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

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

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

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

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

1. SIMBOLOGIA E CONSIDERAZIONI PRELIMINARI.

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

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

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

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

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

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

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

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

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

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

Valgono le seguenti proposizioni, di immediata dimostrazione.

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

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

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

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

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

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

La somma S dei termini di tale progressione è allora

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

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

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

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

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

il terzo membro.

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

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

Poichè per la proposizione (1.1) è

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

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

2. M - TRASFORMATA DI FOURIER.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Teorema 2.2. Le funzioni

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

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

Precisamente risulta

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

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

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

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

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

Per la (2.1) risulta

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

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

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

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

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

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

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

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

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

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

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

3. M - TRASFORMATE DI FUNZIONI DI PROBABILITÁ.

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

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

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

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

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

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

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

Diamo allora le seguenti definizioni.

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

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

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

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

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

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

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

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

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

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

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

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

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

Dimostrazione. Risulta per la (3.3)

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

Inoltre

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

❑

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Nel corso dei due lavori, però, vengono esaminate variabili casuali particolari, in cui $\lvert h(\underline{z})\rvert$ è, per ogni $\underline{z}\in J_n(m)$, sempre uguale o a zero o ad uno, e vengono forniti criteri per la misura della discrepanza da una distribuzione uniforme validi solo per tali variabili.

Se $\underline{X}$ non è uniforme, detto S l'insieme dei $\underline{z}\in J_n(m)-\{\underline{0}\}$ tali che $\lvert h(\underline{z})\rvert\neq 0$, in [1] viene proposto di misurare la vicinanza di $\underline{X}$ da una variabile equidistribuita in $P_n(m)$ tramite il numero

$$(4.1)\qquad \mu_n=\min_{\underline{z}\in S}\lvert\underline{z}\rvert$$

e in [2] viene proposto di misurare tale vicinanza con il numero

$$(4.2)\qquad \sigma_n=\frac{\pi^{n/2}\mu_n^n}{m\,\Gamma\left(\frac{n+2}{2}\right)}$$

esprimente il volume di una ellissoide in R^n, ritenuta particolarmente significativa.

Chiamiamo, per comodità, μ_n e σ_n rispettivamente **vicinanza di Coveyou**

e **di Knuth** e i loro reciproci $M_n=1/\mu_n$ e $S_n=1/\sigma_n$ rispettivamente **discrepanza di Coveyou e di Knuth.**

Definizione 4.1. Diciamo **generatore ricorrente di ordine k di successioni pseudocasuali**, con modulo il numero intero positivo m, una formula del tipo

$$x_{h+k}=G(x_h, x_{h+1}, \ldots, x_{h+k-1}), \tag{4.3}$$

dove G è una funzione definita in $I_k(m)$ ed a valori in I(m).

La funzione G dipende in genere da certi parametri $\alpha_1, \alpha_2, \ldots, \alpha_s$.

La successione $\{x_h\}_{h\in N}$ è determinata dalla funzione G e dai valori $x_0, x_1, \ldots, x_{k-1}$, detti valori iniziali che devono essere fissati a priori in I(m).

Poichè gli elementi di $I_k(m)$ sono m^k, è facile dimostrare che la successione $\{x_h\}_{h\in N}$ è periodica e che, se m è la lunghezza dell'antiperiodo e λ quella del periodo risulta $\mu+\lambda\leq m^k$.

Definizione 4.2. Si dice **successione di numeri pseudocasuali generata** dalla (4.3) la successione di termine generale

$$y_h=x_h/m \tag{4.4}$$

formata da elementi di $P_n(m)$. [1]

Supponendo che λ non sia troppo piccolo (in pratica almeno dell'ordine di 10^8) e trascurando l'antiperiodo, al generatore (4.3) viene associata la variabile casuale X definita in P(m) con probabilità, $\forall x\in P(m)$,

$$f(x)=\frac{n(x)}{\lambda} \tag{4.5}$$

dove con n(x) si indica il numero di volte in cui, in un segmento S della successione di lunghezza λ, situato dopo l'antiperiodo, y_h ha assunto il valore x.

