Η Πιθανοθεωρητική Μέθοδος

Θερινό Σχολείο 2010

Διάλεξη 2η

Μιχάλης Κολουντζάκης

Πανεπιστήμιο Κρήτης

Ηράκλειο, Ιούλιος 2010

Η μέθοδος της μέσης τιμής (μέτρημα με πιθανοθεωρητική γλώσσα)

Τυχαία μεταβλητή $X \in \mathbb{R}$ έχει μέση τιμή $\mu = \mathbb{E}X$. Τότε η X παίρνει τιμές $\geq \mu$ όπως επίσης και τιμές $\leq \mu$.

Πολύ σημαντικό: Γραμμικότητα της μέσης τιμής:

$$\mathbb{E}[aX + bY] = a\mathbb{E}X + b\mathbb{E}Y$$

(χωρίς απαίτηση ανεξαρτησίας για τις X, Y)

Παράδειγμα: Έχουμε λογικές μεταβλητές $x_1, x_2, \ldots$ και N διαζεύξεις μεγέθους 3, π.χ. $C_1 = x_1 \vee \overline{x_5} \vee x_3$, $C_2 = x_3 \vee x_4 \vee \overline{x_2}$, ...

Θέλουμε να επιλέξουμε $x_1 \in \{T, F\}, x_2 \in \{T, F\}, \ldots$ ώστε να ικανοποιήσουμε όσο γίνεται περισσότερες διαζεύξεις.

Επιλογή των λογικών μεταβλητών στην τύχη

Υπάρχει επιλογή των $x_j \in \{T, F\}$ που ικανοποιεί τουλάχιστον τα 7/8 των διαζεύξεων.

Έστω τ.μ. $X_j \in \{T, F\}$ με $\mathbb{P}[X_j = T] = \mathbb{P}[X_j = F] = 1/2$, ανεξάρτητες.

$I_j = \mathbf{1}(C_j$ αληθής$)$, $\mathbb{P}[I_j = 1] = \frac{7}{8}$ (ανεξαρτησία των X_j)

$S = \sum_{j=1}^N I_j =$ πόσες από τις N διαζεύξεις C_k ικανοποιούνται.

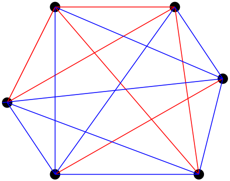
$\mathbb{E}S = \sum_{j=1}^N \mathbb{E}I_j = \sum_{j=1}^N \mathbb{P}[I_j = 1] = \frac{7}{8}N$.

Άρα υπάρχει έκβαση του πειράματος (ανάθεση τιμών στα X_j) ώστε $S \geq \frac{7}{8}N$.

Προσοχή: Η απόδειξη δε μας λέει πώς να βρούμε τέτοια ανάθεση τιμών.

Παράδειγμα: Χρωματισμός ακμών ενός γραφήματος

N κορυφές συνδέεονται όλες μεταξύ τους.
Βάφουμε ακμές κόκκινες ή μπλε.



Σκοπός: Λίγα μονοχρωματικά τρίγωνα.

Βάφουμε κάθε ακμή κόκκινη ή μπλε με πιθ. $1/2$, ανεξάρτητα.

u, v, w κορυφές: $\mathbb{P}\left[\text{τρίγωνο } uvw \text{ μονοχρ.}\right] = 1/4$

(Αφού 2 από τους $8 = 2^3$ ισοπίθανους χρωματισμούς μας δίνουν μονοχρ. τρίγωνο.)

Χρωματισμός ακμών ενός γραφήματος (συνέχεια)

Πλήθος όλων των τριγώνων: $\binom{N}{3}$.

Έστω τ.μ. $I_j = 1$ ανν το j-οστό τρίγωνο μονχρ.

$T := \sum_{j=1}^{\binom{N}{3}} I_j =$ το πλήθος των μονοχρ. τριγώνων

$\mathbb{E}T = \sum_{j=1}^{\binom{N}{3}} \mathbb{E}I_j = \binom{N}{3}\mathbb{P}\left[I_1 = 1\right] = \frac{1}{4}\binom{N}{3}$.

