RATIO MATH. 1.
(1990), 103 - 119

Numeri pseudocasuali ottenuti a partire da successioni in algebre finite su Z_m.

Antonio MATURO
Dipartimento di Scienze e Storia dell'Architettura, Viale Pindaro, 42 - Pescara

Introduzione

Lo studio comparato di vari metodi di generazione di numeri pseudocasuali mi ha spinto a prendere in considerazione alcune caratteristiche comuni ai vari generatori ed a studiare la possibilità di elaborare una teoria generale alla quale possano ricondursi gran parte dei vari metodi di generazione.

I vantaggi di una tale teoria sarebbero notevoli. Si potrebbero conoscere a priori una serie di proprietà matematiche e statistiche di una vasta classe G di generatori, individuandole per analogia e con procedimenti di generalizzazione e astrazione a partire da quelle dei generatori più noti. Questi ultimi potrebbero essere visti come elementi dell'insieme G aventi, oltre alle proprietà a priori, particolari caratteristiche.

In quest'ottica si potrebbero individuare, in G, nuovi generatori particolarmente significativi, ad esempio cercando la sottoclasse di quelli che godono di proprietà assegnate, in dipendenza di certi requisiti o vincoli che si vogliono siano rispettati nei procedimenti di simulazione.

Nel presente lavoro propongo un inquadramento della teoria generale, deducendo da essa criteri per lo studio di alcune sottoclassi di G.

2. Definizioni fondamentali e criteri per la costruzione di successioni di numeri pseudocasuali

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

Utilizziamo, in seguito, con abuso di notazione, i simboli Z_m e S per indicare non solo i sostegni dei corrispondenti anelli ma anche gli anelli stessi. Indichiamo con lettere latine gli elementi di S e con lettere greche quelli di Z_m.

Per semplicità di notazione, e quando ciò non dia luogo ad quivoci, sarà spesso utilizzata la notazione moltiplicativa usuale per le operazioni $\cdot$, $\cdot$ e $\otimes$ e quella additiva usuale per le $+$ e $\oplus$.

Allo scopo di costruire successioni di numeri pseudocasuali introduco le seguenti definizioni.

Definizione 2.1 Diciamo che S è *un'algebra di supporto di dimensione* n su Z_m, se sono soddisfatte le seguenti proprietà

(P1) S è, rispetto all'operazione esterna $\cdot$, un' algebra su Z_m;

(P2) esiste, in S, una base *B* formata da n elementi a cui appartiene l'unità u di S;

(P3) esiste, in S, un elemento x tale che gli elementi di B coincidono, tranne al più l'ordine, con le potenze $x^0 = u, x, x^2, ..., x^{n-1}$;

(P4) l'elemento x è invertibile rispetto a $\otimes$.

Dalla definizione 2.1 si deducono i seguenti

Corollario 2.1.1 Il numero di elementi di S è m^n.

Corollario 2.1.2. Gli elementi $\alpha \cdot u$, con $\alpha \in Z_m$, formano, rispetto a $\oplus$ e $\otimes$ un sottoanello di S isomorfo a Z_m.

Corollario 2.1.3. Se $n \geq 2$, allora $x \in B$ e $x \neq u$.

Definizione 2.2. Chiamiamo *funzione di supporto* una funzione $\psi : S \to Z_m$, dove S è un'algebra di supporto su Z.

In questo lavoro si assumerà l'ipotesi "lineare omogenea"

(LO) la ψ è un epimorfismo fra le strutture $(S, \oplus, *)$ e $(Z_m, +, \cdot)$, dove, al pari di $*$, anche $\cdot$ è vista come operazione esterna con dominio di operatori Z_m.

Sia $\alpha \in Z_m$. Allora α è una classe di residui modulo m e si può determinare il minimo intero non negativo $r(\alpha)$ tale che $r(\alpha) \in \alpha$:

Definizione 2.3. Chiamiamo *funzione ausiliaria di primo tipo,* la

$$\chi : \alpha \in Z_m \to r(\alpha)/m \in [0,1) \tag{2.1}$$

Sia h un intero positivo fissato. Data la h-pla $\alpha = (\alpha_1, \alpha_2, \ldots \alpha_h)$ di elementi di Z_m, indichiamo con $n(\underline{\alpha})$ il numero razionale che, nel sistema di numerazione in base m, si esprime nella forma $0 . r(\alpha_1) r(\alpha_2) \ldots r(\alpha_h)$

Definizione 2.4 Chiamiamo *funzione ausiliaria di secondo tipo* la

$$\omega : \underline{\alpha} \in (Z_m)^h \to n(\underline{\alpha}) \in [0,1) \tag{2.2}$$

La funzione $\chi o \psi$ fa corrispondere a successioni di elementi di S successioni di numeri razionali nell'intervallo [0,1). Esse, se soddisfano a opportuni tests statistici si possono ritenere pseudocasuali.

