$$
\begin{aligned}
87 \bmod 2^4 + 1 &= 2 \\
87 \bmod 2^5 - 1 &= 25 \\
87 \bmod 2^5 + 1 &= 21 \\
87 \bmod 2^6 - 1 &= 24 \\
87 \bmod 2^6 + 1 &= 22
\end{aligned}
$$

Παρατηρείστε ότι δεν είναι δυνατόν να λάβουμε το υπόλοιπο της διαίρεσης χρησιμοποιώντας τα ν τελευταία bits. Για παράδειγμα, το υπόλοιπο της διαίρεσης 87:31 είναι ίσο με 25, αλλά τα 5 τελευταία bits του αριθμού 87 σχηματίζουν τον αριθμό 23. Αυτό σημαίνει ότι, τα ν δεξιότερα bits συμπεριφέρονται το ίδιο τυχαία με τα αριστερότερα bits του αριθμού Z_n. Επομένως, η χρήση των τιμών $2^n \pm 1$, για κάποια ακέραια τιμή του ν, είναι καλύτερη επιλογή, με την προϋπόθεση οι υπολογισμοί να εκτελούνται γρήγορα. Το ζήτημα της γρήγορης εκτέλεσης των υπολογισμών, δεν είναι αντικείμενο αυτού του βιβλίου. Ένας αναγνώστης που ενδιαφέρεται για αυτό το ζήτημα, μπορεί να ανατρέξει στην αναφορά Knuth (1998).

Επιλογή του Ακεραίου Υπολοίπου Η επίτευξη της μέγιστης περιόδου σχετίζεται τόσο από την επιλογή του υπολοίπου, όσο και από την επιλογή του πολλαπλασιαστή. Γενικά, μία μεγάλη περίοδος είναι χρήσιμη, όταν αναφερόμαστε σε ακολουθίες τυχαίων αριθμών. Πρέπει όμως να γίνει κατανοητό, ότι η μεγάλη περίοδος είναι ένα μόνον επιθυμητό χαρακτηριστικό. Για παράδειγμα, υπάρχουν ακολουθίες αριθμών οι οποίες έχουν τη μέγιστη περίοδο m, αλλά δεν είναι δυνατόν να χαρακτηριστούν τυχαίες. Χαρακτηριστικό παράδειγμα είναι η ακολουθία που προκύπτει αν $a = c = 1$, δηλαδή $Z_{n+1} = Z_n \bmod m$.

Στα βιβλία Law and Kelton (2000), Knuth (1998), παρουσιάζονται ορισμένες προτάσεις για τις τιμές του πολλαπλασιαστή a και της προσαύξησης c, ώστε να μεγιστοποιείται η περίοδος, αν η τιμή του m είναι ίση με 2^ν. Ειδικότερα,

Πρόταση 6.1: Αν $m = 2^\nu$ και $c \neq 0$, η μέγιστη περίοδος, έστω P, είναι $m = 2^\nu$, και εμφανίζεται οποτεδήποτε οι αριθμοί c, m είναι σχετικά πρώτοι (δηλαδή ο μέγιστος κοινός διαιρέτης τους είναι 1) και $a = 1 + 4k$, όπου k είναι ένας ακέραιος αριθμός.

Πρόταση 6.2: Αν $m = 2^\nu$ και $c = 0$, η μέγιστη περίοδος P είναι $m/4 = 2^{\nu-2}$, και εμφανίζεται οποτεδήποτε ο σπόρος Z_0 είναι περιτός και ο πολλαπλασιαστής a δίνεται από τη σχέση $a = 3 + 8k$, ή $a = 5 + 8k$, για κάποια ακέραια τιμή του k.

Ακολουθούν δύο παραδείγματα για την κατανόηση των παραπάνω προτάσεων:

ΠΑΡΑΔΕΙΓΜΑ 6.2

Αν $m = 16, c = 5$, και $a = 9$, να βρεθεί η περίοδος της γεννήτριας αν ο σπόρος $Z_0 = 21$. Να δώσετε όλες τις τιμές που εμφανίζονται σε μία περίοδο.

Λύση

Είναι $m = 2^4 = 16$ και $c = 5 \neq 0$. Επίσης, οι αριθμοί c, m είναι σχετικά πρώτοι (ο μέγιστος κοινός διαιρέτης τους είναι 1) και ο πολλαπλασιαστής a έχει τη μορφή $a = 1+4k$. Πράγματι, για $k = 2$, $a = 1+4\times 2 = 9$. Επομένως, ισχύουν όλες οι συνθήκες της Πρότασης 6.1 και η περίοδος είναι η μέγιστη δυνατή, δηλαδή $P = m = 2^4 = 16$. Ο πίνακας που ακολουθεί δίνει τις τιμές που εμφανίζονται μέσα στην περίοδο.

$Z_0 = 21$	$(aZ_0 + c) = 194$	$Z_1 = 194 \bmod 16 = 2$
$Z_1 = 2$	$(aZ_1 + c) = 23$	$Z_2 = 23 \bmod 16 = 7$
$Z_2 = 7$	$(aZ_2 + c) = 68$	$Z_3 = 68 \bmod 16 = 4$
$Z_3 = 4$	$(aZ_3 + c) = 41$	$Z_4 = 41 \bmod 16 = 9$
$Z_4 = 9$	$(aZ_4 + c) = 86$	$Z_5 = 86 \bmod 16 = 6$
$Z_5 = 6$	$(aZ_5 + c) = 59$	$Z_6 = 59 \bmod 16 = 11$
$Z_6 = 11$	$(aZ_6 + c) = 104$	$Z_7 = 104 \bmod 16 = 8$
$Z_7 = 8$	$(aZ_7 + c) = 77$	$Z_8 = 77 \bmod 16 = 13$
$Z_8 = 13$	$(aZ_8 + c) = 122$	$Z_9 = 122 \bmod 16 = 10$
$Z_9 = 10$	$(aZ_9 + c) = 95$	$Z_{10} = 95 \bmod 16 = 15$
$Z_{10} = 15$	$(aZ_{10} + c) = 140$	$Z_{11} = 140 \bmod 16 = 12$
$Z_{11} = 12$	$(aZ_{11} + c) = 113$	$Z_{12} = 113 \bmod 16 = 1$
$Z_{12} = 1$	$(aZ_{12} + c) = 14$	$Z_{13} = 14 \bmod 16 = 14$
$Z_{13} = 14$	$(aZ_{13} + c) = 131$	$Z_{14} = 131 \bmod 16 = 3$
$Z_{14} = 3$	$(aZ_{14} + c) = 32$	$Z_{15} = 32 \bmod 16 = 0$
$Z_{15} = 0$	$(aZ_{15} + c) = 5$	$Z_{16} = 5 \bmod 16 = 5$
$Z_{16} = 5$	$(aZ_{16} + c) = 50$	$Z_{17} = 50 \bmod 16 = 2$
$Z_{17} = 2$	$(aZ_{17} + c) = 23$	$Z_{18} = 23 \bmod 16 = 7$
$Z_{18} = 7$	$(aZ_{18} + c) = 68$	$Z_{19} = 68 \bmod 16 = 4$
$\vdots$	$\vdots$	$\vdots$

Από τον παραπάνω πίνακα, είναι προφανές ότι οι τιμές των τυχαίων αριθμών μέσα στην περίοδο είναι: 2, 7, 4, 9, 6, 11, 8, 13, 10, 15, 12, 1, 14, 3, 0, 5, 2, 7, 4,...κ.ο.κ.

ΠΑΡΑΔΕΙΓΜΑ 6.3

Αν $m = 16, c = 0$, και $a = 11$, να βρεθεί η περίοδος της γεννήτριας αν ο σπόρος $Z_0 = 21$. Να δώσετε όλες τις τιμές που εμφανίζονται σε μία περίοδο.