In generale, per ogni $n\geq 1$ e non troppo elevato (in pratica $n\leq 10$), si associa alla (4.3) la variabile casuale $\underline{X}_n$, definita in $P_n(m)$, con probabilità

$$f(\underline{x})=\frac{n(\underline{x})}{\lambda}\ ,\ \forall \underline{x}\in P_n(m)\ , \tag{4.6}$$

---

(1) Ci limitiamo in questo lavoro, per semplicità, al caso in cui la successione di numeri pseudocasuali è data dalla (4.4), anche se vi sono molti altri criteri per ottenere i numeri y_h. Ad es., per m=2, gli x_h sono cifre binarie. Si possono ottenere numeri pseudocasuali "mettendo insieme" gruppi di tali cifre. Si vedano ad esempio i lavori [6], [7].

dove $n(\underline{x})$ è il numero di volte in cui la n-pla $\underline{y}_h=(y_h, y_{h+1}, \dots, y_{h+n-1})$ ha assunto, al variare di y_h in S, il valore $\underline{x}$.

Evidentemente $\underline{X}_n$ ha n componenti tutte somiglianti ad X, per cui valgono per $\underline{X}_n$ tutte le considerazioni svolte nei paragrafi precedenti.

Definizione 4.3. Diciamo **vicinanza di ordine n** della successione $\{y_h\}_{h\in N}$ da una variabile casuale equidistribuita la vicinanza di $\underline{X}_n$ da una variabile casuale equidistribuita in $P_n(m)$.

In maniera analoga definiamo la discrepanza di ordine n di $\{y_h\}_{h\in N}$ da una variabile casuale equidistribuita.

Le misure di discrepanza M_n e S_n tengono conto solo del disturbo arrecato alla uniformità dall'onda con massima lunghezza d'onda e con modulo dell'ampiezza non nullo . Non viene perciò preso in considerazione

a) il disturbo arrecato dalle altre onde;

b) il valore assunto, per ogni $\underline{z}$, da $|h(\underline{z})|$, quando $|h(\underline{z})|\neq 0$.

In [5] ed in questo lavoro si propongono misure di discrepanza $D_{n,r}$ dipendenti da un parametro "principale" $r\in[1,+\infty)$ e da altri parametri k,α tali che $D_{n,r}$

a) tenga conto delle (I), (II) e delle altre osservazioni emerse in [1] e [2];

b) sia applicabile a qualsiasi variabile casuale $\underline{X}$ definita in $P_n(m)$;

c) per valori particolari dei parametri e per le variabili casuali per cui sono applicabili i criteri M_n e S_n, abbia tali numeri come termini di maggior peso, in modo che, più o meno grossolanamente, $D_{n,r}$ possa essere approssimato da essi;

d) sia un valore particolare di una distanza nello spazio $F_n(m)$;

e) per $r\to+\infty$ e per particolari valori di k e α sia $D_{n,r}=M_n$ o $D_{n,r}=S_n$.

A tale scopo si suggerisce di porre

$$(4.7)\quad D_{n,r}=\Big(\sum_{\underline{z}\in J_n(m)-\{\underline{0}\}} p(\underline{z})|h(\underline{z})|^r\Big)^{1/r}$$

con le seguenti ipotesi sul numero $p(\underline{z})$:

(1) $p(\underline{z})=q(|\underline{z}|)$, dove q è una funzione reale di variabile reale;

(2) $q(x)>0$, $\forall x\geq 0$;

(3) q(x) è strettamente decrescente e tende a zero per $x\to+\infty$.

Essendo $|h(\underline{z})|\leq 1$, $\forall \underline{z}\in J_n(m)$, risulta

$$(4.8)\quad D_{n,r}\leq\Big(\sum_{\underline{z}\in J_n(m)-\{\underline{0}\}} p(\underline{z})\Big)^{1/r}.$$

Poichè il numero di elementi di $J_n(m)$ è, nei casi che vengono considerati in pratica, elevatissimo, per poter calcolare senza troppe difficoltà sia un maggiorante dell'insieme dei numeri $D_{n,r}$ al variare di $\underline{X}$ e sia un valore approssimato del numero $D_{n,r}$, può convenire aggiungere l'ipotesi

(4) $p(\underline{z})$ è, per $|\underline{z}| \to +\infty$, un infinitesimo di ordine superiore ad n.