Se $\Psi = (\psi_1, \psi_2, \ldots, \psi_h)$ è una h-pla di funzioni di supporto,anche la ω o ψ fa corrispondere a successioni di elementi di S successioni di numeri razionali nell'intervallo [0,1).

Si può ritenere che l'uso della (2.1) è opportuno per m molto elevato (ad esempio dell'ordine di 10^{10}), mentre l'uso della (2.2), con h tale da rendere m^h abbastanza grande, lo è per m piccolo. Ad esempio può essere usata per $m = 2$ o per $m = 10$.

Notiamo che, per $h = 1$, la (2.2) si riduce alla (2.1).

Si potrebbero introdurre anche altri tipi di funzioni ausiliarie. In questo lavoro però ci si limiterà a considerare esclusivamente le χ e ω. Ciò non è restrittivo , in quanto i risultati ottenuti sono quasi tutti indipendenti dalla scelta della funzione ausiliaria.

3. Caratterizzazione delle algebre di supporto

Supponiamo che S sia un'algebra su Z_m soddisfacente le (P1) e (P2), con

base $B = \{x_0 = u, x_1, \ldots, x_{n-1}\}$.

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

$$x = \sum_{i=0}^{n-1} \alpha_i x_i \tag{3.1}$$

con opportuni $\alpha_i \in Z_m$.

Se x_r e x_t sono due elementi qualsiasi della base esistono, allora, in Z_m, degli elementi γ_{sti} tali che:

$$x_s \cdot x_t = \sum_{i=0}^{n-1} \gamma_{sti} x_i \tag{3.2}$$

Al variare di s,t,i si ottengono n^3 elementi γ_{sti}, detti *costanti di struttura dell'algebra,* dai quali è possibile determinare ogni prodotto $x \cdot y$ con x e y scelti arbitrariamente in S.

Infatti, se

$$x = \sum_{i=0}^{n-1} \alpha_i x_i \quad , \quad y = \sum_{i=0}^{n-1} \beta_i x_i \ , \tag{3.3}$$

risulta:

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

e, per la (3.2),

$$x \cdot y = \sum_{i=0}^{n-1} \left(\sum_{s=0}^{n-1} \sum_{t=0}^{n-1} \alpha_s \gamma_{sti} \beta_t \right) x_i \tag{3.4}$$

Le grandezze γ_{sti} non sono indipendenti.

Le relazioni di associatività $(x_r x_s)x_t = x_r(x_s x_t)$ implicano che, per ogni scelta degli indici i, r, s, t, da 0 a n-1 valgono le formule

$$\sum_{j=0}^{n-1} \gamma_{rsj} \gamma_{jti} = \sum_{j=0}^{n-1} \gamma_{rji} \gamma_{stj} \ . \tag{3.5}$$

Le relazioni di commutatività $x_r \bullet x_s = x_s \bullet x_r$ implicano che, per ogni scelta di s,t,i, risulta:

$$\gamma_{sti} = \gamma_{tsi} \tag{3.6}$$

Il fatto che $x_o = u$ implica, infine, che, per ogni scelta di s e i, si ha:

$$\gamma_{osi} = \gamma_{soi} = \begin{cases} 0 & per\ s \neq i \\ 1 & per\ s = i \end{cases} \tag{3.7}$$

Le (3.5), (3.6),(3.7) caratterizzano la struttura moltiplicativa delle algebre soddisfacenti le (P1) e (P2).

Infatti, sia S un modulo su Z_m rispetto all'addizione $\oplus$ in S e all'operazione esterna $\cdot$ e sia $B = \{x_o, x_1, ..., x_{n-1}\}$ una sua base.

Si può dimostrare il seguente

Teorema 3.1 Assegnati gli elementi γ_{sti} di Z_m, con s,t,i appartenenti a $\{0, 1, ..., n-1\}$, soddisfacenti le (3.5), la (3.4) definisce, in S, una moltiplicazione $\Diamond$ tale che $(S, +, \Diamond, \cdot)$ è un algebra su Z_m.

Tale algebra è commutativa se vale la (3.6). E' unitaria con $x_o = u$ se vale la (3.7).