Λύση
Είναι $m = 2^4 = 16$ και $c = 0$. Επίσης, ο αριθμός Z_0 είναι περιττός και ο πολλαπλασιαστής a έχει τη μορφή $a = 3 + 8k$. Πράγματι, για $k = 1$, $a = 3 + 8 \times 1 = 11$. Επομένως, ισχύουν όλες οι συνθήκες της Πρότασης 6.2 και η περίοδος είναι η μέγιστη δυνατή, δηλαδή $P = m/4 = 2^{4-2} = 4$. Ο πίνακας που ακολουθεί δίνει τις τιμές που εμφανίζονται μέσα στην περίοδο.

$Z_0 = 21$	$(aZ_0 + c) = 231$	$Z_1 = 231 \bmod 16 = 7$
$Z_1 = 7$	$(aZ_1 + c) = 77$	$Z_2 = 77 \bmod 16 = 13$
$Z_2 = 13$	$(aZ_2 + c) = 143$	$Z_3 = 143 \bmod 16 = 15$
$Z_3 = 15$	$(aZ_3 + c) = 165$	$Z_4 = 165 \bmod 16 = 5$
$Z_4 = 5$	$(aZ_4 + c) = 55$	$Z_5 = 55 \bmod 16 = 7$
$Z_5 = 7$	$(aZ_5 + c) = 77$	$Z_6 = 77 \bmod 16 = 13$
$Z_6 = 13$	$(aZ_6 + c) = 143$	$Z_7 = 143 \bmod 16 = 15$
$Z_7 = 15$	$(aZ_7 + c) = 165$	$Z_8 = 165 \bmod 16 = 5$
$Z_8 = 5$	$(aZ_8 + c) = 55$	$Z_9 = 55 \bmod 16 = 7$
$\vdots$	$\vdots$	$\vdots$

Από τον παραπάνω πίνακα, είναι προφανές ότι οι τιμές των τυχαίων αριθμών μέσα στην περίοδο είναι: 7, 13, 15, 5, 7, 13, 15, 5, ...κ.ο.κ.

Στο βιβλίο Law and Kelton (2000), παρουσιάζεται και μία πρόταση που αφορά τη μεγιστοποίηση της περιόδου, για μία ειδική περίπτωση, όπου ο αριθμός m είναι πρώτος. Ειδικότερα,

Πρόταση 6.3: Όταν ο αριθμός m είναι πρώτος (δεν αναλύεται σε γινόμενο ακεραίων παραγόντων οι οποίοι να είναι στο σύνολό τους διαφορετικοί από το 1), τότε, για $c = 0$, η μέγιστη περίοδος είναι $P = m - 1$ και εμφανίζεται όταν:

α. Ο πολλαπλασιαστής a είναι της μορφής $a^k - 1$, k ακέραιος.

β. Η μικρότερη τιμή του k, τέτοια ώστε ο πολλαπλασιαστής a να διαιρείται από το υπόλοιπο m, είναι $k = m - 1$.

Θα δείξουμε την παραπάνω πρόταση με δύο παραδείγματα.

ΠΑΡΑΔΕΙΓΜΑ 6.4
Αν $m = 11, c = 0$, και $a = 2$, να βρεθεί η περίοδος της γεννήτριας αν ο σπόρος $Z_0 = 24$. Να δώσετε όλες τις τιμές που εμφανίζονται σε μία περίοδο.

Λύση

Το υπόλοιπο $m = 11$ είναι πρώτος αριθμός και $c = 0$. Επίσης, αν γράψουμε όλες τις δυνάμεις του 2, τότε η μικρότερη δύναμη k για την οποία $2^k - 1 \bmod m = 0$ είναι $k = 10$. Πράγματι, $2^{10} - 1 = 1023$ και $1023 \bmod 11 = 0$. Άρα, ικανοποιούνται οι συνθήκες της πρότασης 6.3 και η περίοδος είναι η μέγιστη δυνατή, δηλαδή $P = m - 1 = 10$. Ο πίνακας που ακολουθεί δίνει τις τιμές που εμφανίζονται μέσα στην περίοδο.

$Z_0 = 24$	$(aZ_0 + c) = 48$	$Z_1 = 48 \bmod 11 = 4$
$Z_1 = 4$	$(aZ_1 + c) = 8$	$Z_2 = 8 \bmod 11 = 8$
$Z_2 = 8$	$(aZ_2 + c) = 16$	$Z_3 = 16 \bmod 11 = 5$
$Z_3 = 5$	$(aZ_3 + c) = 10$	$Z_4 = 10 \bmod 11 = 10$
$Z_4 = 10$	$(aZ_4 + c) = 20$	$Z_5 = 20 \bmod 11 = 9$
$Z_5 = 9$	$(aZ_5 + c) = 18$	$Z_6 = 18 \bmod 11 = 7$
$Z_6 = 7$	$(aZ_6 + c) = 14$	$Z_7 = 14 \bmod 11 = 3$
$Z_7 = 3$	$(aZ_7 + c) = 6$	$Z_8 = 6 \bmod 11 = 6$
$Z_8 = 6$	$(aZ_8 + c) = 12$	$Z_9 = 12 \bmod 11 = 1$
$Z_8 = 1$	$(aZ_8 + c) = 2$	$Z_9 = 2 \bmod 11 = 2$
$Z_8 = 2$	$(aZ_8 + c) = 4$	$Z_9 = 4 \bmod 11 = 4$
$Z_8 = 4$	$(aZ_8 + c) = 8$	$Z_9 = 8 \bmod 11 = 8$
$Z_8 = 8$	$(aZ_8 + c) = 16$	$Z_9 = 16 \bmod 11 = 5$
⋮	⋮	⋮

Από τον παραπάνω πίνακα, είναι προφανές ότι οι τιμές των τυχαίων αριθμών μέσα στην περίοδο είναι: 4, 8, 5, 10, 9, 7, 3, 6, 1, 2, 4, 8, 5, ...κ.ο.κ.

Στο επόμενο παράδειγμα, το υπόλοιπο είναι της μορφής $2^\nu - 1$, είναι πρώτος αριθμός, και επαληθεύεται η Πρόταση 6.3.

ΠΑΡΑΔΕΙΓΜΑ 6.5

Αν $m = 7, c = 0$, και $a = 5$, να βρεθεί η περίοδος της γεννήτριας αν ο σπόρος $Z_0 = 19$. Να δώσετε όλες τις τιμές που εμφανίζονται σε μία περίοδο.

Λύση

Το υπόλοιπο $m = 7$ είναι πρώτος αριθμός και $c = 0$. Επίσης, αν γράψουμε όλες τις δυνάμεις του 5, τότε η μικρότερη δύναμη k για την οποία $2^k - 1 \bmod m = 0$ είναι $k = 6$. Πράγματι, $5^6 - 1 = 15,624$ και $15,624 \bmod 7 = 0$. Άρα, ικανοποιούνται οι συνθήκες της πρότασης 6.3 και η περίοδος είναι η μέγιστη δυνατή, δηλαδή $P = m - 1 = 6$. Ο πίνακας που ακολουθεί δίνει τις τιμές που εμφανίζονται μέσα στην περίοδο.

