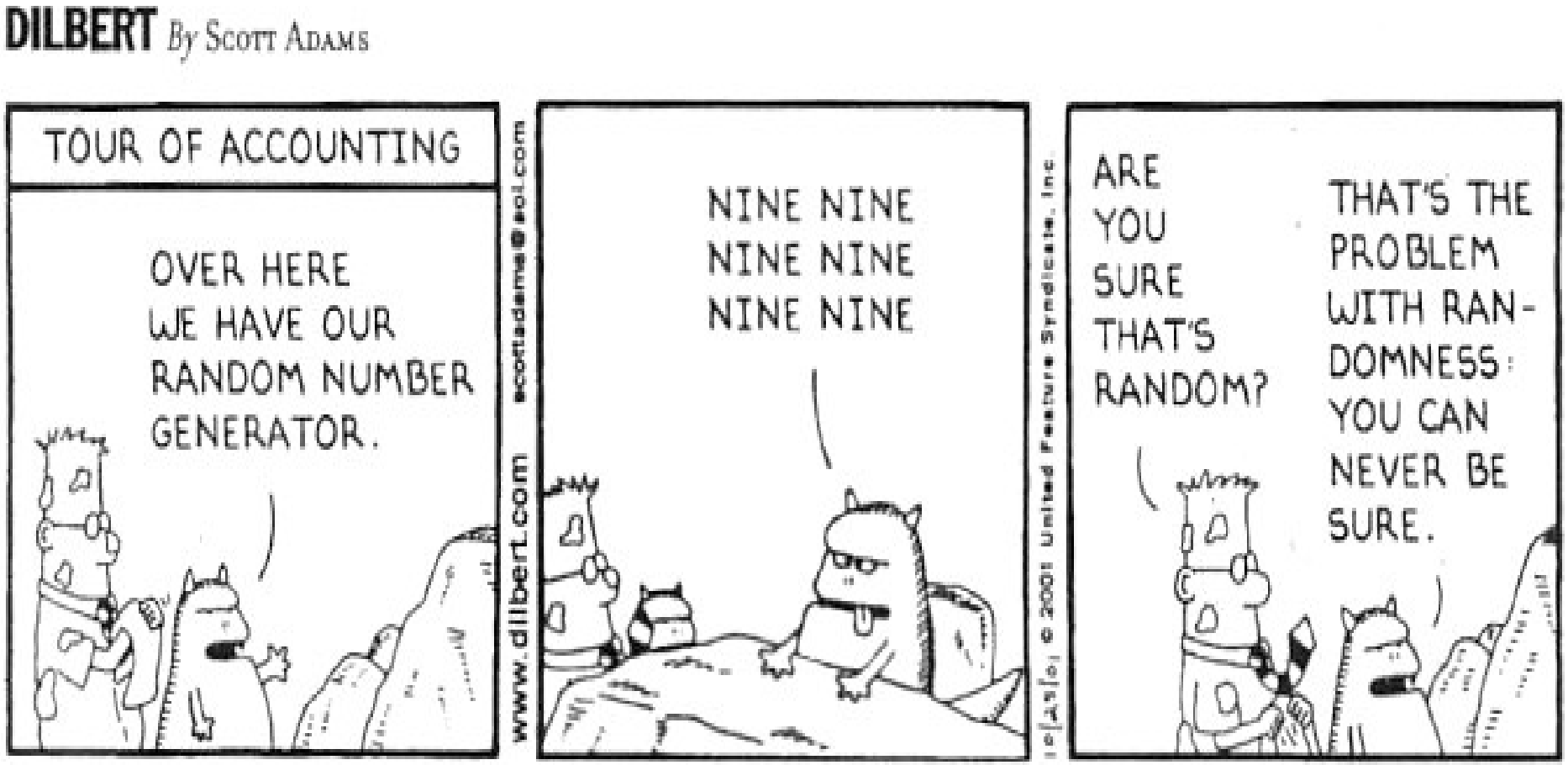
Προσομοίωση Δικτύων

6η Διάλεξη

Στατιστικοί έλεγχοι για Γεννήτριες Τυχαίων Αριθμών

Γιατί


DILBERT By Scott Adams
TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
www.dilbert.com scottadams@aol.com
NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
10/25/01 © 2001 United Feature Syndicate, Inc.

