

Numero 3 - 1992

# RATIO MATHEMATICA

Rivista di  
Matematica Applicata all'Economia e all'Ingegneria

a cura di

**Franco Eugeni e Mario Gionfriddo**

## Comitato Scientifico

Ilio Adorisio, *Roma*

Albrecht Beutelspacher, *Giessen*

Franco Eugeni, *L'Aquila*

Mario Gionfriddo, *Catania*

Giovanni Melzi, *Milano*

Bruno Rizzi, *Roma*

Aniello Russo Spena, *L'Aquila*

Romano Scozzafava, *Roma*

## Indice del fascicolo

|                                                                                                                                                 |         |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Non linear evolutive models for a stock-market with variable fundamental values and asymmetry of information<br>(M. Cenci, A.M. Cerquetti)..... | pag. 1  |
| Criteri di programmazione delle ispezioni sulle costruzioni esistenti e di interpretazione dei risultati sperimentali<br>(M. Ciampoli) .....    | pag. 15 |
| Checking the randomness of pseudorandom sequences from a bayesian viewpoint<br>(G. Di Biase, A. Maturo) .....                                   | pag. 35 |
| On stationary modes of nonlinear dielectric slab structures: a new mathematical approach<br>(R. Lupini, M.G. Messia) .....                      | pag. 49 |
| Su alcune caratterizzazioni delle successioni di numeri pseudocasuali ottenute a partire da algebre di supporto<br>(A. Maturo) .....            | pag. 57 |
| Interpretazione economica dei predicati di canale in un sistema digitale multicanale<br>(F. Mercanti) .....                                     | pag. 81 |
| Alcune osservazioni sulla valutazione della capacità d'una funzione d'utilità<br>(L. Peccati) .....                                             | pag. 85 |
| Considerazioni sul test z per gli indici di Moran<br>(G. Visini) .....                                                                          | pag. 95 |

# **NON LINEAR EVOLUTIVE MODELS FOR A STOCK-MARKET WITH VARIABLE FUNDAMENTAL VALUES AND ASYMMETRY OF INFORMATION<sup>1</sup>**

**Marisa Cenci - Anna Maria Cerquetti**  
University "G. D'Annunzio" - Pescara

## **1. INTRODUZIONE**

There has recently been an increased interest of the economic as well as financial literature in the laws governing the functioning of stock-markets.

The actual performance of stock-markets has pointed to the fact that many of the existing theoretical models, which are typically based on efficiency and other idealistic hypotheses, are unsatisfactory when confronted with empirical reality. This is particularly true for thin markets and in the presence of information asymmetries.

Lately, several authors [8], [9], [14], [15], [6], [7], [4] have advanced an alternative approach dealing with simplified situations and suggesting models for a market with asymmetries of information and "irrationality".

They have studied a market where just one type of financial asset is traded and where the agents involved, although all being "fundamentalists", may be heterogeneous due to differences in information, possibilities of intervention and objectives.

In this paper the models advanced in [4] are generalized in that we abandon some of their linearity assumptions, and we investigate equilibrium and its stability.

---

<sup>1</sup>Work carried out within the Research Project MURST 40% entitled "Models of financial markets microstructure" - National coordinator L. Peccati.

In this case the systems describing the market evolution consist of quadratic nonlinear difference equations.

Moreover the assumptions made on the behavioural functions are very general, such as monotonicity and the passage through (0,0). The conclusions reached about the solutions of equilibrium and their stability are, accordingly, valid for a large class of evolutive models.

In order to explain our presentation, we give the basic hypotheses and the notations used in § 2. In § 3, we study the market equilibrium and its stability within a given session.

In § 4, we suggest a model for the market evolution from one session to the other, and we investigate the equilibrium and the conditions for its stability. In § 5, we examine the consequences of the imitative behaviour on the suggested models.

## 2. BASIC HYPOTHESES AND NOTATIONS

A detailed analysis of the laws governing a market where not all the brokers can negotiate in real time can be carried out only by suggesting two different evolutive models: one which deals with the behaviour of agents within a session, and another one which treats the behaviour from one session to the next.

We denote with  $T=1, \dots, n$  the index of each session and  $t_n(T)$ ,  $n \in \mathbb{N}$ , the sequence of the calls in the  $T$ -th session.

Moreover we assume that agents can be partitioned into three classes. Each class includes agents who are homogeneous both for information received and for their possibilities of intervention in the market.

Non professional brokers (NP) constitute the first class. They can give irrevocable orders only at the beginning of each session; these orders are based on information from previous sessions. NPs have no direct access to negotiations.

Professional agents (P) form the second class and pass on the orders received from NPs. Since they receive informations regarding the ongoing session, they can negotiate on their own behalf when they think it convenient.

The last class of agents is made up by specialists (S); they can get confidential informations and can price stocks on the basis of their fundamental values, as well as on the basis of the market trend. Since all agents within one class are homogeneous, it is not too restrictive to assume that each class consists of one representative agent only.

Our notations will be the following:

- $Q(T)$  the orders given by NPs in the  $T$ -th session
- $B(T)$  the orders given by the Ps in the  $T$ -th session
- $r(T)$  the fundamental value given to a stock by the NP at time  $T$
- $h(T)$  the fundamental value given to a stock by the P agent in the  $T$ -th session

- $k(T)$  the fundamental value given to a stock by S at time T
- $P(T)$  the price of a stock at the end of the T-th session.

The symbols  $h_n(T)$ ,  $k_n(T)$  e  $P_n(T)$  stand for the values reached by the corresponding quantities at the n-th call in the T-th session;  $B_n(T)$  indicates the orders given by the P agent up to the n-th call in the T-th session.

Assuming that the length of each session is constant and equal to D, we get the following relations

$$\lim_{n \rightarrow \infty} t_n = D, \quad \lim_{n \rightarrow \infty} B_n(T) = B(T), \quad \lim_{n \rightarrow \infty} h_n(T) = h(T),$$

$$\lim_{n \rightarrow \infty} k_n(T) = k_n, \quad \lim_{n \rightarrow \infty} P_n(T) = P(T).$$

### 3. MARKET EVOLUTION WITHIN A SESSION

The agents negotiating directly within a session are called P and S. P gives orders according to being a fundamentalist; his transactions at the n-th call can thus be described by

$$B_n(T) - B_{n-1}(T) = -\beta[P_{n-1}(T) - h_n(T)] \quad (3.1)$$

where  $\beta(\bullet)$  is a strictly increasing function, with  $\beta(0)=0$ .

Contrary to what been assumed in [8], [9], [14], [15], [6], [7], we suppose here that the fundamental value given by P be variable within a session, according to

$$h_n(T) = h_{n-1}(T) + \delta[B_{n-1}(T) - B_{n-2}(T)] \quad (3.2)$$

where  $\delta(\bullet)$  is a strictly increasing function, with  $\delta(0)=0$ .

Such a hypothesis allows P to change his mind according to the stock exchange trend within the session. The relationship connecting the stock price fixed by the S at the n-th call with the stock fundamental value and the market trend is

$$P_n(T) = k_n(T) + \eta[Q(T) + B_n(T)] \quad (3.3)$$

where  $\eta(\bullet)$  is a strictly increasing function, with  $\eta(0)=0$ .

Moreover we assume that the fundamental value fixed by the S may change in a session because of factors outside the market, such as confidential information regarding the stock at issue. This value can be expressed by means of

$$k_n(T) = f[k_{n-1}(T)] \quad (3.4)$$

where  $f(\bullet)$  is a nonnegative function.

Delating the dependence on  $T$  when not essential, the system governing the market trend in the  $T$ -th session in the following

$$\begin{cases} B_n = B_{n-1} - \beta[P_{n-1} - h_n] \\ P_n = k_n + \eta[Q(T) + B_n] \\ h_n = h_{n-1} + \delta(B_{n-1} - B_{n-2}) \\ k_n = f(k_{n-1}) \end{cases} \quad (3.5)$$

The initial values for the beginning of the session are

$$B_0(T) = 0, \quad h_0(T) = h_0, \quad P_0(T) = k_0 + \eta[Q(T)]$$

where  $h_0$  e  $k_0$  are known.

### 3.1

We define the system to be in equilibrium if  $B^*$ ,  $h^*$ ,  $k^*$ ,  $P^*$  are solutions of

$$\begin{cases} -\beta[P^* - h^*] = 0 \\ P^* = k^* + \eta[Q(T) + B^*] \\ k^* = f(k^*) \end{cases} \quad (3.6)$$

If  $f(\bullet)$  fulfils the Lipschitz condition with the constant  $L \in (0,1)$  there is one solution only for (3.6) given by:

$$\begin{aligned} B^* &= \eta^{-1}[P^* - k^*] - Q(T) \\ h^* &= P^* \\ k^* &= f(k^*) \end{aligned}$$

From the (3.5), we obtain

$$\begin{cases} B_n = B_{n-1} - \beta[P_{n-1} - h_{n-1} + \delta(B_{n-1} - Z_{n-1})] \\ h_n = h_{n-1} - \delta(B_{n-1} - Z_{n-1}) \\ P_n = k_n + \eta[Q(T) + B_{n-1} - \beta[P_{n-1} - h_{n-1} + \delta(B_{n-1} - Z_{n-1})]] \\ k_n = f(k_{n-1}) \\ Z_n = B_{n-1} \end{cases} \quad (3.7)$$

Using vector notation allows to write the system as follows

$$y_n = G(y_{n-1}) \quad (3.8)$$

where

$$y_n = \begin{pmatrix} B_n \\ h_n \\ P_n \\ k_n \\ Z_n \end{pmatrix} \text{ and } G: \mathfrak{R}^5 \rightarrow \mathfrak{R}^5.$$

At this point local stability of the equilibrium in  $(y^*) = (B^*, h^*, P^*, K^*, Z^*)$  can be asserted if the linear approximation of  $G$  in  $y^*$  is globally stable [13].

If we call  $A$  the Jacobian matrix of  $G$  evaluated at  $y^*$  we get

$$A = \begin{bmatrix} 1 - \beta' \delta' & \beta' & -\beta' & 0 & +\beta' \delta' \\ -\delta' & 1 & 0 & 0 & +\delta' \\ \eta'(\bullet)(1 - \beta' \delta') & \eta'(\bullet)\beta' & -\eta'(\bullet)\beta' & f'(k^*) & \eta'(\bullet)\beta' \delta' \\ 0 & 0 & 0 & f'(k^*) & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (3.9)$$

where we have assumed  $\eta'(\bullet) = \eta'(Q(T) + B^*)$ ,  $\beta' = \beta'(0)$  and  $\delta' = \delta'(0)$  for the sake of brevity.

The eigenvalues of  $A$  are

$$\lambda = 0 \text{ with multiplicity two}$$

$$\lambda = f'(k^*)$$

$$\lambda = 1$$

$$\lambda = 1 + \beta'(0)[- \delta'(0) - \eta'(Q(T) + B^*)].$$

Considered that the necessary and sufficient condition for stability, namely  $|\lambda| < 1$ , is not verified, we can conclude that the equilibrium found is not locally stable. It is known, however, that, since  $\lambda = 1$  is the simple root of the characteristic equation of  $A$ , in case that

$$|f'(k^*)| < 1 \text{ and } \beta'(0) [\delta'(0) + \eta'(Q(T) + B^*)] < 2 \quad (3.10)$$

the linear approximation of  $G$  is stable at  $y^*$  in the sense of Ljapunov. For this reason, if the equilibrium found satisfied (3.10), it will be locally stable in the sense of Ljapunov.

#### 4. MARKET EVOLUTION FROM ONE SESSION TO THE OTHER

The dynamic evolution of the market from one session to the other results from the equations governing the behaviour of each representative agent.

The NP agent behaves as a fundamentalist and in the  $T$ -th session he will negotiate a quantity of stocks equal to

$$Q(T) = -\alpha[P(T-1)-r(T)] \quad (4.1)$$

where  $\alpha(\bullet)$  is a strictly increasing function, with  $\alpha(0)=0$ . The transactions within the same session of agent  $P$  are given by

$$B(T) = -\beta[P(T-1)-h(T)]-Q(T) \quad (4.2)$$

where  $\beta(\bullet)$  is a strictly increasing function passing through  $(0,0)$ .

Note that the two terms in the second member of (4.2) indicate, respectively, the orders carried out autonomously and the orders carried out on the NP's behalf.

In addition we assume that the NP's and  $P$ 's fundamental values can vary according to the outcomes regarding the market trend in the last two sessions.

As a consequence we obtain the following relations

$$r(T) = (1-\omega)r(T-1)+\omega P(T-1)+\gamma[\Delta P(T-1)] \quad (4.3)$$

$$h(T) = h(T-1)-\Omega[Q(T-1)+B(T-1)]-\phi[\Delta Q(T-1)+\Delta B(T-1)] \quad (4.4)$$

where

$$\begin{aligned} \Delta P(T-1) &= P(T-1)-P(T-2) \\ \Delta Q(T-1) &= Q(T-1)-Q(T-2) \\ \Delta B(T-1) &= B(T-1)-B(T-2) \end{aligned}$$

and where  $\gamma(\bullet)$ ,  $\Omega(\bullet)$  and  $\phi(\bullet)$  are strictly increasing functions passing through  $(0,0)$  and  $\omega \in (0,1)$  is a parameter.

Analogously to what we have learned from the analysis regarding a single session, also in the present case the specialist's price and fundamental value

vary according to

$$P(T) = k(T) + \eta[Q(T) + B(T)] \quad (4.5)$$

$$k(T) = f[k(T-1)] \quad (4.6)$$

where  $\eta(\bullet)$  is again a strictly increasing function, with  $\eta(0)=0$  and  $f(\bullet)$  is a nonnegative function.

The market evolution from one session to the other is therefore governed by the following system

$$\begin{cases} Q(T) = -\alpha[P(T-1) - r(T)] \\ B(T) = -\beta[P(T-1) - h(T)] - Q(T) \\ P(T) = k(T) + \eta[Q(T) + B(T)] \\ r(T) = (1-\omega)r(T-1) + \omega P(T-1) + \gamma(\Delta P) \\ h(T) = h(T-1) - \Omega[Q(T-1) + B(T-1)] - \varphi(\Delta Q + \Delta B) \\ k(T) = f[k(T-1)] \end{cases} \quad (4.7)$$

#### 4.1

A market is said to be in equilibrium if the values  $Q^*$ ,  $B^*$ ,  $P^*$ ,  $r^*$ ,  $h^*$ ,  $k^*$  are solutions of

$$\begin{cases} Q^* = -\alpha(P^* - r^*) \\ B^* = -\beta(P^* - h^*) - Q^* \\ P^* = k^* + \eta(Q^* + B^*) \\ r^* = (1-\omega)r^* + \omega P^* \\ h^* = h^* - \Omega[Q^* + B^*] \\ k^* = f(k^*) \end{cases} \quad (4.8)$$

If  $f(\bullet)$  is Lipschitzian with constant  $L \in (0,1)$ , equilibrium is unique and given by

$$P^* = k^* = h^* = r^* \quad B^* = Q^* = 0 \quad (4.9)$$

Therefore, the long run equilibrium is characterized by common views of the three agents, regarding the fundamental value, by its coincidence with the

price, and by the absence of transactions.

Introducing auxiliary variables

$$\begin{aligned} z(T) &= P(T-1) \\ w(T) &= B(T-1) \\ v(T) &= Q(T-1) \end{aligned}$$

the sistem (4.7) can be written equivalently as

$$X(T) = G(X(T-1)) \quad (4.10)$$

where  $(X(T))' = (Q(T), B(T), P(T), r(T), h(T), k(T), z(T), w(T), v(T))$  and  $G: \mathfrak{R}^9 \rightarrow \mathfrak{R}^9$  and where the apex indicates the transposition operation.

Also in this case the local stability of the equilibrium given by (4.5) is guaranteed by the stability of the linear approximation of  $G$  at  $(X^*)' = 0, 0, k^*, k^*, k^*, k^*, 0, 0, 0$ .

If we call  $B$  the Jacobian matrix of  $G$  evaluated at  $X^*$ , we get:

$$B = \begin{bmatrix} 0 & 0 & -\alpha(1-\omega-\gamma') & \alpha'(1-\omega) & 0 & 0 & -\alpha'\gamma' & 0 \\ -\beta'(\Omega'+\varphi') & -\beta'(\Omega'+\varphi') & \alpha'(1-\omega-\gamma')-\beta' & -\alpha'(1-\omega) & \beta' & 0 & \alpha'\gamma' & \beta'\varphi' \\ -\beta'\eta'(\Omega'+\varphi') & -\beta'\eta'(\Omega'+\varphi') & -\eta'\beta' & 0 & \eta'\beta' & f'(k^*) & 0 & \eta'\beta'\varphi' \\ 0 & 0 & \gamma'+\omega & 1-\omega & 0 & 0 & -\gamma' & 0 \\ -(\Omega'+\varphi') & -(\Omega'+\varphi') & 0 & 0 & 1 & 0 & 0 & \varphi' \\ 0 & 0 & 0 & 0 & 0 & f'(k^*) & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (4.11)$$

where, for the sake of brevity, we have written  $\beta' = \beta'(0)$ ,  $\Omega' = \Omega'(0)$ ,  $\varphi' = \varphi'(0)$ ,  $\gamma' = \gamma'(0)$ ,  $\alpha' = \alpha'(0)$ .

The eigenvalues of B are real equal to

$\lambda = 0$  with multiplicity five

$\lambda = f'(k^*)$

$\lambda = 1 - \omega$

$\lambda = [1 - \beta'(0)[\eta'(0) + \Omega'(0) + \varphi'(0)] \pm$

$\pm \sqrt{\{1 - \beta'(0)[\eta'(0) + \Omega'(0) + \varphi'(0)]\}^2 + 4\beta'(0)(\eta'(0) + \varphi'(0))} / 2$

If the conditions

$$|f'(k^*)| < 1, \quad 0 < \omega < 2, \quad \beta'(0)[\Omega'(0) + 2\varphi'(0) + 2\eta'(0)] < 2 \quad (4.12)$$

are satisfied, (4.9) gives a locally stable equilibrium solution.

The first two relations in (4.12) are verified because of the hypotheses on  $\omega$  and  $f(\bullet)$ . The third relation allows the following interpretation: in order to get a locally stable equilibrium, the P agent's behaviour must not be random; rather, if he pays great attention to small variations in the market's performance, he must intervene with autonomous, but not too large, transactions.

## 5. IMITATIVE BEHAVIOUR

The fact that we have assumed that agents are subject to asymmetric information justifies "irrational" behaviour in the sense that the less informed agents try to imitative those better informed.

We will consider here specifically two types of imitative behaviours:

- i) imitation of P agents by NP agents
- ii) imitation of P by NP agents, and imitation of NP agents among each other.

### 5.1

The first type of imitation still allows to identify the three classes of agents (NP, P, S) by means of a single representative agent.

The NP agent's transactions are influenced by P's behaviours in the previous session; therefore

$$Q(T) = -\alpha[P(T-1) - r(T)] + \mu[B(T-1)] \quad (5.1)$$

price, and by the absence of transactions.

Introducing auxiliary variables

$$\begin{aligned} z(T) &= P(T-1) \\ w(T) &= B(T-1) \\ v(T) &= Q(T-1) \end{aligned}$$

the sistem (4.7) can be written equivalently as

$$X(T) = G(X(T-1)) \quad (4.10)$$

where  $(X(T))' = (Q(T), B(T), P(T), r(T), h(T), k(T), z(T), w(T), v(T))$  and  $G: \mathfrak{R}^9 \rightarrow \mathfrak{R}^9$  and where the apex indicates the transposition operation.

Also in this case the local stability of the equilibrium given by (4.5) is guaranteed by the stability of the linear approximation of  $G$  at  $(X^*)' = 0, 0, k^*, k^*, k^*, k^*, 0, 0, 0$ .

If we call  $B$  the Jacobian matrix of  $G$  evaluated at  $X^*$ , we get:

$$B = \begin{bmatrix} 0 & 0 & -\alpha(1-\omega-\gamma') & \alpha'(1-\omega) & 0 & 0 & -\alpha'\gamma' & 0 \\ -\beta'(\Omega'+\varphi') & -\beta'(\Omega'+\varphi') & \alpha'(1-\omega-\gamma')-\beta' & -\alpha'(1-\omega) & \beta' & 0 & \alpha'\gamma' & \beta'\varphi' \\ -\beta'\eta'(\Omega'+\varphi') & -\beta'\eta'(\Omega'+\varphi') & -\eta'\beta' & 0 & \eta'\beta' & f'(k^*) & 0 & \eta'\beta'\varphi' \\ 0 & 0 & \gamma'+\omega & 1-\omega & 0 & 0 & -\gamma' & 0 \\ -(\Omega'+\varphi') & -(\Omega'+\varphi') & 0 & 0 & 1 & 0 & 0 & \varphi' \\ 0 & 0 & 0 & 0 & 0 & f'(k^*) & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (4.11)$$

- $E = [e_{ij}]$  the matrix of the imitation coefficients among NP agents
- $\bar{\alpha}$  the diagonal matrix having the functions  $\alpha_i(\bullet)$  as elements
- $\bar{\omega}$  the diagonal matrix having the parameters  $\omega_i(\bullet)$  as elements

Under the above assumptions the quantity traded by the  $i$ -th NP agent is

$$q_i(T) = -\alpha_i[P(T-1) - r_i(T)] + \mu_i[B(T-1)] + \sum_j e_{ij} q_j(T-1). \quad (5.2)$$

If we indicate with  $\mathbf{1}$  the column vector all of whose  $m$  components are one and with  $\mathbf{I}$  the identity matrix  $m \times m$ , the system governing the market evolution can be written as follows

$$\begin{cases} \underline{q}(T) = -\bar{\alpha}[\mathbf{1}P(T-1) - \underline{r}(T)] + \underline{\mu}[B(T-1)] + E\underline{q}(T-1) \\ B(T) = -\beta[P(T-1) - h(T)] - \mathbf{1}'\underline{q}(T) \\ P(T) = k(T) + \eta[B(T) + \mathbf{1}'\underline{q}(T)] \\ \underline{r}(T) = (\mathbf{I} - \bar{\omega})\underline{r}(T-1) + \bar{\omega}\mathbf{1}P(T-1) + \gamma(\mathbf{1}\Delta P) \\ h(T) = h(T-1) - \Omega[\mathbf{1}'\underline{q}(T-1) + B(T-1)] - \phi[\mathbf{1}'\Delta\underline{q} + \Delta B] \\ k(T) = f[k(T-1)] \end{cases} \quad (5.3)$$

The market is said to be in equilibrium  $\underline{q}^*, B^*, \underline{r}^*, h^*, P^*, k^*$  if these values satisfy the system

$$\begin{cases} \underline{q}^* = -\bar{\alpha}[\mathbf{1}P^* - \underline{r}^*] + \underline{\mu}B^* + E\underline{q}^* \\ B^* = -\beta[P^* - h^*] - \mathbf{1}'\underline{q}^* \\ P^* = k^* + \eta[B^* + \mathbf{1}'\underline{q}^*] \\ \underline{r}^* = (\mathbf{I} - \bar{\omega})\underline{r}^* + \bar{\omega}\mathbf{1}P^* \\ 0 = -\Omega[\mathbf{1}'\underline{q}^* + B^*] \\ k^* = f(k^*) \end{cases} \quad (5.4)$$

If  $f(\bullet)$  is a contraction, we get through simple manipulations from system (5.4) the following relations

$$h^* = P^* = k^*, \quad \underline{r}^* = \mathbf{1} \cdot P^*, \quad B^* = -\mathbf{1}'\underline{q}^*, \quad \underline{q}^*(\mathbf{I} - E) = \underline{\mu}(B^*). \quad (5.5)$$

If it is assumed that the matrix  $(I-E)$  admits its inverse, the last relation of (5.5) gives

$$q^* = (I-E)^{-1} \mu(B^*). \quad (5.6)$$

Substituting (5.6) for the last equation in (5.5) we obtain

$$B^* + 1'(I-E)^{-1} \mu(B^*) = 0. \quad (5.7)$$

This last relation allows to say that the solution

$$B^* = 0 \quad 1'q^* = 0 \quad r^* = 1p^* = 1h^* = 1k^*$$

is the equilibrium solution, although nothing can be said as to its uniqueness and stability.

In fact for particular imitation structures with appropriate functions  $\mu_i(\cdot)$  we can get

$$B^* = -1'(I-E)^{-1} \mu(B^*) \quad (5.8)$$

with  $B^* \neq 0$ .

In case that (5.7) gives  $B^* = 0$  as the only solution, the results obtained as to the equilibrium are not different from the results obtained without imitation.

## 6. CONCLUSION

This paper points out how models, built on very general assumptions regarding the equations governing stock-market performance, can contribute to the understanding and explanation of instability in these markets. This is in particular the case in markets where asymmetry of information generates incontrollable imitative behaviour and where insider information is used for speculative purposes.

We can finally observe that, although the market's performance is conditional on the professional agents' behaviour, it is not that behaviour as such that we were mainly interested in; rather it is its influence on the decisions of the other types of agents.

## REFERENCES

1. V.I. ARNOLD (1979): *"Equazioni differenziali ordinarie"*, Edizioni MIR.
2. S. BARNETT (1983): *"Polynomials and Linear Control Systems"*, Marcel

Dekker, New York

3. E. CASTAGNOLI - L. PECCATI (1979): "*Metodi matematici per l'analisi economica*", ETAS.
4. M. CENCI, A.M. CERQUETTI (1991): "*Modelli evolutivi per un mercato azionario con valori fondamentali variabili nel tempo e asimmetria d'informazione*". Atti del XV CONVEGNO AMASES - Grado (TS).
5. R.M. CONROY, R.L. WINKLER (1986): "*Market Structure: The Specialist as Dealer and Broker*", Journal of Banking and Finance, 10.
6. A. CORNAGLIA (1990): "*A Non linear Model of Stock-Market Behaviour with Imitation*", in corso di stampa.
7. A. CORNAGLIA (1990): "*A Non linear Model of Stock-Market with Institutionally Different Agents and Imitation*", 8<sup>a</sup> Meeting of the Euro Working Group on Financial Modelling, Gieten.
8. L. FERRARI - L. PECCATI (1989): "*Stock-Market Behaviour and Imitation: a Simple Model*", 6<sup>a</sup> Meeting of the Euro Working Group on Financial Modelling, Lieges.
9. L. FERRARI - E. LUCIANO - L. PECCATI (1990): "*Institutionally Different Agents in an Imitative Stock-Market with Asymmetric Information*", 8<sup>a</sup> Meeting of the Euro Working Group on Financial Modelling, Gieten.
10. R. FLAVELL (1989): "*A Model of a Trader*", 6<sup>a</sup> Meeting of the Euro Working Group on Financial Modelling, Liéges.
11. M. B. GARMAN (1976): "*Market Microstructure*" Journal of Financial Economics, 3.
12. T. HO, H.R. STOLL (1980): "*On Dealer Markets under Competition*", Journal of Finance, 35.
13. V. LAKSHMIKANTHAM, D. TRIGIANTE (1988): "*Theory of Difference Equations: Numerical Methods and Application*" Academic Press. New York.
14. E. LUCIANO (1989): "*Equilibrium in a Financial Market with Asymmetric Information, Imitation and Noise*", 6<sup>a</sup> Meeting of the Euro Working Group on Financial Modelling, Liéges.
15. E. LUCIANO (1990): "*Market Making with Irrationalities: The Case of a Specialist Financial Market with Heterogeneous Traders*", 8<sup>a</sup> Meeting of the Euro Working Group on Financial Modelling, Gieten.
16. N.L. STOKEY, R.L. LUCAS (1989): "*Recursive Methods in Economic Dynamics*", Harvard University Press.

## **CRITERI DI PROGRAMMAZIONE DELLE ISPEZIONI SULLE COSTRUZIONI ESISTENTI E DI INTERPRETAZIONE DEI RISULTATI SPERIMENTALI**

**ing. Marcello Ciampoli(\*)**

**SOMMARIO:** L'affidabilità di una costruzione può essere controllata ed a limite incrementata predisponendo un programma di manutenzione, consistente in ispezioni e riparazioni o sostituzioni. Poiché lo svolgimento di tale programma comporta un onere economico spesso rilevante, l'obiettivo della sua pianificazione deve essere quello di specificare una strategia di ispezione e riparazione che risulti ottimale ai fini della minimizzazione dei costi associati all'esercizio della costruzione. Nell'articolo sono trattati alcuni aspetti di questa problematica, con l'intento di fornire un contributo allo sviluppo di una metodologia integrata, di tipo probabilistico e statistico, che permetta di programmare fin dall'inizio le ispezioni sulle costruzioni, alla luce dei possibili interventi su di esse, ed al tempo stesso si avvalga di tecniche efficienti per interpretare i risultati delle indagini eseguite. In merito a questo secondo aspetto, sono affrontati alcuni problemi specifici che intervengono nella valutazione della sicurezza delle costruzioni esistenti, ed in particolare nella caratterizzazione del livello di incertezza e di aleatorietà associato alle variabili di base. Tra essi: la scelta delle distribuzioni di probabilità più idonee; la determinazione dei frattili inferiori delle resistenze dei materiali sulla base di un numero limitato di risultati sperimentali; la definizione della legge di distribuzione di una grandezza derivata, misurata attraverso prove sperimentali ed espressa analiticamente in funzione di più variabili di base. Tali operazioni rappresentano infatti il presupposto essenziale per l'applicazione corretta delle tecniche di analisi probabilistica della sicurezza strutturale.

(\*) Dipartimento di Ingegneria Strutturale e Geotecnica - Università di Roma  
'La Sapienza'

## INTRODUZIONE

Il livello di sicurezza di una costruzione non viene giudicato solo in fase di progetto, ma anche in diverse occasioni che si presentano durante l'esecuzione o l'esercizio: ad esempio, a seguito di ispezioni, sia periodiche che rese necessarie dalla presenza di dissesti, all'atto della progettazione di interventi di riparazione o adeguamento e nel caso di una variazione della destinazione d'uso.

In tali circostanze, la situazione attuale della costruzione può risultare sensibilmente diversa da quella ipotizzata all'atto del progetto; e ciò anche sotto l'aspetto della definizione dei requisiti prestazionali, dei parametri di giudizio e dei criteri di accettazione o rifiuto.

Infatti, le conseguenze economiche della scelta di livelli di sicurezza ottimali, a cui fare riferimento nella verifica dell'affidabilità strutturale, sono completamente differenti nei due casi di costruzione ancora da realizzare o già realizzata, perché, mentre nella fase iniziale di progetto è possibile apportare le necessarie variazioni in modo relativamente agevole, incrementare la resistenza di una costruzione esistente può risultare, se pure tecnicamente possibile, molto oneroso e quindi antieconomico.

Per una costruzione già esistente, tuttavia, sono disponibili (o possono essere resi tali) molti più dati rispetto alla fase di progetto: dati relativi alle caratteristiche dei materiali, alle dimensioni ed allo stato di degrado degli elementi strutturali ed alla storia di carico effettiva.

L'interpretazione di tali informazioni non è però del tutto semplice, soprattutto se esse derivano da fonti diverse o conducono a risultati contrastanti: al di là della possibilità di trarre alcune indicazioni di natura qualitativa, il processo di interpretazione deve essere quindi fondato sull'impiego consapevole di tecniche di elaborazione statistica che tengano conto della effettiva consistenza e della significatività del campione.

Queste brevi considerazioni pongono in evidenza alcuni dei complessi e delicati problemi che sorgono nella valutazione della sicurezza di una costruzione esistente e nella programmazione degli interventi su di essa.

Nel presente lavoro sono trattati diversi aspetti di questa tematica, con l'intento di fornire un contributo allo sviluppo di una metodologia integrata, di tipo probabilistico e statistico, che permetta di programmare fin dall'inizio le ispezioni sulle costruzioni, alla luce dei possibili interventi su di esse, ed al tempo stesso si avvalga di tecniche efficienti per interpretare correttamente i risultati delle indagini eseguite; metodologia che dovrebbe rappresentare lo strumento per una progettazione unitaria, che a partire dalla concezione dell'opera ne segua l'evoluzione per tutta la durata della vita utile, definendo

una sorta di manuale per l'uso, relativo all'analisi del degrado ed alla manutenzione.

È appena il caso di rilevare che la teoria che permette di elaborare una stima consistente della sicurezza strutturale in funzione del livello di conoscenza effettivo dello stato della costruzione (di volta in volta aggiornato attraverso le informazioni addizionali derivanti ad esempio da indagini in sito) è basata sull'applicazione dei principi dell'inferenza bayesiana, accoppiati alle tecniche di valutazione probabilistica dell'affidabilità, come già illustrato in diversi lavori [1], [2],[3],[4],[5].

A tali tecniche non si farà esplicitamente cenno nel seguito, se non in qualche caso, anche se risulterà evidente come il loro impiego sia indispensabile per la programmazione delle ispezioni, e come i metodi di elaborazione statistica dei risultati sperimentali forniscano il necessario supporto ad una corretta applicazione di esse.

## **PROGRAMMAZIONE DELLE ISPEZIONI SULLE COSTRUZIONI**

L'affidabilità di un sistema strutturale può essere controllata e, se necessario, incrementata con un programma di manutenzione consistente in ispezioni periodiche e riparazioni o sostituzioni.

Tale programma è evidentemente costoso: l'obiettivo della sua pianificazione deve essere pertanto quello di specificare una strategia di ispezione e riparazione che risulti ottimale ai fini della minimizzazione dei costi associati all'esercizio della costruzione.

Un programma di ispezioni è definito attraverso:

- la probabilità di ottenere successi, ovvero di ricavare informazioni significative, con un particolare tipo di ispezione;
- il numero e l'intervallo di tempo tra le ispezioni;
- la qualità del componente dopo l'eventuale riparazione.

L'obiettivo fondamentale di un'ispezione è infatti quello di analizzare le condizioni della costruzione sotto un certo numero di aspetti significativi, in modo che, elaborando i risultati ottenuti, sia possibile: aggiornare il livello di conoscenza dello stato attuale della costruzione e quindi dell'evoluzione subita dai fenomeni di degrado; fornire un supporto alle decisioni in merito alla conservazione, alla riparazione, all'adeguamento o alla limitazione della funzionalità; in caso di conformità, limitarsi a stabilire l'opportunità di una nuova ispezione ed a fissarne i tempi di esecuzione.

Gli aspetti che devono essere esaminati dipendono da diversi fattori. Con riferimento a titolo d'esempio al caso della verifica di resistenza di un sistema strutturale, sono da citare: i potenziali meccanismi di collasso e la dipendenza

dal tempo di essi; i livelli di danno considerati critici per gli elementi strutturali; le diverse fonti di incertezza associate sia alla modellazione del comportamento del sistema che alla valutazione della capacità portante degli elementi ed alla quantificazione degli errori di misura o commessi dagli operatori durante lo svolgimento delle indagini e l'interpretazione dei risultati; la storia degli interventi già realizzati sulla costruzione; i fondi messi a disposizione.

L'estensione dell'ispezione dipende dalle informazioni che sono disponibili preliminarmente, ovvero dai dati reperibili riguardo al progetto, alla costruzione, al collaudo e ricavati dalle indagini condotte in precedenza. Soprattutto negli edifici molto antichi, tali informazioni 'a priori' possono essere state completamente perse ed il programma d'indagine di conseguenza deve risultare sufficientemente esteso. Al contrario, nel caso siano disponibili molte informazioni, l'indagine può assumere il carattere di una semplice verifica.

In entrambi i casi il programma di ispezione deve essere definito in modo che il costo di esso sia giustificato dalla significatività delle informazioni ottenute e bilanciato dal valore residuo della costruzione.

Ancora solo da un punto di vista qualitativo, nel caso in cui il meccanismo di danneggiamento di un componente strutturale e la sua evoluzione temporale siano noti (ad esempio in funzione della frequenza di applicazione del carico), sarà possibile definire il tempo in cui si realizzerà la prima ispezione o la durata dell'intervallo tra due ispezioni successive proprio in base al modello di propagazione del danno e quindi valutando gli stati in cui la funzionalità dell'elemento risulti ridotta ad un livello critico. La durata dell'intervallo d'ispezione dipenderà infatti: dallo stato iniziale di danno del componente, ovvero dalla sua condizione all'inizio del programma d'ispezione, dalla sua capacità resistente e dal modo in cui essa degrada; dal modello di danno assunto, che deve essere necessariamente stocastico per tener conto delle diverse cause di aleatorietà ed incertezza; dal livello di soglia in corrispondenza del quale il danno accumulato è considerato critico; dai fattori ambientali o prestazionali che ne influenzano la propagazione.

Il superamento di un livello di soglia del danneggiamento subito da un elemento può essere descritto solo attraverso una funzione di probabilità: la programmazione delle ispezioni richiede pertanto una procedura combinata, probabilistica e di ottimizzazione dei tempi di ispezione, in funzione dell'estensione dei danni e dei livelli di soglia al di sopra dei quali si ritiene necessaria la riparazione.

