture cicliche possibili è uguale al numero p(n) delle partizioni di n [1, 4].

Proposizione 11: Il numero N_{T_i} delle matrici con la stessa struttura ciclica definita dalla partizione (1) è dato dai seguenti prodotti:

$$N_{T_i} = \left(\frac{(n)!}{(n-ka)!\, a^k\, k!}\right)\left(\frac{(n-ka)!}{(n-ka-hb)!\, b^h\, h!}\right)\cdots\cdots\left(\frac{(tc)!}{(0)!\, c^t\, t!}\right) \tag{2}$$

Il numero delle matrici aventi un fissato periodo T è dato da ΣN_{T_i}, dove $1 \leq i <$ p(n) rappresenta il numero di partizioni di n i cui addendi hanno il minimo comune multiplo uguale a T.

Dimostrazione: È necessario chiarire come è stata ottenuta la (2) e, a questo proposito, è sufficiente giustificarne il primo fattore, poiché gli altri si ottengono di conseguenza. Data la partizione (1) si deve, innanzitutto, trovare il numero di combinazioni di classe ka di n elementi; per ciascuna di queste combinazioni si deve calcolare il numero di disposizioni di classe (a-1) di (ka-1) elementi; per ogni tale disposizione, il numero di disposizioni di classe (a-1) di (ka-a-1) elementi, e così via. Si ottiene quindi:

$$\binom{n}{ka}\prod_{i=1}^{k}\{[a(k+1-i)-1]\cdots\cdots[a(k-i)+1]\} = \binom{n}{ka}\frac{(ka-1)!}{\prod_{i=1}^{k-1} i\,a} = \binom{n}{ka}\frac{(ka-1)!}{a^{k-1}(k-1)!} =$$

$$= \frac{n!\,(ka)!}{(ka)!\,(n-ka)!\,ka\;a^{k-1}\,(k-1)!} = \frac{n!}{(n-ka)!\,a^k\,k!} \qquad \blacklozenge$$

Per trovare il massimo periodo ammissibile di un elemento $A \in \mathcal{G}_{(n)}$, $n > 1$, è sufficiente ricercare tra le p(n) partizioni di n le *partizioni migliori*, intendendo con questo termine quelle partizioni i cui addendi forniscono il mcm di valore più elevato.

Basandosi sulle proprietà di cui gode la successione dei numeri primi [5] e ricordando che, dati tre interi u, v e z risulta sempre:

$$(u+v) < uv \quad \text{per} \quad u \geq 2 \;\text{ e }\; v > 2\,,\; u > 2 \;\text{ e }\; v \geq 2$$
$$(u+z)v \gtrless u(v+z) \Leftrightarrow v \gtrless u,$$

si congettura il seguente algoritmo che fornisce una delle *migliori partizioni* di un fissato

intero n.

a) Si scriva n come somma di primi consecutivi p_i (i =1,2, .. , k ; p_1=2) più un eventuale resto R_1, $0 \le R_1 < p_{k+1}$:

(3) $$n = \sum_{i=1}^{k} p_i + R_1$$

b) Se risulta $R_1 = 0$ oppure $R_1 = 1$ la migliore partizione è data dalla (3), ad eccezione del solo caso $n = 3$ nel quale anche se risulta, secondo il passo a), $k = 1$, $p_k = 2$ e $R_1 = 1$, la migliore partizione non è (2+1) bensì 3.

c) Se il resto $R_1 \ge 2$, si ripartisca R_1 nella seguente somma

$$R_1 = \sum_{i=1}^{j} (p_i^2 - p_i) + R_2 \quad , 1 \le j < k \quad \text{e} \quad R_2 < p_{j+1}^2 - p_{j+1} ,$$

e si scriva

$$n = \sum_{i=1}^{j} p_i^2 + p_{j+1} + \ldots + p_k + R_2$$

d) Se il resto $R_2 \ge 2^2$, si operi come al punto c) con

$$R_2 = \sum_{i=1}^{s} (p_i^3 - p_i^2) + R_3 \quad , 1 \le s < j \quad \text{e} \quad R_3 < p_{s+1}^3 - p_{s+1}^2 ,$$

e si scriva

$$n = \sum_{i=1}^{s} p_i^3 + \sum_{i=s+1}^{j} p_i^2 + p_{j+1} + \ldots + p_k + R_3$$

e) Si continui ad operare sui resti successivi finché il t-esimo resto R_t, ottenuto dalla ripartizione $R_{t-1} = \Sigma (p_i^t - p_i^{t-1}) + R_t$, risulta minore di 2^t. Si scriva allora

(4) $$n = \sum_{i=1}^{k} p_i^{\alpha_i} + r_1 , \ \alpha_1 = t , \ \alpha_\nu > 1 \ (\nu \le j) \ \text{e} \ \alpha_\nu = 1 \ (\nu > j) , \ 0 \le r_1 = R_t < 2^{\alpha_1} .$$

f) Se risulta $r_1 = 0$ la migliore partizione è data dalla (4).

g) Se risulta $r_1 \ge 1$ si ricerchi, se esiste, il più piccolo valore $p_\mu^{\alpha_\mu}$ ($1 \le \mu \le k$) tale che $p_\mu^{\alpha_\mu} + a$ ($0 < a \le r_1$) sia uguale a p_{k+1}. Si scelga per n la seguente partizione:

(5) $$\sum_{\substack{i=1 \\ i \ne \mu}}^{k+1} p_i^{\alpha_i} + (r_1 - a)$$

Se $r_2 = r_1 - a = 0$, la (5) è la migliore partizione, altrimenti si continui ad operare su r_2 come fatto per r_1 e così via sino a che un resto r_t è uguale a zero oppure è tale che non esiste un valore $p_\tau^{\alpha_\tau}$ che permetta di ottenere $p_\tau^{\alpha_\tau} + d = p_{k+t}$, ($d \le r_t$).

A titolo d'esempio si applichi, per $n = 9$, l'algoritmo che permette di trovare il massimo periodo ammissibile T_{max} per gli elementi di $\mathcal{G}_{(9)}$:

- usando la (3) del punto a), si ha

$$n = \sum_{i=1}^{2} p_i + R_1$$

ovvero, $9 = 2 + 3 + 4$;

- essendo $R_1 = 4 > 2$, si ripartisca R_1 secondo quanto indicato al punto c)

$$R_1 = \sum_{i=1}^{1} (p_i^2 - p_i) + R_2$$

ovvero, $4 = 2 + 2$;

- si ripartisca n secondo il punto c)

$$n = p_1^2 + p_2 + R_2$$

ovvero, $9 = 4 + 3 + 2$;

- essendo $R_2 = 2$ $(1 < r_1 = R_2 < 2^2)$ si prosegue secondo il punto g) ottenendo, infine,

$$n = p_1^2 + (p_2 + r_1)$$

e quindi l'algoritmo termina poiché $r_2 = 0$. Si può infine scrivere: $9 = 4 + (3+2) = 4 + 5$.

Risulta allora: $T_{max} = \text{mcm}\ (4, 5) = 20$.

Periodo ammissibile T	Numero delle partizioni i	Numero delle matrici con periodo T ΣN_{T_i}
1	1	1
2	4	2.619
3	3	5.768
4	4	30.996
5	1	3.024
6	7	83.160
7	1	25.920
8	1	45.360
9	1	40.320
10	2	27.216
12	2	30.240
14	1	25.920
15	1	24.192
20	1	18.144
Totale	30	362.880 = 9!

Pseudorandom generators based on Lucas Sequences .

A. Di Porto - W. Wolfowicz
Fondazione Ugo Bordoni, Rome, Italy

Abstract: Pseudo-random sequence generators are the heart of stream-cipher systems. This work presents some design criteria for such generators, based on innovative methods. To this aim the Lucas Sequences, reduced modulo a prime p, are taken and suitably manipulated. Modular Exponentiation is the function used to attain the output sequences. The periodicity of the Lucas Sequences allows to define a lower bound for the period of the generated sequences; actually our purpose is to ensure that the sequences which are generated have a period greater than a prefixed value. Furthermore the cryptographic strength of these sequences relies on the one-wayness of the discrete logarithm problem.

1. INTRODUCTION

The pseudorandom sequence generators are the main part of stream-cipher cryptographic devices [1].

Several studies pertaining the definition of pseudo-randomness of a sequence, lead to a large number of works both theoretical and applicative [1,2,3,4,5] where tools belonging to different branches of mathematics are used.

We address to specific publications for the different definitions of pseudorandom sequence and we suppose that the reader is familiar with the meaning and implications of the cryptographic algorithms, and in particular of stream-ciphers.

The aim of this work is to define some non conventional pseudorandom sequence generator, based on mathematical and implementative hypotesis different from those of most generators proposed in the past.

In this work some generator based on modular exponentiation will be examined, utilizing the special sequences of the Lucas Numbers. In these generators the minimum period of the sequences can be taken as a design parameter. For this purpose some elements of Number Theory and the properties of the Lucas Sequences are recalled in section 2; the generators we propose are described and analyzed in section 3 and 4.

Work carried out in the framework of the agreement between the Italian PT Administration and the Fondazione "Ugo Bordoni".

2. FUNDAMENTALS OF NUMBER THEORY REQUIRED FOR THE GENERATOR DESIGN

In this section some definition and fundamental theorem of Number Theory which will be necessary in the generator design, are recalled. Notice that it is not our intention to give here a systematic treatment, which would need much more than only one section; we wish to give the reader a set of notions which are necessary to the following of this paper. We refer to the literature [6,7,8] for a deep insight of the subject.

Let us define *Generalized Lucas Sequence with parameter* s the sequence:

$$V_i(s) = sV_{i-1}(s) + V_{i-2}(s) \tag{1}$$

being s an integer and with the initial conditions

$$V_o(s) = 2 \quad , \quad V_1(s) = s \tag{2}$$

It is proved [6,9,10] that the sequence defined by (1) and (2), reduced modulo an integer n, is periodic, with period T.

Some interesting consideration can be made regarding such period. In particular:

- the sequence $V_i(s) \mod 2^k$, $k \geq 1$, has period $T = 3 \cdot 2^{k-1}$, when s is odd;
- the sequence $V_i(s) \mod 2$ has period $T = 1$, when s is even;
- the sequence $V_i(s) \mod 4$ or $\mod 8$ has period $T = 1$ or $T = 4$ respectively, when $s = 2(2t + 1)$;
- the sequence $V_i(s) \mod 2^k$ has:

  $T = 2^{k-2}$, when $s = 2(2t + 1)$, $k \geq 4$;
  $T = 2$, when $s = 2^v(2t + 1)$, $v \geq 2$, $2 \leq k \leq v$;
  $T = 2^{k-v}$, when $s = 2^v(2t + 1)$, $v \geq 2$, $k > v$;

- given a prime $p > 2$:
  - the period T of $V_i(s) \mod p$ is always an even number greater than 2;
  - if $s^2 + 4$ is a Quadratic Residue[1] (QR) mod p, then the period T of $V_i(s) \mod p$ is $p - 1$ or a divisor of $p-1$;

[1] Given a prime p, the integer a is said to be a quadratic residue mod p , if the congruence $x^2 \equiv a \mod p$ has solutions.

- if $s^2 + 4$ is not a Quadratic Residue (NQR) mod p, then the period T of $V_i(s)$ mod p is $2(p+1)$ or a divisor of $2(p+1)$. Furthermore, if $p+1 = 2^{\alpha}(2k+1)$ with $\alpha \geq 1$, then $T \geq 2^{\alpha+1}$ always;
- let T the period of $V_i(s)$ mod p, then the period of $V_i(s)$ mod p^k, $k \geq 1$, is a divisor of $T \cdot p^{k-1}$.

3. Generators based on modular exponentiation of Lucas Sequences

The content of previous works [4,5] allows to design pseudorandom number generators, taking the period of the generated sequences as a design parameter. Actually the periodicity of the generalized Lucas Sequences when taken modulo a prime p, can be a very useful tool for our purposes. Moreover modular exponentiation of these sequences, as it will be considered in the sequel of this work, allows us to attain unpredictability of the generated sequences and their cryptographic strength, with respect to the previous defined parameter s of the eqns. (1) and (2), when it is considered as a part of the cryptographic key.

Let us consider the two following Lucas Sequences

$$V_h(m) = mV_{h-1}(m) + V_{h-2}(m)\ ; \quad h=h_0, h_0+1, h_0+2, \ldots \text{ and } m \geq 1 \tag{3}$$

$$V_k(n) = nV_{k-1}(n) + V_{k-2}(n)\ ; \quad k=k_0, k_0+1, k_0+2, \ldots \text{ and } n \geq 1\ . \tag{4}$$

Notice that the values $V_{h_o}(m)$ and $V_{k_o}(n)$ can be reached, for every h_0 and k_0 in a logarithmic number of steps, according to the results given in [11,12], instead of applying the recursion indicated by (3) and (4).

Let us consider the sequence given by the following formula

$$C_i = V_h(m)^{V_k(n)} \pmod p\ ;\ i=0, 1, 2, \ldots;\ h=h_0+i\ ;\ k=k_0+i\ ; \tag{5}$$

substituting in eqn. (5) the expressions (3), (4) we get

$$C_i = (mV_{h-1}(m)+V_{h-2}(m))^{nV_{k-1}(n)+V_{k-2}(n)} = \tag{6}$$

$$\sum_{t=0}^{nV_{k-1}(n)+V_{k-2}(n)} \binom{nV_{k-1}(n)+V_{k-2}(n)}{t} (m\,V_{h-1}(m))^{nV_{k-1}(n)+V_{k-2}(n)-t}(V_{h-2}(m))^t =$$

$$m^{nV_{k-1}(n)}(C_{i-1})^n \sum_{t=0}^{V_{k-2}(n)} \binom{nV_{k-1}(n)+V_{k-2}(n)}{t} (m\ V_{h-1}(m)\ )^{V_{k-2}(n)-t}\ (V_{h-2}(m))^t +$$

$$+ \sum_{t=V_{k-2}(n)+1}^{nV_{k-1}(n)+V_{k-2}(n)} \binom{nV_{k-1}(n)+V_{k-2}(n)}{t} (m\ V_{h-1}(m)\ )^{nV_{k-1}(n)+V_{k-2}(n)-t}\ (V_{h-2}(m)\ )^t .$$

From the above expression (6) we can see how the symbol C_i is a function of the previous generated symbol C_{i-1} and of the parameters m and n.

Notice that, if we take m and n as a part of the cryptographic key, the difficulty to find them, given C_i and C_{i-1}, is the same as solving the discrete logarithm problem.

Actually, further algebraic manipulation of (6) can lead to a general expression of (5) having the form

$$C_i \equiv f\,(C_{i-1}, C_{i-2}, m, n\ ) \pmod p\ , \tag{7}$$

but it could be seen that finding m and n, given C_i ,C_{i-1} and C_{i-2}, implies always an inversion of several modular exponentiations.

The equation (5) can be rewritten by Fermat little theorem [6], as follows

$$C_i = <<V_h(m)>_p{}^{<V_k(n)>_{p-1}}>_p \tag{8}$$

where $< x >_p$ denotes the residue of x mod p.

In order to define the period of the sequence $\{C_i\}$, p must be chosen in an appropriate way; according to the choice of p, the parameters m and n play a fundamental role to allow a period long enough for cryptographic purposes.

In the sequel, different possibilities will be shown as far as the expression of p is concerned, and the period will be determined according to the quadratic residuosity of $m^2 + 4$ and $n^2 + 4$. To this regard it is important to notice that a good level of freedom on the choiche of m and n with respect to p, still remains. Actually, for a given p, it can be proven that the number of values of m, $0 \le m \le p - 1$, for which it results $m^2 + 4$ quadratic residue mod p, is $(p + 1) / 2$ or $(p - 1) / 2$ depending on p. The demonstration of this assertion is straightforward and we omit it for sake of brevity.

In the following two examples are given to show how the choiche of p, m and n can be utilized for the design of our generators based on the modular exponentiation of the Lucas Sequences, and how a lower bound for the period of the generated sequences can be attained.

3.1 Generator with $p = 2q + 1$

If $p = 2q + 1$, with q prime, the formula (8) takes the expression

$$C_i = <<V_h(m)>_{2q+1}{}^{<V_k(n)>_{2q}}>_{2q+1} \cdot \tag{9}$$

The choice of the parameters m and n, makes possible the following four cases

Case 1:

$m^2 + 4$ QR mod $2q + 1$

$n^2 + 4$ QR mod q

In such a case the period of the sequence $V_i(m)$ mod $2q + 1$ is a divisor of $2q$, and, being q a prime, it is equal to $2q$.

For the period of $V_i(n)$ mod $2q$ the following considerations can be made: it is the least common multiple between the periods of $V_i(n)$ mod 2 and $V_i(n)$ mod q ; the first of such periods is 1 or 3 depending on the fact if n is even or odd respectively, while the second period is equal to q-1 or to one of its divisors, then it is greater than or equal to 4.

Hence the sequence defined by the eqn. (9) has a period T which equals the least common multiple between the periods of the Lucas sequences respectively base and exponent of the expression (9), and for the above considerations, it results that:

$$T \geq 4q \sim p \tag{10}$$

Case 2:

$m^2 + 4$ QR mod $2q + 1$

$n^2 + 4$ NQR mod q

Then, for the period of $V_i(m)$ mod $2q + 1$, all the considerations of case 1 hold again, while for the period of the sequence $V_i(n)$ mod $2q$ we have: the period of $V_i(n)$ mod 2, is 1 or 3 depending on the fact if n is even or odd; the period of the sequence $V_i(n)$ mod q is greater than or equal to $2^{\alpha+1}$, being $q + 1 = 2^{\alpha}(2k + 1)$, $\alpha \geq 1$. It is possible to conclude that the period T of the sequence defined by the (9) is

$$T \geq 2^{\alpha+1} q \geq 4q \sim p \tag{11}$$

Case 3:

$m^2 + 4$ NQR mod $2q + 1$

$n^2 + 4$ QR mod q

The period of the sequence $V_i(m)$ mod $2q + 1$ is greater than or equal to $2^{\alpha+2}$, being again $q + 1 = 2^{\alpha}(2k + 1)$, $\alpha \geq 1$; the period of the sequence $V_i(n)$ is ≥ 4. In this case it is possible only to say that the period T defined by eqn (9) is:

(12) $$T \geq 2^{\alpha+2} \geq 8$$

Case 4: $m^2 + 4$ NQR mod $2q + 1$
$n^2 + 4$ NQR mod q;

then, again under the hypotesis that $q + 1 = 2^{\alpha}\ (2k + 1)$, $\alpha \geq 1$, the period of the sequence $V_i(m)$ mod $2q + 1$ is $\geq 2^{\alpha+2}$ and the period of the sequence $V_i(n)$ mod q is $\geq 2^{\alpha+1}$.

Hence for the period T of the sequence defined by the (5) we have

(13) $$T \geq 2^{\alpha+2} \geq 8$$

3.2 Generator with $p = 2q - 1$

If $p = 2q - 1$ the equation (8) takes the expression

(14) $$C_i = <<V_h(m)>_{2q-1}{}^{<V_k(n)>_{2q-2}}>_{2q-1} .$$

In order to attain a long period of the sequence generated by eqn. (14) it is sufficient, in this case, to consider only the case $m^2 + 4$ NQR mod p. According to this choiche[10] the sequence $V_i(m)$ has a period equal to $4q$.
Hence the period T of the sequence generated by (14) is

(15) $$T \geq 4q \sim p .$$

From the above considerations it turns out that the generators based on modular exponentiation of Lucas Sequences, defined by equations (8), (1) and (2), generate sequences whith a period greater than or equal to a prefixed value, if the parameters m, n and p are properly chosen (as in the cases 1 and 2 of sec. 3.1 and in sec. 3.2)

To give an idea of the magnitude order of the acceptable values for cryptographic purposes, the sequence generated by the algorithm expressed by (8), has a period of the order 10^{100} if m , n and p are chosen around 10^{100}

4. PSEUDORANDOM GENERATOR

The above generators could be used for cryptographic purposes, because of the unpredictability of the generated sequences. Moreover the possibility of controlling their period is a highly desirable property. Nevertheless a good statistical balancement must be guaranteed. This can be easily obtained by a self-synchronizing scrambler[13], whose input-output equation is

$$y(k) = \sum_{i=1}^{L} c_i\, y(k-i) + u(k) \tag{16}$$

where $u(k)$ and $y(k)$ are the input and the output sequences respectively, c_i, $i=1,..,L$, are p-ary multipliers, and all the calculations are performed mod p.

Globally the final scheme of the pseudorandom generator is represented in fig. 1, where p, m and n are the cryptographic key and the scrambler is completely defined by its characteristic polynomial[14], which can also be considered as a part of the cryptographic key.

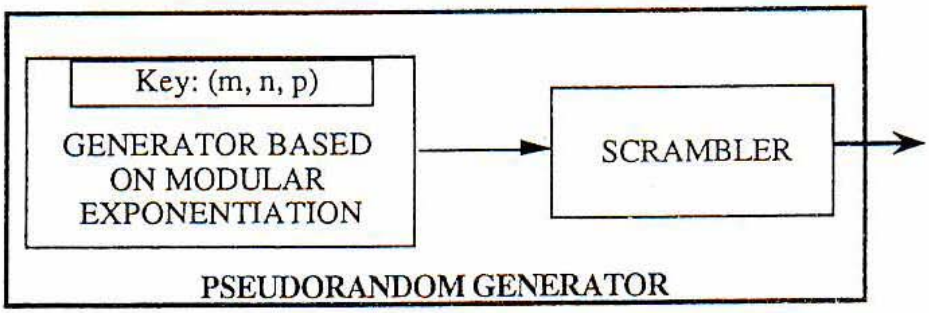


Fig. 1

5. CONCLUSIONS

By the results presented in this work it turns out that the use of the generalized Lucas Sequences allows to attain a pseudorandom number generator, having the period of the generated sequence greater than a prefixed value. This property can be used to generate sequences for cryptographic purposes. Nevertheless the difficulty of designing fast modular exponentiators on large numbers is still to be solved; a great amount of works in this area is being in progress, mainly for VLSI implementation of RSA co-decoders [15].

REFERENCES

[1] W.Diffie, M. E. Hellman : "*Privacy and Authentication: an Introduction to Cryptography.*" Proc. IEEE, Vol. 67, pp. 397-427, March. 1979.

[2] D. Knuth : "*The Art of Computer Programming.*" Vol. 2, *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969.

[3] S. W. Golomb: "*Shift Register Sequences.*" Holden Day, S. Francisco, 1967.

[4] O. Goldreich, H. Krawczyk, M. Luby: "*On the Existence of Pseudorandom Generators.*", presented at Crypto '88, S. Barbara, Aug. 1988.

[5] S. Micali, C.P. Schnorr: "*Efficient, Perfect Random Number Generatoris*", presented at Crypto '88, S. Barbara, Aug. 1988.

[6] G. H. Hardy, E. M. Wright: "*An Introduction to the Theory of Numbers.*" Oxford at the Clarendon Press, 1945.

[7] I. M. Vinogradov: "*Elements of Number Theory.*" Dover Publications, inc. New York, 1954.

[8] A. Di Porto, P. Filipponi: "*A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers.*" Lecture Notes in Computer Science, Vol. 330, pp.211-223, Springer - Verlag 1988.

[9] Bro. A. Brousseau: "*An Introduction to Fibonacci Discovery.*" Santa Clara (CA): The Fibonacci Association, 1965.

[10] A. Di Porto: "*Periodo di Sequenze di Lucas ridotte modulo una potenza intera di 2; considerazioni sugli Pseudoprimi pari di Fibonacci*",FUB Internal Report 3B3490, nov. 1990.

[11] H. Riesel: "*Prime Numbers and Computer Methods for Factorization.*" Birkhäuser, 1985.

[12] A. Di Porto, P. Filipponi, E. Montolivo: "*An Efficient Algorithm for Finding Large Probable Primes*" Note Recensioni e Notizie, Vol.XXXVII, n. 3-4, July-December 1988, pp. 163-168.

[13] O. Brugia: Private communication.

[14] J. E. Savage: "*Some Simple Self-Synchronizing Digital Data Scramblers*", Bell System Tech .Journal, Vol. 46, n.2, feb. 1967, pp. 449-87.

[15] M. Bucci, A. Di Porto: "*Fast Serial-Parallel Multipliers* " Proc of 6th. International Conference, AAECC-6. Lecture Notes in Computer Science, Springer-Verlag, 1989, pp.111-121.

I servizi crittografici delle Marine Britannica e Italiana.

L. Donini

Una analisi comparativa della loro attività nel secondo conflitto mondiale

Sebbene non ci siano elementi sufficienti per stendere un bilancio completo, ritengo possibile effettuare un'analisi comparativa delle attività dei due servizi crittografici indipendentemente dallo sfruttamento di esse attività fu o non fu fatto dai rispettivi Alti Comandi in campo strategico e tattico. Effettuare cioè un confronto esclusivamente tecnico sulla struttura e la qualità dei sistemi di cifratura, sui gradi di difficoltà dei relativi decrittografici, sulla incapacità dimostrata nel raggiungere successi o subire fallimenti.

Un'analisi del genere, che servirà anche a chiarire le cause del successo inglese nella penetrazione delle nostre cifrature meccaniche, deve prendere in considerazione sia la crittografia offensiva o decrittografia, cioè l'attacco alle radiocomunicazioni segrete nemiche, sia quella difensiva, cioè la tutela delle proprie cifrature.

Mi sembra giusto limitare l'analisi ai sistemi di uso pressoché generale per i radiomessaggi di alto grado di segretezza, cioè: i cifrari navali sopracifrati (inglesi e italiani) e le cifrature meccaniche (italiane). Per queste ultime ritengo di poter trascurare in questa sede la macchina ENIGMA impiegata dal SIS (Servizio Informazioni Segrete, della Marina), sia perché essa non fu di uso navale generale, avendola impiegata solo Supermarina in rare occasioni (L'opera ufficiale britannica "British Intelligence in the 2 W.W." - che d'ora in avanti citeremo con la sigla B.I. - a pag.210 del 1° Vol. dice: «solo uno o due messaggi al giorno») e solo nei primi 9 mesi di guerra, sia perché le sue vicende sono assorbite da quelle della ENIGMA delle FF.AA. tedesche, già penetrata dagli Inglesi nel 1940.

2. - I cifrari navali sopracitati

2.1. - Come è noto alla maggior parte dei lettori, tale cifratura è articolata su due operazioni successive. La prima consiste nel sostituire alle parole o frasi del «chiaro» gruppi letterali o numerici segreti (quadricifre, per entrambe le Marine in questione) reperiti nel cifrario o codice vero e proprio. Per esempio (parole e quadricifre sono di fantasia):

chiaro .... Hush most secret stop Cincmed from Adm.London stop ...