Supponiamo ora che l'algebra S sia di supporto e che gli elementi di B siano ordinati in modo che $x_s = x^s$ per $s \in \{0, 1, ..., n-1\}$. Per $n \geq 2$ è $x_1 = x$ e la (P3) equivale alle relazioni $x_1 \bullet x_s = x_{s+1}$, per $0 \leq s < n-1$, ossia alle:

$$\gamma_{1si} = \gamma_{s1i} = \begin{cases} 0 & per\ i \neq s+1 \\ 1 & per\ i = s+1 \end{cases} . \tag{3.8}$$

Poichè B è una base , esistono e sono univocamente determinati, degli elementi $\beta_o, \beta_1, ..., \beta_{n-1}$ di Z_m tali che:

$$x^n = \sum_{i=0}^{n-1} \beta_i x_i = \sum_{i=0}^{n-1} \beta_i x^i \tag{3.9}$$

La (3.9) si può scrivere

$$x\,(x^{n-1} - \sum_{i=1}^{n-1} \beta_i x^{i-1}) = \beta_0 u \tag{3.10}$$

da cui segue che, se β_0 è invertibile in Z_m, risulta:

$$x \cdot (\beta_0^{-1} x^{n-1} - \beta_0^{-1} \sum_{i=1}^{n-1} \beta_i x^{i-1}) = u . \tag{3.11}$$

La (P4) è allora soddisfatta se risulta

$$\beta_0 \text{ è invertibile in } Z_m. \tag{3.12}$$

Supponiamo che sia $n \geq 2$. Poichè $x = x_1$, ponendo $y = x_{n-1}$, dalla (3.4) si deduce

$$x^n = \sum_{i=0}^{n-1} \gamma_{1n-1i} x_i \tag{3.13}$$

e, poichè B è una base, seguono le uguaglianze

$$\beta_i = \gamma_{1\,n-1\,i}, \quad \forall i \in \{0, ..., n-1\} \tag{3.14}$$

$$x^{n+k} = \sum_{i=0}^{n-1} \beta_i x^{i+k} . \tag{3.15}$$

Poichè, per ogni coppia (x_s,x_t) di elementi di B, risulta $x_s \cdot x_t = x^s \cdot x^t = x^{s+t}$, la (3.15) implica, ragionando per ricorrenza su k, che le γ_{sti} sono tutte determinate a partire dagli n valori β_i.

Chiamiamo i β_i *costanti caratteristiche* dell'algebra di supporto S.

Osserviamo che dalla (3.15) si deduce la

$$x^k = \beta_0^{-1} x^{n+k} - \sum_{i=1}^{n-1} \beta_0^{-1} \beta_i x^{i+k} \tag{3.16}$$

particolarmente utile per k negativo, in quanto ci permette di ottenere, per ricorrenza, le potenze negative di x in funzione degli elementi della base.

4. Modelli isomorfi con sostegno Z_m^n

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

$$x \oplus y = (\alpha_0+\beta_0, \alpha_1+\beta_1, ..., \alpha_{n-1}+\beta_{n-1}), \tag{4.1}$$

$$\omega \cdot x = (\omega \alpha_0, \omega \alpha_1, ..., \omega \alpha_{n-1}). \tag{4.2}$$

Rispetto alle operazioni così definite, V è un modulo su Z_m. Esso possiede basi formate da n elementi. Sia $A = \{y_0, y_1, ..., y_{n-1}\}$ una di tali basi.

Sia S una algebra su Z_m soddisfacente le (P1) e (P2) e sia $B = \{x_0, x_1, ..., x_{n-1}\}$ una sua base con $x_0 = u$.

L'applicazione

$$\varphi : \sum_{i=0}^{n-1} \alpha_i x_i \in S \rightarrow \sum_{i=0}^{n-1} \alpha_i y_i \in V \tag{4.3}$$

è un isomorfismo fra S, considerato con la sua struttura di Z_m- modulo, e V.

Si può introdurre, in V, una struttura moltiplicativa ponendo, per definizione,

$$x \cdot y = \varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y)), \quad \forall \ x, y \in V. \tag{4.4}$$

In tal modo V, rispetto alle operazioni ivi definite, soddisfa le (P1) e (P2).

Ciò può essere verificato, anche a prescindere dalle proprietà dell'isoformismo φ, dall'esame delle costanti dei struttura.

Infatti la (4.4) equivale all'affermazione che, se $x = \sum_{i=0}^{n-1} \alpha_i y_i$, $y = \sum_{i=0}^{n-1} \beta_i y_i$ e le γ_{sti} sono le costanti di struttura dell'algebra S, allora

$$x \cdot y = \sum_{i=0}^{n-1} \left(\sum_{s=0}^{n-1} \sum_{t=0}^{n-1} \alpha_s \gamma_{sti} \beta_t \right) y_i \tag{4.5}$$

Le (3.5), (3.6), (3.7), valide per le ipotesi su S, e il teorema 3.1 assicurano allora che V è un' algebra su Z_m soddisfacente le (P1) e (P2) e tale che $y_o = u$.

