Sistemi dinamici instabili e generazione di successioni pseudo–casuali

Luigi Accardi, F. De Tisi, A. Di Libero

Sommario. Si suggerisce una nuova tecnica per la generazione di sequenze casuali. Questa tecnica è fondata sulla teoria dei sistemi dinamici instabili con proprietà ergodiche particolarmente forti (K–sistemi). Vengono discussi alcuni esperimenti i cui risultati sono poi paragonati ai risultati ottenuti con i metodi congruenziali.

Ringraziamenti. Gli autori esprimono la loro gratitudine ai proff. M. Cugiani, A. Giorgilli, I. Bozzini per molte stimolanti e proficue discussioni sull'argomento trattato.

1 Successioni pseudo–casuali e sistemi dinamici

Per le applicazioni dei metodi numerico–statistici, tipo Monte–Carlo, è necessario disporre di algoritmi per la generazione di "successioni casuali": successioni di numeri per i problemi a una dimensione, successioni di vettori per i problemi a più dimensioni. In particolare, poiché è proprio nei problemi a un numero elevato di dimensioni che i metodi numerico–statistici si rivelano vantaggiosi rispetto ai tradizionali metodi di calcolo numerico, il problema di costruire algoritmi per la generazione di successioni di vettori casuali in uno spazio vettoriale n–dimensionale ($n \geq 2$) ha un notevole interesse applicativo.

Come è noto il problema di definire in modo generale che cosa è una "successione casuale" è stato affrontato da diversi punti di vista e solo in tempi relativamente recenti si è arrivati a dimostrare la sostanziale equivalenza delle varie proposte. I risultati di queste ricerche, che non saranno discussi nel presente lavoro e per i quali rimandiamo alla monografia di C.P. Schnorr [1], confermano essenzialmente l'intuizione che una "successione casuale" è una successione che non può essere generata da nessun algoritmo finito, ovvero una successione la cui "legge di generazione" è "infinitamente complicata".

In particolare una tale successione non potrà essere generata dal calcolatore, e perciò il meglio che si può sperare è di riuscire a costruire algoritmi per la produzione di successioni che in qualche modo "simulano" il comportamento di una vera successione casuale; in questo senso si parla di "successioni pseudo–casuali". Quando si dice che una successione non casuale simula il comportamento di una successione casuale, si intende dire che una tale successione gode (almeno in senso approssimato) di alcune delle proprietà che caratterizzano il comportamento delle successioni casuali. Ma poiché queste proprietà sono infinite, ogni criterio effettivo di pseudo–casualità richiederà che tra queste proprietà se ne scelgano un numero finito e, in questo modo, si introdurranno fattori di arbitrarietà nella definizione. Poiché la verifica della presenza o assenza di determinate proprietà di "caoticità" in una successione, si effettua sottoponendo tale successione a dei test statistici, si può dire che ogni gruppo di test statistici definisce una clase di successioni pseudo–casuali (cioè la calsse delle successioni che superano tutti i test del gruppo) e che è impossibile dare una definizione "universale" — cioè non vincolata alla scelta di un numero finito di test statistici – del concetto di successione pseudo–casuale.

La totalità dei metodi usati pe la generazione di successioni pseudo–casuali può essere inquadrata nel seguente schema: una successione pseudo–casuale di punti di un insieme è definita dalla assegnazione di:

i) una funzione $\phi : \Omega \to \Omega$

ii) un sottoinsieme $\Omega_0 \subseteq \Omega$ (i cui punti sono detti "punti iniziali") con la seguente proprietà

– Per ogni $x_0 \in \Omega_0$, l'orbita di x_0 rispetto a ϕ, cioè

$$\Omega(x_0) = \{\phi^n x_0 : n \in \mathbb{N}\}$$

è una successione di punti di Ω che supera alcuni test statistici standard.

Una descrizione dei più comuni test statistici, usati per verificare la caoticità di una successione, si può trovare per esempio nella monografia di M. Cugiani [9].

Poiché alla scelta di un insieme (finito) di test statistici corrisponde la scelta di una definizione di successione pseudo–casuale, uno dei problemi principali della teoria è quello di escogitare dei test statistici che siano nello stesso tempo praticamente attuabili e "significativi". La difficoltà del problema, che peraltro non sarà discusso nel presente lavoro, sta nel fatto che la "significatività" o meno di un test può dipendere dall'uso che si vuol fare

della successione pseudo–casuale: per alcuni problemi, il superamento dei più grossolani test statistici — come l'equidsitribuzione — è tutto ciò che serve; per altri è necessario poter garantire proprietà statistiche più forti.

Da quanto detto finora segue che la teoria della generazione di successioni pseudo–casuali conduce naturalmente allo studio delle proprietà statistiche delle trasformazioni $\phi : \Omega \to \Omega$, dove Ω è un insieme e ϕ — una trasformazione di Ω in sé. Una tale coppia $\{\Omega, \phi\}$ è detta **sistema dinamico** (discreto deterministico) e quella parte della matematica che studia le proprietà statistiche dei sistemi deterministici è la **teoria ergodica**. Nella pratica l'insieme Ω è quasi il cubo unitario nello spazio euclideo reale n–dimensionale R^n, e perciò — identificando le facce opposte del cubo — si è condotti all'analisi delle proprietà statistiche dei **sistemi dinamici descreti sul toro n–dimensionale (reale)**.