Infatti, se vale la (4), la serie $\sum_{\underline{z}\in Z^n-\{\underline{0}\}} p(\underline{z})$ è convergente e detta A la sua somma, risulta $D_{n,r} \le A^{1/r}$ e, per m e r elevati, la somma parziale della serie, limitata ai termini $\underline{z}\in J_n-\{\underline{0}\}$, è molto vicina ad A.

5. SPAZI METRICI DI DENSITÁ DI PROBABILITÁ

Consideriamo l'insieme $F_n(m)$ delle funzioni definite in $P_n(m)$ ed a valori in C.

Per ogni coppia (g_1, g_2) di elementi di $F_n(m)$ aventi come m - coefficienti di Fourier di indice $\underline{z}\in J_n(m)$ rispettivamente $h_1(\underline{z})$ e $h_2(\underline{z})$, consideriamo il numero.

$$(5.1)\quad D_{n,r}(g_1, g_2)=\left(\sum_{\underline{z}\in J_n} p(\underline{z})|h_1(\underline{z})-h_2(\underline{z})|^r\right)^{1/r}$$

dove i $p(\underline{z})$ sono numeri soddisfacenti (1), (2), (3).

Proposizione 5.1. L'applicazione

$$(5.2)\quad D_{n,r}:(g_1, g_2)\in F_m^2(m)\to D_{n,r}(g_1, g_2)$$

è una metrica in $F_n(m)$ per ogni $r\in[1,+\infty)$.

Dimostrazione. Per le (1), (2), (3), si ha $D_{n,r}(g_1, g_2)=0 \Rightarrow h_1(\underline{z})=h_2(\underline{z})$, $\forall \underline{z}\in J_n$.

Allora, per il teorema 2.2, $D_{n,r}(g_1, g_2)=0 \Rightarrow g_1=g_2$.

La proprietà simmetrica è evidente.

Resta da dimostrare che, se g_1, g_2, g_3 sono tre elementi qualsiasi di $F_n(m)$, rispettivamente con m - coefficienti di Fourier $h_1(\underline{z})$, $h_2(\underline{z})$, $h_3(\underline{z})$, $\forall \underline{z}\in J_n$, allora risulta

$$(5.3)\quad D_{n,r}(g_1, g_2)\le D_{n,r}(g_1, g_3)+D_{n,r}(g_2, g_3).$$

Poniamo $a_i(\underline{z})=(-1)^i\, p(\underline{z})^{1/r}[h_i(\underline{z})-h_3(\underline{z})]$, i=1,2.

Allora la (5.3) si può scrivere

$$\left(\sum_{\underline{z}\in J_n(m)}|a_1(\underline{z})+a_2(\underline{z})|^r\right)^{1/r} \le \left(\sum_{\underline{z}\in J_n(m)}|a_1(\underline{z})|^r\right)^{1/r}+\left(\sum_{\underline{z}\in J_n(m)}|a_2(\underline{z})|^r\right)^{1/r}.$$

Essendo $r\ge 1$ si riduce alla disuguaglianza di Minkowsky (cfr. ad es. [3]).❑

Sia $G_n(m)$ il sottoinsieme di $F_n(m)$ formato dalle densità di probabilità delle variabili casuali definite in $P_n(m)$. Allora dalla proposizione 5.1 seguono le:

Proposizione 5.2. $G_n(m)$ è uno spazio metrico rispetto alla distanza data dalla (5.2).

Proposizione 5.3. Se g è un qualsiasi elemento di $G_n(m)$ con m - coefficiente di Fourier $h(\underline{z})$, $\forall \underline{z} \in J_n$ ed u è la densità di probabilità della variabile casuale equidistribuita in $P_n(m)$, allora la distanza $D_{n,r}(g,u)$ si riduce alla (4.7).

Definizione 5.1. Siano S, T, H tre insiemi non vuoti con $T \subseteq R$ e sia $f_\lambda: S \to T$ una funzione dipendente da un parametro $\lambda \in H$. Diciamo che $\underline{z}_0 \in S$ è un punto di massimo uniforme per f_λ al variare di λ se risulta $f_\lambda(\underline{z}_0) \geq f_\lambda(\underline{z})$, $\forall \underline{z} \in S$ e $\forall \lambda \in H$.