1ª Cifr. (C) 1782 8130 6615 8469 0983 3561 1565 8469

La seconda operazione, detta 2ª cifratura o sopracifratura, consiste nel sottrarre cifra, senza i rapporti cioè con modalità 10, i gruppi della 1ª cifratura dai gruppi del cosiddetto «verme di sopracifratura» prelevato da apposite tabelle. Per esempio:

Verme	**(V)**	**2916**	**3410**	**9226**	**0880**	**4534**	**8117**	**4036**	**1912** ..
-1ª cifr.	**(C)**	**-1782**	**8130**	**6615**	**8469**	**0983**	**3561**	**1565**	**8469** ..
Sopra-cifrato	**(S)**	**1234**	**5380**	**3611**	**2421**	**4651**	**5656**	**3571**	**3553**

Vale a dire: S = V - C, per sopracifrare e C = V - S, per eliminare la sopracifratura. E' ovvio che nessun crittografo, anche se in possesso del cifrario nemico, potrà mai decrittare un messaggio sopracifrato non verme casuale o, comunque, incoerente, a lui non noto e usato esclusivamente per quel messaggio. Ma, se nella massa del materiale sotto esame esistono coppie, o terne etc., di messaggi sopracifrati con lo stesso verme, si apre un piccolo spiraglio alla penetrazione, in base a una semplicissima considerazione algebrica. Infatti, la differenza fra due gruppi S_2 e S_1 in 2ª cifratura, sopracifrati con lo stesso gruppo V di Verme è uguale alla differenza fra i due gruppi del codice in 1ª cifratura (C_2 e C_1) che hanno generato i rispettivi gruppi sopracifrati:

$$\begin{array}{r} S_1 = V - C_1 \\ S_2 = V - C_2 \\ \hline S_1 - S_2 = C_2 - C_2 \end{array}$$

Ne consegue che solo le coppie, terne, etc. di messaggi cifrati con lo stesso cifrario e sopracifrati con lo stesso verme costituiscono le basi per avviare la penetrazione.

Per fare ciò il decrittatore deve:

- individuare, se ve ne sono, le coppie o terne, etc. di messaggi sopracifrati con lo stesso verme;

- effettuare, per ciascuna coppia individuata, le differenze fra gruppi omologhi, cioè gruppi che occupano nei due messaggi uguale posizione;

- registrare le differenze che si sono presentate con frequenza sensibilmente maggiore di quella prevedibile secondo le leggi di probabilità;

- per ogni differenza ($S_1 - S_2 = C_2 - C_1$) accettata come significativa assegnare valori numerici arbitrari (C_2 e C_1) ai gruppi di codice che l'hanno generata, cercando poi di collegare fra loro i valori arbitrari in modo da ridurli tutti a una stessa base relativa, tale cioè che detti gruppi «arbitrari» differiscano dai corrispondenti gruppi «reali» (non ancora noti) del codice per una «costante» comune, che col tempo si riuscirà forse a definire, sebbene ciò non sia indispensabile.

Il lavoro anzidetto proseguirà fino ad aver raccolto una quantità di materiale tale da poter attribuire ad alcuni dei gruppi arbitrari di codice il rispettivo significato per iniziare così e poi sviluppare la ricostruzione vera e propria del codice o cifrario in uso, assieme a quella delle relative tabelle di sopracifratura.

2.2. - Non occorre sprecare parole per illustrare quanto sia arduo e faticoso il lavoro che ho succintamente descritto e che il servizio crittografico della nostra Marina riuscì a portare a compimento per i vari cifrari o codici navali inglesi che si avvicendarono dal 1938 a tutto il 1942.

Gli analoghi tentativi inglesi contro i nostri cifrari navali del periodo bellico incontrarono invece completo fallimento, onestamente ammesso dai nostri avversari e più volte lamentato anche nei due volumi del B.I.. Per esempio, a pag.210 di B.I. vol.1° si legge: «I principali cifrari navali italiani, che erano i cifrari usati dalla loro flotta per la maggior parte delle sue comunicazioni importanti, non fu-

rono mai più letti dopo il luglio 1940, eccetto che per pochi brevi intervalli, come risultato di catture, dopo la metà del 1941». Di questo insuccesso non sappiamo quanto fu dovuto a loro minore capacità e impegno e a presumibile minore intensità del nostro traffico radio, e quanto a maggiore efficacia degli accorgimenti e delle contromisure che avevamo introdotto nel nostro complesso «cifrari/sopracifratura» entrato in vigore a metà luglio 1940, proprio perché avevamo potuto sfruttare la conoscenza delle debolezze riscontrate nell'analogo sistema inglese e gli appigli di cui a mano a mano avevamo imparato ad avvalerci per penetrarlo.

2.3. - Le debolezze del sistema inglese erano varie e di vario peso. Mi limito a citarne alcune:

- a) reimpieghi totali di verme, abbastanza frequenti e fino a tre/quattro volte per uno stesso verme; reimpieghi parziali frequentissimi;

- b) periodi di validità, anche se di pochi giorni, delle tabelle di sopracifratura mal commisurati alla intensità del traffico radio;

- c) imperfetto controllo della usura delle tabelle dei vermi. Quando veniva ordinata, con messaggio cifrato, la abrogazione di vermi troppo usati, quasi sempre il danno era già avvenuto;

- d) nelle tabelle che contenevano i vermi di sopracifratura esistevano qua e là (forse per esigenze di rapidità di compilazione) intere righe già esistenti in tabelle abrogate;

- e) i «gruppi indicatori» che, posti all'inizio dei messaggi in cifra, indicavano ai destinatari quale verme era stato usato, furono per molti anni impiegati senza «mascheratura», cioè non disguisati, sicché l'eventuale reimpiego di un verme era direttamente rivelato dall'uguaglianza dei gruppi indicatori;

- f) quando, nel dicembre '40 e fino a buona parte del 1941, gli Inglesi introdussero la «mascheratura» degli indicatori, essa fu piuttosto banale e per di più usata male dai cifratori, tanto da crearci solo due settimane di crisi;

- g) i cifrari non contenevano «omofoni», cioè non assegnavano due o più gruppi segreti diversi per cifrare una data parola di uso molto frequente. Per esempio «fullstop»

poteva essere cifrato in un solo modo (nei nostri cifrari: una ventina di modi diversi); analogamente per «from» etc.;

- h) le voci geografiche erano abbinate, come interpretazione alternativa, a voci di vocabolario iniziati con le stesse due o tre lettere. Così, solo a titolo esemplificativo: 7184 = Give/Gibraltar, 0921 = Last/La Spezia, 4650 = Make/Malta, 2935 = All Concerned/Alexandria, 7714 = Left/Leghorn. Ciò ci era di grande aiuto per identificare la voce geografica quando avevamo già identificato la voce di vocabolario ad essa abbinata, e viceversa;

- i) i messaggi iniziavano quasi sempre con l'indirizzo completo: (to) ..... from .....;

- j) i cifrari si componevano di due parti: la prima parte, che serviva soprattutto per cifrare gli indirizzi, conteneva i nomi dei Comandi, delle Autorità, delle Unità Navali e, inoltre, i numeri, le date, i gradi e i primi di latitudine e longitudine; la seconda era il vocabolario vero e proprio. In entrambe le parti i gruppi cifranti segreti (quadricifre) erano presi a caso dalla sue naturale da 0001 a 9999, sicché quasi tutte le quadricifre si trovavano sia nella prima che nella seconda parte.

Se l'indirizzo prendeva 1, 2, 3 ....., 9 gruppi, il primo gruppo del messaggio in prima cifratura era, rispettivamente, 1111, 2222, 3333, ..., 9999 per indicare al destinatario che per 1, 2, 3, ... 9 gruppi doveva usare la prima parte del cifrario. Se l'indirizzo prendeva più di 9 gruppi, il primo gruppo era 9900 e alla fine dell'indirizzo veniva posto il gruppo 0099 a indicare di passare ad usare la seconda parte. 0099 era anche posto come primo gruppo quando doveva usare subito la seconda parte anziché la prima. Questa particolarità, che ovviamente avevano scopo mnemonico e rimasero in uso per alcuni anni, facevano sì che le differenze relative al 1° gruppo di coppie di messaggi aventi uguale gruppo indicatore, cioè sopracifrati con lo stesso verme (1) avevano solo i seguenti valori 0000, 1111, 2222, ..., 9999, 1122, 2233, ..., 8899, 2211, 3322,

(1) Vds. parag.2.1. Si ricordi che la differenza fra due gruppi in 2ª cifratura, sopracifrati con lo stesso verme, è uguale alla differenza tra i due rispettivi gruppi in 1ª cifratura.

....., 9988, 1199, 9911. Dalla constatazione di questa singolarità al darne la logica spiegazione, per noi il passo fu breve e ci aprì il primo spiraglio per la penetrazione. Fra l'altro potevamo subito sapere quanti gruppi prendevano gli indirizzi, dove si trovava il gruppo segreto per «from» (che non aveva «omofoni», vedi comma g. e dove iniziava il testo vero e proprio con le sue spesso stereotipate frasi iniziali (riferimento ..., risposta ..., prosecuzione ... etc.).

Ma a mio parere, la più grave imprudenza o imprevidenza inglese fu l'aver mantenuto in uso, per tutto il primo anno di guerra con la Germania, lo stesso cifrario navale principale che era in vigore fin dall'epoca della guerra civile spagnola, penetrato da noi (e dai Tedeschi) fin dal 1938. Quando dovetti lasciare il comando di una unità subacquea per prendere nel SIS la direzione della sezione crittografica in cui avevo lavorato, con poche interruzioni, dal 1934, rimasi sorpreso - ma anche molto lieto - nel constatare che il principale bersaglio era ancora quello contro cui mi ero io stesso cimentato dal 1938 all'inizio del 1940.

Era stato questo il motivo che aveva consentito alla nostra sezione crittografica di decrittare, il 4 luglio 1940, l'ordine di operazioni del Comandante della Mediterranean Fleet, che portò al fatto d'armi di Punta Stilo il 9 dello stesso mese, prima occasione, nella storia, di incontro di guerra fra le due flotte, incontro peraltro rimasto inconcludente (2).

Purtroppo, solo due settimane dopo il mio ritorno al servizio crittografico, gli Inglesi abrogarono quel cifrario sostituendolo con due cifrari diversi e introdussero alcuni accorgimenti che però non ci impedirono di riprendere la padronanza della situazione, per entrambi i nuovi cifrari, dopo qualche mese.

---

(2) Pare che in quella occasione anche gli Inglesi avessero ottenuto informazioni, sebbene piuttosto incomplete, sulla intenzione della nostra flotta, da intercettazioni di nostri segnali in chiaro e anche attraverso decrittazione di radiomessaggi ancora cifrati col nostro cifrario prebellico, penetrato a suo tempo dagli Inglesi, che - forse per difficoltà logistiche - fu da noi sostituito solo a metà luglio 1940.

In definitiva, a conclusione della sommaria analisi tecnica svolta relativamente alla «guerra dei cifrari» ritengo di poter affermare che il servizio crittologico della nostra Marina sopravanzò di parecchie lunghezze l'analogo servizio britannico.

3. - La cifratura meccanica della Marina Italiana

Indicherò con la stessa sigla «C38m» usata dal B.I. la nostra macchina cifrante, che era una modifica - pressoché irrilevante dal punto di vista crittografico - di una macchina cifrante svedese disponibile in commercio.

3.1. - L'adozione della C38m - secondo i miei ricordi personali.

E' noto che una precedente versione di quella macchina, offerta alla nostra Marina dall'inventore e costruttore intorno al 1934-'35, era stata respinta dal SIS dopo un accurato esame condotto da una commissione di 4 crittografi, fra i quali il sottoscritto. Nel 1935 quella stessa macchina, evidentemente ritenuta valida dagli specialisti francesi, fu acquistata in massa per quelle FF.AA..

Qualche anno dopo, forse nel 1938, il costruttore svedese ne presentò al nostro Stato Maggiore un nuovo esemplare nel quale aveva introdotto qualche miglioramento, portando i rotori da 5 a 6; ma il principio originale del meccanismo cifrante era sempre quello del 1935. Non so se fu nuovamente consultato il SIS, dato che io ne ero assente perché imbarcato; fatto sta che più tardi, credo nel corso del 1940, quella macchina fu introdotta, ma solo per le comunicazioni segrete di pochi Alti Comandi, a terra e a bordo. Nel frattempo essa era stata acquistata anche dall'Esercito USA che la usò come sistema di medio livello dai Comandi di Divisione in giù fino ai Battaglioni.

Posso pensare che i miglioramenti apportati dal costruttore e la conoscenza degli acquisti fatti in gran quantità da Francia e USA abbiano indotto i nostri organi tecnico-amministrativi a trascurare il parere negativo espresso dal SIS alcuni anni prima.

Io ritengo che per l'epoca, cioè lo stadio in cui si trovava la crittologia, e per le circostanze che l'accompagnarono, essa trova più di una giustificazione. Altro di-

scorso andrà fatto, come vedremo, per il modo in cui la C38m finì per essere impiegata, specie nel periodo cruciale dei nostri trasporti per il Nord Africa.

3.2. - Funzionamento della C38m - Cifratura e decifrazione

3.2.1. - La C38m realizzava attraverso i suoi meccanismi una cifratura a sostituzione polialfabetica con l'impiego di 26 alfabeti segreti ordinati e rovesciati che si ottengono facendo slittare di un posto alla volta il normale alfabeto anglosassone rovesciato. Questi alfabeti sono riportati parzialmente nella Tavola 1, che può essere usata manualmente per questo tipo di cifratura polialfabetica: ogni lettera del testo chiaro viene sostituita con quella ad essa corrispondente nell'alfabeto segreto di volta in volta usando, secondo una successione che costituisce la «chiave» o «verme» di cifratura. Per esempio, utilizzando la Tavola 1:

verme (cioè n.ri degli alfabeti segreti usati)	**23**	**14**	**0**	**12**	**25**	**2**	**13**	**1**	**15**	**12**	**0**
testo chiaro:	**r**	**i**	**f**	**e**	**r**	**i**	**m**	**e**	**n**	**t**	**o**
testo segreto:	**G**	**G**	**V**	**I**	**I**	**U**	**B**	**X**	**C**	**T**	**M**

La stessa tavola può essere usata per decifrare:

verme:	**23**	**14**	**0**	**12**	**25**	**2**	**13**	**1**	**15**	**12**	**0**
testo segreto:	**G**	**G**	**V**	**I**	**I**	**U**	**B**	**X**	**C**	**T**	**M**
testo chiaro:	**r**	**i**	**f**	**e**	**r**	**i**	**m**	**e**	**n**	**t**	**o**

3.2.2. - Il meccanismo cifrante era costituito da:

- a) un certo numero di elementi metallici nelle parti rotanti e fisse all'interno della macchina; piolini, sbarrette, cursori, ciascuno dei quali poteva essere posto, dall'operatore, in posizione attiva o inattiva, venendo così a formare la cosiddetta «chiave interna», in realtà costituita da due componenti, chiamate W e X. Il numero delle chiavi interne diverse che l'operatore poteva impostare era astronomico, vicino ai ventilioni (un numero di 60 cifre), ma l'impostazione, assai laboriosa, richiedeva molta attenzione e molto tempo, sicché si finiva per dover mantenere in

uso una stessa chiave interna per un tempo non breve.

- b) 6 rotori di uguale diametro, affiancati, calettati su un asse orizzontale, ciascuno dei quali poteva essere fatto ruotare, anche manualmente a mezzo di ingranaggi che avevano diverso numero di denti per i diversi rotori, e precisamente 26, 25, 23, 21, 19, 17.

Tavola I

TAVOLA PER LA CIFRATURA MANUALE POLIALFABETICA
CON ALFABETI REGOLARI ROVESCIATI

(chiaro)		ALFABETI SEGRETI																									(chiaro)
n°		0	1	2	3	. . .	.	.	.	12	13	14	15	. . .	.	.	.	23	24	25							
0	a	A	B	C	D	. . .	.	.	.	M	N	O	P	. . .	.	.	.	X	Y	Z							a
1	b	Z	A	B	C					L	M	N	O					W	X	Y							b
2	c	Y	Z	A	B					K	L	M	N					V	W	X							c
3	d	X	Y	Z	A					J	K	L	M					U	V	W							d
4	e	W	X	Y	Z					I	J	K	L					J	U	V							e
5	f	V	W	X	Y					H	I	J	K					S	T	U							f
6	g	U	V	W	X					G	H	I	J					R	S	T							g
7	h	T	U	V	W					F	G	H	I					Q	R	S							h
8	i	S	T	U	V					E	F	G	H					P	Q	R							i
9	j	R	S	T	U					D	E	F	G					O	P	Q							j
0	k	Q	R	S	T					C	D	E	F					N	O	P							k
11	l	P	Q	R	S	. . .	.	.	.	B	C	D	E	. . .	.	.	.	M	N	O							l
12	m	O	P	Q	R					A	B	C	D					L	M	N							m
13	n	N	O	P	Q					Z	A	B	C					K	L	M							n
14	o	M	N	O	P					Y	Z	A	B					J	K	L							o
15	p	L	M	N	O					X	Y	Z	A					I	J	K							p
16	q	K	L	M	N					W	X	Y	Z					H	I	J							q
17	r	J	K	L	M					V	W	X	Y					G	H	I							r
18	s	I	J	K	L					U	V	W	X					F	G	H							s
19	t	H	I	J	K					T	U	V	W					E	F	G							t
20	u	G	H	I	J					S	T	U	V					D	E	F							u
21	v	F	G	H	I					R	S	T	U					C	D	E							v
22	w	E	F	G	H					Q	R	S	T					B	C	D							w
23	x	D	E	F	G					P	Q	R	S					A	B	C							x
24	y	C	D	E	F					O	P	Q	R					Z	A	B							y
25	z	B	C	D	E	. . .	.	.	.	N	O	P	Q	. . .	.	.	.	Y	Z	A							z
n°		0	1	2	3	. . .	.	.	.	12	13	14	15	. . .	.	.	.	23	24	25							
(chiaro)		ALFABETI SEGRETI																									(chiaro)

Sulla corona esterna di ciascun rotore erano incise, in ordine regolare, le lettere dell'alfabeto anglosassone, rispettivamente da A a Z, da A a Z con esclusione di W, da A a Z con esclusione di W, da A a U, da A a S, da A a Q. Lungo la periferia della faccia di destra di ogni rotore erano alloggiati rispettivamente 26, 25, 23, 21, 19, 17 piolini, in corrispondenza delle altrettante lettere incise sui bordi esterni. Come già accennato, ogni piolino poteva essere posto, dall'operatore, in posizione attiva o inattiva. Il numero e la disposizione dei piolini attivi costituiva la com-

ponente X della chiave interna, come detto poc'anzi. Il numero delle componenti X diverse che l'operatore poteva impostare era grandissimo, 2 elevato alla 131ª potenza (un numero di 40 cifre) anche se molte di esse erano sconsigliabili perché troppo semplici.

3.2.3 - Facendo ruotare a mano ciascuno dei 6 rotori, si potevano allineare le rispettive lettere rispetto a una linea di fede costituita da 6 finestrelle praticate nel coperchio della macchina. L'allineamento, così creato dall'operatore, costituiva la cosiddetta «chiave esterna» che l'operatore doveva impostare prima di iniziare la cifratura del messaggio. Nel corso dell'operazione di cifratura, lettera per lettera, ad ogni «battuta» i 6 rotari avanzavano simultaneamente di un passo (vedi Tavola 2) facendo così entrare in gioco, per cifrare la lettera battuta, uno dei 26 alfabeti segreti di sostituzione della già citata tavola 1, secondo una successione, detta «Verme», che era caotica solo apparentemente, poiché in realtà dipendeva dalla legge di formazione generata delle due componenti W e X della chiave interna predisposta dall'operatore.

Per spiegare l'effetto dell'azione combinata delle componenti W e X della chiave interna sarà meglio fare un esempio, anche se un po' «addomesticato» (vedi Tavola 3).

Abbiamo visto in che cosa consisteva la componente X: i 131 (cioè 26+25+23+21+19+17) piolini posti parte in posizione attiva e parte inattivi. La componente W (3) era in realtà costituita da 7 componenti, una per ogni rotore (W_1 W_2 W_3 W_4 W_5 W_6) e una (W_o) indipendente dai rotori. Quando l'operatore impostava la chiave interna poteva far assumere al W_o i valori 1 o 2 e a ciascuno dei restanti w valori da 1 a 9 (4) ma la somma dei sette W doveva dare sempre 27.

---

(3) Per brevità omettiamo di descrivere la struttura meccanica, piuttosto complessa, della componente W. Diciamo solo che si trattava di un cilindro con alcuni cursori, e di sbarrette che l'operatore poteva predisporre in posizione attiva o inattiva.

(4) Materialmente quelli che per semplicità abbiamo chiamato «valori 1 o 2 e valori da 1 a 9» erano il numero di sbarrette poste in posizione attiva dall'operatore (vedi nota precedente).

Consideriamo l'allineamento che nella Tavola 2 corrisponde alla posizione 30 000 000 nel verme generato dalla chiave interna impostata dall'operatore, di cui riportiamo qui di seguito la componente W (vedi Tavola 3):

rotori	**1**	**2**	**3**	**4**	**5**	**6**	**0**
componente	**W**	**5 + 1**	**+8 + 2**	**+6 + 3**	**+2 = 27**		
allineamento (chiave esterna)	**E**	**A**	**T**	**J**	**H**	**P**	

Secondo la componente X della chiave interna predisposta, i 6 piolini alloggiati nei 6 rotori sotto le 6 lettere

Tavola 2

SCHEMA DELLA GENERAZIONE DI UN «VERME» COMPLETO RELATIVO A UNA DATA CHIAVE INTERNA E DELLA CIFRATURA DI UN MESSAGGIO CON CHIAVE ESTERNA DATA

	ROTORI 1 (26)	2 (25)	3 (23)	4 (21)	5 (19)	6 (17)	posizione nel verme	(verme) n° della allabeto segreto		
	A	A	A	A	A	A	0	8		
	B	B	B	B	B	B	1	11		
	C	C	C	C	C	C	2	13		
	D	D	D	D	D	D	3	11		
	.	.	.	.	.	.	.	.		
	Q	Q	Q	Q	Q	Q	16	17		
	R	R	R	R	R	A	17	2		
	S	S	S	S	S	B	18	11		
	T	T	T	T	A	C	19	12		
	U	U	U	U	B	D	20	1		
	V	V	V	A	C	E	21	18		
	W	X	X	B	D	F	22	2		
	X	Y	A	C	E	G	23	12		
	Y	Z	B	D	F	H	24	8		
	Z	A	C	E	G	I	25	13		
	A	B	D	F	H	J	26	5		
	.	.	.	.	.	.	.	.		
(.) chiave esterna	E	A	T	J	H	P	30 000 000	14	vedi Tavola 1 chiaro	segreto
	F	B	U	K	I	Q	30 000 001	23	r	G
	G	C	V	L	J	A	» 2	14	i	G
	H	D	X	M	K	B	» 3	0	l	V
	I	E	A	N	L	C	» 4	12	e	I
	J	F	B	O	M	D	» 5	25	r	I
	K	G	C	P	N	E	» 6	2	l	U
	L	H	D	Q	O	F	» 7	13	m	B
	M	I	E	R	P	G	» 8	1	e	X
	N	J	F	S	Q	H	» 9	15	n	C
	O	K	G	T	R	I	» 10	12	t	T
	P	L	H	U	S	J	» 11	0	e	M
	Q	M	I	A	A	K	» 12	3	v	I
	R	N	J	B	B	L	» 13	14	e	A
	S	O	K	C	C	M	» 14	24	s	G
	.	.	.	.	.	.	.	.	.	.
	Y	Y	V	T	R	P	101 405 848	13	.	.
	Z	Z	X	U	S	Q	101 405 849	15	.	.
	A	A	A	A	A	A	0	8		
	B	B	B	B	B	B	1	11		

dell'allineamento dato e in quelli successivi, nel corso della cifratura, potevano trovarsi in posizione attiva o inattiva. Quelli attivi rendevano attivo il rispettivo w mentre quelli inattivi lo lasciavano inattivo. Il W_0 indipendente dai rotori, era però sempre attivo. Ad ogni avanzamento simultaneo dei 6 rotori i meccanismi interni della macchina facevano entrare in gioco l'alfabeto segreto di sostituzione avente il numero d'ordine (vedi Tavola 1) uguale alla somma, con modalità 26, dei w attivi. L'alfabeto entrato in gioco cifrava la lettera che era stata battuta e che aveva provocato l'avanzamento dei rotori.

Tavola 3

GENERAZIONE DEL «VERME» DI CIFRATURA
PER IL MESSAGGIO DELLA TAVOLA 2

Componente W della chiave interna								
Rotori	(1)	(2)	(3)	(4)	(5)	(6)	(0)	verme n° dello alfabeto segreto
w_1	5	w_2 1	w_3 8	w_4 2	w_5 6	w_6 3	w_0 2	
posiz. 30 000 000	E	A	T	J	H	P		
	+5		+8	+2	6		+2	= 23
" 30 000 001	F	B	U	K	I	Q		
	·	+1	·	+2	+6	+3	+2	= 14
" " 2								
	+5	·	+8	+2	+6	+3	+2	= 26 = 0
" " 3								
	·	·	+8	+2	·	·	+2	= 12
" " 4								
	+5	+1	+8	·	+6	+3	+2	= 25
" " 5								
	·	·	·	·	·	·	+2	= 2
" " 6								
	+5	·	·	·	+6	·	+2	= 13
" " 7								
	+5	+1	+8	+2	+6	+3	+2	= 27 = 1
" " 8								
	+5	·	+8	·	·	·	+2	= 15
" " 9								
	·	+1	·	·	+6	+3	+2	= 12
" " 10								
	+5	·	+8	+2	+6	+3	+2	= 26 = 0
" " 11								
	·	+1	·	·	·	·	+2	= 3
" " 12								
	·	+1	+8	·	·	+3	+2	= 14
" " 13	R	N	J	B	B	L		
	+5	+1	+8	+2	+6		+2	= 24
" " 14								

verme (per gli alfabeti segreti di sostituzione vedi Tav. 1)

Componente X della chiave interna

+ piolino in posizione attiva
· " " " inattiva

Possiamo ora renderci conto, nella Tavola 3, di come è stata generata la porzione di verme che ha cifrato il testo riportato nella Tavola 2.

Per quanto riguarda la chiave esterna, abbiamo già visto che essa era costituita dall'allineamento impostato dall'operatore prima di iniziare la cifratura, nel corso della quale i 6 rotori avanzavano simultaneamente di un passo alla volta. Poiché un giro completo di ciascuno dei 6 rotari comportava un numero di passi diverso: 26, 25, 23, 21, 19, 17, un allineamento impostato all'inizio si ripresentava identico solo dopo 26 x 25 x 23 x 21 x 19 x 17 = 101 405 850 passi simultanei dei 6 rotori (vedi Tavola 2). Questa era dunque la «lunghezza» totale del verme generato dalla chiave interna. Ovviamente, ad ogni chiave interna possibile corrispondeva un verme totale, sempre di quella lunghezza, ma dis struttura (cioé: successione degli alfabeti segreti) sempre diversa.