La teoria ergodica classica studia quei sistemi dinamici $\{\Omega, \phi\}$ tali che su Ω è definita una misura μ invariante rispetto a ϕ, cioè:

$$\mu(A) = \mu(\phi^{-1}(A)) \; ; \qquad A \subseteq \Omega \tag{1}$$

Mediante la teoria ergodica è possibile dare un significato preciso all'affermazione: "la trasformazione $\phi : \Omega \to \Omega$ ha forti proprietà statistiche rispetto a μ" (anche in questo caso il termine "caoticità" non si traduce univocamente in una proprietà matematica, ma dà luogo a una gerarchia continua di condizioni — la gerarchia ergodica — alcune delle quali sono state ampiamente studiate nella letteratura matematica: ergodica, mixing, K–sistema, sistema di Bernoulli, etc.).

Nel tentativo di applicare i risultati della teoria ergodica allos tudio della generazione di successioni pseudo–casuali, si incontrano però due tipi di problemi:

a) Se Ω è un insieme finito, la teoria ergodica su Ω è banale.

b) Tutte le informazioni, fornite dalla teoria ergodica, sul comportamento delle orbite di un sistema dinamico $\{\Omega, \phi, \mu\}$ valgono a meno di insiemi di μ–misura nulla.

Entrambi i problemi hanno la loro origine nel fatto che ogni calcolatore, in questo macchina finita, può descrivere solo insiemi finiti di punti e di conseguenza i fondamenti teorici del problema della generazione di successioni pseudo–casuali vanno ricercati non tanto nella teoria ergodica delle orbite periodiche. Mentre la teoria classica considera in genere misure non atomiche e distingue tra orbite "caotiche" e orbite "regolari" (includendo tra queste

ultime le orbite periodiche), per gli scopi del calcolo numerico è necessario distinguree, tra le stesse orbite periodiche di un sistema dinamico, quelle con un comportamento "regolare" e quelle con un comportamento "caotico".

Occorrerà inoltre trovare dei criteri effettivamente applicabili che garantiscano che, a una certa classe di dati iniziali, corrispondano orbite periodiche con caratteristiche "caotiche". Il problema della generazione, mediante calcolatori, di successioni pseudo–casuali, si può quindi articolare nei seguenti problemi:

I) Quand'è che il comportamento di un'orbita periodica di un sistema dinamico può definirsi "caotico"?

II) Come costruire effettivamente orbite periodiche caotiche?

La letteratura attuale fornisce a queste domande delle risposte di carattere essenzialmente empirico: una successione periodica di punti, viene detta pseudo–casuale se supera certi test statistici a posteriori. I criteri costruttivi assegnati permettono di garantire a priori la lunghezza del periodo, mentre il superamento dei tet statistici si può solo verificare a posteriori.

I metodi di generazione di successioni casuali più diffusi, quelli basati sulla teoria dei campi di Galois e loro varianti (cf. [9]), garantiscono la lunghezza del periodo dell'orbita (almeno in corrispondenza a una certa classe di dati iniziali) con ragionamenti basati sulla teoria dei numeri, ma non riescono a chiarire il legame tra lunghezza del periodo e caoticità dell'orbita.

Questo legame rappresenta l'aspetto teorico più interessante del problema della generazione di successioni pseudo–casuali. Infatti, se da una parte è banale che si possano avere orbite con periodi molto lunghi ma "regolari" (cioè che non presentano un comportamento caotico) dall'altra è un fatto sperimentale che le orbite ottenuti con generatori del tipo "campi di Galois" superano abbastanza bene i test statistici consueti e in questo senso si può dire che esse hanno un comportamento "caotico".

Perciò è naturale chiedersi:

– Quali sono le radici teoriche delle buone proprietà statistiche dei generatori di successioni pseudo–casuali di tipo "campi di Galois"?

Un problema analogo si pone per un altro metodo di generazione di punti casuali, proposto qualche anno fa da uno degli autori del presente lavoro, e che sembra superare i principali test statistici (cf. [9] e le tabelle allegate al paragrafo successivo).

L'idea centrale, su cui si fonda questo metodo, è l'osservazione che i più famosi esempi "fisici" di successioni "casuali" — per es. i lanci di monete o di dadi, la roulette, ecc. – sono ottenuti a partire da sistemi dinamici instabili.

Questa osservazione suggerisce che la teoria generale dei sistemi dinamici instabili possa essere utilmente impiegata nel problema della generazione di successioni pseudo–casuali. In particolare, nel caso del toro, c'è una classe di sistemi dinamici instabili (i cosiddetti automorfismi iperbolici del toro) che è stata ampiamente studiata nella letteratura e che si è dimostrato possedere forti proprietà ergodiche rispetto alla misura di Lebesgue (cf. [2]). Fissando un sistema di coordinate R^n, i punti del toro n–dimensionale possono essere identificati ai vettori $x = (x_1, \ldots, x_n)$, le cui componenti sono definite (mod 1) e gli automorfismi del toro sono le trasformazioni del tipo:

$$x \to Ax(\text{mod } 1) = \phi(x) \tag{2}$$

dove A è una matrice a coefficienti interi con $\det A = \pm 1$ e priva di autovalori sulla circonferenza unitaria.

La congettura che i sistemi del tipo (2) generino, per "quasi tutti" i dati iniziali, delle orbite con buone caratteristiche di "caoticità", risulta — come si è già detto – ben confermata dai dati sperimentali ottenuti al calcolatore.

In questo caso, a differenza di quanto accade con i generaotri di tipo "campi di Golois", è lo stesso metodo costruttivo a fornire una giustificazione intuitiva del comportamento "caotico" delle orbite ottenute: infatti si è usata una funzione ϕ che la teoria garantisce a priori possedere forti proprietà statistiche.

