ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ειδικά Θέματα Θεμελιώσεων της Επιστήμης των Υπολογιστών

Καθηγητής:
Λευτερης Κυρουσης

Διάλεξη 8η: 1 Φεβρουαρίου 2012

1 Εισαγωγικά στοιχεία πιθανοτήτων

Στην παράγραφο αυτή θα παρουσιαστούν βασικά στοιχεία πιθανοτήτων που θα μας είναι χρήσιμα στη συνέχεια. Αρχικά θα δοθούν κάποιοι ορισμοί βασικών εννοιών και μεγεθών, και στη συνέχεια θα παρουσιαστούν γνωστές ιδιότητές τους[1].

1.1 Τυχαίες μεταβλητές[2]

Στα πλαίσια του μαθήματος θα ασχοληθούμε μόνο με διακριτές τυχαίες μεταβλητές, που παίρνουν τιμές στο σύνολο των φυσικών αριθμών.

Επομένως, μια τυχαία μεταβλητή είναι μια συνάρτηση από ένα χώρο τυχαίων πειραμάτων (δειγματοχώρος) στο σύνολο των φυσικών αριθμών:

$$X : \Omega \to \mathbb{N}$$

όπου X μια τυχαία μεταβλητή, Ω ο χώρος τυχαίων πειραμάτων και $\mathbb{N}$ το σύνολο των φυσικών αριθμών.

[1] Τα παραπάνω δε θα παρουσιαστούν με μαθηματική αυστηρότητα καθώς κάτι τέτοιο ξεφεύγει από τα πλαίσια του μαθήματος.

[2] Στα πλαίσια του μαθήματος θα ασχοληθούμε μόνο με διακριτές τυχαίες μεταβλητές που παίρνουν τιμές στο σύνολο των φυσικών αριθμών. Για το λόγο αυτό και ο ορισμός που δίνεται δεν είναι ο γενικός ορισμός των τυχαίων μεταβλητών αλλά αυτών που θα χρησιμοποιηθούν στη συνέχεια.

Συμβολισμοί Συμβολίζουμε με p_k την πιθανότητα η τυχαία μεταβλητή X να πάρει την τιμή k, δηλαδή

$$p_k = Pr\{X = k\} = \sum_{X(\omega)=k} Pr\{\omega \in \Omega\}$$

Η δεύτερη ισότητα λέει ότι η πιθανότητα η τυχαία μεταβλητή X να πάρει την τιμή k είναι ίση με το άθροισμα των πιθανοτήτων των ενδεχομένων του δειγματοχώρου για τα οποία το X(ω) είναι k.

Άλλοι συμβολισμοί που θα χρησιμοποιηθούν είναι οι παρακάτω:

- $r_k = Pr\{X \leq k\}$
- **Αναμενόμενη τιμή :** $E(X) = \sum_{k \geq 0} k \cdot p_k$
- **Διασπορά :** $V(X) = E\Big(\big(X - E(X)\big)^2\Big)$

1.2 Δεσμευμένη ή Υπο συνθήκη Πιθανότητα

Η πιθανότητα η τυχαία μεταβλητή X να πάρει την τιμή k δεδομένου ότι η τυχαία μεταβλητή Υ έχει πάρει την τιμή l λέγεται δεσμευμένη ή υπο συνθήκη πιθανότητα και δίνεται από την παρακάτω σχέση (νόμος του Bayes):

$$Pr\{X = k \mid Y = l\} = \frac{Pr\{X = k \ \& \ Y = l\}}{Pr\{Y = l\}}$$

Ισχύει επίσης το παρακάτω:

$$\begin{aligned} Pr\{X = k \ \& \ Y = l\} &= Pr\{X = k \mid Y = l\} Pr\{Y = l\} \\ &= Pr\{Y = l \mid X = k\} Pr\{X = k\} \end{aligned}$$