3.3. - Decrittazione della C38m

3.3.1 - Riprendiamo in esame l'esempio di cifratura riportato nel punto 3.2.1 e nella Tavola 2:

Verme	**(V)**	**23**	**14**	**0**	**12**	**25**	**2**	**13**	**1**	**15**	**12**	**0**	**3**	**14**	**24**
Chiaro	**(C)**	**r**	**i**	**f**	**e**	**r**	**i**	**m**	**e**	**n**	**t**	**o**	**v**	**o**	**s**
SEGRETO	**(S)**	**G**	**G**	**V**	**I**	**I**	**U**	**B**	**X**	**C**	**T**	**M**	**I**	**A**	**G**

Sostituiamo ad ogni lettera il numero che indica la posizione da essa occupata nell'alfabeto ordinato (A = 0, Z = 25, vedi Tavola 1) e riscriviamo il tutto (vedi Tavola 4, sezione I). Constatiamo che ogni lettera segreta può essere ottenuta sottraendo algebricamente, con modalità 26, la lettera chiara dal rispettivo elemento del verme (V-C = S)

27 - 17 = 6, 14 - 8 = 6, 0 - 5 = -5 + 26 = 21,....

2 - 8 = -6 + 26 = 20, etc.

Dunque, l'operazione di cifratura è identica a quella della sopracifratura nel caso dei cifrari numerici descritta nel punto 2.1, con l'enorme vantaggio, per il decrittatore, che in questo caso non esiste codice segreto; anzi si potrebbe addirittura dire che il codice gli è talmente noto che lo conosce tutto a memoria (se è padrone della lingua).

3.3.2 - Stando così le cose, le decrittazioni di due messaggi cifrati con lo stesso verme non è più un problema serio. Infatti, se si può ipotizzare l'esistenza, in uno dei due testi, di parole o frasi «probabili» - come spesso accade specialmente per i tratti iniziale e finali dei messaggi - si può controllare direttamente sull'altro la validità della ipotesi perché (vedi Tavola 4, Sezione II) essendo, come già detto nel punto 2.1, $S_1-S_2 = C_2-C_1$ si ha $S_1-S_2+C_1 = C_1 = C_2$ e $S_2-S_1+C_2 = C_1$.

Di solito sono sufficienti pochi tentativi per avviare una decrittazione che poi può proseguire passo passo senza grandi difficoltà, fornendo contemporaneamente gli elementi della porzione del verme che ha cifrato i due messaggi:

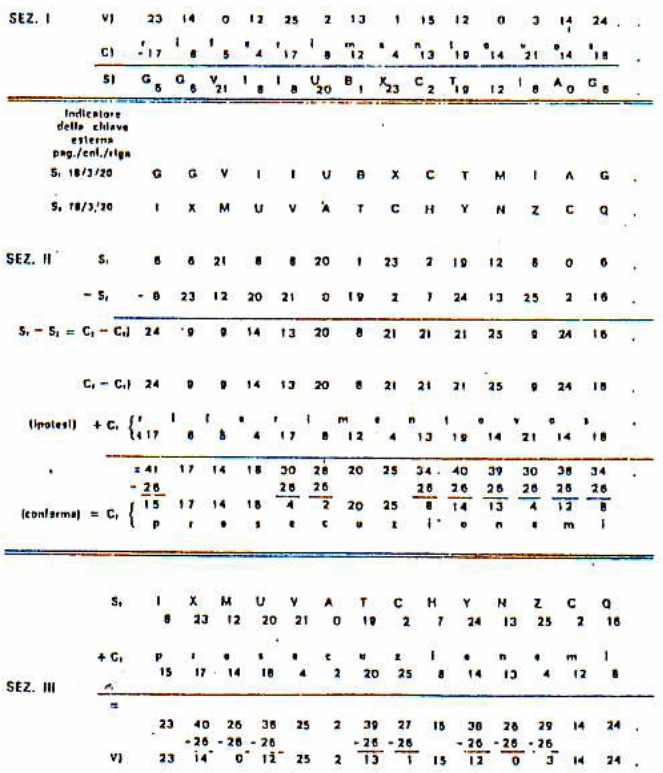
$V-S_2 = C_2$, quindi $S_2+C_2 = V$ (vedi Tavola 4, Sez.III).

3.3.3 - Ultimata la decrittazione (anche se incompleta) dei due messaggi, il decrittatore ha in mano un buon tratto del verme generato dalla chiave interna predisposta dal cifratore. A questo punto, mentre nessuna supposizione sulle rimanenti porzioni del verme sarebbe possibile, in situazione analoga, nel caso di cifrari numerici sopracifrati con vermi casuali o incoerenti (vedi para 2), nel caso della C38m un crittografo abile, se conosceva profondamente la macchina, era in grado di entrare in possesso di tutto il verme (101 405 850 elementi) attraverso la ricostruzione delle componenti W e X delle chiavi interne (vedi Tavola 3) impostando e risolvendo equazioni con un numero di incognite da 1 a 6, oppure empiricamente con reiterati tentativi. Di solito è sufficiente disporre di circa 100 elementi del verme per ricostruire la chiave interna; in casi fortunati possono bastare 40 elementi circa.

Va precisato che il verme così ottenuto dal decrittatore è uguale a quello generato dalla macchina del cifratore ma è «sfasato» rispetto ad esso, nel senso che l'elemento al quale il decrittatore assegna arbitrariamente la posizione 0 (chiave esterna AAAAAA) in realtà occupa nel verme originale una posizione sconosciuta, fra 0 e 101 405 849. Per chiavi interne diverse di sfasamenti saranno, in un primo tempo, diversi ma si riuscirà a mano a mano a ridurli a uno sfasamento arbitrario comune.

Tavola 4

ESEMPIO DI DECRITTAZIONE DI DUE MESSAGGI CIFRATI CON LO STESSO «VERME» E RICOSTRUZIONE DELLA RELATIVA PORZIONE DI «VERME» COL METODO DELLA «PAROLA PROBABILE»



3.3.4 - Una volta in possesso di una chiave interna e quindi di tutto un verme, i crittografi inglesi sarebbero stati in grado di decrittare tutti i messaggi cifrati con quella chiave interna e con qualsiasi chiave esterna senza essere minimamente disturbati dallo sfasamento accennato poco anzi. Ma, data la lunghezza del verme, il numero di prove da fare era così grande che non mi è possibile ora azzardare un giudizio su quale poteva essere il rendimento di tale lavoro, che dipendeva dalla quantità di personale impiegato e, soprattutto, dal sostanziale ausilio di speciali apparec-

chiature «ad hoc» che la tecnologia congiunta anglo-americana era in grado di produrre nel 1941 (5). Comunque, in generale, tali decrittazioni potevano risultare tempestive solo casualmente e certamente il lavoro più redditizio, come quantità e tempestività, era quello di «attaccare» direttamente ogni messaggio ipotizzando l'esistenza di parole o frasi probabili che, se azzeccate, fornivano una porzione di verme di cui non era difficile individuare la posizione occupata nel verme totale, individuare cioè la chiave esterna (fittizia, cioè arbitraria) impostata dal cifratore avversario e quindi decrittare tutto il messaggio.

Nella Tavola 5 è riportato un esempio di determinazione della chiave esterna di un messaggio (S), con chiave interna X e W già nota, partendo dal possesso di un porzione di verme (V) ottenuta ipotizzando il probabile inizio del testo in chiaro (C):

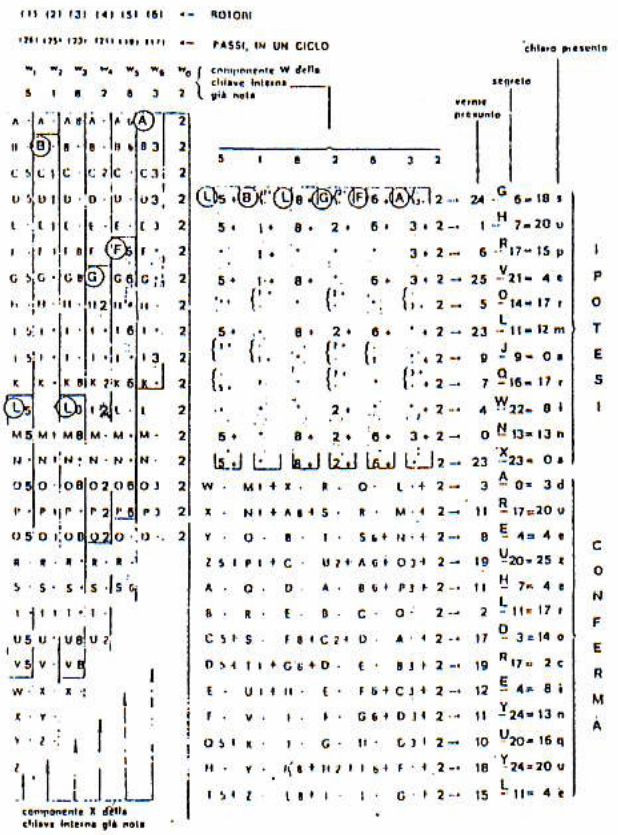
(S)	G 6	H 7	R 17	V 21	O 14	L 11	J 9	Q 16	W 22	N 13	X 23	A R E U H L D R E Y U Y	
+(C)	s 18	u 20	p 15	e 4	r 17	m 12	a 0	r 17	i 8	n 13	a 0		
	24	27	32	25	31	23	9	33	30	26	23		
		-26	-26		-26			-26	-26	-26			
=(V)	24	1	6	25	5	23	9	7	4	0	23		

Può sembrare che con tale metodo la decrittazione sia affidata soltanto al caso; ma se i decrittatori possiedono una profonda esperienza e conoscenza degli argomenti trattati nei messaggi, delle abitudini dei cifratori, del mondo con cui iniziano e terminano di solito i testi, del frasario usato, etc., il metodo anzidetto può divenire quello normale e sistematico e sovente può fruttare anche decrittazioni tempestive.

(5) Lo stesso B.I. accenna più volte all'uso di apparecchiature del genere (le «Bombes», elettromeccaniche; il «Colossus», elaboratore elettronico) nel lavoro di penetrazione del traffico radiocifrato ENIGMA. Del resto anche noi, per accelerare il lavoro contro i cifrari navali inglesi sopracifrati, avevamo realizzato, nel 1942, una modesta apparecchiatura che, utilizzando schede perforate, eseguiva le numerose prove necessarie per individuare quali porzioni di un lungo verme, già da noi ricostruito, avevano sopracifrato altri messaggi non ancora decrittati.

Tavola 5

ESEMPIO DI DETERMINAZIONE DELLA «CHIAVE ESTERNA» ("LBLGFA" POSIZ. 30 002 401) E CONSEGUENTE DECRITTAZIONE DI UN MESSAGGIO CON IL METODO DELLA «PAROLA PROBABILE»



3.3.5 - Il reperimento, nel traffico intercettato, di due o più messaggi cifrati con uguale verme è ovviamente immediato se i «gruppi indicatori» delle chiavi esterne usate non sono «mascherati», come nell'esempio della Tavola 4; altrimenti, ma con maggior lavoro e minor possibilità di successo, si devono ricercare porzioni di cifrato uguali in messaggi diversi, di solito all'inizio e alla fine del testo segreto.

3.3.6 - Se non esistono casi di «reimpiego» di verme, cosa possibile anzi probabile se l'avversario ha impartito oculate norme d'impiego della macchina, non rimane che «attaccare» i messaggi uno alla volta con il metodo delle «parole o frasi probabili» già menzionato, fino a disporre di

tratti di verme abbastanza sicuri e abbastanza lunghi da riuscire a ricostruire le chiavi interne e procedere poi come detto nei punti 3.3.3 e 3.3.4.

3.3.7 - Per concludere, da quanto finora esposto, si evince che la macchina cifrante C38m offriva possibilità di penetrazione incomparabilmente maggiori di quelle offerte dal sistema cifrari navali/sopracifratura descritto nel paragrafo 2.

3.4. - L'uso della C38m da parte della Marina italiana durante il conflitto

3.4.1 - Si tenga presente che, la scelta, la produzione, la regolamentazione la distribuzione dei sistemi di cifratura e il controllo sul loro impiego non erano compiti del SIS - Servizio crittografico, bensì del Reparto Telecomunicazioni (TLC). Il servizio crittografico forniva solo consulenze quando ne era richiesto ma, mentre so con certezza che ciò accade e fu determinante per la sicurezza del complesso «cifrari-sopracifratura» del periodo bellico, ignoro se e in quale misura ciò sia avvenuto per la C38m.

Tavola 6

QUANTITA' DI CHIAVI ESTERNE ASSEGNATE AI VARI COMANDI

2ª Edizione in vigore dal marzo 1942		R.P.
Supermarina e M.M.	3 500	300
Reparto Comunicazioni		200
Com. FF.NN. e Com. 1ª Sq.	500	100
Com. 2ª Sq. e Com. 5ª Div.	300	100
Com. 3ª Div.	200	100
Com. 7ª Div.	200	100
Com. 8ª Div.	200	100
Com. 9ª Div.	200	100
Marina Napoli	200	100
» Taranto	200	100
» Messina	200	100
» Brindisi	200	100
» Albania	500	100
» Morea	1 500	100
» Sud est	800	100
» Egeo	800	100
» Lero	300	100
» Libia	2 000	100
» Tripoli	1 000	100
» Bengasi	500	100
» Tobruk	—	100
Riserva	1 700	600
Totale	15 000	3 000

3ª Edizione (aprile 1942) in vigore dal maggio/giugno 1942	
Supermarina	1 200
Reparto Comunicazioni	1 800
Com. FF.NN. e Com. 1ª Sq.	300
Com. 2ª Sq. e Com. 5ª Div.	200
Com. 3ª Div.	100
Com. 7ª Div.	100
Com. 8ª Div.	100
Com. 9ª Div.	100
Marina Napoli	200
» Taranto	200
» Messina	200
» Brindisi	00
» Albania	500
» Morea	1 200
» Sud est	800
» Egeo	1 200
» Lero	600
» Libia	1 500
» Tripoli	800
» Bengasi	800
Riserva	2 900
Totale	15 000

3.4.2 - Secondo gli elenchi di distribuzione contenuti nei documenti tuttora reperibili le autorità dotate della C38m erano pochissime (6): Solo Alti Comandi a terra e a bordo (vedi Tavola 6 e para 3.4.5), nessuna unità singola di superficie o subacquea.

3.4.3 - Il numero astronomico, intorno ai ventilioni, delle possibili chiavi interne diverse offriva, in teoria, ottime garanzie di sicurezza che però in pratica non potevano essere sfruttate appieno perché la impostazione delle chiavi interne era così delicata, laboriosa e lunga (si pensi che per la sola componente X si dovevano manipolare 131 piolini) che si dovette rinunciare a cambi frequenti come sarebbe stato desiderabile. Perciò all'inizio si stabilì di usare chiavi interne comuni a tutti gli utenti e di cambiarle ogni mese. Questa norma, in vigore almeno fino a tutto il 1942, ma probabilmente fino all'armistizio, era certamente accettabile nel primo periodo del conflitto, con traffico radio C38m non inteso (B.I. dice: nel mese di agosto 1941, 600 messaggi) (7), ma, a mio parere, fu imprudente mantenerla quando quel traffico stava acquistando intensità sempre crescente (B.I. dice: 4000 messaggi nel mese più denso, luglio 1942). In quella situazione fu preferito aumentare il numero delle chiavi esterne a disposizione, passando da 18 00 a circa 40 000.

3.4.4 - Era stato giustamente percepito che il pericolo maggiore stava nel «reimpiego» dei vermi, cioè due o più passaggi cifrati, nello stesso mese, con la stessa chiave esterna; perciò questo fu tassativamente proibito e a ciascuna delle autorità depositarie della C38m furono assegnate serie di chiavi non usabili dalle altre autorità.

Naturalmente non posso escludere che vi sia stata qualche trasgressione alle norme, ma deve essersi trattato di casi del tutto eccezionali, dato il numero delle chiavi esterne a disposizione. Nella Tavola 6 è riportato il prospetto numerico delle assegnazioni delle chiavi esterne nella 2ª e 3ª edizione delle cosiddette «Tabelle delle chiavi esterne per macchina cifrante». Della 1ª edizione non ho

---

(6) Pochissime, in confronto col numero di utenti del cifrario navale generale sopracifrato, che era assegnato anche a quasi tutte le unità navali e ai Comandi Marina minori.

(7) B.I., vol.2°, pag.283.

trovato traccia.

Questi quantitativi erano, a mio parere, oculatamente commisurati alla prevedibile intensità del traffico radio C38m di ogni mese, cioè nell'ambito di una data chiave interna.

3.4.5 - Fin qui, tutto bene; ma vediamo come erano state scelte le chiavi esterne e poi vedremo in che modo veniva indicata, in ogni messaggio, la chiave usata.

Come abbiamo visto nel paragrafo precedente, le chiavi esterne teoricamente possibili erano 101 405 850, ma ci si doveva giustamente preoccupare di evitare che la porzione iniziale di un messaggio potesse casualmente venire cifrata con il tratto di verme che aveva, o avrebbe poi, cifrato la «coda» di un altro messaggio, per non fornire all'avversario un reimpiego, sia pure parziale, di verme. A tal fine, poiché era prescritta per ogni messaggio una lunghezza massima di 500 lettere, si dovevano distanziare le chiavi esterne nel verme totale, generato dalla chiave interna, di un numero di elementi maggiore di 500. Per non ridurre troppo la quantità di chiavi disponibili sarebbe stato largamente sufficiente un distacco medio di circa 1 000 elementi, che avrebbero ridotto in maniera non preoccupante il numero delle chiavi esterne possibili, cioè circa 100.000 (101 405 850 : 1 000.

Fu invece scelto un distanziamento maggiore, che riduceva a circa 40 000 le chiavi esterne disponibili. Evidentemente si pensò, con qualche fondamento, che quel numero era più che sufficiente per coprire le esigenze di un mese. La riduzione predetta non avrebbe recato sensibile vantaggio ai crittografi inglesi perché, una volta ricostruita attraverso fortunate descrizioni la chiave interna del mese, per individuare la chiave esterna di ogni altro messaggio nello stesso mese, avrebbero ugualmente dovuto «provare» tutti i circa cento milioni di possibili chiavi esterne. Ho usato il condizionale perché, purtroppo, nella nostra pianificazione il distanziamento fra le chiavi fu stabilito in un numero fisso di elementi: 2497. Stando così le cose, l'avversario, dopo aver individuato, attraverso qualche decrittazione di messaggi intercettati in un certo mese, alcune chiavi esterne (arbitrarie), poteva constatare che esse erano tutte distanziate fra loro, nel verme totale, di un multiplo di 2497

(8) e a questo punto aveva la possibilità di individuare, con un semplice calcolo, tutte le 40 611 chiavi esterne (arbitrarie) previste nella nostra pianificazione, riducendo così di circa cento milioni a solo circa 40 000(nel caso peggiore) (9) le «prove» da fare per decrittare ogni altro messaggio del mese (10).

Non posso pensare che ai crittografi inglesi sia sfuggita questa imprudente particolarità della nostra pianificazione, devono essersene accorti abbastanza presto e ne hanno certo tratto gran vantaggio per decrittare quei messaggi, ritenuti importanti, che avevano resistito all'attacco diretto con il metodo delle parole o frasi probabili (vedi punto 3.3.5).

3.4.6. - E veniamo ai «gruppi indicatori», come primo e ultimo gruppo del messaggio segreto per indicare al destinatario quale chiave esterna aveva impostato nella macchina prima di iniziare la cifratura di quel messaggio.

I fascicoli che contenevano le «Tabelle delle chiavi esterne» avevano un certo numero di pagine, ripartite fra i vari utenti in base al quantitativo di chiavi a ciascuno assegnate (vedi Tavola 6). Ogni pagina conteneva, disposte su righe e colonne, un certo numero di chiavi prese a caso, senza mai ripeterle, fra le 40 611 della pianificazione. Il cifratore sceglieva ogni volta, in una delle pagine di sua

---

(8) Vedi Tavola 7, in cui sono riportate alcune «chiavi esterne» prese a caso dalle nostre Tabelle delle «chiavi esterne» in uso nel 1941/'42, con le rispettive posizioni nel verme totale, le distanze parziali e le rispettive scomposizioni in fattori primi.

(9) In realtà, poiché il decrittatore non conosceva la posizione, nel verme originale, a partire dalla quale essa stata sviluppata la nostra pianificazione delle 40 611 chiavi a passo 2 497, e poiché 101 405 850 non è multiplo di 2 497, le prove da fare, in un primo tempo, erano circa 80 000 nel caso peggiore, ma presto - a mano a mano che si allargava il campo delle chivi identificate - le prove diminuivano fino a ridursi, nel caso peggiore, a un massimo di circa 40 000.

(10 Qualcosa di simile accadde anche nel nostro lavoro contro i cifrari navali inglesi sopracitati: ci accorgemmo che i vermi prelevati da uno stesso blocco di tabelle di sopracifratura erano distanziati fra loro sempre di un multiplo di 20 elementi (5 quadricifre). Così potemmo ridurre dell'80% le prove da fare.

pertinenza, la chiave da usare e la «smarcava» a matita per evitarne un secondo impiego prima di aver smarcato tutte quelle a sua disposizione. Ultimata la cifratura del messaggio, poneva come 1° e ultimo gruppo del testo segreto un «gruppo indicatore» che, attraverso apposito indice (cioè non in modo esplicito come per semplicità abbiamo posto nell'esempio della Tavola 4, Sezione II), forniva al destinatario pagina, colonna e riga di appartenenza della chiave scelta.

Con tale procedimento è ovvio che solo chi possiede i predetti fascicoli segreti era in grado di interpretare i gruppi indicatori, conoscere cioè le chiavi esterne impiegate nei messaggi. Con una certa imprudenza, fino all'autunno 1942, i gruppi indicatori furono usati senza «mascheratura» di modo che, per l'avversario, gruppi indicatori uguali significavano chiavi esterne uguali. Questa imprudenza, analoga a quella, che si rilevò ben più pericolosa, commessa dagli Inglesi nella sopracifratura dei loro cifrati navali (vedi para 2.3, comma e.), fu probabilmente dovuta all'affidamento posto nella rigida ottemperanza delle norme che vietavano tassativamente il reimpiego delle chiavi. Comunque, vediamo quali potevano essere le conseguenze, a vantaggio dei crittografi inglesi, della «non mascheratura» dei gruppi indicatori. Distinguiamo vari casi:

- a) gruppi indicatori usati una sola volta. Nessuna utilità per i decrittatori;

- b) gruppi indicatori usati due volte in un dato periodo di validità della chiave interna (cioè nel mese). Era il classico caso di due messaggi cifrati con lo stesso verme: conseguenze gravissime (vedi punti da 3.3.2 a 3.3.5 e Tavola 4). Tuttavia, ripeto, un evento del genere non doveva verificarsi e, se eccezionalmente è accaduto, non giustifica, a mio parere, la penetrazione sistematica e tempestiva affermata da B.I.;

- c) gruppi indicatori usati due volte ma in mesi diversi, cioè con chiavi interne diverse e quindi non con lo stesso verme. Questo evento, anche esso vietato dalle norme, poteva eccezionalmente verificarsi a distanza di mesi per esaurimento delle chiavi assegnate ad un dato utente (ma erano previste chiavi di riserva, vedi Tavola 6). Poteva essere di qualsiasi utilità, se i due messaggi venivano decrittati, per fissare fra loro i vermi totali relativi alle

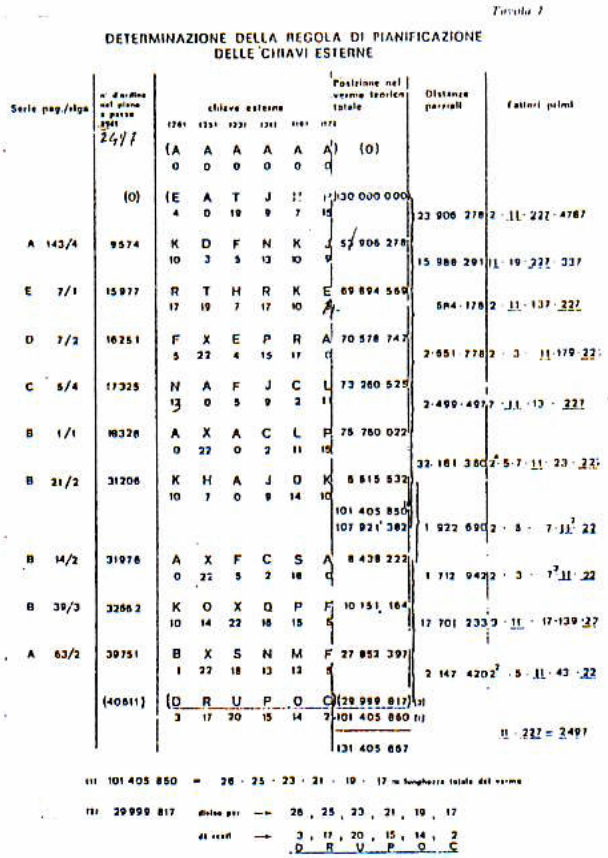


Tavola 1

DETERMINAZIONE DELLA REGOLA DI PIANIFICAZIONE DELLE CHIAVI ESTERNE

Serie pag./riga	n. d'ordine nel piano a passo 2441	chiave esterna	Posizione nel vermo teorico totale	Distanze parziali	Fattori primi
	2411	(A A A A A A)	(0)		
		0 0 0 0 0 0			
	(0)	(E A T J)	(30 000 000)		
		4 0 19 9 7 15		23 906 278	2 · 11 · 227 · 4787
A 143/4	9574	K D F N K J	53 906 278		
		10 3 5 13 10 9		15 988 291	11 · 19 · 227 · 337
E 7/1	15977	R T H R K E	69 894 569		
		17 19 7 17 10 4		584 178	2 · 11 · 137 · 227
D 7/2	16251	F X E P R A	70 578 747		
		5 22 4 15 17 0		2 651 778	2 · 3 · 11 · 179 · 22
C 5/4	17325	N A F J C L	73 260 525		
		13 0 5 9 2 11		2 499 497	7 · 11 · 13 · 227
B 1/1	18328	A X A C L P	75 760 022		
		0 22 0 2 11 15		32 161 380	2^2 · 5 · 7 · 11 · 23 · 227
B 21/2	31206	K H A J O K	8 815 532		
		10 7 0 9 14 10			
			101 405 850		
			107 921 382	1 922 690	2 · 5 · 7 · 11^2 · 22
B 14/2	31978	A X F C S A	8 438 222		
		0 22 5 2 18 0		1 712 942	2 · 3 · 7^2 · 11 · 22
B 39/3	32862	K O X Q P F	10 151 164		
		10 14 22 16 15 5		17 701 233	3 · 11 · 17 · 139 · 227
A 63/2	39751	B X S N M F	27 853 397		
		1 22 18 13 12 5		3 147 420	2^2 · 5 · 11 · 43 · 22
	(40811)	(D R U P O C)	(29 999 817)		
		3 17 20 15 14 2	101 405 850		
			131 405 667		11 · 227 = 2497

(1) 101 405 850 = 26 · 25 · 23 · 21 · 19 · 17 = lunghezza totale del verme

(2) 29 999 817 diviso per → 26 , 25 , 23 , 21 , 19 , 17

di resti → 3 , 17 , 20 , 15 , 14 , 2
D R U P O C

due chiavi interne ricostruite (vedi punto 3.3.3) e poi sfruttare meglio altri eventuali reimpieghi di gruppi indicatori fra i due mesi interessati.

