

ISTITUTO NAZIONALE DI FISICA NUCLEARE

Laboratori Nazionali
di Legnaro

INFN/TC-84/3
20 Febbraio 1984

M. Pavanati: TEST DI CASUALITA' DEL GENERATORE
DI NUMERI PSEUDOCASUALI RAN PER IL VAX 11/780
DIGITALE

Servizio Documentazione
dei Laboratori Nazionali di Frascati

Istituto Nazionale di Fisica Nucleare
Laboratori Nazionali di Legnaro

INFN/TC-84/3
20 Febbraio 1984

M. Pavanati: TEST DI CASUALITA' DEL GENERATORE DI NUMERI
PSEUDOCASUALI RAN PER IL VAX 11/780 DIGITALE

SOMMARIO

Viene analizzata l'efficienza del generatore di numeri pseudo-casuali RAN installato come funzione di libreria nel calcolatore VAX 11/780.

Pur presentando alcuni difetti, significativi nel caso d'impiego in situazioni in cui il requisito di "casualità" in senso stretto rivesta carattere di particolare delicatezza, l'algoritmo risulta accettabile per le normali applicazioni nel campo della fisica.

1. - INTRODUZIONE

Varie tecniche di calcolo quali le simulazioni numeriche e le applicazioni del metodo di Montecarlo richiedono l'uso di generatori aritmetici di sequenze pseudo-casuali.

La bontà della distribuzione dei valori ottenuti da tali algoritmi va verificata in vista di applicazioni pratiche particolarmente sensibili alla "casualità" delle sequenze utilizzate.

Sono state analizzate le caratteristiche del generatore installato sui calcolatori VAX 11/780 DIGITAL, operativi presso i Laboratori Nazionali di Legnaro e presso il Dipartimento di Fisica dell'Università di Padova.

A tale scopo si sono impiegati test statistici normalmente adottati per tali verifiche.

2. - CARATTERISTICHE DELL'ALGORITMO

Nella versione in linguaggio FORTRAN impiegata per l'esecuzione dei test il generatore è fornito come funzione aritmetica di libreria nella forma

$$y = \text{RAN}(i) \quad (1)$$

con y REALE e i INTERO. Per i valori generati è prevista una distribuzione uniforme nell'intervallo $(0, 1)$.

Il funzionamento è basato sull'applicazione del metodo congruenziale lineare moltiplicativo^(1, 2) con cui si ottengono sequenze pseudo-casuali di interi tramite calcolo iterativo dell'espressione intera

$$I_{i+1} = (aI_i + b) \bmod c. \quad (2)$$

a, b, c sono parametri fissati che caratterizzano completamente il comportamento del generatore. Nel caso specifico

$$a = 69069, \quad b = 1, \quad c = 2^{32}.$$

La scelta di c è legata al tipo di rappresentazione binaria intera in 32 bit utilizzata dall'elaboratore.

Il primo elemento della sequenza viene fornito come dato in ingresso, ed inizializza il processo di calcolo, determinando univocamente la sequenza stessa.

I valori reali forniti da RAN vengono ottenuti convertendo i 24 bit più significativi della rappresentazione binaria intera in rappresentazione floating point.

3. - VALUTAZIONE DEL PERIODO DEL GENERATORE

Il metodo congruenziale lineare consente di produrre solo sequenze numeriche periodiche. Teoricamente infatti dall'espressione (2) è possibile ricavare al più 2^{32} valori interi diversi. La ripetizione di un numero in punti diversi della sequenza provoca la ripetizione di tutti i valori compresi tra tali punti.

Nelle applicazioni pratiche la periodicità può essere trascurata solo se il periodo di ripetizione è molto elevato.

Prove ripetute per più inizializzatori indicano che il periodo di RAN non è inferiore a 10^7 .

4. - TEST DEL χ^2 E DI KOLMOGOROV SMIRNOV

Una prima verifica dell'affidabilità del generatore è ottenibile tramite i test del χ^2 e di Kolmogorov-Smirnov.

Per una trattazione matematica approfondita a tale riguardo si rimanda alla bibliografia ormai classica⁽¹⁾. Nel seguito verrà descritta la metodologia seguita nella analisi, per permettere la comprensione dei risultati ottenuti.

4.1. - Test del χ^2

Viene generata una sequenza di N valori. Il codominio di RAN viene suddiviso in K sottointervalli uguali. Se f_i indica il numero di elementi della sequenza che cadono nell'iesimo intervallo la grandezza V calcolata tramite la

$$V = \sum_{i=1}^K \frac{(f_i - \frac{N}{K})^2}{\frac{N}{K}} \quad (3)$$

ha una distribuzione del tipo χ^2 (con buona approssimazione se $N/K \gg 5$).

E' possibile fissare dei livelli di confidenza massimi e minimi per V. In linea di massima un V troppo elevato denuncia disomogeneità nella distribuzione dei valori generati. Viceversa un V troppo basso denota una distribuzione troppo regolare, presumibilmente "non casuale".

In Tabella I sono riportati i valori dei livelli di confidenza a 5% e all'1% in funzione del numero di gradi di libertà $\nu = K-1$ con cui è stata effettuata la scansione del codominio.

TABELLA I - Livelli di confidenza per il test del χ^2 .
Valori ricavati da ref. (1).

K-1	P=99%	P=95%	P=5%	P=1%
10	2.56	3.94	18.31	23.21
20	8.26	10.8	31.41	37.57
30	14.95	18.40	43.77	50.89
40	22.17	26.55	55.64	63.66
50	29.71	34.76	67.50	76.15
60	37.51	43.25	78.90	88.33
70	45.47	51.85	90.33	100.36
80	53.58	60.00	101.66	112.26
90	61.8	69.23	112.92	124.04
100	70.12	78.10	124.09	135.72
150	112.75	122.93	179.27	193.04
200	156.53	168.57	233.62	249.31
250	201.06	214.73	287.46	304.78
300	246.11	261.26	340.00	359.73
350	291.56	308.07	394.13	414.28
400	337.32	355.10	447.10	468.52
500	429.58	449.66	552.53	576.26
600	522.58	544.76	657.43	683.26
700	616.15	640.24	761.94	789.70
800	710.84	736.04	866.15	895.69
900	804.52	832.1	970.10	1001.32
1000	899.2	928.36	1073.83	1106.64
2000	1856.23	1898.24	2103.96	2149.60

Un valore di V al di fuori dei limiti di confidenza al 5% induce a sospettare della sequenza esaminata. Un'analogha condizione per i limiti dell'1% denota una probabile anomalia.

4.2. - Test di Kolmogorov-Smirnov

Per una sequenza di N numeri, posto $F_N(x)$ pari al numero di elementi generati $\leq x$ si calcolano le due grandezze K^+ e K^- tramite le

$$K^+ = \max(F_N(x) - x), \quad K^- = \max(x - F_N(x)). \quad (4)$$

Il metodo di valutazione è poi analogo a quello seguito nel caso del χ^2 . K^+ e K^- devono essere compresi entro limiti fissati.

In Tabella II sono riportati tali limiti K_{\max}^+ e K_{\min}^+ in funzione di N per i livelli di confidenza dell'1% e del 5%

TABELLA II - Test di Kolmogorov-Smirnov: limiti di confidenza ricavati dalla ref. (1).

N	P=99%	P=95%	P=5%	P=1%
10	0.029	0.115	1.166	1.440
20	0.038	0.130	1.184	1.470
30	0.044	0.135	1.192	1.480
50	0.050	0.140	1.200	1.489
100	0.056	0.146	1.207	1.497
500	0.064	0.154	1.216	1.508
1000	0.066	0.156	1.219	1.511
3000	0.068	0.158	1.221	1.514
5000	0.069	0.158	1.221	1.514
100000	0.069	0.159	1.222	1.515
500000	0.070	0.159	1.223	1.517

Entrambi i test valutano dunque le deviazioni della distribuzione dei valori ottenuti da RAN rispetto a quella casuale uniforme teorica.