$Z_0 = 19$	$(aZ_0 + c) = 95$	$Z_1 = 95 \bmod 7 = 4$
$Z_1 = 4$	$(aZ_1 + c) = 20$	$Z_2 = 20 \bmod 7 = 6$
$Z_2 = 6$	$(aZ_2 + c) = 30$	$Z_3 = 30 \bmod 7 = 2$
$Z_3 = 2$	$(aZ_3 + c) = 10$	$Z_4 = 10 \bmod 7 = 3$
$Z_4 = 3$	$(aZ_4 + c) = 15$	$Z_5 = 15 \bmod 7 = 1$
$Z_5 = 1$	$(aZ_5 + c) = 5$	$Z_6 = 5 \bmod 7 = 5$
$Z_6 = 5$	$(aZ_6 + c) = 25$	$Z_7 = 25 \bmod 7 = 4$
$Z_7 = 4$	$(aZ_7 + c) = 20$	$Z_8 = 20 \bmod 7 = 6$
$\vdots$	$\vdots$	$\vdots$

Από τον παραπάνω πίνακα, είναι προφανές ότι οι τιμές των τυχαίων αριθμών μέσα στην περίοδο είναι: 4, 6, 2, 3, 1, 5, 4, 6, ...κ.ο.κ.

Μία σημαντική παρατήρηση, σχετίζεται με την επιλογή του σπόρου Z_0. Η μη προσεκτική επιλογή μπορεί να έχει μη αναμενόμενες επιπτώσεις. Για παράδειγμα, η γεννήτρια του Παραδείγματος 6.5 έχει καλή τιμή υπολοίπου $m = 2^3 - 1 = 7$, η τιμή του πολλαπλασιαστή $a = 5$ σε συνδυασμό με την τιμή υπολοίπου δίνουν στη γεννήτρια τη μέγιστη περίοδο $m = 6$, αλλά αν ο σπόρος έχει τιμή $Z_0 = 21$ η γεννήτρια θα παράγει συνεχώς αποτέλεσμα ίσο με 0!!!!

Όταν ο νέος αριθμός υπολογίζεται διαιρώντας με το m, οι τιμές του κατανέμονται στο διάστημα [0,1). Ο μεγαλύτερος τυχαίος αριθμός που προκύπτει σ' αυτή την περίπτωση είναι $(m-1)/m$, ενώ η διακριτότητα είναι $1/m$. Αν είναι απαραίτητο να περιλαμβάνεται και η τιμή 1 στους τυχαίους αριθμούς, η διαίρεση θα πρέπει να γίνει με το $m - 1$.

Αρκετοί ερευνητές έχουν μελετήσει τις γραμμικές ισοϋπόλοιπες γεννήτριες για να καθορίσουν ικανοποιητικές τιμές των παραμέτρων. Σε υπολογιστές που χρησιμοποιούν λέξεις των 32 bits, η γεννήτρια:

$$Z_{i+1} = (314.159.269 Z_i + 453,806,245) \bmod 2^{11} \tag{6.14}$$

δίνει πολύ καλά αποτελέσματα. Στη γεννήτρια αυτή η παράμετρος a είναι ίση με τα 9 σημαντικά ψηφία του αριθμού π.

Σε υπολογιστές με λέξεις των 36 bits χρησιμοποιόταν η γεννήτρια:

$$Z_{i+1} = (5^{15} Z_i + 1) \bmod 2^{35}$$

Κλείνοντας την παράγραφο αυτή, παραθέτουμε ένα ακόμη παράδειγμα τονίζοντας μερικά από τα χαρακτηριστικά των γραμμικών ισοϋπόλοιπων γεννητριών που παρουσιάστηκαν.

Η γεννήτρια αυτή επιστρέφει τις τιμές R_i

$$R_{i+1} = \begin{cases} \dfrac{Z_{i+1}}{2,147,483,563}, Z_{i+1} > 0 \\ \dfrac{2,147,483,562}{2,147,483,563}, Z_{i+1} = 0 \end{cases}$$

Η συνδυαστική αυτή γεννήτρια έχει περίοδο ίση με

$$P = \frac{(m_1 - 1)(m_2 - 1)}{2} = \frac{2,147,483,562 \times 2,147,483,398}{2} \approx 2^{61} \approx 2 \times 10^{18}$$

Ακόμη και γεννήτριες με τόσο υψηλή περίοδο πιθανόν να μην αρκούν. Μετά από εκτεταμένη μελέτη, ο L'Ecuyer [L'Ecuyer (1999)], κατέληξε στο συνδυασμό των γεννητριών

$$\begin{aligned} X_{i+1} &= 1,403,580X_{1,i-1} - 810,782X_{1,i-2} \ [\text{mod} 2^{32} - 209] \\ U_{i+1} &= 527,612Y_i - 1,370,589Y_{2,i-2} \ [\text{mod} 2^{32} - 22,853] \end{aligned}$$

ώστε να σχηματιστεί η γεννήτρια

$$Z_{i+1} = (Z_{1,i+1} - Z_{2,i+1}) \ [\text{mod} 2^{32} - 209] \tag{6.23}$$

Η γεννήτρια αυτή επιστρέφει τις τιμές R_i

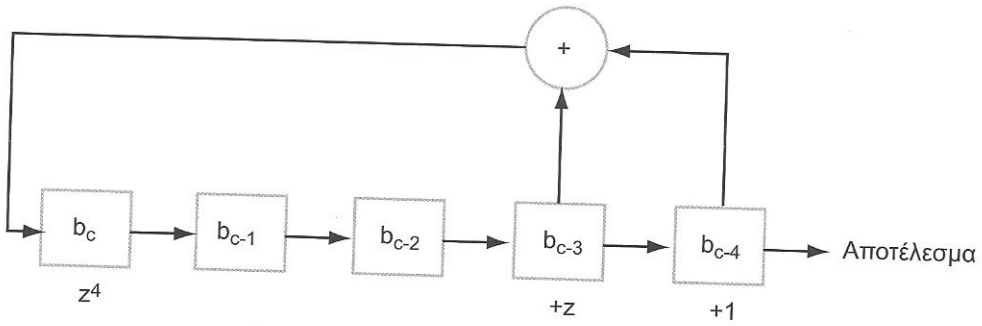
$$R_{i+1} = \frac{Z_{i+1}}{2^{32} - 209}$$

και έχει περίοδο $2^{191} = 3.1 \times 10^{57}$. Ουσιαστικά, η γεννήτρια αυτή μπορεί να χαρακτηριστεί ως **συνδυαστική γεννήτρια αθροιστικών ισοϋπόλοιπων γεννητριών**.

6.4.5 ΓΕΝΝΗΤΡΙΕΣ TAUSWORTHE

Οι γεννήτριες αυτές επεξεργάζονται κάθε bit του τυχαίου αριθμού ξεχωριστά. Για τον λόγο αυτό, είναι ουσιαστικά ανεξάρτητες από τον υπολογιστή στον οποίο χρησιμοποιούνται. Με τις γεννήτριες αυτές επιτυγχάνονται ασύλληπτα μεγάλες περίοδοι (όπως $2^{521} > 10^{156}$ και περισσότερο) ακόμα και σε υπολογιστές με λέξεις των 16 bits. Παράδειγμα γεννήτριας Tausworthe με περίοδο $2^9 - 1$ είναι η εξής:

$$b_i \equiv (c_1 b_{i-1} + c_2 b_{i-2} + .. + c_9 b_{i-9}) \bmod 2 \tag{6.24}$$



Σχήμα 6.6: Καταχωρητής που αντιστοιχεί στο πολυώνυμο $f(Z) = Z^4 + Z + 1$

Στις περισσότερες εφαρμογές των γεννητριών Tausworthe, μόνον δύο από τους συντελεστές c_i της Εξίσωσης (6.24) είναι μη μηδενικοί (ίσοι με τη μονάδα), με αποτέλεσμα η σχέση αυτή να γράφεται:

$$b_i \equiv (b_{i-r} + b_{i-q}) \bmod 2 \tag{6.25}$$

όπου r και q ακέραιοι τέτοιοι ώστε $0 < r < q$. Η Εξίσωση (6.25) είναι μία πρόσθεση modulo 2, η οποία ισοδυναμεί με τη λογική πράξη Αποκλειστικό Ή (συμβολικά, $\bigoplus$) ανάμεσα στα δύο bits. Επομένως, η (6.25) είναι ισοδύναμη με την

$$b_i = \begin{cases} 0, \text{αν } b_{i-r} = b_{i-q} \\ 1, \text{αν } b_{i-r} \neq b_{i-q} \end{cases} \tag{6.26}$$