Poiché almeno nei casi correnti la funzione obiettivo consiste nella minimizzazione del costo totale atteso, la scelta di eseguire un programma di ispezioni deve essere comunque confrontata con le alternative:

- nessuna ispezione e nessuna manutenzione;
- nessuna ispezione e nessuna manutenzione ad intervalli fissi;
- sostituzione senza ispezione.

La possibilità di eseguire tali valutazioni economiche decade nel caso degli

edifici di interesse storico-monumentale, la cui conservazione è comunque motivata da considerazioni legate a valori non monetizzabili. La trattazione che segue si limita pertanto ad esaminare il caso in cui al collasso del sistema sia comunque associabile una valutazione economica.

### OTTIMIZZAZIONE DEI TEMPI D'ISPEZIONE

Questo problema, al di fuori di un'impostazione probabilistica, ha avuto finora soltanto soluzioni empiriche, legate alla considerazione che l'ispezione se troppo prematura fornisce informazioni prive di significato, non essendosi ancora potuto sviluppare alcun danno significativo, se tardiva può vanificare l'opportunità di un intervento di riparazione, essendo troppo grave l'entità del danno cumulato.

Una possibile procedura probabilistica per l'ottimizzazione dei tempi d'indagine su una costruzione, con riferimento ad una assegnata durata della vita utile  $T$ , è quella illustrata nel seguito [6].

Per semplicità di esposizione, viene considerato il caso di un solo componente strutturale, per il quale si ipotizza che l'eventuale intervento di riparazione sia in grado di ripristinare completamente (cioè i livelli originari) l'integrità e la capacità portante e che i tempi dedicati all'ispezione ed alla riparazione siano trascurabili rispetto al periodo di vita utile previsto  $[0, T]$ .

La definizione dei tempi di ispezione ottimali viene svolta con l'obiettivo di minimizzare il costo totale atteso, che risulta composto, oltre che dall'investimento iniziale, dai costi associati al collasso dell'opera ( $C_c$ ), all'indagine ( $C_i$ ) ed alla eventuale riparazione ( $C_r$ ). Ciascun termine del costo totale è a sua volta funzione del tempo; la relativa capitalizzazione richiede considerazioni di una certa complessità e pertanto può essere in prima istanza trascurata o eseguita in termini semplificati, assunto ad esempio che il tasso d'inflazione annuo sia costante.

Sia quindi  $t_i$  l'istante ( $\in [0, T]$ ) in cui si prevede di effettuare l'indagine sulla costruzione e che rappresenta quindi l'incognita del problema. Tale indagine ha evidentemente significato solo se il componente considerato non risulta ancora collassato all'istante  $t_i$ .

Sia poi  $P_f'(t_i)$  la probabilità di collasso dell'elemento all'istante  $t_i$ , valutata con riferimento ad un determinato stato limite:  $[1 - P_f'(t_i)]$  è di conseguenza la probabilità di eseguire l'ispezione.

Nello spirito dell'inferenza bayesiana e con le tecniche illustrate in [1], [2], [3], [4] e [5], è possibile tener conto dei risultati delle indagini svolte durante l'ispezione per aggiornare la stima iniziale ('a priori') della probabilità di collasso  $P_f'(t_i)$  dell'elemento, e quindi per ricavare l'espressione 'a posteriori' della probabilità di collasso residua:  $P_f''(T - t_i)$ .

Evidentemente, nella fase di programmazione delle ispezioni sulle co-

struzioni, non sono noti i risultati delle indagini: essi pertanto devono essere caratterizzati attraverso distribuzioni di probabilità assegnate a priori, derivate ad esempio sulla base di informazioni di natura qualitativa o dell'effettivo rilievo del comportamento nel tempo di costruzioni simili a quella in esame.

L'obiettivo dell'ispezione è quello di fornire un supporto ad una decisione in merito all'attuazione dell'intervento di riparazione, che si renderà necessario nel caso che un efficiente indicatore dello stato di danno del componente abbia superato un valore considerato critico. Il criterio su cui si basa tale decisione è quindi collegato all'aumento della sicurezza residua della costruzione che si ottiene con la riparazione.

Sia quindi  $P_f(t_i)$  la probabilità (ancora stimata a priori) che l'indicatore di danno abbia superato il valore di soglia all'istante  $t_i$ . Evidentemente dovrà essere:  $P_f(t_i) \geq P_f'(t_i)$ .

Sia poi:  $P_f'''(T-t_i)$  la probabilità di collasso residua del componente dopo che è stato completato l'intervento di riparazione: l'espressione di tale funzione viene ricavata aggiornando la stima iniziale della probabilità di collasso. Nella valutazione di essa, occorre tener conto delle incertezze associate all'esecuzione dell'intervento di riparazione: nel caso in esame, per l'ipotesi fatta in merito all'efficacia della riparazione (ovvero di completo ripristino della capacità

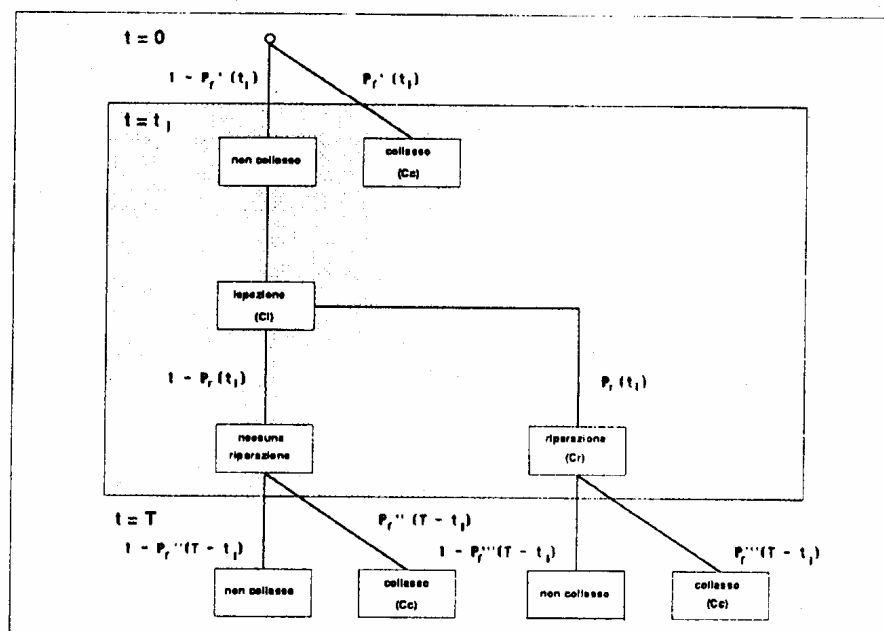


Fig. 1 - Ricerca del tempo d'ispezione: albero degli eventi (da [6])

resistente e dell'integrità dell'elemento), risulterà che la funzione  $P_f'''(\cdot)$  ha la stessa espressione della  $P_f'(\cdot)$ . La funzione  $P_f''(\cdot)$  si ricava invece dall'espressione della  $P_f'(\cdot)$ , ma condizionata al verificarsi dell'evento 'non collasso' del

componente fino all'istante  $t_i$ : tale evento sarà caratterizzato dalla probabilità, definita a priori, che l'indicatore del danno non abbia superato il livello di soglia.

Con riferimento allo schema di fig. 1, in cui sono distinti tutti gli eventi analizzati, che risultano mutuamente esclusivi, il costo totale atteso dell'operazione è pari a:

$$C(t_i, T) = P_f'(t_i) \cdot C_c + [1 - P_f'(t_i)] \cdot \{ C_i + P_f(t_i) \cdot [C_r + P_f''(T - t_i) \cdot C_c] + [1 - P_f(t_i)] \cdot P_f''(T - t_i) \cdot C_c \} \quad (1)$$

Poiché le espressioni di  $P_f'(t_i)$  e  $P_f(t_i)$  sono funzioni crescenti di  $t_i$ , mentre quelle di  $P_f''(T - t_i)$  e  $P_f'''(T - t_i)$  sono funzioni decrescenti di  $t_i$ , esisterà sicuramente un valore di  $t_i$  in corrispondenza del quale il costo totale atteso ha un minimo.

Riguardo ai vincoli da porre alla procedura di ottimizzazione, è evidente intanto che il costo totale atteso dovrà risultare in ogni caso inferiore al costo associato al collasso senza ispezione [pari a  $P_f'(T) \cdot C_c$ ] ed al costo di demolizione e sostituzione senza ispezione. Inoltre si potrà imporre che la probabilità di collasso dell'elemento non risulti mai superiore ad un valore di soglia:  $[P_f'(t_i) \leq P_{f, target}(t_i)]$ , rendendosi in caso contrario comunque necessaria l'ispezione.

Questo tipo di analisi, che nell'inferenza bayesiana assume la denominazione di 'pre-posterior', viene svolto contestualmente alla progettazione dell'opera e permette di determinare il tempo ottimale della prima ispezione sulla costruzione.

In definitiva essa si articola nelle seguenti operazioni:

- definizione di un modello di danno per il componente strutturale e della sua evoluzione nel tempo;
- costruzione della funzione che descrive la variazione nel tempo della probabilità che il danno superi un livello di soglia considerato critico;
- caratterizzazione probabilistica dei possibili risultati di una ispezione;
- valutazione della probabilità di eseguire la riparazione, sulla base del criterio decisionale assunto;
- aggiornamento delle espressioni delle probabilità di collasso con e senza riparazione.

La stessa procedura può essere impiegata per analizzare la condizione effettiva di una costruzione esistente e quindi per valutare l'intervallo tra due successive ispezioni; in tale caso si assumono come dati di partenza ('a priori') quelli derivati attraverso l'esame dei risultati della prima ispezione.

## SCELTA DELLE TECNICHE DI INDAGINE E DELLE DIMENSIONI DEL CAMPIONE

Nella pianificazione del programma di indagini su una costruzione deve essere chiaramente specificato l'obiettivo di esse, essendo differenti le tecniche disponibili per definire le caratteristiche di resistenza o durabilità e più in generale per la verifica della rispondenza alle prescrizioni normative o di progetto.

I criteri di definizione del numero di prove da eseguire (o di campioni da prelevare) dipendono, oltre che dalla disponibilità economica, dalla entità del grado di dissesto osservabile o della non conformità alle specifiche di progetto, e dalla accessibilità degli elementi.

Solo per indagini di routine ed in presenza di danni limitati, si potrà ritenere che i margini di sicurezza adottati nella successiva verifica di sicurezza siano sufficienti a coprire alcuni errori commessi nel campionamento.

Tralasciando i problemi connessi alla verifica della possibilità di combinare i risultati di esperienze eseguite su campioni di popolazioni differenti, uno degli aspetti che richiede qualche considerazione consiste quindi nello stabilire il numero ottimale di prove da eseguire.

Tale valore può essere ricavato imponendo che sia sufficientemente elevata la probabilità che la varianza effettiva della variabile aleatoria in esame sia inferiore ad un valore assegnato. Tale operazione richiede la definizione degli intervalli di confidenza della varianza della variabile campionata, o almeno del limite superiore di essi.

Si ipotizzi quindi di eseguire una serie di misure di una variabile  $X$ , di valore medio  $\mu$  e deviazione standard  $\sigma$ . Siano:  $x_1, x_2, \dots, x_n$ , i risultati delle misure sperimentali e:

$$x^* = \frac{(x_1 + x_2 + \dots + x_n)}{n} \quad (2)$$

$$s^2 = \sqrt{\frac{(\sum_i (x_i - x^*)^2)}{n-1}} \quad (3)$$

gli estimatori non distorti di  $\mu$  e  $\sigma$ .

Si dimostra che, se  $X$  è una variabile gaussiana, la variabile:

$$(n-1) \frac{s^2}{\sigma^2} = \chi_{n-1}^2$$

ha una distribuzione di tipo chi-quadrato a  $(n-1)$  gradi di libertà.

Il numero  $n$  di prove da eseguire dovrà pertanto risultare tale che sia verificata la disuguaglianza:

$$P\left\{\sigma^2(X) < (n-1) \frac{s^2}{\chi^2_{n-1,\alpha}}\right\} = \alpha \quad (4)$$

dove:  $\sigma^2(X)$  è un valore adeguatamente limitato, ad esempio tale che il coefficiente di variazione di  $X$  sia inferiore al 10%;

$\alpha$  è un valore di probabilità assegnato;

$\chi^2_{n-1,\alpha}$  è tale che:  $P\{\chi^2_{n-1} > \chi^2_{n-1,\alpha}\} = \alpha$ .

Nel caso in cui invece siano già disponibili i risultati di una serie di prove che forniscano una stima del valore medio della variabile e della precisione con cui tale parametro è definito, è possibile stabilire la relazione tra il numero di prove già eseguite e quelle da eseguire con un'altra tecnica di prova (ad esempio di più semplice esecuzione), imponendo che per entrambe il valore medio della variabile sia definito con la stessa precisione. In questo caso occorre analizzare gli intervalli di confidenza del valore medio. I relativi limiti sono espressi dalla relazione:

$$E[X] \pm \frac{s}{\sqrt{n-1}} t \quad (5)$$

essendo  $t$  la variabile di Student, il cui valore dipende dal livello di confidenza considerato e dall'ampiezza del campione.

Se ad esempio si vuole stimare la media al livello di confidenza del 95%, occorre fare riferimento ai valori di  $t$  che rappresentano il frattile al 97,5%. Questi valori dipendono dal numero dei gradi di libertà, ma risultano però poco variabili con esso (per:  $n = 10$ ,  $t = 2.26$ ; per:  $n = 120$ :  $t = 1.98$ ).

Indicando con gli indici 1 e 2 le due tecniche di prova a confronto, si ricava di conseguenza in modo approssimato che:

$$\frac{s_1}{\sqrt{n_1-1}} = \frac{s_2}{\sqrt{n_2-1}} \quad (6)$$

e quindi:

$$\sqrt{n_1-1} = \frac{s_1}{s_2} \sqrt{n_2-1} \quad (7)$$

Tale relazione permette di ricavare il valore del numero  $n_1$  di prove da eseguire con la tecnica 1 purché si conoscano, anche attraverso esperienze condotte in occasioni diverse, i valori di  $s_1$  e  $s_2$ .

In via più generale, ed in linea con le indicazioni del paragrafo precedente, è possibile applicare un'analisi bayesiana di tipo 'pre-posterior' anche alla determinazione delle dimensioni ottimali del campione statistico. Infatti, poiché è evidente che l'accuratezza della stima dei parametri di una variabile aleatoria aumenta con il numero di prove eseguite, ma contemporaneamente aumentano i costi ( $C_p$ ) associati all'ispezione, la dimensione ottimale del campione risulterà da un bilanciamento tra la precisione ottenuta ed il costo delle prove. Sviluppando quindi alcune considerazioni riportate in [7], si dimostra che, per una popolazione gaussiana, la dimensione ottimale del campione è espressa attraverso la relazione:

$$n_{opt} = \sigma \left( \sqrt{\frac{c}{k}} - \frac{\sigma}{\sigma'^2} \right) \quad (8)$$

essendo:  $\sigma$  lo scarto quadratico medio dell'errore di misura;  $c$  la stima del costo associato ad un errore unitario nella valutazione del valore medio della variabile;  $k$  il costo di una prova;  $\sigma'^2$  la deviazione standard stimata 'a priori' del valore medio della variabile in esame. Evidentemente, se:

$$\sqrt{\frac{c}{k}} < \frac{\sigma}{\sigma'^2}$$

non dovrà essere eseguita nessuna misura e ci si potrà basare sulle valutazioni effettuate 'a priori'.

## PROBLEMI SPECIFICI CONNESSI ALL'INTERPRETAZIONE DI RISULTATI SPERIMENTALI

Nel seguito vengono esaminati alcuni problemi relativi alla interpretazione dei risultati di una ispezione, ed in particolare alla definizione della distribuzione di probabilità di una variabile aleatoria, sia essa di base, che derivata attraverso una relazione teorica (di cui si voglia al tempo stesso esaminare l'attendibilità), o alla valutazione di un valore della variabile caratterizzato da una assegnata probabilità di realizzarsi. Tali funzioni di distribuzione possono essere impiegate per l'aggiornamento con tecniche bayesiane di funzioni di distribuzione assegnate a priori.

## **SCELTA DELLA FUNZIONE DI DISTRIBUZIONE DI UNA VARIABILE CAMPIONATA**

La scelta della funzione di distribuzione da attribuire ad una variabile aleatoria sulla base dei risultati di un campionamento statistico rappresenta un problema delicato, che richiede la costruzione di un test di verifica e la definizione di un criterio di decisione in base al quale sia possibile rifiutare o accettare l'ipotesi secondo cui gli  $n$  valori osservati costituiscono un campione della funzione di distribuzione ipotizzata a priori.

In alternativa, tale obiettivo può essere raggiunto adottando il metodo della retta di Henry o eseguendo il test di chi-quadrato, proposto da Karl-Pearson nel 1900, o il test di Kolmogorov-Smirnov.

Il primo consiste in un procedimento grafico, che permette di verificare se il campione deriva da una distribuzione normale (o log-normale) ed in caso positivo di stimare i parametri di tale distribuzione. Il suo impiego è basato sulla osservazione che l'ipotesi di normalità (o log-normalità) è verificata se il diagramma che si costruisce riportando in ascissa i valori della variabile ed in ordinata, in scala normale (o log-normale), le frequenze cumulate risulta approssimativamente una retta; se tale condizione è soddisfatta, è immediato derivare il valore medio e la deviazione standard di tale distribuzione.

Il test di chi-quadrato si applica ancora per la verifica dell'ipotesi di normalità e consiste nel suddividere il dominio di definizione della variabile in  $p$  classi disgiunte, di cui sia possibile valutare le frequenze relative, e nel valutare la 'distanza' tra la densità multinomiale teorica e quella empirica che risulta dal campionamento. Senza entrare nel dettaglio della formulazione analitica, peraltro molto semplice, è sufficiente osservare che, se è limitata la probabilità che il quadrato di tale distanza, che ha una distribuzione chi-quadrato, sia inferiore ad un valore assegnato, la distribuzione empirica è molto prossima a quella reale, e risulta quindi verificata l'ipotesi di normalità.

Il test di Kolmogorov-Smirnov consiste invece nel valutare lo scarto massimo tra la funzione di ripartizione empirica e quella teorica; l'ipotesi relativa alla scelta della distribuzione risulta al solito verificata se la probabilità che lo scarto massimo sia inferiore ad un valore assegnato è maggiore di un livello di soglia ritenuto accettabile. Per l'applicazione di questo test a svariati tipi di distribuzione teorica sono disponibili diversi programmi di libreria.

## **CONFRONTO TRA I RISULTATI DI UNA PROVA SPERIMENTALE ED I VALORI RISULTANTI DA UN MODELLO ANALITICO**

Il problema delineato si complica nel caso in cui la grandezza in esame, misurata direttamente, venga espressa anche attraverso una relazione analitica in funzione di un certo numero di variabili di base, variabili in parte misurate

anch'esse direttamente ed in parte solo stimate a partire da valori nominali.

È questo il caso ad esempio delle deformazioni di una trave, rilevate attraverso una prova di carico, ed anche della resistenza del calcestruzzo, ricavata da prove di schiacciamento eseguite su campioni del materiale e controllata attraverso le formule di correlazione che utilizzano i risultati della prove non distruttive eseguite con lo sclerometro e con la tecnica degli ultrasuoni.

Per semplicità di esposizione, si ipotizzi quindi che una variabile aleatoria, ad esempio la resistenza teorica di un elemento strutturale, sia esprimibile come il prodotto di  $p$  variabili di base (che rappresentino le caratteristiche meccaniche e geometriche dell'elemento o grandezze quali l'indice di rimbalzo dello sclerometro o la velocità di propagazione degli ultrasuoni), attraverso una relazione del tipo:

$$R_t = X_1^{\alpha_1} \cdot X_2^{\alpha_2} \cdot \dots \cdot X_p^{\alpha_p} \quad (9)$$

essendo  $\alpha_1, \alpha_2, \dots, \alpha_p$  esponenti reali.

Per tener conto del grado di approssimazione connesso all'impiego della relazione analitica, si ipotizzi ancora che lo scarto tra il valore effettivo di tale grandezza e quello derivato teoricamente sia esprimibile attraverso un fattore di errore  $\Delta$  di tipo moltiplicativo.

La resistenza effettiva dell'elemento risulta pertanto espressa dalla variabile:

$$R = R_t \Delta \quad (10)$$

Per semplificare gli sviluppi del procedimento di stima della distribuzione di probabilità di  $R$ , si ponga poi l'ipotesi che le variabili di base e la variabile d'errore abbiano una legge di distribuzione log-normale e siano tra loro indipendenti.

Passando ai logaritmi, si ricava pertanto che:

$$\ln R = \alpha_1 \ln X_1 + \alpha_2 \ln X_2 + \dots + \alpha_n \ln X_n + \ln \Delta \quad (11)$$

essendo:  $(\ln X_i)$  e  $(\ln \Delta)$  variabili aleatorie a distribuzione normale.

La resistenza effettiva dell'elemento è quindi funzione:

- a) di una variabile aleatoria a distribuzione log-normale  $R_t$ , i cui parametri possono essere calcolati a partire dalle caratteristiche delle variabili di base, combinando le informazioni disponibili a priori con quelle ricavate attraverso le prove [5]:

$$m_{R_t} = E[\ln R_t] = \sum_{i=1}^p \alpha_i E[\ln X_i] \quad (12)$$

$$\begin{aligned}
 s_{R_i}^2 &= \sigma^2 [\ln R_i] = \sum_{i=1}^p \alpha_i^2 \sigma^2 [\ln X_i] = \\
 &= \sum_{i=1}^p \alpha_i^2 \ln(1 + C^2(X_i)) \quad (13)
 \end{aligned}$$

essendo  $C(X_i)$  il coefficiente di variazione di  $X_i$ ;

- b) di una variabile aleatoria log-normale  $\Delta$  nota attraverso la stima dei parametri  $m_\Delta$  e  $s_\Delta$ . Proprio la valutazione degli estimatori di  $m_\Delta$  e  $s_\Delta$  comporta alcune approssimazioni. I valori osservati della variabile d'errore:

$$\ln \delta_i = \ln \frac{r_{ci}}{r_{ti}} \quad (i = 1, n) \quad (14)$$

(gli  $r_{ci}$  sono i valori di  $R$  misurati direttamente, mentre gli  $r_{ti}$  quelli ricavati attraverso l'espressione analitica (9)) permettono di definire una realizzazione del valore medio della variabile d'errore:

$$\ln \Delta^* = \frac{1}{n} \sum_{i=1}^n \ln \delta_i \quad (15)$$

e quindi del fattore medio di correzione del modello analitico. Una realizzazione della varianza di  $\Delta$  è espressa dalla relazione:

$$s^{2*}[\ln \Delta^*] = \frac{1}{n-1} \sum_{i=1}^n (\ln \delta_i - \ln \Delta^*)^2 \quad (16)$$

Risulta pertanto:

$$E[\ln \Delta^*] \cong m_\Delta \quad E[s^{2*}[\ln \Delta^*]] \cong s_\Delta^2$$

Nel caso in cui alcune variabili di base non siano effettivamente misurate, ma solo definite sulla base di valori nominali, e nell'ipotesi che siano noti i valori medi di esse, risulta necessario correggere la stima della varianza della variabile d'errore, secondo la relazione seguente:

$$s^2[\ln \Delta] = s^{2*}[\ln \Delta] + \frac{n-1}{n-2} \sum_{j=1}^p \sigma^2(\ln X_j) \quad (17)$$

La variabile di resistenza  $R$  risulta pertanto una variabile aleatoria a distribuzione log-normale, di parametri:

$$m_R = E[\ln R] = m_{Rt} + m_{\Delta} \quad (18)$$

$$s_R = \sigma[\ln R] = \sqrt{s_{Rt}^2 + s_{\Delta}^2} \quad (19)$$

e di valore caratteristico (corrispondente al frattile di ordine  $k$ ):

$$R_k = \exp(m_{Rt} + m_{\Delta} - u_k \sqrt{s_{Rt}^2 + s_{\Delta}^2}) \quad (20)$$

essendo:

$$u_k = \Phi^{-1}\left(\frac{1+k}{2}\right)$$

e  $\Phi(\cdot)$  la funzione di distribuzione normale standard.

Per tener conto dell'incertezza statistica legata all'impiego di un numero limitato di risultati sperimentali, è opportuno sostituire al valore deterministico  $R_k$  una variabile definita dalla relazione:

$$R_k^E = X^* - k_s S^* \quad (21)$$

e tale che:  $P(R_k^E < R_k) = p$  con  $p$  fissato (ad esempio pari a 0.75).

In via semplificata, tralasciando gli sviluppi del procedimento, è possibile porre:

$$R_k^E = m_{Rt} \exp[\ln \Delta^* - u_k \alpha_k^E s_{Rt} - k_s \alpha_s^E s_{\Delta} [\ln \Delta] - \frac{1}{2} s_{Rt}^2] \quad (22)$$

essendo:

$$\alpha_k^E = \frac{s_{Rt}}{\sqrt{s_{Rt}^2 + s_{\Delta}^2}} \quad \alpha_s^E = \frac{s_{\Delta}}{\sqrt{s_{Rt}^2 + s_{\Delta}^2}}$$

i fattori che pesano le due varianze:

$$k_s = \frac{-nu_k \left(1 - \frac{1}{4(n-1)} + k_{sl}\right)}{n \left[ \left(1 - \frac{1}{4(n-1)}\right)^2 - \frac{u_p^2}{2(n-1)} \right]}$$

con

$$k_{sl} = \sqrt{n^2 u_k^2 \left(1 - \frac{1}{4(n-1)}\right)^2 - n(nu_k^2 - u_p^2) \left[\left(1 - \frac{1}{4(n-1)}\right)^2 - \frac{u_p^2}{2(n-1)}\right]}$$

e:

$$u_p = \Phi^{-1}\left(\frac{1+p}{2}\right),$$

il fattore dipendente dall'ordine del frattile assunto, per un livello di convergenza della predizione pari a  $p$ .

## STIMA DEL VALORE CARATTERISTICO DI UNA VARIABILE DI RESISTENZA

### A) VARIABILI GAUSSIANE

Il valore caratteristico  $c$  della resistenza  $X$  di un materiale viene definito come il frattile inferiore di ordine  $p$  (in generale il 5%) della correlativa distribuzione di probabilità, ed è quindi tale che la probabilità dell'evento:  $\{X \geq c\}$  risulti pari ad  $(1-p)$ .

In generale esso viene ricavato elaborando i risultati di prove su campioni del materiale, ed attribuendo alla resistenza una distribuzione di tipo gaussiano. Se quindi  $X$  è una variabile aleatoria gaussiana con valore medio  $\mu$  e deviazione standard  $\sigma$ , risulta:

$$c = \mu - k \sigma \quad (23)$$

dove  $k$  è un marametro che varia in funzione del valore assunto per  $p$  (per:  $p=0.05$ ,  $k=1.645$ ; per:  $p=0.10$ ,  $k=1.280$ ).

Si ipotizzi quindi di eseguire una serie di prove sperimentali su campioni del materiale, con l'obiettivo di verificare l'ipotesi che il valore caratteristico della resistenza abbia un valore assegnato  $c$ , note alcune informazioni disponibili a priori su  $X$  (e quindi su  $\mathbf{M}$  e  $\Sigma$ ) e dati i risultati delle prove, raccolti nel campione statistico:  $x_1, x_2, \dots, x_n$ . Secondo il modello d'inferenza bayesiana, il valore caratteristico:  $c = \mu - k\sigma$ , che corrisponde ad una distribuzione gaussiana di  $X$ , rappresenta una osservazione della variabile aleatoria:  $C = \mathbf{M} - k\Sigma$ . Utilizzando le informazioni addizionali, è possibile aggiornare la distribuzione di probabilità della variabile  $C$ . Nell'ipotesi infatti che la distribuzione congiunta a priori di  $(\mathbf{M}, \log \Sigma)$  sia non informativa, si ricava [8] per la variabile:

$$\frac{C - x^*}{s / \sqrt{n-1}} = \frac{[(M - x^*) / (\Sigma / \sqrt{n})] - k\sqrt{n}}{\sqrt{[1 / (n-1)][ns^2 / \Sigma^2]}} \quad (24)$$

una distribuzione *t* di Student non centrata, con (n-1) gradi di libertà e parametro di non centralità:

$$\delta = -k\sqrt{n}.$$

Nella relazione precedente, si è posto:

$$x^* = \frac{1}{n} \sum x_j \quad s = \sqrt{\frac{(x_i - x^*)^2}{n-1}}$$

Assegnata la densità di probabilità a posteriori della variabile *C*, è immediato valutarne gli intervalli di confidenza ad un assegnato livello di probabilità. Ad essi è possibile, ad esempio, correlare i criteri di accettazione del materiale: siano infatti  $t_{p_1}$  e  $t_{p_2}$  due frattili di questa densità, corrispondenti a valori di probabilità  $p_1$  e  $p_2$ . L'intervallo di confidenza a probabilità  $(p_2 - p_1)$  della variabile *C* è definito come l'intervallo:

$$\left[ x^* + t_{p_1} s / \sqrt{n-1}, x^* + t_{p_2} s / \sqrt{n-1} \right] \quad (25)$$

In alternativa, è possibile valutare la densità predittiva della resistenza *X* del materiale ed accettare la qualità di esso se risulta soddisfatta la condizione:  $f_x(c | x_1, x_2, \dots, x_n) \leq p$ , essendo *p* un valore di probabilità sufficientemente ridotto (ad esempio il 10%). Al riguardo si dimostra che la densità predittiva è tale che la variabile:

$$\frac{C - x^*}{s} \sqrt{\frac{n-1}{n+1}} \quad (26)$$

ha una densità *t* di Student a (n-1) gradi di libertà.

## B) VARIABILI NON GAUSSIANE

L'ipotesi che la resistenza di un materiale abbia una distribuzione di tipo gaussiano non è accettabile in via di principio, perché tale distribuzione è definita anche per valori negativi della variabile, mentre la grandezza in esame è sicuramente positiva: viene comunque adottata per la semplicità di trattazione analitica e quando il livello di approssimazione che si consegue è dello

stesso ordine di grandezza di quello implicitamente accettato perché connesso alle incertezze del modello di analisi strutturale.

Soprattutto se il numero di risultati sperimentali è limitato, l'ipotesi di normalità fornisce però una stima troppo approssimata dei frattili inferiori della effettiva distribuzione di probabilità della variabile. Tale problema può essere risolto adottando modelli più efficienti di approssimazione della distribuzione reale, così come risulta dal campionamento statistico.

Tra i possibili approcci, appare di un certo interesse un modello di tipo polinomiale [9], definito in modo da assumere in alcuni punti prefissati il valore effettivo della funzione di distribuzione della variabile campionata.

Si consideri pertanto un insieme di  $n$  risultati campionari, di valore pari a:  $x_1, x_2, \dots, x_n$ ; ed ordinati in modo che risulti:  $x_1 < x_2 < \dots < x_n$ . Sia poi  $F(x)$  una funzione definita dalla relazione:

$$F(x) = \frac{i}{1+n}, \quad i = 1, 2, \dots, n \quad (27)$$

e  $Z$  una variabile normale standard tale che:

$$F(x_i) = \Phi(z) \quad (28)$$

La variabile  $Z$  assume quindi in  $n$  punti i valori assunti dalla funzione di distribuzione della variabile  $X$ : in particolare per:  $F(x)=0.5$ , sarà:  $z=0$ . Sia poi:

$$y = a_0 + a_1 z + a_2 z^2 + \dots + a_{p-1} z^{p-1} = \frac{(x/x_\mu)^2 - 1}{2(x/x_\mu)} \quad (29)$$

una approssimazione della  $\Phi(z)$ .  $x_\mu$  è un valore definito opportunamente, in modo da rendere:  $F(x_i)=y$  nel punto medio, e quindi tale che:  $x_\mu = x_k$ , per  $n = (2k-1)$ ; e:  $x_\mu = (x_k + x_{k+1})/2$ , per  $n = 2k$ .

Poiché per  $x=x_k$ , risulta:  $z=0$  ed  $y=0$ , è evidente che deve essere anche:  $a_0=0$ . I rimanenti valori dei coefficienti  $a_i$  vengono ricavati imponendo che:  $F(x_i)=y$  in altri  $(p-1)$  punti.

Se si osserva l'espressione:

$$y = \frac{(x/x_\mu)^2 - 1}{2(x/x_\mu)} \quad (30)$$

si verifica che:

-  $y$  è adimensionale, come è giusto per generalizzare i risultati e renderli

indipendenti dall'unità di misura si X;

- y è tale da render soddisfatte le condizioni al contorno, poiché:  $y \rightarrow -\infty$  per  $x \rightarrow 0$ ; e  $y \rightarrow \infty$  per  $x \rightarrow \infty$

Poiché x è sicuramente positivo, è immediato ricavare che:

$$x = x_{\mu} (y + \sqrt{1 + y^2}) \quad (31)$$

Ponendo a titolo di esempio:  $p=3$ , si ottiene:

$$y = a_1 z + a_2 z^2 \quad (32)$$

ed assumendo che l'identità:  $F(x_i)=y$  sia soddisfatta nei punti 1 ed n (cioè in corrispondenza dei valori rispettivamente minimo e massimo del campione) si ottiene:

$$z_1 = -z_n \quad a_1 = \frac{y_1 - y_n}{2z_1} \quad a_2 = \frac{y_1 + y_n}{2z_1^2}$$

e quindi:

$$y = \left( \frac{y_1 - y_n}{2} \right) \left( \frac{z}{z_1} \right) + \left( \frac{y_1 + y_n}{2} \right) \left( \frac{z}{z_1} \right)^2 \quad (33)$$

Un valore della variabile corrispondente ad un frattile di qualsiasi ordine viene ricavato dalle relazioni precedenti. Da esse si rileva che il rapporto:  $t = z/z_1$ , è funzione dell'ordine del frattile assunto e della numerosità del campione; i suoi valori possono essere pertanto tabellati, così come indicato nella Tabella 1 nel caso del frattile di ordine 0.02 e per n compreso tra 10 e 20.

Il valore caratteristico della variabile si calcola quindi attraverso le seguenti fasi:

a) calcolo di:

$$y_1 = \frac{(x_1 / x_{\mu})^2 - 1}{2(x_1 / x_{\mu})} \quad (34)$$

$$y_n = \frac{(x_n / x_{\mu})^2 - 1}{2(x_n / x_{\mu})} \quad (35)$$

b) valutazione di t in funzione di n e dell'ordine del frattile;

c) calcolo di:

$$y^* = \left( \frac{y_1 - y_n}{2} \right) t + \left( \frac{y_1 + y_n}{2} \right) t^2 \quad (36)$$

c) calcolo di:

$$c = x_\mu (y^* + \sqrt{1 + y^{*2}}) \quad (37)$$

*Tabella 1 - Valori del fattore t corrispondenti al frattile al 2%*

| n | 10   | 11   | 12   | 13   | 14   | 15   | 16   | 17   | 18   | 19   | 20   |
|---|------|------|------|------|------|------|------|------|------|------|------|
| t | 1.53 | 1.49 | 1.43 | 1.39 | 1.37 | 1.34 | 1.31 | 1.29 | 1.27 | 1.25 | 1.23 |

La procedura indicata fornisce quindi una valutazione consistente del valore caratteristico della variabile a partire da un numero limitato di osservazioni di essa.

## CONCLUSIONI

In precedenza sono stati illustrati i criteri generali di una procedura per la programmazione delle ispezioni sulle costruzioni: tale procedura permette di ottimizzare il costo totale atteso del programma di manutenzione attraverso la stima delle probabilità di collasso dei componenti del sistema strutturale. La sua generalizzazione all'analisi dell'intero sistema è peraltro concettualmente semplice, una volta che sia definita la logica funzionale secondo cui i diversi componenti sono associati ai fini della stima dell'affidabilità e siano evidenziati i livelli di danno critici per il complesso dei componenti.

La procedura indicata, che verrà applicata all'analisi di un problema concreto in un prossimo lavoro, è basata sull'impiego combinato delle tecniche dell'inferenza bayesiana e dei metodi avanzati del secondo ordine ai secondi momenti, perché richiede di aggiornare la stima dell'affidabilità strutturale in base alle informazioni desumibili attraverso le indagini svolte in sito.

Nella seconda parte infine sono stati delineati alcuni problemi che si pongono nella interpretazione statistica dei risultati delle prove sperimentali, sia ai fini di una valutazione probabilistica della sicurezza strutturale che della stima di valori delle variabili caratterizzati da un prefissato livello di probabilità. Tali operazioni costituiscono infatti il corretto presupposto su cui basare le successive verifiche di sicurezza.