Poichè in un caso viene analizzata la funzione di frequenza e nell'altro la funzione di distribuzione, le informazioni ottenute sono complementari.

Sequenze ritenute accettabili in base ai risultati di un test possono infatti rivelarsi anomale in seguito al responso dell'altro.

D'altro canto l'esito negativo di una singola prova non implica necessariamente un difetto del generatore. Esso va infatti esaminato sia analizzando sequenze lunghe (andamento globale), sia dal punto di vista "locale" per sequenze con N relativamente basso.

Ripetendo l'analisi per un numero di volte sufficientemente elevato in regioni diverse della sequenza principale è possibile stabilire se le anomalie si verificano con frequenza compresa nei limiti di confidenza previsti.

Tutto il procedimento dev'essere replicato utilizzando inizializzatori diversi: un generatore ottimale dovrebbe essere poco influenzato dalla scelta di un tale parametro.

4.3. - Test del χ^2 e di Kolmogorov-Smirnov: risultati

Sono state analizzate sequenze ricavate da 5 diversi inizializzatori, riportati in Tabella III.

TABELLA III

A=616318177	B=65537
C=1234567689	D=1234567
E=2222222	

L'analisi globale è stata condotta per $N = 10000, 50000, 100000$. In Fig. 1 sono visibili i risultati relativi al test del χ^2 per vari casi, in funzione del numero di gradi di libertà impiegati per la scansione.

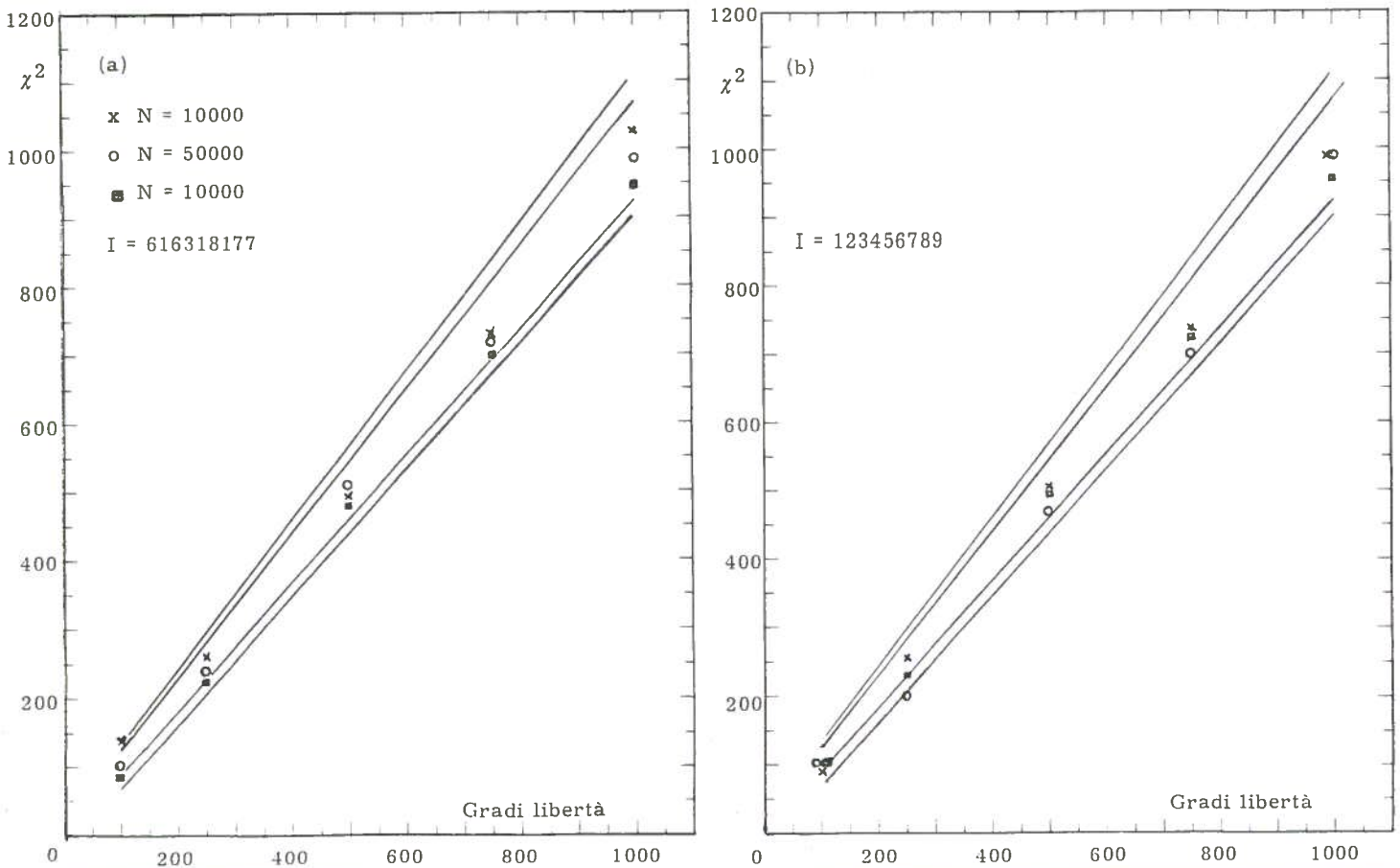


FIG. 1 - Esito del test del χ^2 globale per RAN: inizializzatori A (a) e C (b).

In linea di massima i valori rientrano nella norma. L'anomalia della sequenza di C per N=50000 (χ^2 troppo basso) appare in sè scarsamente significativa. Tuttavia, considerando la percentuale di prove anomale individuate nell'analisi per ripetizione del test (2000 iterazioni per N=10000, inizializzatori A e C) risulta evidente una tendenza del generatore a fornire sequenze con χ^2 basso (cfr. Tabella IV).

TABELLA IV - Percentuale di sequenze risultate anomale nel test del χ^2 globale. La statistica si riferisce, per I, N, K fissati, a 2000 campionamenti. Le righe indicate con > riguardano i casi di valori di χ^2 troppo alto. Le righe indicate con < quelli di χ^2 troppo basso. Sono riportati solo i risultati che possono indicare un cattivo funzionamento del generatore.

I	N	K	P=1%	P=5%	
123456789	10000	100	1.05%	5.05%	>
			1.25%	5.95%	<
		500	0.85%	5.15%	>
			1.45%	5.3%	<
		1000	0.60%	5.00%	>
616318177	10000		0.65%	5.00%	<
		100	0.8%	3.85%	>
			1.45%	5.75%	<

L'analisi locale è stata condotta per N=1000, 3000, 5000. I risultati del test del χ^2 compaiono in Fig. 2. Nella maggior parte dei casi considerati, in particolare per N=1000, il χ^2 è al di sotto dei limiti previsti.

L'analisi per prove ripetute conferma un tale comportamento: la percentuale di prove risultate anomale si discosta dal valore teorico previsto in modo sensibile (cfr. Tabella V). Si nota inoltre una dipendenza nell'andamento dei valori ottenuti dalla scelta dell'inizializzatore.

TABELLA V - Test del χ^2 , analisi locale: percentuale di valori anomali. Statistica, per ogni I, N, K, di 2000 iterazioni. Le righe indicate con il simbolo > si riferiscono ai casi in cui il χ^2 risulta troppo alto. Quelle indicate con < si riferiscono ai casi di χ^2 troppo basso. Sono riportati solo i risultati che possono indicare un difetto di RAN.