Dalla formula (5.1) si deduce la

Proposizione 5.4. Siano g_1, g_2 elementi di $G_n(m)$ aventi come m - coefficienti di Fourier di indice $\underline{z} \in J_n(m)$ rispettivamente $h_1(\underline{z})$ e $h_2(\underline{z})$ e sia $p(\underline{z})$ una funzione definita in $J_n(m)$ e soddisfacente le (1), (2), (3).

Se la funzione $f_r(\underline{z}) = (p(\underline{z}))^{1/r} |h_1(\underline{z}) - h_2(\underline{z})|$ è dotata di un punto dimassimo uniforme $\underline{z}_0$ al variare di r ed esiste $\lim_{r \to +\infty} D_{n,r}(g_1, g_2)$ allora

$$(5.4) \quad \lim_{r \to +\infty} D_{n,r}(g_1, g_2) = |h_1(\underline{z}_0) - h_2(\underline{z}_0)| \lim_{r \to +\infty} (p(\underline{z}_0))^{1/r} .$$

In particolare, per $g_1 = g$, con m-coefficiente di Fourier $h(\underline{z})$ e per $g_2 = u$, densità di probabilità della variabile casuale equidistribuita in $P_n(m)$, si ha

$$(5.5) \quad \lim_{r \to +\infty} D_{n,r} = |h(\underline{z}_0)| \lim_{r \to +\infty} (p(\underline{z}_0))^{1/r} .$$

Dimostrazione. Poniamo, per ogni $\underline{z} \in J_n(m)$, $f_r(\underline{z}) = p(\underline{z})^{1/r} |h_1(\underline{z}) - h_2(\underline{z})|$, $\forall r \geq 1$.

Se $\underline{z}_0$ è un punto di massimo uniforme per $f_r(\underline{z})$ al variare di r dalla (5.1) segue

$$(5.6) \quad D_{n,r}(g_1, g_2) = f_r(\underline{z}_0) \left[1 + \sum_{\underline{z} \in J_n - \{\underline{z}_0\}} \left(f_r(\underline{z}) / f_r(\underline{z}_0) \right)^r \right]^{1/r} .$$

Poichè $\underline{z}_0$ è un punto di massimo uniforme per $f_r(\underline{z})$ e $r \geq 1$ l'espressione fra parentesi quadre è non inferiore a 1 e limitata al variare di r per cui, per $r \to +\infty$, ha limite 1.

Segue che

$$\lim_{r \to +\infty} D_{n,r}(g_1, g_2) = \lim_{r \to +\infty} f_r(\underline{z}_0) = |h_1(\underline{z}_0) - h_2(\underline{z}_0)| \lim_{r \to +\infty} p(\underline{z}_0)^{1/r} \quad \square$$

Esempio 5.1

In [5] è stato suggerito di porre

$$(5.7) \qquad p(\underline{z}) = (k/|\underline{z}|^{\alpha})^r, \text{ con } \alpha > 0, |\underline{z}| \neq 0, k > 0.$$

Poichè per $|\underline{z}|=1$ si ha $p(\underline{z})=k^r$, per ogni $h>0$, ponendo $p(\underline{0})=(k+h)^r$ si ottiene una funzione $p(\underline{z})$ soddisfacente le (1), (2), (3) del paragrafo 4, e, per $\alpha>n/r$, anche alla (4).

Risulta

$$f_r(\underline{z})=p(\underline{z})^{1/r}|h_1(\underline{z})-h_2(\underline{z})|=\begin{cases}(k+h)\cdot|h_1(\underline{0})-h_2(\underline{0})| & \text{per } \underline{z}=\underline{0}\\ \dfrac{k}{|\underline{z}|^{\alpha}}|h_1(\underline{z})-h_2(\underline{z})| & \text{per } \underline{z}\neq\underline{0}\end{cases}$$

La $f_r(\underline{z})$ è costante al variare di r e quindi le condizioni di esistenza di un massimo uniforme e del $\lim_{r\to+\infty} p(\underline{z})^{1/r}$ sono banalmente soddisfatte.