Tuttavia un esame più approfondito della situazione mostra che per trasformare questa "giustificazione intuitiva" in argomento matematico occorre arrivare a livelli molto fini della teoria ergodica e della teoria dei sistemi dinamici.

In effetti, le proprietà statistiche della funzione ϕ (automorfismo iperbolico del toro) sono garantite soltanto per le orbite con punto iniziale a coordinate irrazionali, mentre si può dimostrare che tutte (e sole) le orbite con punto iniziale razionale sono periodiche. Poiché ovviamente è solo su quest'ultimo tipo di orbite che un calcolatore può operare, anche in questo caso si pone la domanda:

– Quali sono le radici teoriche del comportamento caotico della maggior parte" delle orbite periodiche degli automorfismi iperbolici del toro n–dimensionale?

Queta formulazione del problema, oltre a essere più specifica di quella relativa ai campi di Galois, ci fornisce anche la chiave interpretativa per connettere il metodo di generazione di successioni pseudo–casuali, basato

sulla teoria dei sistemi dinamici instabili, con quello basato sui campi di Galois. Infatti quest'ultimo metodo conduce alla iterazione di trasformazioni del tipo:

$$x \to Ax(\text{mod } 1) \tag{3}$$

dove x è ancora un vettore a n–componenti (definite (mod 1)), A ancora una matrice a coefficienti interi, ma questa volta non necessariamente $\det A = \pm 1$. Quest'ultima circostanza implica che questa volta ci troviamo di fronte a un endomorfismo invece che un automorfismo del toro n–dimensionale. Una tale trasformazione non conserva la misura di Lebesgue ma, se $|\det A| = N$, il toro viene "ricoperto N volte" dalla trasformazione. Riassumendo:

– La teoria degli endomorfismi (iperbolici) del toro n–dimensionale fornisce un contesto matematico che unifica i metodi di generazione di successioni casuali di tipo campi di Galois con quelli basati sulla teoria dei sistemi dinamici.

Nella teoria ergodica degli endomorfismi del toro occorrerà tener conto del fatto che la misura di Lebesgue non è conservata (ma moltiplicata per un intero). È ragionevole tuttavia attendersi che il carattere caotico di quasi tutte le orbite permanga (anzi peggiori) nel passagtgio da automorfismo a endomorfismi. Se diamo per scontanto quest'ultimo fatto, possiamo spiegare le buone proprietà statistiche, empiricamente verificate dagli esperimenti al calcolatore, di tutti e due i metodi di generazione menzionati sopra, mediante il seguente:

Principio Euristico. Le orbite periodiche, con periodo lungo di un sistema dinamico con forti proprietà di stocasticità su una varietà differenziabile compatta (o almeno di misura finita, nel caso di varietà riemanniane) hanno un comportamento caotica che "simula" quello delle orbite aperiodiche.

I dati, finora raccolti con esperimenti fatti al calcolatore sembrano confermare la validità del principio euristico enunciato sopra. Nelle tabelle, allegate al § (2) sono riportati alcuni di questi dati. Naturalmente restano aperti i problemi di trovare una formulazione matematicamente soddisfacente del principio euristico enunciato sopra e di stabilirne la validità.

A questo proposito osserviamo che una prima proprietà che è ragionevole attendersi è che le orbite periodiche con periodo lungo di un sistema dinamico con forti proprietà stocastiche si distribuiscono tanto più uniformemente quando più lungo è il periodo.

Per trasformazioni, che conservano la misura μ – indotta dalla misura di Lebesuge – sulla varietà Ω un modo di esprimere quantitativamente questa

proprietà è che la trasformazione $\phi : \Omega \to \Omega$ soddisfi, per ogni funzione $f : \Omega \to \mathbb{R}$ abbastanza regolare, una relazione del tipo:

$$1/N \sum_{n=1}^{N} f(\phi^n x_0) - \int_\Omega f d\mu = 0(1/N^\alpha) \tag{4}$$

per ogni x_0 appartenente a un'orbita periodica di periodo N e per qualche $\alpha > 0$.

Recentemente alcuni risultati del tipo (4) sono stati stabiliti per particolari sistemi dinamici $\{\Omega, \phi, \mu\}$. Per esmpio da R. Bowen nel caso del flusso geodesico su una varietà riemanniana [3] e da P. Sarnak nel caso del flusso orociclo sugli elementi di una superficie di Riemann con la metrica di Poincaré [21].

Un altro risultato, a sostegno del principio euristico enunciato sopra, è una conseguenza del "teorema delle pseudo–orbite", valido per i C–sistemi (e perciò in particolare per gli automorfismi iperbolici del toro), secondo cui un segmento arbitrariamente lungo di un'orbita aperiodica può essere approssimato con precisione arbitraria da un'orbita periodica (cf. [4], [10]). Per alcuni sistemi dinamici vale un risultato ancora più forte, cioè la cosiddetta "proprietà di specificazione" il cui contenuto intuitivo è che con una singola orbita periodica è possibile approssimare con precisione arbitraria due segmenti arbitrariamente lunghi di due diverse orbite aperiodiche.