Con l'edizione delle «Tabelle delle chiavi esterne» entrata in vigore il 1° ottobre 1942 fu introdotta finalmente una buona procedura per mascherare i gruppi indicatori. Ciò fa pensare che nell'estate 1942, periodo di massima intensità del traffico radio C38m, qualche trasgressore alle norme sia realmente avvenuta e sia stata constatata dal servizio di controllo esercitato dal reparto Comunicazioni dello Stato Maggiore Marina. Si dovrebbe anche dedurre che trasgressori preoccupanti non ve ne siano state in precedenza, se con le edizioni entrate in vigore nel marzo e maggio/giugno 1942 fu mantenuta la «non mascheratura» dei

gruppi indicatori.

3.4.7. - I testi in chiaro dei messaggi segreti

Qui stava, a mio parere, un altro punto debole del nostro traffico radio C38m, forse quello che - dopo una laboriosa e fortunata penetrazione iniziale - ha progressivamente agevolato sempre più i decrittatori inglesi, a mano a mano che acquistavano esperienza e conoscenza degli argomenti e del modo in cui essi venivano trattati nei messaggi. Inizi e finali stereotipati, abitudini dei cifratori, ed altro, devono aver permesso ai decrittatori di azzardare, spesso con fondamento, parole e frasi probabili, come ho accennato nel punto 3.3.2, per «attaccare» messaggi singoli senza bisogno di attendere i reimpieghi di verme, forse veramente rarissimi. Nei periodi di massima intensità del traffico radio questo può essere stato il modo più generalizzato per penetrare largamente le nostre comunicazioni C38m.

3.5. - La penetrazione inglese nella C38m della Marina italiana

3.5.1. - La C38m, come le altre macchine HAGELIN che da due decenni l'avevano preceduta nel mercato non era sconosciuta per gli inglesi.

Quella ditta era svedese, con fabbrica a Stoccolma, e il suo titolare, uomo d'affari anch'esso svedese subito dopo l'occupazione nazista della Norvegia aveva raggiunto gli Stati Uniti d'America, piazzando subito una cinquantina di esemplari presso le FF.AA. americane. Già nel 1935, come detto nel parag.3.1., aveva largamente fornito le FF.AA. francesi. La macchina doveva dunque essere ben nota agli Inglesi che non avranno mancato di studiarla attentamente dal punto di vista della sicurezza crittografica.

C'è da supporre con fondamento che, data l'alleanza con la Francia e gli stretti legami con gli Americani, qualche esemplare molto simile alla C38m fosse già nello loro mani all'inizio del conflitto.

Nonostante questa situazione decisamente vantaggiosa gli Inglesi, dopo avere constatato l'uso della C38m nelle comunicazioni radio segrete della Marina italiana, per ben se mesi, dal dicembre '40 al giugno '41, non ottennero alcun risultato.

3.5.2. - Vediamo cosa dicono gli Inglesi. Nel 2° volume del B.I. a pag.22 si legge:

«La C38m italiana, intercettata per la prima colta nel dicembre 1940, fu penetrata a partire dall'estate 1941» e a pag.283-284:

«Per la fine di giugno 1941 furono ricostruite le chiavi interne della C38m per i mesi di maggio e giugno e furono letti un po' di messaggi attuali. La prima intelligence da quella fonte per il Medio Oriente fu inviata il 23 giugno 1941. (...omissis) Per il 10 luglio furono ricostruite le chiavi interne di luglio, dopodiché si andò avanti fino all'armistizio decrittando regolarmente (with routine) con poco o nessun ritardo e con interruzioni progressivamente sempre più brevi alla fine di ogni mese, quando gli Italiani introducevano nuove chiavi interne, ma con interruzioni più serie in una o due occasioni durante il 1942. Verso la fine del 1941 le interruzioni mensili furono ridotte a meno di tre giorni e verso la fine del 1942 a meno di 24 ore».

Dunque, fra dicembre '40 e giugno '41;
- a) non ci sono stati casi di reimpiego di vermi, cosa verisimile dato il tassativo divieto della nostra regolamentazione, specie in rapporto al non ancora intenso traffico C38m; oppure
- b) se c'è stato qualche reimpiego, gli Inglesi non hanno saputo sfruttarlo, cosa poco verosimile;
- c) non avendo decrittato messaggi, i crittografi inglesi non hanno ancora acquisito né l'esperienza tale da poter applicare con successo il metodo delle «parole e frasi probabili» (vedi punti 3.3.4 e 3.3.6) né la conoscenza del punto debole della nostra pianificazione delle chiavi esterne (vedi punto 3.4.3).

Nonostante tutto ciò, a fine giugno '41 gli Inglesi hanno «sfondato» la C38m in maniera tale da poter ricostruire anche le chiavi interne del mese precedente, ricostruite in 10 giorni le chiavi interne di luglio e da quel momento iniziare una decrittazione sistematica e tempestiva, addirittura «with routine», tanto da «dare dal luglio 1941 in poi notizie in anticipo di praticamente ogni convoglio o nave isolata che partivano con truppe e rifornimenti attraver-

so il Mediterraneo, identificando di solito le navi di scorta coinvolte» (11).

Quale improvvisa folgorazione ha illuminato le menti dei crittografi inglesi sul finire della primavera 1941? Francamente un così rapido e sostanziale salto di qualità e di quantità mi lascia perplesso.

Si deve pensare che nella primavera del 1941 sia accaduto qualcosa che ha aiutato in modo sostanziale gli inglesi a "sfondare" la nostra C38m. Soltanto il Naval Intelligence britannico potrebbe rivelare che cosa accadde.

4. CONCLUSIONE

Da quanto ho esposto si conferma, a mio parere, che nel 2° conflitto mondiale il servizio crittografico della Marina italiana - sotto l'aspetto strettamente tecnico e tenuto conto dei diversi gradi di difficoltà e di vulnerabilità dei sistemi contrapposti - non ha avuto nulla da invidiare a quello britannico. Tutt'altro.

Tengo però a precisare che la valutazione semplicistica sopra riportata non ha valore assoluto nei riguardi del confronto con i nostri avversari di allora, perché non dimentico la vasta ed efficiente penetrazione inglese nelle radiocomunicazioni cifrate con la ENIGMA tedesca, problema che presentava un grado di difficoltà ben più alto che non con la C38m. Mi mancano, per ora, elementi sufficienti per trattare criticamente quell'interessante argomento.

LUIGI DONINI

(11) B.I. vol. pag.284.2

Ratio Math. n. 7 - 1994
57 - 73

PROBABILITÀ CONDIZIONATE E APPRENDIMENTO DALL'ESPERIENZA: UN'APPLICAZIONE DEL TEOREMA DI BAYES

Angelo Gilio
Dipartimento di Matematica - Universtà di Catania
Viale A. Doria, 6 - 95125 Catania

1. INTRODUZIONE

La matematica entra in molte situazioni della vita quotidiana, fornendoci concetti e metodi che permettono di analizzare problemi, al fine di prendere decisioni in modo razionale. Essendo in generale la nostra informazione incompleta, i problemi reali sono spesso caratterizzati da incertezza e di norma, prima di prendere delle decisioni, è opportuno ridurre tale incertezza predisponendo dei metodi per aumentare la nostra informazione. In tali situazioni la matematica ci mette a disposizione gli strumenti della statistica e del calcolo delle probabilità, al fine di esprimere, in base allo stato di conoscenza, le nostre valutazioni nei riguardi delle diverse ipotesi possibili. Lo strumento fondamentale per rappresentare in modo dinamico la conoscenza è quello della probabilità condizionata e del teorema di Bayes, che inquadra sul piano formale il meccanismo di "apprendimento dall'esperienza".

Il teorema di Bayes è lo strumento matematico con il quale, modificandosi lo stato di informazione, si calcolano le probabilità finali di determinate ipotesi, a partire da quelle iniziali delle stesse. Questa metodologia può essere sviluppata nella sua piena generalità se l'insegnamento della probabilità nella scuola viene basato sull'approccio soggettivo, secondo il quale, la probabilità di un evento, per un certo individuo, è la misura numerica del suo "grado di fiducia" nel verificarsi dell'evento stesso (cfr. de Finetti, 1970, Scozzafava, 1993). Tale grado di fiducia dipende strettamente dallo stato di informazione dell'individuo e si modifica sulla base di nuove informazioni. L'adozione della visione soggettiva nell'insegnamento della probabilità si rivela una scelta valida anche sotto

l'aspetto formativo, che è un obiettivo fondamentale della scuola (cfr. Gilio, 1990, 1993, Scozzafava, 1990).

In questo lavoro il meccanismo di apprendimento dall'esperienza viene illustrato applicando la formula di Bayes con riferimento al caso di un acquirente che deve decidere se accettare o rifiutare un lotto di articoli, che il fornitore garantisce essere tutti esenti da difetti. L'acquirente, sospettando che vi sia un articolo difettoso, prima di accettare il lotto vuole effettuare dei controlli in modo tale che, subordinatamente all'ipotesi che un certo numero di articoli scelti a caso siano risultati esenti da difetti, la probabilità che il lotto contenga un pezzo difettoso sia minore o uguale di un prefissato valore α, giudicato accettabile dall'acquirente.

Il lavoro include un'Appendice in cui è riportato un programma in Turbo Pascal 6.0 realizzato da Angelo Bossi, studente iscritto al secondo anno di Ingegneria Chimica dell'Università "La Sapienza" di Roma (a.a. 1992/93).

Tale programma permette di:

1) scegliere la dimensione del lotto e il valore della soglia probabilistica α;

2) calcolare i valori e tracciare il diagramma delle funzioni che, al variare del numero di controlli effettuati, descrivono la relazione fra la probabilità finale e quella iniziale che nel lotto vi sia un articolo difettoso;

3) tabulare, in funzione del valore α e del numero di articoli da controllare, gli intervalli di valori di appartenenza della probabilità iniziale in corrispondenza dei quali la probabilità finale risulta minore o uguale ad α, determinando così l'accettazione del lotto da parte dell'acquirente.

L'uso di tali intervalli consente un approccio "qualitativo", nel senso che l'acquirente, per stabilire il numero di controlli da effettuare, non ha bisogno di specificare esattamente il valore della probabilità iniziale, ma soltanto l'intervallo di appartenenza.

2. FORMULAZIONE DEL PROBLEMA

Indichiamo con N la dimensione del lotto, cioè il numero totale di articoli, e con n il numero di controlli. Consideriamo gli eventi:

H = "il lotto contiene un articolo difettoso",
H^c = "il lotto non contiene articoli difettosi",
E_i = "l'i-esimo articolo controllato è non difettoso", i = 1, 2, ..., n.

Posto P(H) = p, introduciamo le funzioni $f_1(p)$, $f_2(p)$, ..., $f_n(p)$ così definite:

$$f_k(p) = P(H \mid E_1 E_2 \ldots E_k), \qquad k = 1, 2, \ldots, n,$$

dove il simbolo $E_1 E_2 \ldots E_k$ rappresenta l'evento intersezione degli eventi E_1, E_2, ..., E_k.

Il valore p è la probabilità iniziale secondo l'acquirente che sia vero l'evento H, mentre $f_k(p)$ rappresenta in funzione di p la probabilità finale di H dopo k controlli, cioè la probabilità di H condizionata all'ipotesi che siano stati controllati k articoli e che siano risultati tutti non difettosi.

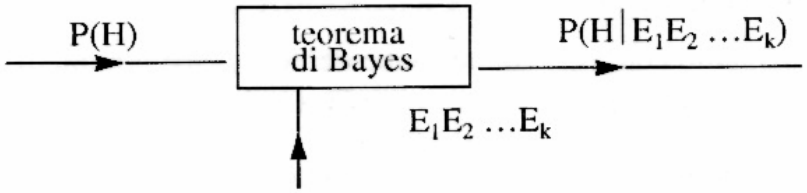
La regola in base alla quale l'acquirente decide di accettare o rifiutare il lotto è la seguente: procedendo con estrazioni a caso (senza restituzione) si effettuano controlli successivi su articoli del lotto. Il lotto viene rifiutato se uno degli articoli controllati risulta difettoso. Se, invece, gli articoli man mano esaminati risultano tutti non difettosi la procedura viene interrotta e il lotto viene accettato, in corrispondenza del valore n tale che:

$$f_n(p) = P(H \mid E_1 E_2 \ldots E_n) \leq \alpha,$$

dove la soglia probabilistica α è scelta dall'acquirente.

Ovviamente, se $p \leq \alpha$ l'acquirente accetta il lotto senza effettuare controlli.

Il meccanismo di aggiornamento delle probabilità è rappresentato nello schema seguente:



Esso si basa sull'uso iterato della seguente formula:

$$P(H|E_1E_2\ldots E_k) = \frac{P(H)\,P(E_1E_2\ldots E_k|H)}{P(H)\,P(E_1E_2\ldots E_k|H) + P(H^c)\,P(E_1E_2\ldots E_k|H^c)},$$

che, applicata per k = 1, 2, ..., n, fornisce ad ogni passo le probabilità finali dell'evento H date da:

$$P(H|E_1) = \frac{P(H)\,P(E_1|H)}{P(H)\,P(E_1|H) + P(H^c)\,P(E_1|H^c)},$$

$$P(H|E_1E_2) = \frac{P(H)\,P(E_1E_2|H)}{P(H)\,P(E_1E_2|H) + P(H^c)\,P(E_1E_2|H^c)},$$

.....

$$P(H|E_1E_2\ldots E_n) = \frac{P(H)\,P(E_1E_2\ldots E_n|H)}{P(H)\,P(E_1E_2\ldots E_n|H) + P(H^c)\,P(E_1E_2\ldots E_n|H^c)}.$$

Nel nostro caso si ha:

$$P(E_1|H) = \frac{N-1}{N}, \qquad P(E_1E_2|H) = \frac{N-1}{N}\frac{N-2}{N-1} = \frac{N-2}{N},$$

.....

$$P(E_1E_2\ldots E_n|H) = \frac{N-1}{N}\frac{N-2}{N-1}\cdots\frac{N-n}{N-n+1} = \frac{N-n}{N},$$

$$P(E_1|H^c) = P(E_1E_2|H^c) = \ldots P(E_1E_2\ldots E_n|H^c) = 1,$$

da cui si ottiene:

$$P(H|E_1) = \frac{p\,\frac{N-1}{N}}{p\,\frac{N-1}{N} + (1-p)} = \frac{(N-1)\,p}{N-p} = f_1(p)\ ,$$

$$P(H|E_1E_2) = \frac{p\,\frac{N-2}{N}}{p\,\frac{N-2}{N} + (1-p)} = \frac{(N-2)\,p}{N-2p} = f_2(p)\ ,$$

.....

$$P(H|E_1E_2\ldots E_n) = \frac{p\,\frac{N-n}{N}}{p\,\frac{N-n}{N} + (1-p)} = \frac{(N-n)\,p}{N-np} = f_n(p)\ .$$

Nel caso in esame, la condizione $f_n(p) = P(H|E_1E_2\ldots E_n) \le \alpha$ equivale alla disuguaglianza $\frac{(N-n)\,p}{N-np} \le \alpha$, che è soddisfatta se e solo se $p \le \frac{N\alpha}{N - n(1-\alpha)}$.

Ad esempio, per $N = 6$ si ha

$$P(H|E_1) = f_1(p) = \frac{5p}{6-p}\ , \qquad P(H|E_1E_2) = f_2(p) = \frac{4p}{6-2p}\ ,$$

$$\ldots\ , \qquad P(H|E_1E_2)\ldots E_5 = f_5(p) = \frac{p}{6-5p}\ .$$

Se l'acquirente giudica accettabile una soglia probabilistica $\alpha = 0.2$, utilizzando la disuguaglianza $p \le \frac{N\alpha}{N - n(1-\alpha)}$ con $N = 6$, $\alpha = 0.2$, $n = 1, 2, \ldots$, ai fini dell'accettazione del lotto sarà sufficiente un controllo se la probabilità iniziale p è tale che $f_1(p) \le 0.2$, cioè se $p \le \frac{3}{13} \cong 0.2308$.

Se la probabilità iniziale p è maggiore di $\frac{3}{13}$ saranno sufficienti due controlli se risulta $f_2(p) \leq 0.2$, cioè se è soddisfatta la condizione $p \leq \frac{3}{11} \cong 0.2727$.

Nel caso $p > \frac{3}{11}$ la procedura termina dopo tre passi se si ha $f_3(p) \leq 0.2$, cioè se $p \leq \frac{1}{3} \cong 0.3333$.

Nel caso $p > \frac{1}{3}$ la procedura termina dopo quattro passi se $f_4(p) \leq 0.2$, cioè se $p \leq \frac{3}{7} \cong 0.4286$.

Nel caso $p > \frac{3}{7}$ la procedura termina dopo cinque passi se $f_5(p) \leq 0.2$, cioè se $p \leq \frac{3}{5} = 0.6$.

Osserviamo infine che nel caso $p > 0.6$ la condizione $f_n(p) \leq \alpha$ è soddisfatta solo per $n = N = 6$, cui corrisponde $f_6(p) = 0$. In questo caso infatti il "sospetto" iniziale dell'acquirente, rappresentato dalla probabilità iniziale $P(H) = p$, è troppo alto e, affinché la probabilità di H scenda al di sotto di α, è necessario controllare tutti gli articoli. Al contrario, nel caso $p \leq 0.2$ l'acquirente accetta il lotto senza effettuare controlli.

In questo esempio, quindi, l'intervallo $[0, 1]$ dei possibili valori di p viene suddiviso nei sottointervalli

$$I_0 = [0, 0.2], \quad I_1 = (0.2, \tfrac{3}{13}], \quad I_2 = (\tfrac{3}{13}, \tfrac{3}{11}],$$

$$I_3 = (\tfrac{3}{11}, \tfrac{1}{3}], \quad I_4 = (\tfrac{1}{3}, \tfrac{3}{7}], \quad I_5 = (\tfrac{3}{7}, \tfrac{3}{5}], \quad I_6 = (\tfrac{3}{5}, 1].$$

Il numero (minimo) di controlli che l'acquirente deve predisporre è pari all'intero n tale che $p \in I_n$.

In generale, per un lotto di N pezzi, utilizzando la disuguaglianza $p \le \frac{N\alpha}{N - n(1 - \alpha)}$ si ottengono i sottointervalli:

$$I_0 = [0, \alpha], \qquad I_1 = (\alpha, \frac{N\alpha}{N - (1 - \alpha)}], \qquad I_2 = (\frac{N\alpha}{N - (1 - \alpha)}, \frac{N\alpha}{N - 2(1 - \alpha)}],$$

$$\dots, I_n = (\frac{N\alpha}{N - (n - 1)(1 - \alpha)}, \frac{N\alpha}{N - n(1 - \alpha)}], \dots, I_N = (\frac{N\alpha}{N - (N - 1)(1 - \alpha)}, 1]$$

e si ha $f_n(p) \le \alpha$ se $p \in I_n$.

3. ASPETTI GENERALI

Il problema fin qui esaminato costituisce una versione semplificata di una situazione più generale. Infatti abbiamo supposto che il lotto contiene al più un pezzo difettoso, cioè il numero aleatorio X di articoli difettosi nel lotto può assumere soltanto il valore 1 (corrispondente all'ipotesi H) oppure il valore 0 (corrispondente all'ipotesi H^c). In generale, però, i valori possibili di X sono gli interi da 0 fino ad N e, introdotti gli eventi

$$H_k = \text{"nel lotto vi sono k pezzi difettosi"}, \qquad k = 0, 1, \dots, N,$$

l'acquirente dovrebbe valutare le probabilità iniziali

$$P(H_k), \qquad k = 0, 1, \dots, N$$

per poi calcolare, per $n = 1, 2, \dots$, le probabilità finali

$$P(H_k \mid E_1E_2 \dots E_n), \qquad k = 0, 1, \dots, N,$$

utilizzando la formula di Bayes.

La versione semplificata si può adottare nei casi in cui le ipotesi $H_2, H_3, \dots, H_N$ vengono trascurate perché si ritengono "molto piccole" le loro probabilità. In effetti in molte situazioni si ha $P(H_k) \cong 0$ per $k \ge 2$ e quindi $P(X \ge 1) \cong P(X = 1)$.

Si consideri ad esempio il caso in cui X rappresenta il numero di bombe nascoste nei bagagli di un aereo, oppure X rappresenta il numero di componenti guasti del motore di tale aereo, e così via.

Nel caso specifico, inoltre, la versione semplificata si può giustificare sulla base di un atteggiamento probabilistico ben preciso dell'acquirente. Infatti, la probabilità di trovare pezzi difettosi durante i controlli (e quindi di rifiutare il lotto) è tanto più alta quanti più pezzi difettosi vi sono nel lotto. Quindi, dal punto di vista dell'acquirente, è ragionevole ritenere che il fornitore, ammesso che abbia deciso di inserire qualche articolo difettoso nel lotto, ha in tal caso interesse ad inserirne un numero molto basso. Pertanto, sotto l'aspetto probabilistico, il modo migliore di premunirsi contro la presenza di articoli difettosi è quello di supporre che al più ve ne sia uno, il che corrisponde ad assumere:

$$P(X \geq 1) = P(X = 1), \quad \text{cioè} \quad P(X \geq 2) = 0.$$

Questo atteggiamento si può caratterizzare in modo formale. Infatti, posto:

$$P(X = 0) = 1 - p, \quad P(X = k) = \lambda_k, \quad k = 1, 2, \ldots, N,$$

$$P(X \geq 1) = p = \lambda_1 + \lambda_2 + \ldots \lambda_N,$$

con p assegnato, si può verificare che, fra tutte le distribuzioni di probabilità iniziali del tipo

$$\pi = (1 - p, \lambda_1, \ldots, \lambda_N),$$

quella che richiede il numero più grande di controlli, affinché sia soddisfatta la condizione (di accettazione del lotto)

$$P(X \geq 1 \mid E_1 E_2 \ldots E_n) \leq \alpha,$$

è la distribuzione π_0 tale che $\lambda_1 = p$, $\lambda_2 = \ldots = \lambda_N = 0$, cioè

$$\pi_0 = (1 - p, p, 0, \ldots, 0),$$

per la quale si ha $P(X \geq 1) = P(X = 1)$.

Infatti, tenendo conto che $P(E_1 E_2 \ldots E_n | X = 0) = 1$, si ha:

$$P(X = 0 | E_1 E_2 \ldots E_n) = \frac{P(X = 0)\ P(E_1 E_2 \ldots E_n | X = 0)}{\sum_{k=0}^{N} P(X = k)\ P(E_1 E_2 \ldots E_n | X = k)} =$$

$$= \frac{(1 - p)}{(1 - p) + \sum_{k=1}^{N} \lambda_k\ P(E_1 E_2 \ldots E_n | X = k)} .$$

Osserviamo, inoltre che la probabilità $P(E_1 E_2 \ldots E_n | X = k)$ è pari al rapporto $\binom{N - k}{n} / \binom{N}{n}$ se l'evento $E_1 E_2 \ldots E_n$ è compatibile con l'evento $(X = k)$, mentre è nulla se tali eventi sono incompatibili. Pertanto, risulta

$$P(E_1 E_2 \ldots E_n | X = 1) \geq P(E_1 E_2 \ldots E_n | X = 2) \geq \ldots \geq P(E_1 E_2 \ldots E_n | X = n),$$

da cui segue

$$P(X = 0 | E_1 E_2 \ldots E_n) \geq \frac{(1 - p)}{(1 - p) + \left(\sum_{k=1}^{N} \lambda_k \right) P(E_1 E_2 \ldots E_n | X = 1)} =$$

$$= \frac{(1 - p)}{(1 - p) + p \dfrac{N - n}{N}} = \frac{N(1 - p)}{N - np}$$

e quindi

$$P(X \geq 1 | E_1 E_2 \ldots E_n) = 1 - P(X = 0 | E_1 E_2 \ldots E_n) \leq$$

$$\leq 1 - \frac{N(1 - p)}{N - np} = \frac{(N - n)p}{N - np} = P(H | E_1 E_2 \ldots E_n) = f_n(p) .$$

In conclusione, subordinatamente all'ipotesi che gli articoli man mano esaminati siano tutti esenti da difetti, la distribuzione di probabilità iniziale $\pi = (1 - p, \lambda_1, \ldots, \lambda_N)$ che "ritarda" il più possibile l'accettazione del lotto, cioè per la quale la probabilità $P(X \geq 1 | E_1 E_2 \ldots E_n)$ scende più lentamente al disotto della soglia α, è data da $\pi_0 = (1 - p, p, 0, \ldots, 0)$.
Tale distribuzione concentra il valore $p = \lambda_1 + \lambda_2 + \ldots + \lambda_N$ sull'evento $(X = 1)$, corrispondente all'ipotesi H nella versione semplificata del problema.

BIBLIOGRAFIA

[1] DE FINETTI B. (1970), *Teoria delle probabilità*. Einaudi Editore, Torino.

[2] GILIO A. (1990), *Aspetti algebrici e geometrici nell'insegnamento della probabilità soggettiva*, Archimede, 1, Genn. - Marzo, 32 - 41.

[3] GILIO A. (1993), *Probabilità di eventi come previsioni di numeri aleatori*, Induzioni, 7, Luglio - Dicembre, 39 - 48.

[4] SCOZZAFAVA R. (1990), *Per un insegnamento "fusionista" della probabilità e della statistica nelle scuole secondarie*, Matematica Oggi: dalle idee alla scuola (a cura di Fulvia Furinghetti), Cidi di Genova, Irrsae Liguria, Edizioni Scolastiche Bruno Mondadori, 251 - 256.

[5] SCOZZAFAVA R. (1993), *La probabilità soggettiva e le sue applicazioni*, Ed. Veschi, Masson (Milano).

APPENDICE

Programma per calcolatore in Turbo Pascal 6.0

In questa Appendice viene riportato un programma in Turbo Pascal 6.0 realizzato dallo studente Angelo Bossi, che consente di analizzare il problema con l'aiuto del calcolatore e permette in particolare di:

1) scegliere il valore dei parametri N, α;
2) calcolare i valori e tracciare il grafico delle funzioni $f_1(p)$, $f_2(p)$, ..., $f_{N-1}(p)$;
3) determinare gli intervalli $I_1, I_2, \ldots, I_n$.