Επειδή η ακολουθία $b_{i-1}, b_{i-2}, ..., b_{i-q}$ μπορεί να περάσει από 2^q καταστάσεις (διαφορετικούς συνδυασμούς τιμών μεταξύ των διαφόρων b_i), η μέγιστη περίοδός της είναι ίση με 2^q. Ας σημειθεί ότι η κατάσταση $b_{i-1}, b_{i-2}, ..., b_{i-q} = 0, 0, ..., 0$ οδηγεί σε μία ακολουθία των b_i η οποία δεν θα αλλάξει ποτέ (επειδή $0 \bigoplus 0 = 0$). Για την (6.24), μπορούμε να ορίσουμε ένα χαρακτηριστικό πολυώνυμο, το οποίο έχει τη μορφή

$$Z^q + b_{i-1}Z^{q-1} + b_{i-2}Z^{q-2} + ... + b_{i-q}Z^1 + 1 \tag{6.27}$$

Το πολυώνυμο αυτό ορίζει έναν **καταχωρητή ολίσθησης με ανατροφοδότηση** (Feedback Shift Register). Πρόκειται για μία παράταξη από bits, που ολισθαίνουν προς τα δεξιά κατά ένα πλήθος θέσεων (συνήθως μία θέση) και το bit b_i λαμβάνεται από την πράξη $\bigoplus$ (πρόσθεση modulo 2) συγκεκριμένων bits. Το Σχήμα 6.6 απεικονίζει έναν καταχωρητή, για $q = 4$ και $r = 3$. Σύμφωνα με την (6.25), η αναδρομή είναι $b_i = b_{i-3} + b_{i-4}$. Όπως φαίνεται από το Σχήμα, το χαρακτηριστικό πολυώνυμο για αυτήν την αναδρομή είναι το $f(Z) = Z^4 + Z + 1$. Για να σχηματίσουμε τυχαίους αριθμούς Z_i, πρέπει να ενώσουμε l bits που παράγονται με αυτόν τον τρόπο. Επίσης, πρέπει να ορίσουμε ως σπόρο μία αρχική

κατάσταση της ακολουθίας των b_i. Τα επόμενα παραδείγματα, δείχνουν τον τρόπο παραγωγής τυχαίων αριθμών.

ΠΑΡΑΔΕΙΓΜΑ 6.7

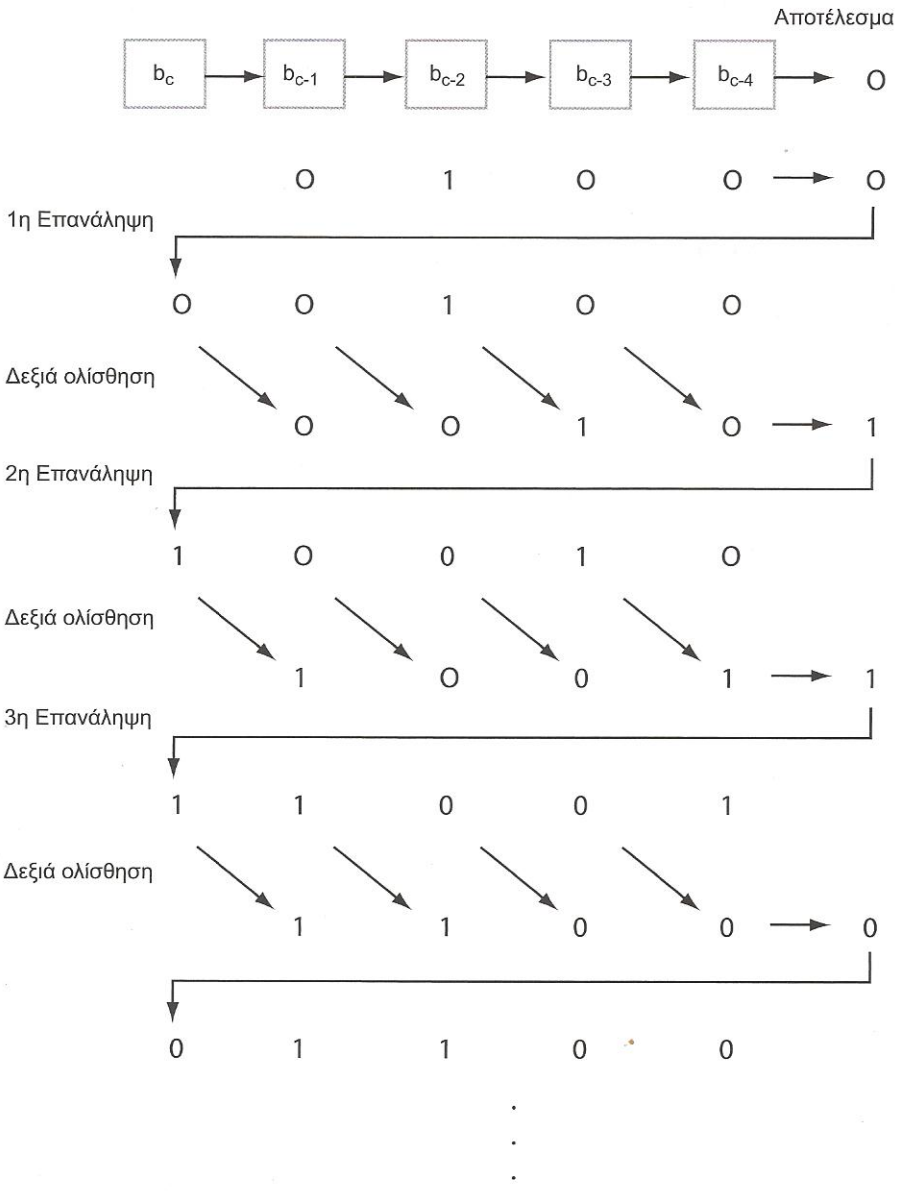
Έστω $r = 3$, και $q = 4$. Να δώσετε τα πρώτα 16 bits που παράγονται από τη γεννήτρια Tausworthe και τους τυχαίους αριθμούς που παράγονται, αν $l = 4$. Η αρχική κατάσταση είναι $b_{i-1}, b_{i-2}, b_{i-3}, b_{i-4} = 0, 1, 0, 0$.

Λύση

Το χαρακτηριστικό πολυώνυμο, όπως αναφέρθηκε και παραπάνω, είναι $f(Z) = Z^4 + Z + 1$. Σε κάθε επανάληψη, γίνεται μία δεξιά ολίσθηση των bits. Το αποτέλεσμα προκύπτει από την πράξη $b_{i-3} \bigoplus b_{i-4}$ και μεταφέρεται στη θέση b_i ώστε να γίνει η νέα ολίσθηση. Σχηματικά, αυτό φαίνεται στο Σχήμα 6.7. Το σχήμα απεικονίζει τις τρεις πρώτες επαναλήψεις. Αρχικά, παράγεται το αποτέλεσμα από τη λογική πράξη $b_3 \bigoplus b_4 = 0 \bigoplus 0 = 0$. Το αποτέλεσμα ανατροφοδοτείται στο bit b_i και στη συνέχεια γίνεται η πρώτη δεξιά ολίσθηση, με την οποία θα προκύψουν οι τιμές $b_{i-1}, b_{i-2}, b_{i-3}, b_{i-4} = 0010$. Αυτή τη φορά, η λογική πράξη $b_3 \bigoplus b_4$ δίνει αποτέλεσμα $1 \bigoplus 0 = 1$. Η τιμή αυτή αποτελεί το αποτέλεσμα της δεύτερης επανάληψης, το οποίο ανατροφοδοτείται στο bit b_i και στη συνέχεια γίνεται η επόμενη δεξιά ολίσθηση με την οποία θα προκύψουν οι τιμές $b_{i-1}, b_{i-2}, b_{i-3}, b_{i-4} = 1001$. Η διαδικασία επαναλαμβάνεται και στα υπόλοιπα βήματα. Ο παρακάτω πίνακας δείχνει τις τιμές των καταστάσεων (τιμές των $b_{i-1}, b_{i-2}, b_{i-3}, b_{i-4}$) και το τελικό αποτέλεσμα.