Γιατί

- Καλή πρακτική ο έλεγχος μιας Γ.Τ.Α. πριν τη χρήση της
- Μεγάλος ο ρόλος του τρόπου υλοποίησης στην ποιότητα μιας Γ.Τ.Α.
- Στόχος ο έλεγχος της στατιστικής συμπεριφοράς των παραγόμενων αριθμών
- Το πέρασμα ενός ελέγχου δεν εγγυάται την καλή ποιότητα μιας Γ.Τ.Α.
- Το κόψιμο από έναν έλεγχο εγγυάται την κακή ποιότητα μιας Γ.Τ.Α.

Έλεγχοι

- Στα πλαίσια του μαθήματος θα ασχοληθούμε με:
  1. Έλεγχος συχνότητας
  2. Σειριακός έλεγχος
  3. Έλεγχος αυτοσυσχέτισης
  4. Έλεγχος συνεχόμενων ροών (runs test)
  5. Έλεγχος χ^2
  6. Έλεγχος Kolmogorov-Smirnov
- Οι 1-3 ελέγχουν την τυχαιότητα μιας ακολουθίας bits
- Οι 4-6 ελέγχουν την τυχαιότητα ψευδο-τυχαίων αριθμών στο [0,1]

Τρόπος λειτουργίας

- Οι στατιστικοί έλεγχοι ελέγχουν αν μια συγκεκριμένη υπόθεση είναι αληθής
- Η υπο-έλεγχο υπόθεση καλείται *μηδενική υπόθεση* H_0 *(null hypothesis)*
- Για τον έλεγχο της υπόθεσης, συλλέγονται δεδομένα και με βάση αυτά γίνεται ο στατιστικός έλεγχος της υπόθεσης

Παράδειγμα

- Μηδενική υπόθεση H_0: “Το 30% των αυτοκινήτων είναι κόκκινα”
- Συλλέγουμε ένα αντιπροσωπευτικό δείγμα από αυτοκίνητα
- Υπολογίζουμε το ποσοστό p_{red} των κόκκινων
- Ακόμα κι αν η υπόθεση είναι αληθής, δεν μπορούμε να περιμένουμε ότι $p_{red}=0.30$
- Ο στατιστικός έλεγχος θα δείξει αν η διαφορά του p_{red} με το 0.30 οφείλεται στην τυχαιότητα του δείγματος ή στο ότι η H_0 είναι ψευδής

Έλεγχος Γ.Τ.Α.

- Είσοδος: Δείγμα της παραγόμενης από την Γ.Τ.Α. ακολουθία αριθμών
- Μηδενική υπόθεση H_0: “η παραγόμενη ακολουθία τυχαίων αριθμών είναι τυχαία”
- Ο έλεγχος θα αποφανθεί για το αν η H_0 είναι αληθής ή ψευδής
- Το αποτέλεσμα είναι πιθανοτικό (όχι ντετερμινιστικό)
  - Με κάποια πιθανότητα δεχόμαστε ή απορρίπτουμε την H_0

Λάθη στον έλεγχο υποθέσεων

- 2 τύποι λαθών
  - Τύπος I: false negative
  - Τύπος II: false positive
- Η πιθανότητα απόρριψης της H_0 ενώ είναι αληθής

  (α) καλείται επίπεδο σημαντικότητας (level of significance)
- Πρακτικά το α παίρνει τιμές 0.01 ή 0.05

Real situation	**Decision**	
	H_o is not rejected	*H_0 is rejected*
H_o is true	Valid	Type I error
H_o is not true	Type II Error	Valid