Vale il seguente

Teorema 4.1. Se S è un'algebra su Z_m soddisfacente le (P1) e (P2), definendo in V una moltiplicazione $\bullet$, per mezzo delle (4.3), (4.4), o in maniera equivalente della (4.5), V assume la struttura di algebra su Z_m isomorfa ad S ed avente le stesse costanti di struttura.

Supponiamo ora che S sia un'algebra di supporto.

Sia x l'elemento di S soddisfacente le (P3) e (P4) e ammettiamo che gli elementi di B siano ordinati in modo che $x_i = x$, per $i = 0, 1, ..., n-1$. Introdotto l'isomorfismo φ, sia $y = \varphi(x)$. Dalla (4.4) o dalla (3.8) si vede subito che $y_i = y$, che la (3.9) equivale alla

$$y^n = \sum_{i=0}^{n-1} \beta_i y^i \tag{4.6}$$

e che la invertibilità di x implica quella di y.

Le considerazioni svolte si possono riassumere enunciando il seguente

Teorema 4.2 Sia S un'algebra di supporto di dimensione n su Z_m, avente le costanti caratteristiche β_i e sia $y = \varphi(x)$. La (4.6) e le condizioni $y_i = y^i$ definiscono, in V, una struttura moltiplicativa rispetto alla quale V è un algebra di supporto su Z_m di dimensione n isomorfa, tramite la φ, ad S.

Come vedremo in seguito, fissati in Z_m gli elementi β_i in modo tale che β_0 sia invertibile, esiste (ed è unica a meno di isomorfismi) un'algebra di supporto S che ha le β_i come costanti caratteristiche.

Di conseguenza vale il seguente

Teorema 4.3 Fissata, nel modulo V su Z_m, la base $A = \{y_o, y_1, .., y_{n-1}\}$ e fissati, in Z_m, gli elementi $\beta_0, \beta_1, .., \beta_{n-1}$ tali che β_0 sia invertibile, esiste, ed è univocamente definita, una moltiplicazione $\bullet$ in V tale che, rispetto ad essa, V è un'algebra di supporto di dimensione n su Z_m ed inoltre

(M1) $y_0 = u$ e, per $n \geq 2$, $y_i = y_{1i}$;

(M2) vale la (4.6)

5. Esempi di costruzione di successioni di numeri pseudocasuali a partire da algebre con sostegno V

Sia $V = Z_m^n$ il modulo su Z_m definito nel paragrafo precedente e sia $B = \{x_0, x_1, .., x_{n-1}\}$ una base qualsiasi di V.

Per il teorema 4.3, fissati in Z_m degli elementi $\beta_0, \beta_1, .. \beta_{n-1}$, sono determinati degli elementi γ_{sti} soddisfacenti le (3.5), (3.6), (3.7), (3.8), (3.12) e, per $n \geq 2$, la (3.14).

La (3.4) definisce, allora, una moltiplicazione rispetto alla quale V ha la struttura di algebra di supporto.

In essa $x_0 = u$ e, per le (3.8), $x_i = (x_1)^i$. Poniamo, come al solito, $x = x_1$.

Sia ψ una funzione di supporto (LO).

Molti generatori di numeri pseudocasuali possono essere ottenuti come casi particolari del seguente procedimento

(G1) si considera, in Z_m, la asuccessione di termine generale $y_k = \psi(x^k)$, con $n \in N_0$;

(G2) si trasforma, per mezzo di una funzione ausiliaria, la successione ottenuta in una, $\{z_k\}_{k \in N0}$ di numeri razionali nell'intervallo [0,1).

Prescindiamo, per il momento, dalla funzione ausiliaria e chiamiamo, con abuso di linguaggio, non essendo ancora state verificate le proprietà statistiche e non trattandosi di elementi di [0,1), successione di numeri pseudocasuali la $\{z_k\}_{k \in N0}$

Cominciamo con l'esaminare il caso in cui B è la base usuale, ossia, per ogni i, x_{i-1} ha la componente i-sima uguale a 1 e le altre tutte nulle.

In tal caso vale il seguente

Teorema 5.1 Data la matrice, di ordine n,

$$A = \begin{bmatrix} 0 & 0 & \dots & 0 & \beta_0 \\ 1 & 0 & \dots & 0 & \beta_1 \\ . & . & \dots & . & . \\ 0 & 0 & \dots & 1 & \beta_{n-1} \end{bmatrix}, \tag{5.1}$$

le potenze di x soddisfano alla relazione ricorrente

$$x^{k+1} = A\, x^k \quad , \text{ per ogni } k \in Z. \tag{5.2}$$

Dimostrazione. E'immediato verificare che la (5.2) è valida per $0 \leq k \leq n-1$. Ammesso che essa valga per $0 \leq k \leq h$, con un fissato $h \geq n-1$, risulta, per la (3.15),

$$(5.3)\quad x^{h+2} = \sum_{i=0}^{n-1} \beta_i x^{i+h+2-n} = A \sum_{i=0}^{n-1} \beta_i x^{i+h+1-n} = A x^{h+1}$$

per cui essa vale anche per $k = h+1$. In base al principio di induzione matematica la (5.3) è allora valida per ogni $k \in N_0$.