Tutte queste proprietà possono essere considerate come primi esempio di risultati riguardanti quella "teoria ergodica delle orbite periodiche" cui abbiamo accennato sopra. Essi non sono ancora sufficienti per rispondere in modo soddisfacente ai vari problemi da noi incontrati nel tentativo di spiegare il motivo teorico del successo sperimentale dei metodi di generazione di successioni pseudo–casuali. Ciò prova che, nonostante il florido sviluppo avuto in questi ultimi anni dalla teoria ergodica, in questo campo c'è ancora moltissimo da fare. Tuttavia, nonostante i numerosi problemi che restano aperti è indubbio che la teoria ergodica in senso lato (includente cioè la teoria ergodica delle orbite periodiche) costituisce un prezioso strumento sia per la comprensione teorica della teoria delle successioni pseudo–casuali, sia per indirizzare la ricerca di algoritmi espliciti per la costruzione di tali successioni.

2 Descrizione dei test statistici

2.1 χ^2 test per l'uniforme distribuzione (UD)

Questo è certamente il test più largamente citato [9].

Si suddivide T_n in un certo numero r di cellette; si calcola poi l'ipervolume di tali cellette; si supponga che ogni celletta abbia volume v_i. Se T_n è il toro unitario di volume 1 si avrà: $\sum v_i = 1$. Cosı v_i è la probabilità di individuare un punto T_n all'interno della celletta i.

Se una sequenza lunga N è uniformemente distribuita in T_n il numero dei punti interni alla celletta i, N_i, dovrà essere $v_i N$, o almeno approssimarsi a tale valore.

I tests χ^2 danno una valutazione di questa approssimazione. Si pone:

$$V = \sum_{i=1}^{r} \frac{(N_i - v_i N)^2}{v_i N}$$

e si confronta questa statistica coi valori della distribuzione χ^2 con $r-i$ gradi di libertà.

Questo metodo ha tuttavia un grave limite; il numero di cellette cresce sequenzialmente con la dimensione dello spazio; cosı una partizione in 100 intervallini sulla circonferenza unitaria può dare un'informazione significativa, per T_2 diventa insufficiente, e per $T_2(n \geq 3)$ comincia ad essere insignificante. Una soluzione potrebbe essere quella di effettuare un campinamento. Limitandosi a T_2, tuttavia, e incrociando questo test con altri i valori ottenuti possono essere di una certa affidabilità. Poiché si è suddiviso T_2 in 100 quadratini di $\frac{1}{10}$ di lato si avrà:

$$V = \sum_{i=1}^{100} \frac{(N_i - 10^{-2} N)^2}{10^{-2} N}$$

cosı per $N = 10000$

$$V = \sum_{i=1}^{100} \frac{(N_i - 100)^2}{100}$$

i valori cosı ottenuti saranno valutati nel seguente modo:

$$P_0 \leftrightarrow P_1 \text{ e } P_{99} \leftrightarrow P_{100} \text{ rigettati: } NO^{--}, NO^{++}$$

$$P_1 \leftrightarrow P_5 \text{ e } P_{95} \leftrightarrow P_{99} \text{ sospetti: } NO^{--}, NO^{++}$$

$$P_5 \leftrightarrow P_{95}$$

Ovviamente riteniamo superato il test se almeno il 90% delle sequenze ottenute da un generatore è valutato SI.

2.2 Run test

RUN UP, RUN DOWN (RUP, RUD)

Considerata una sequenza di punti T_n, si può dare un criterio per individuare una monotonia crescente o decrescente a tale sequenza.

Un modo molto facile è quello di studiare tale monotonia lungo ciascuno degli assi coordinat; cosı tale problema si riduce a quello della monotonia lineare. Un punto (a, b) suddivide cosı T_2 in due regioni attraverso l'asse delle x, e in altre due attraverso l'asse delle y.

Poiché T_2 è unitario non cambia la probabilità passando da rettangoli a segmenti di una retta

13.2cm8.8cmacdetidilifig1.eps

$$\mu_2(R(x)) = \mu_1(S(x)) = x$$

il problema resta cosı ridotto al caso lineare.

Vogliamo ora determinare quale sia il numero medio di catene ascendenti (per le discendenti il discorso è del tutto analogo) in una sequenza casuale uniformemente distribuita. Basterà calcolare quale è su T_1 il valore medio della probabilità che una catena ascedente si spezzi; ciò accadrà quando $x_{n+1} < x_n$; tale valore medio sarà allora:

$$\int_0^1 x_n dx_n = 1/2$$

7.8cm2.1cmacdetidilifig2.eps

Cosicché dopo una sequenza di N variabili casuali uniformente distribuite in $[0, 1]$, il numero di catene ascendenti (comprese quelle lunghe 1) sarà $\frac{1}{2} N$.

Nello stesso modo possiamo rispondere al successivo quesito:

In una successione casuale uniformemente distribuita quante saranno le catene di lunghezza i?

Esaminiamo i vari casi:

$i = 1$; ciò corrisponde alla situazione $x_{n+2} < x_{n+1} < x_n$ ossia

5.9cm1.5cmacdetidilifig3.eps

da cui

$$N \int_0^1 \int_0^{x_n} x_{n+1} \cdot e x_{n+1} \cdot dx_n = N \frac{1}{6} = N_1$$

$$i = 2 \; ; \quad x_{n+1} < x_n; \; x_{n+2} > x_{n+1} \; ; \quad x_{n+3} < x_{n+2}$$

7.8cm2.6cmacdetidilifig4.eps

da cui

$$N \int_0^1 \int_0^{x_n} \int_{x_{n+1}}^1 x_{n+2} \cdot dx_{n+2} \cdot dx_{n+1} \cdot dx_n = N \frac{5}{24} = N_2$$

e cosı via: $i = 3 \; N_3 = N \frac{11}{120}$

$$i = 4 \; N_4 = N \frac{19}{720}$$

$$i = 5 \; N_5 = N \frac{29}{5040}$$

$$i \geq 6 \; N_6 = N \frac{1}{840}$$

Chiaramente in una sequenza di queste catene sussiste una certa correlazione tra le lunghezze: a catene lunghe seguiranno catene brevi e viceversa. Si può trovare [17] una statistica V, tale he se O_i è il numero di catene lunghe i osservate, risulti

$$V = \sum_{\substack{l \leq i \\ j \leq 6}} \frac{(O_i - N_i)(O_j - N_j)}{N} a_{ij}$$

ove a_{ij} sono gli elementi di una opportuna matrice simmetrica (una condizione importante è che $N > 4000$).