1.3 Ανεξαρτησία μεταβλητών

Δυο τυχαίες μεταβλητές λέγονται **ανεξάρτητες** όταν

$$Pr\{X = k \ \& \ Y = l\} = Pr\{X = k\} Pr\{Y = l\}$$

Με βάση τα παραπάνω, δυο τυχαίες μεταβλητές X,Υ είναι ανεξάρτητες αν

$$Pr\{X = k \mid Y = l\} = Pr\{X = k\}$$

ή αντίστοιχα

$$Pr\{Y = l \mid X = k\} = Pr\{Y = l\}$$

Δυο τυχαίες μεταβλητές λέγονται **θετικά συσχετισμένες** όταν

$$Pr\{X = k \ \& \ Y = l\} > Pr\{X = k\}Pr\{Y = l\}$$

και **αρνητικά συσχετισμένες** όταν

$$Pr\{X = k \ \& \ Y = l\} < Pr\{X = k\}Pr\{Y = l\}$$

1.4 Γραμμικότητα της Αναμενόμενης Τιμής

Έστω Χ,Υ δυο οποιεσδήποτε τυχαίες μεταβλητές.

$$E(X + Y) = E(X) + E(Y)$$

Λήμμα 1.1

$$E(X) = \sum_{k \geq 0} k \cdot p_k = \sum_{\omega \in \Omega} X(\omega) \cdot Pr\{\omega\}$$

Για το λήμμα αυτό δε θα δοθεί απόδειξη, μπορεί όμως κανείς να διαπιστώσει ότι το αριστερό μέλος είναι ο έξυπνος τρόπος μέτρησης της αξίας νομισμάτων που αναφέρθηκε σε προηγούμενη διάλεξη (διάλεξη 4, παράγραφος 2) και το δεξί μέλος ο 'χαζός' τρόπος μέτρησης της αξίας νομισμάτων.

Απόδειξη της Γραμμικότητας της Αναμενόμενης Τιμής Χρησιμοποιώντας το παραπάνω λήμμα, θα αποδείξουμε τη Γραμμικότητα της Αναμενόμενης Τιμής.

$$E(X + Y) =$$

$$\sum_{\omega \in \Omega} (X(\omega) + Y(\omega)) \cdot Pr\{\omega\} =$$

$$= \sum_{\omega \in \Omega} X(\omega) \cdot Pr\{\omega\} + \sum_{\omega \in \Omega} Y(\omega) \cdot Pr\{\omega\} =$$

$$= E(X) + E(Y)$$

Θεώρημα 1.2 *Έστω X, Υ **ανεξάρτητες** τυχαίες μεταβλητές. Τότε, ισχύουν τα παρακάτω:*

$$E(X \cdot Y) = E(X) \cdot E(Y)$$

$$V(X + Y) = V(X) + V(Y)$$

Η απόδειξη θα δοθεί μόνο για τη δεύτερη σχέση.

$$V(X + Y) =$$

$$
\begin{aligned}
&= E\Big(\big((X+Y)-E(X+Y)\big)^2\Big) = \\
&= E\Big(\big(X+Y-E(X)-E(Y)\big)^2\Big) = && \textit{γραμμικότητα αναμ. τιμής} \\
&= E\Big(\big((X-E(X))+(Y-E(Y))\big)^2\Big) = \\
&= E\Big((X-E(X))^2+(Y-E(Y))^2+2(X-E(X))(Y-E(Y))\Big) = \\
&= E\Big((X-E(X))^2\Big) + E\Big((Y-E(Y))^2\Big) + E\Big(2(X-E(X))(Y-E(Y))\Big) = && \textit{γραμμικότητα αναμ. τιμής} \\
&= V(X)+V(Y) + E\Big(2(X-E(X))(Y-E(Y))\Big)
\end{aligned}
$$

Στη συνέχεια εξετάζουμε μόνο τον τρίτο όρο:

$$E\Big(2(X-E(X))(Y-E(Y))\Big) =$$

$$
\begin{aligned}
&= 2 \cdot E\Big((X-E(X))(Y-E(Y))\Big) && \textit{γραμμικότητα αναμ. τιμής} \\
&= 2 \cdot E\Big(XY-E(X)Y-XE(Y)+E(X)E(Y)\Big) = \\
&= 2 \cdot \Big(E(XY)-E(X)E(Y)-E(X)E(Y)+E(X)E(Y)\Big) = && \textit{γραμμικότητα αναμ. τιμής} \\
&= 2 \cdot \Big(E(XY)-E(X)E(Y)\Big) = \\
&= 2 \cdot \Big(E(X)E(Y)-E(X)E(Y)\Big) = && \textit{αφού X,Υ ανεξάρτητες} \\
&= 0
\end{aligned}
$$