La relazione (5.3) si può anche scrivere, dato che A è invertibile, poichè tale è β_0,

$$(5.4)\qquad x^k = A^{-1} x^{k+1} \quad , \text{ per ogni } k \in Z.$$

Essa è valida per ogni $k \in N_0$.

Ammesso che valga per $0 \geq k \geq h$, con un fissato $h \leq 0$, risulta, per la (3.16),

$$(5.5)\qquad x^{h-1} = \beta_0^{-1} x^{n+h-1} - \sum_{i=1}^{n-1} \beta_0^{-1} \beta_i x^{i+h-1} =$$

$$= A^{-1}(\beta_0^{-1} x^{n+h} - \sum_{i=1}^{n-1} \beta_0^{-1} \beta_i x^{i+h}) = A^{-1} x^h \ ,$$

per cui essa è valida anche per $k = h-1$. In base al principio di induzione matematica la (5.2) è allora valida anche per valori negativi di k.

Dal teorema 5.2 si ottengono i seguenti

Corollario 5.1.1 Le potenze di x soddisfano alla relazione

$$(5.6)\qquad x^k = A^k x_0$$

ossia, detto a_{ij}^k l'elemento generico della matrice A^k,

$$(5.7) \qquad x^k = \begin{bmatrix} a_{11}^k \\ a_{21}^k \\ \cdots \\ \cdots \\ \cdots \\ a_{n-1}^k \end{bmatrix}$$

Dimostrazione. La (5.6) è vera per $k=0$. Se essa è vera per $k=h>0$ risulta $x^{h+1}=Ax^h=A(A^hx_0)=A^{h+1}x_0$ e quindi è vera anche per $k=h+1$. Se essa è vera per $k=-h<0$ risulta $x^{-h-1}=A^{-1}(x^{-h})=A^{-1}(A^{-h}x_0)=A^{-h-1}x_0$ e quindi è vera anche per $k=-h-1$.

Corollario 5.1.2 La successione di termine generale y_k soddisfa alla relazione

$$(5.8) \qquad y_k = \psi_0 A^k x_0 ,$$

dove y_0 è il vettore riga $[\psi(x_0), \psi(x_1), ..., \psi(x_{n-1})]$, ossia alla:

$$(5.9) \qquad y_\kappa = \psi(x_0)a_{11}^k + \psi(x_1)a_{21}^k + ... + \psi(x_{n-1})a_{n1}^k .$$

Dimostrazione. Se B è una qualsiasi matrice di ordine n e $v=[v_0, v_1, ..., v_{n-1}]'$ è un qualsiasi elemento di V, risulta, per le proprietà di linearità di ψ,

$$(5.10) \qquad \psi(Bv) = \psi_0 Bv$$

La (5.6) implica allora la (5.8) e la (5.7) implica la (5.9).

Esempi notevoli di funzioni di supporto (LO) sono:

(S1) $\forall z \in V$, $\psi(z) = z_i$ (i-sima componente di z) ;

(S2) $\forall z \in V$, $\psi(z) = \sum_{i=1}^{n} z_i$;

(S3) $\forall z \in V$, $\psi(z) = \sum_{i=1}^{n} \alpha_i z_i$, con $\alpha_i \in Z_m$ e tali che almeno uno di essi sia invertibile.

La (S3) include, come casi particolari, i primi due.

La espressione di y_k si riduce, nei tre casi considerati, rispettivamente alle

(5.11.1) $$y_k = a_{i1}^k ,$$

(5.11.2) $$y_k = \sum_{i=1}^{n} a_{i1}^k ,$$

(5.11.3) $$y_k = \sum_{i=1}^{n} \alpha_i \, a_{i1}^k \ .$$

Consideriamo ora il caso in cui la base $B = \{x_0, x_1, ..., x_{n-1}\}$ non sia quella usuale. Sia $F = \{z_0, z_1, ..., z_{n-1}\}$ e sia B la matrice avente come colonne i vettori $x_0, x_1, ..., x_{n-1}$.

Se v è un qualsiasi elemento di V e v^* è il vettore delle sue coordinate rispetto alla base B risulta

(5.12) $$v = B v^*, \quad v^* = B^{-1} v$$

Sia le potenze di $v \in V$ che le relazioni fra esse come la (4.6) non dipendono dal sistema di riferimento scelto.