Osservazione 5.1. Dalla (5.5), per $p(\underline{z})$ definita dalla (5.7), seguono come casi particolari le discrepanze M_n e S_n.

Infatti le (5.5) e (5.7) implicano

$$\lim_{r\to+\infty} D_{n,r} = \max_{\underline{z}\in J_n(m)-\{\underline{0}\}} k|h(\underline{z})|/|\underline{z}|^{\alpha} \quad . \tag{5.8}$$

Se $\underline{z}_0$ è un massimo per $f_r(\underline{z})$ tale che $|h(\underline{z}_0)|=1$ allora

$$\lim_{r\to+\infty} D_{n,r}=\frac{k}{|\underline{z}_0|^{\alpha}} \tag{5.9}$$

e si riduce alla M_n ponendo $k=1$, $\alpha=1$ e alla S_n ponendo

$$k=\left[\frac{m\Gamma\left(\frac{n+2}{2}\right)}{\pi^{n/2}}\right],\quad \alpha=n\,.$$

❑

6. SPAZIO H_n E GIUSTIFICAZIONI DELLE IPOTESI SU $p(\underline{z})$

Consideriamo l'insieme $H_n=\bigcup_{m=1}^{\infty} F_n(m)$

Definizione 6.1. Se $g_1\in F_n(m_1)$ e $g_2\in F_n(m_2)$ sono due elementi di H_n, con m_1-coefficienti e m_2-coefficienti di Fourier rispettivamente $h_1(\underline{z})$ e $h_2(\underline{z})$, diciamo che g_1 è equivalente a g_2 e scriviamo $g_1\sim g_2$ se, $\forall \underline{z}\in Z_n$, $h_1(\underline{z})=h_2(\underline{z})$.

La relazione $\sim$ in H_n gode evidentemente delle proprietà riflessiva, simmetrica e transitiva, per cui è una relazione d'equivalenza. Sia $Q_n=H_n/\sim$ l'insieme quoziente.

Proposizione 6.1. Se $g_1\in F_n(m_1)$ e $g_2\in F_n(m_2)$ sono densità di probabilità di

distribuzioni uniformi rispettivamente in $P_n(m_1)$ ed in $P_n(m_2)$, allora $g_1 \sim g_2$.

Dimostrazione. Immediata conseguenza delle proposizioni 3.1 e 3.2. ❑

Osservazione 6.1. Tenuto conto delle (2.2), se ampliamo l'insieme H_n con l'aggiunzione della densità di probabilità u della distribuzione uniforme continua in $[0,1)^n$ e se consideriamo la relazione $\sim$ in $H_n \cup \{u\}$, si vede immediatamente che u è equivalente alle densità di probabilità considerate nella proposizione 6.1. Si vede, inoltre, che il prolungamento canonico di una qualsiasi di tali densità di probabilità coincide con u.

Indichiamo con $\hat{g}$ la classe di equivalenza di $g \in H_n$. Siano $g_1 \in F_n(m_1)$ e $g_2 \in F_n(m_2)$ elementi di H_n e $h_1(\underline{z})$ e $h_2(\underline{z})$ i rispettivi m_1-coefficienti e m_2-coefficienti di Fourier.

Associamo alla coppia $(\hat{g}_1, \hat{g}_2)$ il numero

$$(6.1) \qquad D_{n,r}(\hat{g}_1, \hat{g}_2) = \left(\sum_{\underline{z} \in Z_n} p(\underline{z}) |h_1(\underline{z}) - h_2(\underline{z})|^r \right)^{1/r}, \qquad r \geq 1$$

L'applicazione

$$D_{n,r} : (\hat{g}_1, \hat{g}_2) \in Q_n^2 \to D_{n,r}(\hat{g}_1, \hat{g}_2)$$

è una distanza in Q_n.

Se $Q_n(m)$ è il sottoinsieme di Q_n formato dalle classi $\hat{g}_1$, con $g_1 \in F_n(m)$, si vede subito che l'applicazione

$$\varphi : g_1 \in F_n(m) \to \hat{g}_1 \in Q_n(m)$$

è un isomorfismo fra spazi metrici.