Έλεγχος συχνότητας

- Από τους πιο σημαντικούς
- Αν μια Γ.Τ.Α. αποτύχει σε αυτόν τον έλεγχο, το πιθανότερο είναι να αποτύχει και σε άλλους πιο εξεζητημένους
- Σε μια τυχαία ακολουθία bit, ο αριθμός των 0 και των 1 θα πρέπει να είναι (περίπου) ίδιος
- Αυτό είναι που ελέγχεται με τον έλεγχο συχνότητας

Έλεγχος συχνότητας: Βήματα

1. Παραγωγή m τυχαίων αριθμών και ένωσή τους σε μια ακολουθία bits

   Έστω n το μήκος της ακολουθίας.

2. Μετατροπή των 0 σε -1
3. Πρόσθεση των bits: $S_n=X_1+X_2+...+X_n$
4. $$S_{obs} = \frac{|S_n|}{\sqrt{n}}$$
5. $$P\text{-}value = erfc\left(\frac{S_{obs}}{\sqrt{2}}\right) \quad , \quad \operatorname{erfc}(x) = 1 - \operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2}\, dt.$$

Έλεγχος συχνότητας: Απόφαση

- Αν P-value < 0.01 απορρίπτουμε την H_0
- Η ακολουθία bit πρέπει να έχει μήκος μερικών χιλιάδων
- Η P-value είναι μικρή όταν τα $|S_n|$ ή $|S_{obs}|$ είναι μεγάλα
  - Όταν δηλαδή υπάρχουν πολλά 1 ή 0 (-1)
- π.χ. 1011010101
  - $S_n=1+(-1)+1+1+(-1)+1+(-1)+1+(-1)+1=2$
  - $S_{obs}=0.6324$
  - $\text{P-value}=\text{erfc}(0.4471)=0.5271>0.01$
  - Άρα η ακολουθία γίνεται δεκτή ως τυχαία

Σειριακός έλεγχος

- Μια ακολουθία από k bits παράγει 2^k συνδυασμούς
- Κάθε συνδυασμός έχει την ίδια πιθανότητα εμφάνισης, αν η ακολουθία είναι τυχαία
- Ο σειριακός έλεγχος αποφασίζει για το αν ο αριθμός των εμφανίσεων αυτών των συνδυασμών είναι ομοιόμορφα κατανεμημένος
- Αν k=1, τότε έχουμε έλεγχο συχνότητας

Σειριακός έλεγχος

- Έστω *e* η ακολουθία *n* bits που παρήγαγε μια Γ.Τ.Α (n>100)
- Ο σειριακός έλεγχος ελέγχει την τυχαιότητα των αλληλεπικαλυπτόμενων ομάδων από *k*, *k-1*, *k-2* bits της *e*, όπου $k<log_2 n-2$

Σειριακός έλεγχος: Βήματα

1. Επαύξησε την e προσθέτοντας
   τα πρώτα k-1 bits στο τέλος της -> e'_1. Ομοίως
   με τα πρώτα k-2 bits -> e'_2 και
   με τα πρώτα k-3 bits -> e'_3
2. Υπολόγισε τη συχνότητα εμφανίσεων για κάθε
   συνδυασμό από k , k-1 και k-2 bits
   χρησιμοποιώντας αντίστοιχα τις ακολουθίες e'_1,e'_2
   και e'_3.

Έστω f_i, f_i', f_i'' η συχνότητα εμφάνισης του i-οστού συνδυασμού k , k-1 και k-2 bits αντίστοιχα

Σειριακός έλεγχος: Βήματα

3. Υπολόγισε τα

$$S_k^2 = \frac{2^k}{n}\sum_i f_i^2 - n \qquad S_{k-1}^2 = \frac{2^{k-1}}{n}\sum_i f_i'^2 - n \qquad S_{k-2}^2 = \frac{2^{k-2}}{n}\sum_i f_i''^2 - n$$