Il programma consiste in una serie di procedure, alcune delle quali riguardano la presentazione grafica, mentre altre si riferiscono agli aspetti probabilistici e numerici del problema.

```
Program Tabula Guasti;
Uses Crt, Dos, Graph;
Const
 MaxNum=300;{Modificare questo valore per variare la dimensione dell'array}
 CoordX=60;
 CoordY=450;
 Triangle1: array[1..4] of PointType =
  ((x: 620; y: 450 ),(x: 600 ; y:440 ),
   (x: 600 ; y:460 ),(x: 620 ; y:450 ));
 Triangle2: array[1..4] of PointType =
  ((x: 60; y:0 ),(x: 50; y:20 ),
   (x: 70; y:20),(x: 60; y:0 ));
Var n,l,m,h,k,conta,x,alfaind,probind,g,inizio,fine,ind,i1,i2:Integer;
   GrDriver,GrMode,ErrCode:Integer;
   y1,alfa,y,prob:Real;
   tab:array[1..MaxNum] of Integer;
   ch,risposta,scelta,modo,ris:Char;
   label 1,2,3,4;
Procedure Intro;   {Pagina introduttiva}
begin
    for conta:=1 to 8 do WriteLn;
    WriteLn('          Programmato in Turbo Pascal 6.0 da Angelo Bossi');
    for conta:=1 to 8 do WriteLn;
    Write('      ');
    WriteLn('N.B.=E" possibile graficare le N-1 curve solo per N < ',MaxNum);
    Write(' Per entrare in ambiente grafico e" necessaria una scheda');
    WriteLn(' grafica VGA o EGA');
```

```
    WriteLn('                    Premi <INVIO> per continuare...');
    for conta:=1 to 3 do WriteLn;
    TextColor(0);ReadLn;TextColor(15);
end;

Procedure Tabula;
{Questa procedura calcola le probabilita' al variare di alfa e n
 e ne stampa il valore;per migliorare la leggibilita' della
 tabella e' stato introdotta una visualizzazione a pagina}
label 1;
begin
1: ClrScr;
   TextColor(10);
   WriteLn(' 1) Per tutti i possibili valori della soglia');
   WriteLn(' 2) Solo per un particolare valore della soglia');
   WriteLn;TextColor(15);
   Write(' Qual e'' la tua scelta? ');
   ReadLn(ris);
   if ris='1' then begin i1:=1; i2:=19; end;
   if ris='2' then begin
      WriteLn;Write(' Immetti il valore della soglia:=');
      ReadLn(alfa);
      if (alfa<0) or (alfa>1) then goto 1;
      i1:=1;
      i2:=1;
   end;
   if (ris<>'1') and (ris<>'2') then goto 1;
   l:=1;          {Inizializzazione per la tabulazione}
   repeat
     ClrScr;
     TextColor(10);
     Writeln('                    TABULAZIONE SU ',n,' PEZZI');
     if ris='1' then Writeln else for k:=1 to 10 do WriteLn;
     TextColor(15);
     Write(' `');
{Condizione per la tabulazione a pagine}
     if (l+7-n)<0 then m:=l+7 else m:=n-1;
     for conta:=l to m  do begin
        if conta<10 then Write('       ',conta)
        else if conta<100 then Write('      ',conta)
           else Write('     ',conta);
     end;
     TextColor(15);
     Writeln;
{Questi 2 cicli FOR sono la parte centrale di questa procedura;
 tramite una ricorsione infatti viene calcolato ,memorizzato
 in un array e poi stampato il valore di alfa e di n}
     for k:=i1 to i2 do begin
        if ris='1' then alfa:=k/20;
        g:=Round(alfa*100);    {normalizzazione di alfa}
        if g<10 then Write('0.0',g,';  ') else Write('0.',g,';  ');
        for h:=l to m do begin
           tab[h]:=Round((10000*alfa*n)/((n-h)+alfa*h));
           if tab[h]<1000 then Write('0.0',tab[h],';  ')
```

```
            else Write('0.',tab[h],';  ');
        end;
        Writeln;
    end;
    if ris='2' then for k:=1 to 10 do WriteLn;
    Write('Premi <INVIO>');
    TextColor(0);
    ReadLn;
    l:=m+1;
  until l>n-1; {Condizione per la fine della tabulazione a pagine}
  TextColor(10);
  Write('                          Fine Tabulazione');
  Sound(880);Delay(150);NoSound;
  ReadLn;
end;

Procedure Tabula1;
{Questa procedura calcola la F(p) al variare della probabilita'
 e del numero dei componenti del lotto e ne stampa il valore;
 per migliorare la leggibilita' della tabella e' stato introdotta
 una visualizzazione a pagina}
label 1;
begin
1: ClrScr;
  TextColor(10);
  WriteLn(' 1) Per tutti i possibili valori della probabilita'"');
  WriteLn(' 2) Solo per un particolare valore della probabilita'");
  WriteLn;TextColor(15);
  Write(' Qual e" la tua scelta? ');
  ReadLn(ris);
  if ris='1' then begin i1:=1; i2:=19; end;
  if ris='2' then begin
    WriteLn;Write(' Immetti il valore della probabilita":=');
    ReadLn(prob);
    if (prob<0) or (prob>1) then goto 1;
    i1:=1;
    i2:=1;
  end;
  if (ris<>'1') and (ris<>'2') then goto 1;
  l:=1;          {Inizializzazione per la tabulazione}
  repeat
    ClrScr;
    TextColor(10);
    Writeln('                          TABULAZIONE SU ',n,' PEZZI');
    if ris='1' then Writeln else for k:=1 to 10 do WriteLn;
    TextColor(15);
{Condizione per la tabulazione a pagine}
    if (l+7-n)<0 then m:=l+7 else m:=n-1;
    if m<100 then Write('  p ') else Write('  p  ');
    for conta:=l to m  do begin
       if conta<10 then Write('    F',conta,'(p)')
       else if conta<100 then Write('   F',conta,'(p)')
           else Write('  F',conta,'(p)');
    end;
```

```
    TextColor(15);
    WriteIn;
    for k:=i1 to i2 do begin
       if ris='1' then prob:=k/20;
       g:=Round(prob*100);     {normalizzazione della probabilita'}
       if g<10 then Write('0.0',g,';  ') else Write('0.',g,';  ');
       for h:=l to m do begin
          tab[h]:=Round((10000*prob*(n-h))/(n-prob*h));
          if tab[h]<10 then Write('0.000',tab[h],';  ')
            else if tab[h]<100 then Write('0.00',tab[h],';  ')
                 else if tab[h]<1000 then Write('0.0',tab[h],';  ')
                   else Write('0.',tab[h],';  ');
       end;
       WriteIn;
    end;
    if ris='2' then for k:=1 to 10 do WriteLn;
    Write('Premi <INVIO>');
    TextColor(0);
    ReadLn;
    l:=m+1;
  until l>n-1; {Condizione per la fine della tabulazione a pagine}
  TextColor(10);
  Write('                          Fine Tabulazione');
  Sound(880);Delay(150);NoSound;
  ReadLn;
end;

Procedure Curve;
{I 2 cicli FOR ,come nella procedura TABULA, sono qui usati
 per calcolare le coordinate(espresse in pixel) delle curve}
begin
    for h:=inizio to fine do begin
       SetColor(h+8);SetLineStyle(0,0,1);
       if (h mod 8)=0 then SetColor(h+1);
       MoveTo(CoordX,CoordY);  {sposto il cursore nell'origine degli assi}
       for x:=1 to 100 do begin
          y:=((n-h)*x/100)/(n-(h*x/100));
          LineTo(CoordX+x*5,Round(CoordY-(y*400)));
       end;
       SetColor(15);
       SetLineStyle(1,0,1);
{Tracciano l'indicatore di alfa e le relative probabilita' e viceversa}
       if ch='1' then begin
         alfaind:=60+Round((500*alfa*n)/((n-h)+alfa*h));
         Line(60,GetMaxY-Round(alfa*400)-29,
              alfaind,GetMaxY-Round(alfa*400)-29);
         Line(alfaind,450,alfaind,GetMaxY-Round(alfa*400)-29);
       end;
       if ch='2' then begin
         y1:=((n-h)*prob)/(n-(h*prob));
         probind:=GetMaxY-Round((y1*400)+28);
         if h=inizio then ind:=probind;
         Line(Round((prob*500)+60),450,Round((prob*500)+60),ind);
         Line(60,probind-1,Round((prob*500)+60),probind-1);
```

```
        end;
      end;
end;
Procedure Grafica;
{Questa procedura, sfruttando i dati di TABULA o TABULA1 permette la
 visualizzazione grafica delle curve rappresentanti le probabilita'
 in un sistema cartesiano(F(p),P)}
label 2,4;
begin
    TextColor(15);
    WriteLn;
4:  if ch='1' then begin
      Write(' Inserisci la soglia probabilistica alfa:=');
      ReadLn(alfa);
      if (alfa>1) and (alfa<0) then goto 4;
    end else begin
    Write(' Inserisci la probabilita'':=');
      ReadLn(prob);
      if (prob>1) and (prob<0) then goto 4;
    end;
    ClrScr;
    GrDriver := Detect;
    InitGraph(GrDriver,GrMode,'');     {Inizializzazione grafica}
    ErrCode := GraphResult;
    if ErrCode = grOk then
    begin
        if (GrDriver<>9) and (GrDriver<>4) then goto 2;
        SetColor(15);
        SetLineStyle(0,0,1);
        Line(30,450,600,450);
        Line(60,20,60,480);   {Assi Cartesiani}
        Line(60,50,560,50);
        Line(560,50,560,450);
        FillPoly(SizeOf(Triangle1) div SizeOf(PointType), Triangle1);
        FillPoly(SizeOf(Triangle2) div SizeOf(PointType), Triangle2);
{Scala di valori}
        for conta:=1 to 20 do
           Line(12+conta*25+35,448,12+conta*25+35,452);
        for conta:=1 to 20 do
           Line(conta*25+35,445,conta*25+35,455);
        for conta:=1 to 11 do
           Line(conta*50+10,442,conta*50+10,458);
        for conta:=1 to 20 do
           Line(58,GetMaxY-(10+conta*20+9),62,GetMaxY-(10+conta*20+9));
        for conta:=1 to 20 do
           Line(55,GetMaxY-(conta*20+9),65,GetMaxY-(conta*20+9));
        for conta:=1 to 11 do
           Line(52,GetMaxY-(conta*40-11),68,GetMaxY-(conta*40-11));
        SetColor(10);
        SetTextStyle(2,0,6);OutTextXY(25,460,'0.0');
        OutTextXY(100,460,'0.1');OutTextXY(25,400,'0.1');
        OutTextXY(150,460,'0.2');OutTextXY(25,360,'0.2');
        OutTextXY(200,460,'0.3');OutTextXY(25,320,'0.3');
        OutTextXY(250,460,'0.4');OutTextXY(25,280,'0.4');
```

```
        OutTextXY(300,460,'0.5');OutTextXY(25,240,'0.5');
        OutTextXY(350,460,'0.6');OutTextXY(25,200,'0.6');
        OutTextXY(400,460,'0.7');OutTextXY(25,160,'0.7');
        OutTextXY(450,460,'0.8');OutTextXY(25,120,'0.8');
        OutTextXY(500,460,'0.9');OutTextXY(25, 80,'0.9');
        OutTextXY(550,460,'1.0');OutTextXY(25, 40,'1.0');
        SetColor(14);SetTextStyle(1,0,2);
        OutTextXY(10,0,'F(p)');OutTextXY(600,457,'P');
        Curve;      {Richiamo la procedure che traccia le curve}
        SetLineStyle(0,0,1);
        Line(60,50,560,50);
        Line(560,50,560,450);
        SetColor(14);SetTextStyle(2,0,6);
        OutTextXY(250,5,'Premi <INVIO>');
        Sound(880);Delay(150);NoSound;
        TextColor(0);
        ReadLn;
2:      CloseGraph;
    end;
end;

{PROGRAMMA PRINCIPALE}
begin
    ClrScr;
    TextBackGround(0);
    TextColor(15);
    Intro;
1:  ClrScr;
    TextColor(15);
    Write(' Inserisci il numero dei componenti del lotto :=');
    ReadLn(n);
    if (n<2) or (n>MaxNum) then goto 1;
4:  ClrScr;
    TextColor(10);
    WriteLn(' 1) Tabulazione');
    WriteLn(' 2) Grafico');
    WriteLn(' 3) Modifica i valori');
    WriteLn(' 4) Uscita');
    TextColor(15);
    WriteLn;
    Write(' Qual e'' la tua scelta? ');
    ReadLn(scelta);
    if scelta='1' then goto 2 else
      if scelta='2' then goto 3 else
        if scelta='3' then goto 1 else
          if scelta='4' then begin ClrScr;Exit; end else goto 4;
    Sound(831);Delay(150);NoSound;
2:  ClrScr;
    TextColor(10);
    WriteLn('1) Calcolo della probabilita'' data la soglia probabilistica');
    WriteLn('2) Calcolo della F(p) data la probabilita''');
    WriteLn('3) Uscita');
    TextColor(15);
    WriteLn;
```

```
    Write('Qual e'' la tua scelta? ');
    ReadLn(modo);
    if modo='1' then Tabula else
      if modo='2' then Tabula1 else
        if modo='3' then begin ClrScr;Exit; end else goto 2;
    goto 4;
3:  ClrScr;
    TextColor(10);
    WriteLn(' 1) Indicatore di F(p)');
    WriteLn(' 2) Indicatore di p');
    WriteLn;
    TextColor(15);
    Write(' Qula e'' la tua scelta ? ');
    ReadLn(ch);
    if (ch<>'1') and (ch<>'2') then goto 3;
    ClrScr;
    TextColor(10);
    WriteLn(' 1) Grafico di tutte le curve');
    WriteLn(' 2) Grafico di un sottinsieme di tutte le curve');
    WriteLn(' 3) Grafico di una sola curva');
    WriteLn(' 4) Uscita');
    WriteLn;
    WriteLn;TextColor(15);
    Write(' Qual e'' la tua scelta ? ');
    ReadLn(risposta);
    if risposta='1' then begin inizio:=1; fine:=n-1; Grafica; end;
    if risposta='2' then begin
    WriteIn;
    Write(' Componente iniziale del lotto:=');
    ReadLn(inizio);
    if (inizio<0) or (inizio>n-1) then goto 3;
    WriteLn;
    Write(' Componente finale del lotto:=');
    ReadLn(fine);
    if (fine>n-1) or (fine<inizio) then goto 3;
    Grafica;
    end;
    if risposta='3' then begin
    WriteLn;
    Write(' Componente del lotto:=');
    ReadLn(inizio);
    if (inizio<0) or (inizio>n-1) then goto 3;
    fine:=inizio;
    Grafica;
    end;
    if risposta='4' then begin
      ClrScr;
      exit;
    end;
    if (risposta<>'1') and (risposta<>'2') and
      (risposta<>'3') and (risposta<>'4') then goto 3;
    goto 4;
   end.
```

Osservazioni sulla distribuzione dei numeri primi dei tipi (6n - 1) e (6n + 1) - n ≥ 1 intero.

F. Eugeni, Dip. di Ingegneria Elettrica, L'Aquila
G. Moro, Ammiraglio della Riserva, Roma

Sommario - Si riportano i principali elementi, emersi dall' analisi effettuata sulla distribuzione dei numeri primi dei tipi (6n-1) e (6n+1) - per $1 \le n \le 16666667$ - cioè per $1 \le (x) \le 100000002$, ove (x) indica la "fascia" da 0 ad (x) degli interi di riferimento.
Si accenna ad un confronto fra gli elementi emersi sulla distribuzione dei primi dei tipi (6n-1) e (6n+1) e su quelli della distribuzione dei primi dei tipi (xn-1) e (xn+1).

1. Generalità sulla teoria dei Numeri

Nell'edificio generale della Teoria dei Numeri giocano un ruolo primario i "Numeri Primi".Un Primo è un numero maggiore di 1 che è divisibile solo per se stesso e per l'unità. A tentativi si trovano subito i numeri primi:

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47.

Fin dai tempi di Euclide è ben noto che l'insieme dei numeri primi è infinito,ma tale insieme non è "concretamente noto" nel senso che non si conosce una legge che ci permetta di dire se un dato numero è primo o no. In realtà esiste il teorema di Wilson asserente che "n" è un primo se e solo se:

$(n-1)! \equiv -1$ modulo "n"

Ci si convince facilmente che questo teorema non è atto a caratterizzare l'insieme dei primi. Non si conosce alcun insieme contenente infiniti primi. Dunque non si sa molto della distribuzione dei numeri primi.
Perfino la loro distribuzione in intervalli corti sembra estrema mente irregolare.
Questo è il motivo per cui appare impossibile trovare una formula semplice che descriva la distribuzione de numeri primi in qualunque dettaglio.
Euclide ha provato che ci sono infiniti numeri primi;Legendre e Gauss nel 1800,hanno ipotizzato alcuni dei teoremi fondamentali: la teoria allo stato attuale è un miscuglio di problemi irrisolti,congetture più o meno logiche e solo alcuni teoremi dimostrati.
I teoremi dimostrati coprono ,inoltre, solo casi molto semplici, comparati alle supposizioni esistenti.
Le dimostrazioni sono in genere molto complicate basandosi su teoremi della teoria delle funzioni.
Nella ricerca di formule che producano tutti numeri primi (e nessun altro numero) sono stati trovati alcuni polinomi notevoli, i cui valori contengono una percentuale sorprendentemente alta di numeri primi .
Uno di questi è:

$$P(x) = x^2 - x + 17$$

che è numero primo per x=0,1,2,3,...,16 ma risulta composto per x=17,dato che $P(17) = 17^2 - 17 + 17$. Ancora un'alta percentuale per il polinomio:

$$x^2 - x + 41$$

che produce numeri primi per x=0,1,2,...,40 ed è composto naturalmente per x=41. Un altro polinomio più ricco in numeri primi dei precedenti è:

$$2x^2 - 199$$

che produce 150 numeri primi per x=0,1,2,...,198.
La dimostrazione che nessun polinomio(non costante) può produrre solo numeri primi è abbastanza semplice.
Precisando quanto detto in precedenza ,in realtà esistono formule che producono tutti numeri primi e nessun altro numero;tuttavia,queste sono un "imbroglio" poichè esse presuppongono in qualche modo due cose:

1. la conoscenza dell'insieme dei primi
2. fanno affidamento sulla falsa definizione di un numero primo come numero non-composto.

Esistono vari esempi di queste formule,alcuni complicatissimi da dimostrare,altri molto lunghi,ma tutti indiscutibilmente contengono qualche errore.
Alcuni di essi si basano sull'esistenza di un polinomio speciale che produce solo primi positivi.
In realtà polinomi così fatti non esistono il che ci induce a pensare che si debba ricorrere a qualche stratagemma per arrivare ad un polinomio che produce tutti numeri primi positivi ed un largo numero di interi composti negativi.
Riportiamo ora l'estremamente brillante prova di Euclide dell'infinità dei numeri primi.
Egli dimostrerà che dato un insieme finito di primi si può costruire un altro insieme di primi più grande che nel precedente non ci sta.
Supponi che esista solo un numero finito di numeri primi, $p_1, p_2, \ldots p_n$.
Ora considera l'intero $N = p_1, p_2, \ldots p_n + 1$.
Nessuno dei numeri primi esistenti divide N,dato che la divisione N / p_i darà sempre resto 1.
Così o N è un (nuovo) numero primo,oppure N contiene un (nuovo) fattore primo,che è diverso da tutti quelli dati.
Perciò concludiamo che ci deve essere un infinità di numeri primi.
Molti matematici ,nel corso dei secoli,si sono cimentati nello studio dei numeri primi.
Molte menti geniali nel campo delle scienze matematiche hanno cercato di svelare questo misterioso segreto che permea i numeri primi.
Alcuni di essi hanno elaborato teorie complicatissime, altri, teoremi più semplici ma tutti sono arrivati ad una stessa conclusione:
<< Niente di preciso si sa sui numeri primi >>.
Esempi di quanto detto sono proprio le formule di Gauss e Legendre.
Sia Gauss che Legendre,indipendentemente l'uno dall' altro,si interessarono del grande mistero dei numeri primi.
Si occuparono entrambi di un problema che in qualche modo può essere considerato una restrizione al problema più generale del calcolo dei numeri primi.
Essi,infatti, si occuparono del calcolo del numero dei numeri primi minori o uguali di un certo x fissato indicato con $\pi(x)$.
1. Dal loro studio si ottengono risultati davvero interessanti:
Si vede che la densità dei numeri primi in un intorno di x decresce lentamente al crescere di x.

2. paragonando i valori trovati per $x = k^n$ e $x = k^{2n}$ con $k \in \mathbb{N}$ si nota che la densità dei numeri primi è approssimativamente dimezzata quando x è elevata al quadrato.
A livello matematico la densità che appare nella 2. può essere descritta con buona approssimazione dalla funzione 1/ln (x) poichè, ad esempio:

$$1/\ln(x^2) = 0,5/\ln(x)$$

Se si stila una tabella per la densità dei primi del tipo $x = k^n$ e 1/ln(x) notiamo solo delle piccole differenze tra i valori dell'una e dell'altra che sono dovute ad irregolarità locali nella distribuzione dei numeri primi , che più pesantemente influenza il numero dei numeri primi in intervalli brevi più che in quelli ampi.
Verso la fine del 1800(1896) Hadamard e De la Vallèe-Poussin, anche essi indipendentemente l'uno dall'altro , provarono quello che andò sotto il nome di Teorema Dei Numeri Primi, il cui enunciato è il seguente:
$\pi(x)$ è approssimativamente uguale a li(x) (dove li(x) è il logaritmo intero di x).
Questo teorema si ricollega all'approssimazione di Gauss, infatti , il suo unico scopo è quello di fornire informazioni sull'errore introdotto dall'approssimazione di Gauss.
Più precisamente esso afferma che l'errore relativo dell'approssimazione tende a 0 quando x tende ad ∞.
Le approssimazioni a $\pi(x)$ di Gauss e Legendre sono state trovate con metodi empirici.
Il matematico Riemann, invece, fu il primo che sistematicamente dedusse relazioni tra i numeri primi e le già note funzioni di Gauss e Legendre.
Egli prese spunto da una relazione scoperta già da Eulero:

$$\tau(s) = \sum_{1}^{\infty} 1/n^s = \prod_{p} 1/1 - p^{-1}$$

dove il prodotto infinito è preso sopra tutti i numeri primi.

Questa funzione $\tau(s)$ prese il nome di funzione zita di Riemann ed assunse una importanza eccezionale perchè da essa si possono dedurre molte proprietà dei numeri primi .
Essa , in sostanza, trasforma le proprietà dei numeri primi nelle proprietà della somma perchè rapporta ciascun numero primo "p" alla semplice somma:

$$\sum_{1}^{\infty} n^{-s}$$

Il legame che esiste tra la funzione zita di Riemann ed i numeri primi risulta evidente osservando, nella già citata formula $\tau(s) = \prod_{p} 1/1-p^{1}$, il prodotto infinito .Attraverso questo studio Riemann trovò che la funzione

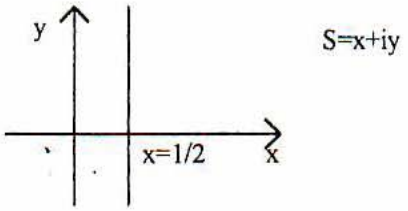
$$f(x) = \sum_{1}^{\infty} (1/n)\pi(x^{1/n})$$

è di importanza vitale , più che $\pi(x)$ stesso, per lo studio della relazione desiderata tra $\pi(x)$ e $\tau(s)$.
Nel 1859 lo stesso Riemann pubblicò la seguente formula:

$$f(x) = li(x) - \sum_{p} li(x^{p}) + \int_{x}^{\infty} \frac{dt}{(t^{2}-1)t\ln t} - \ln 2 \quad (1.0)$$

che nel 1859 fu provata da Maugoldt.
In relazione a numerose indagini effettuate da egli stesso sulla (1.0), Riemann formulò la sua famosa congettura, per cui è stata trovata, probabilmente, una prova da H. Matsumoto nel 1984 (questa prova non è stata ancora studiata attentamente da altri matematici per poter essere ritenuta valida).

Riemann formulò così la sua celebre congettura che ancora oggi è un mistero da scoprire.
Nella congettura si afferma che i numeri complessi s=x+iy , fra i quali $\tau(s)=0$, sono infiniti e sono tutti situati sulla retta $x=\frac{1}{2}$ del piano di Gauss, come rappresentato nel grafico seguente:



Attraverso teoremi di natura molto complessa è stato provato da Brent e da altri matematici che la congettura di Riemann, per un numero finito di zeri (circa 1000000000), risulta essere vera cioè che effettivamente $x=\frac{1}{2}$.

E' possibile dalla $f(x)=\sum_{1}^{\infty}\frac{1}{n}\pi(x^{1/n})$, precedentemente citata, esprimere $f(x)$ in funzione di $\pi(x)$.
Se si vuole trovare un collegamento in questo senso, si può far uso della seguente formula inversa : $\pi(x)=\sum_{1}^{\infty}\frac{\mu(n)}{n}li(x^{1/n})$ dove la funzione $\mu(n)$ è la funzione di Mobius,definita da:

$\mu(n)=$ a) 1 se n=1
b) 0 se n contiene alcuni fattori primi multipli
c) (-1^k) se n è il prodotto di k distinti numeri primi

Se, come detto precedentemente, f(x) è approssimata da li(x) si ottiene quella che va sotto il nome di Formula dei Numeri Primi di Riemann:

$$R(x) = \sum_{1}^{\infty} \frac{\mu(n)}{n} li(x^{1/n})$$

La chiave di lettura di questa formula è proprio l'approssimazione di Gauss a li(x).

Da un attento esame della formula di Riemann si possono osservare i seguenti due fatti:

1. per ampi valori di x , li(x) ed in particolare R(x), sono prossimi a $\pi(x)$.
2. R(x)-π(x) ha un grande numero di variazioni di segno , che spesso caratterizzano una buona approssimazione .

Dall' osservazione 2) si può trarre l'impressione che li(x) sia sempre maggiore di $\pi(x)$.

Questa ,in realtà, è una famosa vecchia congettura nella teoria dei numeri primi.

Il primo ad interessarsi al problema del segno di li(x)-π(x) fu Littewood, il quale dimostrò che tale funzione cambia segno infinite volte.

Inoltre i limiti di Littewood per li(x)-π(x) mostrano che tale differenza , per alcuni grandi valori di x, può diventare molto più ampia di li(x)-R(x).

Grazie a tale osservazione , la buona approssimazione di R(x) a $\pi(x)$ risulta essere ingannevole.

Quanto detto è un chiaro esempio di come, spesso, ragionamenti basati su evidenze numeriche possano condurre a conclusioni completamente errate.