Υπάρχει χρωματισμός με 2 χρώματα των ακμών του πλήρους γραφήματος K_n με πλήθος μονοχρωματικών τριγώνων

$$T \le \frac{1}{4}\binom{N}{3}.$$

Και πάλι δε μας λέει η απόδειξη πώς να βρούμε ένα τέτοιο.

Παράδειγμα: Προσθαφαιρέσεις διανυσμάτων

N διανύσματα στο $\mathbb{R}^d$: $v_1, \ldots, v_N$ με μήκος $|v_j| \le 1$. Τότε μπορούμε να επιλέξουμε τα πρόσημα $\epsilon_1, \ldots, \epsilon_N = \pm 1$ ώστε το

$$u = \epsilon_1 v_1 + \cdots \epsilon_N v_N$$

να έχει μήκος $|u| \le \sqrt{N}$.

Επιλέγουμε $\epsilon_j = \pm 1$ με ίδια πιθανότητα και ανεξάρτητα.

Για $i \ne j$: $\mathbb{E}\epsilon_i \epsilon_j = \mathbb{E}\epsilon_i \mathbb{E}\epsilon_j = 0 \cdot 0 = 0$ (από ανεξαρτησία)

Προσθαφαιρέσεις διανυσμάτων (συνέχεια)

$$
\begin{aligned}
\mathbb{E}|u|^2 = \mathbb{E}u \cdot u &= \mathbb{E}\sum_{i,j=1}^{N} \epsilon_i \epsilon_j v_i \cdot v_j \\
&= \sum_{i,j=1}^{N} v_i \cdot v_j \mathbb{E}\epsilon_i \epsilon_j \\
&= \sum_{i,j=1}^{N} v_i \cdot v_j \mathbf{1}\left(i = j\right) \\
&= \sum_{j=1}^{N} |v_j|^2 \\
&\le N.
\end{aligned}
$$

Άρα υπάρχει επιλογή προσήμων ώστε $|u|^2 \le N$ ή $|u| \le \sqrt{N}$.

Παράδειγμα: Αριθμητικές Πρόοδοι

Θεώρημα (van der Waerden, 1927)

Έστω $k \in \mathbb{N}$. Αν το N είναι αρκετά μεγάλο τότε όπως και να χρωματίσουμε με δύο χρώματα τους αριθμούς $1, 2, \ldots, N$ υπάρχει μονοχρ. αριθμητική πρόοδος (ΑΠ) μήκους k.

Πόσο μεγάλο πρέπει να είναι το N σε σχέση με το k για να υπάρχει ΑΠ μήκους k;

Θα δείξουμε ότι το N πρέπει να είναι $> 2^{k/2}$ αν για κάθε χρωματισμό υπάρχει k-ΑΠ.

Έστω $N \leq 2^{k/2}$ και χρωματίζουμε τυχαία τους $1, 2, \ldots, N$ κόκκινους ή μπλε.

Αριθμητικές Πρόοδοι (συνέχεια)

Αν S μια k-ΑΠ ορίζουμε $I_S = \mathbf{1}$ (η S είναι μονοχρ.).

Τότε $\mathbb{P}[I_S = 1] = 2 \cdot 2^{-k} = 2^{1-k}$.

Μια k-ΑΠ καθορίζεται από το 1ο και το 2ο στοιχείο της
$\Rightarrow$ πλήθος k-ΑΠ $\le \binom{N}{2}$

$$\begin{aligned}
\mathbb{P}[\text{υπάρχει μονοχρ. } k\text{-ΑΠ}] &\le \sum_{S \text{ είναι } k\text{-ΑΠ}} \mathbb{P}[I_S = 1] \\
&\le 2^{1-k}\binom{N}{2} = 2^{1-k}\frac{N(N-1)}{2} \\
&< 2^{-k}N^2 \\
&\le 1 \ \text{ αφού } N \le 2^{k/2}.
\end{aligned}$$

Άρα με θετική πιθανότητα δεν υπάρχει μονοχρ. k-ΑΠ.

Παράδειγμα: Σύνολα χωρίς αθροίσματα

Σύνολο A λέγεται "χωρίς αθροίσματα" αν

$$\forall x, y, z \in A : x + y \neq z.$$

Π.χ. οι περιττοί ακέραιοι, το σύνολο $\{N, N+1, \ldots, 2N-1\}$.