4. Υπολόγισε τα
   - $\Delta S^2_k = S^2_k - S^2_{k-1}$
   - $\Delta^2 S^2_k = S^2_k - 2S^2_{k-1} + S^2_{k-2}$
5. $\text{P-value}_1 = \text{igamc}(2^{k-2}, \Delta S^2_k/2)$

   $\text{P-value}_2 = \text{igamc}(2^{k-3}, \Delta^2 S^2_k/2)$

Σειριακός έλεγχος: Απόφαση

- Αν P-value$_1$ ή P-value$_2$ < α, τότε απορρίπτουμε την H_0

Σειριακός έλεγχος: Παράδειγμα

e=0011011101, n=10, k=3

1.
   - Προσθέτουμε τα k-1=2 bits στο τέλος της e -> e'_1=001101110100
   - Ομοίως με τα k-2=1 bits -> e'_2=00110111010
   - k-3=0 bits -> e'_3=e
2. Υπολογισμός των εμφανίσεων
   - Συνδυασμοί με 3 bits: c_1=000, c_2=001, c_3=010, c_4=011, c_5=100, c_6=101, c_7=110, c_8=111
   - Οι εμφανίσεις τους: f_1=0, f_2=1, f_3=1, f_4=2, f_5=1, f_6=2, f_7=2, f_8=0

Σειριακός έλεγχος: Παράδειγμα

2. Υπολογισμός των εμφανίσεων (συνέχεια)
   - Συνδυασμοί με 2 bits: $c'_1=00$, $c'_2=01$, $c'_3=10$, $c'_4=11$
   - Οι εμφανίσεις τους : $f'_1=1$, $f'_2=3$, $f'_3=3$, $f'_4=3$
   - Συνδυασμοί 1-bit $c''_1=0$, $c''_2=1$
   - Οι εμφανίσεις τους: $f''_1=4$, $f''_2=6$
3. $S^2_3=2^3/10*(0+1+1+4+1+4+4+1)-10=2.8$

   $S^2_2=2^2/10*(1+9+9+9)-10=1.2$

   $S^2_1=2/10*(16+36)-10=0.4$

Σειριακός έλεγχος: Παράδειγμα

4. $\Delta S^2_k = S^2_3 - S^2_2 = 2,8-1,2=1.6$

   $\Delta^2 S^2_k = S^2_3 - 2\ S^2_2 + S^2_1 = 0.8$

5. $\text{P-value}_1 = \text{igamc}(2,0.8) = 0.9057$

   $\text{P-value}_2 = \text{igamc}(1,0.4) = 0.8805$

Αφού P-value_1 και $\text{P-value}_2 > 0.01$ η ακολουθία περνάει τον έλεγχο

Έλεγχος αυτοσυσχέτισης

- Έστω e μια ακολουθία από n bits
- Σύγκριση της e με ολισθημένες εκδόσεις της
- Η ολίσθηση μιας τυχαίας ακολουθίας παράγει διαφορετικό αποτέλεσμα

Έλεγχος αυτοσυσχέτισης: Βήματα

1. Έστω e_i η ολισθημένη έκδοση της e κατά i θέσεις.

   Δεδομένου d, 1≤d≤n/2, υπολογίζουμε τον αριθμό των bits που διαφέρουν τα e_i και e_{i+d}, όπου 0<i<n-d-1, ως εξής

$$A(d) = \sum_{i=0}^{n-d-1} e_i \oplus e_{i+d}$$

2. Έπειτα υπολογίζουμε το εξής στατιστικό

$$S = \frac{2\left(A(d) - \frac{n-d}{2} \right)}{\sqrt{n-d}}$$

Έλεγχος αυτοσυσχέτισης: Βήματα

3. Το S ακολουθεί την κανονική κατανομή N(0,1). Για παράδειγμα για επίπεδο σημαντικότητας 5%, δεχόμαστε την H_0 αν $S \leq 1.96$