Επομένως, όταν Χ,Υ είναι ανεξάρτητες

$$V(X+Y) = V(X) + V(Y)$$

2 Πιθανογεννήτριες Συναρτήσεις

Οι πιθανογεννήτριες είναι γεννήτριες συναρτήσεις και ορίζονται ως εξής:

$$P(z) = \sum_{k \geq 0} p_k \cdot z^k$$

Η παραπάνω γεννήτρια συνάρτηση λέγεται πιθανογεννήτρια συνάρτηση γιατί οι συντελεστές του z^k είναι πιθανότητες.

2.1 Ιδιότητες πιθανογεννητριών συναρτήσεων

$P(1) = 1$
$P'(z) = \sum_{k \geq 1} k p_k z^{k-1}$
Έχοντας υπολογίσει τον τύπο της πρώτης παραγώγου της πιθανογεννήτριας συνάρτησης, αν θέσουμε όπου $z = 1$ θα λάβουμε την πρώτη παράγωγο του

$P'(1)$ για το οποίο ισχύει:
$P'(1) = \sum_{k\geq 1} kp_k = E(X) \Rightarrow E(X) = P'(1)$

Θεώρημα 2.1 *Έστω X μια τυχαία μεταβλητή. Τότε θα ισχύει:*

$$V(X) = P''(1) + P'(1) - \big(P'(1)\big)^2$$

Ακολουθεί η απόδειξη:

$V(X) =$
$= E\Big(\big(X - E(X)\big)^2\Big) =$
$= \sum_{k\geq 0} \big(k - P'(1)\big)^2 P_k =$ $\qquad E(X) = P'(1)$ *και* $E(X) = \sum_{k\geq 0}(1 - r_k)$
$= \sum_{k\geq 0} \big(P'(1)\big)^2 P_k - 2\sum_{k\geq 0} kP'(1)P_k + \sum_{k\geq 0} k^2 P_k$

Θα υπολογίσουμε κάθε έναν από τους τρείς αυτούς όρους χωριστά.

Για το πρώτο άθροισμα ισχύει:

$$\sum_{k\geq 0} \big(P'(1)\big)^2 P_k = \big(P'(1)\big)^2 \sum_{k\geq 0} P_k = \big(P'(1)\big)^2 \cdot 1 = \big(P'(1)\big)^2$$

Για το δεύτερο άθροισμα ισχύει:

$$\sum_{k\geq 0} kP'(1)P_k = P'(1)\sum_{k\geq 0} kP_k = P'(1) \cdot P'(1) = \big(P'(1)\big)^2$$

, όπου χρησιμοποιήθηκε η σχέση $\sum_{k\geq 0} kP_k = E(X) = P'(1)$.

Για το τρίτο άθροισμα θα χρειαστεί να υπολογίσουμε αρχικά τη δεύτερη παράγωγο της πιθανογεννήτριας συνάρτησης για την τιμή 1. Ισχύει:

$$P(z) = \sum_{k\geq 0} P_k z^k$$

$$P'(z) = \sum_{k\geq 0} kP_k z^{k-1}$$

$$P''(z) = \sum_{k\geq 0} k(k-1)P_k z^{k-2}$$

$$P''(z) \cdot z + P'(z) = \sum_{k\geq 1} k^2 P_k z^{k-1}$$

$$P''(1) + P'(1) = \sum_{k\geq 0} k^2 P_k$$

Επομένως, $\sum_{k\geq 0} k^2 P_k = P''(1) + P'(1)$.

Επιστρέφοντας στην απόδειξη, καταλήγουμε πως:

$$V(X) = P''(1) + P'(1) - \left(P'(1)\right)^2$$

Ροπές τυχάιας μεταβλητής: Η ροπή $i-$οστής τάξης ορίζεται ως $\sum_{k\geq 0} k^i P_k$. Για παράδειγμα, η ροπή πρώτης τάξης θα ισούται με $\sum_{k\geq 0} kP_k$ και πρόκειται για την αναμενομένη τιμή.