Sotto queste condizioni V avrà una χ^2 distribuzione con sei gradi di libertà. Come per il test precedente anche qui useremo lo stesso criterio di classificazione per i risultati dei tests.

RUN ALOW – BELOW (RAB)

Si ripartisca T_2 in due sottoinsiemi R_1 e R_2, misurabili e tali che $(R_1) = (R_2) = 1/2$ e $R_1 \cup R_2 = T_2$. Di tali partizioni ne esistono infinite, quindi per qualunque esisterà sempre una partizione per la quale la sequenza si comporta in modo singolare. Si supporrà quindi che la partizione sia eseguita secondo un principio di semplicità $(R_1) = (R_2) = 1/2$ e $R_1 \cup R_2 = T_2$. Di tali partizione ne esistono infinite, quindi per qualunque sequenza esisterà sempre una partizione per la quale la sequenza si comporta in modo singolare. Si supporrà quindi che la partizione sia eseguita secondo un principio di semplicità (R_1 e R_2 connessi, forma 'regolare') e di utilità (rispondenza a richieste nelle applicazioni). Nei tets effettuati si sono proposte le seguenti partizioni

11.5cm1.7cmacdetidilifig5.eps

le prime due tengono conto della dimensione spaziale; le seconde sono equivalenti allo stesso test fatto a una dimensione.

Sia N il numero dei punti della sequenza; N_1 il numero di quelli che cadono in R_1; N_2 il numero di quelli che cadono in R_2, infine sia f il numero di volte che la sequenza salta da una regione all'altra.

Detto ciò la statistica z:

$$z = \frac{r - \mu + 1/2}{\sigma}$$

ove

$$\sigma^2 = \frac{2N_1N_2(2N_1N_2 - N_1 - N_2)}{(N_1 + N_2)^2(N_1 + N_2 - 1)}$$

$$\mu = \frac{2N_1N_2}{N_1 + N_2} + 1$$

è una normale standardizzata [8].

Anche per questa useremo gli stessi criteri d'accettazione prima ricordati.

Nel caso di trasformazioni del tipo $\phi_{M,2}$, occorre che la parità delle cifre di M non compaia masi in uno dei seguenti modi:

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} ; \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} ; \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} ; \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

In questi casi infatti per qualsiasi punto iniziale, dopo poche iterazioni, verrà generato il punto $(0,0)$ da cui ovviamente non si può più uscire.

Questa osservazione esclude la possibilità di considerare $\phi_{C,2}$.

Un'altra avvertenza da seguire è che l'ultima cifra delle coordinate dei punti iniziali non sia tale che venga azzerata per una potenza di ϕ.

Precisiamo ora i valori a cui si è fatto riferimento in 2.1/.2/.3 per le distribuzioni χ^2_{99}, χ^2_6 e Z.

	$P_{.01}$	$P_{.05}$	$P_{.95}$	$P_{.99}$
	NO^{--}	NO^-	SI	NO^+	NO^{++}
χ^2_{99}	69.3	77.	123.2	134.6
χ^2_6	.872	1.64	12.6	16.8
Z	-2.33	-1.645	1.645	2.33

(1) Tavole dei risultati per 40 seque3nze di 10000 punti

Note

i) – (tavola dei ϕ_A): I risultati di RAB ($X = Y$) e $RAB(X - 1 - Y)$ non devono stupire, giacché i parametri del test sono stati costruiti sull'ipotesi a priori che i salti avvenissero con probabilità $1/2$ mentre un semplice calcolo mostra che nel nostro caso la probabilità deve essere $1/3$, e infatti quest'ultimo risultato è pienamente confermato dai dati sperimentali.

ii) – (tavola dei ϕ_B): In questo caso le probabilità di salto dedotte dalla teoria sono effettivamente $1/2$ e perciò anche $RAB(X = Y)$ va bene (cfr. la nota i).

iii) – (tavola dei ϕ_C): Per i risultati di $RAB(X = Y)$ e $RAB(X = 1 - Y)$ rimandiamo alla posta i).