Έλεγχος αυτοσυσχέτισης: Παράδειγμα

- Έστω η σειρά

11100 01100 01000 10100 11101 11100 10010 01001

επαναλαμβανόμενη 4 φορές

- Για d=8
  - A(8)=100
  - S=3.8933 > 1.96

Άρα δεν περνάει τον έλεγχο

Έλεγχος συνεχόμενων ροών

- Ελέγχεται η ανεξαρτησία των παραγόμενων αριθμών
- Ορίζουμε ως συνεχόμενη ροή μια μη-διακοπτόμενη ακολουθία μονοτονικά αυξανόμενων
- Για παράδειγμα στην ακολουθία

0.8, 0.7, 0.75, 0.55, 0.6, 0.7,0.3, 0.4, 0.5

έχουμε κατα σειρά μια ροές μήκους 1, 2, 3, 3

Έλεγχος συνεχόμενων ροών

- Γενικά r_i ο αριθμός των ροών με μήκος i
  - Στο προηγούμενο παράδειγμα $r_1=1$, $r_2=1$, $r_3=2$
  - Για i≥6, όλες οι ροές ομαδοποιούνται σε μια
- Υπολογίζεται το:

$$R = \frac{1}{n} \sum_{1 \le i \ , \ j \le 6} (r_i - nb_i)(r_j - nb_j)a_{ij} \ , \ 1 \le i \le 6, \ 1 \le j \le 6,$$

που ανήκει στην χ^2 κατανομή με 6 βαθμούς ελευθερίας

Έλεγχος χ^2

- Ελέγχει αν οι παραγόμενοι τυχαίοι αριθμοί είναι ομοιόμορφα κατανεμημένοι
- Έστω μια ακολουθία τυχαίων αριθμών που βρίσκονται στο [0,1]
- Χωρίζουμε το [0,1] σε k υποδιαστήματα ίσου μήκους
- Ορίζουμε ως f_i το πλήθος των τυχαίων αριθμών που βρίσκονται στο i-οστό υποδιάστημα
- Καλούμε τις f_i, τιμές παρατήρησης

Έλεγχος χ^2

- Αν οι παραγόμενοι τυχαίοι αριθμοί είναι ομοιόμορφα κατανεμημένοι, τότε το μέσο πλήθος αριθμών σε κάθε υποδιάστημα θα είναι n/k
- Αναφερόμαστε σε αυτήν την τιμή ως θεωρητική τιμή
- Ο έλεγχος χ^2 μετράει κατά πόσο οι διαφορές ανάμεσα στις τιμές παρατήρησης και τη θεωρητική τιμή οφείλονται σε τυχαιότητα ή σε μη ομοιόμορφη κατανομή της υπο εξέταση ακολουθίας

Έλεγχος χ^2

- Η μετρική απόφασης δίνεται από τον τύπο:

$$\chi^2 = \frac{k}{n}\sum_{i=1}^{k}(f_i - \frac{n}{k})^2$$

με k-1 βαθμούς ελευθερίας

- Η H_0 απορρίπτεται όταν η τιμή χ^2 που υπολογίζεται είναι μεγαλύτερη από αυτή που παίρνουμε από τους πίνακες με την χ^2 κατανομή για k-1 βαθμούς ελευθερίας και α επίπεδο σημαντικότητας