b_{i-1}	b_{i-2}	b_{i-3}	b_{i-4}	**Αποτέλεσμα**
1	0	0	0	0
0	1	0	0	0
0	0	1	0	1
1	0	0	1	1
1	1	0	0	0
0	1	1	0	1
1	0	1	1	0
0	1	0	1	1
1	0	1	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	0
0	1	1	1	0
0	0	1	1	0
0	0	0	1	1
1	0	0	0	0

Λαμβάνοντας τα bits των αποτελεσμάτων ανά $l = 4$, σχηματίζουμε τις τιμές $(0011)_2 = (3)_{10}$, $(0101)_2 = (5)_{10}$, $(1110)_2 = (13)_{10}$, και $(0011)_2 = (3)_{10}$.



Σχήμα 6.7: Σχηματική αναπαράσταση της παραγωγής τυχαίων bits του Παραδείγματος 6.7

ΠΑΡΑΔΕΙΓΜΑ 6.8

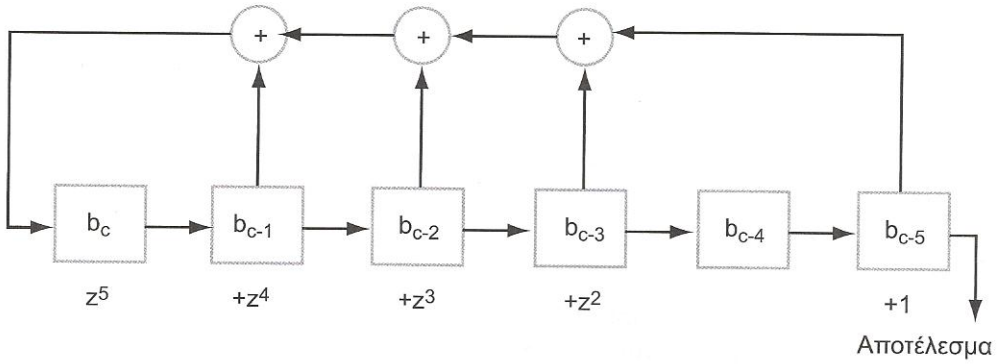
Να δώσετε τα πρώτα 16 bits που παράγονται από τη γεννήτρια Tausworthe και τους τυχαίους αριθμούς που προκύπτουν αν $l = 4$. Η έξοδος παράγεται από την αναδρομή $b_i = b_{i-1} + b_{i-2} + b_{i-3} + b_{i-5}$ (mod) 2 και η αρχική κατάσταση είναι $b_{i-1}, b_{i-2}, b_{i-3}, b_{i-4}, b_{i-5} = 1, 0, 0, 0, 1$. Να δώσετε το πολυώνυμο $f(Z)$ και να σχεδιάσετε τον καταχωρητή ολίσθησης με ανατροφοδότηση.

Λύση

Είναι $q = 5$ και το χαρακτηριστικό πολυώνυμο είναι $f(Z) = Z^5 + Z^4 + Z^3 + Z^2 + 1$. Ο καταχωρητής απεικονίζεται στο Σχήμα 6.8. Ο παρακάτω πίνακας δείχνει τις τιμές των καταστάσεων (τιμές των $b_{i-1}, b_{i-2}, b_{i-3}, b_{i-4}, b_{i-5}$) και τα bits που προκύπτουν ως αποτέλεσμα. Ας σημειωθεί ότι η λογική πράξη $\bigoplus$ για περισσότερα από 2 bits δίνει αποτέλεσμα 1, αν το πλήθος των μονάδων είναι περιττό και 0 αν το πλήθος των μονάδων είναι άρτιο.

b_{i-1}	b_{i-2}	b_{i-3}	b_{i-4}	b_{i-5}	**Αποτέλεσμα**
1	0	0	0	1	0
0	1	0	0	0	1
1	0	1	0	0	0
0	1	0	1	0	1
1	0	1	0	1	1
1	1	0	1	0	0
0	1	1	0	1	1
1	0	1	1	0	0
0	1	0	1	1	0
0	0	1	0	1	0
0	0	0	1	0	0
0	0	0	0	1	1
1	0	0	0	0	1
1	1	0	0	0	0
0	1	1	0	0	0
0	0	1	1	0	1

Π.χ., στην πέμπτη γραμμή, η πράξη $b_i = b_{i-1} \bigoplus b_{i-2} \bigoplus b_{i-3} \bigoplus b_{i-5} = 1 \bigoplus 0 \bigoplus 1 \bigoplus 1 = 1$ γιατί το πλήθος των μονάδων είναι περιττό (3). Ομοίως, στην αμέσως επόμενη (έκτη) γραμμή, είναι $b_i = b_{i-1} \bigoplus b_{i-2} \bigoplus b_{i-3} \bigoplus b_{i-5} = 1 \bigoplus 1 \bigoplus 0 \bigoplus 0 = 0$ γιατί το πλήθος των μονάδων είναι άρτιο (2). Η τιμή του b_{i-4} δεν λαμβάνει μέρος στους υπολογισμούς. Λαμβάνοντας τα bits των αποτελεσμάτων ανά $l = 4$, σχηματίζουμε τις τιμές $(0101)_2 = (5)_{10}$, $(1010)_2 = (10)_{10}$, $(0001)_2 = (1)_{10}$, και $(1001)_2 = (9)_{10}$.



Σχήμα 6.8: Καταχωρητής ολίσθησης με ανατροφοδότηση για το πολυώνυμο $f(Z) = Z^5 + Z^4 + Z^3 + Z^2 + 1$

6.5 ΕΛΕΓΧΟΣ ΤΥΧΑΙΟΤΗΤΑΣ

Οι γεννήτριες τυχαίων αριθμών θα πρέπει να ελέγχονται για να διαπιστωθεί αν παρουσιάζουν τις απαραίτητες ιδιότητες. Ο υπολογισμός του μέσου όρου και της διασποράς των τυχαίων αριθμών δεν αρκούν για να αποδείξουν ότι οι αριθμοί είναι ανεξάρτητοι, ομοιόμορφα και ταυτόσημα κατανεμημένοι στο διάστημα [0,1). Για παράδειγμα, η σειρά των αριθμών:

$$\underbrace{\frac{2.5}{3}, \frac{2.5}{3} \ldots, \frac{2.5}{3}}_{8}, \underbrace{\frac{0.5}{3}, \frac{0.5}{3} \ldots, \frac{0.5}{3}}_{8}$$

έχει ακριβώς το μέσο όρο και τη διασπορά της θεωρητικής κατανομής αλλά οι αριθμοί της σειράς κάθε άλλο παρά τυχαίοι είναι.