Usando come sistema di riferimento la base B i vettori $x_0, x_1, ..., x_{n-1}$ hanno come vettori delle coordinate quelli della base usuale per cui dalla (5.2) segue

(5.13) $$x^{k+1\,*} = A \, x^{k\,*}$$

Allora, per la (5.12), risulta

(5.14) $$x^{k+1} = B A B^{-1} x^k \ .$$

Posto $A^* = B A B^{-1}$, le (5.6) e (5.8) sono, in tal caso, sostituite rispettivamente dalle

(5.15) $$x^k = A^{*k} x_0 ,$$

(5.16) $$y_k = \psi_0 A^{*k} x_0 \ .$$

Presentiamo un esempio di algebra su V che, pur soddisfacendo le (P1) e (P2), non è di supporto .

Si assuma, in V, la base B in modo che sia $x_0 = (1, 1, ..., 1)$ e, per $i \neq 0$, x_i uguale al vettore $(i+1)$-simo della base usuale.

Definiamo, in V, una moltiplicazione ponendo, per $x = (\alpha_0, \alpha_1, ..., \alpha_{n-1})$ e $y = (\beta_0, \beta_1, ..., \beta_{n-1})$,

$$x\,y = (\alpha_0\beta_0,\ \alpha_1\beta_1,\ \ldots,\ \alpha_{n-1}\ \beta_{n-1}) \tag{5.17}$$

Si può facilmente dimostrare che la moltiplicazione (5.17) gode della *proprietà associativa e di quella distributiva rispetto all'addizione in V ed* inoltre che valgono, rispetto al complesso delle operazioni, i vari assiomi di un'algebra. Il fatto che, rispetto alla (5.17), V è un'algebra si può anche vedere mostrando che le costanti di struttura verificano le (3.5).

Infatti la (5.17) implica le

$$x_s\,x_t = \begin{cases} x_t \ \textit{per}\ \ s = 0\ \textit{oppure}\ s = t \\ x_s \ \textit{per}\ \ t = 0 \\ 0 \ \textit{negli altri casi} \end{cases} \tag{5.18}$$

per cui

$$\gamma_{sti} = \begin{cases} 1 \ \textit{per}\ \ s = 0\ e\ i = t\ . \\ \quad \textit{oppure per}\ t = 0\ e\ \ i = s\ \ \textit{oppure per}\ \ s = t = i\ . \\ 0 \ \textit{negli altri casi} \end{cases} \tag{5.19}$$

Le formule (3.5) si riducono a

$$\gamma_{rsr}\ \gamma_{rti}\ + \gamma_{rss}\ \gamma_{sti}\ = \gamma_{rsi}\ \gamma_{sts}\ + \gamma_{rti}\ \gamma_{stt}\ .$$

Considerando tutti i possibili valori di r,s,t,i, tenendo conto della (5.19) si vede che le (3.5) sono soddisfatte. Allora, in base al teorema 3.1, V e un'algebra.

Se $x = (\beta_o, \beta_1, \ldots, \beta_{n-1})$, la (3.1) si riduce a

$$x = \beta_0\ x_0\ +\ \sum_{i=1}^{n-1}\ (\beta_i\ -\ \beta_o)\,x_i$$

e viceversa, se $x = \sum_{i=0}^{n-1}\ \alpha_i\ x_i$, risulta

$$x\ = (\alpha_0\,,\ \alpha_1\ +\ \alpha_0,\ \ldots,\ \alpha_{n-1}\ +\ \alpha_0).$$

Si puo osservare che, per $n > 1$, la (5.17) implica che $x_1 y = \beta_1\, x_1$ e, in particolare, $x_{12} = x_1$. Segue che x_1, essendo diverso dall'unità, non è invertibile e, per $n > 2$, nessun x può soddisfare alla(P3).

L'algebra costruita non è di supporto per nessun $n > 1$.

6. Algebre di supporto di dimensione 1 o 2 e successioni di numeri pseudocasuali ottenute da esse

Consideriamo le algebre di supporto di dimensione 1. Per il teorema 4.2 non si viene meno alla generalità ponendo $S = V = Z_m$.

Un'algebra di supporto di dimensione 1 viene allora costruita introducendo una opportuna moltiplicazione in Z_m considerato come modulo su Z_m.

In base al corollario 2.1.2, tale moltiplicazione non può che identificarsi con quella ordinaria in Z_m.

Poichè,in tal modo, sono soddisfatti gli assiomi (P1), (P2), (P3), (P4), segue che esiste un'unica algebra di supporto di dimensione 1 su Z_m, avente la base $B = \{x_0 = 1\}$ e l'unica costante di struttura $\gamma_{000} = 1$.