I	N	K	P=1%	P=5%	
123456789	1000	100	0.85%	4.25%	>
			0.85%	5.7%	<
		60	1.05%	4.8%	>
			1.4%	6.45%	<
		50	0.55%	3.5%	>
			1.5%	5.7%	<
		20	0.75%	3.65%	>
616318177	1000		1.3%	6.3%	<
		40	0.65%	4.15%	>
			1.45%	6.8%	<
		20	0.54%	3.45%	>
65537	1000		1.57%	6.9%	<
		50	1.25%	4.65%	>
			1.35%	6.15%	<
		40	0.85%	4.55%	>
			1.15%	7.15%	<
		20	0.6%	3.25%	>
	1.3%	7.9%	<		

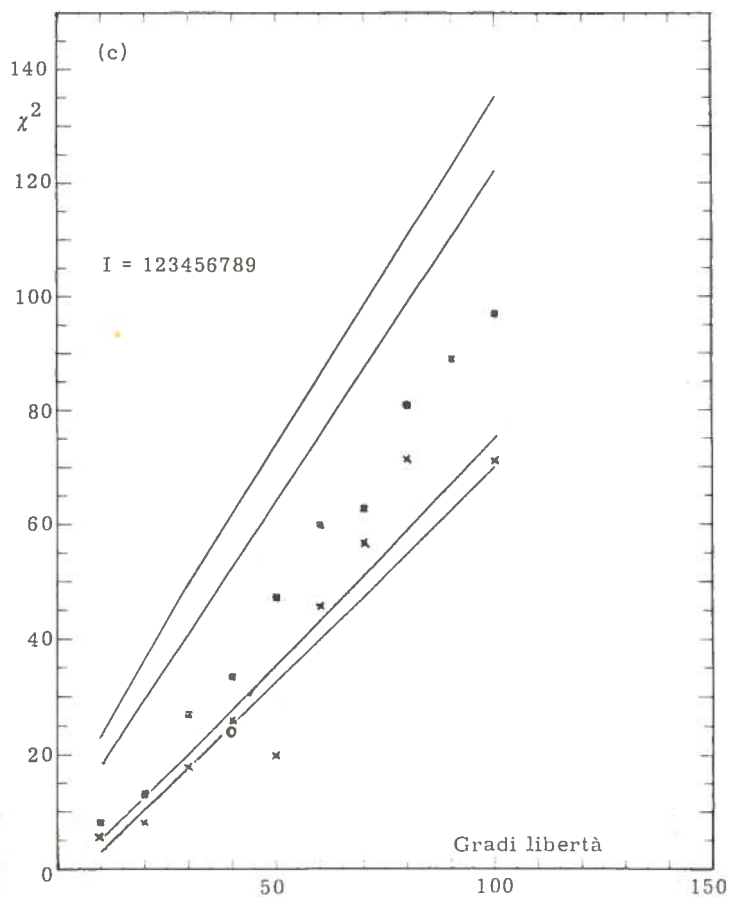
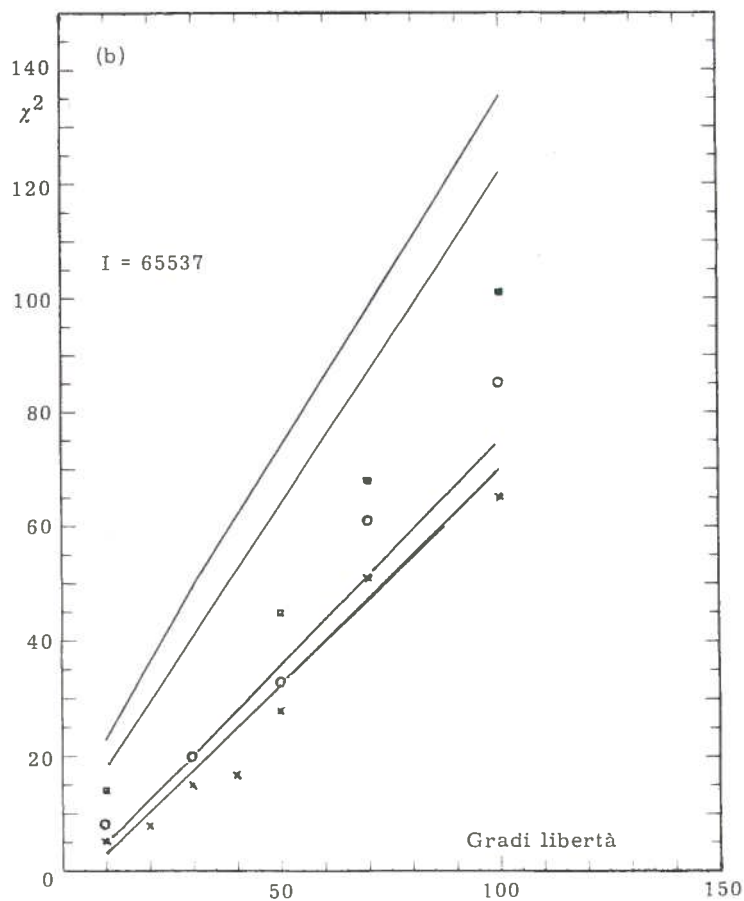
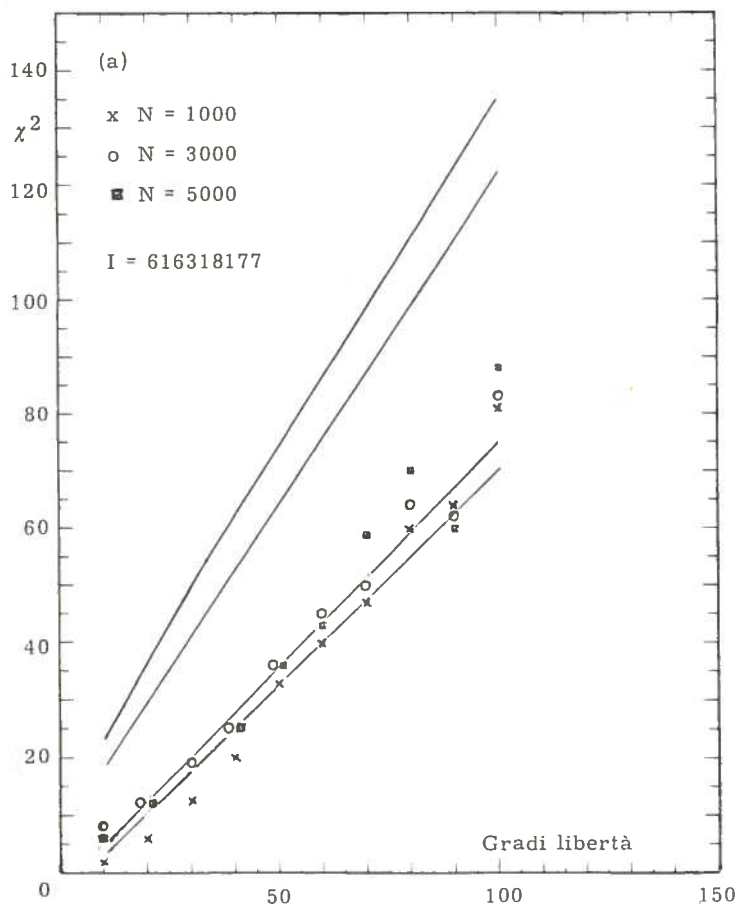


FIG. 2 - Esito del test del χ^2 locale per RAN, inizializzatori A, B, C (fig. (a), (b), (c)): il χ^2 risulta troppo basso per N = 1000.

Un'ulteriore conferma si può avere dal responso del test di Kolmogorov-Smirnov. E' evidente (cfr. Tabella VI) che i valori di K^+ e K^- per $N=1000$ sono troppo bassi (al di fuori dei limiti di confidenza del 5%).

TABELLA VI - Test di Kolmogorov-Smirnov: risultati ottenuti per RAN, RNDM, RNDM2. I valori anomali sono segnati con asterischi.