**BIBLIOGRAFIA**

1. MADSEN, H.O. (1987): "*Model Updating in Reliability Theory*", in: Reliability and Risk Analysis in Civil Engineering, Vol. 1, Atti della: International Conference on Application of Statistics and Probability ICASP'5, Vancouver, Canada, Maggio, 565
2. CIAMPOLI, M., PINTO, P.E. (1989): "*Metodi per la valutazione della sicurezza delle strutture esistenti*", Atti del Congresso AICAP'89, Napoli, Maggio, 21
3. CIAMPOLI, M. (1989): "*Reliability Evaluation of Existing Structures: Updating Technique to Account for Experimental Data*", Atti della Conferenza Internazionale su: "Monitoring Surveillance and Predictive Maintenance of Plants and Structures", AIPnD, Taormina, Ottobre
4. RADOGNA, E.F., NAPOLI, P. (1990): "*Revised Safety Criteria/Rules*", C.E.B. General Task Group 21 "Re-design of Concrete Structures" State-of-the-Art Report, Cap. 3 (di prossima pubblicazione); CIAMPOLI, M. (1990): "*Revised Safety Criteria/Rules*", C.E.B. General Task Group 21 "Re-design of Concrete Structures" State-of-the-Art Report, Appendice al Cap. 3 (di prossima pubblicazione)
5. CIAMPOLI, M., NAPOLI, P., RADOGNA, E.F. (1990): "*Criteri generali per la stima della sicurezza nelle costruzioni esistenti*", L'Industria Italiana del Cemento, Fascicolo di Novembre 1990
6. FUJITA, M., SCHALL, G., RACKWITZ, R. (1989): "*Adaptive Reliability-Based Inspection Strategies for Structures subjected to Fatigue*", Atti della: 5<sup>th</sup> International Conference on Structural Safety and Reliability ICOSSAR '89, San Francisco, California, Agosto, 1619
7. ANG, A.H.-S., TANG, W.H. (1984): "*Probability Concepts in Engineering Planning and Design, Vol. II: Decision, Risk and Reliability*", John Wiley & Sons, New York
8. DITLEVSEN, O. (1981): "*Uncertainty Modeling with Applications to Multidimensional Civil Engineering Systems*". McGraw-Hill, USA
9. JAEGER, L.G., BAKHT, B. (1990): "*Lower Fractiles of Materiale Strength from Limited Test Data*", in: Structural Safety, N. 7, 67

## CHECKING THE RANDOMNESS OF PSEUDORANDOM SEQUENCES FROM A BAYESIAN VIEWPOINT(\*)

Giuseppe Di Biase<sup>(\*)</sup> and Antonio Maturo<sup>(\*)</sup>

Università "G. D'Annunzio" - Chieti

**Sommario.** Viene affrontato il problema della verifica di casualità di successioni di numeri pseudocasuali, soprattutto da un punto di vista bayesiano. Nel lavoro vengono proposti dei criteri operativi di carattere convenzionale adatti per la verifica della bontà dei generatori ed alcune analisi bayesiane. In particolare viene esaminata, da un punto di vista teorico, quella sostitutiva del test classico delle frequenze, la cui applicazione numerica è stata effettuata dagli stessi autori in [5].

**Abstract.** After illustrating the classic and the bayesian approaches to the analysis of randomness of pseudorandom sequences, the bayesian viewpoint is further dealt with, since up to now, it has not been exhaustively analysed. A bayesian analysis which can replace the frequency test is also presented. The numerical application and its results can be found in [5].

---

(\*) Work carried out within the Research Project MURST 40% entitled "Mathematical Statistics". National coordinator L. Piccinato.

<sup>(\*)</sup> Dipartimento di Scienze, Storia dell'Architettura e Restauro - Viale Pindaro, 42 - 65127 Pescara

<sup>(\*)</sup> Facoltà di Farmacia - Via degli Agostiniani - Chieti

## 1. STATISTICAL ANALYSIS OF PSEUDORANDOM GENERATORS

Let  $N$  be the set of natural numbers, and  $X$  a continuous random variable uniformly distributed over  $(0,1)$ .

Let  $\{X_i\}_{i \in N}$  be a sequence of independent random variables having the same distribution as  $X$ . If  $x_i$  (for each  $i \in N$ ) is a realization of  $X_i$ , the sequence  $\{x_i\}_{i \in N}$  is called a **sequence of random numbers**.

For each  $m \in N$ ,  $X^{(m)}$  is a standard discrete random variable with parameter  $m$  uniformly distributed, i.e. with values in  $\{0, 1/m, 2/m, \dots, (m-1)/m\}$ , each with probability  $1/m$ .

$X^{(m)}$  has the characteristic function

$$H_m(u) = (1/m)(e^{iu} - 1)/(e^{iu/m} - 1).$$

Therefore it results that:

$$\lim_{m \rightarrow +\infty} H_m(u) = (e^{iu} - 1)/iu,$$

where the value of the limit defines the characteristic function of the random variable  $X$ , so that the sequence  $\{X^{(m)}\}_{m \in N}$  converges in distribution to  $X$ .

Since computers employ only rational numbers with a limited number of decimal-coded digits, the sequence  $\{X_i\}_{i \in N}$  can be replaced by a sequence  $\{X_i^{(m)}\}_{i \in N}$  of independent random variables having the same distribution as  $X^{(m)}$ , for sufficiently large  $m$ . Instead of the sequence  $\{x_i\}_{i \in N}$ , it is then considered the sequence  $\{x_i^{(m)}\}_{i \in N}$  where  $x_i^{(m)}$  corresponds to a realization of  $X_i^{(m)}$ , called **sequence of random numbers** too.

In practice, given a value of  $m$ , the sequence of values  $x_i^{(m)}$  taken by  $X_i^{(m)}$ ,  $i \in N$ , is replaced by a sequence  $\{z_i\}_{i \in N}$  of values obtained with the computer applying the recursive formula:

$$y_{i+1} = f(\alpha_1, \alpha_2, \dots, \alpha_h; y_i), \quad i \in N, \quad (1.1)$$

where  $f$  is a function of the variable  $y_i$ , defined from  $I_m = \{0, 1, 2, \dots, m-1\}$  to  $I_m$ , and depending on the parameters  $\alpha_1, \alpha_2, \dots, \alpha_h$ . Therefore, if the starting number  $y_1 \in I_m$  is fixed, a sequence  $\{y_i\}_{i \in N}$  of elements of set  $I_m$  is obtained.

Subsequently, assuming  $z_i = y_i/m$ , a sequence whose space is  $\{0, 1/m, \dots, (m-1)/m\}$  is obtained.

This procedure may seem completely illogical. In fact, according to it, they are not considered random numbers, but numbers obtained out of a formula in

a deterministic way. These are called **pseudorandom numbers**.

The procedure can be justified by the subjective definition of pseudorandom numbers (see i.e. Bruno Baldessari (1987), [1], Alfredo Rizzi (1989), [11]) according to which the sequence  $\{z_i^{(m)}\}_{i \in \mathbb{N}}$  is said **pseudorandom** if:

(1) a user who knows the generator (1.1) can univocally generate the sequence;

(2) a user who does not know the generator, can assume that the sequence  $\{z_i\}_{i \in \mathbb{N}}$  is a realization of a sequence  $\{X_i^{(m)}\}_{i \in \mathbb{N}}$  of standard discrete random variables with parameter  $m$  uniformly distributed.

In fact, if the function  $f$  and its parameters are given in the correct way, the evaluation of  $y_{i+1}$  starting from  $y_i$  is the result of a "randomness effect" similar to the one resulting from mixing cards. As a matter of fact, even in this case, the card position is deterministic and its randomness depends on the fact that the operator does not know it.

In the formula (1.1), to obtain sequences concurring with Baldessari's subjective definition, it is necessary that the operator who generates the sequence knows well its mathematical and statistical properties, so that it may seem random to any observer.

We obtain this by assuming  $f$  equal to a function as simple as possible. For example the formula

$$y_{i+1} = (ay_i + b) \bmod m, \quad i \in \mathbb{N}, \quad a, b \in I_m \quad (1.2)$$

is largely used.

The mathematical and statistical properties of the sequence  $S = \{y_i\}_{i \in \mathbb{N}}$ , obtained by generator (1.2), vary considerably according to the variation of the two parameters  $a$  e  $b$ , of the modulo  $m$  and of the starting point  $y_1$  (see A. Rizzi (1977), [10], Cera and Maturo (1983), [2] and [3], Maturo (1989), [7], Maturo and Piscione (1990), [8]).

Let then consider a sequence  $\{y_i\}_{i \in \mathbb{N}}$  whose space  $I_m$  is obtained from any formula of the (1.1) type, and let  $z_i = y_i/m$ .

A classical approach largely used in order to prove the randomness of the sequence is the following.

Once we have fixed  $n \in \mathbb{N}$ , we ask if the null hypothesis  $H_0$  can be accepted:  $z_i$  are determinations of independent random variables  $Z_i$  having continuous uniform distribution or discrete normalized uniform distribution with parameter  $m$  of the random variable  $Z = X^{(m)}$ .

For this purpose check the finite sequence  $S = \{z_i\}_{i \in \{1, 2, \dots, n\}}$  of length  $n$  by means of a set of statistical tests.

Some of the most common tests are (see A. Rizzi (1977) e (1989), [10] e [11], Knuth (1969), [6], Maturo (1989), [8], Cera e Maturo (1983) e (1990), [2] e [4], Tausworthe (1965), [14]): Test on the mean; on the numbers variance; on the numbers frequency; on the digits frequency; on the number pairs frequency;

on the digit pairs frequency; on the numbers correlation; on the digits correlation; on the complete sequences; the runs test; the gaps test.

The non-parametric checking methods, used in the aforementioned studies are based on the following steps:

a) consider suitable statistics  $D_k = D_k(Z_1, Z_2, \dots, Z_n)$ ,  $k=1, 2, \dots, r$ , assuming nonnegative real values that, **in certain situations regarded as «ideal»**, assume the value zero. The  $D_k$  usually have asymptotic or chi-square distribution or they are equal to absolute value of a symmetric distribution with respect to zero and tabulated (i.e. Student's t-distribution or standardized normal one).

b) For each  $k$  a "small" number  $\alpha_k \in (0,1)$  is fixed, (usually  $\alpha_k=0.01$  or  $\alpha_k=0.001$  or a value between the two), called level of significance, and consequently a real number  $\beta_k$  such that  $\text{prob}(D_k \geq \beta_k) = \alpha_k$  is determined. The pair  $T_k = (D_k, \beta_k)$  is called **statistical test at level of significance  $\alpha_k$** .

c) Let  $d_k$  the value of  $D_k$  for  $Z_i = z_i$ , with  $i=1, 2, \dots, n$ . If  $d_k \geq \beta_k$ ,  $H_0$  is rejected with respect to the test  $T_k$ , if this not,  $H_0$  is accepted.

d) The sequences for which the hypothesis  $H_0$  is accepted, with respect to each of the  $T_k$  tests, are considered "acceptable" with respect to the set of tests.

The principle according to which the hypothesis  $H_0$  is rejected, if  $d_k \geq \beta_k$ , is based on the following points:

(1) **probabilistic evaluation**: the event  $E_k = (D_k \geq \beta_k)/H_0$  has very small probability  $\alpha_k$  of occurring. Since he has occurred, that leads to consider the hypothesis  $H_0$  false;

(2) **psychological evaluation**: if  $d_k \geq \beta_k$  then the value of  $D_k$  is very far from the, "ideal value", zero.

Some authors (see i.e. R. Scozzafava (1989), [12], A. Maturo and A. Piscione (1990), [8]) have made the following observations:

a) the confusion between  $E_k$  and the event  $A_k = H_0/(D_k \geq \beta_k)$ . According to (1), since the probability of  $E_k$  is little, the probability of  $A_k$  is little too.

Such conclusions lead to paradoxical consequences.

In fact anyone can see that, whatever the finite sequence  $\underline{z}$  of length  $n$  is, if the  $z_i$  are numbers with  $q$  decimal digits, being  $\text{prob}(\underline{z}/H_0) = 10^{-nq}$  and then it result  $\text{prob}(\underline{z}/H_0) = 10^{-nq}$ .

Since, for each  $\alpha_k > 0$ , there is a positive integer  $n$  such that  $10^{-nq} < \alpha_k$ , for a fixed  $\alpha_k$  it is possible to determine a positive integer  $m$  such that, for each  $n \geq m$ , the event  $\underline{z}/H_0$  has probability lower than  $\alpha_k$ .

Therefore, following the same procedure described in Par. 1 we are led to reject  $H_0$  whatever  $\underline{z}$  would be, as long as  $n \geq m$ .

b) The disturbing element put in by (2). The psychological point of view lead us "to reject the tail" of distribution of  $D_k$ , since in it there are values which are very far from the ideal value of  $D_k$ , "0". On the other hand, from a rigorously probabilistic point of view, if  $a$  is a nonnegative real number minor than  $\beta_k$ , and  $b$  is a real number such that the event:  $E_{ak} = (a \leq D_k \leq b)/H_0$ , has a probability  $\alpha_k$ , the

event  $E_{ak}$  may play the same role as the event  $E_k$  in the accepting-rejecting game. For example, assuming  $a=0$ , the test would lead us to reject the "first part" of the distribution.

c) The lack of consideration of alternative hypotheses to  $H_0$ . If we assume that the event  $A_{0k}=H_0/(D_k \geq \beta_k)$  has very little probability, that is not a sufficient reason for rejecting  $H_0$ . In fact it may happen that there are many alternative hypotheses  $H_i$ , with  $i=0, 1, 2, \dots, m$ , and that all the events  $A_{ik}=H_i/(D_k \geq \beta_k)$  have very little probability. In this case, then, if  $d_k \geq \beta_k$ , should all the hypotheses be rejected?

At this point the replacement of the classical checking methods by a Bayesian one, is proposed, since the latter gives the following advantages:

a) apart from the hypotheses  $H_0$ , it takes into consideration a set of alternative hypotheses to be compared with  $H_0$ ;

b) it only gives probabilistic outcomes, without recurring to procedures which do not belong to the probability theory.

Therefore the problem is how to find Bayesian analysis which can replace classical models. However, we cannot think of replacing them with the Bayesian analysis based on numbers frequency alone, in fact this may lead to erroneous results.

Using such procedures it may appear that the banal sequences, which are not random, such as  $\{z_i = (i \bmod m)/m\}_{i \in \mathbb{N}^*}$ , look better than others. These drawbacks, however, are not sufficient for refusing the Bayesian approach.

## 2. BAYESIAN ANALYSIS

In order to check the randomness of pseudorandom sequences from a bayesian viewpoint, it is suitable to replace each classical test with a bayesian one. For example, a sample randomness check can be done by replacing each of the eleven quoted tests with a bayesian analysis.

Therefore, the following general procedure is proposed.

From the pseudorandom numbers finite sequence  $\underline{z} = \{z_1, z_2, \dots, z_n\}$ , obtained as shown in Par. 1, another one of the kind:

$$T = \{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_{n-r}\}$$

comes out, where  $r$  is a suitable positive integer,  $r < n$ , with the  $\underline{u}_k$  vectors of  $\mathbb{R}^k$ ,  $k \geq 1$ , functions of the vector  $(z_1, z_2, \dots, z_n) \in \mathbb{R}^n$  and realizations of the  $k$ -dimensional random variables  $\underline{U}_k$  which are equidistributed and independents.

The  $\underline{U}_k$  depend on certain parameters, and for their suitable values, they

have the same distribution as those requested by the classical test replaced.

After all suppose that:

- (1) the vectors  $\underline{u}_i$  are realizations of random variables  $\underline{U}_i^{(\alpha_1, \alpha_2, \dots, \alpha_n)}$  which are equidistributed, independent and functions of the parameters  $(\alpha_1, \alpha_2, \dots, \alpha_n)$ ;
- (2) in ideal conditions of randomness, the parameters  $\alpha_1, \alpha_2, \dots, \alpha_n$  take the values  $\mu_1, \mu_2, \dots, \mu_n$ .

Let  $A$  be the set of the values taken by the parameter  $\underline{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n)$ . Suppose that on a suitable subalgebra of  $\mathcal{P}(A)$  to which belong all the elementary events  $\{a\}$ , with  $a \in A$ , a comparative probability has been assigned by a relation of "not more possible" (see i.e. Scozzafava (1984), [13], and Maturo (1989), [9]).

Suppose, moreover, that, being  $\mathcal{F}$  the collection of finite subsets of  $A$ , a positive real function  $f$ , defined in  $A$ , and called pseudodensity, has been assigned.

The function  $f$  is strictly compatible with the comparative probability definition, being such that, for each pair of events of  $\mathcal{F}$ ,  $E_1 = \{a_1, a_2, \dots, a_n\}$ ,  $E_2 = \{b_1, b_2, \dots, b_m\}$ ,  $a_i \in A$ ,  $b_j \in A$ ,  $i=1, 2, \dots, n$ ,  $j=1, 2, \dots, m$ , it follows:

$$\sum_{i=1}^n f(a_i) \leq \sum_{j=1}^m f(b_j) \Leftrightarrow E_1 \text{ is not more possible than } E_2. \quad (2.1)$$

Let us consider two possibilities:

(a)  $A$  is a countable set,  $A = \{a_1, a_2, \dots, a_n, \dots\}$ ;

(b)  $A$  is a measurable  $\mathbb{R}^n$ -set with non-zero measure, and  $\int_A f(\underline{\alpha}) d(\underline{\alpha})$  exists, being either finite or not.

If (a) is true compute the sum of the series  $\sum_{i=1}^{\infty} f(a_i)$ .

If this sum is finite and equals to a real number  $M$ , then being:  $p(a_i) = f(a_i)/M$ , the function:  $p: a_i \in A \rightarrow p(a_i)$  is a probability.

If (b) is true and  $\int_A f(\underline{\alpha}) d(\underline{\alpha})$  is a finite real number  $M$ , then:  $p(\underline{\alpha}) = f(\underline{\alpha})/M$ , is probability density function (pdf).

In the following the symbol  $\int_A f(\underline{\alpha}) d(\underline{\alpha})$  will indicate also:  $\sum_{i=1}^{\infty} f(a_i)$ , and the expression "probability density function" to name also the probabilities in the (a) case.

In many papers R. Scozzafava (see i.e. [13]), has shown that the Bayes theorem, valid for prior distributions given by probabilities or probability density functions can be generalized to the case in which the prior distribution is simply given by a pseudodensity.

In the case at hand, if  $f(\underline{\alpha})$ ,  $\underline{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_n) \in A$ , is the prior pseudodensity, and  $p(\underline{u}/\underline{\alpha})$  is the pseudodensity of  $\underline{U} = (U_1, U_2, \dots, U_n)$  conditional on  $\underline{\alpha}$ , the

generalized Bayes theorem takes up the form:

$$g(\underline{\alpha}/\underline{u}) = k f(\underline{\alpha}) p(\underline{u}/\underline{\alpha}) \quad (2.2)$$

where  $k$  is a function of  $\underline{u}$  and  $g(\underline{\alpha}/\underline{u})$  is the posterior pseudodensity.

If  $g(\underline{\alpha}/\underline{u})$  is a pdf it then follows:

$$k = \frac{1}{\int_A g(\underline{\alpha}/\underline{u}) d\underline{\alpha}}.$$

By applying this formula (2.2), the problem is to estimate if  $g(\underline{\alpha}/\underline{u})$  "aims to help" the value  $\underline{\mu}=(\mu_1, \mu_2, \dots, \mu_h)$ .

For this tree conventional operative criteria can be followed:

### 1. Criterion of the distance of the absolute maximum of $g$ from the ideal point $\underline{\mu}$

The extreme absolute point  $\underline{\beta}$  of the function  $g(\underline{\alpha}/\underline{u})$  can be identified, under the hypothesis of existence and uniqueness, and then the distance between  $\underline{\beta}$  and  $\underline{\mu}$  can be evaluated. According to the Bayesian analysis, the sequences with a minor distance are to be preferred.

The procedure then requires:

a) the identification the collection of the lines passing through  $\underline{\mu}$ :

$$\begin{cases} x_1 = \mu_1 + \tau_1 t \\ x_2 = \mu_2 + \tau_2 t \\ \dots\dots\dots \\ \dots\dots\dots \\ x_h = \mu_h + \tau_h t \end{cases}, t \in \mathbb{R}$$

with  $\tau_1, \tau_2, \dots, \tau_h$  satisfying the condition:

$$\tau_1^2 + \tau_2^2 + \dots + \tau_h^2 = 1.$$

This means that for  $t=0$  we obtain the point  $\underline{\mu}$  and that  $|t|$  is equal to the distance of the point  $\underline{x}=(x_1, x_2, \dots, x_h)$  from  $\underline{\mu}$ .

b) The search of the extreme point of  $g$  on a suitable number of such lines by solving problems with one variable functions and by comparing the outcomes obtained. If  $g$  is a regular function,  $h$  directions pairwise orthogonals

can be sufficient.

c) Being  $\mu^{(n)}$  the extreme point of the constriction of  $g$  at the union of the considered lines (if there are many extreme points, the one with the smaller  $|t|$ , will be considered), assume a positive number "small"  $\sigma$  and consider the distance  $\delta^{(n)}$  between  $\mu^{(n)}$  and  $\mu$ .

If  $\delta^{(n)} < \sigma$  the generator is considered "good" with respect to the adopted criterion, but, in order to "accept" it, further analysis must be carried out, where further factors of randomness are taken into consideration.

## 2. Criterion of probability in the intervals or in the circles with center $\mu$

Let  $g(\alpha/\underline{u})$  be a probability density function.

Fixed either a suitable interval or circle  $I$ , with center  $\mu$ , calculate the probability that  $\alpha$  belongs to  $I$ . According to the bayesian analysis the sequences with a major probability are preferred.

## 3. Criterion of the confidence interval or confidence circle

Fixed a level of probability  $\theta$  and calculated the extreme point  $\beta$  of the function  $g(\alpha/\underline{u})$  we determine an interval or circle  $I_\theta$  with center  $\beta$  such that the probability that  $\alpha$  belongs to  $I_\theta$  is equal to  $\theta$ .

It has to be admitted that the sequence  $\underline{u}$  is pseudorandom, according to the proceeding analysis and at confidence level  $\theta$ , if and only if  $\theta \in I_\theta$ .

Let us consider some of such analyses:

**1. Bayesian analysis of the frequencies;** let's  $\underline{u}_i = z_i$ , for each  $i \in \{1, 2, \dots, n\}$ ;

**2. Bayesian analysis of the pairs;** for each  $i \in \{1, 2, \dots, n-1\}$  let's  $\underline{u}_i = [z_i, z_{i+1}]'$ . It results:  $r=1$ ;

**3. Bayesian analysis of the k-ple;** it is a generalization of the previous analyses. Let's  $\underline{u}_i = [z_i, z_{i+1}, \dots, z_{i+k-1}]'$ , for each  $i \in \{1, 2, \dots, n-k+1\}$ . It results:  $r=k-1$ ;

**4. Bayesian analysis of the runs;** consider  $m$  sequences  $\underline{z}^j = \{z_1^j, \dots, z_n^j\}$  and suppose that for each  $i$  and  $j$   $z_i^j \neq z_{i+1}^j$  (it is in practice always true). Assume:

$$\underline{u}_{ij} = \begin{cases} 0 & \text{for } i > 1 \text{ and } z_i^j < z_{i+1}^j < z_{i+2}^j \text{ or } z_i^j > z_{i+1}^j > z_{i+2}^j \\ 1 & \text{otherwise} \end{cases}$$

for each  $i \in \{1, 2, \dots, n-2\}$  and for each  $j \in \{1, 2, \dots, m\}$ .

For each sequence  $\underline{z}$  the number (called runs number)

$$v_j = \sum_{i=1}^n u_{ji}$$

can be considered. These numbers can be considered as independents.

The ideal distribution of the  $v_j$  (see i.e. A. Rizzi (1977), [10]) is the gaussian one, with mean  $(2n-1)/3$  and variance  $(16n-29)/90$ .

The parameters on which the inference procedure is made are the mean  $\theta$  and the variance  $\sigma^2$ .

Assuming  $\underline{\alpha}=(\theta, \sigma)$ ,  $\underline{v} = (v_1, v_2, \dots, v_m)$ , the relation (2.2) is replaced by:

$$g(\underline{\alpha}/\underline{v}) = k f(\underline{\alpha}) p(\underline{v}/\underline{\alpha}).$$

The Bayesian analysis, illustrated in this work, equivalent to the frequency classical test, can be described in the following way:

(1) let us consider the hypothesis  $H_0$  as an element of a collection of hypotheses  $(H_\alpha)_{\alpha \in A}$ , where  $A$  is a set of indexes, such that for a certain value  $\mu$  of  $A: H_\mu = H_0$  then results. Then, in a subjective way and following suitable criteria, let us assign, to each hypothesis  $H_\alpha$ , the value  $f(\alpha)$ ,  $\alpha \in A$ , of a probability density function defined in  $A$  or, more generally, of a pseudodensity.

(2) Starting from a given sequence  $\underline{z}=\{z_1, z_2, \dots, z_n\}$  of pseudorandom numbers varying between  $[0,1)$ , calculate the likelihoods  $p(\underline{z}/H_\alpha)$ ,  $\alpha \in A$ ;

(3) using the Bayes formula

$$g(H_\alpha/\underline{z}) = k f(H_\alpha) p(\underline{z}/H_\alpha), \quad (2.3)$$

with  $k$  function only of  $\underline{z}$ , calculate the posterior probability density function (or more generally, the pseudodensity);

(4) by suitable conventional criteria, for example 1, 2 or 3, consider if the hypothesis  $\alpha=\mu$  is preferred.

Starting from the  $H_0$  hypothesis of  $Z_i$  independence and equidistribution, it follows that each sequence  $S'$  obtained as a permutation of  $\underline{z}$ , originates the same likelihoods and, therefore, the same  $g$  values.

This implies that the Bayes theory **gives information only about the frequencies of the  $z_i$  values taken by the  $Z_i$ , and therefore it can replace only the frequency classical test.**

However, such Bayesian analysis is just one particular case of those we have considered in the  $\underline{u}=z_i$  hypotheses.

Assuming other hypotheses for the  $\underline{u}$ , we obtain further Bayesian analysis which can replace further classical tests.

Now an example of Bayesian analysis based on frequencies will be illustrated.

### 3. AN EXAMPLE OF BAYES ANALYSIS AS FREQUENCY TEST

Assume each random variable  $Z_i$ , ( $i=1, \dots, n$ ), varying in the interval  $[0,1)$ , and distributed as a Beta one, with parameters:  $a, b > 0$ . The probability density function is then:

$$p(z; a, b) = \begin{cases} [1 / B(a, b)] z^{a-1} (1-z)^{b-1}, & \text{for } z \in (0,1) \\ 0 & \text{for } z \notin (0,1) \end{cases} \quad (3.1)$$

where  $B(a, b) = \int_0^1 z^{a-1} (1-z)^{b-1} dz$

The choice can be justified accordingly to the following points:

- (i) the Beta distribution varies in the interval  $(0,1)$ , like any element of the pseudorandom number sequence;
- (ii) assuming a determinated set of values for the parameters ( $a=b=1$ ), the Beta law is trasformed in the continuous uniform distribution, as it happens following null hypothesis.

Since the  $a$  and  $b$  parameters of the Beta distribution are unknown, they can be thought as random numbers on which the statistical inference is drawn, with the aim of obtaining a posterior probability density function.

In the inference procedure, the examined parameters are therefore collected in a random vector  $\underline{\theta}=(a,b)$ .

As a prior distribution for each of the two parameters, the Gamma law with two parameters  $\tau, \mu > 0$ , can be assumed whose pdf is expressed by:

$$h(x; \tau, \mu) = \begin{cases} [\tau / \Gamma(\mu)] e^{-\tau x} (\tau x)^{\mu-1}, & \text{for } x > 0 \\ 0 & \text{for } x < 0 \end{cases} \quad (3.2)$$

If the two components of  $\underline{\theta}$  can be considered as independent, the probability density function of the random vector  $\underline{\theta}=(a,b)$  is the following one:

$$f(a, b; \tau, \mu) = [\tau^\mu / \Gamma(\mu)] e^{-\tau a} a^{\mu-1} [\tau^\mu / \Gamma(\mu)] e^{-\tau b} b^{\mu-1}, \quad (3.3)$$

with  $(a, b) \in (0, +\infty) \times (0, +\infty)$ .

The partial derivatives of the function  $f$  are continuous in the set:  $A = (0, +\infty) \times (0, +\infty)$ ; then the extreme points correspond to the ones that make nul these derivatives. It follows therefore:

$$\frac{\partial f}{\partial a} = 0 \text{ for } a = \frac{\mu-1}{\tau}, \quad \frac{\partial f}{\partial b} = 0 \text{ for } b = \frac{\mu-1}{\tau} \quad (3.4)$$

Then, only one extreme point of  $f$  function exists, this being the point:  $P = ((\mu-1)/\tau, (\mu-1)/\tau)$ .

It is therefore:

$$\begin{aligned} \frac{\partial^2 f}{\partial a^2} &= \left[ (\tau^\mu / \Gamma(\mu)) \right]^2 b^{\mu-1} e^{-\tau b} e^{-\tau a} a^{\mu-3} [-2\mu(\mu-1) + \mu^2 a^2 + (\mu-1)(\mu-2)] \\ \frac{\partial^2 f}{\partial b^2} &= \left[ (\tau^\mu / \Gamma(\mu)) \right]^2 a^{\mu-1} e^{-\tau a} e^{-\tau b} b^{\mu-3} [-2\mu(\mu-1) + \mu^2 b^2 + (\mu-1)(\mu-2)] \\ \frac{\partial^2 f}{\partial a \partial b} &= \left[ (\tau^\mu / \Gamma(\mu)) \right]^2 [(\mu-1)a^{\mu-2} e^{-\tau a} - \tau e^{-\tau a} a^{\mu-1}] b^{\mu-1} e^{-\tau b} [(\mu-1)b - \tau] \end{aligned}$$

Assuming that the partial derivatives are equal to zero if valuated in  $(1,1)$ , it results that:

$$\tau = \mu - 1 \quad (3.5)$$

A direct consequence of this hypothesis is that:

$$\frac{\partial^2 f}{\partial a^2} < 0, \quad \frac{\partial^2 f}{\partial b^2} < 0, \quad \frac{\partial^2 f}{\partial a \partial b} = 0$$

and therefore the Hessian matrix:

$$H = \begin{bmatrix} \frac{\partial^2 f}{\partial a^2} & \frac{\partial^2 f}{\partial a \partial b} \\ \frac{\partial^2 f}{\partial a \partial b} & \frac{\partial^2 f}{\partial b^2} \end{bmatrix}$$

is negative definite. Therefore  $P$  is a maximum for  $f$ , and this hypothesis corresponds to substantiate the null hypothesis:  $a=1, b=1$ .

Denoting by  $p(\underline{z}/(a,b))$  the pdf of  $\underline{Z}=(Z_1, Z_2, \dots, Z_n)$ , conditional on  $\theta=(a,b)$ , according to the Bayes theorem, it follows therefore:

$$g((a,b)/\underline{z}) = k f(a,b; \tau, \mu) p(\underline{z}/(a,b)) \quad (3.6)$$

where, if  $g((a,b)/\underline{z})$  is a pdf,

$$k = \frac{1}{\iint_A g((a,b)/\underline{z})} da db. \quad (3.7)$$

According to the independence condition:

$$\begin{aligned} p(\underline{z}/(a,b)) &= \prod_{i=1}^n p(z_i/(a,b)) = \\ &= [\Gamma(a+b)/\Gamma(a)\Gamma(b)]^n (z_1 z_2 \dots z_n)^{a-1} [(1-z_1)(1-z_2)\dots(1-z_n)]^{b-1}. \end{aligned}$$

Therefore, considering the relation (3.5), it follows that:

$$\begin{aligned} g((a,b)/\underline{z}) &= k [\tau^\mu / \Gamma(\mu)]^2 (ab)^\tau e^{-\tau(a+b)} * \\ &* [\Gamma(a+b)/\Gamma(a)\Gamma(b)]^n (z_1 \dots z_n)^{a-1} [(1-z_1)\dots(1-z_n)]^{b-1}. \end{aligned} \quad (3.8)$$

Let assume that  $\theta$  has a uniform distribution. This can be derived interpreting the relation (3.3) as a pseudodensity.

Therefore, by assuming two arbitrary points, belonging to  $A$ ,  $(a_1, b_1)$  and  $(a_2, b_2)$ , calculate the limit:

$$\lim_{\tau \rightarrow 0} \frac{f(a_1, b_1; \tau, \mu)}{f(a_2, b_2; \tau, \mu)}$$

It results equal to:

$$\begin{aligned} \lim_{\tau \rightarrow 0} \frac{[\tau^\mu / \Gamma(\mu)] e^{-\tau a_1} a_1^{\mu-1} [\tau^\mu / \Gamma(\mu)] e^{-\tau b_1} b_1^{\mu-1}}{[\tau^\mu / \Gamma(\mu)] e^{-\tau a_2} a_2^{\mu-1} [\tau^\mu / \Gamma(\mu)] e^{-\tau b_2} b_2^{\mu-1}} = \\ = \left[ \frac{(a_1 b_1)}{(a_2 b_2)} \right]^{\mu-1}. \end{aligned} \quad (3.9)$$

The limit of the pseudodensity expressed by (3.3), is, a part from a costant:

$$f(a,b; 0,\mu) = (ab)^{\mu-1}. \quad (3.10)$$

According to the relation (3.5), being  $\tau=0$ , it then results:  $\mu=1$ . The limit (3.9) then equals 1, and the pseudodensity (3.10) is the uniform one.

It is easy to derive that the one expressed by the (3.10) is not a pdf. Infact, being  $\mu>0$ , it follows that:

$$\iint_A (ab)^{\mu-1} da db = +\infty.$$

Nonetheless, the Bayes Theorem (3.6) is valid altogether, also if the condition (3.7) is not satisfied.

In the particular case:  $\tau=0$ , assuming  $f(a,b; \tau,\mu)$  as the pseudodensity, expressed by the relation (3.10) it results that:

$$f(a,b; 0,\mu) = (ab)^{\mu-1}$$

and the (3.8) is equal to:

$$g((a,b)/\underline{z}) = k (ab)^{\mu-1} [\Gamma(a+b) / \Gamma(a)\Gamma(b)]^n * \\ * (z_1 z_2 \dots z_n)^{a-1} [(1-z_1)(1-z_2) \dots (1-z_n)]^{b-1}. \quad (3.11)$$

If the (3.5) is valid, the (3.11) then reduces to:

$$g((a,b)/\underline{z}) = k [\Gamma(a+b) / \Gamma(a)\Gamma(b)]^n * \\ * (z_1 \dots z_n)^{a-1} [(1-z_1) \dots (1-z_n)]^{b-1}. \quad (3.12)$$

The numerical application and its results of this procedure based on the criterion of the distance of the absolute maximum of  $g$  from the ideal point  $\underline{\mu}$  can be found in G. Di Biase and A. Maturo (1990), [5].

## REFERENCES

1. B. Baldessari (1987). *Aspetti probabilistici della crittografia*, Atti del I Simposio Nazionale su "Stato e Prospettive della Ricerca Crittografica in Italia", pp. 9-21.
2. N. Cera e A. Maturo (1983). *Confronto fra alcuni generatori di numeri pseudocasuali*, Facoltà di Architettura, Pescara.

3. N. Cera e A. Maturò (1983). *Generazione di numeri pseudocasuali per mezzo di relazioni di ricorrenza in campi di Galois*, Facoltà di Architettura, Pescara.
4. N. Cera e A. Maturò (1990). *Analisi della bontà di alcuni generatori di numeri pseudocasuali per la cifratura dei messaggi e la simulazione*, Ratio Mathematica, 2, pp. 83-86.
5. G. Di Biase e A. Maturò (1990). *Su un'analisi bayesiana per la verifica di casualità di successioni pseudorandom: software applicativo ed interpretazione dei risultati*. Atti del Convegno "Classificazione e analisi dei dati, Metodi, Software, Applicazioni", 11-12 ott. 1990, Pescara, pp. 115-129.
6. D.E. Knuth (1969). *The art of Computer programming vol. 2*, Addison Wesley, London.
7. A. Maturò (1989). *Numeri pseudocasuali*, Libreria dell'Università, Pescara.
8. A. Maturò e A. Piscione (1990). *Probabilità e statistica con il calcolatore: problematiche di carattere logico ed operativo*, Metron, vol. XLVIII, n. 14, pp. 509-532.
9. A. Maturò (1989). Probabilità finitamente additive a valori nel campo delle serie bilatere, Rendiconti di Matematica VII, 9, pp. 67-85.
10. A. Rizzi (1977). *Generazione di distribuzioni statistiche mediante un elaboratore elettronico*, Istituto di Statistica e Ricerca sociale C. Gini, Roma.
11. A. Rizzi (1989). *Verifiche di Pseudo-Casualità in Crittografia*, Atti del 2° Simposio Nazionale su "Stato e Prospettive della Ricerca Crittografica in Italia", pp. 3-21.
12. R. Scozzafava (1989). *La probabilità soggettiva e le sue applicazioni*, Masson, Milano.
13. R. Scozzafava (1984). *A Survey of Some Common Misunderstandings Concerning the Role and Meaning of Finitely Additive Probabilities in Statistical Inference*, Statistica, 44, pp. 21-45.
14. R.C. Tausworthe (1965). *Random numbers generated by linear recurrence modulo two*, Mathematics of Computation, 19.