3 Στοιχεία Μαθηματικής Λογικής

Στην ενότητα αυτή θα παρουσιαστόυν βασικές έννοιες της μαθηματικής λογικής.

3.1 Προτασιακή Λογική

Η προτασιακή λογική περιλαμβάνει εκφράσεις οι οποίες αποτελούνται από προτάσεις αποτελούμενες από:

- προτασιακές μεταβλητές ενός bit, δηλαδή μεταβλητές που θα έιναι είτε αληθείς είτε ψευδείς. Για παράδειγμα, $(p, q, r, ...)$ ή/και $(p_1, p_2, p_3, ...)$
- κανόνες, ευρέως γνωστούς ως λογικές πράξεις

Οι κανόνες αυτοί είναι οι εξής:

$\wedge$	and/και
$\vee$	or/ή
$\rightarrow$	implies/έπεται
$\neg$	not/όχι
$\leftrightarrow$ ή $\equiv$	implication/ισοδυναμία

Για κάθε λογική πράξη δημιουργούνται πίνακες αληθείας για τις μεταβλητές που συμμετέχουν στον υπολογισμό. Πίνακες αληθείας δημιουργούνται για κάθε έκφραση που σχηματίζεται στην προτασιακή λογική. Για να κατανοήσουμε περισσότερο την έννοια του πίνακα αληθείας, ας δούμε για παράδειγμα τον πίνακα αληθείας της πράξης λογικού ΚΑΙ ($\wedge$).

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Ιδιαίτερο ενδιαφέρον έχει ο πίνακας αληθείας του λογικού implies ($\rightarrow$) ο οποίος φαίνεται στη συνέχεια:

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Η λογική της λογικής πράξης 'έπεται' είναι η διατήρηση της αλήθειας. Στην πρώτη περίπτωση είναι σαφές πως η αλήθεια διατηρείται ενώ στη δεύτερη συμβαίνει το ακριβώς αντίθετο. Στην τρίτη και στην τέταρτη περίπτωση δεν υπάρχει αλήθεια, εξάρχής, για να διατηρηθεί λόγω του ότι η υπόθεση της έκφρασης (η μεταβλητή p) είναι ψευδής. Άρα, το αποτέλεσμα είναι αληθές.

3.2 Ενδιαφέρουσες Ιδιότητες

Μια ενδιαφέρουσα ιδιότητα περιλαμβάνει την πράξη 'έπεται' ως εξής:

$$A \rightarrow B \equiv \neg A \vee B$$

Δύο ακόμα ενδιαφέροντες και πολύ χρήσιμοι τύποι είναι οι κανόνες De Morgan:

$$\neg(A \wedge B) \equiv \neg A \vee \neg B$$

και

$$\neg(A \vee B) \equiv \neg A \wedge \neg B$$

Στη συνέχεια παρουσιάζεται η ιδιότητα της επιμεριστικότητας στη προτασιακή λογική:

$$A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$$

και

$$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$$

Στην προτασιακή λογική, όταν έχουμε έκφραση που αποτελεί σύζευξη διαζεύξεων, τότε λέμε πως η έκφραση είναι σε Συζευκτική Κανονική Μορφή (ΣΚΜ) ή Conjuctive Normal Form (CNF). Μια έκφραση σε CNF θα είναι στη μορφή:

$$(... \vee ... \vee ...) \wedge (... \vee ... \vee ...) \wedge .... \wedge (... \vee ... \vee ...)$$

όπου, κάθε παρένθεση αποτελεί ένα clause ενώ κάθε μεταβλητή που είναι σε διάζευξη μέσα στις παρενθέσεις αποτελεί ένα literal.

Οι κανόνες De Morgan και οι τύποι που προκύπτουν από την ιδιότητα της επιμεριστικότητας και παρουσιάστηκαν προηγουμένως είναι χαρακτηριστικές περιπτώσεις Συζευκτικής Κανονικής Μορφής.