I	N	K+	K-
TEST KOLMOGOROV SMIRNOV GENERATORE RAN			
123456789	1000	0.646	0.457
	3000	0.421	0.916
	5000	0.620	0.918
	10000	0.427	0.818
616318177	1000	*0.125*	0.515
	3000	0.276	0.686
	5000	0.997	*0.150*
	1000	*0.124*	1.167
65537	3000	0.249	0.822
	5000	0.268	0.932
	10000	0.447	0.769
	1000	0.419	0.784
1234567	3000	0.524	0.899
	5000	0.507	0.764
	5000	0.801	0.521
	5000	0.801	0.521
TEST KOLMOGOROV SMIRNOV GENERATORE RNDM (CERNLIB)			
	1000	0.692	0.884
		1.030	0.464
TEST KOLMOGOROV SMIRNOV GENERATORE RNDM2 (CERNLIB)			
	1000	*0.043*	*1.423*
	3000	0.692	0.217
	5000	0.565	0.841
	10000	0.903	0.570

A titolo di confronto si è condotta un'identica analisi per i generatori RNDM e RNDM2 della libreria di subroutine CERNLIB (CERN).

RNDM, creato per essere impiegato su macchine che utilizzano rappresentazione numerica a 64 bit (CDC7600) non presenta un rendimento ottimale se sfruttato su elaboratori con rappresentazione a 32 bit (VAX, IBM 370) (cfr. quanto dichiarato nel manuale CERNLIB⁽³⁾).

RNDM2 invece è stato realizzato appositamente per essere impiegato su macchine a 32 bit.

I risultati ottenuti per il test del χ^2 , riportati in Fig. 3 evidenziano effettivamente un cattivo funzionamento di RNDM (valori di χ^2 troppo elevati), mentre il comportamento di RNDM2 risulta accettabile, almeno localmente.

L'analisi per prove ripetute indica comunque che, su un ampio intervallo, il comportamento dei tre generatori si può ritenere praticamente equivalente.

Il test di Kolmogorov-Smirnov fornisce invece per RNDM2 un responso meno buono che per RAN, a causa dell'anomalia riscontrabile per $N=1000$ (cfr. Tabella VI), al di fuori dei limiti di confidenza dell'1%.

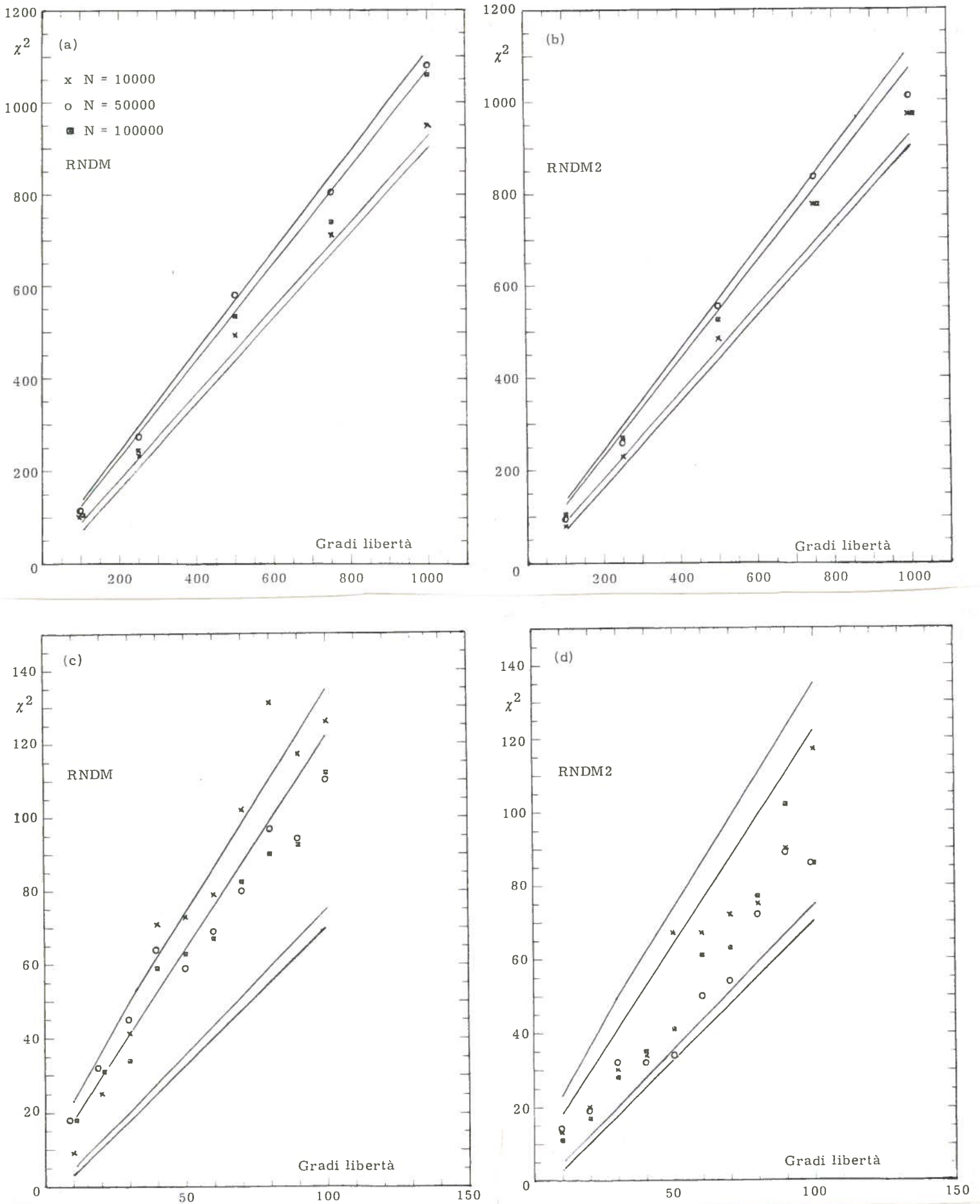


FIG. 3 - Esito dei test del χ^2 globali (fig. (a), (b)) e locali (fig. (c), (d)) per RNDM e per RNDM2 : i valori di χ^2 per RNDM risultano in generale troppo elevati.

5. - TEST DI CORRELAZIONE

Data una sequenza principale (U(i), i = 1, ..., N) si sono ricercate eventuali correlazioni tra elementi di sottosequenze ottenute per campionamento, del tipo (V(j), j = i(1+1)), (W(k), k = i(1+1)+1): è stato calcolato il coefficiente di correlazione

$$r = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \quad \sigma_{xy} = \frac{1}{N-1} \sum_i (x_i - \bar{x})(y_i - \bar{y}) \quad (5)$$

e l'analisi è stata ripetuta in zone diverse della sequenza principale. I valori di r sono stati mediati, e si è potuto calcolare uno scarto dal valor medio per la distribuzione ottenuta.

I risultati relativi al caso l = 1 sono riportati, per alcuni inizializzatori, in Tabella VII e non indicano particolari anomalie. I coefficienti di correlazione risultano prossimi a 0.

TABELLA VII - Risultati del test di correlazione. Per ogni inizializzatore I sono riportati i valori medi (V.M.) e gli scarti quadratici (R.M.S.) dei coefficienti di correlazione relativi a sequenze di lunghezza N, calcolati per n iterazioni.

I	N	n	V.M.	R.M.S.
123456789	500	100	-0.16E-2	4.20E-2
65537	500	100	-0.39E-2	4.42E-2
616318177	500	100	+0.14E-2	4.02E-2
	2500	100	-0.27E-2	1.72E-2

6. - TEST DI MONOTONICITA'

Ciascuna sequenza principale può essere considerata come composta da una successione di sottosequenze ad andamento monotono crescente o decrescente di lunghezza variabile.

Il test del χ^2 è stato applicato alla distribuzione ottenuta per l'evento "generazione di una sottosequenza di lunghezza K", la cui funzione di frequenza teorica è

$$A(K, N) = \frac{2[(K^2 + 3K + 1)N - (K^3 + 3K^2 - K - 4)]}{(K + 3)!} \quad (6)$$

Il responso di una simile analisi non consente un'interpretazione diretta di eventuali anomalie rilevate, ai fini delle usuali applicazioni pratiche: ci si deve limitare a verificare se una data sequenza ha superato o no la prova.