Se x è un elemento invertibile di Z_m e $\beta_0 = x$, la (3.9) si riduce alla

$$x = \beta_0 x_0 = \beta_0 x^0 \tag{6.1}$$

e le (3.15) e (3.16) si riducono, rispettivamente, alle

$$x^{k+1} = \beta_0 x^k \; ; \quad x^k = \beta_0^{-1} x^{k+1} \; . \tag{6.2}$$

Se ψ è una funzione di supporto (LO) risulta, allora

$$\psi(x) = \beta_0 \psi(1) \quad , \quad \psi(x^{k+1}) = \beta_0 \psi(x^k) \; . \tag{6.3}$$

Poniamo $\psi(x^k) = y_k \quad , \quad \beta_0 = a \quad , \quad \psi(1) = y_0$.

Le (6.3) si riducono alla relazione ricorrente, in Z_m,

$$y_{k+1} = a y_k \; , \; \textit{con} \; y_0 \; \textit{assegnato.} \tag{6.4}$$

Alla successione $\{x^k\}_{k \in N0}$ delle potenze di x corrisponde tramite la ψ, la successione (6.4) ossia il generatore moltiplicativo con moltiplicatore $r(a)$ e seme $r(y_0)$.

Si noti come il fatto che β_0 sia invertibile si traduce nella classica condizione $(r(a), m) = 1$.

Poichè ψ è un epimorfismo fra gruppi additivi aventi una moltiplicazione esterna con dominio di operatori Z_m, per ogni $y \in Z_m$ deve esistere un $z \in Z_m$ tale che $\psi(z) = z\,\psi(1) = y$. Ciò avviene se e solo se $\psi(1)$ è invertibile. Questo fatto, in riferimento al generatore moltiplicativo, si traduce nell'altra classica condizione $(r(y_0),m) = 1$.

Consideriamo ora le algebre di supporto di dimensione 2.

Sempre per il teorema 4.2, si può prendere $S = V = Z_{m2}$ e costruire un'algebra introducendo una opportuna moltiplicazione in V considerato come modulo su Z_m.

Sia $A = \{x_0, x_1\}$ una base di V e imponiamo le condizioni

$$(6.5) \qquad \begin{cases} x_0 x_0 = x_0 \\ x_0 x_1 = x_1 x_0 = x_1 \\ x_1 x_1 = \beta_0 x_0 + \beta_1 x_1 \end{cases}$$

con β_0 invertibile in Z_m.

Esse si traducono nel fatto che le matrici γ_{sti}, con i fissato, delle costanti di struttura sono

$$[\gamma_{st0}] = \begin{bmatrix} 1 & 0 \\ 0 & \beta_0 \end{bmatrix}, \qquad [\gamma_{st1}] = \begin{bmatrix} 0 & 1 \\ 1 & \beta_1 \end{bmatrix}.$$

Si può facilmente dimostrare che tali costanti soddisfano le (3.5),(3.6), (3.7), (3.8), (3.12), per cui definiscono un'algebra di supporto, in cui $x_0 = u$.

Se $y = \delta_0 x_0 + \delta_1 x_1$ e $z = \gamma_0 x_0 + \gamma_1 x_2$, in base alla (3.4) risulta

$$(6.6) \qquad y \cdot z = \sum_{i=0}^{1} \Big(\sum_{s=0}^{1} \sum_{t=0}^{1} \delta_s \gamma_t \gamma_{sti} \Big) x_i ,$$

ossia, per le (6.5),

$$(6.7) \quad y \cdot z = (\delta_0 \gamma_0 + \delta_1 \gamma_1 \beta_1) x_0 + (\delta_1 \gamma_0 + \delta_0 \gamma_1 + \delta_1 \gamma_1 \beta_1) x_1$$

Poniamo $x_1 = x$. L'ultima delle (6.5) si può scrivere

$$(6.8) \qquad x^2 = \beta_0 x^0 + \beta_1 x$$

ed è un caso particolare della (3.9).

Le (3.15) e (3.16) si scrivono, rispettivamente

$$x^{k+2} = \beta_0 x^k + \beta_1 x^{k+1} , \tag{6.9}$$

$$x^k = \beta_0^{-1} x^{k+1} - \beta_0^{-1} \beta_1 x^{k+1} . \tag{6.10}$$

Sia ψ una funzione di supporto (LO). Risulta, per le (6.8) e (6.9),

$$\psi(x^{k+2}) = \beta_0 \psi(x^k) + \beta_1 \psi(x^{k+1}) . \tag{6.11}$$

Poniamo

$$\psi(x^k) = y^k , \quad \beta_0 = a_0 , \quad \beta_1 = a_1 . \tag{6.12}$$

Le (6.11) si riducono alla relazione ricorrente, in Z_m,

$$y_{k+2} = a_0 y_0 + a_1 y_{k+1} , \quad \textit{con } y_0 \textit{ e } y_1 \textit{ assegnati} . \tag{6.13}$$

Alla successione $\{x^k\}_{k \in No}$ delle potenze di x corrsponde la successione ottenuta dalla (6.13), ossia dal generatore lineare omogeneo del 2º ordine.