Se si ammette per vera l'ipotesi di Riemann, il Teorema dei Numeri Primi si può scrivere nella forma: $\pi(x) \underset{c}{=} li(x) + o(\sqrt{x}\ln(x))$, dove "c" indica che questo risultato è solo una congettura che deve essere ancora provata .

Nel 1962 furono scoperte da Barkley e D. Sehoenfeld, a testimonianza di come questo ramo della matematica sia a tutt'oggi sconosciuto, alcune eleganti inesattezze per i valori di $\pi(x)$.

Supponi che a et b sono interi positivi e considera tutti i numeri interi formanti una progressione aritmetica an+b , n=0,1,2,... .
Quanti di questi numeri minori o uguali ad x sono primi?

Indica questo totale con $\pi_{a,b}(x)$. Affinchè an+b non contenga affatto alcun numero primo, è chiaro che il più grande divisore comune (a,b) di a et b deve essere uguale ad 1 (eccetto che nell'ovvio caso in cui "b" è un numero primo et "a" è preso come multiplo di "b", nel qual caso an+b conterrà proprio un numero primo, "b").
Se questa condizione è soddisfatta, una certa proporzione di tutti i numeri primi , $\frac{1}{\varphi(a)}$, dove φ(a) è la funzione di Eulero, appartiene alla serie aritmetica non appena $x \to \infty$ . .
Utilizzando il Teorema dei Numeri Primi, questo dà il seguente Teorema di Dirichlet, la cui prova non fu completata fino a quando De la Vallée-Paussin diede la sua prova del Teorema dei Numeri Primi:

$$\lim_{x \to \infty} \frac{\pi_{a,b}}{li(x)}(x) = \frac{1}{\varphi(a)}$$

Il Teorema di Dirichlet afferma che i numeri primi sono approssimativamente equi-distribuiti tra quelle serie aritmetiche della forma an+b , per un valore fissato di "a", che contiene diversi numeri primi.
Il Teorema di Dirichlet ci dice anche che ogni serie aritmetica an+b con (a,b)=1, contiene infinitamente molti numeri primi.
Tanto per dare un esempio: ci sono infinitamente molti numeri primi che terminano in 33333, come 733333,1133333, 2633333,2833333,... , perchè la serie 100000n+33333 contiene, a lungo andare $\frac{1}{40000}$ di tutti i numeri primi.

Spesso ci può interessare qualche problema ben posto ma di difficoltà non così elevata come quella dei grandi problemi insoluti. In questo ambito si inquadra lo studio della distribuzione dei primi di forma prestabilita entro intervalli definiti.
Nel presente ambito si può inquadrare un lavoro di G. Moro [ ].
Nel seguente lavoro si affronta un'analisi sulla distribuzione dei numeri primi delle forme $6n \pm 1$ per $1 \le n \le 16666667$.

2.-L'analisi delle successioni.

2.1-Premessa.

G. Moro aveva ottenuto in lavori precedenti (1)-(2), dei risultati ottenuti nello studio della distribuzione dei primi dei tipi (6n-1) e (6n+1), nella "fascia" $0 \le (x) \le 400002^n - (n \le 66667)$. Indichiamo con:

(1) $M_{6,5}(x)$-il numero dei primi del tipo (6n-1)

(2) $M_{6,1}(x)$-il numero dei primi del tipo (6n+1)

(3) $S_6(x)=M_{6,5}(x)-M_{6,1}(x)$- lo "scarto", fra:
-i numeri dei primi del tipo (5x-1);
-e quello del tipo (6x+1);
contenuti in (x).

(4) $DS_6(x)=S_6(xm+1)-S_6(xm)$ lo "spostamento" fra:
-lo "scarto" relativo alla "fascia" (xm+1);
-e lo "scarto" relativo alla "fascia" (xm), che la precede immediatamente.

I principali risultati ottenuti, si possono così sintetizzare:

(1) "Fascia" $0 \le (x) \le 400002$.
(5) $S_6(x)$, è sempre positivo, per (x) qualsiasi.

(2) Per i "gruppi" di valori di (x), che coprono la "fascia" $0 \le (x) \le 400002$, così definiti:

$$0 \le (x) \le 100000$$
$$100001 \le (x_2) \le 2000$$
$$200001 \le (x_3) \le 300000$$
$$300001 \le (x_4) \le 400002$$

si è fatto variare (x) a passo 1000 - a partire da 0. Per ciascuno dei quattro "gruppi" di valori di (x) di cui sopra, si sono così ottenuti 100 valori, equidistanti, crescenti di (x).
Per ciascuno di questi quattro "gruppi" di valori di (x), si sono determinati 100 valori di:
$M_{6,5}(x)$ $M_{6,1}(x)$ e di $S_6(x)=M_{6,5}(x)-M_{6,1}(x)$

Nell'ambito di ciascuno dei quattro "gruppi" di valori di (x), per $S_6(x)$, si sono determinati:
(6) i valori minimi: $S_6(x)$min.
(7) i valori massimi: $S_6(x)$max.
(8) i valori medi (aritmetici, su 100 valori): $S_6(x)$med.

Ecco i risultati ottenuti:

"gruppo"	$S6(x_1)$				
	N°.	Valori			
	Valori	min.	med.	max	(med+max):2
(x_1)	100	5	23.83	42	23,5
(x_2)	100	7	29.18	65	36
(x_3)	100	18	47.99	80	49
(x_4)	100	34	57.77	83	58,5

Come considerazione di carattere generale, si può fare la seguente constatazione:
"al crescere di (x), i singoli valori di $S_6(x)$-a passo 1000- sono fluttuanti, ma generalmente crescenti".

(10)

Le caratteristiche rilevate nell'andamento dei valori di $S_6(x)$, ci hanno convinto della opportunità di estendere le vecchie ricerche effettuate fino ad (x)=400002, a valori ben maggiori di (x).
Solo recentemente, però, (1991), si è potuto disporre dell'uso dei mezzi di calcolo, e del contributo del personale idoneo, necessari per poter effettuare le ricerche che ci eravamo prefisse.

* * * * * * * *

3- Ricerche effettuate per $0 \le (x) \le 100000002$.

3.1- Generalità.

Le ricerche sono state condotte a "passo" 10^x facendo assumere ad (x) i seguenti valori:

$10^x - 2 \cdot 10^x - 3 \cdot 10^x - \ldots\ldots - 10^x \cdot 10^x$

Con tale "passo" di avanzamento di (x) sono stati determinati i valori dei parametri (vedere: (1)-(2)-(3)-(4)).

(10) $M_{6,5}(x)$-(11)$M_{6,1}(x)$-(12)$S_6(x)=M_{6,5}(x)-M_{6,1}(x)$

(13) $DS_6(x)=S_6[(m+1)10^x]-S_6(m10^x)$

($m \ge 1$, intero).

Dall'esame dei 10^x valori di $S_6(x)$, come sopra indicato, risultano confermati i "fenomeni" già rilevati per $0 \le (x) \le 400002$ - a passo "1000" (anzichè 10000, come in questo caso), e cioè:

- $S_6(x)$ è sempre positivo (1x)→(5)
- i valori di $S_6(x)$ si presentano fluttuanti, ma generalmente crescenti, anche se il rapporto $S_6(x):(x)$ presenta andamento decrescente, al crescere di (x). (15)→(10)

3.2- Grafico (campionato) dei valori di $S_6(x)$.

Per fornire un'idea immediata dell'andamento dei valori di $S_6(x)$, poichè non è pensabile di rappresentare in modo chiaro e completo i 10^x dati disponibili, ci si è limitati a riportare (vedere Delegato 1) una campionatura del loro grafico, relativa ai seguenti valori di (x):

$0 \le (x) \le 20 \cdot 10^5$ (parte iniziale)

*

$50 \cdot 10^5 \le (x) \le 55 \cdot 10^5$ (parte valori "bassi" di $S_6(x)$)

*

$70 \cdot 10^5 \le (x) \le 75 \cdot 10^5$ (parte valori "più alti" di $S_6(x)$)

*

$95 \cdot 10^5 \le (x) \le 100 \cdot 10^5$ (parte finale)

Per rendere la parte del "grafico" riportata, compatibile con lo spazio disponibile, si è proceduto con le seguenti modalità:

(1) Si sono considerati i seguenti valori crescenti di (x):

$$250\cdot10^3 - 500\cdot10^3 - 750\cdot10^3 - 10^5 - 1250\cdot10^3 - 1500\cdot10^3$$

(x_1) (x_2) (x_3) (x_4) (x_5) (x_6)

* * * *

$$\text{-------}99500\cdot10^3 - 99750\cdot10^3 - 100\cdot10^6$$

(x_{398}) (x_{399}) (x_{400})

("passo" di avanzamento: $250\cdot10^3$).

(2) - Per ciascun valore di (x): (x_1)-(x_2)-(x_3)-.....-(x_{400}), si sono considerati, per $S_6(x)$, i seguenti valori:

$S_6(x)$min.

$\Rightarrow$ rilevati a "passo" 10^x

$S_6(x)$max.

$S_6(x)$med.- Media aritmetica di tutti i 25 valori di $S_6(x)$ rilevati in (x).
La campionatura del grafico, come già detto, è riportata nell'allegato 1.
Da tale grafico si rileva, immediatamente, quanto segue:
- è confermata - per $0 \le (x) \le 100000002$ - la validità delle (5)-(10), relative a $0 \le (x) \le 400002$;
- i valori minimi e massimi di $S_6(x)$, nelle varie "fascie" considerate, generalmente, non sono equidistanti rispetto ai relativi $S_6(x)$med.

3.3- Ulteriori ricerche in programma.

(Con la speranza di poter disporre dei mezzi, e dell'aiuto, necessari per poterle realizzare).
Da un primo esame, specifico, dei singoli valori dei parametri:
$S_6(x)$- vedere (12) e $DS_6(x)$ - vedere (13) determinati, e tabulati, per (x) crescente a "passo" 10^x, è emersa l'opportunità, per cercare di chiarire i meccanismi (se ne esistono e sono determinabili) che regolano le loro fluttuazioni, di effettuare le statistiche frequenziali dei valori assunti dai predetti due parametri.
Per un primo approccio dello studio del problema, tali due statistiche potrebbero essere effettuate con le seguenti modalità di base:

(1)- Raggruppare i valori determinati (per (x) crescente a "passo" 10^x) nei "gruppi" di seguito indicati:

$(x_1) \to 5 \cdot 10^5; (x_2) \to 10 \cdot 10^5; (x_3) \to 15 \cdot 10^5; \ldots\ldots$

$\ldots\ldots; (x_{18}) \to 90 \cdot 10^5; (x_{19}) \to 95 \cdot 10^5; (x_{20}) \to 100 \cdot 10^5.$

Effettuare la statistica frequenziale di $S_6(x)$, e quella di $DS_6(x)$, nell'ambito di ciascuno dei 20 suddetti "gruppi".

(2)- Dalle statistiche degli $S_6(x)$ e dei $DS_6(x)$ di cui al precedente punto (1), sommando i loro risultati, come di seguito indicato, passare alla statistica degli $S_6(x)$ e dei $DS_6(x)$, relative ai seguenti "super gruppi":

$(x_1)' \to (x_1)+(x_2)$; $(x_2)' \to (x_1)+(x_2)+(x_3)$;

$(x_3)' \to (x_1)+(x_2)+(x_3)+(x_4)$; $(x_4)' \to (x_1)+(x_2)+(x_3)+(x_4)+(x_5)$

*

$(x_5)' \to (x_6)+(x_7)$; $(x_6)' \to (x_6)+(x_7)+(x_8)$;

$(x_7)' \to (x_6)+(x_7)+(x_8)+(x_9)$; $(x_8)' \to (x_5)+(x_7)+(x_8)+(x_9)+(x_{10})$

*

$(x_9)' \to (x_{11})+(x_{12})$; $(x_{10})' \to (x_{11})+(x_{12})+(x_{13})$; .....

..... ; $(x_{12})' \to (x_{11})+(x_{12})+(x_{13})+(x_{14})+(x_{15})$

*

$(x_{13})' \to (x_{16})+(x_{17})$; ..... ; $(x_{15})' \to (x_{16})+(x_{17})+(x_{18})+(x_{19})+(x_{20})$

* *

$(x_1)'' \to (x_4)'+(x_8)'$ $(x_2)'' \to (x_9)'+(x_{13})'$

* *

$(x_1)''' \to (x_1)''+(x_2)''$

Esaminare, infine, nell'ambito dei singoli "gruppi" e "super gruppi" i risultati delle varie statistiche effettuate per $S_6(x)$ e $DS_6(x)$ allo scopo di stabilire, se, e quanto le stesse si scostano dalla casualità teorica.

4 - Osservazioni.

Si sono confrontati i risultati ottenuti nello studio della distribuzione dei numeri primi del tipo $(6n \mp 1)$ con quelli - analoghi - relativi alla distribuzione dei numeri primi del tipo $(4n \mp 1)$, riportati nella pubblicazione (3) (vedere pagg. 79-84).
Dal confronto effettuato, almeno fino ad $(x) \leq 100 \cdot 10^6$, fra la distribuzione dei numeri primi del tipo $(6n \mp 1)$ e quella dei numeri primi del tipo $(4n \mp 1)$, unico elemento di differenziazione, che potrebbe presentare qualche interesse, è il seguente:
- i valori degli $S_o(x)$ sono sempre positivi;
- mentre quelli degli omologhi $S_n(x)$, pur essendo generalmente positivi, presentano saltuariamente "piccoli gruppi" (condensati) di valori negativi. Le distanze (sull'asse delle (x)) di questi "gruppi" di valori negativi, apparentemente si presentano irregolarmente.

* * *

Ringraziamenti
Gli autori ringraziano i signori CAMPITELLI ANDREA e DE BERARDINIS LUCA , alievi della facoltà di Ingegneria dell' Università dell'Aquila, per aver curato , anche criticamente , la redazione di questo lavoro.

Bibliografia
(1) - G. Moro - "memoria": "*Osservazioni sulla distribuzione dei numeri primi del tipo* $(6n \pm 1)$" - Atti del "Primo simposio su stato e prospettive della ricerca crittografica in Italia" - pagg. 156-161 - (Fondazione Ugo Bordoni - Roma 30-31 nov. 1987).
(2) - G. Moro - "Analisi crittografica e ricerca scientifica" - "Dimostrazione - Rienunciazione dell'ultimo teorema di Fermat" - Cap. V. (Pubblicazione edita a cura della Fondazione Ugo Bordoni - Roma 1990.)-
(3) - H. Poiesel.- *Prime Numbers and Computer methods for factorization-*
(Birkbauser - 1985).
(4) - M. Cerasoli, F. Eugeni e M. Protasi, *Elementi di Matematica Discreta,*
(Zanichelli, Bologna 1988).

Note on cipher hypersystem

S. Innamorati, Dip. di Matematica, Politecnico di Milano
F. Zuanni, Dip. di Ingegneria Elettrica, Università degli Studi, L'Aquila

Abstract.- Recently, see [2], cryptographic structures derived from generalized designs and hyperstructures have been investigated. In this paper we deal with cipher-hypersystems constructed by using finite geometry.

1. - Introduction.

Cryptography is the study of methods of sending messages that cannot be read by an unauthorized person. An old problem is the frequency analysis of the occurrences in the ciphertext. In the history of cryptography considerable efforts have been performed towards the construction of cryptosystems which have only few statistical information on the occurrences. A famous example is the homophones which are different symbols with the same meaning. As it is well-known, classical cipher-systems, such as the ancient Vigenere's square, are algebraic structures. In recent years, (cfr.[2]) algebraic hyperstructures have been considered in order to avoid frequency analysis. The aim of this paper is to look at cipher hypersystems constructed by using finite geometry.
The reason of using such structures is that it is very hard to discover the geometric connection of a pattern of points.

2. - Geometric spaces, hypergroupoids and cipher systems

Firstly, we recall some definitions.

A geometric space is a pair $(P,\mathcal{B})$, where P is a non-empty set of elements called points and $\mathcal{B}$ is a non-empty family of subsets of P called blocks.

A c-set C of a geometric space $(P,\mathcal{B})$ is said to be a c-arc if

1) $|B \cap C| \leq 2 \qquad \forall B \in \mathcal{B}$;

2) $\exists B \in \mathcal{B} \; : \; |B \cap C| = 2$.

Moreover a c-set C is said to be an intersection set if

$$B \cap C \neq \emptyset \qquad \forall B \in \mathcal{B} .$$

Of course, if each subset B of $\mathcal{B}$ has at least three points then the complementary set of a c-arc is an intersection set. An intersection set whose complementary set is an intersection set too is called a blocking set. Since many of today's applications deal with discrete geometric structures, the study of c-sets having graphic properties, such as arcs, intersection and blocking sets, is of interest to many authors (see [1],...,[14]).

Let t, v, k and λ be non-negative integers, with $v>k>t\geq 2$.

A geometric space $(\mathcal{P},\mathcal{B})$ is said to be a t-(v,k,λ) design if

1) $|P| = v$;

2) $|B| = k \qquad \forall B \in \mathcal{B}$;

3) each t-set of P is contained in exactly λ blocks of $\mathcal{B}$.

A t-(v,k,1) design is also called a Steiner system S(t,k,v).

Let A be a non-empty finite set called alphabet. Let us consider two subsets T and K of A, which are the set of the letters of the cleartext and the set of the keywords, respectively.

Moreover we suppose that the ciphertext symbols are elements of a family $\mathcal{C}$ of subsets of A.

A cipher system is a pair (A,f) where f is a function

$$f: \; T \times K \longrightarrow \mathcal{C}$$

such that

$$\forall C \in \mathcal{C} \; , \; \forall k \in K \quad \exists! t \in T \quad : \quad f(t,k) = C \; .$$

Let P be a non empty v-set. A function

$$o : P \times P \longrightarrow 2^P - \{\emptyset\}$$

is said to be a hyperoperation on P. The pair (P,o) is called a Marty hypergroupoid.

We will show that such three structures have a strict mutual relationship.

A geometric space $(P,\mathcal{B})$ defines a hypergroupoid (P,o) in the following natural way by setting for each $x,y\in P$

$$xoy = \bigcup_{\substack{B\in\mathcal{B}\\ x,y\in B}} B .$$

Let (P,o) be a Marty hypergroupoid. As with the previous notation, let A, T and K be three subsets of P. The pair $(A,o|_A)$ is an algebraic cipher hypersystem if
$\forall t\in T,\ k\in K,\ C\in\mathcal{C}$ the equation $tok = C$ has a unique solution.

Now it is clear how to deduce a cipher hypersystem from a geometric space, passing through a hyperstructure. To complete the scheme, the final step is to consider cipher hypersystems deduced directly from geometric spaces.

Let $(P,\mathcal{B})$ be a geometric space. The sets A, T and K, introduced before, will be subsets of P. Let us consider a family of subsets of A $\mathcal{C} = (C_{tk})_{t\in T,k\in K}$ such that

1) $(t_1,k_1)\neq(t_2,k_2) \Rightarrow C_{t_1k_1} \neq C_{t_2k_2}$.

Then it is naturally defined a function f

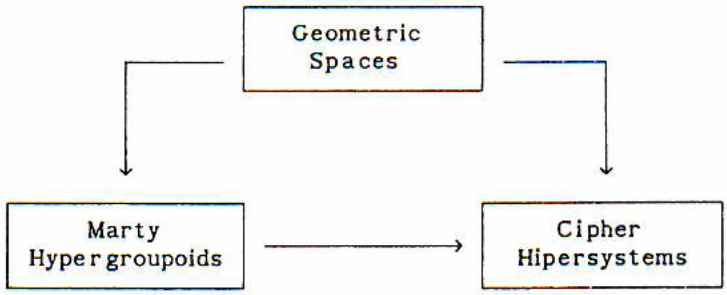
$$f : T\times K \longrightarrow \mathcal{C}$$

$$(t,k)\in T\times K \longrightarrow C_{tk}\in\mathcal{C}$$

such that

$$\forall C\in\mathcal{C},\ \forall k\in K\ \ \exists! t\in T\ :\ f(t,k) = C .$$

So the pair (A,f) is a cipher hypersystem.
We observe that 1) is a strong condition, in fact in section 3 we present an example of cipher hypersystem in which 1) doesn't hold.
The mutual relationship between the structures introduced before can be summarized in the following diagram



3. - An example of cipher hypersystem

In this section we will present an example of cipher hypersystem obtained by a geometric space.

Let $\mathcal{D}=(S,\mathcal{B})$ be a S(t,k,v) Steiner system, t>2. It is well-known that $\mathcal{D}$ is a (t-1)-(v,k,λ) design where λ=(v-t+1)/(k-t+1). Fix a c-arc $\mathcal{T}$. A cipher system can be obtained by considering the set S as the alphabet and the arc $\mathcal{T}$ as the cleartext set T and as the keywords set K.

Let us suppose that we want to send a message consisting of several points and denote one of these by m. In order to cipher m by a key h we choose at random one of the blocks through m and h. Let B denote this block. The ciphertext C is a set of (t-1) points chosen at random by B-{h,m}. The receiver knows the key h of the system. When he receives C he computes the unique block B through the t-set C∪{h}. The message is $\mathcal{T}\cap B-\{h\}$. If $\mathcal{T}\cap B-\{h\}=\emptyset$ then the system assumes the key h as the message m.

Since an unauthorized person doesn't know the correct key h he has 1/λ possibilities to guess the block B.

To increase the security we assume that the users of the cryptographic system have access to a fixed sequence of c-arcs.

An ideal cipher system is the one that the ciphertext contains no statistical information.

The two previous choices have been introduced in order to avoid fequency analysis of the ciphertext occurrences.

References

[1] L.BERARDI, *Constructing 3-designs from spreads and lines*, Discrete Math. 74 (1989), 331-332.

[2] L.BERARDI, F.EUGENI and S.INNAMORATI, *Generalized designs, linear spaces, hypergroupoids and algebraic cryptography*, Proc. IV int. congress on AHA, World Scientific, 1990, 55-65.

[3] A.BEUTELSPACHER and F.EUGENI, *Geometrie finite e crittosistemi*, Atti del II Simposio Naz. "Stato e prospettive della ricerca crittografica in Italia", Roma Novembre 1989.

[4] A.BICHARA and G.KORCHMAROS, n^2*-sets in a projective plane which determine exactly* n^2+n *lines*, J. of Geometry, Vol. 15/2, 1980, 175-181.

[5] M.CERASOLI, F.EUGENI and M.PROTASI, *Elementi di Matematica Discreta*, Zanichelli Bologna, 1986.

[6] P.CORSINI, *Prolegomeni alla Teoria degli Ipergruppi*, Quad. dell'Istituto di Informatica e Sistemistica, Udine 1982.

[7] F.EUGENI, *Combinatorics and Cryptography*, Lecture given at the Int. Conf. "COMBINATORICS '90", Gaeta (Italy), May 1990.

[8] F.EUGENI and M.GIONFRIDDO, *On the minimum number of blocks of a maximal partial spread in* STS(v) *and* SQS(v), Journal of Geometry 36 (1989), 37-48.

[9] M.GIONFRIDDO, *Hypergroups associated with multihomomorphisms between generalized graphs*, Atti del Convegno su "Sistemi binari e loro applicazioni", Taormina (Italy) 1978, 161-174.

[10] B.SEGRE, *Lectures on modern geometry*, Cremonese Roma, 1961.

[11] G.TALLINI, *Strutture grafiche proiettive*, Liguori Napoli, 1967.

[12] G.TALLINI, *Geometric hyperquasigroups and line space*, Acta Univ. Carolinae 25 (1984), 69-73.

[13] G.TALLINI, *On Steiner hypergroups and linear codes*, Atti del Convegno su "Ipergruppi, altre strutture multivoche e loro applicazioni", Udine (Italy) 1985, 87-91.

[14] M. TALLINI SCAFATI, *Sui (k;n)-archi di un piano grafico finito, con particolare riguardo a quelli con due caratteri*, Nota I e II, Rend. Acc. Naz. Lincei, 8, 40 (1966), 812-818, 1020-1025.

Rappresentazione geometrica di parole.

Carlo Felice Manara

§.1 - Indichiamo con b un vettore ad n componenti b(i) ($1 \leq i \leq n$) ciascuna delle quali vale 0 oppure 1. Si ha quindi per ogni i:

(1) $$(b(i) = 0) \vee (b(i) = 1) .$$

Nel seguito un vettore cosiffatto sara' anche chiamato "vettore binario". Indichiamo con B l'insieme di tutti i vettori b. Si ha:

$$B = \text{Cardinalita' di } B = 2^n$$

§.2 - Indichiamo con c un vettore ad n componenti c(i) ($1 \leq i \leq n$), ciscuna delle quali sia un numero reale positivo; si avra' quindi, per ogni indice i:

(2) $$c(i) > 0.$$

Indichiamo con C l'insieme di tutti i vettori c.

§.3 - Considerato un vettore b di B, poniamo:

(3) $$s(b) = b \times c = \Sigma\, b(i)c(i) \quad (1 \leq i \leq n),$$

prodotto scalare dei due vettori b e c.

Per un dato intero naturale n, indichiamo con S(n) l'insieme di tutti i numeri s(n) definiti dalla (3). Si ha ovviamente:

$$S(n) = \text{Cardinalita' di } S(n) \leq 2^n.$$

OSSERVAZIONE 1 - L'insieme S(n) e' ovviamente costituito da tutte le somme di un numero qualunque di componenti del vettore c, compresa la somma nulla.

§.4 - Indichiamo con J l'insieme degli indici interi da 1 a 2^n, ed indichiamo con R(n) l'insieme degli elementi di S(n), ordinato secondo l'ordinamento stabilito nei reali dalla relazione " $\leq$ ".

Pertanto, indicato con r(j) un elemento di R(n) ($1 \leq j \leq 2^n$), si avra':

a) esiste un vettore **b** di B tale che sia:

(4) $$r(j) = s(b);$$

b) per ogni indice j si ha:

(5) $$r(j) \leq r(j+1).$$

§.5 - OSSERVAZIONE 2 - Per ogni intero n, e' possibile scegliere il vettore **c** in modo che l'insieme S(n) (e quindi anche R(n)) sia costituito da numeri tutti diversi tra loro, e quindi siano valide, invece delle (5), le:

(6) $$r(j) < r(j+1).$$

OSSERVAZIONE 3 - Qualora le (6) fossero verificate, si avrebbe una bijezione (corrispondenza biunivoca) tra i vettori di B e gli elementi di R(n); quindi ognuno di questi ultimi potrebbe essere assunto come coordinata unica, o come "cifra" del corrispondente elemento di B.

OSSERVAZIONE 4 - Le condizioni (6) possono essere soddisfatte in molti modi; e' noto per es. che esse sono verificate quando gli elementi del vettore **c** sono scelti in modo tale che, per ogni indice i, l'elemento c(i) sia maggiore della somma di tutti quelli che hanno indice inferiore.