Si tratta comunque di un test molto sensibile alla "non casualità" delle sequenze prodotte; è stato usato dalla stessa DIGITAL per il controllo di un generatore installato su PDP-8⁽⁴⁾.

In Fig. 4 sono riportati vari risultati ottenuti per RAN, RNDM, RNDM2: quasi tutte le sequenze di RAN superano il test, fatta eccezione per quelle corrispondenti ad I = 1234567 (valori di χ^2 al di fuori dei limiti di confidenza dell'1%) e ad I = 616318177 (valori di χ^2 al di fuori dei limiti di confidenza del 5%).

RNDM supera regolarmente il test, mentre per RNDM2 si ha un valore di χ^2 al di fuori dei limiti di confidenza del 5% (N = 50000).

In ogni caso il comportamento dei tre generatori si può considerare pressochè equivalente.

7. - TEST DI SIMULAZIONE

I test precedentemente descritti, pur risultando efficaci nel rivelare caratteristiche "non random" di un generatore non sono da soli sufficienti a garantirne l'affidabilità. Alcuni algoritmi, pur avendo superato tutti i test, all'atto dell'impiego si sono rivelati difettosi⁽⁵⁾.

Si è pertanto effettuata un'ulteriore analisi, centrata sullo studio del comportamento del generatore quando utilizzato per produrre punti in uno spazio a 2 o 3 dimensioni. Tale applicazione è spesso richiesta in campo fisico, ad esempio quando si debbano simulare fenomeni di trasporto, o l'emissione di particelle da una sorgente.

Il principale difetto da individuare in tali casi è la tendenza ad addensare i punti generati in regioni di spazio privilegiate (ad es. in piani distinti: si parla in tal caso di "striatura" dello spazio).

Per rilevare l'anomalia si sono usati due metodi: il primo basato sul calcolo diretto del χ^2 , il secondo realizzato sfruttando tecniche di reiezione.

7.1. - Metodo diretto

I punti generati risultano distribuiti in un cubo (un quadrato nel caso bidimensionale) di lato 1. Le loro coordinate vengono ottenute direttamente dalla sequenza principale, raggruppando gli elementi della sequenza in terne (coppie). Lo spazio viene suddiviso in celle identiche, e alla scansione realizzata si applica il test del χ^2 .

Anche in questo caso si è effettuata un'analisi globale (N = 10000, 50000, 100000) e una locale (N = 1000, 3000, 5000) per gli inizializzatori già usati in precedenza.

Per la scansione si sono sfruttate strutture a reticolo in 2 e 3 dimensioni di vario tipo. I risultati ottenuti sono riportati in Fig. 5.

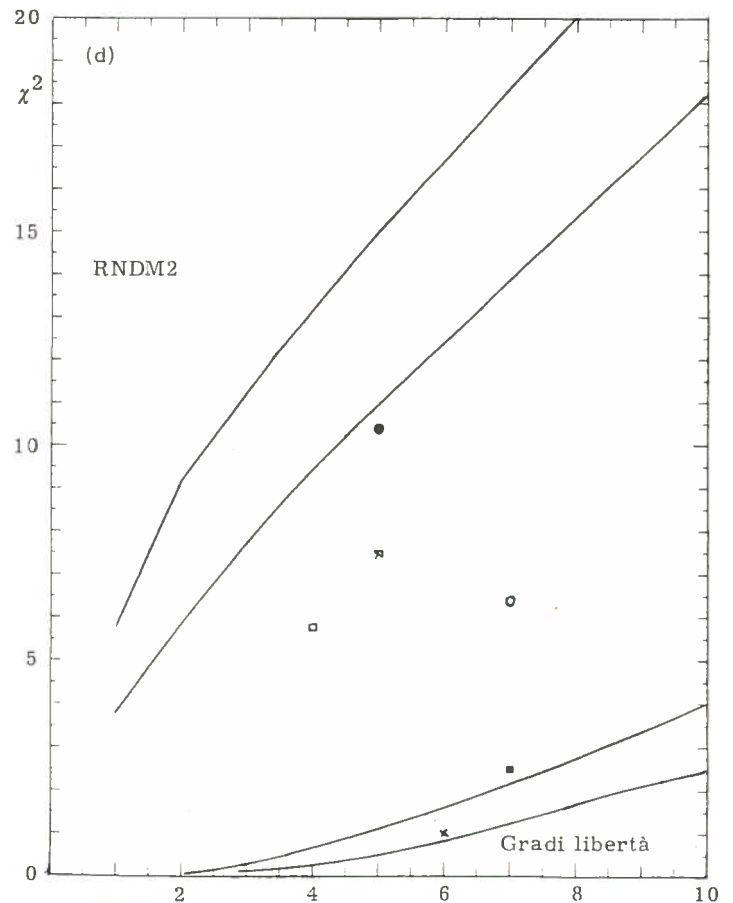
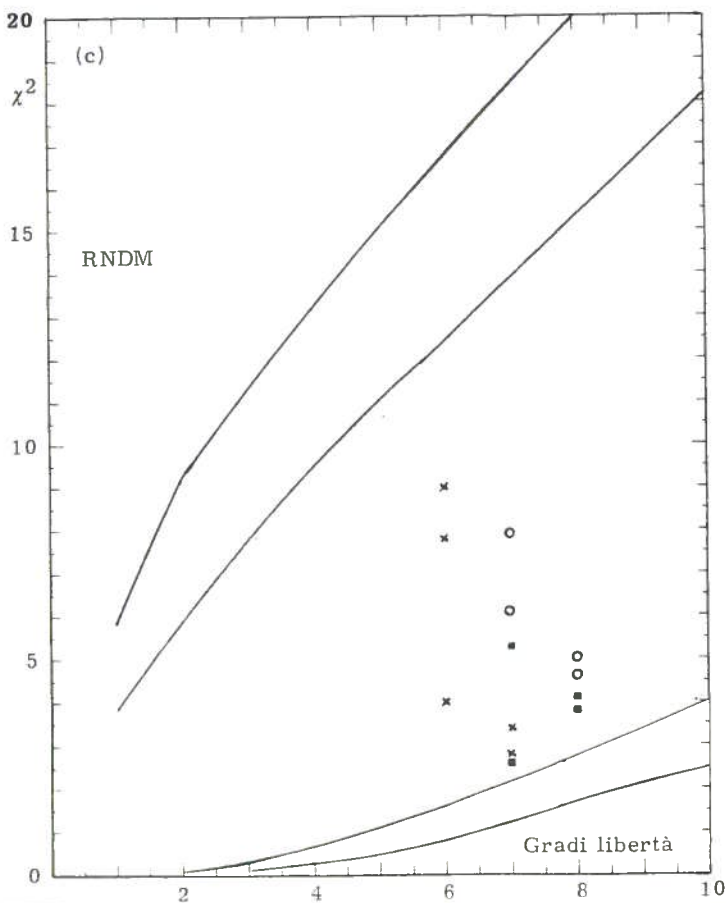
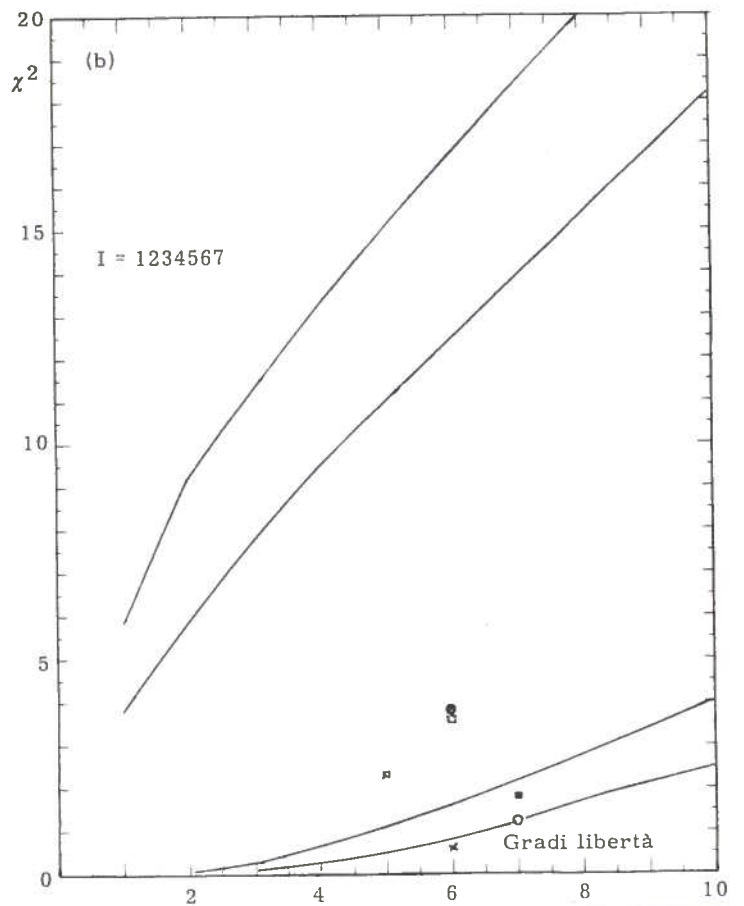
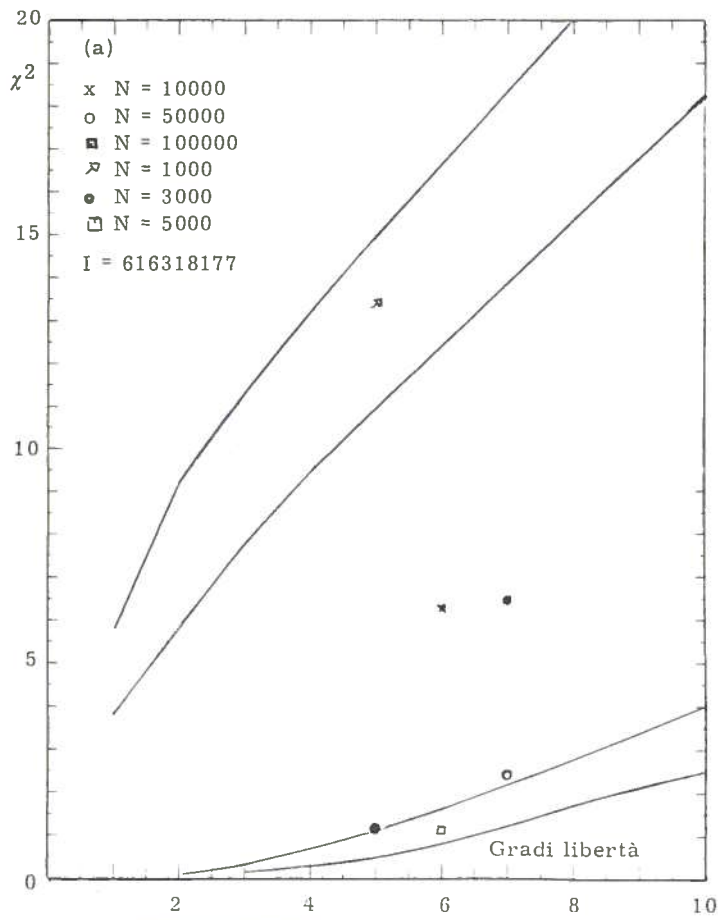