Ο στόχος αυτής της παραγράφου είναι να παρουσιάσει στατιστικά μέτρα με τα οποία ελέγχεται η τυχαιότητα μίας ακολουθίας αριθμών. Μέχρι τώρα, παρουσιάστηκαν τρόποι παραγωγής τυχαίων αριθμών, αλλά δεν δόθηκε καμία πραγματικά εγγύηση για το αν αυτοί οι αριθμοί είναι επαρκώς τυχαίοι. Σύμφωνα με τον Knuth, "αν επρόκειτο να δώσουμε σε έναν τυχαία επιλεγμένο άνθρωπο χαρτί και μολύβι και του ζητούσαμε να γράψει 100 τυχαία δεκαδικά ψηφία, οι πιθανότητες να παράγει ικανοποιητικό αποτέλεσμα θα ήταν ελάχιστες. Οι άνθρωποι έχουν την τάση αποφυγής πραγμάτων που μοιάζουν μη τυχαία, όπως για παράδειγμα δύο ίσα διαδοχικά ψηφία (παρά το γεγονός ότι περίπου ένα ανά 10 ψηφία θα πρέπει να ισούται με το προηγούμενό του. Επίσης, αν δείχναμε στον ίδιο άνθρωπο έναν πίνακα με πραγματικά τυχαία ψηφία, είναι πιθανό να μας έλεγε ότι τα ψηφία αυτά δεν είναι καθόλου τυχαία" [Kunth (1998)].

Υπάρχει ένα πολύ μεγάλο πλήθος από ελέγχους οι οποίοι μπορούν να χρησιμοποιηθούν για να ελέγξουμε την τυχαιότητα μίας ακολουθίας αριθμών. Αυτό που πρέπει να γίνει κατανοητό είναι ότι δεν μπορούμε να είμαστε (και στην

πραγματικότητα δεν είμαστε) σίγουροι ότι αν μία ακολουθία περάσει επιτυχώς από ένα σύνολο ελέγχων, ότι δεν θα αποτύχει σε έναν άλλο έλεγχο. Στην ενότητα αυτή θα παρουσιάσουμε τους πιο συνηθισμένους από αυτούς και θα δώσουμε κάποια ενδεικτικά παραδείγματα. Ορισμένοι άλλοι, απλώς θα περιγραφούν σύντομα. Ένας αναγνώστης που ενδιαφέρεται για περισσότερες λεπτομέρειες, μπορεί να ανατρέξει στην προτεινόμενη βιβλιογραφία που βρίσκεται στο τέλος του κεφαλαίου, ενώ και το Διαδίκτυο αποτελεί μία θαυμάσια πηγή πόρων για το συγκεκριμένο ζήτημα.

6.5.1 ΕΛΕΓΧΟΣ ΣΥΧΝΟΤΗΤΑΣ

Ο πρώτος και πιο βασικός ίσως έλεγχος που πρέπει να γίνει σε μία γεννήτρια τυχαίων αριθμών, είναι αν οι αριθμοί που παράγει είναι ομοιόμορφα κατανεμημένοι. Δύο έλεγχοι είναι διαθέσιμοι για το σκοπό αυτό. Ο έλεγχος Kolmogorov-Smirnov και ο έλεγχος x^2. Αμφότεροι μετρούν το βαθμό στον οποίο συμφωνεί η κατανομή του δείγματος των τυχαίων αριθμών με τη θεωρητική ομοιόμορφη κατανομή. Οι υποθέσεις τους είναι οι εξής:

H_0 : Οι αριθμοί R_i είναι ομοιόμορφα κατανεμημένοι στο [0,1]

H_1 : Οι αριθμοί R_i δεν είναι ομοιόμορφα κατανεμημένοι στο [0,1]

όπου $R_i = \frac{Z_i}{m}$. Η H_0 ονομάζεται **μηδενική υπόθεση** και η H_1 **εναλλακτική υπόθεση**.

Στα παραδείγματα που θα ακολουθήσουν σε αυτή την ενότητα, θα χρησιμοποιήσουμε τα αποτελέσματα που έδωσε μία γραμμική ισοϋπόλοιπη γεννήτρια με $m = 128,\ c = 11,\ a = 9$, και $Z_0 = 21$. Ο Πίνακας 6.3 παραθέτει τους 100 πρώτους τυχαίους αριθμούς που παρήγαγε αυτή η γεννήτρια στο διάστημα [0,1].

Έλεγχος Kolmogorov-Smirnov Ο έλεγχος Kolmogorov-Smirnov συγκρίνει τη συνάρτηση κατανομής $F(x) = x,\ 0 \leq x \leq 1$, με μία εμπειρική συνάρτηση $E(x)$, η οποία λαμβάνεται από το δείγμα των N συνολικά παρατηρήσεων, $R_1,\ R_2, R_3, ...R_N$. Η συνάρτηση $E(x)$ ορίζεται ως

$$E(x) = \frac{\text{πλήθος των παρατηρήσεων } R_i \leq x}{N} \tag{6.28}$$

Ο έλεγχος Kolmogorov-Smirnov βασίζεται στον υπολογισμό των ακόλουθων στατιστικών μέτρων:

$$K_n^+ = \max_{1 \leq i \leq N} \left\{ \frac{i}{N} - E(x_i) \right\} = \max_{1 \leq i \leq N} \left\{ \frac{i}{N} - R_i \right\}$$

$$K_n^- = \max_{1 \leq i \leq N} \left\{ E(x_i) - \frac{i-1}{N} \right\} = \max_{1 \leq i \leq N} \left\{ R_i - \frac{i-1}{N} \right\}$$

Πίνακας 6.3: 100 τυχαίοι αριθμοί μίας γραμμικής ισοϋπόλοιπης γεννήτριας, $m = 128$, $c = 11$, $a = 9$, και $Z_0 = 21$

0.57	0.15	0.43	0.89	0.03	0.37	0.39	0.61	0.50	0.59
0.36	0.32	0.98	0.81	0.33	0.04	0.44	0.02	0.30	0.76
0.91	0.24	0.27	0.48	0.38	0.46	0.24	0.20	0.85	0.69
0.20	0.92	0.31	0.91	0.17	0.64	0.79	0.12	0.14	0.35
0.25	0.34	0.11	0.07	0.72	0.56	0.08	0.80	0.19	0.78
0.05	0.51	0.66	0.99	0.02	0.23	0.13	0.21	0.99	0.95
0.60	0.43	0.96	0.67	0.06	0.65	0.93	0.39	0.54	0.87
0.90	0.10	0.00	0.09	0.87	0.83	0.47	0.31	0.83	0.54
0.94	0.53	0.80	0.26	0.41	0.75	0.77	0.98	0.88	0.97
0.74	0.70	0.35	0.18	0.71	0.42	0.82	0.40	0.68	0.13

Το μέτρο K_n^+ υπολογίζει τη μέγιστη απόκλιση ανάμεσα στην εμπειρική συνάρτηση E και τη συνάρτηση κατανομής F, όταν το E έχει μικρότερη τιμή από το F ενώ το K_n^- υπολογίζει τη τη μέγιστη απόκλιση όταν το E έχει μεγαλύτερη τιμή από το F. Ο έλεγχος Kolmogorov-Smirnov υλοποιείται με τα ακόλουθα βήματα:

Βήμα 1. Τοποθέτηση των ανεξάρτητων παρατηρήσεων R_1, $R_2, ...R_N$ κατά αύξουσα σειρά, $R_1 \leq R_2 \leq, ... \leq R_N$.

Βήμα 2. Υπολογισμός των K_n^+, K_n^-.

Βήμα 3. Υπολογισμός της μέγιστης τιμής μεταξύ των K_n^+ και K_n^-, έστω K_n, δηλαδή $K_n = \max(K_n^+, K_n^-)$.

Βήμα 4. Εύρεση της κρίσιμης τιμής K μέσα από τον πίνακα πιθανοτήτων των κατανομών K_n^+, K_n^-. Ο πίνακας αυτός παρατίθεται στη συνέχεια.

Βήμα 5. Αν η τιμή K_n είναι μεγαλύτερη από την τιμή K, απορρίπτεται η μηδενική υπόθεση, επομένως οι αριθμοί δεν είναι ομοιόμορφα κατανεμημένοι.