## ON STATIONARY MODES OF NONLINEAR DIELECTRIC SLAB STRUCTURES: A NEW MATHEMATICAL APPROACH

R. Lupini, M.G. Messia (\*)

### INTRODUCTION

The amplitude  $E(x)$  of stationary T.E. modes propagating in nonlinear dielectric slab structures obey the following nonlinear ordinary differential equation [1, 2, 3, 4]:

$$E'' + (-\beta^2 + \epsilon(x, E))E = 0 \quad (1)$$

where  $x$  ranges in  $(-\infty, +\infty)$ , the prime denotes differentiation with respect to  $x$ ,  $\beta$  is the wave number in a direction orthogonal to  $x$ ,  $\epsilon(x, E)$  is the nonlinear permittivity, depending both on  $x$  and  $E$ . In (1) the lengths have been non dimensionalized with respect to the free space wavelength.

Solutions to eq. (1) representing guided waves must also satisfy the asymptotic conditions at infinity

$$\lim_{|x| \rightarrow +\infty} E, E' = 0 \quad (2)$$

For a single slab extending in the  $x$ -range  $(-a, a)$ , the form typically taken by  $\epsilon(x, E)$  is [1].

---

(\*) Dipartimento di Matematica, "Vito Volterra",  
Facoltà di Ingegneria - Università di Ancona

$$\varepsilon(x, E) = \varepsilon_{1,2}^0 + g_{1,2}(|E|)$$

where the indices 1,2 refer to the ranges  $|x| > a$  and  $|x| < a$ , respectively, and  $\varepsilon_{1,2}^0$  are constants;  $g_{1,2}(|E|)$  are non decreasing (non increasing) functions of  $|E|$ , such that  $g_{1,2}(0)=0$ , representing the effect of focussing (defocussing) nonlinear polarization of the media. At the interfaces between the media 1 and 2, that is at  $x=\pm a$ ,  $E$  and  $E'$  must be continuous.

The linear case, as obtained by setting  $g_{1,2}=0$  in eq. (1), reduces to a linear eigenvalue problem that admits solutions only for discrete values of  $\beta$ , when  $\gamma_1 = b^2 - \varepsilon_1^0 > 0$  and  $\gamma_2 = \beta^2 - \varepsilon_2^0 < 0$ . On the contrary, the nonlinear problem exhibits a totally different class of solutions, for any  $\beta$ , which we shall study in the extreme case when the corresponding linear problem has no solution, that is when  $\gamma_1 > \gamma_2 > 0$ ; we shall also assume that  $0 < g_1 < g_2$ , that  $g_{1,2}$  is monotone increasing (focussing nonlinearity), and  $\gamma_1 < \sup g_1$ .

Qualitative properties of the solutions will be pointed out making use of phase plane analysis of the structure of the orbits of the dynamical system associated with (1), a technique which has been already applied to nonlinear eigenvalue problems in bounded domains arising in population dynamics and reaction diffusion equations [5], [6].

## QUALITATIVE PROPERTIES OF THE SOLUTIONS

Let us consider the two plane dynamical systems

$$\begin{cases} u' = v \\ v' = (\gamma_1 - g_1(|u|))u \end{cases} \quad (1a)$$

and

$$\begin{cases} u' = v \\ v' = (\gamma_2 - g_2(|u|))u \end{cases} \quad (1b)$$

where  $u$  represents  $E$ . It is clear that any solution of (1) is composed of two pieces of orbits of (1a) issuing and entering  $(0,0)$  matched at  $x=\pm a$  by a piece of orbit of (1b) in a "time" interval  $2a$ .

We remark that by reflection symmetry of the slab structure around  $x=0$ , if  $u(x)$  is a solution, then  $u(-x)$  and  $-u(-x)$  are solutions, therefore when in the following we shall speak of uniqueness, it will be meant uniqueness apart from the change of sign of  $u$  of  $x$  or of both.

Assuming that  $g_{1,2}$  are Lipschitz continuous, the qualitative structure of the

orbits of system (1a) is represented in figure (1).

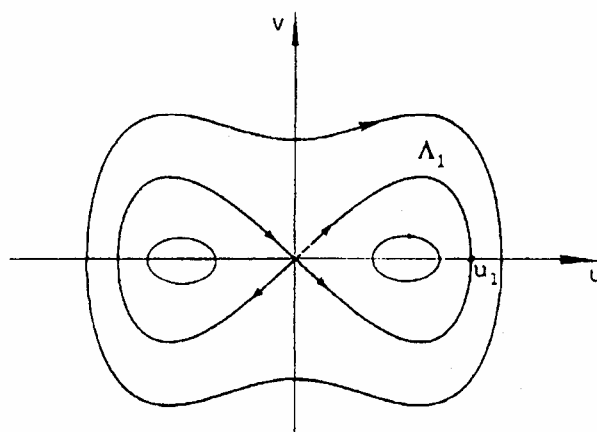


Fig. 1

Note the homoclinic loop  $\Lambda_1$  whose branches issuing and entering  $(0,0)$  provide the pieces of solutions of eq. (1) for  $|x| > a$  that satisfy the asymptotic conditions at infinity.

On the other hand, the qualitative structure of the orbits of system (1b) is represented in figure (2), where also the homoclinic loop  $\Lambda_1$  is reported. The conditions  $\gamma_1 > \gamma_2 > 0$  and  $0 < g_1 < g_2$  guarantee that the second homoclinic loop  $\Lambda_2$  is inside the first one  $\Lambda_1$ . It is clear from the above figure that the solutions of problem (1) (2) can be made to correspond in a one to one manner to the pieces of periodic orbits of (1b) connecting  $\Lambda_1$  with itself in a 'time' interval  $2a$ . This can only be achieved by means of periodic orbits of (1b) outside the homoclinic loop  $\Lambda_2$  and crossing the  $u$  axis in the range  $(u_2, u_1)$ , where  $(u_2, 0)$  and  $(u_1, 0)$  are the intersections of  $\Lambda_2$  and  $\Lambda_1$  respectively with the  $u$  axis.

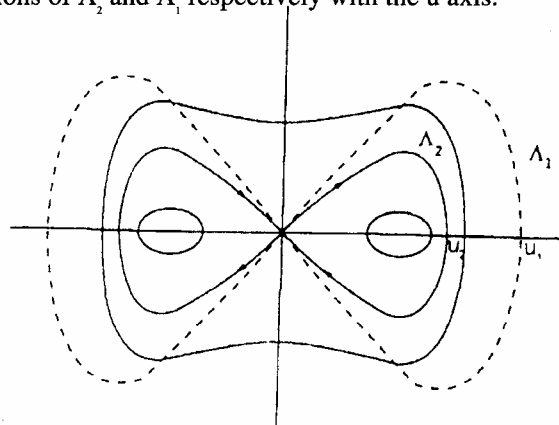


Fig. 2

We shall show that any periodic orbit, say  $P_{\bar{u}}$ , through  $(\bar{u}, 0)$ , with  $u_2 < \bar{u} < u_1$ , intersects  $\Lambda_1$  at a single point in the quadrant  $u > 0, v > 0$ . In fact we note first that the smooth functions

$$V_{1,2}(u) = \int_0^u (g_{1,2} - \gamma_{1,2}) du, \quad \text{by the conditions on } \gamma_{1,2} \text{ and } g_{1,2}$$

stated above, take the form qualitatively reproduced in fig. (3). In particular  $V_2 > V_1$  except at  $0 = (0, 0)$ .

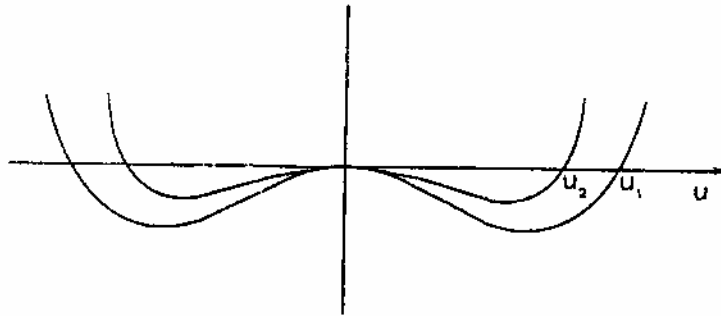


Fig. 3

The homoclinic loop  $\Lambda_1$  satisfies the equation

$$\frac{v^2}{2} + V_1(u) = 0$$

while any periodic orbit  $P_{\bar{u}}$ , outside  $\Lambda_1$  satisfies  $\frac{v^2}{2} + V_2(u) = V_2(\bar{u}) > 0$ , with  $\bar{u} > u_2$ . The intersections of  $P_{\bar{u}}$  with  $\Lambda_1$  are then given by

$$V_2(u) - V_1(u) = V_2(\bar{u}) \quad (3)$$

Now, as  $V_2(u) - V_1(u)$ , and  $V_2(\bar{u})$  are monotone increasing for positive values of their arguments, it follows that for any  $\bar{u} \in (u_2, u_1)$  equation (3) has one positive solution, say  $h(\bar{u})$ . Moreover it is easy to see that  $h(\bar{u}) < \bar{u}$ ,  $\lim_{\bar{u} \rightarrow u_2} h(\bar{u}) = 0$ ,  $\lim_{\bar{u} \rightarrow u_1} h(\bar{u}) = u_1$  and  $h'(\bar{u}) > 0$ .

Let us  $\Lambda_1^{ij}$  the piece of  $\Lambda_1$  belonging to the quadrant of the  $(u,v)$ -plane corresponding to the set of signs  $i,j \in \{+,-\}$ ; moreover let us denote by  $T(\bar{u})$  the period of  $P_{\bar{u}}$  and let

$$\tau(\bar{u}) = \int_{h(\bar{u})}^{\bar{u}} \frac{du}{\sqrt{2(V_2(\bar{u}) - V_2(u))}}, \text{ be the time needed to connect } \Lambda_1^{++} \text{ to the } u$$

axis along  $P_{\bar{u}}$ , being  $u_2 < \bar{u} < u_1$ . We can classify the types of matchings and of solutions of problem (1) (2), into three classes

$S^{(k)}$ :  $P_{\bar{u}}$  connects  $\Lambda_1^{++}$  to  $\Lambda_1^{+-}$ ; that is

$$\sigma_k(\bar{u}) \stackrel{\text{def}}{=} \frac{k}{2} T(\bar{u}) + \tau(\bar{u}) = a, \quad k = 0, 1, 2, \dots \quad (4)$$

The corresponding solutions of problem (1) (2) will then be given by the piecewise smooth curve  $\widehat{OP} \cup P_{\bar{u}}^{(k)} \cup \widehat{PP'} \cup \widehat{P'O}$  where  $P_{\bar{u}}^{(k)}$  denotes the  $k$ -fold iterate of the periodic orbit  $P_{\bar{u}}$  (See Fig. 4 in the case  $k=0$ )

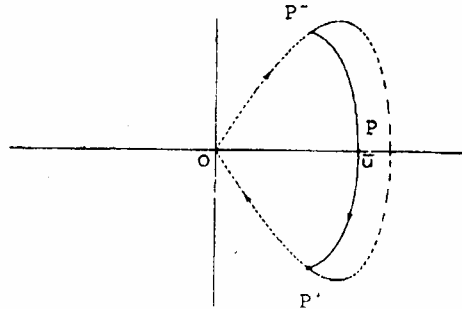


Fig. 4

Mode  $S^{(k)}$  is symmetric and has  $2k$  zeros in  $(-a, a)$ .

$A^{(k)}$ :  $P_{\bar{u}}$  connects  $\Lambda_1^{++}$  to  $\Lambda_1^{-+}$ ; that is

$$\alpha_k(\bar{u}) \stackrel{\text{def}}{=} ((2k+1)/4) T(\bar{u}) + \tau(\bar{u}) = a, \quad k = 0, 1, 2, \dots \quad (5)$$

(Figure 5 in the case  $k=0$ ). Mode  $A^{(k)}$  is antisymmetric and has  $2k+1$  zeros in  $(-a, a)$ .

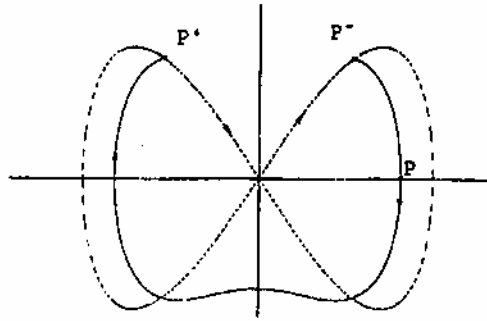


Fig. 5

$W^0$ :  $P_0$  connects  $\Lambda_1^{++}$  to  $\Lambda_1^{-}$ ; that is

$$W_k(\bar{u}) \stackrel{\text{def}}{=} ((2k+1)/4)T(\bar{u}) = a, \quad k = 0, 1, 2, \dots \quad (6)$$

Mode  $W^0$  is neither symmetric nor antisymmetric (Figure 6 in the case  $k=0$ ).

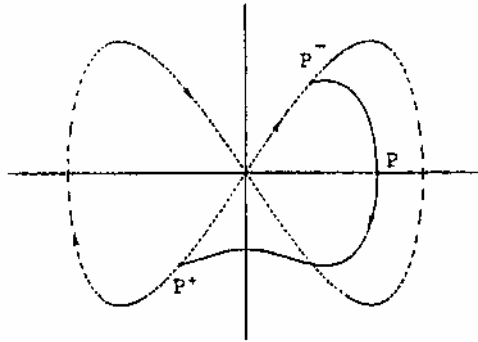


Fig. 6

In order to discuss the existence and uniqueness of the above solutions, we note that  $\tau(\bar{u})$  is monotone increasing in the range  $(u_2, u_1)$ , and  $\lim_{\bar{u} \rightarrow u_2} \tau(\bar{u}) = +\infty$ ,  $\lim_{\bar{u} \rightarrow u_1} \tau(\bar{u}) = 0$ . As a consequence mode  $S^0$  always exists and is unique.

On the other hand

$$T(\bar{u}) = 4 \int_0^{\bar{u}} \frac{du}{\sqrt{2(V_2(\bar{u}) - V_2(u))}} \text{ is monotone}$$

increasing in  $(u_2, u_1)$ , and  $\lim_{\bar{u} \rightarrow u_2} T(\bar{u}) = +\infty$ ,

$$\lim_{\bar{u} \rightarrow u_1} T(\bar{u}) \stackrel{\text{def}}{=} T_1 = 4 \int_0^{u_1} \frac{du}{\sqrt{2(V_2(\bar{u}) - V_2(u))}}$$

The qualitative graphs of the functions  $\alpha_k$ ,  $\sigma_k$  and  $w_k$  are reported in figure (7)

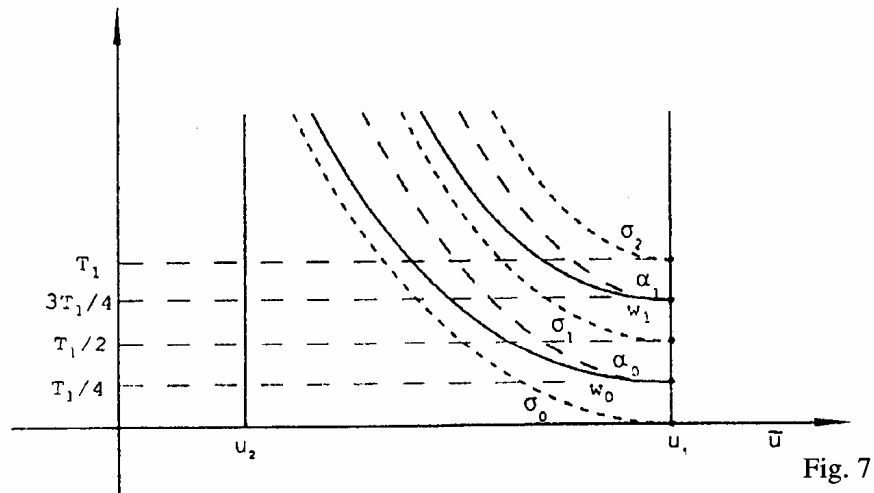


Fig. 7

If we denote by  $\bar{\sigma}_k$ ,  $\bar{\alpha}_k$  and  $\bar{w}_k$  the  $\bar{u}$  values solving equation (4) (5) and (6) respectively, it is clear that

$$\bar{\sigma}_0 < \bar{w}_0 < \bar{\alpha}_0 < \dots < \bar{\sigma}_{k-1} < \bar{w}_{k-1} < \bar{\alpha}_{k-1} < \bar{\sigma}_k < \bar{w}_k < \bar{\alpha}_k < \dots$$

whenever such solutions exist. Moreover, if one of the above solutions exists then also the previous ones in the above list exist. In particular, for  $((2k+1)/4)T_1 < a < ((k+1)/a)T_1$ , all the modes less than  $S^{(k+1)}$  exist, while if  $(K/2)T_1 < a < ((2k-1)/4)T_1$ , all the modes less than  $W^{(k)}$  exist. Therefore  $W^{(k)}$  and  $A^{(k)}$  are generated by increase of  $a$  through  $(k/2)T_1$ , while  $S^{(k)}$  is generated by increase of  $a$  through  $(k/2)T_1$ .

## CONCLUSIONS

The qualitative effects of the non-linear polarization of the media on the propagation of TE modes in dielectric slab structures has been pointed out by use of phase-plane analysis of the associated second order, ordinary differential equation. In particular symmetric structures that do not allow for the existence of linear bounded modes have been shown to admit a class of non-linear modes

of three types: symmetric, antisymmetric and neither symmetric nor antisymmetric. The analyses based on the direct numerical integration of the equation published so far [9] [10] do not seem to have pointed out this and other important pieces of information which, on the other hand, can be obtained in an almost elementary way by use of the analysis presented in this paper.

## REFERENCES

1. G.I. Stegeman, C.T. Seaton, J. Chilwell, and S.D. Smith, "*Nonlinear waves guided by thin films*", Appl. Phys. Lett., vol. 44, pp. 830-833, May 1984.
2. C.T. Seaton, J.D. Valera, R.L. Shvemaker, G.I. Stegeman, J.T. Chilwell, and S.D. Smith, "*Calculations of nonlinear TE waves guided by thin dielectric films bounded by nonlinear media*", IEEEJ. Quantum Electron., vol. QE-21, pp. 774-783, July 1985.
3. G.I. Stegeman, C.T. Seaton, F. Ariyasu, R.R. Wallis, A.A. Maradudin "*Non-linear electromagnetic waves guided by a single interface*", J. Appl. Phys. 58(7), pp. 2453-2459, October 1985.
4. G.I. Stegeman, C.T. Seaton, "*Non-linear integrated optics*", J. Appl. Phys. vol. 58, pp. R. 57-R.78 1985.
5. A. Liberatore, P. de Mottoni "*Un caso di biforcazione per un problema al contorno unidimensionale con non linearità di tipo concavo*", Rendiconti di Matematica (3) Vol. 3, Serie VII, 1983.
6. J. Smoller, "*Shock waves and Reaction-Diffusion Equations*", Springer Verlag, N.Y., 1983.
7. P. Lambkin and K.A. Shore, "*Non-linear optical waveguiding in semiconductors*", Journal de physique, colloque C2, supplement au n. 6, Tome 49, pp. 293-296, 1988.
8. P. Lambkin and K.A. Shore, "*Nonlinear semiconductor ridge waveguides*" Colloquium on Non-linear optical Waveguides, London, June 2, Paper 12, 1988.
9. K. Hayata, M. Nagai, M. Koshiba, "*Finite Element for Nonlinear Slab-Guided waves*", Preprint.
10. P. Lambkin, "*Non-linear semiconductor waveguides*", Transfer Report Nov. 1988.

# SU ALCUNE CARATTERIZZAZIONI DELLE SUCCESSIONI DI NUMERI PSEUDOCASUALI OTTENUTE A PARTIRE DA ALGEBRE DI SUPPORTO

Antonio Maturo<sup>(\*)</sup>

## 1. INTRODUZIONE

Siano  $(Z_m, +, \cdot)$  l'anello degli interi modulo  $m$ ,  $(S, \oplus, \otimes)$  un anello commutativo unitario e  $*$  una operazione esterna in  $S$  avente  $Z_m$  come dominio degli operatori.

**Definizione 1.1** Diciamo che  $S$  è un'algebra di supporto di dimensione  $n$  su  $Z_m$  se sono soddisfatte le seguenti proprietà

- (P1)  $S$  è, rispetto all'operazione esterna  $*$ , un'algebra su  $Z_m$ ;
- (P2) esiste, in  $S$ , una base  $\mathcal{B}$  formata da  $n$  elementi a cui appartiene l'unità  $u$  di  $S$ ;
- (P3) esiste, in  $S$ , un elemento  $x$  tale che gli elementi di  $\mathcal{B}$  coincidono, tranne al più l'ordine, con le potenze  $x^0 = u, x, x^2, \dots, x^{n-1}$ ;
- (P4) l'elemento  $x$  è invertibile rispetto a  $\otimes$ .

In [9] sono state studiate alcune proprietà delle algebre di supporto e delle successioni di numeri pseudocasuali ottenute da esse.

In questo lavoro si esaminano alcune caratterizzazioni di tali successioni e si presentano alcuni esempi.

---

<sup>(\*)</sup> Dipartimento di Scienze, Storia dell'Architettura e Restauro - Università "G. D'Annunzio" - Viale Pindaro 42 - Pescara.

## 2. COSTRUZIONE DI ALGEBRE DI SUPPORTO PER MEZZO DI POLINOMI SU $Z_m$

Sia  $P(y)$  l'insieme dei polinomi a coefficienti in  $Z_m$ . Esso, rispetto all'addizione e moltiplicazione in  $P(y)$  e al prodotto di un elemento di  $Z_m$  per un polinomio costituisce un'algebra commutativa su  $Z_m$  avente come unità il polinomio che si riduce all'unità di  $Z_m$ .

Sia  $f(y)$  un polinomio di grado  $n \geq 1$  e sia  $(f(y))$  l'ideale da esso generato, formato dai prodotti  $f(y) \cdot g(y)$ , al variare di  $g(y)$  in  $P(y)$ .

Sia  $S = P(y)/(f(y))$  l'insieme quoziente di  $P(y)$  rispetto all'ideale  $(f(y))$ . Indichiamo con  $[p(y)]$  la classe di equivalenza a cui appartiene il generico polinomio  $p(y)$ .

Poniamo, per ogni  $p(y), q(y)$  in  $P(y)$  e per ogni  $\alpha \in Z_m$

$$\begin{cases} [p(y)] + [q(y)] = [p(y) + q(y)] \\ [p(y)] \cdot [q(y)] = [p(y) \cdot q(y)] \\ \alpha[p(y)] = [\alpha p(y)] \end{cases} \quad (2.1)$$

Rispetto alle operazioni appena definite  $S$  è, com'è noto, una algebra commutativa unitaria, detta *algebra quoziente* di  $P(y)$  rispetto a  $(f(y))$ . In particolare  $(f(y)) = [f(y)] = [0]$ .

**Teorema 2.1** Se  $f(y)$  è un polinomio di grado  $n$  monico o comunque avente il coefficiente di  $y^n$  invertibile, allora ad ogni elemento di  $S$  appartiene uno e un solo polinomio di grado minore di  $n$ .

*Dimostrazione* Per un noto teorema, nelle condizioni ammesse per  $f(y)$ , per ogni  $g(y)$  esistono e sono univocamente determinati due polinomi  $q(y)$  ed  $r(y)$ , detti quoziente e resto della divisione di  $g(y)$  per  $f(y)$  tali che

$$\begin{cases} g(y) = f(y) \cdot q(y) + r(y) \\ \text{grado di } r(y) < \text{grado di } f(y) \end{cases} \quad (2.2)$$

Le (2.2) implicano che, per ogni  $g(y)$ , esiste un  $r(y)$ , di grado minore di  $n$ , tale che  $r(y) \in [g(y)]$ . Se vi fosse anche un  $r_1(y) \neq r(y)$  di grado minore di  $n$  tale che  $r_1(y) \in [g(y)]$  dovrebbe esistere un  $q_1(y)$  tale che  $g(y) = f(y)q_1(y) + r_1(y)$  il che è contro l'unicità della coppia  $(q(y), r(y))$  soddisfacente le (2.2).  $\square$

Osserviamo che se  $f(y) = \alpha_0 + \alpha_1 y + \dots + \alpha_n y^n$  è tale che  $\alpha_n$  è un divisore dello zero il teorema 2.1 non è più valido.

Infatti se  $\beta$  è un elemento non nullo di  $Z_m$  tale che  $\beta\alpha_n=0$  il prodotto  $\beta f(y)$  è un elemento di  $[0]$  di grado minore di  $n$  e, in genere, è diverso da 0.

Se  $f(y)$  è tale che  $\alpha_n$  è invertibile si può sempre supporre, ai fini della costruzione dell'algebra quoziente  $S$ , che  $\alpha_n=1$ . In caso contrario basta sostituire ad  $f(y)$  il polinomio  $f_1(y)=\alpha_n^{-1}f(y)$ . Esso è tale che  $(f(y))=(f_1(y))$ .

Supponiamo, dunque, da ora in poi, che il polinomio  $f(y)$  sia monico.

**Teorema 2.2** L'Algebra  $S$  soddisfa gli assiomi (P1), (P2), (P3) e, se  $\alpha_0$  è invertibile in  $Z_m$ , anche l'assioma (P4).

*Dimostrazione* Consideriamo gli elementi  $[1], [y], [y^2] \dots [y^{n-1}]$ . Essi sono indipendenti. Infatti, data una loro combinazione lineare a coefficienti in  $Z_m$

$$\beta_0[1] + \beta_1[y] + \beta_2[y^2] + \dots + \beta_{n-1}[y^{n-1}], \quad (2.3)$$

risulta

$$\begin{aligned} \beta_0[1] + \beta_1[y] + \dots + \beta_{n-1}[y^{n-1}] &= [0] \Leftrightarrow \\ \Leftrightarrow [\beta_0 + \beta_1 y + \dots + \beta_{n-1} y^{n-1}] &= [0]. \end{aligned}$$

Per il teorema 2.1 ciò implica che  $\beta_0 + \beta_1 y + \dots + \beta_{n-1} y^{n-1}$  è il polinomio nullo, ossia che  $\beta_0 = \beta_1 = \dots = \beta_{n-1} = 0$ .

Se  $[g(y)]$  è un qualsiasi elemento di  $S$ , esiste, per il teorema 2.1, un  $r(y) \in [g(y)]$  di grado minore di  $n$ .

Sia  $r(y) = \rho_0 + \rho_1 y + \dots + \rho_m y^m$ , con  $m < n$ . Allora  $[g(y)] = [r(y)] = \rho_0[1] + \rho_1[y] + \dots + \rho_m[y^m]$ , per cui  $[g(y)]$  è combinazione lineare di  $[1], [y], \dots, [y^{n-1}]$ .

L'insieme  $\mathcal{B} = \{[1], [y], \dots, [y^{n-1}]\}$  costituisce quindi una base di  $S$ .

Poiché, per ogni  $[g(y)] \in S$ , risulta, per le (2.1),  $[g(y)] \cdot [1] = [g(y)]$ ,  $[1]$  è l'elemento unitario di  $S$  e quindi vale la (P2).

Sempre per le (2.1) si ha, per ogni intero non negativo  $i$ ,  $[y]^i = [y^i]$ . Ciò implica la (P3).

Infine, se  $\alpha_0$  è invertibile in  $Z_m$ , poiché

$$[f(y)] = \alpha_0[1] + \alpha_1[y] + \dots + \alpha_n[y^n] = [0], \quad (2.4)$$

si ha

$$-\alpha_0^{-1}(\alpha_1[y] + \alpha_2[y^2] + \dots + \alpha_n[y^n]) = [1],$$

ossia

$$[y](-\alpha_0^{-1})(\alpha_1 + \alpha_2[y] + \dots + \alpha_n[y^{n-1}]) = [1],$$

il che dimostra che  $[y]$  è invertibile rispetto alla moltiplicazione in  $S$ .  $\square\square\square$

In conclusione, per  $f(y)$  monico e  $\alpha_0$  invertibile,  $S$  è un'algebra di supporto di dimensione  $n$ .

Poniamo  $x=[y]$ ,  $u=[1]$ ,  $0=[0]$ . Tale algebra ha la base  $\mathcal{B} = \{x=u, x, x^2, \dots, x^{n-1}\}$ .

La (2.4) implica, essendo  $\alpha_n=1$ ,

$$x^n = (-\alpha_0)u + (-\alpha_1)x + \dots + (-\alpha_{n-1})x^{n-1}. \quad (2.5)$$

Dalla (2.5) segue che tale algebra coincide con quella ottenuta introducendo, nel modulo  $S$  su  $Z_m$ , la moltiplicazione in  $S$  individuata dalle costanti caratteristiche

$$\beta_i = -\alpha_i, \text{ per } i = 0, 1, \dots, n-1. \quad (2.6)$$

Consideriamo l'insieme  $V = Z_m^n$  delle  $n$ -ple di elementi di  $Z_m$ . Introduciamo, in  $V$  una addizione  $\oplus$  e una moltiplicazione  $\bullet$  di un elemento  $V$  per un elemento di  $Z_m$ , ponendo, per  $x = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ ,  $y = (\beta_0, \beta_1, \dots, \beta_{n-1})$  in  $V$  e  $\omega$  in  $Z_m$ ,

$$x \oplus y = (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \dots, \alpha_{n-1} + \beta_{n-1}), \quad (2.7)$$

$$\omega \bullet x = (\omega\alpha_0, \omega\alpha_1, \dots, \omega\alpha_{n-1}) \quad (2.8)$$

Rispetto alle operazioni così definite,  $V$  è un modulo su  $Z_m$ . Esso possiede basi formate da  $n$  elementi.

Sia  $\mathcal{B} = \{x_0=u, x_1, \dots, x_{n-1}\}$  una di tali basi.

Ogni  $x \in S$  è esprimibile, in una sola maniera, nella forma:

$$x = \sum_{i=0}^{n-1} \alpha_i x_i \quad (2.9)$$

con opportuni  $\alpha_i \in Z_m$ .

Se  $x_s$  e  $x_t$  sono due elementi qualsiasi della base esistono, allora, in  $Z_m$ , degli elementi  $\gamma_{st}$  tali che:

$$x_s \bullet x_t = \sum_{i=0}^{n-1} \gamma_{st} x_i \quad (2.10)$$

Al variare di  $s, t$  si ottengono  $n^2$  elementi  $\gamma_{st}$ , detti *costanti di struttura*

dell'algebra, dai quali è possibile determinare ogni prodotto  $x \cdot y$  con  $x$  e  $y$  scelti arbitrariamente in  $S$ .

Infatti se

$$x = \sum_{i=0}^{n-1} \alpha_i x_i, \quad y = \sum_{i=0}^{n-1} \beta_i x_i, \quad (2.11)$$

risulta:

$$x \cdot y = \sum_{s=0}^{n-1} \alpha_s x_s \cdot \sum_{t=0}^{n-1} \beta_t x_t = \sum_{s=0}^{n-1} \sum_{t=0}^{n-1} \alpha_s \beta_t x_s \cdot x_t$$

e, per la (2.10)

$$x \cdot y = \sum_{i=0}^{n-1} \left( \sum_{s=0}^{n-1} \sum_{t=0}^{n-1} \alpha_s \beta_t \gamma_{sti} \right) x_i \quad (2.12)$$

Tenuto conto dei teoremi 4.1 e 4.2 di [9] possiamo precisare il teorema 4.3 di [9] enunciando il seguente

**Teorema 2.3** Sia  $V = Z_m^n$  il modulo di dimensione  $n$  su  $Z_m$  con le operazioni (2.7) e (2.8) e sia  $\mathcal{B} = \{x_0, x_1, \dots, x_{n-1}\}$  una sua base.

Le condizioni

$$x_i x_s = x_{s+1} \quad \text{per } s = 0, 1, \dots, n-2 \quad (2.13)$$

$$x^n = \sum_{i=0}^{n-1} \beta_i x_i \quad (2.14)$$

con  $\beta_0$  invertibile, definiscono, per mezzo della (2.12) un'unica algebra di supporto, tale che  $x_i = x_i^1$  per  $i=0, 1, \dots, n-1$ .

Essa è isomorfa all'algebra quoziente  $S=P(y)/(f(y))$ , dove

$$f(y) = y^n - \sum_{i=0}^{n-1} \beta_i y^i. \quad (2.15)$$

### 3. SUL PERIODO DELLE SUCCESSIONI DI NUMERI PSEUDOCASUALI OTTENUTE, CON PARTICOLARE RIFERIMENTO AI CASI $N=1$ E $N=2$

Siano  $S$  un'algebra di supporto di dimensione  $n$  su  $Z_m$ ,  $\mathcal{B} = \{x_0=u, x, x^2, \dots, x^{n-1}\}$  una sua base e

$$x^n = \sum_{i=0}^{n-1} \beta_i x^i. \quad (3.1)$$

Se  $z$  è un elemento di  $S$  invertibile rispetto alla moltiplicazione le potenze  $z^h$  costituiscono un gruppo ciclico moltiplicativo, sottogruppo del gruppo moltiplicativo  $I$  costituito dall'insieme degli elementi di  $S$  invertibili rispetto alla moltiplicazione. In particolare ciò avviene per  $z=x$ , dato che  $x$  è invertibile.

**Definizione 3.1** Sia  $z$  un elemento di  $S$  invertibile rispetto alla moltiplicazione e sia  $\psi$  una funzione di supporto.

Definisco *successione canonica* ottenuta a partire da  $z$  di  $S$  per mezzo della  $\psi$  la successione  $\{y_k = \psi(z^k)\}_{k \in \mathbb{N}_0}$  in  $Z_m$ .

Data una successione  $\{y_k\}_{k \in \mathbb{N}_0}$  di elementi di  $Z_m$ , perché essa possa essere considerata successione di numeri pseudocasuali (più precisamente trasformabile in una successione di numeri pseudocasuali per mezzo di una funzione ausiliaria) occorre che soddisfi determinati requisiti matematici e statistici, alcuni di carattere generale, altri di carattere particolare relativi ai problemi per i quali viene utilizzata la successione.

Di fondamentale importanza è il fatto che la successione sia periodica con le seguenti proprietà:

(PP1) l'antiperiodo è nullo;

(PP2) il periodo è noto e sufficientemente lungo (in pratica, per i problemi più comuni, basta che sia dell'ordine di  $10^{10}$ ).

La (PP1) è certamente soddisfatta per le successioni canoniche. Per quanto riguarda la (PP2) cominciamo con l'osservare che se  $|I|$  è il numero di elementi di  $I$ , il periodo  $\mu(z)$  del gruppo ciclico generato da un  $z \in I$  è, per il teorema di Lagrange, un divisore di  $|I|$ . Il periodo  $\lambda(z, \psi)$  della successione canonica ottenuta a partire da  $z$  per mezzo della  $\psi$  è un divisore di  $\mu(z)$  e quindi anche di  $|I|$ .

**Definizione 3.2** Sia  $z$  un elemento di  $I$ . Dico che  $z$  è *primitivo in  $S$*  se risulta  $\mu(z) = |I|$ .

Dico che  $z$  è *massimale in  $S$*  se, per ogni  $v \in I$ , risulta  $\mu(v) \leq \mu(z)$ .

I problemi più importanti relativi al periodo delle successioni canoniche sono:

- (PS1) calcolo di  $|I|$ ;
- (PS2) ricerca di valori  $\beta_0, \beta_1, \dots, \beta_{n-1}$  delle costanti caratteristiche che massimizzano  $|I|$ ;
- (PS3) ricerca di valori  $\beta_0, \beta_1, \dots, \beta_{n-1}$  delle costanti caratteristiche che rendono  $|I|$  numero primo oppure tali che i divisori di  $|I|$  abbiano proprietà assegnate;
- (PS4) ricerca degli elementi primitivi di  $S$  o, se non vi sono elementi primitivi, di quelli massimali;
- (PS5) ricerca di condizioni su  $\psi$  o sulle  $\beta_i$  tali che sia  $\lambda(z, \psi) = \mu(z)$ .