	$\phi_{A,2}$					$\phi_{A,10}$				
	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
UD-100	2	6	24	4	4	2	3	31	2	2
RUP-X	-	2	32	2	4	-	2	33	4	1
RUP-Y	1	1	31	3	4	-	2	25	8	5
RUD-X	1	1	34	1	3	-	-	34	2	4
RUD-Y	-	-	34	1	5	-	1	35	2	1
RAB (X=Y)	-	-	-	-	40	-	-	-	-	40
RAB (X=0.5)	-	-	-	-	40	-	-	-	-	40
RAB (Y=0.5)	-	3	33	2	2	1	1	34	3	-
CORR-X	1	3	33	2	1	1	1	34	3	-
CORR-Y	1	3	31	4	1	-	6	32	1	1
CORR-XY	-	-	37	3	-	-	-	38	-	2
CORR-YX	-	-	40	-	-	-	-	40	-	-

$\phi_{B,2}$					$\phi_{B,10}$				
NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
1	1	36	2	-	1	5	28	3	3
-	2	36	2	-	-	2	37	1	-
1	3	34	1	1	-	-	40	-	-
-	-	38	1	1	-	1	36	2	1
-	-	38	1	1	-	3	35	-	-
-	4	33	3	-	-	2	33	-	1
-	3	35	1	1	-	4	35	1	1
-	-	39	1	-	-	-	38	2	-
-	2	38	-	-	-	2	28	-	-
-	1	37	2	-	-	1	37	2	-
-	2	35	3	-	-	1	37	2	-
-	1	37	2	-	-	3	36	1	-
-	1	38	1	-	-	-	39	1	-

	$\phi_{C,1039}$					$\phi_{C,10}$				
	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
UD-100	5	5	27	-	3	1	3	32	3	1
RUP-X	-	2	33	-	2	-	1	34	4	1
RUP-Y	-	2	33	3	1	-	-	35	4	1
RUD-X	-	1	37	2	-	-	2	34	2	2
RUD-Y	-	2	33	4	1	-	1	34	2	2
RAB $(X=Y)$	40	-	-	-	0	40	-	-	-	-
RAB $(X=1+Y)$	-	-	-	-	40	-	-	-	-	40
RAB $(X=0.5)$	-	1	39	-	-	1	1	38	-	-
RAB $(Y=0.5)$	-	-	39	1	-	1	6	31	1	1
CORR-X	-	-	39	1	-	-	4	31	3	1
CORR-Y	-	-	40	-	-	1	1	34	4	-
CORR-XY	-	1	36	1	2	2	-	36	1	1
CORR-YX	1	3	29	4	3	-	2	36	2	-

	$\phi_{D,2}$					$\phi_{D,10}$				
NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
-	3	33	3	1	2	2	34	2	-
1	1	36	1	1	-	4	35	1	-
-	2	34	4	-	-	3	34	2	1
-	3	34	3	-	-	1	37	2	-
-	2	36	2	-	-	1	36	3	-
1	1	38	-	-	1	1	37	-	1
1	4	32	3	-	-	5	34	1	-
-	1	37	2	-	-	1	37	1	1
-	2	37	1	-	1	1	37	1	-
-	2	37	-	1	-	1	38	1	-
1	-	37	2	-	-	2	34	4	-
-	3	36	1	-	-	-	34	5	1
-	2	37	1	-	-	-	40	-	-

(2) Tavole dei risultati per 4 sequenze di $j \cdot 10^4 (j = 2, 3, 4)$ punti

– Punti iniziali: (.3, .8); (.364, .859); (.8, .3); (.859, .364).

– In ogni colonna il primo numero è riferito alle sequenze lunghe $2 \cdot 10^4$, il secondo per quelle lunghe $3 \cdot 10^4$, il terzo per quelle lunghe $4 \cdot 10^4$.

	$\phi_{A,2}$					$\phi_{A,10}$				
	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
UD-100	-	-	344	100	-	-	100	234	010	100
RUP-X	-	-	321	122	001	-	-	333	001	110
RUP-Y	-	-	333	100	001	-	-	323	110	011
RUD-X	-	-	222	221	001	-	-	332	001	111
RUD-Y	-	-	344	100	-	-	-	343	101	-
RAB $_{(X=Y)}$	-	-	-	-	444	-	-	-	-	444
RAB $_{(X=1-Y)}$	-	-	-	-	444	-	-	-	-	444
RAB $_{(X=0.5)}$	-	110	234	100	-	-	-	223	121	100
RAB $_{(Y=0.5)}$	-	-	333	-	111	-	-	444	-	-
CORR-X	-	101	233	110	-	111	020	213	100	-
CORR-Y	101	111	231	001	-	-	010	434	-	-
CORR-XY	-	-	444	-	-	-	-	333	111	-
CORR-YX	-	-	444	-	-	-	-	444	-	-

$\phi_{B,2}$					$\phi_{B,10}$				
NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
-	-	344	-	100	-	-	444	-	-
-	-	323	110	011	-	-	433	011	-
-	-	433	011	-	-	-	444	-	-
-	-	432	001	011	-	-	433	011	-
-	-2	433	011	-	-	-	444	-	-
-	121	323	-	-	-	-	444	-	-
-	-	444	-	-	-	-	444	-	-
-	-	444	-	-	-	010	434	-	-
-	-	444	-	-	-	-	444	-	-
-	-	334	110	-	-	-	444	-	-
001	110	333	-	-	-	010	434	-	-
-	-	444	-	-	-	-	444	-	-
-	-	444	-	-	-	010	434	-	-

	$\phi_{C,1039}$					$\phi_{C,10}$				
	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
UD-100	101	010	332	-	-	-	-	444	-	-
RUP-X	010	101	323	010	-	-	110	334	-	-
RUP-Y	-	-	444	-	-	-	-	444	-	-
RUD-X	-	010	434	-	-	-	-	444	-	-
RUD-Y	-	-	434	010	-	-	100	344	-	-
RAB $_{(X=Y)}$	444	-	-	-	-	444	-	-	-	-
RAB $_{(X=1-Y)}$	-	-	-	-	444	-	-	-	-	444
RAB $_{(X=0.5)}$	-	111	333	-	-	-	-	444	-	-
RAB $_{(Y=0.5)}$	-	-	443	001	-	111	-	333	-	-
CORR-X	-	-	444	-	-	-	-	444	-	-
CORR-Y	-	-	444	-	-	-	-	333	-	111
CORR-XY	-	-	444	-	-	-	-	444	-	-
CORR-YX	-	-	433	010	001	-	010	434	-	-