Θεώρημα (Erdős, 1965)

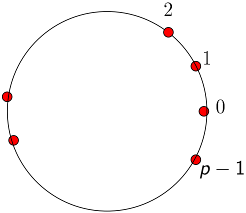
Αν $E \subseteq \mathbb{N}$ έχει $|E| = N$ τότε υπάρχει υποσύνολο $A \subseteq E$ που είναι χωρίς αθροίσματα και

$$|A| \geq N/3.$$

Επιλογή του $A \subseteq E$ είναι πιθανοθεωρητική αλλά δεν είναι η προφανής επιλογή.

Το να επιλέξουμε αν θα κρατήσουμε ένα στοιχείο του E ή όχι δε γίνεται ανεξάρτητα για κάθε στοιχείο.

Το πεπερασμένο σώμα $\mathbb{Z}_p$, p πρώτος αριθμός



$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. Πράξεις $+, \times$ γίνονται mod p.

Αντιμεταθετικός δακτύλιος.

Σημαντικό: Όταν p πρώτος αριθμός το $\mathbb{Z}_p$ είναι *σώμα*:
κάθε $x \in \mathbb{Z}_p \setminus \{0\}$ έχει μοναδικό πολλαπλασιαστικό αντίστροφο x^{-1}:

$$x \cdot x^{-1} = 1 \bmod p.$$

Παράδειγμα: $5^{-1} = 8 \bmod 13$ αφού $5 \cdot 8 = 40 = 3 \cdot 13 + 1 = 1 \bmod 13$

Σύνολα χωρίς αθροίσματα (συνέχεια)

$E = \{e_1 < e_2 < \cdots < e_N\}$ και p πρώτος αριθμός $p > e_N$.

<u>Παρατήρηση:</u> Αν $A \subseteq \{1, 2, \ldots, p-1\}$ είναι χωρίς αθροίσματα $\bmod p$
$\Rightarrow$ είναι χωρίς αθροίσματα στο $\mathbb{Z}$

Παίρνουμε t τυχαίο στο $\{1, 2, \ldots, p-1\}$ (ομοιόμορφα κατανεμημένο)

<u>Παρατήρηση:</u> Το σύνολο $M = \left\{\left\lceil \frac{p}{3} \right\rceil, \ldots, \left\lfloor \frac{2p}{3} \right\rfloor\right\}$ είναι χωρίς αθροίσματα $\bmod p$.

tM επίσης χωρίς αθροίσματα $\bmod p$ $(tx + ty = tz \Rightarrow x + y = z)$

$E \cap tM$ (πολ/σμός $\bmod p$) υποσύνολο του E χωρίς αθροίσματα $\bmod p$.

Ορίζουμε την τ.μ. $X = |E \cap tM|$.
Θέλουμε να δείξουμε ότι μπορεί να γίνει μεγάλη.

Σύνολα χωρίς αθροίσματα (τέλος)

$$
\begin{aligned}
\mathbb{E}|X| = \mathbb{E}|E \cap tM| &= \mathbb{E}\sum_{s\in E} \mathbf{1}\left(\exists m \in M : tm = s\right) \\
&= \mathbb{E}\sum_{s\in E} \mathbf{1}\left(t^{-1}s \in M\right) \\
&= \sum_{s\in E} \mathbb{P}\left[t^{-1}s \in M\right] = \sum_{s\in E} \mathbb{P}\left[t \in sM^{-1}\right] \\
&= \sum_{s\in E} \frac{|M|}{p-1} \\
&= \sum_{s\in E} \frac{\frac{p}{3}+o(p)}{p-1} = \frac{\frac{p}{3}+o(p)}{p-1} N \\
&= (\frac{1}{3}+o(1))N \quad (\text{για } p \to \infty).
\end{aligned}
$$

Άρα υπάρχει t ώστε $|E \cap tM| \geq (\frac{1}{3}+o(1))N$.

p τεράστιο $\Rightarrow$ Υπάρχει υποσύνολο του E με $\geq N/3$ στοιχεία και χωρίς αθροίσματα.