FIG. 4 - Esito del test di monotonicit  per RAN, inizializzatori A e D (fig. (a), (b)), e per RNDM e RNDM2 (fig. (c), (d)).

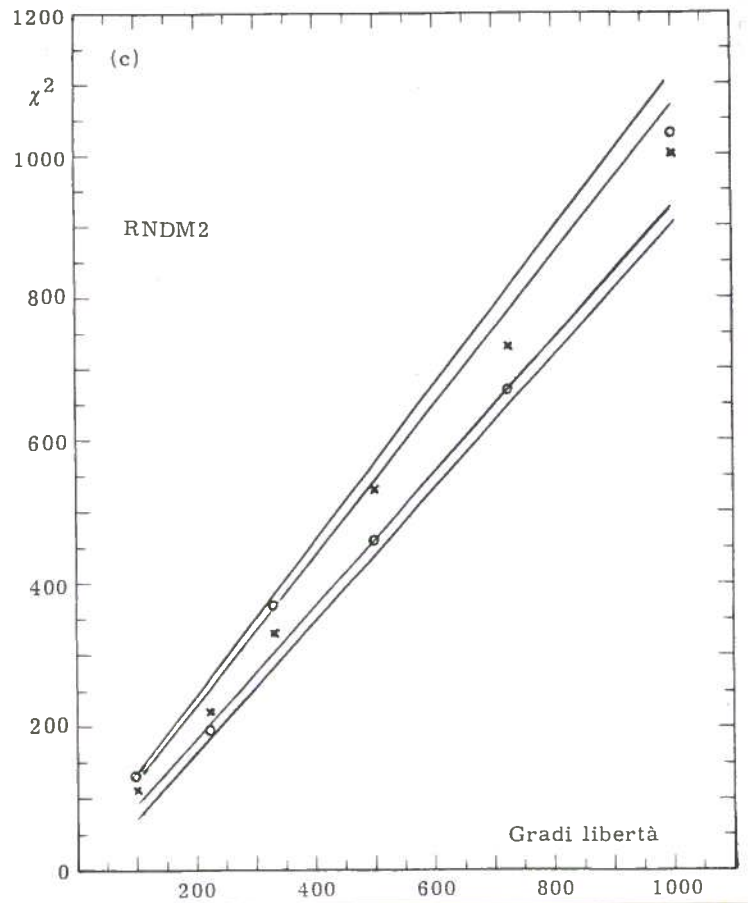
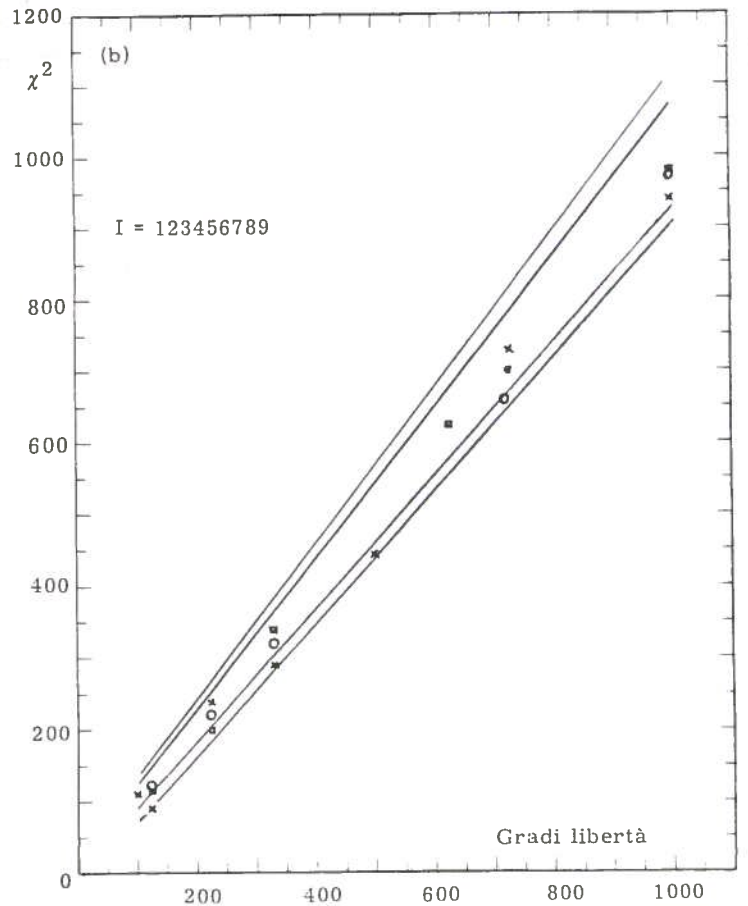
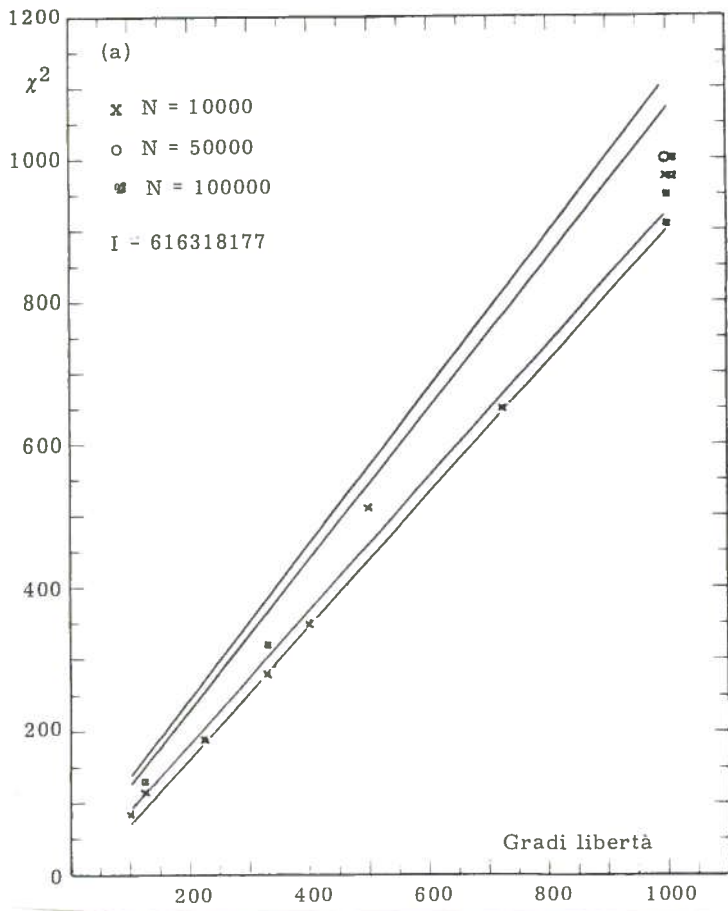