Έλεγχος χ^2: Παράδειγμα

- Θέλουμε να ελέγξουμε την τυχαιότητα ενός ζαριού με 60 ρίψεις

	1	2	3	4	5	6
παρατηρήσεις	8	9	13	12	10	8
αναμενόμενες	10	10	10	10	10	10

$X^2 = [(8-10)^2+(9-10)^2+(13-10)^2+(12-10)^2+(10-10)^2+(8-10)^2] / 10 = 2.2$

Έλεγχος χ^2: Παράδειγμα

- Βαθμοί ελευθερίας 6-1=5, α=0.05

ν	p					
	0.9	0.95	0.975	0.98	0.99	0.995
1	2.7055	3.8415	5.0239	5.4119	6.6349	7.8794
2	4.6052	5.9915	7.3778	7.8240	9.2103	10.5966
3	6.2514	7.8147	9.3484	9.8374	11.3449	12.8382
4	7.7794	9.4877	11.1433	11.6678	13.2767	14.8603
5	9.2364	11.0705	12.8325	13.3882	15.0863	16.7496
6	10.6446	12.5916	14.4494	15.0332	16.8119	18.5476
7	12.0170	14.0671	16.0128	16.6224	18.4753	20.2777
8	13.3616	15.5073	17.5345	18.1682	20.0902	21.9550
9	14.6837	16.9190	19.0228	19.6790	21.6660	23.5894
10	15.9872	18.3070	20.4832	21.1608	23.2093	25.1882

άρα αφού 2.2 < 11.0705 η H_0 γίνεται δεκτή

Έλεγχος Kolmogorov-Smirnov (KS)

- Ο Έλεγχος χ^2 βασίζεται στο ζυγισμένο άθροισμα των τετραγωνισμένων διαφορών ανάμεσα στις παρατηρημένες και τις αναμενόμενες εμφανίσεις
- Ο Έλεγχος KS εστιάζει στην μέγιστη διαφορά ανάμεσα στην υπο-έλεγχο κατανομή (εμπειρική) και την θεωρητική κατανομή
- Για να δημιουργήσουμε την εμπειρική κατανομή μετράμε για κάθε τιμή πόσες από τις υπόλοιπες είναι μικρότερες ή ίσες από αυτήν

(α) Έστω οι παρακάτω τιμές από μια Γ.Τ.Α. στο U[0,1]

0.887
0.793
0.837
0.907
0.587
0.325
0.999
0.951
0.495
0.838
0.636
0.595
0.881
0.319
0.122
0.012
0.953
0.752
0.351
0.116

(a)

(β) Τις ταξινομούμε

0.887	0.012
0.793	0.122
0.837	0.116
0.907	0.319
0.587	0.325
0.325	0.351
0.999	0.495
0.951	0.587
0.495	0.595
0.838	0.636
0.636	0.752
0.595	0.793
0.881	0.837
0.319	0.838
0.122	0.881
0.012	0.887
0.953	0.907
0.752	0.951
0.351	0.953
0.116	0.999
(a)	(b)