Tuttavia con queste scelte si giunge ad avere degli elementi rappresentati da numeri molto grandi, al crescere di n; per esempio, supponendo che tutti gli elementi di **c** siano numeri naturali, e scegliendo c(1) = 1, gli elementi del vettore **c** crescono piu' rapidamente degli elementi della successione di Fibonacci. E' possibile invece scegliere gli elementi del vettore **c** in modo che esssi costituiscano una successione decrescente, ed anche che siano maggiorati dagli elementi di una serie convergente a termini positivi.

La dimostrazione di questo fatto puo' essere data induttivamente.

I) La cosa e' vera per n = 2, infatti basta prendere:

$$c(1) > c(2) > 0.$$

In questo caso gli elementi di R(2) sono 4, e precisamente:

$$0 \ , \ c(2) \ , \ c(1) \ , \ c(1)+c(2);$$

essi sono ovviamente tutti distinti tra loro, e corrispondono rispettivamente ai vettori b di componenti:

$$(0,0) \quad (0,1) \quad (1,0) \quad (1,1).$$

II) Supponiamo ora vere tutte le (6) per un dato valore di n, e dimostriamo che si puo' scegliere un vettore **c** di (n+1) componenti in modo che le (6) continuino ad essere rispettate.

Indichiamo con **c'** un vettore ad (n+1) componenti, tra le quali le prime n coincidono con quelle di **c**; indichiamo con R' l'insieme di tutte le $2^{(n+1)}$ somme di elementi di **c'**. La cardinalita' di R' e' quindi il doppio di quella di R(n); essi sono gli elementi di R' in cui non entra la nuova componente c(n+1) di **c'**, e che quindi corrispondono a vettori di B per cui si ha b(n+1) = 0.

Gli altri 2^n elementi di R' si ottengono da quelli di R sommando ad ognuno di essi la nuova componente c(n+1) di **c'**.

Poniamo ora:

$$(7) \qquad d(j) = r(j+1) - r(j) \qquad (1 \leq j \leq 2^{(n-1)}),$$

e sia u il minimo dei numeri d(j).

Si osserva ora che tutti gli elementi di R' che appartengono al primo gruppo di 2^n elementi sono distinti tra loro, per ipotesi. Se poi si sceglie c(n+1) in modo che sia

$$(8) \qquad c(n+1) < u$$

anche tutti gli elementi del secondo gruppo sono tutti distinti (tra loro, ovviamente, ma anche) da tutti gli elementi del primo gruppo.

OSSERVAZIONE 5 - Quando si supponga che n possa non esser superiormente limitato, la condizione (8) e' compatibile con con ogni condizione di convergenza della serie:

$$(9) \qquad \Sigma \, c(j).$$

§.6 - Indichiamo con m un numero naturale, e sia A un alfabeto, costituito da m simboli tutti distinti tra loro:

$$(10) \qquad a(i) \quad (1 \leq i \leq m).$$

Sia N un numero naturale e sia P una successione di N elementi di A; diremo, secondo l'uso, che P e' una "parola", e che gli elementi dell'alfabeto A che compaiono nei vari posti di P sono le "lettere" della P stessa.

Ovviamente la P e' determinata quando si assegni la lettera dell'alfabeto A che compare ad ogni posto della successione P; indicando con j l'indice di una lettera in A e con i il posto di un elemento nella successione P, la parola P e' quindi determinata da una funzione numerica p che assegna j in funzione di i:

(11) $$j = p(i)$$

§.7 - Per rappresentare una parola P ad n lettere si puo' far ricorso ad una matrice rettangolare Q (N x m) ad N righe ed m colonne; indicato con q(i,j) l'elemento di Q che appartiene alla riga di indice i ($1 \leq i \leq N$) ed alla colonna di indice j ($1 \leq j \leq m$), porremo

(12) $$q(i,j) = 1$$

se e solo se la lettera di posto i di P e' l'elemento di posto j dell'alfabeto, e porremo

(13) $$q(i,j) = 0$$

in ogni altro caso.

Di conseguenza si ha che:

1) in ogni riga della matrice Q vi e' un solo elemento uguale ad 1 e gli altri sono tutti zero;

2) ogni colonna di Q e' un vettore di tipo **b**, le cui N componenti valgono soltanto 1 oppure 0: quindi ogni colonna di Q puo' corrispondere ad un elemento dell'insieme S(n); tale numero puo' essere considerato come la "cifra" del vettore **b**, se gli N elementi del vettore **c** sono stati scelti come e' chiarito nella Oss.4. Per quanto e' stato detto nella osservazione citata, tali "cifre" sono tutte diverse tra loro.

§.8 - Cio' che e' stato detto finora puo' essere esposto sotto forma geometrica con la seguente procedura.

Sia E uno spazio euclideo ad m dimensioni, avente cioe' un numero di dimensioni uguale a quello delle lettere dell'alfabeto considerato; indichiamo con X un punto di E e siano:

$$x(1),\ x(2),\ .....,\ x(m)$$

le sue coordinate cartesiane. Scegliendo come coordinate i numer' di S(n) corrispondenti alla prima, alla seconda, alla m-esima colonna della matrice Q, il punto X rappresentera' in modo biunivoco la parola P.

OSSERVAZIONE 6 - Da cio' che e' stato esposto nei NN 1...5 si deduce che, scelta una successione **c** che soddisfi alla condizione (8), ogni vettore binario **b** puo' essere rappresentato con un unico numero reale che, come abbiamo detto puo' essere considerato come la sua "cifra"; se poi le componenti del vettore **c** sono razionali tale "cifra" e' ovviamente un numero razionale. Se quest'ultimo e' rappresentato sotto forma di frazione irriducibile, allora si ha che ogni vettore binario **b** puo' essere "cifrato" con una coppia ordinata di numeri naturali.

Gli sviluppi dei NN 6...8 permettono una rappresentazione geometrica dell'insieme delle parole su uno spazio euclideo E ad m dimensioni; si potrebbe cosi definire una metrica sull'insieme delle parole, e quindi anche una topologia; in particolare si potrebbero interpretare le abituali operazioni sulle parole con operazioni geometriche sullo spazio, e le relazioni tra parole come relazioni tra i punti che le rappresentano; per esempio si ha facilmente che tutte le parole scritte nell'alfabeto A che hanno la medesima lunghezza N sono rappresentate da punti di E che appartengono all'iperpiano avente equazione:

$$\Sigma\ x(j) = \Sigma\ c(i) \quad (1 \leq j \leq m,\ 1 \leq i \leq N)$$

Carlo Felice MANARA
Via G.B.Piranesi, 22
20137 MILANO

Su alcune strutture di spazio metrico con sostegno l'insieme delle variabili casuali associate a successioni di numeri a caso

A. Maturo, Dip. di Scienze, Storia dell'Architettura e Restauro, Viale Pindaro 42, 65127 Pescara

Sommario: Si mostra come, generalizzando i concetti relativi all'analisi di Fourier di successioni di numeri pseudocasuali ed introducendo la nozione di variabile casuale n-dimensionale associata ad una successione di numeri pseudocasuali, si può dotare in più modi l'insieme di tali variabili casuali di una struttura di spazio metrico soddisfacente ad opportune condizioni assegnate.

In particolare, in tali spazi metrici, la distanza di una variabile casuale X da una variabile casuale uniforme continua o discreta normalizzata si può interpretare come discrepanza di ordine n fra una successione di numeri pseudocasuali associata ad X e la condizione di equidistribuzione in $[0,1]^n$.

Come casi particolari si ottengono le condizioni prese in considerazione nei lavori [1], [2], [5].

1. SIMBOLOGIA E CONSIDERAZIONI PRELIMINARI.

Sia Z l'insieme dei mumeri interi. Per ogni intero m>0, poniamo

$$I(m) = Z \cap [0, m),\ J(m) = Z \cap [-m/2, m/2),$$

$$P(m) = \{x \in R : "\exists\, z \in I(m) : x=z/m"\},$$

ossia $P(m) = \{0, 1/m, 2/m, \ldots, (m-1)/m\}$.

Quando dal contesto non vi sia possibilità di equivoco, al posto di I (m),

J(m), P (m) useremo semplicemente i simboli I, J, P.

Per ogni intero $n > 1$ e per ogni insieme X, usiamo indifferentemente i simboli X^n e X_n per indicare il prodotto cartesiano di n insiemi uguali ad X. Con X_1 e X^1 indichiamo, inoltre, l'insieme X.

Per ogni $x \in R$ e per ogni $\underline{x} \in R^n$, poniamo

$e(x) = \exp(2\pi i x) = \cos 2\pi x + i \operatorname{sen} 2\pi x,$

$$\varepsilon(\underline{x}) = \begin{cases} 1 & \text{se } \underline{x} \in Z^n \\ 0 & \text{se } \underline{x} \in R^n - Z^n \end{cases}$$

Valgono le seguenti proposizioni, di immediata dimostrazione.

Proposizione 1.1. Se $\underline{x}=(x_1, x_2, \ldots, x_n)$, allora $\varepsilon(\underline{x})=\varepsilon(x_1)\,\varepsilon(x_2) \ldots \varepsilon(x_n)$.

Proposizione 1.2. La funzione e(x) è periodica di periodo 1.

Proposizione 1.3. Per ogni coppia di interi (m,z), con $m > 0$, risulta

$$(1.1) \quad \frac{1}{m}\sum_{r=0}^{m-1} e(zr/m) = \varepsilon(z/m) .$$

Dimostrazione. Se z è multiplo di m, per la proposizione 1.2, si ha $\forall r \in N$ $e(zr/m)=e(0)=1$, per cui il primo membro della (1.1) è uguale ad 1. D'altra parte, per come è stato definito $\varepsilon(x)$, anche il secondo membro è uguale ad 1 e quindi la proposizione è dimostrata.

Se z non è multiplo di m, poichè $e(zr/m)=[e(z/m)]^r$, i termini della sommatoria a primo membro formano una progressione geometrica di ragione $e(z/m) \neq 1$.

La somma S dei termini di tale progressione è allora

$$S=\frac{1-[e(z/m)]^m}{1-e(z/m)}=\frac{1-e(z)}{1-e(z/m)}=0.$$

Dato che pure il secondo membro è nullo, anche in questo caso la proposizione è dimostrata. ❑

Proposizione 1.4. Se m è un intero positivo e $\underline{z} \in Z^n$, risulta

$$(1.2) \quad \frac{1}{m^n}\sum_{\underline{r} \in I_n(m)} e(\underline{z}\cdot\underline{r}/m) = \frac{1}{m^n}\sum_{\underline{s} \in J_n(m)} e(\underline{z}\cdot\underline{s}/m) = \varepsilon(\underline{z}/m) .$$

Dimostrazione. L'uguaglianza fra i primi due membri della (1.2) è immediata conseguenza del fatto che sottraendo m ad una o più componenti di $\underline{r}$, l'argomento $\underline{z}\cdot\underline{r}/m$ varia di una quantità intera h e, per la proposizione 1.2, risulta $e(\underline{z}\cdot\underline{r}/m)=e(\underline{z}\cdot\underline{r}/m+h)$. Dimostriamo, allora, l'uguaglianza fra il primo e

il terzo membro.

Sia $\underline{r}=(r_1, r_2,\ldots, r_n)$. Poichè $e(\underline{z}\cdot\underline{r}/m)=\prod_{i=1}^{n} e(z_i r_i/m)$, si ha che

$$(1.3)\quad \frac{1}{m^n}\sum_{\underline{r}\in I_n(m)} e(\underline{z}\cdot\underline{r}/m)=\prod_{i=1}^{n}\frac{1}{m}\sum_{r_i=0}^{m-1} e(z_i r_i/m).$$

Poichè per la proposizione (1.1) è

$$(1.4)\qquad \varepsilon(\underline{z}/m)=\prod_{i=1}^{n}\varepsilon(z_i/m)\,,$$

confrontando le (1.1), (1.3), (1.4) si deduce l'asserto. ❑

2. M - TRASFORMATA DI FOURIER.

Sia $g(\underline{x})$ una funzione definita in un insieme $S\subseteq[0,1)^n$ ed a valori nel campo C dei numeri complessi.

Definizione 2.1. Se $S\supseteq P_n(m)$, diciamo **m-trasformata di Fourier della $g(\underline{x})$** la funzione

$$(2.1)\quad h:\underline{z}\in Z_n \rightarrow \begin{cases} 0 \text{ per } \underline{z}\in Z^n - J_n(m) \\ \dfrac{1}{m^n}\displaystyle\sum_{\underline{x}\in P_n(m)} e(-\underline{z}\cdot\underline{x})\, g(\underline{x}) \text{ per } \underline{z}\in J_n(m) \end{cases}$$

Inoltre, per ogni $\underline{z}\in Z^n$, chiamiamo $h(\underline{z})$ **m-coefficiente di Fourier di indice $\underline{z}$ della $g(\underline{x})$.**

Qualora non vi siano equivoci sul valore di m, parleremo semplicemente di trasformata e coefficienti di Fourier.

Osservazione 2.1. Notiamo che se $S=[0,1)^n$, risulta, sotto opportune ipotesi sulla $g(\underline{x})$,

$$(2.2)\quad h^*(\underline{z})=\lim_{m\to+\infty} h(\underline{z})=\int_{[0,1)^n} e(-\underline{z}\cdot\underline{x})\, g(\underline{x})\, d\underline{x}\,,$$

ossia gli m - coefficienti di Fourier della $g(\underline{x})$ tendono, per $m\to+\infty$, ai coefficienti $h^*(\underline{z})$ della serie di Fourier, n - dimensionale, di tale funzione.

Su tale osservazione possono basarsi criteri per confrontare certe distribuzioni di probabilità "eterogenee", ossia discrete con diverso insieme di definizione o una continua e una discreta.

Teorema 2.1. Le funzioni definite in $P_n(m)$ ed a valori in C formano, rispetto alle consuete operazioni, uno spazio vettoriale $F_n(m)$ su C di dimensione m^n.

Dimostrazione. Il fatto che $F_n(m)$ sia uno spazio vettoriale su C è una immediata conseguenza di considerazioni elementari.

Si consideri ora, per ogni $\underline{y} \in P_n(m)$, la funzione

$$(2.3)\quad f_{\underline{y}} : \underline{x} \in P_n(m) \to \varepsilon(\underline{y}-\underline{x})$$

Le m^n funzioni (2.3) sono linearmente indipendenti.

Infatti, data una loro qualsiasi combinazione lineare con coefficienti $a_{\underline{y}}$, risulta, tenendo conto della definizione di $\varepsilon(\underline{x})$,

$$\sum_{\underline{y}\in P_n(m)} a_{\underline{y}} f_{\underline{y}} = \underline{0} \Leftrightarrow \forall \underline{x} \in P_n(m)\ ,\ \sum_{\underline{y}\in P_n(m)} a_{\underline{y}} \varepsilon(\underline{y}-\underline{x}) = 0$$

$$\Leftrightarrow\ \forall \underline{x} \in P_n(m)\ ,\ a_{\underline{x}} = 0\ .$$

Inoltre, se g è una qualsiasi funzione definita in $P_n(m)$, si ha, per ogni $\underline{x} \in P_n(m)$,

$$g(\underline{x}) = \sum_{\underline{y}\in P_n(m)} g(\underline{y})\ \varepsilon(\underline{y}-\underline{x})\ ,$$

per cui g è combinazione lineare delle $f_{\underline{y}}$ con coefficienti $g(\underline{y})$.

Segue che le $f_{\underline{y}}$ formano una base di $F_n(m)$ e quindi l'asserto. ❑

Teorema 2.2. Le funzioni

$$(2.4)\quad e_{\underline{z}} : \underline{x} \in P_n(m) \to e(\underline{z}\cdot\underline{x})\ ,\ \text{con}\ \underline{z} \in J_n(m),$$

costituiscono una base di $F_n(m)$. Di conseguenza ogni funzione g definita in $P_n(m)$ si può esprimere in una sola maniera come combinazione lineare delle funzioni $e_{\underline{z}}$.

Precisamente risulta

$$(2.5)\quad g = \sum_{\underline{z}\in J_n(m)} h(\underline{z})\ e_{\underline{z}},$$

dove i coefficienti $h(\underline{z})$ sono gli m - coefficienti di Fourier della funzione g.

Dimostrazione. Poichè le funzioni $e_{\underline{z}}$ sono m^n, per dimostrare che esse formano una base di $F_n(m)$ basta far vedere che ogni funzione g definita in $P_n(m)$ è combinazione lineare di esse.

A tale scopo, consideriamo, per ogni $\underline{x} \in P_n(m)$, l'espressione

$$(2.6)\quad S(\underline{x}) = \sum_{\underline{z}\in J_n(m)} h(\underline{z})\ e(\underline{z}\cdot\underline{x}).$$

Per la (2.1) risulta

$$S(\underline{x}) = \sum_{\underline{z}\in J_n(m)} \frac{1}{m^n} \sum_{\underline{v}\in P_n(m)} e(-\underline{z}\cdot\underline{v})\, g(\underline{v})\, e(\underline{z}\cdot\underline{x}) =$$

$$= \sum_{\underline{v}\in P_n(m)} \left[\frac{1}{m^n} \sum_{\underline{z}\in J_n(m)} e(\underline{z}\cdot(\underline{x}-\underline{v})) \right] g(\underline{v}).$$

Per la (1.2) l'espressione fra parentesi quadre è uguale a $\varepsilon(\underline{x}-\underline{v})$. Segue che $S(\underline{x})=g(\underline{x})$ e quindi, per la (2.6), vale la (2.5). ❑

Corollario 2.1. Ogni funzione g definita in $P_n(m)$ si può scrivere nella forma

$$(2.7)\quad g(\underline{x}) = \sum_{\underline{z}\in J_n(m)} h(\underline{z}) e(\underline{z}\cdot\underline{x}) \;,\; \forall \underline{x}\in P_n(m) \;,$$

e la (2.7) è l'unica maniera in cui g si può esprimere come combinazione lineare delle $e_{\underline{z}}$.

Segue che due funzioni g_1 e g_2 definite in $P_n(m)$coincidono se e solo se hanno gli stessi m - coefficienti di Fourier.

Osservazione 2.2. Se $g(\underline{x})$ è definita in un insieme S tale che $P_n(m)\subseteq S\subseteq[0,1)^n$, le considerazioni svolte nei teoremi 2.1. e 2.2 si intendono riferite alla restrizione di g all'insieme $P_n(m)$.

In tale ordine di idee possiamo notare che, se $S=[0,1)^n$, sotto opportune ipotesi sulla $g(\underline{x})$, la (2.7) tende, per $m\to+\infty$, alla serie di Fourier n - dimensionale della $g(\underline{x})$

$$(2.8)\quad g(\underline{x}) = \sum_{\underline{z}\in Z_n} h^*(\underline{z})\, e(\underline{z}\cdot\underline{x}) \;,$$

dove gli $h^*(\underline{z})$ sono dati dalle (2.2).

3. M - TRASFORMATE DI FUNZIONI DI PROBABILITÁ.

Sia X una variabile casuale definita nell'insieme P(m) e sia $\underline{X}=(X_1, X_2, \ldots, X_n)$ una variabile casuale n - dimensionale le cui componenti siano somiglianti ad X.

Definizione 3.1. Diciamo **funzione di probabilità** di $\underline{X}$ la funzione, definita in $P_n(m)$

$$f:\underline{x}\in P_n(m) \;\to\; \text{prob}\,(\underline{X}=\underline{x})$$

Sia ora, per ogni $\underline{x}\in P_n(m)$, $H(\underline{x})$ l'intervallo semiaperto superiormente di primo estremo $\underline{x}$ e dimensioni tutte uguali a 1/m. La misura di $H(\underline{x})$ è uguale a $1/m^n$.

Se immaginiamo di ripartire uniformemente su tale intervallo la massa di probabilità $f(\underline{x})$, ogni punto $\underline{y} \in H(\underline{x})$ avrà densità di probabilità

$$\tilde{g}(\underline{x}) = f(\underline{x}) \cdot m^n \ .$$

L'idea alla base di tali considerazioni è quella di rendere in qualche modo confrontabili due variabili casuali discrete n - dimensionali, definite rispettivamente in $P_n(m_1)$ e $P_n(m_2)$ con $m_1 \neq m_2$, e una di queste con una variabile casuale continua definita in $[0,1)^n$.

Diamo allora le seguenti definizioni.

Definizione 3.2. Sia $f(\underline{x})$ la funzione di probabilità $\underline{X}$. Diciamo **funzione densità di probabilità** di $\underline{X}$ o associata ad $f(\underline{x})$ la funzione,

$$(3.1) \qquad g: \underline{x} \in P_n(m) \rightarrow f(\underline{x}) \cdot m^n .$$

Diciamo, inoltre, prolungamento canonico della g a $[0,1)^n$ la funzione

$$(3.2) \qquad \tilde{g}: \underline{y} \in H(\underline{x}) \ \rightarrow \ f(\underline{x}) \cdot m^n \ .$$

Definizione 3.3. Diciamo **m-trasformata e m - coefficienti di Fourier** della funzione di probabilità $f(\underline{x})$ o della variabile casuale $\underline{X}$ rispettivamente la m–trasformata e gli m–coefficienti della funzione densità di probabilità di $\underline{X}$.

Tenuto conto delle (2.1) e (3.1) si ha allora che l' m - coefficiente di Fourier di indice $\underline{z}$ di $f(\underline{x})$ è

$$(3.3) \quad h(\underline{z}) = \begin{cases} \sum_{\underline{x} \in P_n(m)} e(-\underline{z} \cdot \underline{x}) f(\underline{x}), \text{ per } \underline{z} \in J_n(m) \\ 0 \ , \text{ per } \underline{z} \in Z^n - J_n(m). \end{cases}$$

Inoltre, sostituendo nella (2.7) a $g(\underline{x})$ l'espressione $f(\underline{x}) \cdot m^n$, si può scrivere

$$(3.4) \quad f(\underline{x}) = \frac{1}{m^n} \sum_{\underline{z} \in J_n(m)} h(\underline{z}) \, e(\underline{z} \cdot \underline{x}), \ \forall \underline{x} \in P_n(m) \ .$$

Nelle ipotesi su $\underline{X}$ ammesse all'inizio del paragrafo, detta $f(\underline{x})$ la funzione di probabilità di $\underline{X}$, valgono le seguenti proposizioni.

Proposizione 3.1. I coefficienti di Fourier $h(\underline{z})$ sono tali che

$$(3.5) \quad |h(\underline{z})| \leq 1 \ , \ \forall \underline{z} \in Z_n \ ,$$

$$(3.6) \qquad h(\underline{0}) = 1.$$

Dimostrazione. Risulta per la (3.3)

$$|h(\underline{z})| \le \sum_{\underline{x}\in P_n(m)} |e(-\underline{z}\cdot\underline{x})f(\underline{x})| = \sum_{\underline{x}\in P_n(m)} f(\underline{x}) = 1$$

Inoltre

$$h(\underline{0}) = \sum_{\underline{x}\in P_n(m)} f(\underline{x}) = 1$$

❑

Proposizione 3.2. La variabile casuale $\underline{X}$ è equidistribuita in $P_n(m)$ se e solo se

(3.7) $\qquad h(\underline{z}) = 0, \quad \forall\, \underline{z} \neq \underline{0}$.

Dimostrazione. Se $\underline{X}$ è equidistribuita in $P_n(m)$ si ha, per ogni $\underline{x}\in P_n(m)$, $f(\underline{x})=1/m^n$, per cui, per ogni $\underline{z}\in J_n(m)-\{\underline{0}\}$, risulta

$$h(\underline{z}) = \frac{1}{m^n} \sum_{\underline{x}\in P_n(m)} e(-\underline{z}\cdot\underline{x}) .$$

Posto $\underline{v}=m\underline{x}$, si ha allora, per la (1.2),

$$h(\underline{z}) = \frac{1}{m^n} \sum_{\underline{v}\in I_n(m)} e(-\underline{z}\cdot\underline{v}/m) = \varepsilon(-\underline{z}/m) = 0 .$$

Viceversa, se valgono le (3.7), dalla (3.4) si deduce che $f(\underline{x})=1/m^n$, $\forall \underline{x}\in P_n(m)$. ❑

Proposizione 3.3. Per ogni $\underline{z}\in J_n(m)$ avente tutte le componenti diverse da $-m/2$, risulta $|h(\underline{z})| = |h(-\underline{z})|$.

Dimostrazione. Cominciamo con l'osservare che, se $\underline{z}$ ha tutte le componenti di diverse da $-m/2$, allora $\underline{z}\in J_n(m) \Rightarrow -\underline{z}\in J_n(m)$.

Per ogni numero complesso $\underline{x}$, indichiamo con $Re(x)$ e $Im(x)$ le parti reale e immaginaria di x.

Poichè, $\forall \underline{x}\in P_n(m)$, $Re(e(-\underline{z}\cdot\underline{x}))=Re(e(\underline{z}\cdot\underline{x}))$, $Im(e(-\underline{z}\cdot\underline{x}))=-Im(e(\underline{z}\cdot\underline{x}))$ ed $f(\underline{x})$ è un numero reale, dalle (3.3) si deduce

$$Re(h(\underline{z}))=Re(h(-\underline{z})),\ Im(h(\underline{z}))=-Im(h(-\underline{z})),$$

da cui segue che $|h(\underline{z})| = |h(-\underline{z})|$.❑

4. MISURE DI VICINANZA E DI DISCREPANZA DI UNA DISTRIBUZIONE DA QUELLA UNIFORME.

Sia $\underline{X}$ una variabile casuale definita in $P_n(m)$ e siano $f(\underline{x})$ e $g(\underline{x})$ rispettivamente le funzioni di probabilità e di densità di probabilità di $\underline{X}$.

La (2.7) può essere interpretata, da un punto di vista fisico, come scomposizione della funzione $g(\underline{x})$ in una costante $h(\underline{0})=1$ e in più onde n - dimensionali aventi i seguenti parametri

frequenza	$\underline{z}$,
numero d'onda	$\lvert\underline{z}\rvert$,
lunghezza d'onda	$1/\lvert\underline{z}\rvert$,
ampiezza	$h(\underline{z})$,
modulo dell'ampiezza	$\lvert h(\underline{z})\rvert$.

Per la proposizione (3.2) la $\underline{X}$ è equidistribuita se e solo se tutte le onde hanno ampiezza nulla. In caso contrario, per assegnare una misura della discrepanza di $\underline{X}$ dalla variabile casuale equidistribuita in $P_n(m)$, si deve tener conto dei valori assunti dai parametri elencati.

Nei lavori [1], [2], vengono messi in evidenza i seguenti fatti:

(I) a parità di modulo dell'ampiezza il contributo alla discrepanza aumenta con l'aumentare della lunghezza d'onda;

(II) a parità di lunghezza d'onda il contributo alla discrepanza aumenta con l'aumentare del modulo dell'ampiezza.

Nel corso dei due lavori, però, vengono esaminate variabili casuali particolari, in cui $\lvert h(\underline{z})\rvert$ è, per ogni $\underline{z}\in J_n(m)$, sempre uguale o a zero o ad uno, e vengono forniti criteri per la misura della discrepanza da una distribuzione uniforme validi solo per tali variabili.