Per $r(a_0) = r(a_1)$, $r(y_0) = 0$, $r(y_1) = 1$ esso fornisce la classica successione di Fibonacci modulo m.

Il fatto che ψ sia un epimorfismo implica che, per ogni $y \in Z_m$, esistono α_0 e α_1 tali che

$$\alpha_0 y_0 + \alpha_1 y_1 = y , \tag{6.14}$$

ossia che l'ideale in Z_m generato da y_0 e y_1 coincide con Z_m. Ciò avviene o se almeno uno fra y_0 e y_1 è invertibile, oppure se non esistono divisori dello zero che dividano sia y_0 che y_1.

Infatti la (6.14) ammette soluzioni se e solo se ammette soluzioni intere $r(\alpha_0)$, $r(\alpha_1)$, k l'equazione

$$r(\alpha_0) r(y_0) + r(\alpha_1) r(y_1) + km = r(y) , \tag{6.15}$$

ossia se e solo se

(6.16) $D(r(y_0), r(y_1), m) = D(r(y_0), r(y_2), m, r(y))$.

Se uno fra y_0 e y_1 è invertibile oppure non esistono divisori dello zero che dividano sia y_0 che y_1 risulta $D(r(y_0), r(y_1), m) = 1$ e quindi la (6.16) è soddisfatta. Se, invece, esiste un divisore dello zero δ che divide sia y_0 che y_1 allora la (6.16) ammette soluzioni solo se δ divide anche y. Non ammette soluzioni se, ad esempio, y è invertibile, dato che, in tal caso, $D(r(y), m) = 1$.

BIBLIOGRAFIA

(1) G.Ascoli **Lezioni di Algebra**. Editrice Tirrenia. Torino. 1965

(2) A.C. Arvillas and D.G. Matitsas **Partitioning the period of a class of m-sequences and application to pseudorandom number generation**. Journal of the Association for Computing Machinery. Vol 25. 1978

(3) M. Curzio **Lezioni di Algebra**. Liguori Editore Napoli. 1967

(4) I: Glazman-Y. Liubitch **Analyse linèare dans le espaces de dimensions finies**. Editions Mir Moscou. 1974

(5) S.W. Golomb **Shift register sequences**. Holden-Dsy, Inc. London. 1965

(6) D.E. Knuth **The art of computer programming**. Vol 2. Seminumerical Algorithms. Addison-Wesley. London. 1969

(7) T.G: Lewis and W.H. Payne **Generalized feedback shift register pseudorandom number algorithm**. Journal of the Association for Computing Machinery. Vol 20. 1973

(8) A. Maturo **Numeri pseudocasuali**. Montefeltro Edizioni Urbino. 1982

(9) A. Maturo N.Cera ***Confronto fra alcuni generatori di numeri pseudocasuali***. Ratio Math. 2, in corso di stampa.

(10) A. Maturo N. Cera **Generazione di numeri pseudocasuali per mezzo di relazioni di ricorrenze su campi di Galois**. Periodico di Matematiche, in corso di stampa.

(11) W.W. Peterson-E.J. Weldon **Error-correcting codes**. Massachusetts Institute of Technology Press. Cambridge. 1972

(12) I.S. Reed and R. Turn **A generalization of shift register sequences generators**. Journal of the Association for Computing machinery. Vol 16. 1969

(13) A. Rizzi **Su un metodo per la generazione di sequenze di simboli binari pseudo-casuali**. Metron. Vol XXIX. 1971

(14) A. Rizzi **Generazione di simboli binari pseudocasuali mediante polinomi primitivi**. Statistica. 1982

(15) C.S. Smith **Multiplicative pseudo-random number generators with prime modulus**. Journal of the Association for Computing Machinery. Vol 18. 1971

(16) R.C. Tausworthe. **Random numbers generated by linear recurrence modulo two**. Mathematics of Computation 19. 1965

(17) J.P.R. Tootil-W.D. Robinson and A.G. Adams **The runs up and down performance of Tausworthe pseudorandom number generators**. Journal of Association for Computing Machinery. Vol 18. 1971

(18) G. Zappa-R. Permutti **Gruppi, corpi, equazioni**. Feltrinelli. 1972

(19) N. Zierlir **Linear recurring sequences**. J Soc. Industr. Appl. Math. Vol 7. 1959