Ovviamente le successioni canoniche prese in maggiore considerazione sono quelle ottenute a partire da  $x$ . Di conseguenza ha molta importanza la determinazione di costanti caratteristiche che rendono  $x$  elemento primitivo o massimale.

Tutti i problemi sono risolti se si riesce a trovare che  $|I|$  è un numero primo. In tal caso, infatti, per ogni  $z \neq u$ ,  $\lambda(z, \psi) = \mu(z) = |I|$ .

Vediamo ora alcuni risultati relativi ai casi  $n=1$  e  $n=2$ .

Caso  $n=1$ . Come si è visto in [9], si può assumere  $S=Z_m$  e la successione  $\{x^k\}_{k \in N_0}$  si riduce alla  $\{\beta_0^k\}_{k \in N_0}$ .

Rinviano a [8] per le dimostrazioni, si vede che valgono i seguenti teoremi:

- (T1)  $|I| = \Phi(m)$ , dove  $\Phi$  è l'indicatore di Eulero-Gauss;
- (T2) se  $m$  è primo  $\Phi(m) = m-1$ . Gli elementi primitivi sono  $\Phi(m-1)$ ;
- (T3) se  $m = p^s$ , con  $p \neq 2$ ,  $\Phi(m) = m - (m/p)$ . Il numero di elementi primitivi è  $\Phi(m - (m/p))$ ;
- (T4) se  $m = 2^s$ ,  $\Phi(m) = m/2$ . Per  $s > 2$  non vi sono elementi primitivi. Gli elementi massimali hanno periodo  $\mu = m/4$  e, per  $s > 3$  sono i  $\beta_0 \in I$  tali che  $r(\beta_0) \equiv 3 \pmod{8}$  o  $r(\beta_0) \equiv 5 \pmod{8}$ ;
- (T5) se  $m = p_1^{s_1} p_2^{s_2} \dots p_r^{s_r}$ , con  $p_1, p_2, \dots, p_r$  numeri primi,  $\Phi(m) = m[1 - (1/p_1)][1 - (1/p_2)] \dots [1 - (1/p_r)]$ . Se  $\mu_1, \mu_2, \dots, \mu_r$  sono i massimi periodi ottenibili in corrispondenza dei moduli  $p_1^{s_1}, p_2^{s_2}, \dots, p_r^{s_r}$ , gli elementi massimali hanno periodo  $\mu$  uguale al minimo comune multiplo di  $\mu_1, \mu_2, \dots, \mu_r$ . Nel caso di maggior interesse, in cui  $m = 10^s$ , risulta, perciò,  $\Phi(m) = 2m/5$  e, per  $s \geq 4$ ,  $\mu = m/20$ . Per  $s \geq 5$  si trovano  $16m/100$  elementi massimali.

Caso  $n=2$ . Sia  $\mathcal{B} = \{u, x\}$ ,  $x^2 = \beta_0 u + \beta_1 x$ .

In base ai teoremi 2.1, 2.2, 2.3, gli elementi di  $S$  si possono identificare con le classi di equivalenza dei polinomi  $\alpha_0 + \alpha_1 y$  su  $Z_m$  di grado inferiore a 2, determinate dall'ideale generato dal polinomio

$$f(y) = y^2 - \beta_1 y - \beta_0 \quad (3.1)$$

e risulta  $[\alpha_1 y + \alpha_0] = \alpha_1 x + \alpha_0 u$ .

Poiché il monoide  $(S, \cdot)$  è finito, i suoi elementi non invertibili sono le classi  $[\alpha_1 y + \alpha_0]$  tali che esiste un polinomio  $\delta_1 y + \delta_0$  con  $\delta_1$  e  $\delta_0$  non entrambi nulli per cui  $[\alpha_1 y + \alpha_0] \cdot [\delta_1 y + \delta_0] = [0]$ .

Ciò avviene se e solo se esiste un  $\gamma_0 \in Z_m$  tale che

$$\gamma_0(y^2 - \beta_1 y - \beta_0) = (\alpha_1 y + \alpha_0)(\delta_1 y + \delta_0). \quad (3.2)$$

Limitiamoci, per semplicità, a considerare i casi in cui  $m$  è primo oppure  $m=p^r$  con  $p$  numero primo.

(a) Se  $\gamma_0$  è invertibile, moltiplicando, eventualmente, ambo i membri della (3.2) per  $\gamma_0^{-1}$ , si può supporre  $\gamma_0 = 1$ .

In tal caso la (3.2) equivale alle

$$\begin{cases} \alpha_1 \delta_1 = 1 \\ \alpha_0 \delta_0 = -\beta_0 \\ \alpha_1 \delta_0 + \alpha_0 \delta_1 = -\beta_1 \end{cases} \quad (3.3)$$

Si deduce che la (3.2) ammette soluzioni se e solo se  $\alpha_0$  e  $\alpha_1$  sono entrambi invertibili ed inoltre

$$f(-\alpha_0 \alpha_1^{-1}) = 0 \quad (3.4)$$

(b) Se  $\gamma_0 = 0$  la (3.2) equivale alle

$$\begin{cases} \alpha_1 \delta_1 = 0 \\ \alpha_0 \delta_0 = 0 \\ \alpha_1 \delta_0 + \alpha_0 \delta_1 = 0 \end{cases} \quad (3.5)$$

con  $\delta_0$  e  $\delta_1$  non entrambi nulli.

Le (3.5) ammettono soluzioni non banali se e solo se nè  $\alpha_1$  nè  $\alpha_0$  sono invertibili.

Infatti, se  $\alpha_1$  fosse invertibile, per la prima di esse sarebbe  $\delta_1=0$  e per la terza sarebbe  $\delta_0=0$ . Analogamente, se  $\alpha_0$  fosse invertibile, per la seconda e la terza delle (3.5) sarebbe  $\delta_1=\delta_0=0$ .

Viceversa, se nè  $\alpha_1$  nè  $\alpha_0$  sono invertibili, allora o  $\alpha_1=\alpha_0=0$ , oppure, se  $m=p^s$  con  $s>1$ , esiste un intero  $r$  tale che  $0<r<s$  e  $\alpha_0$  e  $\alpha_1$  hanno entrambi il divisore  $[p^r]$ . Nel primo caso la (3.5) è soddisfatta da ogni coppia  $(\delta_0, \delta_1)$ , nel secondo caso da tutte le coppie tali che sia  $\delta_0$  che  $\delta_1$  sono multipli di  $[p^{s-r}]$ .

(c) se  $\gamma_0$  è un divisore dello zero non nullo, ciò che può verificarsi solo se  $m=p^s$  con  $s>1$ , valgono le

$$\begin{cases} \alpha_1 \delta_1 = \gamma_0 \\ \alpha_0 \delta_0 = -\beta_0 \gamma_0 \\ \alpha_1 \delta_0 + \alpha_0 \delta_1 = -\beta_1 \gamma_0 \end{cases} \quad (3.6)$$

Escludiamo il caso in cui sia  $\alpha_0$  che  $\alpha_1$  sono non invertibili, dato che, in tali ipotesi, si è già visto che la (3.2) ammette una soluzione  $(\gamma_0, \delta_0, \delta_1)$ , con  $\gamma_0=0$ .

Moltiplicando, eventualmente, la (3.2) per un fattore invertibile si può sempre porre  $\gamma_0=[p^r]$  per un certo intero  $r$  tale che  $0<r<s$ .

Se  $\alpha_1$  è invertibile, dalle (3.6) si vede che  $\delta_0$  e  $\delta_1$  hanno entrambi  $\gamma_0$  come divisore.

Esistono, quindi, due elementi  $\delta'_0$  e  $\delta'_1$  tali che  $\delta_0=\delta'_0 \gamma_0$ ,  $\delta_1=\delta'_1 \gamma_0$ .

Poniamo  $c_0=r(\gamma_0)$ ,  $b_1=r(\beta_1)$ ,  $a_1=r(\alpha_1)$ ,  $d'_1=r(\delta'_1)$ , rispetto al modulo  $m$ .

Le (3.6) si possono scrivere

$$\begin{cases} a_1 d'_1 c_0 \equiv c_0 \pmod{m} \\ a_0 d'_0 c_0 \equiv -c_0 b_0 \pmod{m} \\ (a_1 d'_0 + a_0 d'_1) c_0 \equiv -c_0 b_1 \pmod{m} \end{cases} \quad (3.7)$$

Esse implicano le

$$\begin{cases} a_1 d'_1 \equiv 1 \pmod{m/c_0} \\ a_0 d'_0 \equiv -b_0 \pmod{m/c_0} \\ a_1 d'_0 + a_0 d'_1 \equiv -b_1 \pmod{m/c_0} \end{cases} \quad (3.8)$$

e possono scriversi nella forma (3.3) in  $Z_{m/c_0}$ .

Poiché  $m=p'$ , e  $b_0$  è primo con  $m$ , per le (3.7)  $a_0, d'_0, d'_1$  non possono essere divisibili per  $p$ , per cui  $\alpha_0, \delta'_0, \delta'_1$  sono invertibili in  $Z_m$ .

Alle medesime formule e considerazioni si perviene partendo dall'ipotesi che  $\alpha_0$  è invertibile.

Si deduce che le (3.6) ammettono soluzioni se e solo se  $\alpha_1$  e  $\alpha_0$  sono entrambi invertibili ed inoltre esiste un intero  $k$  tale che

$$f(-\alpha_0 \alpha_1^{-1}) = k[m / c_0] \quad (3.9)$$

In conclusione, quindi, la (3.2) è soddisfatta con  $\gamma_0$  divisore dello zero se e solo se  $\alpha_1$  e  $\alpha_0$  sono elementi invertibili tali che

$$f(-\alpha_0 \alpha_1^{-1}) \text{ è un divisore dello zero.} \quad (3.10)$$

Possiamo allora enunciare il seguente

**Teorema 3.1** Se  $m=p'$  con  $p$  primo, un polinomio  $\alpha_1 y + \alpha_0$  è tale che  $[\alpha_1 y + \alpha_0]$  è un divisore dello zero in  $S$  se e solo se è soddisfatta una delle seguenti condizioni

(D1)  $\alpha_1$  e  $\alpha_0$  sono entrambi invertibili in  $Z_m$  e  $f(-\alpha_0 \alpha_1^{-1})$  è nullo o è un divisore dello zero;

(D2) né  $\alpha_1$  né  $\alpha_0$  sono invertibili in  $Z_m$ .

*Esempio 3.1* Si consideri il polinomio  $f(y)=y^2-y-2$  in  $Z_m$  con  $m=3^2$ . Gli elementi di  $S$  sono 81.

Determiniamo i polinomi  $\alpha_1 y + \alpha_0$  soddisfacenti la (D1).

Posto  $h = -\alpha_0 \alpha_1^{-1}$ , si vede che  $f(h)$  è nullo o divisore dello zero con  $h$  invertibile per  $h=2,5,8$ . In corrispondenza, facendo variare  $\alpha_1$  fra i  $\Phi(9)=6$  elementi invertibili di  $Z_m$ , si ottengono 18 polinomi. Facendo variare  $\alpha_0$  e  $\alpha_1$  fra i 3 elementi non invertibili di  $Z_m$  si ottengono 9 polinomi soddisfacenti la (D2).

Segue che  $|I| = 81 - 27 = 54$ .

Poniamo  $x=[y]$ . Il periodo di  $x$  è un divisore di 54. Precisamente, essendo

$$x^3=3x+2, \quad x^6=3x+4, \quad x^9=9, \quad x^{18}=1,$$

risulta  $\mu(x) = 18$ .

*Esempio 3.2* Si consideri il polinomio  $f(y)=y^2-y-1$  in  $Z_m$  con  $m=3^2$ . Non esistono polinomi soddisfacenti la (D1). La (D2) è, ovviamente, sempre

soddisfatta da 9 polinomi.

Segue che  $|I| = 81 - 9 = 72$ .

Poniamo  $x=[y]$ . Essendo

$$\begin{aligned} x^4 &= 3x+2, & x^6 &= 8x+5, & x^8 &= 3x+4, & x^{12} &= 8, \\ x^{18} &= 8x+8, & x^{24} &= 1, \end{aligned}$$

risulta  $\mu(x) = 24$ .

*Esempio 3.3* Si consideri il polinomio  $f(y)=y^2-y-1$  e sia  $m=5$ . Risulta  $f(1)=4$ ,  $f(2)=1$ ,  $f(3)=0$ ,  $f(4)=1$ . I divisori di  $f(y)$  sono i 4 polinomi  $\alpha_i(y-3)$ , con  $\alpha_i=1, 2, 3, 4$ .

La (D2) è verificata solo per  $\alpha_1=0$  e  $\alpha_0=0$ .

Gli elementi di  $I$  sono allora  $5^2-5=20$  e il periodo di  $x=[y]$  è un divisore di 20.

Risulta  $x^2=x+1$ ,  $x^4=3x+2$ ,  $x^5=3$ ,  $x^{10}=4$ ,  $x^{20}=1$ .

L'elemento  $x$  è primitivo in  $S$ .

Prendiamo  $S=V$  e scegliamo in  $V$  la base usuale. La successione  $\{x^k\}_{k \in \mathbb{N}_0}$  si riduce alla

(1,0), (1,1), (2,1), (3,2), (0,3), (3,0), (3,3), (1,3), (4,1), (0,4), (4,0), (4,4), (3,4), (2,3), (0,2), (2,0), (2,2), (4,2), (1,4), (0,1), .....

#### 4. CASO IN CUI $m$ È PRIMO

Sia  $m$  un numero primo. Allora  $Z_m$  è un campo. Con riferimento alle notazioni utilizzate nel paragrafo 2., si deduce che

(C1)  $S=P(y)/(f(y))$  è uno spazio vettoriale su  $Z_m$ ;

(C2)  $P(y)$  è un anello euclideo e quindi anche un anello principale.

La (C2) implica che ogni  $f(y) \in P(y)$  verifica il teorema 2.1. Il fatto che  $Z_m$  è un campo implica che la condizione " $a_0$  invertibile" del teorema 2.2 si riduce alla " $a_0 \neq 0$ ".

Per il calcolo di  $|I|$  vale il seguente

**Teorema 4.1** Gli elementi di  $S-I$  sono tutti e soli quelli del tipo  $[g(y)]$  con  $g(y)$  polinomio di grado minore di  $n$  e tali che  $D(f(y), g(y))$  ha grado maggiore o uguale ad 1.

*Dimostrazione* Se  $[g(y)] \in S-I$  devono esistere un polinomio  $h(y)$  non nullo e di grado minore di  $n$  e un polinomio  $r(y)$  tali che

$$g(y) h(y) = f(y) r(y). \quad (4.1)$$

Se  $f(y)$  fosse primo con  $g(y)$ , per la (C2)  $f(y)$  sarebbe un divisore di  $h(y)$ , il che è assurdo poiché il grado di  $h(y)$  è minore di quello di  $f(y)$ .

Viceversa, se  $g(y)$  è non nullo e ha grado minore di  $n$  e  $D(f(y), g(y)) = d(y)$ , ha grado maggiore o uguale ad 1, detti  $h(y)$  e  $k(y)$  i quozienti delle divisioni di  $f(y)$  e  $g(y)$  per  $d(y)$ , essi sono non nulli e di grado minore di  $n$ .

Risulta  $g(y) \cdot h(y) = k(y) \cdot d(y) \cdot h(y) = k(y) \cdot f(y)$ . Posto  $r(y) = k(y)$ ,  $h(y)$  e  $r(y)$  soddisfano la (4.1). Allora  $[g(y)] \cdot [h(y)] = 0$  e quindi  $[g(y)] \in S-I$ .  $\diamond\diamond$

**Corollario 4.1.1** Risulta  $|I| = m^n - 1$  se e solo se  $f(y)$  è irriducibile.

*Dimostrazione* Basta osservare che le condizioni su  $g(y)$  del teorema 4.1 sono, in tal caso, soddisfatte solo se  $g(y)$  è il polinomio nullo.  $\diamond\diamond\diamond$

**Corollario 4.1.2**  $S = P(y)/(f(y))$  è un campo se e solo se  $f(y)$  è irriducibile.

*Dimostrazione* Basta osservare che ogni  $g(y)$  non nullo e di grado minore di  $n$  è tale che  $[g(y)]$  è invertibile.  $\diamond\diamond$

Nel seguito del paragrafo ammettiamo che  $m$  è primo e che  $f(y)$  è un polinomio su  $Z_m$  di grado  $n \geq 1$ . Indichiamo, inoltre, con  $k$  il numero  $m^n - 1$ .

Vale il seguente

**Teorema 4.2** Se  $f(y)$  è irriducibile, il campo  $S$  è un campo di riducibilità completa del polinomio  $y^k - 1$  su  $Z_m$ . Le radici di tale polinomio sono tutte distinte e ogni  $z \in S - \{0\}$  coincide con una di esse.

*Dimostrazione* Se  $z \in S - \{0\}$ , il periodo di  $z$  è un divisore di  $k$ , per cui  $z^k - 1 = 0$ . Il polinomio  $y^k - 1$  ha dunque, in  $S$ ,  $k$  radici distinte e poichè  $k$  è il massimo numero delle sue radici segue il teorema  $\diamond\diamond\diamond$

I problemi (PS1), (PS2) e, talvolta, (PS3) sono risolti dall'imporre che il polinomio  $f(y)$  sia irriducibile. Il problema (PS4) è, invece, risolto dal seguente

**Teorema 4.3** Se  $f(y)$  è irriducibile esistono, in  $S$ ,  $\Phi(m^n - 1)$  elementi primitivi.

*Dimostrazione* Sia  $k = q_1^{r_1} q_2^{r_2} \dots q_s^{r_s}$ , con  $q_1, q_2, \dots, q_s$  numeri primi distinti.

Il polinomio  $y^{q_i^{r_i}} - 1$  è, per ogni  $i = 1, 2, \dots, s$ , un divisore di  $y^k - 1$  ed ha quindi, per il teorema 4.2,  $q_i^{r_i}$  radici distinte. Esse formano rispetto alla moltiplicazione in  $S$  un gruppo ciclico  $C_{q_i^{r_i}}$ . Infatti, posto  $g = q_i^{r_i}$ , risulta

$$(a^g = 1 \text{ e } b^g = 1) \Rightarrow ((ab^{-1})^g = a^g(b^g)^{-1} = 1).$$

Se il massimo ordine degli elementi di  $C_i$  non fosse  $q_i^{r_i}$ , sarebbe un suo divisore  $q_i^{r_i-h}$ , con  $h$  intero positivo.

Allora si avrebbe, per ogni  $a \in C_i$ ,

$$a^{q_i^{r_i-h}} = 1$$

e quindi ogni  $a \in C_i$  sarebbe radice del polinomio  $y^{q_i^{r_i-h}} - 1$ .

Poiché quest'ultimo ha, al più,  $q_i^{r_i-h}$  radici distinte risulterebbe  $|C_i| \leq q_i^{r_i-h}$ . Ciò è assurdo in quanto  $|C_i| = q_i^{r_i}$ .

Scegliamo ora, in  $S$ , per ogni  $i$ , un elemento  $a_i \in C_i$  di massimo ordine e si consideri l'elemento  $a = a_1 \cdot a_2 \cdot \dots \cdot a_s$ .

L'ordine  $h$  di  $a$  è uguale a  $k$ . Infatti, se così non fosse, poiché  $h$  è un divisore di  $k$ , esisterebbe almeno un  $q_i$  tale che  $k/q_i$  è multiplo di  $h$ , ossia, per un certo intero  $d$ ,  $hd = k/q_i$ .

Allora sarebbe

$$a^{k/q_i} = a^{hd} = 1^d = 1$$

e, d'altra parte

$$a^{k/q_i} = a_1^{k/q_i} a_2^{k/q_i} \dots a_s^{k/q_i} = a_i^{q_i^{r_i-1}} \neq 1,$$

il che è assurdo

Gli elementi di  $C_i$  di ordine  $q_i^{r_i}$  sono, per i ragionamenti appena visti, le radici di  $y^{q_i^{r_i}} - 1$  che non sono radici di  $y^{q_i^{r_i-1}} - 1$  e quindi sono in numero di  $q_i^{r_i} - q_i^{r_i-1} = \Phi(q_i^{r_i})$ .

Allora gli elementi di  $S$  del tipo  $a = a_1 \cdot a_2 \cdot \dots \cdot a_s$ , con  $a_i$  di ordine massimo in  $C_i$ , sono

$$\Phi(q_1^{r_1}) \cdot \Phi(q_2^{r_2}) \dots \Phi(q_s^{r_s}) = \Phi(q_1^{r_1} \cdot q_2^{r_2} \dots q_s^{r_s}) = \Phi(m^n - 1). \diamond\diamond\diamond$$

Il teorema 4.3 generalizza al caso in cui  $n$  è un intero positivo qualsiasi la proprietà (T2) relativa al caso in cui  $n=1$ .

Il corollario 4.1.2 e i teoremi 4.2 e 4.3 ci assicurano che, se esiste un polinomio  $f(y)$  su  $Z_m$ , irriducibile di ordine  $n$ , allora esiste un campo  $S$ , ampliamento di  $Z_m$  che ha le seguenti proprietà:

(K1) è un campo di riducibilità completa del polinomio  $y^k - 1$  su  $Z_m$ ;

(K2) ha  $m^n$  elementi.

I teoremi di isomorfismo fra campi di riducibilità completi di uno stesso polinomio sul campo  $Z_m$  ci assicurano, inoltre, che ogni campo  $K$  che goda della proprietà (K1) è un ampliamento di  $Z_m$  formato da  $m^n$  elementi ed è isomorfo ad  $S$ .

I teoremi visti, però, non ci assicurano che effettivamente esiste, per ogni  $n$ , un polinomio  $g(y)$  su  $Z_m$  irriducibile e quindi un campo  $S$  che gode delle proprietà (K1) e (K2).

Per motivi di completezza riportiamo due teoremi che mostrano che, per ogni  $n$ , esistono un tale polinomio e un tale campo.

**Teorema 4.4** Sia  $m$  un numero primo ed  $n$  un intero positivo. Se  $S$  è un campo di riducibilità completa del polinomio, su  $Z_m$ ,  $y^k-1$ , con  $k=m^n-1$  allora

(GF1)  $S$  ha  $m^n$  elementi;

(GF2) esiste, in  $S$ , un elemento di ordine moltiplicativo  $k$ .

*Dimostrazione* Il polinomio derivato di  $y^k-1$  è  $ky^{k-1}$ . Una radice  $x$  di  $y^k-1$ , essendo diversa da zero, è tale che  $x^{k-1} \neq 0$ . Inoltre, poiché  $S$  ha caratteristica  $m$  e  $k$  è primo con  $m$  è  $kx^{k-1} \neq 0$ . Segue che le radici di  $y^k-1$  sono tutte semplici.

Indichiamo con  $T$  l'insieme di tali radici. Se  $x$  e  $z$  sono elementi di  $T$  risulta  $(xz^{-1})^k = x^k(z^{-1})^k = 1$  e quindi  $xz^{-1}$  è elemento di  $T$ .

Inoltre se  $x$  e  $z$  sono elementi di  $T \cup \{0\}$  risulta, poiché  $S$  ha caratteristica  $m$ ,

$$(x-z)^{m^n} = x^{m^n} - z^{m^n} = x-z,$$

per cui anche  $x-z$  è elemento di  $T \cup \{0\}$ . Sia  $T^* = T \cup \{0\}$ .

Allora  $T^*$  è un campo contenente tutte le radici di  $y^k-1$  e contenuto in  $S$ . Poiché  $S$  è campo di riducibilità completa di tale polinomio deve essere  $T^* = S$ .

Dato che  $T^*$  ha  $m^n$  elementi vale la (GF1).

Ragionando come nel teorema 4.3 si deduce anche la (GF2).  $\diamond\diamond\diamond$

**Teorema 4.5** Se  $m$  è un numero primo ed  $n$  è un intero positivo qualsiasi esiste un polinomio  $f(y)$  irriducibile di grado  $n$  su  $Z_m$ .

*Dimostrazione* Sia  $S$  un campo di riducibilità completa del polinomio, su  $Z_m$ ,  $y^k-1$ , con  $k=m^n-1$ .

Per il teorema 4.4 esiste, in  $S$ , un elemento primitivo  $x$ .

$S$ , essendo un ampliamento di  $Z_m$ , è uno spazio vettoriale su  $Z_m$ . Gli elementi  $1, x, x^2, \dots, x^{n-1}$  formano una base.

Infatti sono linearmente indipendenti, perché, se così non fosse,  $x$  sarebbe radice di un polinomio di grado  $n_1 \leq n-1$  e l'insieme delle potenze di  $x$ , essendo

ognuna di esse combinazione lineare di  $1, x, x^2, \dots, x^{n-1}$  sarebbe formato al più di  $m^{n-1}-1$  elementi, contro l'ipotesi che  $x$  è primitivo. Inoltre, ogni elemento di  $S$  è combinazione lineare di essi dato che  $S$  ha  $m^n$  elementi, tanti quante sono le combinazioni lineari distinte di  $1, x, x^2, \dots, x^{n-1}$ .

Siano ora  $\beta_0, \beta_1, \dots, \beta_{n-1}$  elementi di  $Z_m$  tali che

$$x^n = \beta_0 u + \beta_1 x + \dots + \beta_{n-1} x^{n-1}, \quad (4.2)$$

e si consideri il polinomio

$$f(y) = y^n - \beta_{n-1} y^{n-1} - \beta_{n-2} y^{n-2} - \dots - \beta_1 y - \beta_0. \quad (4.3)$$

Esso è irriducibile in  $Z_m$ , poiché altrimenti  $x$  sarebbe radice di una sua componente  $f_i(y)$  di grado  $n_i$  tale che  $1 \leq n_i \leq n-1$  e gli elementi  $1, x^1, x^2, \dots, x^{n-1}$  non sarebbero linearmente indipendenti.  $\diamond\diamond\diamond$

In base ai teoremi di isomorfismo fra campi di riducibilità completi dello stesso polinomio su  $Z_m$  il campo di riducibilità completa del polinomio  $y^k - 1$  con  $k=m^n-1$  è unico a meno di isomorfismi.

Per il teorema 4.5 esso può, per ogni  $n$ , pensarsi ottenuto come quoziente  $P(y)/(f(y))$  con  $f(y)$  polinomio irriducibile di grado  $n$  su  $Z_m$ .

Poiché il suo ordine è  $m^n$  esso coincide con il campo di Galois  $GF(m^n)$ .

In riferimento alle notazioni utilizzate nel teorema 4.4 e al polinomio  $f(y)$  definito dalla (4.3) un isomorfismo fra il campo  $S$  e il campo  $T=P(y)/(f(y))$  è dato dalla applicazione

$$\rho: \sum_{i=0}^{n-1} \delta_i x^i \in S \rightarrow \left[ \sum_{i=0}^{n-1} \delta_i y^i \right] \in T, \quad (4.4)$$

dove  $\delta_0, \delta_1, \dots, \delta_{n-1}$  sono generici elementi di  $Z_m$ .

In particolare, essendo  $x$  primitivo in  $S$ ,  $\rho(x)=[y]$  lo è in  $T$ .

In seguito identifichiamo elementi corrispondenti tramite la (4.4) e scriviamo, in particolare,  $x=[y]$ .

Immediata conseguenza dei teoremi 4.4 e 4.5 è il

**Teorema 4.6** Esiste, in  $P(y)$ , un polinomio irriducibile  $f(y)$  tale che, nel campo  $S=P(y)/(f(y))$ ,  $x=[y]$  è un elemento primitivo.  $\diamond\diamond\diamond$

Delle caratterizzazioni delle radici di un polinomio  $f(y)$  irriducibile in  $Z_m$  sono fornite dai seguenti

**Teorema 4.7** Se  $f(y)$  è un polinomio irriducibile di grado  $n$  ed  $S$  è il campo

di riducibilità completa del polinomio, in  $Z_m$ ,  $y^k-1$ , allora

(R1)  $f(y)$  è un divisore di  $y^k-1$  ed ha le radici distinte;

(R2) se  $z \in S$  è una radice di  $f(y)$ , allora  $1, z, z^2, \dots, z^{n-1}$  sono linearmente indipendenti.

*Dimostrazione* Per il teorema 4.2,  $S$  coincide, a meno di isomorfismi, con  $P(y)/(f(y))$ . Poniamo allora  $S=P(y)/(f(y))$  e  $x=[y]$ . I polinomi  $y^k-1$  e  $f(y)$  hanno, in  $S$ , entrambi la radice  $x$ . Il massimo comune divisore fra  $f(y)$  e  $y^k-1$ , che appartiene a  $P(y)$ , ha allora grado positivo. Poiché  $f(y)$  è irriducibile in  $Z_m$ , esso divide  $y^k-1$  e, dato che quest'ultimo ha radici distinte sono tali anche quelle di  $f(y)$ .

Sia ora  $z$  una radice di  $f(y)$ .

Se  $1, z, z^2, \dots, z^{n-1}$  non fossero linearmente indipendenti,  $z$  sarebbe radice di un polinomio  $g(y)$  a coefficienti in  $Z_m$  di grado  $n_1 < n$ . Allora  $D(f(y), g(y))$  avrebbe grado positivo e quindi  $f(y)$  non sarebbe irriducibile.  $\diamond\diamond$

**Teorema 4.8** Sia  $f(y)$  un polinomio irriducibile,  $S=P(y)/(f(y))$  e  $z$  una radice di  $f(y)$  in  $S$ . Le radici di  $f(y)$  sono le potenze

$$z, z^m, z^{m^2}, \dots, z^{m^{n-1}}. \quad (4.5)$$

Esse hanno tutte lo stesso ordine.

*Dimostrazione* Sia  $f(y) = y^n + \alpha_{n-1}y^{n-1} + \alpha_{n-2}y^{n-2} + \dots + \alpha_0$  e sia  $z$  una sua radice.

Risulta

$$\begin{aligned} 0 &= f(z) = f(z)^m = (z^m)^n + \alpha_{n-1}(z^m)^{n-1} + \dots + \alpha_1(z^m) + \alpha_0 = \\ &= (z^m)^n + \alpha_{n-1}(z^m)^{n-1} + \dots + \alpha_1(z^m) + \alpha_0 = f(z^m). \end{aligned}$$

Allora anche  $z^m$  è radice di  $f(y)$ . Per induzione si vede che sono radici tutte le (4.5). Esse sono a due a due distinte.

Infatti, se così non fosse, esisterebbero due interi  $j$  e  $i$  con  $0 \leq j < i < n$  tali che  $z^{m^j} = z^{m^i}$ .

Allora sarebbe

$$z = z^{m^n} = (z^{m^j})^{m^{n-j}} = (z^{m^i})^{m^{n-j}} = z^{m^{n+j-i}}$$

e quindi

$$z^{m^{n+j-i}} = 1.$$

Posto quindi  $q=n+j-i$ ,  $z$  sarebbe radice del polinomio  $x^{m^q}-1$ , con  $q < n$ . Allora le sue potenze, per il teorema 4.4, sarebbero elementi di un campo di ordine  $m^q$ ,

e gli elementi  $1, z, z^2, \dots, z^{n-1}$  sarebbero linearmente dipendenti, ciò che contraddice il teorema 4.7.

Poiché  $f(y)$  ha  $n$  radici, esse sono tutti e soli gli elementi (4.5).

Allora, se  $x$  e  $t$  sono due radici di  $f(y)$ , risulta per certi  $i$  e  $j$

$$x=t^{m^i}, \quad t=x^{m^j}.$$

Se  $x$  ha ordine  $p$  risulta

$$t^p=(x^{m^j})^p=(x^p)^{m^j}=1,$$

per cui l'ordine di  $t$  non supera quello di  $x$ . Scambiando i ruoli di  $x$  e  $t$  segue la seconda parte del teorema.  $\diamond\diamond$

**Definizione 4.1** Un polinomio irriducibile di grado  $n$  si dice appartenente all'ordine  $d$  se le sue radici hanno nel campo  $GF(m^n)$ , ordine moltiplicativo  $d$ .

**Definizione 4.2** Un polinomio irriducibile di grado  $n$  si dice primitivo se le sue radici hanno, nel campo  $GF(m^n)$ , ordine moltiplicativo  $k=m^n-1$ .

Il teorema 4.6 ci assicura che, per ogni  $n$ , esiste un polinomio primitivo di ordine  $n$ .

Inoltre, dal teorema 4.5 segue il

**Teorema 4.9** Un polinomio  $f(y)$  di grado  $n \geq 1$  su  $Z_m$  che ha come radice un elemento  $x$  primitivo di  $GF(m^n)$  è irriducibile e primitivo.

**Dimostrazione** Il polinomio  $f(y)$  è irriducibile. Infatti, se così non fosse,  $x$  sarebbe radice di un polinomio di grado  $n_1 < n$ . Le potenze di  $x$  sarebbero allora combinazioni lineari di  $1, x, x^2, \dots, x^{n_1-1}$  e sarebbero al più  $m^{n_1}$ . Allora, per il teorema 4.8  $f(y)$  è primitivo.  $\diamond\diamond$

Se  $f(y)$  appartiene all'ordine  $d$  ogni sua radice è radice di  $x^d-1$ , per cui  $f(y)$ , essendo irriducibile, divide  $x^d-1$ .

Poiché  $d$  deve dividere  $k=m^n-1$ , segue il

**Teorema 4.10** Un polinomio  $f(y)$  su  $Z_m$ , irriducibile e di grado  $n$ , è primitivo se e solo se non è divisore di alcun polinomio  $x^d-1$  con  $k$  divisore proprio di  $m^n-1$ .

**Teorema 4.11** Un polinomio  $f(y)$  su  $Z_m$  di grado  $n$  è irriducibile e primitivo se e solo se sono soddisfatte le seguenti condizioni:

(IP1) per ogni  $n_1 < n$  il massimo comune divisore di  $f(y)$  e  $y(y^{k_1}-1)$  con  $k_1 = m^{n_1}-1$  è uguale a 1,  
 (IP2)  $f(y)$  non divide alcun polinomio del tipo  $y^d-1$  con  $d$  divisore non banale di  $m^n-1$ .

*Dimostrazione* Se  $f(y)$  è irriducibile e primitivo le condizioni (IP1) e (IP2) sono evidenti. Viceversa, se vale (IP1),  $f(y)$  non ha fattori irriducibili di grado  $n_1 < n$ , per cui è irriducibile.

Allora la (IP2) implica che esso è primitivo.  $\diamond\diamond\diamond$

*Esempio 4.1* Riprendiamo il polinomio  $f(y) = y^2-y-1$  su  $Z_5$ .

Risulta  $k=5^2-1=24$ . Per  $n_1=1$ ,  $k_1=5-1=4$ . Per vedere se  $f(y)$  è irriducibile o riducibile, essendo il termine noto diverso da zero, si può considerare  $\delta(y)=D(f(y), y^4-1)$ . Risulta  $\delta(y)=y-3$ , per cui  $f(y)$  è riducibile.

*Esempio 4.2* Determiniamo i polinomi  $f(y)=y^2+\alpha_1y+\alpha_0$  irriducibili in  $Z_5$  e, fra essi, quelli primitivi.

Il polinomio  $f(y)$  è riducibile se e solo se o ha il termine noto  $\alpha_0=0$  oppure ha un divisore comune con  $y^4-1$ .

Risulta

$$\begin{cases} f(1)=0 & \text{per } \alpha_1 = -\alpha_0 - 1 \\ f(2)=0 & \text{per } \alpha_1 = -3\alpha_0 - 2 \\ f(3)=0 & \text{per } \alpha_1 = -2\alpha_0 + 2 \\ f(4)=0 & \text{per } \alpha_1 = -\alpha_0 + 1 \end{cases} \quad (4.6)$$

Al variare di  $\alpha_0$  si ottengono, al più, 20 coppie distinte  $(\alpha_0, \alpha_1)$  che soddisfano una delle (4.6).

Poiché le possibili coppie  $(\alpha_0, \alpha_1)$  sono 25, ci sono almeno 5 polinomi irriducibili.

Per  $\alpha_0=1$  si ottengono polinomi irriducibili per  $\alpha_1=1,4$ .

Per  $\alpha_0=2$  si ottengono per  $\alpha_1=1,4$ . Per  $\alpha_0=3$  si ottengono per  $\alpha_1=2,3$ . Per  $\alpha_0=4$  si ottengono per  $\alpha_1=2,3$ . I polinomi irriducibili sono 8.

I divisori non banali di  $m^2-1=24$  sono 2, 3, 4, 6, 8, 12.

Se  $f(y)$  divide  $y^2-1$  oppure  $y^4-1$  è riducibile. Si tratta quindi di vedere, fra gli 8 polinomi irriducibili, quali di essi dividono  $y^3-1$ ,  $y^6-1$  oppure  $y^{12}-1$ .