Se $\underline{X}$ non è uniforme, detto S l'insieme dei $\underline{z}\in J_n(m)-\{\underline{0}\}$ tali che $\lvert h(\underline{z})\rvert\neq 0$, in [1] viene proposto di misurare la vicinanza di $\underline{X}$ da una variabile equidistribuita in $P_n(m)$ tramite il numero

$$\mu_n=\min_{\underline{z}\in S}\lvert\underline{z}\rvert \tag{4.1}$$

e in [2] viene proposto di misurare tale vicinanza con il numero

$$\sigma_n=\frac{\pi^{n/2}\mu_n^n}{m\,\Gamma\left(\frac{n+2}{2}\right)} \tag{4.2}$$

esprimente il volume di una ellissoide in R^n, ritenuta particolarmente significativa.

Chiamiamo, per comodità, μ_n e σ_n rispettivamente **vicinanza di Coveyou**

e **di Knuth** e i loro reciproci $M_n=1/\mu_n$ e $S_n=1/\sigma_n$ rispettivamente **discrepanza di Coveyou e di Knuth.**

Definizione 4.1. Diciamo **generatore ricorrente di ordine k di successioni pseudocasuali**, con modulo il numero intero positivo m, una formula del tipo

$$x_{h+k}=G(x_h, x_{h+1}, \ldots, x_{h+k-1}), \tag{4.3}$$

dove G è una funzione definita in $I_k(m)$ ed a valori in I(m).

La funzione G dipende in genere da certi parametri $\alpha_1, \alpha_2, \ldots, \alpha_s$.

La successione $\{x_h\}_{h\in N}$ è determinata dalla funzione G e dai valori $x_0, x_1, \ldots, x_{k-1}$, detti valori iniziali che devono essere fissati a priori in I(m).

Poichè gli elementi di $I_k(m)$ sono m^k, è facile dimostrare che la successione $\{x_h\}_{h\in N}$ è periodica e che, se m è la lunghezza dell'antiperiodo e λ quella del periodo risulta $\mu+\lambda\leq m^k$.

Definizione 4.2. Si dice **successione di numeri pseudocasuali generata** dalla (4.3) la successione di termine generale

$$y_h=x_h/m \tag{4.4}$$

formata da elementi di $P_n(m)$. [1]

Supponendo che λ non sia troppo piccolo (in pratica almeno dell'ordine di 10^8) e trascurando l'antiperiodo, al generatore (4.3) viene associata la variabile casuale X definita in P(m) con probabilità, $\forall x\in P(m)$,

$$f(x)=\frac{n(x)}{\lambda} \tag{4.5}$$

dove con n(x) si indica il numero di volte in cui, in un segmento S della successione di lunghezza λ, situato dopo l'antiperiodo, y_h ha assunto il valore x.

In generale, per ogni $n\geq 1$ e non troppo elevato (in pratica $n\leq 10$), si associa alla (4.3) la variabile casuale $\underline{X}_n$, definita in $P_n(m)$, con probabilità

$$f(\underline{x})=\frac{n(\underline{x})}{\lambda}\ ,\ \forall \underline{x}\in P_n(m)\ , \tag{4.6}$$

---

(1) Ci limitiamo in questo lavoro, per semplicità, al caso in cui la successione di numeri pseudocasuali è data dalla (4.4), anche se vi sono molti altri criteri per ottenere i numeri y_h. Ad es., per m=2, gli x_h sono cifre binarie. Si possono ottenere numeri pseudocasuali "mettendo insieme" gruppi di tali cifre. Si vedano ad esempio i lavori [6], [7].

dove $n(\underline{x})$ è il numero di volte in cui la n-pla $\underline{y}_h=(y_h, y_{h+1}, \dots, y_{h+n-1})$ ha assunto, al variare di y_h in S, il valore $\underline{x}$.

Evidentemente $\underline{X}_n$ ha n componenti tutte somiglianti ad X, per cui valgono per $\underline{X}_n$ tutte le considerazioni svolte nei paragrafi precedenti.

Definizione 4.3. Diciamo **vicinanza di ordine n** della successione $\{y_h\}_{h\in N}$ da una variabile casuale equidistribuita la vicinanza di $\underline{X}_n$ da una variabile casuale equidistribuita in $P_n(m)$.

In maniera analoga definiamo la discrepanza di ordine n di $\{y_h\}_{h\in N}$ da una variabile casuale equidistribuita.

Le misure di discrepanza M_n e S_n tengono conto solo del disturbo arrecato alla uniformità dall'onda con massima lunghezza d'onda e con modulo dell'ampiezza non nullo . Non viene perciò preso in considerazione

a) il disturbo arrecato dalle altre onde;

b) il valore assunto, per ogni $\underline{z}$, da $|h(\underline{z})|$, quando $|h(\underline{z})|\neq 0$.

In [5] ed in questo lavoro si propongono misure di discrepanza $D_{n,r}$ dipendenti da un parametro "principale" $r\in[1,+\infty)$ e da altri parametri k,α tali che $D_{n,r}$

a) tenga conto delle (I), (II) e delle altre osservazioni emerse in [1] e [2];

b) sia applicabile a qualsiasi variabile casuale $\underline{X}$ definita in $P_n(m)$;

c) per valori particolari dei parametri e per le variabili casuali per cui sono applicabili i criteri M_n e S_n, abbia tali numeri come termini di maggior peso, in modo che, più o meno grossolanamente, $D_{n,r}$ possa essere approssimato da essi;

d) sia un valore particolare di una distanza nello spazio $F_n(m)$;

e) per $r\to+\infty$ e per particolari valori di k e α sia $D_{n,r}=M_n$ o $D_{n,r}=S_n$.

A tale scopo si suggerisce di porre

$$(4.7)\quad D_{n,r}=\Big(\sum_{\underline{z}\in J_n(m)-\{\underline{0}\}} p(\underline{z})|h(\underline{z})|^r\Big)^{1/r}$$

con le seguenti ipotesi sul numero $p(\underline{z})$:

(1) $p(\underline{z})=q(|\underline{z}|)$, dove q è una funzione reale di variabile reale;

(2) $q(x)>0$, $\forall x\geq 0$;

(3) q(x) è strettamente decrescente e tende a zero per $x\to+\infty$.

Essendo $|h(\underline{z})|\leq 1$, $\forall \underline{z}\in J_n(m)$, risulta

$$(4.8)\quad D_{n,r}\leq\Big(\sum_{\underline{z}\in J_n(m)-\{\underline{0}\}} p(\underline{z})\Big)^{1/r}.$$

Poichè il numero di elementi di $J_n(m)$ è, nei casi che vengono considerati in pratica, elevatissimo, per poter calcolare senza troppe difficoltà sia un maggiorante dell'insieme dei numeri $D_{n,r}$ al variare di $\underline{X}$ e sia un valore approssimato del numero $D_{n,r}$, può convenire aggiungere l'ipotesi

(4) $p(\underline{z})$ è, per $|\underline{z}| \to +\infty$, un infinitesimo di ordine superiore ad n.

Infatti, se vale la (4), la serie $\sum_{\underline{z}\in Z^n-\{\underline{0}\}} p(\underline{z})$ è convergente e detta A la sua somma, risulta $D_{n,r} \le A^{1/r}$ e, per m e r elevati, la somma parziale della serie, limitata ai termini $\underline{z}\in J_n-\{\underline{0}\}$, è molto vicina ad A.

5. SPAZI METRICI DI DENSITÁ DI PROBABILITÁ

Consideriamo l'insieme $F_n(m)$ delle funzioni definite in $P_n(m)$ ed a valori in C.

Per ogni coppia (g_1, g_2) di elementi di $F_n(m)$ aventi come m - coefficienti di Fourier di indice $\underline{z}\in J_n(m)$ rispettivamente $h_1(\underline{z})$ e $h_2(\underline{z})$, consideriamo il numero.

$$(5.1)\quad D_{n,r}(g_1, g_2)=\left(\sum_{\underline{z}\in J_n} p(\underline{z})|h_1(\underline{z})-h_2(\underline{z})|^r\right)^{1/r}$$

dove i $p(\underline{z})$ sono numeri soddisfacenti (1), (2), (3).

Proposizione 5.1. L'applicazione

$$(5.2)\quad D_{n,r}:(g_1, g_2)\in F_m^2(m)\to D_{n,r}(g_1, g_2)$$

è una metrica in $F_n(m)$ per ogni $r\in[1,+\infty)$.

Dimostrazione. Per le (1), (2), (3), si ha $D_{n,r}(g_1, g_2)=0 \Rightarrow h_1(\underline{z})=h_2(\underline{z})$, $\forall \underline{z}\in J_n$.

Allora, per il teorema 2.2, $D_{n,r}(g_1, g_2)=0 \Rightarrow g_1=g_2$.

La proprietà simmetrica è evidente.

Resta da dimostrare che, se g_1, g_2, g_3 sono tre elementi qualsiasi di $F_n(m)$, rispettivamente con m - coefficienti di Fourier $h_1(\underline{z})$, $h_2(\underline{z})$, $h_3(\underline{z})$, $\forall \underline{z}\in J_n$, allora risulta

$$(5.3)\quad D_{n,r}(g_1, g_2)\le D_{n,r}(g_1, g_3)+D_{n,r}(g_2, g_3).$$

Poniamo $a_i(\underline{z})=(-1)^i\, p(\underline{z})^{1/r}[h_i(\underline{z})-h_3(\underline{z})]$, i=1,2.

Allora la (5.3) si può scrivere

$$\left(\sum_{\underline{z}\in J_n(m)}|a_1(\underline{z})+a_2(\underline{z})|^r\right)^{1/r} \le \left(\sum_{\underline{z}\in J_n(m)}|a_1(\underline{z})|^r\right)^{1/r}+\left(\sum_{\underline{z}\in J_n(m)}|a_2(\underline{z})|^r\right)^{1/r}.$$

Essendo $r\ge 1$ si riduce alla disuguaglianza di Minkowsky (cfr. ad es. [3]).❑

Sia $G_n(m)$ il sottoinsieme di $F_n(m)$ formato dalle densità di probabilità delle variabili casuali definite in $P_n(m)$. Allora dalla proposizione 5.1 seguono le:

Proposizione 5.2. $G_n(m)$ è uno spazio metrico rispetto alla distanza data dalla (5.2).

Proposizione 5.3. Se g è un qualsiasi elemento di $G_n(m)$ con m - coefficiente di Fourier $h(\underline{z})$, $\forall \underline{z} \in J_n$ ed u è la densità di probabilità della variabile casuale equidistribuita in $P_n(m)$, allora la distanza $D_{n,r}(g,u)$ si riduce alla (4.7).

Definizione 5.1. Siano S, T, H tre insiemi non vuoti con $T \subseteq R$ e sia $f_\lambda: S \to T$ una funzione dipendente da un parametro $\lambda \in H$. Diciamo che $\underline{z}_0 \in S$ è un punto di massimo uniforme per f_λ al variare di λ se risulta $f_\lambda(\underline{z}_0) \geq f_\lambda(\underline{z})$, $\forall \underline{z} \in S$ e $\forall \lambda \in H$.

Dalla formula (5.1) si deduce la

Proposizione 5.4. Siano g_1, g_2 elementi di $G_n(m)$ aventi come m - coefficienti di Fourier di indice $\underline{z} \in J_n(m)$ rispettivamente $h_1(\underline{z})$ e $h_2(\underline{z})$ e sia $p(\underline{z})$ una funzione definita in $J_n(m)$ e soddisfacente le (1), (2), (3).

Se la funzione $f_r(\underline{z}) = (p(\underline{z}))^{1/r} |h_1(\underline{z}) - h_2(\underline{z})|$ è dotata di un punto dimassimo uniforme $\underline{z}_0$ al variare di r ed esiste $\lim_{r \to +\infty} D_{n,r}(g_1, g_2)$ allora

$$(5.4) \quad \lim_{r \to +\infty} D_{n,r}(g_1, g_2) = |h_1(\underline{z}_0) - h_2(\underline{z}_0)| \lim_{r \to +\infty} (p(\underline{z}_0))^{1/r} .$$

In particolare, per $g_1 = g$, con m-coefficiente di Fourier $h(\underline{z})$ e per $g_2 = u$, densità di probabilità della variabile casuale equidistribuita in $P_n(m)$, si ha

$$(5.5) \quad \lim_{r \to +\infty} D_{n,r} = |h(\underline{z}_0)| \lim_{r \to +\infty} (p(\underline{z}_0))^{1/r} .$$

Dimostrazione. Poniamo, per ogni $\underline{z} \in J_n(m)$, $f_r(\underline{z}) = p(\underline{z})^{1/r} |h_1(\underline{z}) - h_2(\underline{z})|$, $\forall r \geq 1$.

Se $\underline{z}_0$ è un punto di massimo uniforme per $f_r(\underline{z})$ al variare di r dalla (5.1) segue

$$(5.6) \quad D_{n,r}(g_1, g_2) = f_r(\underline{z}_0) \left[1 + \sum_{\underline{z} \in J_n - \{\underline{z}_0\}} \left(f_r(\underline{z}) / f_r(\underline{z}_0) \right)^r \right]^{1/r} .$$

Poichè $\underline{z}_0$ è un punto di massimo uniforme per $f_r(\underline{z})$ e $r \geq 1$ l'espressione fra parentesi quadre è non inferiore a 1 e limitata al variare di r per cui, per $r \to +\infty$, ha limite 1.

Segue che

$$\lim_{r \to +\infty} D_{n,r}(g_1, g_2) = \lim_{r \to +\infty} f_r(\underline{z}_0) = |h_1(\underline{z}_0) - h_2(\underline{z}_0)| \lim_{r \to +\infty} p(\underline{z}_0)^{1/r} \quad \square$$

Esempio 5.1

In [5] è stato suggerito di porre

$$(5.7) \qquad p(\underline{z}) = (k/|\underline{z}|^{\alpha})^r, \text{ con } \alpha > 0, |\underline{z}| \neq 0, k > 0.$$

Poichè per $|\underline{z}|=1$ si ha $p(\underline{z})=k^r$, per ogni $h>0$, ponendo $p(\underline{0})=(k+h)^r$ si ottiene una funzione $p(\underline{z})$ soddisfacente le (1), (2), (3) del paragrafo 4, e, per $\alpha>n/r$, anche alla (4).

Risulta

$$f_r(\underline{z})=p(\underline{z})^{1/r}|h_1(\underline{z})-h_2(\underline{z})|=\begin{cases}(k+h)\cdot|h_1(\underline{0})-h_2(\underline{0})| & \text{per } \underline{z}=\underline{0}\\ \dfrac{k}{|\underline{z}|^{\alpha}}|h_1(\underline{z})-h_2(\underline{z})| & \text{per } \underline{z}\neq\underline{0}\end{cases}$$

La $f_r(\underline{z})$ è costante al variare di r e quindi le condizioni di esistenza di un massimo uniforme e del $\lim_{r\to+\infty} p(\underline{z})^{1/r}$ sono banalmente soddisfatte.

Osservazione 5.1. Dalla (5.5), per $p(\underline{z})$ definita dalla (5.7), seguono come casi particolari le discrepanze M_n e S_n.

Infatti le (5.5) e (5.7) implicano

$$\lim_{r\to+\infty} D_{n,r} = \max_{\underline{z}\in J_n(m)-\{\underline{0}\}} k|h(\underline{z})|/|\underline{z}|^{\alpha} \quad . \tag{5.8}$$

Se $\underline{z}_0$ è un massimo per $f_r(\underline{z})$ tale che $|h(\underline{z}_0)|=1$ allora

$$\lim_{r\to+\infty} D_{n,r}=\frac{k}{|\underline{z}_0|^{\alpha}} \tag{5.9}$$

e si riduce alla M_n ponendo $k=1$, $\alpha=1$ e alla S_n ponendo

$$k=\left[\frac{m\Gamma\left(\frac{n+2}{2}\right)}{\pi^{n/2}}\right],\quad \alpha=n\,.$$

❑

6. SPAZIO H_n E GIUSTIFICAZIONI DELLE IPOTESI SU $p(\underline{z})$

Consideriamo l'insieme $H_n=\bigcup_{m=1}^{\infty} F_n(m)$

Definizione 6.1. Se $g_1\in F_n(m_1)$ e $g_2\in F_n(m_2)$ sono due elementi di H_n, con m_1-coefficienti e m_2-coefficienti di Fourier rispettivamente $h_1(\underline{z})$ e $h_2(\underline{z})$, diciamo che g_1 è equivalente a g_2 e scriviamo $g_1\sim g_2$ se, $\forall \underline{z}\in Z_n$, $h_1(\underline{z})=h_2(\underline{z})$.

La relazione $\sim$ in H_n gode evidentemente delle proprietà riflessiva, simmetrica e transitiva, per cui è una relazione d'equivalenza. Sia $Q_n=H_n/\sim$ l'insieme quoziente.

Proposizione 6.1. Se $g_1\in F_n(m_1)$ e $g_2\in F_n(m_2)$ sono densità di probabilità di

distribuzioni uniformi rispettivamente in $P_n(m_1)$ ed in $P_n(m_2)$, allora $g_1 \sim g_2$.

Dimostrazione. Immediata conseguenza delle proposizioni 3.1 e 3.2. ❑

Osservazione 6.1. Tenuto conto delle (2.2), se ampliamo l'insieme H_n con l'aggiunzione della densità di probabilità u della distribuzione uniforme continua in $[0,1)^n$ e se consideriamo la relazione $\sim$ in $H_n \cup \{u\}$, si vede immediatamente che u è equivalente alle densità di probabilità considerate nella proposizione 6.1. Si vede, inoltre, che il prolungamento canonico di una qualsiasi di tali densità di probabilità coincide con u.

Indichiamo con $\hat{g}$ la classe di equivalenza di $g \in H_n$. Siano $g_1 \in F_n(m_1)$ e $g_2 \in F_n(m_2)$ elementi di H_n e $h_1(\underline{z})$ e $h_2(\underline{z})$ i rispettivi m_1-coefficienti e m_2-coefficienti di Fourier.

Associamo alla coppia $(\hat{g}_1, \hat{g}_2)$ il numero

$$(6.1) \qquad D_{n,r}(\hat{g}_1, \hat{g}_2) = \left(\sum_{\underline{z} \in Z_n} p(\underline{z}) |h_1(\underline{z}) - h_2(\underline{z})|^r \right)^{1/r}, \qquad r \geq 1$$

L'applicazione

$$D_{n,r} : (\hat{g}_1, \hat{g}_2) \in Q_n^2 \to D_{n,r}(\hat{g}_1, \hat{g}_2)$$

è una distanza in Q_n.

Se $Q_n(m)$ è il sottoinsieme di Q_n formato dalle classi $\hat{g}_1$, con $g_1 \in F_n(m)$, si vede subito che l'applicazione

$$\varphi : g_1 \in F_n(m) \to \hat{g}_1 \in Q_n(m)$$

è un isomorfismo fra spazi metrici.

Lo spazio metrico (Q_n, D_n) si può quindi considerare un prolungamento di ognuno degli spazi metrici $(F_n(m), D_n)$.

Con abuso di linguaggio, se $g_1 \in \hat{g}_1$ e $g_2 \in \hat{g}_2$, chiameremo, in seguito, distanza fra g_1 e g_2 la distanza fra le classi $\hat{g}_1$ e $\hat{g}_2$.

Chiamiamo inoltre **distribuzione uniforme** la classe di equivalenza contenente la densità di probabilità della distribuzione uniforme in $F_n(m)$, per ogni m, e, con abuso di linguaggio, anche ogni elemento di tale classe.

Osservazione 6.2. Notiamo, anche se è ovvio, che l'espressione fra parentesi nella (6.1) ha sempre un numero finito di termini non nulli.

Allo scopo di chiarire aspetti significativi della formula (6.1), che giustificano, almeno da un punto di vista intuitivo, i requisiti richiesti nel paragrafo precedente alla funzione $p(\underline{z})$, presentiamo due tipi di ragionamento che conducono alle medesime conclusioni.

1° ragionamento. Sia $\underline{X}$ una variabile casuale in $P_n(m)$ e sia $\underline{Y}$ una variabile

casuale somigliante ad $\underline{X}$, ma considerata definita in $P_n(rm)$, con r intero maggiore di 1. Siano, inoltre, f_1 e f_2 le funzioni di probabilità, rispettivamente, di $\underline{X}$ e $\underline{Y}$.

Risulta

$$(6.2) \quad f_2(\underline{x}) = \begin{cases} f_1(\underline{x}) & ,\forall \underline{x} \in P_n(m) \\ 0 & ,\forall \underline{x} \in P_n(r\ m) - P_n(m) \ . \end{cases}$$

Detti $h_1(\underline{z})$ e $h_2(\underline{z})$ gli m-coefficienti e rm-coefficienti di Fourier, rispettivamente, di f_1 e f_2, risulta inoltre, per ogni $\underline{z} \in J_n(m)$,

$$(6.3) \quad h_2(\underline{z}) = \sum_{\underline{x} \in P_n(r \cdot m)} e(-\underline{z} \cdot \underline{x}) f_2(\underline{x}) = \sum_{\underline{x} \in P_n(m)} e(-\underline{z} \cdot \underline{x}) f_1(\underline{x}) = h_1(\underline{z}) \ ,$$

e per $\underline{z} \in J_n(rm) - J_n(m)$,

$$(6.4) \quad \begin{cases} h_1(\underline{z}) = 0 \\ h_2(\underline{z}) = \sum_{\underline{x} \in P_n(r \cdot m)} e(-\underline{z} \cdot \underline{x}) f_2(\underline{x}) = \sum_{\underline{x} \in P_n(m)} e(-\underline{z} \cdot \underline{x}) f_1(\underline{x}) \ . \end{cases}$$

Consideriamo per semplicità, il caso in cui $\underline{X}$ sia uniforme. Allora si ha

$$h_1(\underline{z}) = h_2(\underline{z}) = 0 \ , \ \forall \underline{z} \in J_n(m) - \{0\} \ ,$$

mentre, essendo $f_1(\underline{x}) = 1/m^n$, $\forall \underline{x} \in P_n(m)$, dalla proposizione 1.4, posto $\underline{r} = m\underline{x}$, segue che

$$h_2(\underline{z}) = \frac{1}{m^n} \sum_{\underline{r} \in I_n(m)} e(-\underline{z} \cdot \underline{r} / m) = \varepsilon(-\underline{z} / m) \ ,$$

per cui, per $\underline{z} \in J_n(rm) - J_n(m)$,

$$h_2(\underline{z}) = \begin{cases} 1 \text{ se le componenti di } \underline{z} \text{ sono tutte multiple di m} \\ 0 \text{ negli altri casi.} \end{cases}$$

Esaminando gli rm-coefficienti di Fourier della $\underline{Y}$ si vede quindi che compaiono coefficienti $h_2(\underline{z}) \neq 0$, con $\underline{z} \neq \underline{0}$, associati ad onde con numero d'onda $|\underline{z}|$ molto elevato.

Se $m = 10^h$, per un certo h, ed r=10, i valori assunti da $\underline{X}$ sono numeri con h cifre decimali e il passare della variabile casuale $\underline{X}$ alla variabile casuale $\underline{Y}$ equivale alla richiesta della cifra decimale h+1. La comparsa degli $h_2(\underline{z}) \neq 0$ con $|\underline{z}|$ elevato si può allora ritenere collegata alla maggiore richiesta di precisione. Il fatto che questi coefficienti di Fourier siano associati alla cifra decimale meno significativa fa attribuire loro, nella formula alla distanza, un peso molto inferiore a quello dei coefficienti con $|\underline{z}|$ piccolo e ciò rende ragione alle ipotesi assunte sui $p(\underline{z})$.

2° *ragionamento*. Si consideri una distribuzione mista, formata da una massa di probabilità δ situata in un punto $\underline{x}_0 \in P_n(m)$ e dalla rimanente massa $1-\delta$ distribuita uniformemente in $[0, 1)^n$. Approssimando la distribuzione con una variabile casuale $\underline{X}$ in $P_n(m)$, riunendo in $\underline{x} \in P_n(m)$ la massa di probabilità relativa all'intervallino $H(\underline{x})$ semiaperto superiormente di primo estremo $\underline{x}$ e dimensioni tutte uguali a $1/m^n$, la funzione di probabilità di $\underline{X}$ ha, per $\underline{z} \in J_n(m)-\{0\}$, come coefficienti di Fourier i numeri

$$h_2(\underline{z}) = \sum_{\underline{x} \in P_n(m)} e(-\underline{z}\cdot\underline{x})(1-\delta)/m^n + e(-\underline{z}\cdot\underline{x}_0)\delta \ ,$$

ossia per la (1.2)

(6.5) $\quad h_2(\underline{z}) = e(-\underline{z}\cdot\underline{x}_0)\delta \ .$

Se m_1 è un intero maggiore di m tale che $\underline{x}_0 \in P_n(m_1)$, approssimando la distribuzione con una variabile casuale $\underline{Y}$ in $P_n(m_1)$ con criteri di approssimazione analoghi a quelli seguiti per $\underline{X}$, la funzione di probabilità di $\underline{Y}$ ha, per $\underline{z} \in J_n(m_1)-\{\underline{0}\}$, i coefficienti di Fourier

(6.6) $\quad h_2(\underline{z}) = e(-\underline{z}\cdot\underline{x}_0)\delta \ .$

Nel passaggio dalla variabile casuale $\underline{X}$ alla variabile casuale $\underline{Y}$, assieme alla maggiore richiesta di precisione si è avuto, come nel primo ragionamento, la comparsa di altri coefficienti di Fourier non nulli con $|\underline{z}|$ elevato. Appare ragionevole quindi concludere, come nel ragionamento precedente, che tali coefficienti devono avere poco peso nella formula della distanza in quanto collegati alle cifre meno significative dei valori assunti dalla variabile casuale in esame.

BIBLIOGRAFIA

[1] *R.R.Coveyou, R.D.Macpherson*: Fourier Analysis of uniform random number generators. Journal of Association for Computing Machinery 14, 1967.

[2] *D.E.Knuth*: The art of computer programming, seminumerical algorithms. Addison Wesley. London, 1981.

[3] *A.N.Kolmogorov, S.V.Fomin*: Elementi della teoria delle funzioni e dell'analisi funzionale. Edizioni Mir, Mosca, 1980.

[4] *A.Maturo, N.Cera*: Confronto tra alcuni generatori di numeri pseudocasuali. Periodico di Matematiche 2, 1991, p. 38-64.

[5] *A. Maturo*: Sull'analisi di Fourier di successioni di numeri pseudocasuali, Atti SPRCI '89, P 188/198.

[6] *A.Rizzi*: Generazione di distribuzioni statistiche mediante un elaboratore elettronico. Ist. di Statistica G. Gini, Roma, 1977.

[7] *A.Rizzi*: Generazione di simboli binari pseudocasuali mediante polinomi primitivi. Statistica, 2, 1982.