$\phi_{D,2}$					$\phi_{D,10}$				
NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
001	-	443	-	-	-	-	344	100	-
-	010	423	011	-	-	-	444	-	-
-	-	444	-	-	-	-	432	-	011
-	-	443	-	001	-	-	443	001	011
-	0112	433	-	-	-	100	344	-	-
-	001	443	-	-	-	-	434	010	-
-	-	444	-	-	-	-	444	-	-
-	-	344	100	-	-	-	322	122	-
-	100	344	100	-	-	111	333	-	-
-	100	344	-	-	-	001	443	-	-
-	001	322	001	110	-	-	433	011	-
-	-	444	-	-	-	-	444	-	-
-	-	434	010	-	-	-	444	-	-

(3) Tavole dei risultati per 4 sequenze di $j \cdot 10^4 (j = 5, 6, 7)$ punti

In ogni colonna il primo numero è riferito alle sequenze lunghe $5 \cdot 10^4$, il secondo a quelle di $5 \cdot 10^4$, il terzo a quelle di $7 \cdot 10^4$.

	$\phi_{A,2}$					$\phi_{A,10}$				
	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
UD-100	-	-	333	100	011	-	001	342	101	-
RUP-X	-	-	221	112	111	-	-	333	001	100
RUP-Y	-	-	333	-	111	-	-	222	-	222
RUD-X	-	-	222	011	211	-	110	112	222	-
RUD-Y	-	-	332	112	-	-	-	422	022	-
RAB $_{(X=Y)}$	-	-	-	-	444	-	-	-	-	444
RAB $_{(X=1-Y)}$	-	-	-	-	444	-	-	-	-	444
RAB $_{(X=0.5)}$	-	011	323	110	-	-	-	444	-	-
RAB $_{(Y=0.5)}$	-	-	333	-	111	-	-	434	010	-
CORR-X	110	001	222	100	011	110	001	333	-	-
CORR-Y	110	001	333	-	-	-	-	444	-	-
CORR-XY	-	-	444	-	-	-	-	334	110	-
CORR-YX	-	-	444	-	-	-	-	444	-	-

	$\phi_{B,2}$					$\phi_{B,10}$			
NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
-	-	334	110	-	-	011	433	-	-
-	-	121	211	112	-	-	322	022	100
-	-	333	101	010	-	-	444	-	-
-	-	110	212	122	-	-	332	111	001
-	-	333	111	-	-	-	444	-	-
100	122	222	-	-	-	-	444	-	-
-	-	444	-	-	-	-	444	-	-
-	-	444	-	-	-	100	344	-	-
-	-	444	-	-	-	-	444	-	-
-	110	334	-	-	-	-	444	-	-
-	110	334	-	-	-	-	444	-	-
-	-	444	-	-	-	-	444	-	-
-	100	344	-	-	-	-	444	-	-

	$\phi_{C,1039}$					$\phi_{C,10}$				
	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
UD-100	202	-	132	110	-	-	-	444	-	-
RUP-X	-	-	444	-	-	-	-	444	-	-
RUP-Y	-	-	433	-	011	-	-	433	011	-
RUD-X	-	-	444	-	-	-	-	444	-	-
RUD-Y	-	001	433	010	-	-	-	444	-	-
RAB $_{(X=Y)}$	444	-	-	-	-	444	-	-	-	-
RAB $_{(X=1-Y)}$	-	-	-	-	444	-	-	-	-	444
RAB $_{(X=0.5)}$	100	011	333	-	-	-	-	444	-	-
RAB $_{(Y=0.5)}$	-	100	344	-	-	111	-	333	-	-
CORR-X	-	-	444	-	-	-	-	444	-	444
CORR-Y	-	-	444	-	-	-	-	333	-	111
CORR-XY	-	-	434	010	-	-	-	444	-	111
CORR-YX	-	-	434	010	-	-	-	444	-	111

	$\phi_{D,2}$					$\phi_{D,10}$			
NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
100	-	344	-	-	-	-	443	001	-
-	-	444	-	-	-	110	334	-	-
-	-	433	011	-	-	-	433	010	001
-	-	444	-	-	-	100	344	-	-
-	-	444	-	-	-	-	444	-	-
011	100	333	-	-	-	-	444	-	-
-	-	433	011	-	-	001	443	-	-
-	-	444	-	-	-	-	433	011	-
-	111	333	-	-	-	-	444	-	-
-	-	444	-	-	-	-	344	100	-
-	111	222	111	-	-	-	333	111	-
-	100	344	111	-	-	-	443	001	-
-	-	444	-	-	-	-	444	-	-

(4) Tavole dei risultati per 4 sequenze di $j \cdot 10^4 (j = 8, 9, 10)$ *punti*

Punti iniziali: Vedi tavv. (2).

In ogni colonna il primo numero è riferito alle sequenze lunghe $8 \cdot 10^4$, il secondo a quelle di $9 \cdot 10^4$, il terzo a quelle di $10 \cdot 10^4$.