Posto  $S=P(y)/(f(y))$  e  $x=[y]$ , risulta

$$x^2 = -\alpha_1 x - \alpha_0. \quad (4.7)$$

Vediamo i vari casi

$$(1) \quad \alpha_i=1, \quad \alpha_0=1, \quad x^2=4x+4.$$

Risulta  $x^3=1$  e il polinomio appartiene al periodo 3.

$$(2) \quad \alpha_i=4, \quad \alpha_0=1, \quad x^2=x+4.$$

Risulta  $x^3=4$ ,  $x^6=1$  e il polinomio appartiene al periodo 6.

$$(3) \quad \alpha_i=1, \quad \alpha_0=2, \quad x^2=4x+3.$$

Risulta  $x^3=4x+2$ ,  $x^6=2$ ,  $x^8=3x+1$ ,  $x^{12}=4$ ,  $x^{24}=1$ , il polinomio è primitivo.

$$(4) \quad \alpha_i=4, \quad \alpha_0=2, \quad x^2=x+3.$$

Risulta  $x^3=4x+3$ ,  $x^6=2$ ,  $x^8=2x+1$ ,  $x^{12}=4$ ,  $x^{24}=1$ , il polinomio è primitivo.

$$(5) \quad \alpha_i=2, \quad \alpha_0=3, \quad x^2=3x+2.$$

Risulta  $x^3=x+1$ ,  $x^6=3$ ,  $x^8=4x+1$ ,  $x^{12}=4$ ,  $x^{24}=1$ , il polinomio è primitivo.

$$(6) \quad \alpha_i=3, \quad \alpha_0=3, \quad x^2=2x+2.$$

Risulta  $x^3=x+4$ ,  $x^6=3$ ,  $x^8=x+1$ ,  $x^{12}=4$ ,  $x^{24}=1$ , il polinomio è primitivo.

$$(7) \quad \alpha_i=2, \quad \alpha_0=4, \quad x^2=3x+1.$$

Risulta  $x^3=3$ ,  $x^6=4$ ,  $x^8=2x+4$ ,  $x^{12}=1$ , il polinomio appartiene al periodo 12.

$$(8) \quad \alpha_i=3, \quad \alpha_0=4, \quad x^2=2x+1.$$

Risulta  $x^3=2$ ,  $x^6=4$ ,  $x^8=3x+4$ ,  $x^{12}=1$ , il polinomio appartiene al periodo 12.

## 10. PRIME CONSIDERAZIONI STATISTICHE ED ESEMPI ELEMENTARI

Tenuto conto dei teoremi di omomorfismo fra gruppi e di quelli sui gruppi quozienti si vede subito che il fatto che  $\psi$  sia un epimorfismo implica che, per ogni  $\alpha$  di  $Z_m$ , i sottoinsiemi di  $S$  del tipo  $\psi^{-1}(\alpha)$  hanno lo stesso numero di elementi.

Poiché  $|S| = m^n$  e le classi laterali del nucleo  $N = \psi^{-1}(0)$  sono  $m$ , risulta allora, per ogni  $\alpha$ ,  $|\psi^{-1}(\alpha)| = m^{n-1}$ .

In conseguenza di ciò c'è da attendersi che, se la successione di termine generale  $x^n$  ha periodo dell'ordine di  $|S|$ , ossia se il rapporto  $\rho = \mu(x)/|S|$  è vicino all'unità, allora la successione  $y_n = \psi(x^n)$  ha una distribuzione delle frequenze assimilabile a quella ottenuta, per mezzo di prove casuali e indipendenti, a partire da una variabile casuale  $UD(m)$ , uniforme discreta di parametro  $m$ .

Il caso più favorevole è quello in cui  $S$  è un campo e  $x$  è un elemento primitivo. Infatti, in tali ipotesi  $\mu(x) = |S| - 1$  e 0 l'unico elemento di  $S$  non appartenente alla successione canonica generata da  $x$ .

Detta  $fr(\alpha)$  la frequenza assoluta con cui è raggiunto il valore  $\alpha$  nella successione di termine generale  $y_n$ , risulta allora

$$\text{fr}(\alpha) = \begin{cases} m^{n-1} & \text{per } \alpha \neq 0 \\ m^{n-1} - 1 & \text{per } \alpha = 0 \end{cases} \quad (5.1)$$

La discrepanza della distribuzione delle corrispondenti frequenze relative rispetto alla variabile casuale  $UD(m)$  è del tutto soddisfacente rispetto ad un qualsiasi test sulle frequenze.

Le precedenti considerazioni non escludono, comunque, un buon comportamento statistico delle successioni canoniche ottenute nel caso in cui  $S$  non è un campo e il rapporto  $\rho = \mu(x)/|S|$  è piuttosto basso.

Basta, ad esempio, ricordare che il generatore moltiplicativo è stato sempre usato con successo con il modulo  $m=2^n$ , pur essendo  $\rho=1/4$  per gli elementi massimali e con il modulo  $m=10^n$  in cui, sempre per gli elementi massimali,  $\rho=1/20$ .

In [10] abbiamo mostrato come, anche con tali valori di  $\rho$ , con una opportuna scelta dei parametri il generatore moltiplicativo soddisfi ampiamente ai più importanti tests statistici.

La preferenza data, nella pratica, a tali generatori moltiplicativi rispetto a quello con modulo primo per il quale  $\rho \approx 1$ , fa ritenere che, anche per  $n > 1$ , non è detto che sia da preferire il caso in cui  $S$  è un campo.

Requisiti come la rapidità e la semplicità delle elaborazioni, l'uso del sistema di numerazione binario o decimale, considerazioni statistiche o matematiche di vario genere possono portare a scegliere anelli  $S$  con divisori dello zero in cui gli elementi massimali abbiano periodo piccolo rispetto a  $m^n$ .

Concludiamo esaminando due esempi elementari, allo scopo di illustrare qualche applicazione della teoria svolta. Le successioni ottenute, data la brevità del periodo, non sono significative dal punto di vista statistico, anche se la prima di esse già presenta degli aspetti interessanti.

*Esempio 5.1* Consideriamo il caso in cui  $m=5$ . Nel paragrafo 4 abbiamo visto che il polinomio  $y^2+4y+2$  è primitivo. Il sostegno di  $GF(5^2)$  può essere preso uguale a  $V = \mathbb{Z}_5^2$ . Le costanti caratteristiche dell'algebra  $S = \mathbb{P}(y)/(y^2+4y+2)$  sono  $\beta_1=1$  e  $\beta_0=3$ .

Costruiamo, in  $S$ , la successione  $\{x^k\}_{k \in \mathbb{N}_0}$ , ponendo

$$1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad x = [y] = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Dato che  $x$  è primitivo in  $S$  la successione è formata da 24 vettori distinti. Essi sono i seguenti

|                                        |                                        |                                        |                                        |                                        |                                        |                                        |                                        |
|----------------------------------------|----------------------------------------|----------------------------------------|----------------------------------------|----------------------------------------|----------------------------------------|----------------------------------------|----------------------------------------|
| $\begin{vmatrix} 1 \\ 0 \end{vmatrix}$ | $\begin{vmatrix} 0 \\ 1 \end{vmatrix}$ | $\begin{vmatrix} 3 \\ 1 \end{vmatrix}$ | $\begin{vmatrix} 3 \\ 4 \end{vmatrix}$ | $\begin{vmatrix} 2 \\ 2 \end{vmatrix}$ | $\begin{vmatrix} 1 \\ 4 \end{vmatrix}$ | $\begin{vmatrix} 2 \\ 0 \end{vmatrix}$ | $\begin{vmatrix} 0 \\ 2 \end{vmatrix}$ |
| $\begin{vmatrix} 1 \\ 2 \end{vmatrix}$ | $\begin{vmatrix} 1 \\ 3 \end{vmatrix}$ | $\begin{vmatrix} 4 \\ 4 \end{vmatrix}$ | $\begin{vmatrix} 2 \\ 3 \end{vmatrix}$ | $\begin{vmatrix} 4 \\ 0 \end{vmatrix}$ | $\begin{vmatrix} 0 \\ 4 \end{vmatrix}$ | $\begin{vmatrix} 2 \\ 4 \end{vmatrix}$ | $\begin{vmatrix} 2 \\ 1 \end{vmatrix}$ |
| $\begin{vmatrix} 3 \\ 3 \end{vmatrix}$ | $\begin{vmatrix} 4 \\ 1 \end{vmatrix}$ | $\begin{vmatrix} 3 \\ 0 \end{vmatrix}$ | $\begin{vmatrix} 0 \\ 3 \end{vmatrix}$ | $\begin{vmatrix} 4 \\ 3 \end{vmatrix}$ | $\begin{vmatrix} 4 \\ 2 \end{vmatrix}$ | $\begin{vmatrix} 1 \\ 1 \end{vmatrix}$ | $\begin{vmatrix} 3 \\ 2 \end{vmatrix}$ |

Fra le possibili applicazioni (LO) scegliamo quella,  $\psi$ , che ad ogni  $v \in V$  associa la somma delle componenti.

La successione di termine generale  $y_k = \psi(x^k)$  è

$$\begin{cases} 1, 1, 4, 2, 4, 0, 2, 2, 3, 4, 3, 0, \\ 4, 4, 1, 3, 1, 0, 3, 3, 2, 1, 2, 0, \dots \end{cases} \quad (5.2)$$

di periodo 24.

Le frequenze assolute sono, per ogni  $\alpha$  appartenente a  $Z_5$ ,

$$\text{fr}(\alpha) = \begin{cases} 5 & \text{per } \alpha \neq 0 \\ 4 & \text{per } \alpha = 0 \end{cases} \quad (5.3)$$

conformemente con la (5.1).

Pur con le riserve dovute alla estrema brevità della successione appare opportuno rilevare che oltre alla buona distribuzione delle frequenze dei singoli elementi sono chiaramente visibili altre buone proprietà statistiche, ad esempio la distribuzione della frequenza delle coppie e quella dei runs totali.

**Esempio 5.2** Consideriamo, per  $m=3$ , il polinomio  $f(y)=y^3-y^2-y-1$  e l'algebra  $S=P(y)/(f(y))$ . Poiché  $f(1)=f(2)=1$ ,  $f(y)$  è irriducibile e quindi  $S$  è un campo con  $3^3=27$  elementi.

Il periodo di  $x=[y]$  è un divisore di 26.

Risulta

$$x^3 = x^2 + x + 1, \quad x^{13} = (x^3)^4 x = (x^2 + 1)^2 x = (x^2 + 2x + 2)x = 1,$$

per cui la successione  $\{x^k\}_{k \in \mathbb{N}_0}$  ha periodo 13 e l'elemento  $x$  non è primitivo.

Prendendo  $S=V$  e la base usuale si ottiene la successione di vettori

$$\begin{array}{c}
 \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array} \\
 \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \\
 \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array} \\
 \\
 \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array} \\
 \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array} \dots \\
 \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \end{array}, \begin{array}{|c|} \hline 1 \\ \hline \end{array}, \begin{array}{|c|} \hline 0 \\ \hline \end{array}
 \end{array}$$

Per ogni  $v$  appartenente a  $V$ , prendiamo  $\psi(v)$  come nell'esercizio precedente.

La successione di termine generale  $y_k = \psi(x^k)$  è

$$1, 1, 1, 0, 2, 0, 2, 1, 0, 0, 1, 1, 2.$$

La distribuzione delle frequenze non è buona come nel caso precedente, in cui  $x$  era primitivo.

## BIBLIOGRAFIA

1. G. Ascoli *Lezioni di Algebra*. Editrice Tirrenia. Torino. 1965
2. A.C. Arvillas and D.G. Matitsas *Partitioning the period of a class of m-sequences and application to pseudorandom number generation*. Journal of the Association for Computing Machinery. Vol. 25. 1978.
3. M. Curzio *Lezioni di Algebra*. Liguori Editore Napoli. 1967.
4. I. Glazman, Y. Luibitch *Analyse linéaire dans les espaces de dimensions finies*. Editions Mir Moscou. 1974.
5. S.W. Golomb *Shift register sequences*. Holden-Dsy, Inc. London. 1965.
6. D.E. Knuth *The art of computer programming*. Vol. 2. Seminumerical Algorithms. Addison-Wesley. London. 1969.
7. T.G. Lewis and W.H. Payne *Generalized feedback shift register pseudorandom number algorithm*. Journal of the Association for Computing Machinery. Vol. 20. 1973.
8. A. Maturo *Numeri pseudocasuali*. Montefeltro Edizioni Urbino. 1982.
9. A. Maturo *Numeri pseudocasuali ottenuti a partire da successioni in algebre finite su  $Z_m$* . Ratio Mathematica 1. 1990.
10. A. Maturo, N. Cera *Confronto fra alcuni generatori di numeri pseudocasuali* Periodico di Matematiche 2, 1991.
11. A. Maturo, N. Cera *Generazione di numeri pseudocasuali per mezzo di relazioni di ricorrenza su campi di Galois*. Periodico di Matematiche 2, 1990.
12. W.W. Peterson, E.F. Weldon *Error-correcting codes*. Massachusetts Institute of Technology Press. Cambridge. 1972.

## INTERPRETAZIONE ECONOMICA DEI PREDICATI DI CANALE IN UN SISTEMA DIGITALE MULTICANALE

Fabio Mercanti

**SUNTO:** Attraverso il concetto di *Sistema Digitale Multicanale* (SDM, MELZI-ALLEVI[1]) si mostra come i *predicati di canale* di un tale SDM possano essere assunti con vantaggio come modelli matematici delle proprietà di un sistema macro o microeconomico.

**ABSTRACT** - Through the conception of *Multichannel Digital System*(SDM, MELZI-ALLEVI 1) it has been shown how the *channel predicates* of such a system can be assumed as mathematical models of the properties of a macro or microeconomical system.

O. In questa nota si riprendono alcuni risultati di MERCANTI[2] e si danno alcune ulteriori interpretazioni in *termini economici* dei fenomeni a soglia in un *Sistema Digitale Multicanale* (SDM, MELZI-ALLEVI [1]).

Queste interpretazioni economiche riguardano il fatto che gli *stati* dei vari canali di un SDM, e lo stesso stato istantaneo del sistema, che sono insiemi non ordinati di *parole* su un alfabeto, possono essere riguardati come un modello matematico dei vettori di grandezze fluenti in un sistema economico. Queste interpretazioni preludono, come si vedrà nel § V, ad una maniera, che appare nuova ed assai suggestiva, di modellizzare matematicamente le grandezze economiche con insiemi discreti di oggetti algebrici.

Allora i fenomeni a *soglia* che in [2] sono visti come soglie percettive, possono essere riguardati come i ben noti fenomeni di isteresi economica, e possono essere in tal modo interpretati in termini algebrico-combinatori, all'interno della teoria dei SDM attualmente in studio.

1. Il punto di partenza è la definizione di SDM (§ 0).

Tale definizione richiede alcune premesse di tipo essenzialmente *algebrico*. Il linguaggio e la simbologia usati nel seguito sono quelli introdotti in MELZI-MERCANTI [3] e MELZI [4].

Sia  $T$  un alfabeto costituito da un numero finito di caratteri. Sia  $\mathcal{G}$  (grammatica) l'insieme infinito numerabile delle parole su  $T$  e sia  $P(\mathcal{G})$  l'insieme delle parti di  $\mathcal{G}$ . Gli elementi di  $P(\mathcal{G})$  costituiscono un'algebra di Boole  $\mathcal{B}$ . Si introducano inoltre tra le parole su  $T$  alcune operazioni, opportunamente definite e godenti di proprietà formali facilmente trattabili ed estendibili agli *insiemi di parole*, ossia agli elementi di  $P(\mathcal{G})$ . In tal modo si può definire una struttura algebrica  $\mathcal{A}$  che è una *estensione* dell'algebra  $\mathcal{B}$  di Boole su  $P(\mathcal{G})$ .

2. Mediante l'algebra  $\mathcal{A}$  del § 1 si può definire l'idea di SDM ([1]) che appare come una generalizzazione assai spontanea e promettente del concetto classico di un sistema dinamico (ALLEVI [5]).

Un SDM può essere definito come un vettore

$$S = [C_0, C_1, \dots, C_n] \quad (1)$$

ad elementi in  $P(\mathcal{G})$  e funzione di un tempo discreto  $t_i$ , con le seguenti clausole.

2.1 L'insieme  $\{C_0, C_1, \dots, C_n\}$  delle componenti del vettore  $S$  è ripartito nell'elemento

$C_0$  (*stato del sistema al tempo  $t_i$* ),

negli elementi

$C_1, C_2, \dots, C_r$  (*canali di entrata al tempo  $t_i$* )

e negli elementi

$C_{n+1}, \dots, C_n$  (*canali di uscita al tempo  $t_i$* ),

valendo l'ovvia relazione  $s+r=n$ , con  $r$  numero dei canali di entrata ed  $s$  numero dei canali di uscita.

Tra lo stato  $C_0(t_i)$ , i canali di entrata  $C_1(t_i), \dots, C_r(t_i)$  ed i canali di uscita  $C_{n+1}(t_i), \dots, C_n(t_i)$  sussistono le *relazioni funzionali*

$$C_0(t_{i+1}) = F(C_0(t_i), C_1(t_i), \dots, C_r(t_i)), \quad i=1, 2, \dots, \quad (2)$$

$$C_j(t_{i+1}) = F_j(C_0(t_i)), \quad j=r+1, r+2, \dots, n \quad (3)$$

Le relazioni funzionali (2), (3) esprimono rispettivamente, come è d'uso nella teoria dei sistemi dinamici, che lo stato  $C_0$  al tempo  $t_{i+1}$  è funzione dello stato  $C_0$  e delle entrate  $C_1, C_2, \dots, C_r$  al tempo precedente, e che le uscite  $C_{r+1}, \dots, C_n$  al tempo  $t_{i+1}$  sono funzioni dello stato  $C_0$  al tempo precedente.

Le funzioni  $F$  e  $F_j$  sono funzioni da  $P(\mathcal{S})$  a  $P(\mathcal{S})$  indipendenti del tempo. La (2) e la (3) definiscono evidentemente una applicazione  $\sigma$  dell'insieme  $\mathcal{S}$  dei vettori (1) in sè. Questa applicazione viene detta *funzione caratteristica*  $F_{\text{SDM}}$  del SDM. È da notare che, al presente, parlando di funzioni si intende sempre riferirsi al concetto di  $\mathcal{A}$ -funzione ([3],[4]), nel senso che tutti i legami fra insiemi di parole devono concepirsi come espressi mediante i *predicati e le operazioni* della algebra  $\mathcal{A}$  (§ 1).

3. Si consideri un vettore  $S(t_i)$  funzione del tempo  $t_i$  (§ 2, (1)). Se le componenti di  $S(t_i)$  soddisfano un predicato composto con uno o più predicati dell'algebra  $\mathcal{A}$  (§ 1) si può dire che  $S(t_i)$  *soddisfa un  $\mathcal{A}$ -predicato  $\mathcal{P}$* . Se  $C_j(t_i)$  con  $j=1, 2, \dots, n$  (§2) è il  $j$ -esimo canale di un SDM si dirà che quel canale *gode del predicato* ovvero *gode della proprietà  $\mathcal{P}$*  al tempo  $t_i$ . Analogamente è chiaro che cosa si debba intendere dicendo che lo stato di un SDM gode di una data  $\mathcal{A}$ -proprietà al tempo  $t_i$ .

In particolare assume rilevanza lo studio di un SDM dotato di una sola entrata e di una sola uscita. In tal caso prende senso la affermazione «*se l'entrata di un SDM gode di una proprietà  $\mathcal{P}$  al tempo  $t_i$  allora l'uscita gode di una proprietà  $\mathcal{Q}$  al tempo  $t_{i+1}$* ». Detto  $\Sigma$  un SDM dotato di una sola entrata e di una sola uscita, sia  $P_i$  una proprietà posseduta dall'uscita al tempo  $t_i$  e  $Q_i$  una proprietà posseduta dall'uscita al tempo  $t_i$ . Se  $t_j = t_{i+1}$  si può dire che  $Q_j$  è una  $\Sigma$ -conseguenza di  $P_i$ , e si scrive

$$P_i \xrightarrow{\Sigma} Q_{i+1} \quad (4)$$

Si noti che il fatto che valga la (4) dipende in generale dallo stato  $C_0(t_i)$  di  $\Sigma$  (§ 2,(3)), per modo che la (4) può essere precisata con la

$$P_i \xrightarrow{\Sigma, C_0(t_i)} Q_{i+1}.$$

4. La definizione di SDM si presta alla formulazione di diversi problemi. In particolare per il SDM  $\Sigma$  del § 3 si possono formulare in generale un *problema*

*diretto ed un problema inverso, nei seguenti termini.*

**4.1 Problema diretto.** Per un determinato SDM costruire la *categoria degli stati* concependo gli stati come oggetti ed i predicati di canale come morfismi.

**4.2 Problema inverso.** Costruire un SDM  $\Sigma$  tale che valga la (4) del § 3 per ogni tempo  $t_i$ . Ciò significa caratterizzare lo stato  $C_0(t_0)$  al tempo  $t_0$  e la funzione caratteristica  $F_t$  (§ 2) di  $\Sigma$  in modo tale che valga la (2) del § 2 per ogni tempo  $t_i$ .

5. Il problema diretto 4.1 ed il problema inverso 4.2 ammettono alcune suggestive interpretazioni.

Lo stato  $C_0(t_i)$  al tempo  $t_i$  di un SDM può essere pensato come un modello matematico dello stato di un micro o di un macrosistema economico. In tal caso la scelta di una funzione caratteristica (§ 2) equivale ad un'importante presa di posizione sulla "bontà" di una data modellazione matematica di un sistema economico mediante in SDM. I predicati di canale possono essere assunti come modelli matematici delle più svariate proprietà economiche di un dato sistema economico. Si può pensare ad esempio al *comportamento degli operatori*, ai *vincoli di movimento del sistema*, alla *razionalità od alla irrazionalità del comportamento dei operatori*, ai più svariati *fenomeni a soglia*.

Nel caso particolare di un SDM dotato di una sola uscita (§ 4) della funzione caratteristica (4) corrisponde alla modellazione matematica di un *sistema finanziario particolarmente semplice*: quello in cui due soli operatori intrattengono rapporti di compravendita di titoli contro liquidità monetaria con regimi di scadenze e di interessi di contrattati.

## BIBLIOGRAFIA

1. G. MELZI e E. ALLEVI, *Sistemi dinamici e sistemi digitali*, In corso di pubblicazione.
2. F. MERCANTI, *Una suggestiva analogia fra fenomeni biologici e fenomeni economici a soglia*, Ratio Mathem., Pescara, 2 (1991), 161-165.
3. G. MELZI e F. MERCANTI, *An Algebraic-combinatory Theory of real nervous System*, Rend. Sem. Matem. di Brescia, Italy, 9 (1988), 107-121.
4. G. MELZI, *Sulla definizione di semiautoma*, Rend. Sem. Matem. di Brescia, Italy, 10 (1988), 23-50.
5. E. ALLEVI, *Una speciale classe di sistemi dinamici*, In corso di pubblicazione.

# ALCUNE OSSERVAZIONI SULLA VALUTAZIONE DELLA CAPACITÀ D'UNA FUNZIONE D'UTILITÀ

Lorenzo Peccati  
Un. di Torino e Un. "Bocconi"  
Dicembre 1991

## 1. INTRODUZIONE

In molte pratiche applicazioni soprattutto di tipo assicurativo<sup>1</sup> le preferenze individuali in presenza di rischio sono modellizzate attraverso una funzione d'utilità bernulliana  $u$  analiticamente piuttosto comoda:

$$u(x) = x - \frac{1}{2B}x^2 \quad x \leq B$$

La funzione d'utilità così definita è brevemente detta *utilità quadratica*, e il parametro  $B$  può dirsi *capacità* della funzione  $u$ .

La valutazione della capacità può farsi sottoponendo al decisore la possibilità di negoziare la somma aleatoria  $X$  che ha la seguente distribuzione di probabilità (prima riga: determinazioni; seconda riga: probabilità corrispondenti):

$$X = \begin{Bmatrix} 0 & V \\ 1 - \pi & \pi \end{Bmatrix}$$

ove  $V > 0$  e  $0 < \pi < 1$ .

---

<sup>1</sup> Si veda, per es., Daboni (1988).

Tale negoziazione può farsi sia proponendo al soggetto di acquistare  $X$ , contro il pagamento di un prezzo massimo  $\alpha V$  (con  $0 \leq \alpha \leq 1$ ), sia di vendere il diritto a  $X$  contro riscossione di un prezzo minimo che denoterà ancora con  $\alpha V$ .

La dichiarazione di  $\alpha$  da parte del decisore "rivela" il valore del parametro  $B$  che caratterizza la funzione d'utilità. Viene fatto enunciare al soggetto nient'altro che il *certo equivalente per il compratore o per il venditore*<sup>2</sup>.

In presenza di avversione al rischio il decisore fisserà  $\alpha < \pi$  (e questo sarà nel seguito supposto).

Interessa segnalare che, anche attraverso la fissazione di  $\alpha$  (con  $\alpha < \pi$ ), non è affatto detto che la stima per  $B$  che ne scaturisce sia sensata.

Indicherò, nel prossimo paragrafo, qual è l'insieme in cui si può scegliere  $\alpha$  affinché la stima di  $B$  non sia insensata. Nel paragrafo successivo introdurrò una famiglia di funzioni d'utilità che generalizza quella di partenza, mostrando come anche per esse si ripresenti il problema e come possa essere analogamente risolto. Seguiranno alcune riflessioni conclusive.

## 2. VALORI AMMISSIBILI NEL CASO QUADRATICO

Consideriamo dapprima il caso del compratore che acquista la somma aleatoria  $X$  contro pagamento del prezzo certo  $\alpha V$ . Supponiamo, ripeto, che  $\alpha < \pi$ .

Dovrà essere:

$$E[u(X - \alpha V)] = 0$$

onde, vista la specificazione analitica di  $u$ :

$$E \left[ (X - \alpha V) - \frac{1}{2B} (X - \alpha V)^2 \right] = 0$$

si trae:

$$B = \frac{E[(X - \alpha V)^2]}{2E(X - \alpha V)}$$

Osservato che:

$$E(X) = \pi V \quad ; \quad E(X^2) = \pi V^2 ;$$

---

<sup>2</sup> Si veda PECCATI (1990)

$$E[(X - \alpha V)^2] = V^2(\pi - 2\alpha\pi + \alpha^2)$$

si ha subito:

$$B = \frac{V(\pi - 2\alpha\pi + \alpha^2)}{2(\pi - \alpha)}$$

Perché la stima possa aver senso bisogna che il massimo valore del guadagno per il decisore  $V - \alpha V = (1 - \alpha)V$  non ecceda la capacità  $B$ .

La condizione:

$$(1 - \alpha)V \leq \frac{V(\pi - 2\alpha\pi + \alpha^2)}{2(\pi - \alpha)}$$

si riduce (essendo, per ipotesi,  $\alpha < \pi$ ) a:

$$\alpha^2 - 2\alpha + \pi \leq 0$$

per  $\alpha$  deve allora aversi:

$$1 - \sqrt{1 - \pi} \leq \alpha \leq 1 + \sqrt{1 - \pi}$$

La disuguaglianza di destra è ovviamente vera quella di sinistra fornisce un confine inferiore non banale per  $\alpha$ .

Osservato che banalmente  $\alpha_0(\pi) \stackrel{d}{=} 1 - \sqrt{1 - \pi} \leq \pi$  poiché possa aver senso una stima di  $B$  ricavata dall'elicitazione del prezzo unitario  $\alpha$  deve essere:

$$1 - \sqrt{1 - \pi} \leq \alpha < \pi$$

Si controlla facilmente che anche vedendo il problema dal punto di vista del venditore nella muta<sup>3</sup>. In tal caso la condizione che deve esser soddisfatta è:

$$E\left(X - \frac{1}{2B}X^2\right) = \alpha V - \frac{1}{2B}\alpha^2 V^2$$

Se ne trae la stima per  $B$ :

---

<sup>3</sup>Questo è interessante perché è nota la non equivalenza in generale dei due punti di vista nel caso di utilità quadratica.

$$B = \frac{V(\pi - \alpha^2)}{2(\pi - \alpha)}$$

Perché  $B$  sia accettabile deve essere  $V \leq B$ . Sostituendo si ritrova la limitazione inferiore per  $\alpha$  col confine  $\alpha_0(\pi)$ .

La tavola seguente dà tale confine inferiore  $\alpha_0(\pi) = 1 - \sqrt{1 - \pi}$  per  $\alpha$  al variare di  $\pi$ :

| $\pi$ | $\alpha_0(\pi)$ |
|-------|-----------------|
| 0     | 0               |
| 0.05  | 0.02532         |
| 0.10  | 0.05132         |
| 0.15  | 0.07805         |
| 0.20  | 0.1056          |
| 0.25  | 0.134           |
| 0.30  | 0.1633          |
| 0.35  | 0.1938          |
| 0.40  | 0.2254          |
| 0.45  | 0.2584          |
| 0.50  | 0.2929          |
| 0.55  | 0.3292          |
| 0.60  | 0.3675          |
| 0.65  | 0.4084          |
| 0.70  | 0.4523          |
| 0.75  | 0.5             |
| 0.80  | 0.5528          |
| 0.85  | 0.6127          |
| 0.9   | 0.6838          |
| 0.95  | 0.7764          |
| 1.00  | 1               |

Come si vede la limitazione per  $\alpha$  è piuttosto severa.

### 3. UNA GENERALIZZAZIONE

In letteratura, con riferimento alla classe di funzioni d'utilità definite da:

$$u(x) = \frac{x^\gamma}{\gamma}$$

definite per  $x > 0$ , con  $\gamma \neq 0$  reale qualsiasi, si parla di classe *HARA*. L'acronimo sta per *Hyperbolic Absolute Risk Aversion*.

Detta  $r$  l'avversione (assoluta)<sup>4</sup> al rischio nel senso di (de Finetti)-Arrow-Pratt:

$$r(x) = - \frac{u''(x)}{u'(x)}$$

si ottiene:

$$r(x) = \frac{1}{x}$$

che giustifica il nome. La popolarità di tale classe di funzioni d'utilità, facilmente intuibile per la loro semplicità dal punto di vista analitico, non appare del tutto giustificata. La limitazione  $x > 0$  ne rende problematica l'applicazione corretta quando si debba tener distinta la posizione del venditore da quella del compratore. Anche quando sia certo che una somma aleatoria non può esser in nessun caso negativa, se si tratta di valutarla per la vendita, non si possono presentare valori negativi per l'argomento di  $u$ , ma nel caso dell'acquisto la differenza tra somma acquistata e prezzo può, generalmente, anche "pescare" nel negativo, con insuperabili difficoltà.

È affatto evidente che sotto la sigla *HARA* possono rientrare anche altre funzioni d'utilità, con avversione al rischio iperbolica e più interessanti dal punto di vista delle applicazioni finanziarie.

Considero la seguente funzione iperbolica di avversione al rischio:

$$r(x) = \frac{A}{B - x}$$

con  $x < B$  e  $A$  parametro positivo. Nel caso quadratico si ha:

<sup>4</sup>Si veda, per es., COPELAND-WESTON (1988).

<sup>5</sup>E nelle applicazioni finanziarie si deve.

$$-\frac{u''(x)}{u'(x)} = -\frac{-1/B}{1-x/B} = \frac{1}{B-x}$$

e a tale espressione si riduce  $r(x)$  quando  $A=1$ . Pare legittimo parlare di classe *HARA* anche con riferimento alle funzioni d'utilità con tale avversione al rischio, funzioni impiegabili per  $x < B$  e quindi più adatte per un corretto impiego in ambito finanziario. Su questa classe di funzioni d'utilità fermerò la mia attenzione in questo paragrafo.

Risolvendo l'equazione differenziale:

$$-\frac{u''(x)}{u'(x)} = \frac{A}{B-x}$$

con le condizioni al contorno  $u(0)=0$  e  $u'(0)=1$  s'ottiene:

$$u(x) = \frac{B - B^{-A}(B-x)^{A+1}}{A+1}$$

che ovviamente si riduce alla quadratica se  $A=1$ .

Suppongo, nel seguito, in perfetta analogia con la situazione esaminata nel paragrafo 2, che  $A$  sia nota e mi propongo studiare la stima di  $B$  attraverso l'indicazione di un prezzo per il solito ammontare aleatorio  $X$ . Non si otterranno più equazioni esplicitamente solubili in  $B$ , che possono essere peraltro risolte in concreto attraverso metodi numerici. Mi limiterò a indicare sotto quali restrizioni esista (e sia unica) una stima per  $B$ .

Comincio dal caso del *venditore*. L'equazione  $u(\alpha V) = \pi u(V)$  diviene:

$$\frac{B - B^{-A}(B - \alpha V)^{A+1}}{A+1} = \pi \frac{B - B^{-A}(B - V)^{A+1}}{A+1}$$

con semplici passaggi si riduce a:

$$(1 - \pi)B^{A+1} = (B - \alpha V)^{A+1} - (B - V)^{A+1}$$

Dirò nel seguito  $P(B)$  il primo e  $S(B)$  il secondo membro dell'equazione in  $B$ . Interessa, naturalmente, una soluzione per la stessa, che sia maggiore di  $V$  in quanto il massimo valore che può assumere  $X$  non deve superare la capacità di  $u$ . Affronto sbrigativamente le classiche questioni di esistenza e unicità.

Per quanto concerne l'esistenza la strada è semplice.

Osservo subito che  $S(B) = o[P(B)]$  per  $B \rightarrow +\infty$  e quindi definitivamente

$P(B) > S(B)$ . Noto anche che ponendo  $B=V$  in  $P$  e  $S$  si ottiene:

$$P(V) = (1 - \pi)V^{A+1}; S(V) = (1 - \alpha)^{A+1}V^{A+1}$$

L'esistenza è garantita se  $P(V) < S(V)$  stante la continuità di tali due funzioni. Ora, tale condizione si riduce facilmente a:

$$\alpha > \alpha_0(\pi, A) = 1 - (1 - \pi)^{1/(A+1)}$$

che visibilmente generalizza quella individuata nel precedente paragrafo per il caso quadratico.

Per provare l'unicità i calcoli non sono così brevi, ma si può comunque arrivare in porto. Basta riprendere l'equazione di partenza

$$u(\alpha V) = \pi u(V)$$

e osservare che equivale alla seguente:

$$\frac{1 - (1 - \alpha V / B)^{A+1}}{1 - (1 - V / B)^{A+1}} = \pi$$

che si riscrive, più semplicemente:

$$\frac{1 - (1 - \alpha y)^{A+1}}{1 - (1 - y)^{A+1}} = \pi$$

con  $y = V/B \in (0; 1)$ . Basta mostrare che il primo membro è funzione monotona di  $y$  per avere l'unicità garantita. Posto  $f(y) = 1 - (1 - y)^{A+1}$ , la funzione di cui c'è interesse provare la monotonia è definita da  $\psi(y) = f(\alpha y) / f(y)$ . Si controlla senza difficoltà che  $\psi(0^+) = \alpha$  e che  $\psi(1) = 1 - (1 - \alpha)^{A+1} > \alpha$ . La condizione  $\psi'(y) > 0$  equivale a:

$$\alpha \frac{f'(\alpha y)}{f(y)} > \frac{f'(y)}{f(y)}$$

che, a sua volta è garantita se  $D \ln[f(y)]$  decresce. Posto  $g(y) = \ln f(y)$ , basta allora provare che  $g''(y) < 0$  in  $(0; 1)$ . Si ha:

---

\*Al solito, ad essa si riduce con  $A=1$ .

$$g'(y) = (A+1) \frac{1}{(1-y)^{-A} - 1 + y}$$

onde:

$$g''(y) = (A+1) \frac{-1}{[(1-y)^{-A} - 1 + y]^2} \left[ 1 + \frac{A}{(1-y)^{A+1}} \right] < 0$$

e si ha l'asserto.

Passo ora al caso del *compratore*. L'equazione che definisce il certo equivalente e dalla quale dovrebbe riuscire determinato  $B$  è la seguente:

$$\pi \frac{B - B^{-A} [B - V(1-\alpha)]^{A+1}}{A+1} + (1-\pi) \frac{B - B^{-A} (B - \alpha V)^{A+1}}{A+1} = 0$$

Considerazioni analoghe a quelle svolte poco sopra garantiscono l'unicità di un'eventuale soluzione. Quanto all'esistenza, si può osservare che:

- per  $B \rightarrow +\infty$  il primo membro è asintotico a  $B(1-\pi)/(A+1)$  e dunque è positivo;
- per  $B = V(1-\alpha)$  esso si riduce a:

$$\pi \frac{V(1-\alpha)}{A+1} + (1-\pi) \frac{V(1-\alpha) - [V(1-\alpha)]^{-A} (V - \alpha V + \alpha V)^{A+1}}{A+1}$$

Il segno di tale quantità è lo stesso di:

$$\pi + (1-\pi)[1 - (1-\alpha)^{-A-1}]$$

Esiste una soluzione se tale quantità è negativa. Pochi passaggi conducono a provare che essa lo è se:

$$\alpha > \alpha_0(\pi, A) = 1 - (1-\pi)^{1/(A+1)}$$

coincidente con la limitazione data sopra.

---

<sup>1</sup>KEENEY-RAIFFA (1976).

#### 4. RIFLESSIONI CONCLUSIVE

Può interessare confrontare tale nuovo confine inferiore per  $\alpha$  con quello individuato nel par. 2 per il caso quadratico e cioè  $\alpha_0(\pi, 1)$ .

Si conclude facilmente che questo nuovo confine riesce più stringente (ossia  $\alpha_0(\pi, A) > \alpha_0(\pi, 1)$ ) se  $A < 1$ . Questo ovviamente discende dal fatto che  $\alpha_0(\pi, A)$  decresce al crescere di  $A$ . Rammentando, a questo punto qual è il significato strategico del parametro  $A$  si desume che, nella classe di funzioni di utilità in esame, quanto maggiore è l'avversione al rischio del valutatore, tanto più basso è il confine di compatibilità del certo equivalente con tale tipo di funzione. E questo è consolante.

#### BIBLIOGRAFIA

- L. DABONI (1988): *Lezioni di Tecnica Attuariale delle Assicurazioni contro i danni*. LINT, Trieste.
- T.E. COPELAND, J.F. WESTON (1988): *Financial Theory and Corporate Policy*, 3rd ed., Addison Wesley, Reading, Mass.
- R.L. KEENEY, H. RAIFFA (1976): *Decisions with multiple objectives: Preferences and Value Tradeoffs*. Wiley, New York.
- L. PECCATI (1990): 'Certainty equivalent and time', *Eighth Meeting of the EURO-Working Group on Financial Modelling*, Gieten, November.

## CONSIDERAZIONI SUL TEST Z PER GLI INDICI DI MORAN

Giuliano Visini

**Riassunto** - In questa nota l'autore considera gli indici di Moran, ne esamina i primi due momenti e analizza i comportamenti dei relativi tests z dandone un'efficace rappresentazione parametrica.

**Summary** - Moran index is the objet of this work, the author takes into examination the first two moments and analyzes the line of conduct of the relative z tests giving of them a clarifying parametrical representation.

### 1. INTRODUZIONE

L'analisi spaziale si scontra di continuo tra tre esigenze contrastanti che rispondono a tre angolazioni diverse, eppur complementari, per affrontare lo stesso problema: una modalità territoriale, articolata per unità di rilevamento statistico, di quale processo soggiacente è la realizzazione? Come valutarne la eventuale casualità? Come rappresentarne la variabilità nello spazio, in modo da poterne rilevare in maniera corretta, le relazioni di vicinato tra elementi contigui statistico-territoriali?

La letteratura offre una pluralità di risposte parziali, ed anche questo contributo si muove ed intende procedere in uno specifico sentiero disciplinare, ma nella piena consapevolezza di una struttura concettuale di fondo pluridisciplinare, contesto non solo scientifico, ma anche culturale.

Il tema centrale da esplicitare, in seguito nei termini propri del linguaggio formale, è quello delle tendenze centrali in un territorio privo di gerarchizzazioni aprioristiche dei luoghi: ogni unità di rilevamento è considerato "luogo centrale", dal quale procedere all'esplorazione dello spazio circostante al fine di individuare l'incidenza della "posizione geografica" nelle realizzazioni di un dato processo.

Il fatto che esso si debba necessariamente assumere come in una logica probabilistica - come tale negazione dell'autocorrelazione spaziale - costringe da un lato, a considerare le relazioni di contiguità, e, da un altro, le condizioni che giustificano una distribuzione normale delle stesse in relazione a variabili aleatorie di modalità qualitative.

## 2. GLI INDICI DI MORAN: MEDIA E VARIANZA

Posto  $N_n = \{1, 2, \dots, n\}$  ed  $n \geq 2$ , sia  $\{a_i \mid i \in N_n\}$  una suddivisione territoriale finita di un territorio e sia il vettore aleatorio

$$\underline{K} = (K_1, K_2, \dots, K_n)$$

costituito da una n-pla di variabili aleatorie (v.a.) di modalità qualitative (ad es. variabili policrome) ciascuna osservabile sulla corrispondente unità territoriale  $a_i (i \in N_n)$ .

Se le distribuzioni delle v.a.  $K_i (i \in N_n)$  sono tra loro mutuamente indipendenti e identicamente distribuite e se indichiamo con:

- a)  $K = \{B, R, V, \dots, N\}$ ,  
(ove ad es.: B=Bianco, R=rosso, V=verde, ..., N=nero), lo spazio campionario di ogni singola v.a.  $K_i$ ;
  - b)  $p_{ir}$  la probabilità della modalità r-esima della v.a.  $K_i$  osservabile sull'unità territoriale i-esima;
  - c)  $K^n$ , l'universo dei campioni relativo alla situazione osservabile sulle unità territoriali  $a_i (i \in N_n)$ ;
- il modello relativo resta definito da:

$$\{\underline{K}, K^n, \quad k \geq 2, \quad \prod_{i=1}^n p_{ir}, \quad \sum_{r=1}^k p_{ir} = 1\}.$$

Introdotta poi un criterio di contiguità spaziale tra le unità territoriali, resta definito un operatore di associazione L,

$$L: \{a_i \mid i \in N_n\} \rightarrow \{a_j \mid j \in N_n\},$$

che esprime una corrispondenza generalmente multivoca e non ovunque definita, tale che:

$$L(a_i) \subseteq \{a_j \mid j \in N_n, j \neq i\}$$

nel caso valga l'implicazione:

$$a_j \in L(a_i) \implies a_i \in L(a_j) \quad (j \in N_n),$$

l'operatore di associazione lo diremo simmetrico.

La rappresentazione di  $L$  nell'insieme prodotto cartesiano  $\{a_i \mid i \in N_n\} \times \{a_i \mid i \in N_n\}$  come  $\{a_p, a_q \mid a_q \in L(a_p), p \in N_n\}$  induce sulla matrice aleatoria

$$\underline{K} \cdot \underline{K}' = (K_{ij})_{i \in N_n, j \in N_n}$$

una limitazione ristretta alle sole variabili aleatorie  $K_p$  i cui indici  $p$  e  $q$  siano rispettivamente quelli corrispondenti alle unità territoriali poste nella relazione  $a_q \in L(a_p)$  per ogni  $p \in N_n$ . Per tale limitazione si considera assegnata la distribuzione di  $\underline{K} \cdot \underline{K}'$ .

In tal modo per ciascun operatore di associazione  $L$  è possibile considerare la tavola aleatoria di variabili aleatorie

|   | B        | R        | V        | . | . | N        |
|---|----------|----------|----------|---|---|----------|
| B | $N_{BB}$ | $N_{BR}$ | $N_{BV}$ | . | . | $N_{BN}$ |
| R | $N_{RB}$ | $N_{RR}$ | $N_{RV}$ | . | . | $N_{RN}$ |
| V | $N_{VB}$ | $N_{VR}$ | $N_{VV}$ | . | . | $N_{VN}$ |
| . | .        | .        | .        | . | . | .        |
| . | .        | .        | .        | . | . | .        |
| N | $N_{NB}$ | $N_{NR}$ | $N_{NV}$ | . | . | $N_{NN}$ |

(Tav. 2.1)

le cui determinazioni sono costituite dalle possibili frequenze assolute associate alle limitazioni predette dei risultati individuati dallo spazio

$$IK^2 = \{BB, BR, BV, \dots, BN, \dots, NB, NR, NV, \dots, NN\}$$

e le cui distribuzioni di probabilità si ottengono per "riduzione" da quelle di  $\underline{K} \cdot \underline{K}'$ .

Gli elementi della tav. 2.1, noti come indici di contiguità di Moran, costituiscono una misura dell'influenza che modalità disposte su zone contigue

esercitano vicendevolmente.

Ipotizzata  $p_r = p_r(i \in N_r)$ , con probabilità a priori che si abbia a realizzare l'evento  $r$ -esimo su una unità territoriale, di tali indici sono noti i momenti.

Infatti, considerate le variabili di comodo:

$$\begin{aligned} S_0 &= \sum_{i=1}^n L_{i.} = \sum_{j=1}^n L_{.j} \\ S_1 &= \left( \sum_{i=1}^n \sum_{j=1}^n (\delta_{ij} + \delta_{ji})^2 \right) / 2 \\ S_2 &= \left( \sum_{i=1}^n (L_{i.} + L_{.i})^2 \right) / 2 \\ \text{ove} \quad \delta_{ij} &= 1 \text{ se } a_j \in L(a_i) \\ \delta_{ij} &= 0 \text{ se } a_j \notin L(a_i) \\ L_{i.} &= \sum_{j=1}^n \delta_{ij} \\ L_{.j} &= \sum_{i=1}^n \delta_{ij} \end{aligned}$$

le medie e le varianze restano individuate dalle:

I) nel caso in cui due unità territoriali contigue abbiano medesimo colore, ad es. RR:

$$\begin{aligned} E(N_{RR}) &= (S_0 p_R^2) / 2 \\ \text{Var}(N_{RR}) &= (S_1 p_R^2 + (S_2 - 2S_1) p_R^3 + (S_1 - S_2) p_R^4) / 4 \end{aligned}$$

II) nel caso in cui due unità territoriali contigue abbiano diversità assegnata di colore ad es. RN:

$$\begin{aligned} E(N_{RN}) &= S_0 p_R p_N \\ \text{Var}(N_{RN}) &= (2S_1 p_R p_N + (S_2 - 2S_1) p_R p_N (p_R + p_N) + 4(S_1 - S_2) p_R^2 p_N^2) / 4 \end{aligned}$$

III) nel caso in cui due unità territoriali contigue abbiano generici colori diversi:

$$\begin{aligned} E(N_{BR...N}) &= S_0 \sum_{r=1}^{k-1} \sum_{s=r+1}^k p_r p_s \\ \text{Var}(N_{BR...N}) &= S_0 \sum_{r=1}^{k-1} \sum_{s=r+1}^k p_r p_s + (2S_1 - 5S_2) \sum_{r=1}^{k-2} \sum_{s=r+1}^{k-1} \sum_{t=s+1}^k p_r p_s p_t + \end{aligned}$$

$$+4(S_1 - S_2) \left( \sum_{r=1}^{k-1} \sum_{s=r+1}^k p_r p_s - 2 \sum_{r=1}^{k-3} \sum_{s=r+1}^{k-2} \sum_{t=s+1}^{k-1} \sum_{u=t+1}^k p_r p_s p_t p_u \right) / 4$$

Infine, se l'operatore di associazione spaziale è simmetrico, introdotte le variabili di comodo

$$A = \sum_{i=1}^n L_i / 2 = \sum_{j=1}^n L_j / 2$$

$$D = \sum_{i=1}^n \binom{L_i}{2} = \sum_{j=1}^n \binom{L_j}{2}$$

legate alle precedenti dalle:

$$A = S_0 / 2 = S_1 / 4$$

$$D = (S_2 - 2S_1) / 8 = (S_2 - 4S_0) / 8$$

le medie e le varianze si trasformano nelle:

$$I') \quad E(N_{RR}) = A p_R^2$$

$$\text{Var}(N_{RR}) = A p_R^2 + 2D p_R^3 - (A + 2D) p_R^4$$

$$II') \quad E(N_{RN}) = 2A p_R p_N$$

$$\text{Var}(N_{RN}) = A p_R p_N + 2D p_R p_N (p_R + p_N) - 4(A + 2D) p_R^2 p_N^2$$

$$III') \quad E(N_{BR...N}) = 2A \sum_{r=1}^{k-1} \sum_{s=r+1}^k p_r p_s$$

$$\begin{aligned} \text{Var}(N_{BR...N}) = & 2(A + D) \sum_{r=1}^{k-1} \sum_{s=r+1}^k p_r p_s - 2(4A + 5D) \sum_{r=1}^{k-2} \sum_{s=r+1}^{k-1} \sum_{t=s+1}^k p_r p_s p_t + \\ & - 4(A + 2D) \left( \sum_{r=1}^{k-1} \sum_{s=r+1}^k p_r^2 p_s^2 - 2 \sum_{r=1}^{k-3} \sum_{s=r+1}^{k-2} \sum_{t=s+1}^{k-1} \sum_{u=t+1}^k p_r p_s p_t p_u \right) \end{aligned}$$

### 3. LA VARIANZA NELLE SUE COMPONENTI

Come è possibile osservare i valori medi e le varianze degli indici dipendono, oltre che dalle probabilità  $p_r$ , che si realizzi l'evento  $r$ -esimo sull'unità territoriale  $i$ -esima, anche dalle variabili  $A$  e  $D$ , a loro volta, dipendenti dalla numerosità  $n$  delle unità territoriali.

In particolare, i valori medi sono influenzati solamente dalla variabile  $A$ , mentre le varianze lo sono generalmente da entrambi.

Ora i valori assumibili da A sono propri anche di altre possibili ipotesi di operatori di associazione, mentre i valori assumibili da D diversificano talune di queste ipotesi, che, essendo scelta del ricercatore, sono soggettive.

Nell'esempio, che si riporta, riferito al caso in cui  $n=5$ , accanto alle colonne dei valori assunti da A e D è posta la colonna F delle numerosità delle possibili ipotesi di operatori di associazione simmetrici corrispondenti.

| A | D | F  | A | D  | F   | A  | D  | F  |
|---|---|----|---|----|-----|----|----|----|
| 1 | 0 | 10 | 5 | 5  | 12  | 7  | 13 | 30 |
| 2 | 0 | 15 | 5 | 6  | 120 | 7  | 14 | 60 |
| 2 | 1 | 30 | 5 | 7  | 60  | 7  | 15 | 30 |
| 3 | 1 | 30 | 5 | 8  | 60  | 8  | 18 | 15 |
| 3 | 2 | 60 | 6 | 9  | 70  | 8  | 19 | 30 |
| 3 | 3 | 30 | 6 | 10 | 75  | 9  | 24 | 10 |
| 4 | 3 | 70 | 6 | 11 | 60  | 10 | 30 | 1  |
| 4 | 4 | 75 | 6 | 12 | 5   |    |    |    |
| 4 | 5 | 60 |   |    |     |    |    |    |
| 4 | 6 | 5  |   |    |     |    |    |    |

D'altra parte le varianze espresse dalle I') sono monotone crescenti rispetto a D mentre quelle espresse dalle II') sono monotone non decrescenti rispetto a D, come anche quelle espresse dalle III'), almeno nei casi per i quali è  $k=3, 4$ .

È allora di interesse ricercare una (o più d'una) relazione che consenta di stabilire i valori assumibili da D fissato A, essendo D funzione multivoca di A.

Il sistema 3.1, a variabili intere, formalizza l'interesse della ricerca e, come tipica formulazione di un problema di programmazione a variabili intere ed a soluzione ottima intera massimizzante o minimizzante, consente di determinare la serie marginale dei valori massimi indicata  $D_{\max}$  o quella dei valori minimi indicata  $D_{\min}$  di D.

$$(3.1) \begin{cases} \sum_{i=0}^{n-1} \left( ix_i + \sum_{j=i+1}^{n-1} x_j \right) - D = 0 & ((\max D) \text{ o } (\min D)) \\ \sum_{i=0}^{n-1} ix_i = A \\ 1 \leq A \leq \binom{n}{2} \\ 0 \leq x_i \leq 1 \end{cases}$$

La serie marginale dei valori  $D_{\min} = D_{\min}(A)$ , soluzione ottima minimizzante

il sistema (3.1), è definibile attraverso la:

$$D_{\min}(A) = (2A \pmod n) (\text{int}(2A/n) + 1)^2 + (n - 2A \pmod n) (\text{int}(2A/n))^2 / 2 - A.$$

Per la serie marginale dei valori massimi  $D_{\max} = D_{\max}(A)$  si individuano immediatamente le corrispondenze:

$$\begin{aligned} 1 \leq A \leq n-1 & \quad D_{\max}(A) = \binom{A}{2} \\ A = n & \quad D_{\max}(A) = \binom{n-1}{2} + 2 \\ A = 2n-3 & \quad D_{\max}(A) = n(n-2) \\ A = h + \binom{n-1}{2} \quad (0 \leq h \leq n-1) & \quad D_{\max}(A) = \binom{h}{2} + (n-h-1) \binom{n-2}{2} + h \binom{n-1}{2} \end{aligned}$$

Tuttavia, per quest'ultima si constata delle regolarità con possibilità di algoritmare negli intervalli di tipo I e J sotto specificati:

$$\begin{aligned} I_1 &= [1, n-1] \\ I_{r_1} &= \left[ 1 + \sum_{i=1}^{r_1-1} (n-i), \sum_{i=1}^{r_1} (n-i) \right] \quad (r_1 \in N_{n-1}) \\ I_{n-1} &= \left[ \binom{n}{2}, \binom{n}{2} \right] \\ J_1 &= \left[ \binom{n-1}{2} + 1, \binom{n}{2} \right] \\ J_{r_2} &= \left[ \binom{n-r_2}{2} + 1, \binom{n-r_2+1}{2} \right] \quad (r_2 \in N_{n-1}) \\ J_{n-1} &= [1, 1]. \end{aligned}$$

Infatti, se si considera il valore assunto da A, individuati gli indici  $r_1$  e  $r_2$  dei rispettivi intervalli di appartenenza di tipo I e J e gli indici  $h_1$  e  $h_2$  di rispettiva posizione all'interno di questi intervalli per cui:

$$A = h_1 + \sum_{i=1}^{r_1-1} (n-i) = h_2 + \binom{n-r_2}{2}$$

si ha in corrispondenza:

$$\begin{aligned} D_{\max}(A) = \max & \left[ 2(r_1-1)h_1 + \binom{h_1}{2} + \sum_{s=1}^{r_1-1} \left( 2(s-1)(n-s) + \binom{n-s}{2} \right); \right. \\ & \left. \binom{n-r_2}{2} h_2 + \binom{h_2}{2} + (n-r_2-h_2) \binom{n-r_2-1}{2} \right] \end{aligned}$$

ove  $h_1 \in N_{n-r_1}$  e  $h_2 \in N_{n-r_2}$ .

Supposto poi che la probabilità  $p_r$  che si realizzi l'evento  $r$ -esimo su una unità territoriale sia costante per ogni evento di  $K$ , ossia  $p_r = 1/k$ , le relazioni precedenti I', II' e III' si riducono alle:

$$\begin{aligned} \text{I'')} \quad & E(N_{RR}) = A / k^2 \\ & \text{Var}(N_{RR}) = (Ak^2 + 2Dk - (A + 2D)) / k^4 \\ \text{II'')} \quad & E(N_{RN}) = 2A / k^2 \\ & \text{Var}(N_{RN}) = 2(Ak^2 + 2Dk - 2(A + 2D)) / k^4 \\ \text{III'')} \quad & E(N_{BR...N}) = A(k - 1) / k \\ & \text{Var}(N_{BR...N}) = A(k - 1) / k^2. \end{aligned}$$

Come è osservabile, nella III'' la varianza è indipendente da  $D$  ed ancora nel particolare caso di  $k=2$  perde di significato la III'' e le I'' e le II'' diventano:

$$\begin{aligned} \text{I''')} \quad & E(N_{RR}) = A / 4 \\ & \text{Var}(N_{RR}) = (3A + 2D) / 16 \\ \text{II''')} \quad & E(N_{RN}) = A / 2 \\ & \text{Var}(N_{RN}) = A / 4 \end{aligned}$$

#### 4. LE DISTRIBUZIONI CAMPIONARIE DEGLI INDICI DI MORAN

In condizioni di indipendenza delle osservazioni spaziali e di equiprobabilità delle modalità rilevabili, l'ipotesi statistica che si vuole provare attraverso il test  $z$  è la presenza o meno di autocorrelazione spaziale, ossia se l'osservazione di una modalità di una variabile qualitativa in una unità territoriale influenzi quelle in unità contigue e viceversa ne resti da queste influenzata.

##### 4.1 CASO DELLA VARIABILE $N_{BR...N}$

Essendo  $K = \{B, R, \dots, N\}$  e  $|K| = k$ , indicata con  $r$  la genera modalità sia nelle ipotesi formulate  $p_r = 1/k$  ( $r \in K$ ). Con riferimento alla variabile casuale  $N_{BR...N}$ , indicata con  $x$  una sua determinazione, è

$$z_{BR...N} = z_k = (xk - A(k - 1)) / \sqrt{A(k - 1)}$$

Questa è funzione reale delle variabili intere  $x$ ,  $A$ ,  $k$ , ed in quanto definita per

$$\left\{ \begin{array}{l} k \geq 2 \\ 1 \leq A \leq \binom{n}{2} \\ 0 \leq x \leq \binom{n}{2} - \sum_{h=1}^{n-k} \text{int}((n-h)/k) \\ x \leq A \end{array} \right.$$

lo è anche di  $n$  con l'aggiunta della dipendenza delle determinazioni  $x$  da  $n, k$  e dagli operatori di associazione  $L$ .

Per ciascun  $n$ ,  $z_k$  è rappresentabile in uno spazio  $R^4$  da una nuvola di punti non minore di

$$\frac{1}{2} \left( \binom{n}{2}^2 + 3 \binom{n}{2} \right) - \left( \sum_{h=1}^{n-k} \text{int}((n-h)/k) \right) - \sum_{k=1}^{\text{int}(n/2)} \binom{n-2h+1}{2}$$

Essa è limitata inferiormente da

$$z_{k|x=0} = -\sqrt{A(k-1)}$$

limitata superiormente da

$$z_{k|x=A} = \sqrt{A/(k-1)} \text{ per } 1 \leq A \leq \binom{n}{2} - \sum_{h=1}^{n-k} \text{int}((n-h)/k)$$

e maggiorata da

$$z_{k|x=A} = \sqrt{A/(k-1)} \text{ per } \binom{n}{2} - \sum_{h=1}^{n-k} \text{int}((n-h)/k) < A \leq \binom{n}{2}$$

essendo per queste  $\lim_{k \rightarrow +\infty} z_{k|x=0} = -\infty$  e  $\lim_{k \rightarrow +\infty} z_{k|x=A} = 0$ .

Se poi la  $z_k$  si pensa definita da variabili reali, essa ha differenziale totale

$$\begin{aligned} dz_k = & \left( k / \sqrt{A(k-1)} \right) dx + \left( (A - k(A+x)) / (2A\sqrt{A(k-1)}) \right) dA + \\ & + \left( ((x-A)k - 2x + A) / (2(k-1)\sqrt{A(k-1)}) \right) dk \end{aligned}$$

con componenti  $\partial z_k / \partial x$  sempre positiva,  $\partial z_k / \partial A$  sempre negativa e  $\partial z_k / \partial k$  sempre negativa ed ha per differenziale secondo una forma quadratica indefinita.

Impossibilitati a rappresentare graficamente la  $z_k$  che nella sua generalità è dipendente da  $x$ ,  $A$ ,  $k$  e da  $n$ , se ne mostra una rappresentazione parametrica.

Considerati come parametri le variabili  $n$  e  $k$ , le superfici di livello  $\sigma_n$  sono configurabili in una serie di spazi  $R_{nk}^3$  doppiamente indicati e se, inoltre, si ipotizza, in ciascuno di essi, parametro, la variabile  $A$ , si ha di tali  $R_{nk}^3$ , una rappresentazione planare con sistema di riferimento  $xz_k$ .

Stabilito poi un livello di significatività  $\alpha$ , (sia ad es.  $\alpha=0.05$ ), e tracciate nei piani  $xz_k$  le rette  $z_k = \pm 1.96$  restano, per ciascuna rappresentazione parametrica planare, individuate tre zone una di accettazione caratterizzata dai valori di  $z_k$  tali che  $-1.96 < z_k < +1.96$  e due di rifiuto l'una per valori di  $z_k \geq +1.96$  e l'altra per valori di  $z_k \leq -1.96$  per le quali si parla rispettivamente di autocorrelazione spaziale positiva e negativa.

A scopo illustrativo si presentano rappresentazioni parametriche planari di  $z_k$  per diversi valori di  $n$  e di  $k$  (fig. 4.1.n.k) che rendono evidenti alcune interrelazioni significative di tipo matematico-statistico tra le variabili  $x$ ,  $A$ ,  $k$ ,  $n$ .

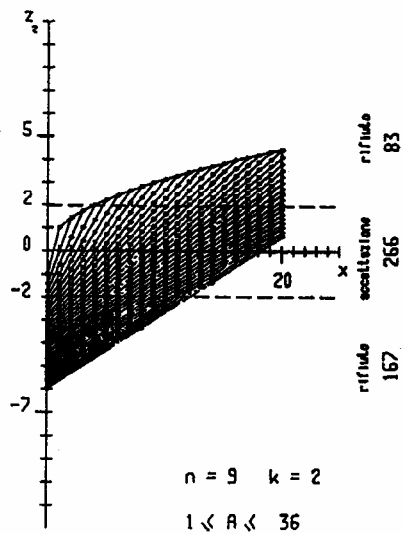


Fig. 4.1.9.2 punti = 516

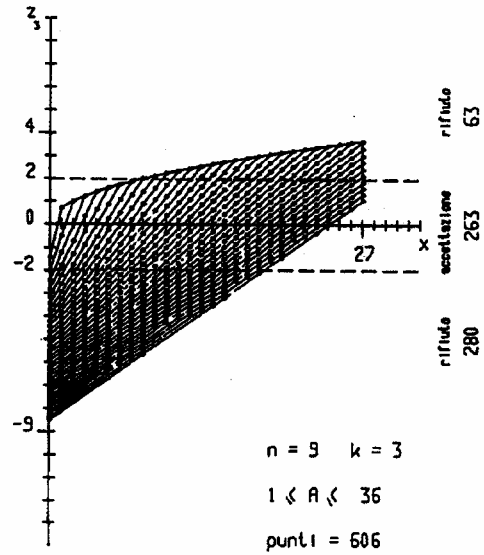


Fig. 4.1.9.3

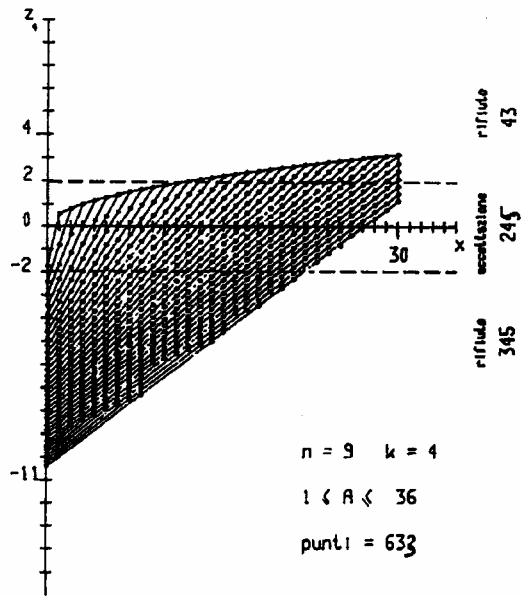


Fig. 4.1.9.4

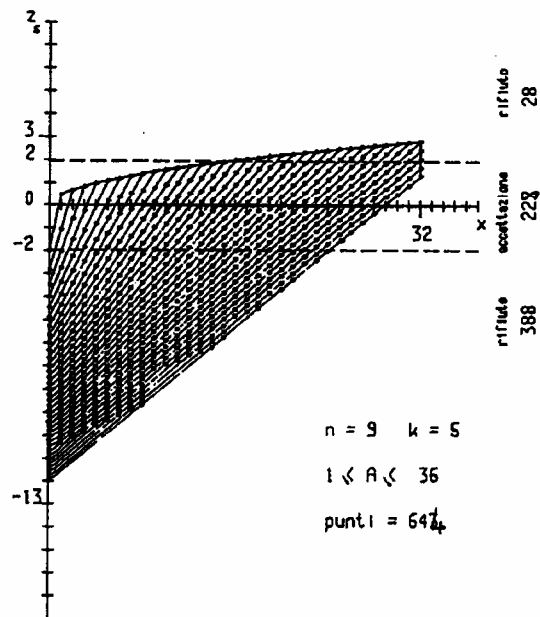


Fig. 4.1.9.5

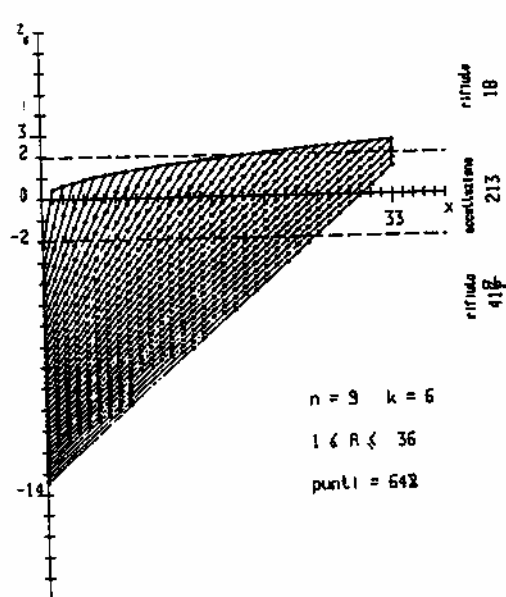


Fig. 4.1.9.6

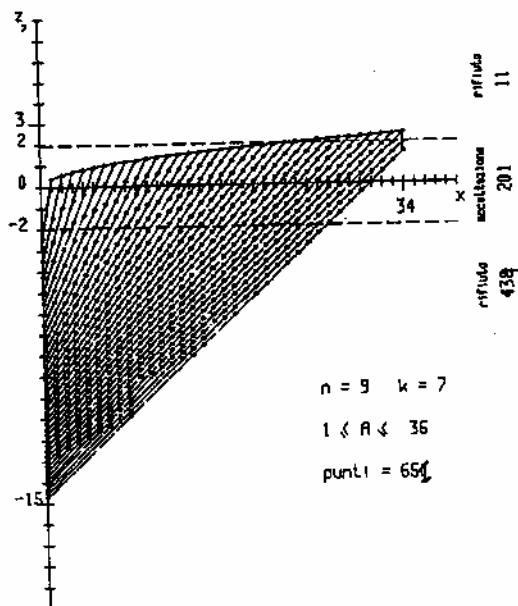


Fig. 4.1.9.7

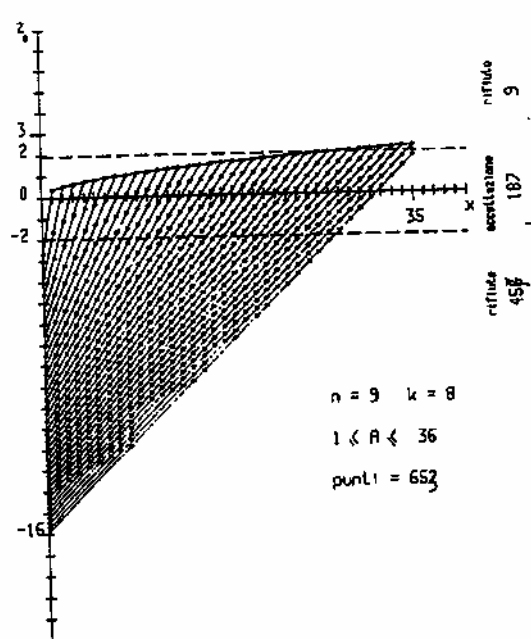


Fig. 4.1.9.8

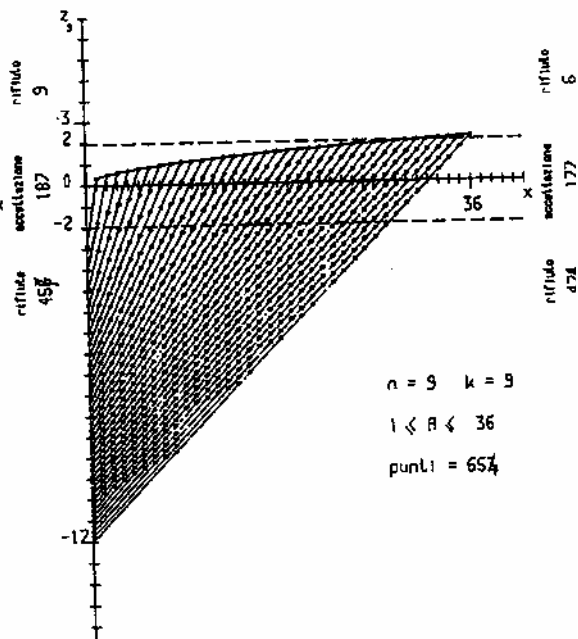


Fig. 4.1.9.9

Si riportano nel seguito alcune considerazioni di tipo matematico:

- nelle rappresentazioni parametriche planari di  $z_k$  i punti corrispondenti ad  $A=\text{costante}$  sono allineati;
- per ogni fissato  $k$ , se  $n > n'$  i punti della fig. 4.1.  $n'.k$  sono anche punti della fig. 4.1.  $n.k$ ;
- la simmetria dei valori è limitata al solo caso  $k=2$  e per valori di  $A \leq \binom{n}{2} - \text{int}((n-1)/2)^2$ ;
- per ogni fissato  $n$ , se  $k > k'$  si ha :

$$0 < z_{k'|x=A} < z_{k|x=A} \text{ per } 0 \leq A \leq \binom{n}{2} - \sum_{h=1}^{n-k'} \text{int}((n-h)/k');$$

- per ogni fissato  $n$ , se  $k > k'$  si ha :

$$|\{z_{k''} | z_{k''} < 0\}| \geq |\{z_{k'} | z_{k'} < 0\}|;$$

- per ogni fissato  $k$ ,  $z_k$  è dotata di:

$$\text{minimo assoluto } \min z_k = -\sqrt{\binom{n}{2}}(k-1) \text{ e}$$

$$\text{massimo assoluto } \max z_k = \sqrt{\binom{n}{2} - \sum_{h=1}^{n-k} \text{int}((n-h)/k)} / (k-1);$$

- per  $k=2$ , caso di modalità dicotomiche, è  $z_2 = (2x - A) / \sqrt{A}$  rappresentabile in una serie di

$$1/2 \left( \binom{n}{2} - 3 \binom{n}{2} \right) - \left( \sum_{h=1}^{n-2} \frac{\text{int}((n-h)/2)}{2} \right) - \sum_{h=1}^{\text{int}(n/2)} \binom{n-2h+1}{2}$$

$$\text{punti con } \min z_2 = -\sqrt{\binom{n}{2}} \text{ e } \max z_2 = \sqrt{\binom{n}{2} - \text{int}(((n-1)/2)^2)};$$

- per  $k=n$ , caso in cui le modalità cromatiche siano pari al numero delle unità territoriali, è per  $z_n$ :

$$\min z_n = -(n-1)\sqrt{n/2} \text{ e } \max z_n = \sqrt{n/2}.$$

Infine accanto alle considerazioni matematiche le rappresentazioni ne evidenziano alcune statistiche:

- all'aumentare di  $k$ , numerosità delle modalità cromatiche, i valori espressi da  $z_k$  tendono a collocarsi nella zona di rifiuto caratterizzata dalla presenza di autocorrelazione negativa;
- esiste  $k=k^*$ , con  $k^*$  minimo dipendente dal numero delle unità territoriali  $n$  e dal livello di significatività  $\alpha$ , tale che l'insieme dei valori  $z_k$  appartenenti

- alla zona di rifiuto con la presenza di autocorrelazione positiva è vuoto;
- esiste  $k=k^{**}$ , con  $k^{**}$  minimo dipendente da  $n$  ed  $\alpha$ , tale che i valori di  $z_{rs,k}$  nella zona di accettazione siano solo  $\binom{n}{2}$ .

#### 4.2 CASO DELLA VARIABILE $N_{rs}$

Se ci si limita a tener conto solo di congiunzioni che realizzano coppie prescelte di eventi di tipo  $rs$  con  $r \neq s$  per la variabile casuale  $N_{rs}$ , indicata con  $x$  una sua determinazione, è

$$z_{rs,k} = (k^2 x - 2A) / \sqrt{2Ak^2 + 4Dk - 4(A + 2D)}.$$

Questa è funzione reale delle variabili intere  $x, A, D, k$  ed in quanto definita per

$$\left\{ \begin{array}{l} k \geq 2 \\ 1 \leq A \leq \binom{n}{2} \\ 0 \leq x \leq \binom{n}{2} - \text{int}(((n-1)/2)^2) \\ x \leq A \\ D_{\min}(A) \leq D \leq D_{\max}(A), \end{array} \right.$$

con l'aggiunta della dipendenza delle determinazioni  $x$  da  $n, k$  e dagli operatori  $L$  e di quella dei valori  $D$  da  $n, A$  e dagli stessi operatori  $L$ .