FIG. 5 - Esito del test del χ^2 multi dimensionale e globale per RAN, in_izializzatori A e C (fig. (a), (b)), e per RNDM2 (fig. (c)).

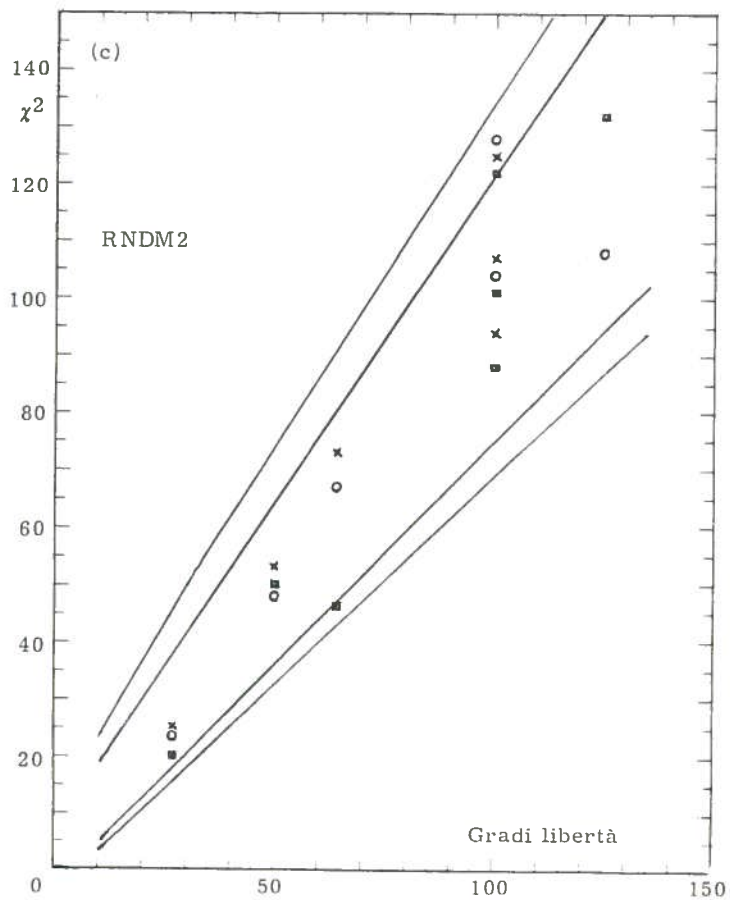
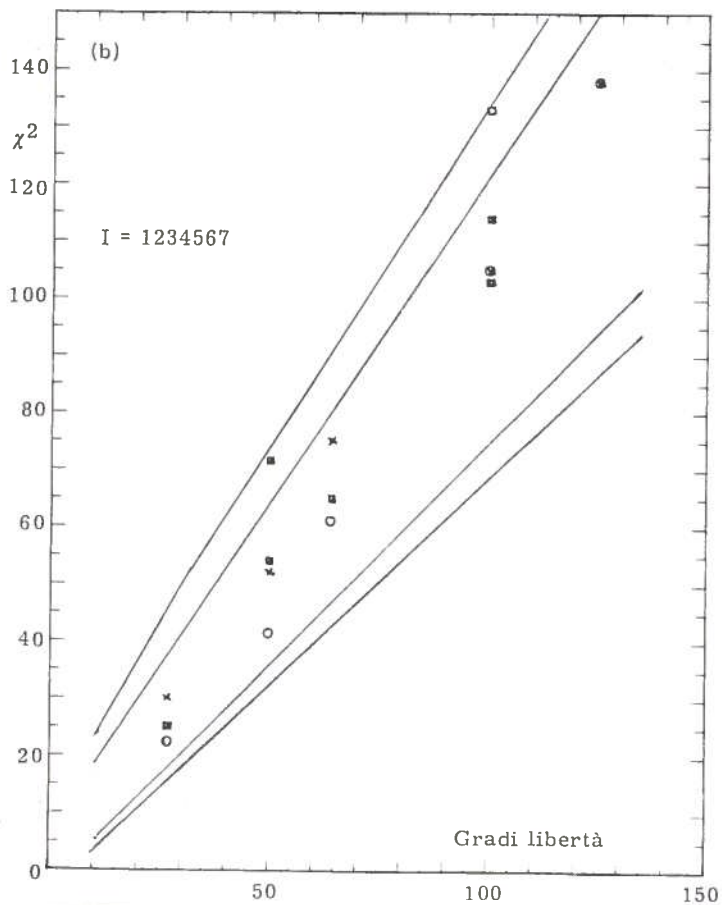
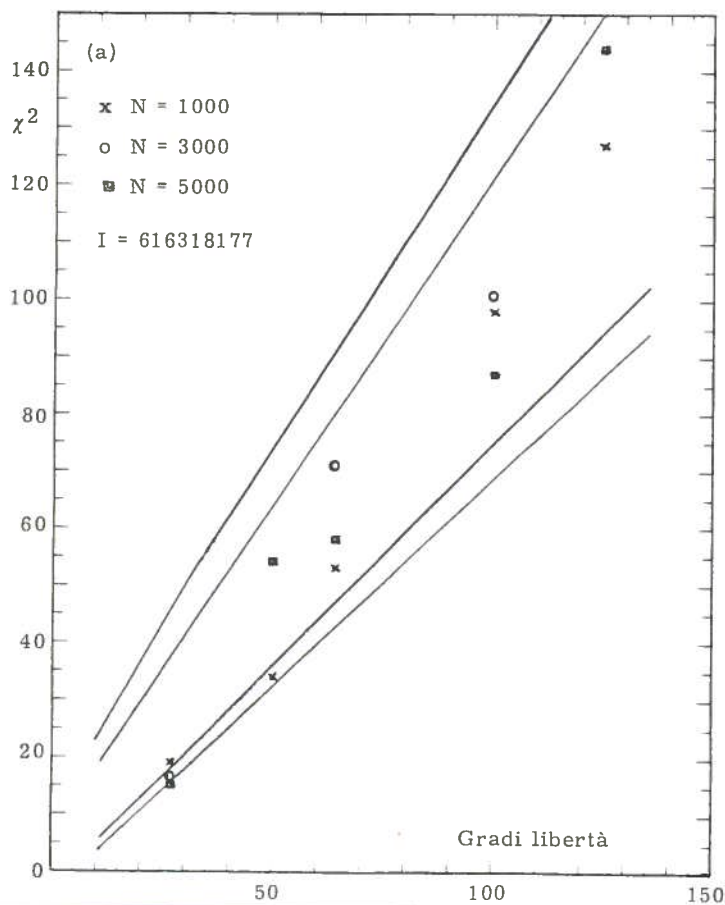