Ο Πίνακας 6.4 παρουσιάζει κρίσιμες τιμές για διάφορα επίπεδα σημαντικότητας και για τιμές του N από 1-15 και διάφορα επίπεδα σημαντικότητας a. Η τιμή του a δείχνει την πιθανότητα απόρριψης της μηδενικής υπόθεσης. Επίσης, δίνονται οι τιμές για $N > 35$. Πίνακες με περισσότερες τιμές διατίθενται στα περισσότερα βιβλία στατιστικής.

Πίνακας 6.4: Κρίσιμες τιμές για τον έλεγχο Kolmogorov-Smirnov

N	$K_{0.1}$	$K_{0.05}$	$K_{00.1}$
1	0.950	0.975	0.995
2	0.776	0.842	0.929
3	0.642	0.708	0.828
4	0.564	0.624	0.733
5	0.510	0.565	0.669
6	0.470	0.521	0.618
7	0.438	0.486	0.577
8	0.411	0.457	0.543
9	0.388	0.432	0.514
10	0.368	0.410	0.490
11	0.352	0.391	0.468
12	0.338	0.375	0.450
13	0.325	0.361	0.433
14	0.314	0.349	0.418
15	0.304	0.338	0.404
> 35	$1.22/\sqrt{N}$	$1.36/\sqrt{N}$	$1.63/\sqrt{N}$

Το παράδειγμα 6.9 δείχνει τον τρόπο εφαρμογής των βημάτων, ώστε να ελεγχθεί η ομοιόμορφη κατανομή των πρώτων 10 αριθμών που παρήγαγε η γεννήτρια του Πίνακα 6.3.

ΠΑΡΑΔΕΙΓΜΑ 6.9

Έστω ότι επιθυμούμε να ελέγξουμε, χρησιμοποιώντας τον έλεγχο Kolmogorov-Smirnov και για επίπεδο σημαντικότητας $a = 5\%$, αν οι 10 πρώτοι αριθμοί της γεννήτριας του Πίνακα 6.3 είναι ομοιόμορφα κατανεμημένοι. Η τιμή $a = 5\%$ δείχνει την πιθανότητα απόρριψης της μηδενικής υπόθεσης. Εφαρμόζουμε τα βήματα που παρατέθηκαν παραπάνω:

Βήμα 1. Τοποθέτηση των ανεξάρτητων παρατηρήσεων κατά αύξουσα σειρά: 0.03, 0.15, 0.37, 0.39, 0.43, 0.50, 0.57, 0.59, 0.61, 0.89.

Βήμα 2. Υπολογισμός των K_n^+, K_n^-. Ο παρακάτω πίνακας δείχνει και τους ενδιάμεσους υπολογισμούς των i/N και $(i-1)/N$, ώστε να διευκολυνθεί ο αναγνώστης. Οι τιμές των K_n^+, K_n^- δίνονται στις δύο τελευταίες γραμμές του πίνακα, αντίστοιχα. Τελικά, λαμβάνοντας τις μέγιστες τιμές, έχουμε $K_n^+ = 0.29$, $K_n^- = 0.17$.

i	1	2	3	4	5	6	7	8	9	10
R_i	0.03	0.15	0.37	0.39	0.43	0.50	0.57	0.59	0.61	0.89
i/N	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
$(i-1)/N$	0	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
K_n^+	0.07	0.05	-0.07	0.01	0.07	0.10	0.13	0.21	0.29	0.11
K_n^-	0.03	0.05	0.17	0.09	0.03	0.00	-0.03	-0.11	-0.19	-0.01

Βήμα 3. Υπολογισμός της μέγιστης τιμής μεταξύ των K_n^+ και K_n^-, έστω K_n: $K_n = \max(K_n^+,\ K_n^-) = \max(0.29, 0.17) = 0.29$.

Βήμα 4. Εύρεση της κρίσιμης τιμής K μέσα από τον πίνακα πιθανοτήτων των κατανομών K_n^+, K_n^- (Πίνακας 6.4). Για $a = 0.05$ και $N = 10$, $K = 0.410$.

Βήμα 5. Η τιμή $K_n = 0.29$ είναι μικρότερη από την τιμή $K = 0.410$, άρα δεχόμαστε τη μηδενική υπόθεση, επομένως οι 10 πρώτοι αριθμοί που παράγει η γεννήτρια είναι ομοιόμορφα κατανεμημένοι στο [0,1].

Παρατηρείστε ότι σε ανάλογο συμπέρασμα θα καταλήγαμε για τιμές του $a = 0.1$ ή $a = 0.01$. Δείτε τις σχετικές τιμές του Πίνακα 6.4. Είναι $K = 0.368$ για $a = 0.1$ και $K = 0.490$ για $a = 0.01$. Αμφότερες οι τιμές είναι μεγαλύτερες της τιμής του K_n.

Προφανώς, με παρόμοιο τρόπο μπορούν να ελεγχθούν συνολικά και οι 100 αριθμοί, αλλά κάτι τέτοιο θα αυξήσει πολύ τους υπολογισμούς. Επίσης, μπορούμε να ελέγξουμε "τοπικά" οποιοδήποτε άλλο τμήμα N τιμών της γεννήτριας. Γενικά, ο έλεγχος Kolmogorov-Smirnov έχει την ιδιότητα να ανιχνεύει την τυχαία ή μη τυχαία συμπεριφορά, τόσο τοπικά όσο και συνολικά. Ένα καλό παράδειγμα, είναι η ανίχνευση τοπικά, αλλά και σε μεγαλύτερα δείγματα (η έννοια "συνολικά" είναι κάπως σχετική, δεδομένου ότι δεν μπορούμε γενικά να περιορίσουμε το δείγμα) της μη τυχαιότητας της ακολουθίας Fibobacci. Δείτε την Άσκηση 6.10.

Ο Έλεγχος χ^2 Ο έλεγχος x^2 είναι από τους πιο συνηθισμένους στατιστικούς ελέγχους. Το πιο χαρακτηριστικό παράδειγμα ελέγχου x^2 [Knuth (1998)] είναι αυτό της ρίψης ζαριών. Αν χρησιμοποιήσουμε δύο ζάρια που δεν είναι "πειραγμένα", δηλαδή καθένα από αυτά έχει την ίδια πιθανότητα να εμφανίσει τιμή 1, 2, 3, 4, 5, ή 6, τότε, η πιθανότητα p_s να λάβουμε καθένα από τα πιθανά αθροίσματα s, από 2 ως 12 είναι η εξής:

Άθροισμα	2	3	4	5	6	7	8	9	10	11	12
πιθανότητα	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

Για παράδειγμα, το άθροισμα 8 λαμβάνεται από τους συνδυασμούς 2+6, 3+5, 4+4, 5+3, 6+2, δηλαδή 5/36 συνδυασμοί δίνουν άθροισμα 8.

Αν κάποιος ρίξει τα ζάρια b φορές, κάθε άθροισμα θα πρέπει να ληφθεί κατά προσέγγιση περίπου bp_s φορές. Π.χ. για $b = 72$, το άθροισμα 8 θα πρέπει να προκύψει $\frac{72 \times 5}{36}$=10 φορές. Αντίστοιχα, στις 72 ρίψεις, θα πρέπει να αναμένουμε 2 φορές να έρθουν "εξάρες". Όμως, θα έχει τύχει σε αρκετούς από εσάς να δείτε σε μία απλή παρτίδα τάβλι (π.χ. μία παρτίδα πόρτες), όπου ένας παίκτης πιθανότατα δεν θα ρίξει τα ζάρια 72 φορές, να φέρει "εξάρες" περισσότερες από 2 φορές. Σε αυτήν την περίπτωση, πολλοί παίκτες θεωρούν ότι ίσως ο αντίπαλός τους είναι υπερβολικά τυχερός καθώς οι ζαριές του "αποκλίνουν από το φυσιολογικό". Αυτή η απόκλιση από το φυσιολογικό ή αναμενόμενο, εξετάζεται με τη μέθοδο x^2 (Βλ. Άσκηση 6.13). Πιο συγκεκριμένα, η μέθοδος εξετάζει τα τετράγωνα των διαφορών των παρατηρημένων και των αναμενόμενων τιμών.