	$\phi_{A,2}$					$\phi_{A,10}$				
	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
UD-100	-	-	333	100	011	-	011	322	-	111
RUP-X	-	-	122	100	222	-	-	321	122	001
RUP-Y	011	100	222	-	111	-	-	111	101	232
RUD-X	-	-	111	101	232	-	-	211	211	022
RUD-Y	-	-	222	101	121	-	-	224	220	-
RAB $_{(X=Y)}$	-	-	-	-	444	-	-	-	-	444
RAB $_{(X=1-Y)}$	-	-	-	-	444	-	-	-	-	444
RAB $_{(X=0.5)}$	-	111	333	-	-	-	-	444	-	-
RAB $_{(Y=0.5)}$	-	-	333	-	111	-	-	434	010	-
CORR-X	011	-	222	110	100	-	111	333	-	-
CORR-Y	100	011	222	110	001	-	-	444	-	-
CORR-XY	-	-	444	-	-	-	-	444	-	-
CORR-YX	-	-	444	-	-	-	-	444	-	-

	$\phi_{B,2}$					$\phi_{B,10}$			
NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
-	-	333	010	101	110	101	233	-	-
-	-	101	111	232	-	-	322	121	001
-	-	440	-	-	-	-	444	-	-
-	-	110	223	111	-	-	222	-	222
-	-	444	-	-	-	-	344	100	-
-	211	123	110	-	-	-	444	100	-
-	-	444	-	-	-	-	444	-	-
-	-	444	-	-	-	-	444	-	-
-	-	444	-	-	-	-	444	-	-
-	-	444	-	-	-	-	444	-	-
-	-	334	100	-	-	-	444	-	-
-	011	433	-	-	-	-	444	-	-
-	111	333	-	-	-	-	444	-	-

	$\phi_{C,1039}$					$\phi_{C,10}$				
	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
UD-100	111	-	333	-	-	-	110	334	-	-
RUP-X	-	-	332	111	001	-	-	444	-	-
RUP-Y	-	-	332	001	111	-	-	232	212	-
RUD-X	-	-	444	-	-	-	-	332	001	111
RUD-Y	-	-	433	001	010	-	-	444	-	-
RAB $(X=Y)$	444	-	-	-	-	444	-	-	-	-
RAB $(X=1-Y)$	-	-	-	-	444	-	-	-	-	444
RAB $(X=0.5)$	-	101	343	-	-	-	-	444	-	444
RAB $(Y=0.5)$	-	-	444	-	-	111	-	333	-	-
CORR-X	-	-	444	-	-	-	-	444	-	-
CORR-Y	-	-	444	-	-	-	-	333	-	111
CORR-XY	-	-	444	-	-	-	100	244	100	-
CORR-YX	-	-	434	010	-	-	111	333	-	-

	$\phi_{D,2}$					$\phi_{D,10}$				
NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}	NO^{--}	NO^{-}	SI	NO^{+}	NO^{++}
001	010	433	-	-	-	-	444	-	-
-	-	444	-	-	-	-	444	-	-
-	-	333	111	-	-	-	233	111	100
-	-	333	110	001	-	010	434	111	100
-	-	444	-	-	-	-	334	110	-
110	001	333	-	-	-	-	444	-	-
-	100	334	010	-	-	011	433	-	-
-	-	444	-	-	-	-	443	001	-
-	100	344	-	-	-	-	444	-	-
-	-	444	-	-	-	-	444	-	-
-	110	224	110	-	-	-	344	100	-
-	-	444	-	-	-	-	333	111	-
-	-	444	-	-	-	-	444	-	-

References

[1] Schnorr C.P., *Zufälligkeit und wahrscheinlichkeit*, Springer–Verlag n. 218.

[2] Arnold–Avez, *Problémes ergodiques de la mécanique classique*, 1967.

[3] Bowen R., "The equidistribution of closed geodesics", *Amer. J. Math.* **94** (1972), 413–423.

[4] Boxen R., *Equilibrium states and the ergodic theory of Anosov diffeomorphisms*, Springer LNM, n. 470.

[5] Bozzini T.–De Tisi F., *Statistica* (parte I), 1980.

[6] Bozzini T., *Sequenze pseudo–casuali con proprietà di equidistribuzione in R^n*, 1977.

[7] Champernowne D., *The construction of decimals normal in the scale of ten*, 1933.

[8] Copeland A.–Erods P., *Note on normal numbers*, 1946.

[9] Cugiani M., *Metodi numerico statistici*, 1980.

[10] Denker M., and Jacobs K. (ed.), *Ergodic theory*, Springer LNM, n. 729.

[11] Di Libero A., *Tesi. Scuola di perfezionamento in Matematica applicata*, Università di Milano, 1981.

[12] Dixon W.–Massey F., *Introduction to statistical analysis*, 1969.

[13] Dudewicz E.–Ralley T., *The handbook of random number generation and testing*, 1981.

[14] Gotusso L., *Successioni uniformemente distribuite*, 1963.

[15] Grafton R., *The runs–up and runs–down tests*, 1981.

[16] Hardy–Wright, *The theory of numbers*, 1960.

[17] Knuth D., *The art of computer programming* (vol. II), 1981.

[18] Lewis T.–Payne W., *Generalized feedback shift register*, 1973.

[19] Niven I.–Zuckerman H., *On the definition of normal numbers*, 1953.

[20] Riccaldone M., *Metodi ergodici per la generazione di punti casuali e applicazioni all'integrazione Monte–Carlo multipla*, Tesi U.S.M., A.A. 79/80.

[21] Sarnak P., "Asymptotic behavior of periodic orbits of the Horocycle flow and Einstein Series", *Commun. on Pure and Appl. Math.* **34** (1981), 719–739.

[22] Sigmund K., *Nombres normaux et theorie ergodique*, 1976.