Lo spazio metrico (Q_n, D_n) si può quindi considerare un prolungamento di ognuno degli spazi metrici $(F_n(m), D_n)$.

Con abuso di linguaggio, se $g_1 \in \hat{g}_1$ e $g_2 \in \hat{g}_2$, chiameremo, *in seguito*, distanza fra g_1 e g_2 la distanza fra le classi $\hat{g}_1$ e $\hat{g}_2$.

Chiamiamo inoltre **distribuzione uniforme** la classe di equivalenza contenente la densità di probabilità della distribuzione uniforme in $F_n(m)$, per ogni m, e, con abuso di linguaggio, anche ogni elemento di tale classe.

Osservazione 6.2. Notiamo, anche se è ovvio, che l'espressione fra parentesi nella (6.1) ha sempre un numero finito di termini non nulli.

Allo scopo di chiarire aspetti significativi della formula (6.1), che giustificano, almeno da un punto di vista intuitivo, i requisiti richiesti nel paragrafo precedente alla funzione $p(\underline{z})$, presentiamo due tipi di ragionamento che conducono alle medesime conclusioni.

1° ragionamento. Sia $\underline{X}$ una variabile casuale in $P_n(m)$ e sia $\underline{Y}$ una variabile

casuale somigliante ad $\underline{X}$, ma considerata definita in $P_n(rm)$, con r intero maggiore di 1. Siano, inoltre, f_1 e f_2 le funzioni di probabilità, rispettivamente, di $\underline{X}$ e $\underline{Y}$.

Risulta

$$(6.2) \quad f_2(\underline{x}) = \begin{cases} f_1(\underline{x}) & ,\forall \underline{x} \in P_n(m) \\ 0 & ,\forall \underline{x} \in P_n(r\ m) - P_n(m) \ . \end{cases}$$

Detti $h_1(\underline{z})$ e $h_2(\underline{z})$ gli m-coefficienti e rm-coefficienti di Fourier, rispettivamente, di f_1 e f_2, risulta inoltre, per ogni $\underline{z} \in J_n(m)$,

$$(6.3) \quad h_2(\underline{z}) = \sum_{\underline{x} \in P_n(r \cdot m)} e(-\underline{z} \cdot \underline{x}) f_2(\underline{x}) = \sum_{\underline{x} \in P_n(m)} e(-\underline{z} \cdot \underline{x}) f_1(\underline{x}) = h_1(\underline{z}) \ ,$$

e per $\underline{z} \in J_n(rm) - J_n(m)$,

$$(6.4) \quad \begin{cases} h_1(\underline{z}) = 0 \\ h_2(\underline{z}) = \sum_{\underline{x} \in P_n(r \cdot m)} e(-\underline{z} \cdot \underline{x}) f_2(\underline{x}) = \sum_{\underline{x} \in P_n(m)} e(-\underline{z} \cdot \underline{x}) f_1(\underline{x}) \ . \end{cases}$$

Consideriamo per semplicità, il caso in cui $\underline{X}$ sia uniforme. Allora si ha

$$h_1(\underline{z}) = h_2(\underline{z}) = 0 \ , \ \forall \underline{z} \in J_n(m) - \{0\} \ ,$$

mentre, essendo $f_1(\underline{x}) = 1/m^n$, $\forall \underline{x} \in P_n(m)$, dalla proposizione 1.4, posto $\underline{r} = m\underline{x}$, segue che

$$h_2(\underline{z}) = \frac{1}{m^n} \sum_{\underline{r} \in I_n(m)} e(-\underline{z} \cdot \underline{r} / m) = \varepsilon(-\underline{z} / m) \ ,$$

per cui, per $\underline{z} \in J_n(rm) - J_n(m)$,

$$h_2(\underline{z}) = \begin{cases} 1 \text{ se le componenti di } \underline{z} \text{ sono tutte multiple di } m \\ 0 \text{ negli altri casi.} \end{cases}$$

Esaminando gli rm-coefficienti di Fourier della $\underline{Y}$ si vede quindi che compaiono coefficienti $h_2(\underline{z}) \neq 0$, con $\underline{z} \neq \underline{0}$, associati ad onde con numero d'onda $|\underline{z}|$ molto elevato.