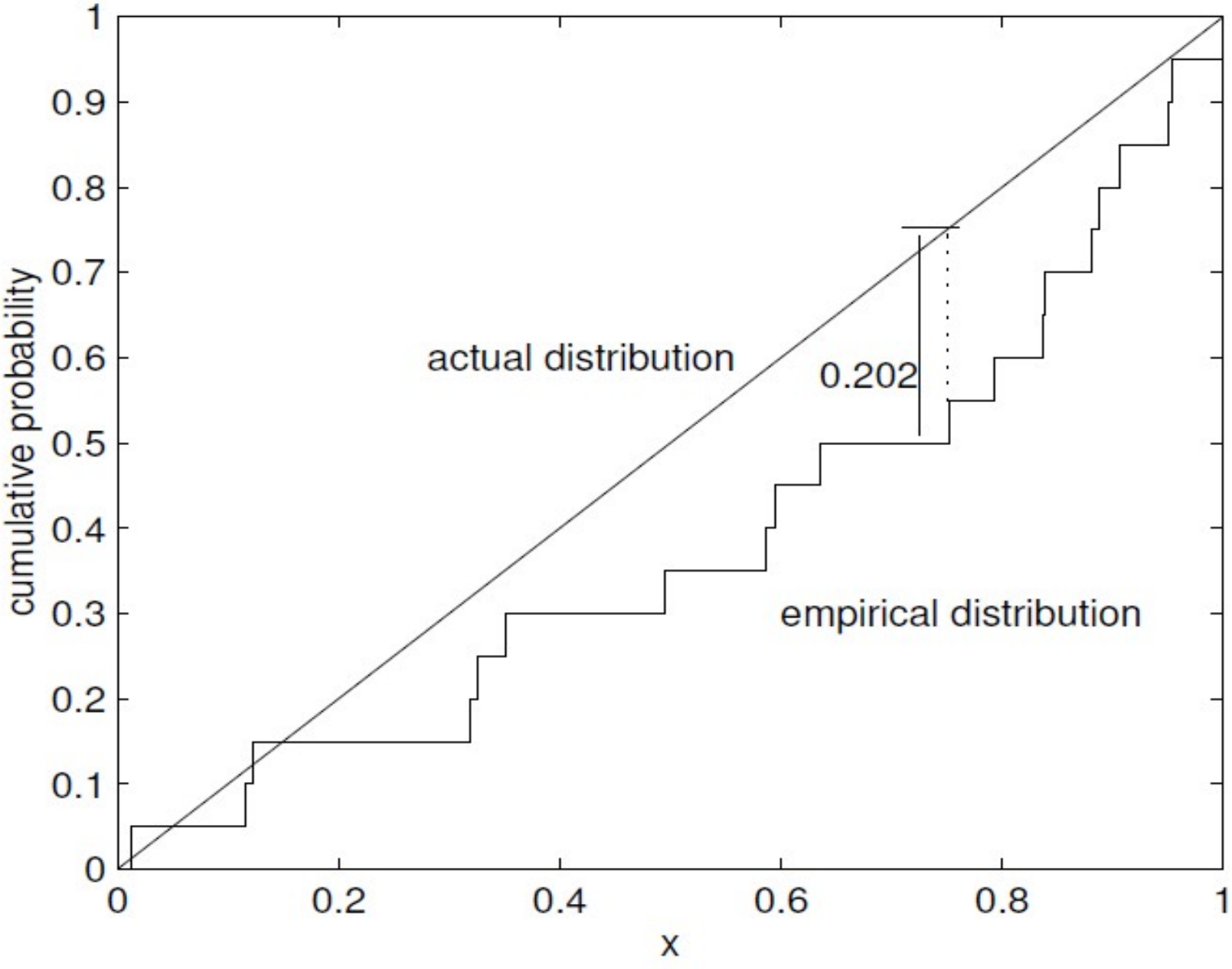
(γ) Υπολογίζουμε το ποσοστό των τιμών που είναι ≤ από κάθε τιμή

(a)	(b)	(c)
0.887	0.012	0.05
0.793	0.122	0.10
0.837	0.116	0.15
0.907	0.319	0.20
0.587	0.325	0.25
0.325	0.351	0.30
0.999	0.495	0.35
0.951	0.587	0.40
0.495	0.595	0.45
0.838	0.636	0.50
0.636	0.752	0.55
0.595	0.793	0.60
0.881	0.837	0.65
0.319	0.838	0.70
0.122	0.881	0.75
0.012	0.887	0.80
0.953	0.907	0.85
0.752	0.951	0.90
0.351	0.953	0.95
0.116	0.999	1.00

(δ) Υπολογίζουμε τη διαφορά στις στήλες c και b

(a)	(b)	(c)	(d)
0.887	0.012	0.05	0.038
0.793	0.122	0.10	0.022
0.837	0.116	0.15	0.034
0.907	0.319	0.20	0.119
0.587	0.325	0.25	0.075
0.325	0.351	0.30	0.051
0.999	0.495	0.35	0.145
0.951	0.587	0.40	0.187
0.495	0.595	0.45	0.145
0.838	0.636	0.50	0.136
0.636	0.752	0.55	0.202
0.595	0.793	0.60	0.193
0.881	0.837	0.65	0.187
0.319	0.838	0.70	0.138
0.122	0.881	0.75	0.131
0.012	0.887	0.80	0.087
0.953	0.907	0.85	0.057
0.752	0.951	0.90	0.051
0.351	0.953	0.95	0.003
0.116	0.999	1.00	0.001

Αποτέλεσμα


cumulative probability
x
actual distribution
empirical distribution
0.202
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
0.2
0.4
0.6
0.8
1