Η μέθοδος x^2 χωρίζει τις παρατηρήσεις σε n κλάσεις και χρησιμοποιεί το μέτρο

$$x^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \tag{6.29}$$

όπου O_i το παρατηρούμενο πλήθος παρατηρήσεων στην κλάση i και E_i είναι το αναμενόμενο πλήθος παρατηρήσεων στην κλάση i. Στην ομοιόμορφη κατανομή, το αναμενόμενο πλήθος παρατηρήσεων σε κάθε κλάση E_i είναι

$$E_i = \frac{N}{n} \tag{6.30}$$

όπου N είναι το πλήθος των παρατηρήσεων.

Ο έλεγχος x^2 υλοποιείται με τα ακόλουθα βήματα:

Βήμα 1. Χωρισμός των παρατηρήσεων σε n διαστήματα, υπολογισμός των E_i και καταμέτρηση των O_i.

Βήμα 2. Υπολογισμός των $\frac{(O_i - E_i)^2}{E_i}$ για κάθε κλάση i και άθροιση όλων αυτών των τιμών, ώστε να προκύψει η τιμή x^2.

Βήμα 3. Εύρεση της κρίσιμης τιμής x_c^2 μέσα από τον πίνακα πιθανοτήτων της κατανομής x^2. Ο πίνακας αυτός παρατίθεται στη συνέχεια.

Βήμα 4. Αν η τιμή x^2 είναι μεγαλύτερη από την τιμή x_c^2, απορρίπτεται η μηδενική υπόθεση, άρα οι αριθμοί δεν είναι ομοιόμορφα κατανεμημένοι.

Πίνακας 6.5: Κρίσιμες τιμές για τον έλεγχο x^2

n	$x^2_{0.005}$	$x^2_{0.01}$	$x^2_{0.025}$	$x^2_{0.05}$	$x^2_{0.1}$
1	7.88	6.63	5.02	3.84	2.71
2	10.60	9.21	7.38	5.99	4.61
3	12.84	11.34	9.35	7.81	6.25
4	14.96	13.28	11.14	9.49	7.78
5	16.7	15.1	12.8	11.1	9.2
6	18.5	16.8	14.4	12.6	10.6
7	20.3	18.5	16.0	14.1	12.0
8	22.0	20.1	17.5	15.5	13.4
9	23.6	21.7	19.0	16.9	14.7
10	25.2	23.2	20.5	18.3	16.0
11	26.8	24.7	21.9	19.7	17.3
12	28.3	26.2	23.3	21.0	18.5
13	29.8	27.7	24.7	22.4	19.8
14	31.3	29.1	26.1	23.7	21.1
15	32.8	30.6	27.5	25.0	22.3

Ο Πίνακας 6.5 παρουσιάζει κρίσιμες τιμές για διάφορα επίπεδα σημαντικότητας a και για τιμές του n από 1-15. Πίνακες με περισσότερες τιμές διατίθενται στα περισσότερα βιβλία στατιστικής.

Το Παράδειγμα 6.10 που ακολουθεί ελέγχει την ομοιόμορφη κατανομή των τυχαίων αριθμών που παρήγαγε η γραμμική ισοϋπόλοιπη γεννήτρια με παραμέτρους $m = 128$, $c = 11$, $a = 9$, και $Z_0 = 21$ (Πίνακας 6.3).

ΠΑΡΑΔΕΙΓΜΑ 6.10

Έστω ότι επιθυμούμε να ελέγξουμε χρησιμοποιώντας τον έλεγχο x^2 και για επίπεδο σημαντικότητας $a = 5\%$, αν οι 100 αριθμοί της γεννήτριας του Πίνακα 6.3 είναι ομοιόμορφα κατανεμημένοι. Το πλήθος των διαστημάτων είναι $n = 10$. Εφαρμόζουμε τα βήματα που παρατέθηκαν παραπάνω:

Βήμα 1. Χωρισμός των παρατηρήσεων σε $n = 10$ διαστήματα [0,0.1), [0.1,0.2),... [0.9,1) Οι τιμές των E_i και O_i δίνονται στη δεύτερη και τρίτη στήλη του πίνακα που ακολουθεί.

Βήμα 2. Υπολογισμός των $\frac{(O_i - E_i)^2}{E_i}$ για κάθε κλάση i και άθροιση όλων αυτών των τιμών, ώστε να προκύψει η τιμή x^2. Οι στήλες 3, 4, και 5 του πίνακα περιέχουν όλους τους ενδιάμεσους υπολογισμούς, ώ-

στε να διευκολυνθεί ο αναγνώστης. Το άθροισμα των τιμών της τελευταίας στήλης, είναι η τιμή x^2 και ισούται με 3.

Διάστημα	O_i	E_i	$O_i - E_i$	$(O_i - E_i)^2$	$\frac{(O_i-E_i)^2}{E_i}$
1	10	10	0	0	0.0
2	10	10	0	0	0.0
3	9	10	-1	1	0.1
4	13	10	3	9	0.9
5	9	10	-1	1	0.1
6	8	10	-2	4	0.4
7	8	10	-2	4	0.4
8	9	10	-1	1	0.1
9	11	10	1	1	0.1
10	13	10	3	9	0.9

Βήμα 3. Από τον πίνακα πιθανοτήτων της κατανομής x^2 (Πίνακας 6.5), για $n = 10$ και $a = 0.05$, είναι $x^2_{0.05} = 18.3$.

Βήμα 4. Η τιμή x^2 είναι κατά πολύ μικρότερη από την τιμή x^2_c, επομένως γίνεται αποδεκτή η μηδενική υπόθεση. Οι 100 αριθμοί της γεννήτριας είναι ομοιόμορφα κατανεμημένοι.

Κλείνοντας την παρουσίαση της ενότητας που αφορά τους ελέγχους συχνότητας, πρέπει να τονίσουμε ότι και οι δύο έλεγχοι που παρουσιάστηκαν, ο Kolmogorov-Smirnov και ο x^2 είναι αποδεκτοί και γενικά εφαρμόσιμοι. Ωστόσο, ο πρώτος μπορεί να εφαρμοστεί σε μικρά δείγματα (π.χ. 20 παρατηρήσεων). Αντίθετα, η εφαρμογή του ελέγχου x^2 σε τόσο μικρά δείγματα φαίνεται να είναι τετριμμένη.

6.5.2 ΕΛΕΓΧΟΣ ΡΟΩΝ

Όπως παρουσιάστηκε στην Ενότητα 6.3, μία από τις ιδιότητες των τυχαίων αριθμών είναι η ανεξαρτησία. Ο έλεγχος ροών είναι ένας έλεγχος ανεξαρτησίας των δεδομένων. Με τον έλεγχο αυτό δεν ελέγχεται η ομοιομορφία στην κατανομή. Μία ακολουθία μπορεί να ελεγχθεί για αύξουσες και φθίνουσες ροές. Ας υποθέσουμε ότι εξετάζουμε τις αύξουσες ροές (ομοίως εξετάζουμε και τις φθίνουσες). Ο έλεγχος αυξουσών ροών αφορά το μήκος των τμημάτων που είναι ταξινομημένα με αύξουσα σειρά μέσα στην ακολουθία. Για παράδειγμα, θεωρείστε τις 10 πρώτες τυχαίες τιμές του Πίνακα 6.3: