# 22A004 - Προχωρημένα Θέματα Θεωρίας Πληροφορίας
# Τελική Εξέταση Ιουνίου 2015

• Διάρκεια Εξέτασης: 3 ώρες. 3 προβλήματα (το φυλλάδιο έχει 8 σελίδες – ελέγξτε το!)

• Βαθμός εξέτασης = μονάδες/10. Σύνολο μονάδων: 100.

• Οι απαντήσεις σας σε κάθε ερώτημα θα πρέπει να είναι επαρκώς αιτιολογημένες. Επιτρέπεται η χρήση (χωρίς απόδειξη) οποιουδήποτε θεωρήματος και οποιασδήποτε ιδιότητας έχει αναφερθεί στο μάθημα ή βρίσκεται στο βιβλίο ή/και στις σημειώσεις ή/και στα φυλλάδια αρκεί να το διευκρινίσετε.

• Παρακαλείστε να επισυνάψετε ΟΛΑ τα πρόχειρα που χρησιμοποιήσατε κατά τη διάρκεια της εξέτασης.

• Παρακαλείστε να γράφετε το όνομά σας και να αριθμείτε άμεσα όλα τα φύλλα που σας δίνονται από τον επιτηρητή, συμπεριλαμβανομένων των προχείρων.

• Σύμφωνα με το Άρθρο 50 παρ. 6 του Εσωτερικού Κανονισμού Λειτουργίας του Πανεπιστημίου Πατρών και το Νόμο, απαγορεύεται το κάπνισμα μέσα στην αίθουσα κατά τη διάρκεια του διαγωνίσματος. Θα σας επιτραπεί, όμως, να βγείτε έξω για να καπνίσετε. Επίσης, απαγορεύεται επικοινωνία μεταξύ διαγωνιζομένων χωρίς άδεια επιτηρητή. Τέλος, απαγορεύεται η χρήση κινητών τηλεφώνων ή άλλων μέσων επικοινωνίας.

• Παρακαλώ συμπληρώστε το όνομά σας στο παρακάτω εδάφιο. Μπορείτε να κρατήσετε τα θέματα όταν τελειώσετε. Οι λύσεις θα είναι διαθέσιμες σύντομα.

**ΚΑΛΗ ΕΠΙΤΥΧΙΑ!**

Όνομα: ______________________________________________

| Βάρη προβλημάτων | |
|---|---|
| 1ο θέμα | 35 |
| 2ο θέμα | 30 |
| 3ο θέμα | 35 |

**Η ΣΕΛΙΔΑ ΑΥΤΗ ΕΙΝΑΙ ΚΕΝΗ ΕΣΚΕΜΜΕΝΑ**

1. **Εντροπία, Σχετική Εντροπία και Αμοιβαία Πληροφορία (35 μονάδες)**

   (α) **Φράγματα για την Εντροπία (12 μονάδες)**
   Θεωρούμε *διακριτή* τ.μ. $X$ με p.m.f. $p_1, p_2, \ldots, p_M$.
   Έστω ότι $p_1 = \frac{1}{2}$. Δείξτε ότι

   $$1 \leq H(X) \leq 1 + \frac{1}{2}\log_2(M-1),$$

   όπου η $H(X)$ μετράται σε bits.

   Μπορούμε να επιτύχουμε τα φράγματα με ισότητα; Αν ναι, με ποιες κατανομές (δηλαδή με ποιες τιμές των $p_i$;) (6 μονάδες)

   Γενικεύστε για αυθαίρετη (αλλά γνωστή) τιμή της $p_1$. (6 μονάδες)

   (β) **Αμοιβαία Πληροφορία (8 μονάδες)**
   Θεωρούμε τ.μ. $U, X$ και $Y$. Η από κοινού p.m.f. τους ικανοποιεί τη σχέση

   $$p(u, x, y) = p(u, x)p(y|x).$$

   Μπορούμε να συγκρίνουμε την $I(U;Y)$ με την $I(X;Y)$; Δηλαδή μπορούμε να πούμε αν η $I(U;Y)$ είναι $\leq$, $=$ ή $\geq$ σε σχέση με την $I(X;Y)$;

   Αιτιολογήστε την απάντησή σας.

   (γ) **Σχετική Εντροπία (15 μονάδες)**
   Θεωρούμε δύο *διακριτές* κατανομές $p_1, p_2, \ldots, p_M$ και $q_1, q_2, \ldots, q_M$. Χωρίς βλάβη της γενικότητας θεωρούμε ότι οι $p_i$ είναι τοποθετημένες σε αύξουσα σειρά, δηλαδή

   $$p_1 \leq p_2 \leq \cdots \leq p_M.$$

   Δείξτε ότι η $D(p||q)$ ελαχιστοποιείται όταν και οι $q_i$ είναι τοποθετημένες σε αύξουσα σειρά.

   *Υπόδειξη:* Υποθέστε ότι στην $p_i$ έχουμε αντιστοιχίσει κάποια $q_l$ η οποία είναι μεγαλύτερη από κάποια άλλη τιμή $q_j$ την οποία έχουμε αντιστοιχίσει στην $p_k$ ($p_k \geq p_i$). Τι συμβαίνει αν αντιστοιχίσουμε την $q_j$ στην $p_i$ και την $q_l$ στην $p_k$;

2. **AEP (30 μονάδες)**

   (α) **(15 μονάδες)**
   Στο μάθημα είδαμε ότι ο *τύπος* (ή εμπειρική κατανομή), $\pi(a; x^n)$, μίας συγκεκριμένης ακολουθίας $x^n \triangleq x_1, x_2, \ldots, x_n$ ορίζεται ως

   $$\pi(a; x^n) \triangleq \frac{1}{n} N(a; x^n) \text{ για όλα τα } a \in \mathcal{X},$$

   όπου $N(a; x^n)$ είναι ο αριθμός των εμφανίσεων της τιμής $a$ στην ακολουθία $x^n$.
   Θεωρούμε ότι η ακολουθία παίρνει διακριτές τιμές και ότι το $\mathcal{X}$ είναι πεπερασμένο.

   (i) **(10 μονάδες)**
   Δείξτε ότι ο αριθμός όλων των πιθανών τύπων για ακολουθίες μήκους $n$ δεν μπορεί να υπερβεί την τιμή $(n+1)^{|\mathcal{X}|}$.
   *Υπόδειξη:* Πόσες τιμές μπορεί να πάρει ο $\pi(a; x^n)$ για δεδομένο $a$;

   (ii) **(5 μονάδες)**
   Έστω ότι θέλουμε να μεταδώσουμε τον *τύπο* της ακολουθίας (και όχι την ακριβή ακολουθία $x^n$). Δείξτε ότι ο απαιτούμενος ρυθμός μετάδοσης τείνει στο $0$ καθώς $n \to \infty$.
   *Υπενθύμιση:* $R \triangleq \frac{\log M}{n}$.

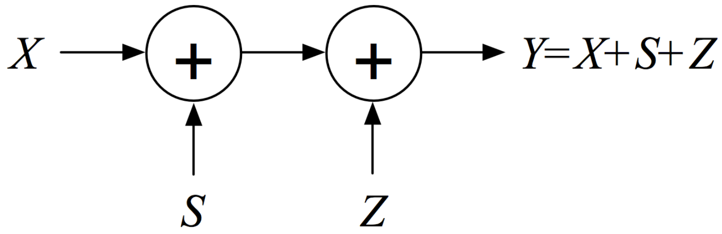
   (β) **(15 μονάδες)**
   Θεωρούμε μια πηγή *χωρίς μνήμη* που παράγει *συνεχείς* τ.μ. με βάση τη συνάρτηση πυκνότητας πιθανότητας $f(x) = c \cdot 2^{-x^4}$. Η $c$ είναι κατάλληλη σταθερά προκειμένου η $f(x)$ να είναι pdf και δε χρειάζεται να την υπολογίσετε.
   Δείξτε ότι, για οποιοδήποτε $\epsilon > 0$,

   $$\Pr\left\{\frac{1}{n}\sum_{i=1}^{n} x_i^4 \leq h(x) + \log_2 c + \epsilon\right\} \to 1 \text{ για } n \to \infty.$$

   *Υπόδειξη:* Ποιο είναι το σύνολο, $A_\epsilon^{(n)}$, των ασθενώς τυπικών ακολουθιών και τι ισχύει όταν $n \to \infty$;

3. **Κακόβουλος παρεμβολέας (35 μονάδες)**

   Θεωρούμε μετάδοση σε Γκαουσιανό Κανάλι με ισχύ $\mathbb{E}\left[X^2\right] = P$. Ο πομπός χρησιμοποιεί λευκή Γκαουσιανή στοχαστική διαδικασία, $X_k \sim \mathcal{N}(0, P)$. Η στοχαστική διαδικασία $\{Z\}$ είναι λευκός Γκαουσιανός θόρυβος (διακριτού χρόνου). Δηλαδή, είναι i.i.d. με $Z_k \sim \mathcal{N}(0, N_z)$. Επίσης, η $\{Z\}$ είναι ανεξάρτητη από τη $\{X\}$. Ωστόσο, όπως φαίνεται στο Σχήμα 1, ένας κακόβουλος παρεμβολέας προσθέτει ένα σήμα $\{S\}$ στο σήμα $\{X\}$ που εκπέμπει ο πομπός. Σκοπός του παρεμβολέα είναι να ελαττώσει το ρυθμό μετάδοσης που μπορούμε να επιτύχουμε.




Σχήμα 1: Γκαουσιανό κανάλι με κακόβουλο παρεμβολέα.

   (α) **(7 μονάδες)**

   Υποθέστε, αρχικά, ότι ο παρεμβολέας δε γνωρίζει το σήμα $\{X\}$. Το μόνο που μπορεί να κάνει είναι να δημιουργεί λευκο Γκαουσιανό θόρυβο που είναι ανεξάρτητος από το σήμα $\{X\}$ και από το θόρυβο $\{Z\}$. Δηλαδή, δημιουργεί i.i.d. στοχαστική διαδικασία $\{S\}$ με $S_k \sim \mathcal{N}(0, N_s)$.

   Ποιος είναι ο μέγιστος επιτεύξιμος ρυθμός μετάδοσης (έστω $R_1$); Μπορεί ο $R_1$ να γίνει *ακριβώς* ίσος με $0$;

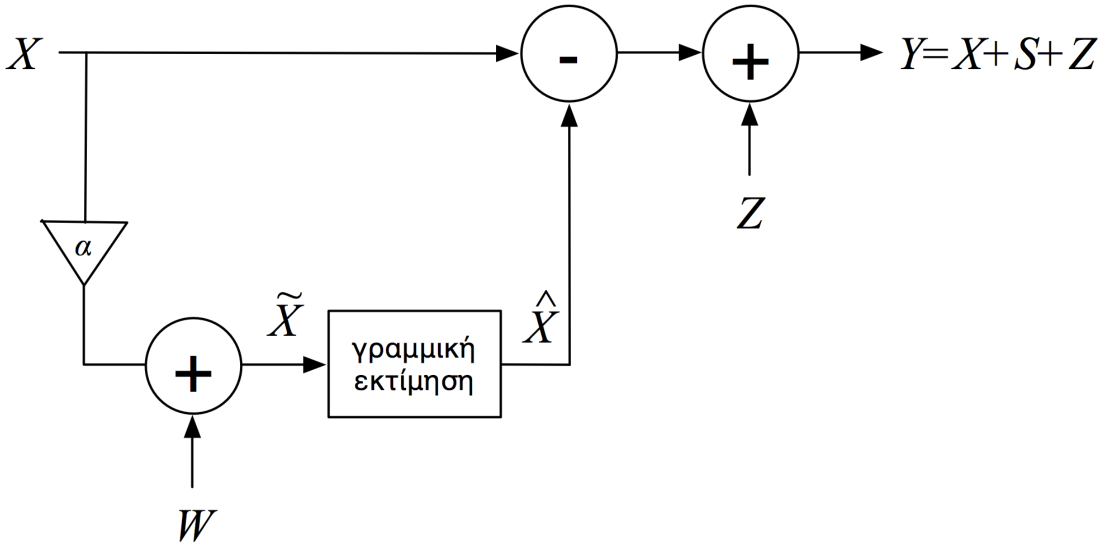
ΣΥΝΕΧΕΙΑ ΣΤΗΝ ΕΠΟΜΕΝΗ ΣΕΛΙΔΑ

(β) **(16 μονάδες)**

Υποθέστε, τώρα, ότι ο παρεμβολέας μπορεί να μετρήσει το σήμα $\{X\}$ (με θόρυβο), όπως φαίνεται στο Σχήμα 2. Το $\alpha$ είναι ένας *γνωστός* συντελεστής απόσβεσης: $\alpha \leq 1$. Δηλαδή,

$$\tilde{X}_k = \alpha X_k + W_k,$$

όπου $\{W\}$ είναι λευκός Γκαουσιανός θόρυβος με $W_k \sim \mathcal{N}(0, N_w)$ και ανεξάρτητος του $\{Z\}$.




Σχήμα 2: Κακόβουλος παρεμβολέας με γραμμικό εκτιμητή.

Ο παρεμβολέας εκτιμά το $X_k$ από τη μέτρηση $\tilde{X}_k$ χρησιμοποιώντας το γραμμικό εκτιμητή

$$\hat{X}_k = \frac{\alpha P}{\alpha^2 P + N_w} \tilde{X}_k.$$

Αποδεικνύεται ότι ο παραπάνω εκτιμητής ελαχιστοποιεί το μέσο τετραγωνικό σφάλμα $\mathbb{E}\left[(\hat{X} - X)^2\right]$.

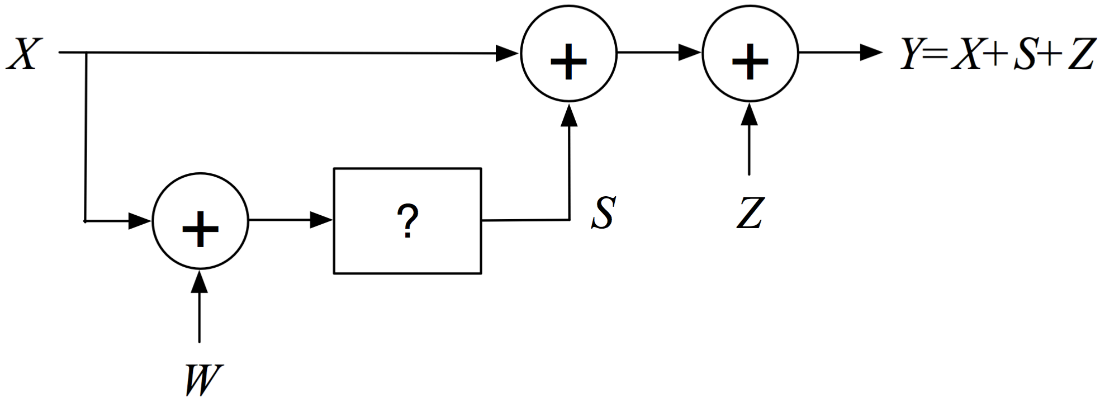
Στη συνέχεια, ο παρεμβολέας θέτει $S_k = -\hat{X}_k$, όπως φαίνεται στο Σχήμα 2. Δηλαδή, αφαιρεί την εκτίμηση $\hat{X}_k$ από το $X_k$.

i. Βρείτε το μέγιστο επιτεύξιμο ρυθμό μετάδοσης, έστω $R_2$. (12 μονάδες)
ii. Πού συγκλίνει η τιμή της $R_2$ όταν $N_w \to 0$; (2 μονάδες)
iii. Δείξτε ότι για $\alpha = 1$ και $N_w = N_z$, $R_2 > 0$. (2 μονάδες)

ΣΥΝΕΧΕΙΑ ΣΤΗΝ ΕΠΟΜΕΝΗ ΣΕΛΙΔΑ

(γ) **(12 μονάδες)**

Υποθέστε, τώρα, ότι $\alpha = 1$, όπως φαίνεται στο Σχήμα 3. Επίσης, $N_w = N_z$, δηλαδή τα $W_k$ έχουν την ίδια διασπορά με τα $Z_k$ (αλλά παραμένουν ανεξάρτητα). Σχεδιάστε ένα σύστημα στο κουτί του Σχήματος 3 με το οποίο να πετυχαίνουμε ρυθμό μετάδοσης $R_3 = 0$, δηλαδή να εμποδίζουμε τον πομπό να μεταδώσει οτιδήποτε.




Σχήμα 3: Κακόβουλος παρεμβολέας που επιτυγχάνει $R_3 = 0$.

Θεωρούμε ότι

• Οι ισχείς των θορύβων $N_w = N_z$ είναι μη μηδενικές.

• Για την έξοδο $S_k$ του κουτιού πρέπει να ισχύει $\mathbb{E}[S^2] \leq P$.

• Ο παρεμβολέας γνωρίζει το βιβλίο κωδίκων (codebook) που χρησιμοποιεί ο πομπός.

• Ο παρεμβολέας είναι τέλεια συγχρονισμένος με τον πομπό, δηλαδή γνωρίζει πότε ξεκινά η μετάδοση κάθε κωδικής λέξης.

• Ο πομπός μεταδίδει με ρυθμό μετάδοσης που δεν υπερβαίνει την τιμή $\frac{1}{2}\log\left(1+\frac{P}{N_z}\right) = \frac{1}{2}\log\left(1+\frac{P}{N_w}\right)$.

• Το σύστημα στο κουτί μπορεί να είναι όσο πολύπλοκο θέλουμε.

**Η ΣΕΛΙΔΑ ΑΥΤΗ ΕΙΝΑΙ ΚΕΝΗ ΕΣΚΕΜΜΕΝΑ**