La funzione  $z_{rs,k}$  è limitata inferiormente da

$$z_{rs,k|x=0} = -2A / \sqrt{2Ak^2 + 4Dk - 4(A + 2D)},$$

per la quale è  $\lim_{k \rightarrow +\infty} z_{rs,k|x=0} = 0$ .

È limitata superiormente da

$$z_{rs,k|x=A} = A(k^2 - 2) / \sqrt{2Ak^2 + 4Dk - 4(A + 2D)}$$

per  $1 \leq A \leq \binom{n}{2} - \text{int}(((n-1)/2)^2)$  ed è solamente maggiorata da

$z_{rs,k|x=A}$  per  $\binom{n}{2} - \text{int}(((n-1)/2)^2) < A \leq \binom{n}{2}$ , avendosi per questa

$$\lim_{k \rightarrow +\infty} z_{rs,k|x=A} = +\infty.$$

Pensata la  $z_{rs,k}$  definita da variabili reali continue, questa ha differenziale totale:

$$\begin{aligned} dz_{rs,k} = & \left( k^2 / \sqrt{2A(k^2 - 2) + 4D(k - 2)} \right) dx + \\ & - \left( (k^2 x + 2A)(k^2 - 2) - 8D(k - 2) / \sqrt{(2A(k^2 - 2) + 4D(k - 2))^3} \right) dA + \\ & + \left( 2(k^2 x + 2A)(k - 2) / \sqrt{(2A(k^2 - 2) + 4D(k - 2))} \right) dD + ((2kx(Ak^2 + 3Dk + \\ & - 4A - 8D) + 4A(Ak + D)) / \sqrt{(2A(k^2 - 2) + 4D(k - 2))^3}) dx \end{aligned}$$

con componenti  $\partial z_{rs,k} / \partial x$  sempre positiva,  $\partial z_{rs,k} / \partial A$  sempre negativa,  $\partial z_{rs,k} / \partial D \geq 0$  per  $(k^2 x - 2A)(k - 2) \geq 0$ ,  $\partial z_{rs,k} / \partial k$  sempre positiva.

Se si considerano inizialmente quali parametri le variabili  $n, k$  si hanno ipersuperfici di livello rappresentabili in spazi  $R_{nk}^4$  e se inoltre si considerano parametri  $A$  e  $D$  si ottengono di  $z_{rs,k}$  rappresentazioni planari con sistema di riferimento  $xz_{rs,k}$ .

Si stabilisca poi anche per  $z_{rs,k}$  il livello di significatività  $\alpha$ , (nell'es. è  $\alpha=0.05$ ), si traccino nei piani  $xz_{rs,k}$  le rette corrispondenti di delimitazione delle regioni di accettazione, in tal modo accanto a delle considerazioni di tipo matematico:

- nelle rappresentazioni parametriche planari di  $z_{rs,k}$  i punti corrispondenti ad  $A=\text{costante}$  e  $D=\text{costante}$  sono allineati;
- per ogni fissato  $k$ , se  $n'' > n'$  della fig. 4.2.  $n'.k_{rs}$  sono anche punti della fig. 4.2.  $n''.k_{rs}$ ;
- nel caso sia  $k=2$ , la  $z_{rs,k} = z_2 = (2x - A) / \sqrt{A}$  è indipendente da  $D$ ; se ne evidenziano anche alcune di tipo statistico quali:
- all'aumentare di  $k$  i valori espressi da  $z_{rs,k}$  tendono a collocarsi nella zona di rifiuto caratterizzata dalla presenza di autocorrelazione positiva;
- esiste  $k=k^{***}$ , con  $k^{***}$  minimo dipendente dal numero delle unità territoriali  $n$  e dal livello di significatività  $\alpha$ , tale che l'insieme dei valori  $z$  appartenenti alla zona di accettazione sia minimo.

Tali considerazioni matematico-statistiche sono rese intuitive attraverso le rappresentazioni illustrate (fig. 4.2.  $n.k_{rs}$ ) pur se limitate ai valori marginali degli intervalli di variabilità di  $D$ .

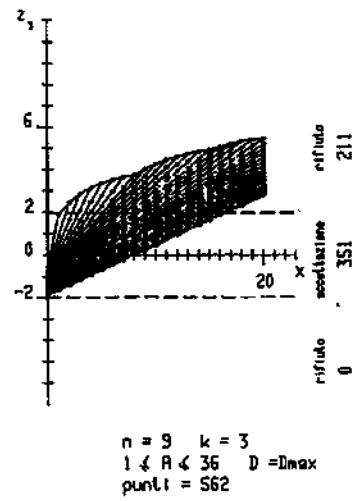
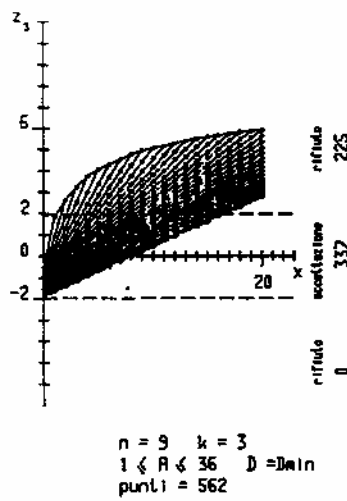


Fig. 4.2.9.3

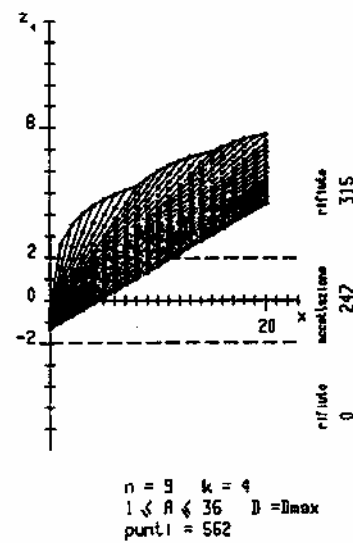
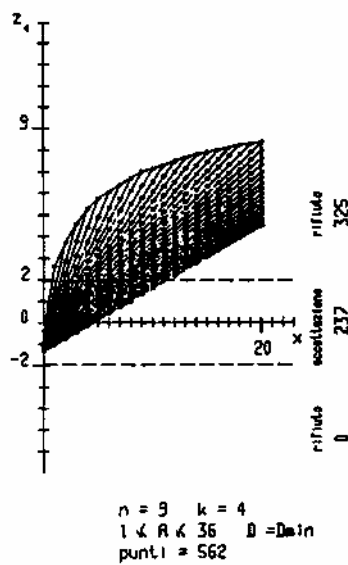
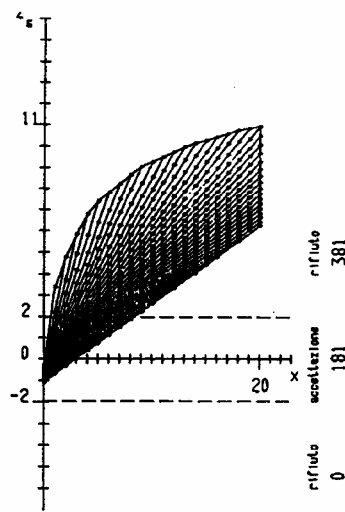
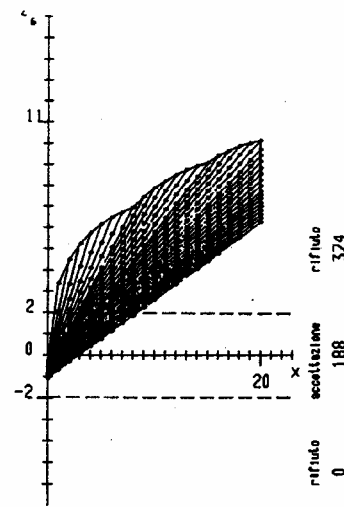


Fig. 4.2.9.4

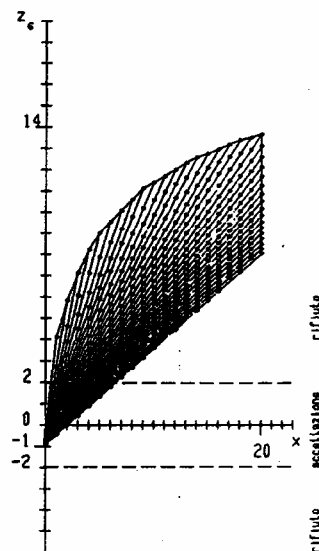


$n = 9 \quad k = 5$   
 $1 \leq A \leq 36 \quad D = D_{\min}$   
 punti = 562

Fig. 4.2.9.5

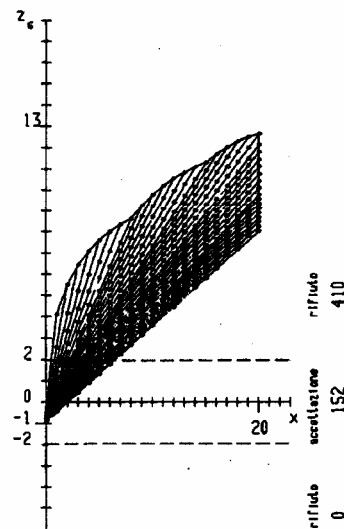


$n = 9 \quad k = 5$   
 $1 \leq A \leq 36 \quad D = D_{\max}$   
 punti = 562



$n = 9 \quad k = 6$   
 $1 \leq A \leq 36 \quad D = D_{\min}$   
 punti = 562

Fig. 4.2.9.6



$n = 9 \quad k = 6$   
 $1 \leq A \leq 36 \quad D = D_{\max}$   
 punti = 562

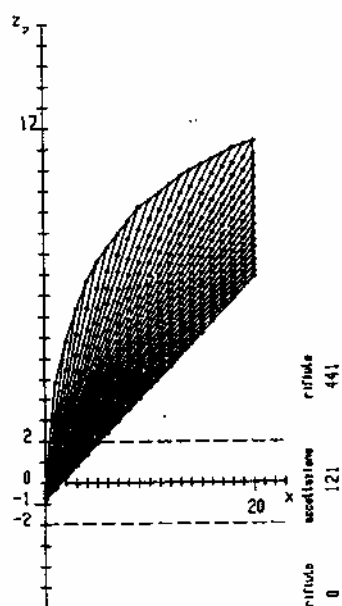
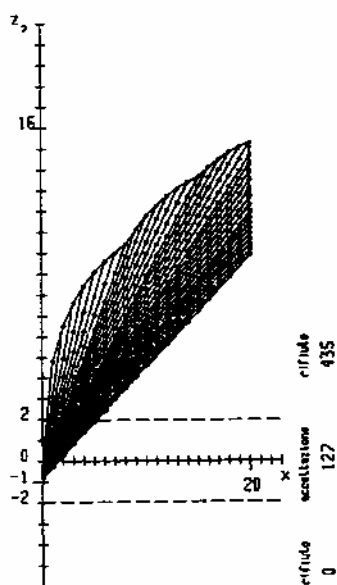


Fig. 4.2.9.7



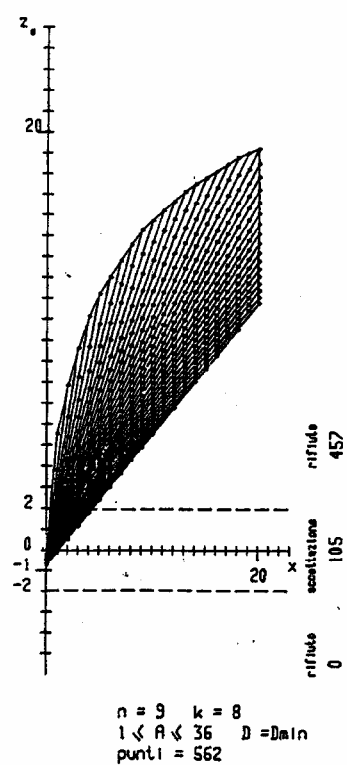
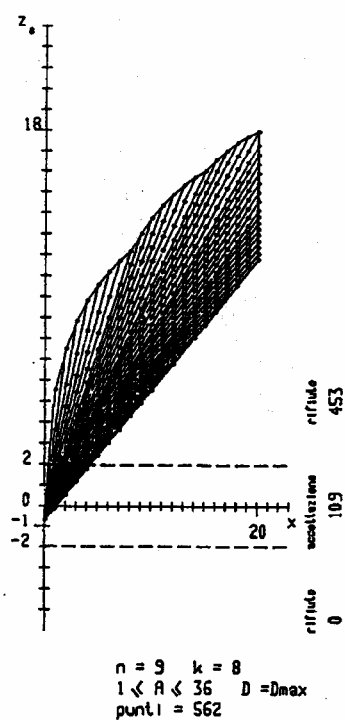


Fig. 4.2.3.8



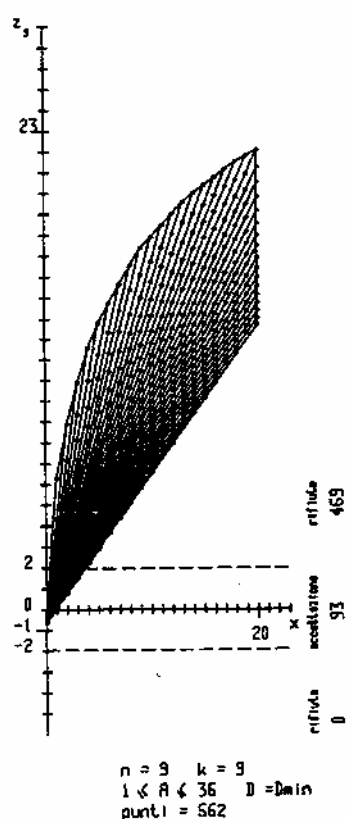
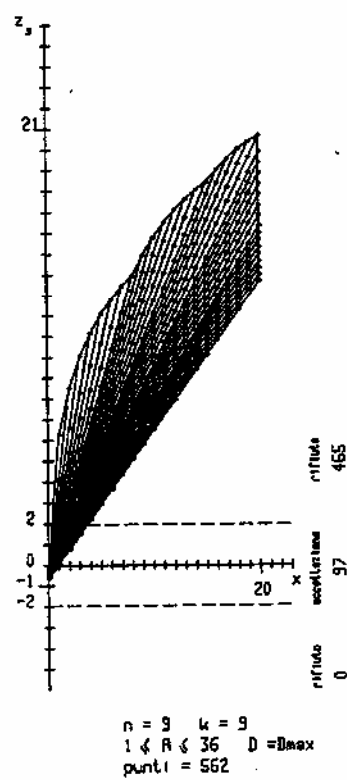


Fig. 4.2.3.9



### 4.3 CASO DELLA VARIABILE $N_{rr}$

Infine, se si fa riferimento alla variabile casuale  $N_r$  è

$$z_{rr,k} = (k^2x - A) / \sqrt{Ak^2 + 2Dk - (A + 2D)}$$

funzione reale delle variabili intere  $x$ ,  $A$ ,  $D$ ,  $k$  ed  $n$  definita per:

$$\begin{cases} k \geq 2 \\ 0 \leq x \leq A \\ 1 \leq A \leq \binom{n}{2} \\ D_{\min}(A) \leq D \leq D_{\max}(A) \end{cases}$$

con l'attenzione riservata (4.2) per le determinazioni di  $x$  e per i valori assumibili dalla variabile  $D$ .

È limitata inferiormente da  $z_{rr,k}|_{x=0}$  e superiormente da  $z_{rr,k}|_{x=A}$  aventi rispettivamente  $\lim_{k \rightarrow \infty} z_{rr,k}|_{x=0} = 0$  e  $\lim_{k \rightarrow \infty} z_{rr,k}|_{x=A} = +\infty$ .

Considerata la  $z_{rr,k}$  definita da variabili reali continue essa ha differenziale totale:

$$\begin{aligned} dz_{rr,k} = & \left( k^2 / \sqrt{A(k^2 - 1) + 2D(k - 1)} \right) dx + \\ & - \left( ((k + 1)(A + k^2x) + 4D) / \sqrt{4(k - 1)(Ak + A + 2D)^3} \right) dA + \\ & + \left( (k - 1)(k^2x - A) / \sqrt{A(k^2 - 1) + 2D(k - 1)} \right) dD + \\ & \left( (k^3xA + 3k^2xD + k(A^2 - 2xA - 4xD) + AD) / \sqrt{((k - 1)(Ak + A + 2D))^3} \right) dk \end{aligned}$$

con componenti  $\partial z_{rr,k} / \partial x$  sempre positiva,  $\partial z_{rr,k} / \partial A$  sempre negativa,  $\partial z_{rr,k} / \partial D \geq 0$  per  $k^2x - A \geq 0$ ,  $\partial z_{rr,k} / \partial x$  sempre positiva.

Si traggono infine dalla  $z_{rr,k}$  le seguenti osservazioni:

- nelle rappresentazioni parametriche di  $z_{rr,k}$  i punti corrispondenti ad  $A = \text{costante}$  e  $D = \text{costante}$  sono allineati e costituiscono una nuvola di al più

$$1/2 \left( \binom{n}{2}^2 + 3 \binom{n}{2} \right) - \sum_{h=2}^{n-2} \binom{n-h}{2} \text{ punti};$$

- per ogni fissato  $k$ , se  $n' > n$  i punti della fig. 4.3.  $n'.k_n$  sono anche punti della fig. 4.3.  $n''.k_n$ ;

- nel caso sia  $k=2$ , si ha  $z_{n,2} = (4x - A)\sqrt{3A + 2D}$  con  $\min z_{n,2} = -\sqrt{\binom{n}{2}}/3$

$$\text{e } \max z_{n,2} = 3\binom{n}{2} / \sqrt{3\binom{n}{2} + 2};$$

- nel caso sia  $k \geq n$  si ha l'equivalenza logica  $z_{n,k} < 0 \iff x=0$ .

Tali osservazioni si rendono evidenti nelle rappresentazioni parametriche planari (fig. 4.3. n.k.) pur se limitate ai valori marginali  $D_{\min}(A)$  e  $D_{\max}(A)$ .

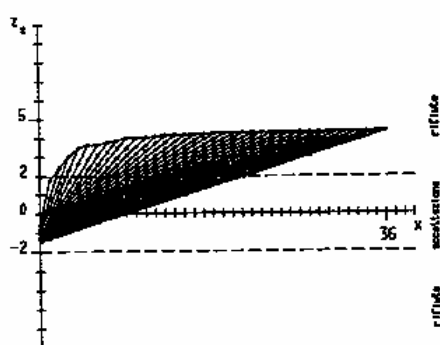
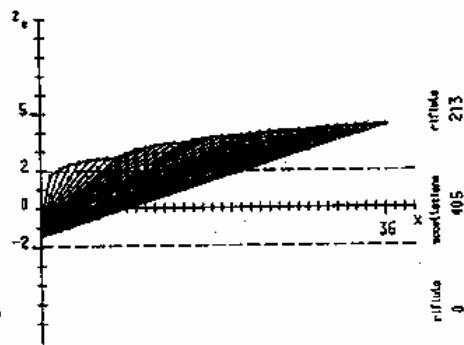


Fig. 4.3.9.2

$n = 9$   $k = 2$   
 $1 \leq A \leq 36$   $D = D_{\min}$   
 punti = 618



$n = 9$   $k = 2$   
 $1 \leq A \leq 36$   $D = D_{\max}$   
 punti = 618

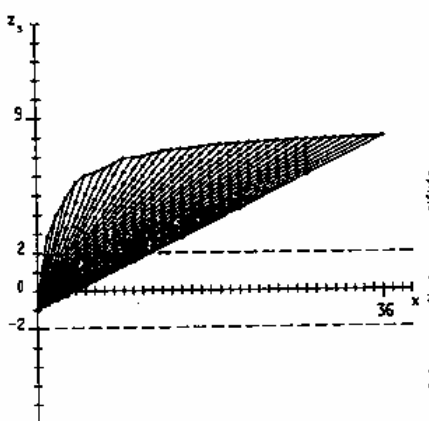
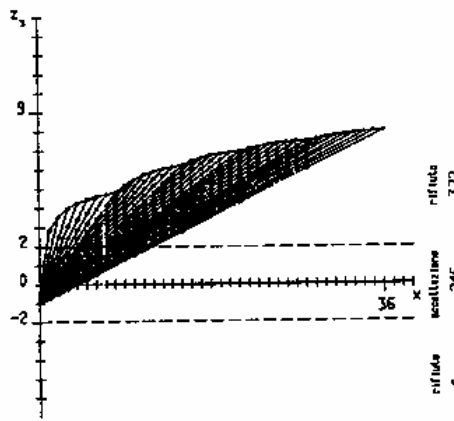


Fig. 4.3.9.3

$n = 9$   $k = 3$   
 $1 \leq A \leq 36$   $D = D_{\min}$   
 punti = 618



$n = 9$   $k = 3$   
 $1 \leq A \leq 36$   $D = D_{\max}$   
 punti = 618

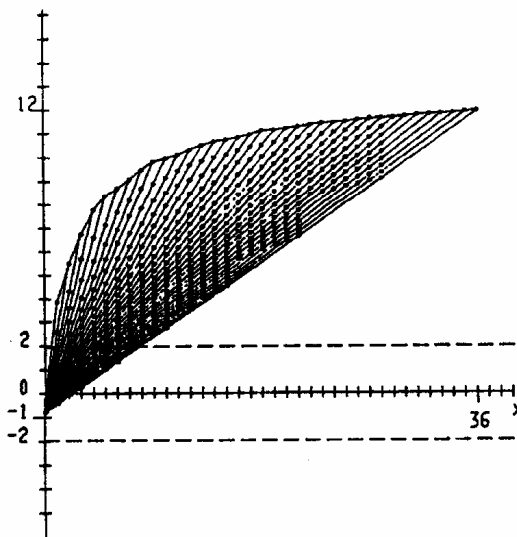
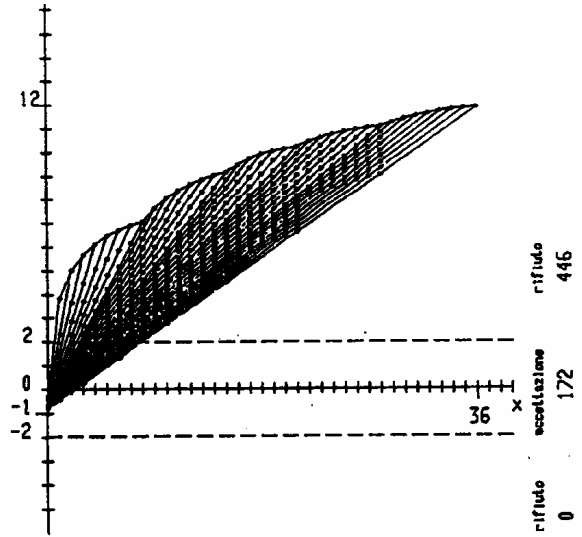


Fig. 4.3.9.4

$n = 9 \quad k = 4$   
 $1 \leq A \leq 36 \quad D = D_{min}$   
 punti = 618



$n = 9 \quad k = 4$   
 $1 \leq A \leq 36 \quad D = D_{max}$   
 punti = 618

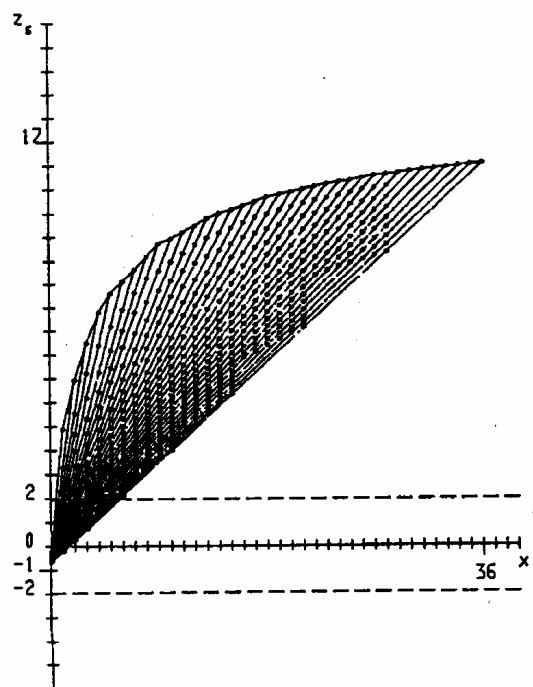
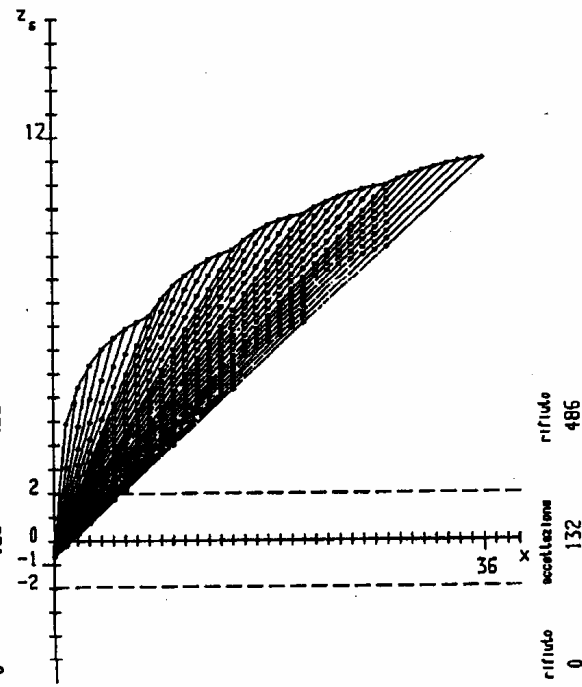
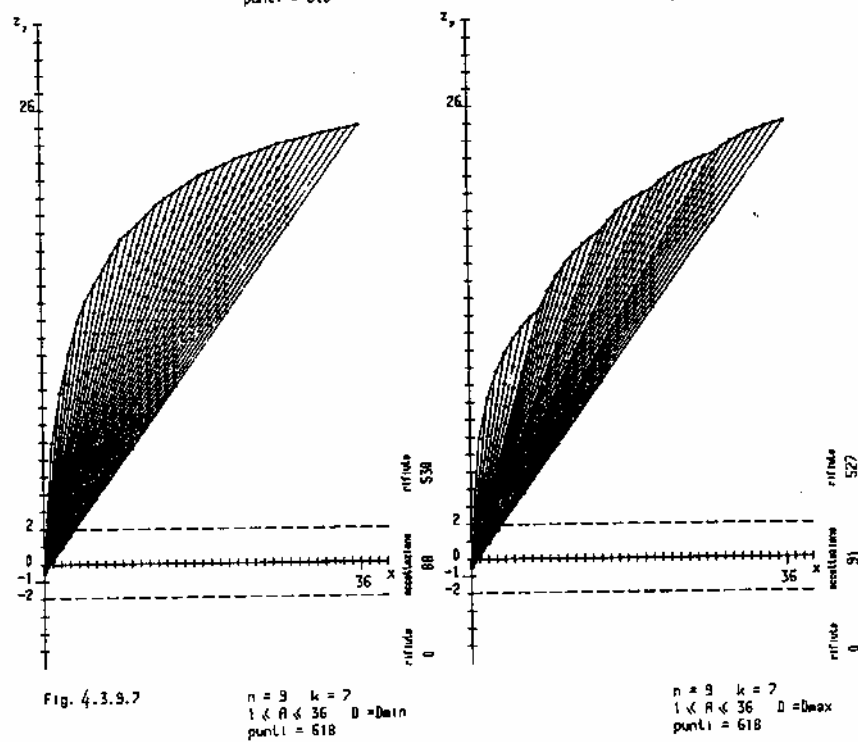
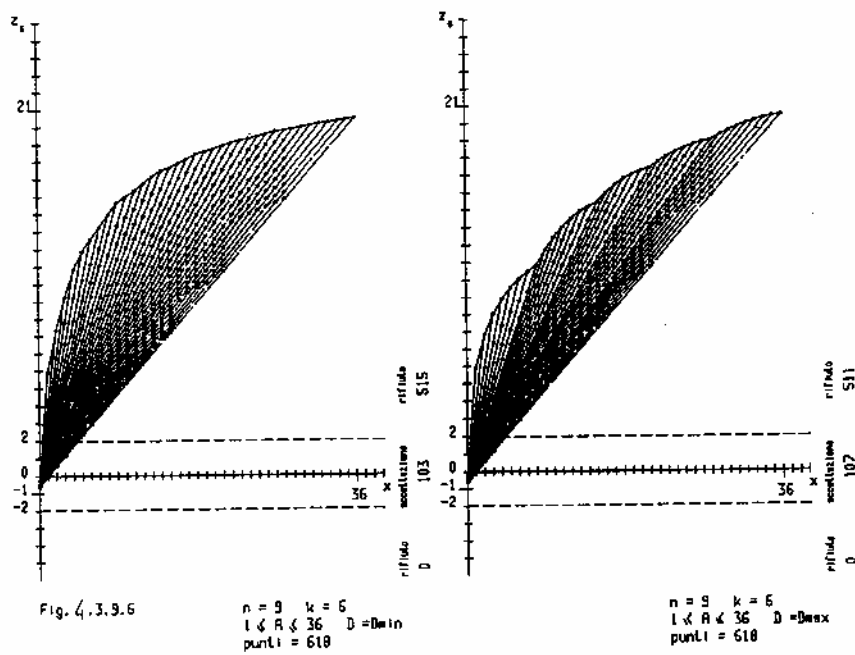


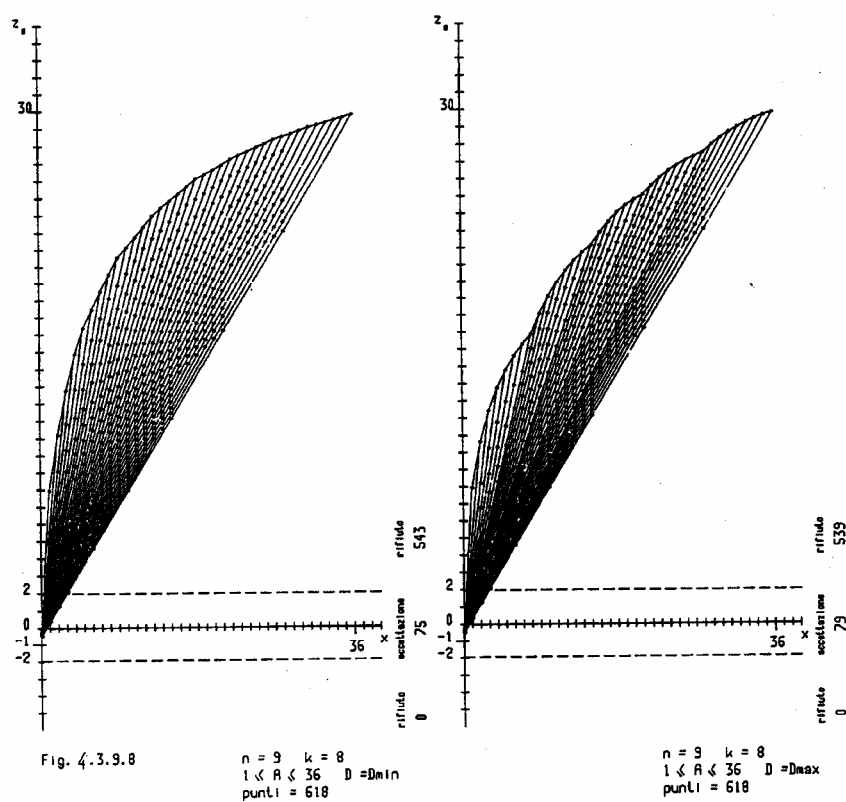
Fig. 4.3.9.5

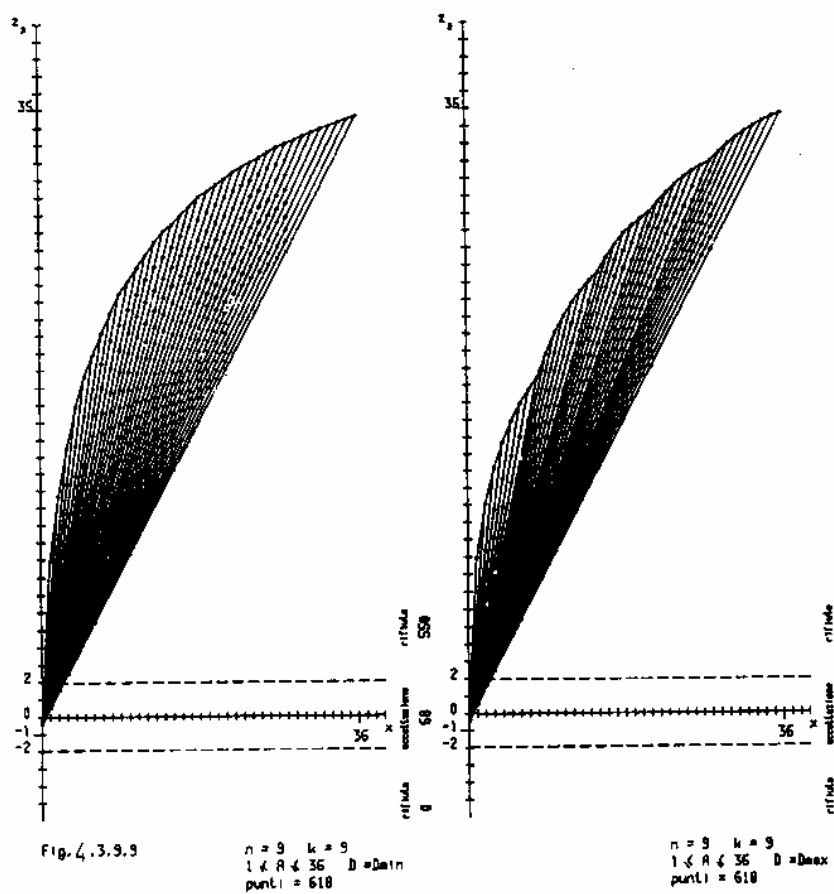
$n = 9 \quad k = 5$   
 $1 \leq A \leq 36 \quad D = D_{min}$   
 punti = 618



$n = 9 \quad k = 5$   
 $1 \leq A \leq 36 \quad D = D_{max}$   
 punti = 618







## 5. CONCLUSIONI

L'itinerario seguito induce a legittimare un'asserzione di fondo ed alcune possibili implicazioni.

La prima si riassume nell'incidenza della numerosità policromica  $k$  sulla capacità del test  $z$  a svolgere il suo ruolo in tutte le condizioni operative, il che, in altre parole, parla di una necessità di riconsiderare non tanto il campo di applicabilità del test, quanto, piuttosto, la sua formulazione in generale.

Le implicazioni ulteriori, ed in particolare quelle desumibili dalle simulazioni effettuate, secondo cui  $k$  possa essere al più dell'ordine di  $\sqrt{n}$ , necessitano di ulteriori ricerche finalizzate all'individuazione di un valido criterio per definire la soglia.

In questa strada si cercheranno ulteriori approfondimenti e collegamenti tra sistema informativo e sistema descrittivo dei fatti territoriali.

## BIBLIOGRAFIA

1. Anselin L. (1980) "*Estimation methods for spatial autoregressive structures: a study in spatial econometrics*", Ithaca, Cornell N.J. University.
2. Bahrenberg G., Fischer M., Nijdam P. (1984) "*Recent development in spatial data analysis. Methodology measurement models*", Gower Aldershot.
3. Cliff A.D., Ord J.K. (1981a) "*Spatial and temporal analysis: autocorrelation in space and time*", in Wrigley N. e Bennet R.J. (eds), *Quantitative Geography: A British View*, Londra, Routledge e Kegan, 104-110.
4. Cliff A.D., Ord J.K. (1981b) "*The effects of spatial autocorrelation of geographical modelling*", in Craig R.D. e Labowitz M.L. (eds), *Future trends in Geomathematics*, Londra, Pion, 108-137.
5. Gatrell A.C. (1979), "*Autocorrelation in spaces*", *Environment and Planning A* 11, 507-516.
6. Hubert L.J., Golledge R.G. e Costanzo C.N. (1981) "*Generalized procedures for evaluating spatial autocorrelation*", *Geographical Analysis* 13, 224-233.
7. Martin R.L. (1974) "*On autocorrelation, bias and the use of first spatial differences in regression analysis*", *Area* 6, 185, 194.
8. Moran P. (1950), "*Notes on continuous stochastic phenomena*", *Biometrika* 37, 17-23.
9. Sclocco T. e Visini G. (1982), "*Sui primi due momenti della statistica joint-count di Moran*", *Atti VI Congresso A.M.A.S.E.S.*, 621-642.
10. Wrigley N. (1985), "*Categorical data analysis for geographer and environmental scientists*", Longman, New York.