FIG. 6 - Esito del test del χ^2 multi dimensionale locale per RAN, iniziizzatori A e D (fig. (a), (b)), e per RNDM2 (fig. (c)).

Pur indicando anomalie, i test per l'analisi locale danno risultati migliori di quelli ottenuti nel caso analogo unidimensionale: i valori di χ^2 sono distribuiti entro i livelli di confidenza dell'1%. Al contrario, per l'analisi globale si ottengono χ^2 troppo bassi.

I risultati ottenuti per i generatori RNDM e RNDM2 sono poco migliori di quelli di RAN (cfr. Fig. 6).

7.2. - Metodo di reiezione

In una prima versione del test si è semplicemente ristretta l'area esaminata nella precedente analisi bidimensionale, selezionando i punti compresi all'interno di un cerchio di raggio unitario.

La procedura di reiezione consiste nel prelevare dalla sequenza principale coppie (x, y) e nell'eliminare quelle coppie per cui vale la $x^2 + y^2 > 1$.

Mantenendo il tipo di scansione a celle già descritto più sopra si sono ottenute distribuzioni numeriche unidimensionali sezionando il cerchio lungo diametri perpendicolari. Per ogni punto si è inoltre calcolata la coordinata polare angolare θ riferita ad un sistema di coordinate con origine nel centro del cerchio.

Alle tre distribuzioni, che la teoria prevede uniformi, è stato applicato il test del χ^2 unidimensionale. Si è poi determinato, per i punti prodotti, il rapporto di reiezione

$$R = \text{punti selezionati} / \text{punti estratti}.$$

I risultati sono riportati in Tabella VIII. Le uniche anomalie rilevate corrispondono al caso $N = 5000$: i valori del χ^2 per le due sezioni sono troppo bassi (rispettivamente oltre il limite di confidenza del 5% e dell'1%).

In tutti i casi, sia per RAN che per RNDM2, i rapporti di reiezione sono molto prossimi a quelli teorici.

Una seconda versione del test è stata realizzata impiegando un'altra tecnica di reiezione. Le coppie (x, y) sono ancora selezionate all'interno di un cerchio di raggio unitario. Dopo che una coppia è stata generata viene estratto un'altro elemento della sequenza principale: si ottiene così una terna (x, y, z) corrispondente ad un punto in uno spazio tridimensionale. Se vale l'espressione $x^2 + y^2 + z^2 \leq 1$ il punto viene accettato, altrimenti si estraggono in successione altri z , finché la condizione non risulta soddisfatta (si selezionano cioè i punti all'interno di una sfera di raggio unitario).

L'analisi del χ^2 viene effettuata, come nella prima versione, sulle coppie (x, y) . La differenza rispetto al caso precedente risiede solo nel diverso metodo di campiona

mento della sequenza principale. I risultati sono riportati in Tabella VIII. Nessuna anomalia viene rilevata.

TABELLA VIII - Test di reiezione: i primi due gruppi di dati si riferiscono alla prima versione del metodo di reiezione; il terzo gruppo (relativo solo a RAN) alla seconda versione. I valori di χ^2 segnati con asterisco sono al di fuori dei limiti di confidenza.

I	N	R	CHIQ.Y	CHIQ.X	CHIQ.THETA
TEST REIEZIONE VERSIONE 1 GENERATORE RAN					
123456789	1000	0.795	13.17	8.60	47.76
	5000	0.780	*2.49*	*3.37*	45.74
	50000	0.783	7.72	8.313	42.736
616318177	1000	0.785	12.01	7.16	48.2
	4000	0.793	6.69	7.32	48.65
	50000	0.786	7.798	19.587	54.382
TEST REIEZIONE VERSIONE 1 GENERATORE RNDM (CERNLIB)					
	1000	0.799	13.75	8.875	*78.2*
	5000	0.767	9.28	*22.112*	49.88
	10000	0.783	9.999	13.91	*68.57*
	50000	0.788	10.475	17.825	54.78
TEST REIEZIONE VERSIONE 2 GENERATORE RAN					
123456789	1000	0.409	4.364	14.06	44.4
	5000	0.433	15.13	6.00	53.32
	10000	0.435	11.632	9.433	58.18
616318177	1000	0.446	8.000	3.869	48.2
	5000	0.438	7.066	3.016	34.4
	10000	0.440	10.698	2.896	40.75
1234567	1000	0.434	7.000	10.846	59.00
	5000	0.437	16.54	17.61	50.8
	10000	0.440	12.03	15.04	45.94

8. - CONCLUSIONI

I test effettuati indicano che, dal punto di vista della "casualità" in senso strettamente teorico, le sequenze numeriche prodotte da RAN sono poco soddisfacenti.

I test del χ^2 e di Kolmogorov-Smirnov rivelano che le distribuzioni di valori ottenute sono localmente troppo regolari (χ^2 , K^+ , K^- al di sotto dei limiti di confidenza).

RAN va quindi usato con prudenza in applicazioni particolarmente delicate, soprattutto quando il numero di estrazioni casuali richiesto sia basso.

Il confronto con un generatore "buono" come RNDM2 della libreria CERNLIB mostra comunque come quest'ultimo riveli caratteristiche di poco migliori.

Restringendo l'analisi al settore delle applicazioni pratiche più frequenti nel campo della fisica, quali le simulazioni e i calcoli basati sul metodo di Montecarlo, il rendimento di RAN si può comunque considerare sufficientemente affidabile: i risultati dei test di generazione di punti, assieme agli esiti del test di correlazione non

evidenziano anomalie gravi nelle distribuzioni ottenute.

Va sottolineato il fatto che, agli effetti di questo tipo di applicazioni, l'eccessiva uniformità delle distribuzioni numeriche, cui si è accennato più sopra (riscontrata in parte anche nei test multidimensionali) è comunque da ritenersi meno dannosa della tendenza opposta. La "casualità" nel senso stretto del termine riveste in tali casi un'importanza relativa se confrontata con il requisito di omogeneità di scansione dello spazio in cui i punti vengono generati.

BIBLIOGRAFIA

- (1) - D. E. Knuth, The Art of Computer Programming (Addison Wesley, 1971), Vol. 2.
- (2) - C. J. Everett, Number theory of the congruential random number generators, In formal report Los Alamos, University of California LA-6667-MS (1977).
- (3) - CERN Library Short Write Up.
- (4) - DECUS Program Library, A pseudo random number generator for the PDP-8 use with FOCAL, FOCAL8-1.
- (5) - H. Borgwaldt and V. Brandl, Evidence of significant bias in an elementary random number generator, Kernforschungszentrum Karlsruhe, report KfK-3107 (1981).