Se $m = 10^h$, per un certo h, ed r=10, i valori assunti da $\underline{X}$ sono numeri con h cifre decimali e il passare della variabile casuale $\underline{X}$ alla variabile casuale $\underline{Y}$ equivale alla richiesta della cifra decimale h+1. La comparsa degli $h_2(\underline{z}) \neq 0$ con $|\underline{z}|$ elevato si può allora ritenere collegata alla maggiore richiesta di precisione. Il fatto che questi coefficienti di Fourier siano associati alla cifra decimale meno significativa fa attribuire loro, nella formula alla distanza, un peso molto inferiore a quello dei coefficienti con $|\underline{z}|$ piccolo e ciò rende ragione alle ipotesi assunte sui $p(\underline{z})$.

2° *ragionamento*. Si consideri una distribuzione mista, formata da una massa di probabilità δ situata in un punto $\underline{x}_0 \in P_n(m)$ e dalla rimanente massa $1-\delta$ distribuita uniformemente in $[0, 1)^n$. Approssimando la distribuzione con una variabile casuale $\underline{X}$ in $P_n(m)$, riunendo in $\underline{x} \in P_n(m)$ la massa di probabilità relativa all'intervallino $H(\underline{x})$ semiaperto superiormente di primo estremo $\underline{x}$ e dimensioni tutte uguali a $1/m^n$, la funzione di probabilità di $\underline{X}$ ha, per $\underline{z} \in J_n(m)-\{0\}$, come coefficienti di Fourier i numeri

$$h_2(\underline{z}) = \sum_{\underline{x} \in P_n(m)} e(-\underline{z} \cdot \underline{x})(1-\delta)/m^n + e(-\underline{z} \cdot \underline{x}_0)\delta ,$$

ossia per la (1.2)

(6.5) $\quad h_2(\underline{z}) = e(-\underline{z} \cdot \underline{x}_0)\delta .$

Se m_1 è un intero maggiore di m tale che $\underline{x}_0 \in P_n(m_1)$, approssimando la distribuzione con una variabile casuale $\underline{Y}$ in $P_n(m_1)$ con criteri di approssimazione analoghi a quelli seguiti per $\underline{X}$, la funzione di probabilità di $\underline{Y}$ ha, per $\underline{z} \in J_n(m_1)-\{\underline{0}\}$, i coefficienti di Fourier

(6.6) $\quad h_2(\underline{z}) = e(-\underline{z} \cdot \underline{x}_0)\delta .$

Nel passaggio dalla variabile casuale $\underline{X}$ alla variabile casuale $\underline{Y}$, assieme alla maggiore richiesta di precisione si è avuto, come nel primo ragionamento, la comparsa di altri coefficienti di Fourier non nulli con $|\underline{z}|$ elevato. Appare ragionevole quindi concludere, come nel ragionamento precedente, che tali coefficienti devono avere poco peso nella formula della distanza in quanto collegati alle cifre meno significative dei valori assunti dalla variabile casuale in esame.

BIBLIOGRAFIA

[1] *R.R.Coveyou, R.D.Macpherson*: Fourier Analysis of uniform random number generators. Journal of Association for Computing Machinery 14, 1967.

[2] *D.E.Knuth*: The art of computer programming, seminumerical algorithms. Addison Wesley. London, 1981.

[3] *A.N.Kolmogorov, S.V.Fomin*: Elementi della teoria delle funzioni e dell'analisi funzionale. Edizioni Mir, Mosca, 1980.

[4] *A.Maturo, N.Cera*: Confronto tra alcuni generatori di numeri pseudocasuali. Periodico di Matematiche 2, 1991, p. 38-64.

[5] *A. Maturo*: Sull'analisi di Fourier di successioni di numeri pseudocasuali, Atti SPRCI '89, P 188/198.

[6] *A.Rizzi*: Generazione di distribuzioni statistiche mediante un elaboratore elettronico. Ist. di Statistica G. Gini, Roma, 1977.

[7] *A.Rizzi*: Generazione di simboli binari pseudocasuali mediante polinomi primitivi. Statistica, 2, 1982.