# 22A004 - Προχωρημένα Θέματα Θεωρίας Πληροφορίας
# Τελική Εξέταση Ιουνίου 2015
# Ενδεικτικές Λύσεις (προσωρινές)

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)

   Απάντηση:

   Εφαρμόζουμε αρχή διαχωρισιμότητας της εντροπίας. Έστω τ.μ. $Z$ η οποία ισούται με $1$ όταν $X = x_1$ και $0$ όταν $X \neq x_1$.

   $$\begin{aligned} H(X,Z) &= H(Z) + H(X|Z) \\ &= H(p_1) + p_1 \cdot 0 + (1-p_1)H(X|X \neq x_1). \end{aligned}$$

   Η $H(X|X \neq x_1)$ ισούται με $0$ όταν η τιμή της $X$ δεδομένου ότι $X \neq x_1$ είναι ντετερμινιστική. Δηλαδή, όταν, δεδομένου ότι $X \neq x_1$, $X = x_j$ με πιθανότητα $1$ για κάποιο $j \neq 1$. Επομένως, όταν η $X$ ακολουθεί κατανομή Bernoulli με παράμετρο $p_1$: $p_j = 1 - p_1$ για κάποιο $j \neq 1$ και για όλα τα άλλα $k$, $p_k = 0$. Σε αυτήν την περίπτωση, το κάτω φράγμα επιτυγχάνεται με ισότητα και $H(X) = H(p_1)$.

   Αντιστρόφως, για να μεγιστοποιήσουμε την $H(X|X \neq x_1)$ πρέπει να χρησιμοποιήσουμε ομοιόμορφη κατανομή στις τιμές $x_2, x_3, \ldots, x_M$, δηλαδή $p_j = \frac{1-p_1}{M-1}$ $j = 2, \ldots, M$, οπότε $H(X|X \neq x_1) = \log_2(M-1)$.

   (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.

Απάντηση:

Στη γενική περίπτωση, $p(u,x,y) = p(u,x)p(y|x,u)$. Επομένως, στο συγκεκριμένο πρόβλημα, $p(y|x,u) = p(y|x)$ και $U \to X \to Y$.

Συνεπώς, από την ανισότητα επεξεργασίας δεδομένων,

$$I(U;Y) \leq I(X;Y).$$

(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 $p_k$;

Απάντηση:

Έστω $D_1$ η σχετική εντροπία στην πρώτη αντιστοίχιση και $D_2$ η σχετική εντροπία στη δεύτερη αντιστοίχιση. Αν αφαιρέσουμε,

$$\begin{aligned} D_1 - D_2 &= p_i \log \frac{p_i}{q_l} + p_k \log \frac{p_k}{q_j} - p_i \log \frac{p_i}{q_k} + p_k \log \frac{p_k}{q_l} \\ &= -p_i \log q_l - p_k \log q_j + p_i \log q_k + p_k \log q_l \\ &= (p_k - p_i) \log \frac{q_l}{q_j} > 0, \end{aligned}$$

επειδή $p_k \geq p_i$ και $q_l > q_j$. Συνεπώς, αν ανταλλάξουμε τις θέσεις των $q_j$ και $q_k$ η σχετική εντροπία ελαττώνεται. Μπορούμε να συνεχίσουμε να ανταλλάσσουμε έως ότου τα $q_i$ διαταχθούν και αυτά σε αύξουσα σειρά.

2. **ΑΕΡ (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 $a$;

Απάντηση:

Μπορούμε να έχουμε από $0$ έως $n$ εμφανίσεις μιας δεδομένης τιμής $a$ στην ακολουθία. Επομένως, για δεδομένο $a$ η $\pi(a; x^n)$ μπορεί να πάρει $n+1$ τιμές. Οι συνδυασμοί για όλες τις $|\mathcal{X}|$ τιμές του $a$ είναι $(n+1)^{|\mathcal{X}|}$.

Παρατηρήστε ότι εάν γνωρίζουμε τις τιμές της $\pi(a; x^n)$ για $|\mathcal{X}|-1$ τιμές του $a$ η τιμή της $\pi(a; x^n)$ για την τιμή της $a$ που απομένει μπορεί να προσδιοριστεί με μοναδικό τρόπο (δεδομένου ότι το μήκος της ακολουθίας είναι σταθερό και ίσο με $n$). Επομένως, ο αριθμός όλων των πιθανών τύπων για ακολουθίες μήκους $n$ δεν μπορεί να υπερβεί την τιμή $(n+1)^{|\mathcal{X}|-1}$.

(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:* $R \triangleq \frac{\log M}{n}$.

Απάντηση:

$M = (n+1)^{|\mathcal{X}|}$. Συνεπώς,

$$R = \frac{\log M}{n} = \frac{\log(n+1)^{|\mathcal{X}|}}{n} = \frac{|\mathcal{X}| \log(n+1)}{n} \to 0 \text{ για } n \to \infty.$$

(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 $\epsilon > 0$,

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

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

Απάντηση:

Το σύνολο $A_\epsilon^{(n)}$ των ασθενώς τυπικών ακολουθιών αποτελείται από τις ακολουθίες που ικανοποιούν τη σχέση

$$h(X) - \epsilon \le -\frac{1}{n} \log f(x^n) \le h(X) + \epsilon.$$

Ισοδύναμα,

$$-\frac{1}{n} \log\left( c^n 2^{-\sum_{i=1}^n x_i^4} \right) \le h(X) + \epsilon \Rightarrow$$

$$-\log c + \frac{1}{n} \sum_{i=1}^{n} x_i^4 \le h(X) + \epsilon \Rightarrow$$

$$\frac{1}{n} \sum_{i=1}^{n} x_i^4 \le h(X) + \log c + \epsilon.$$

Γνωρίζουμε, επίσης, ότι, όταν $n \to \infty$, για οποιοδήποτε $\epsilon > 0$ και για οποιαδήποτε ακολουθία $x^n$ ισχύει ότι

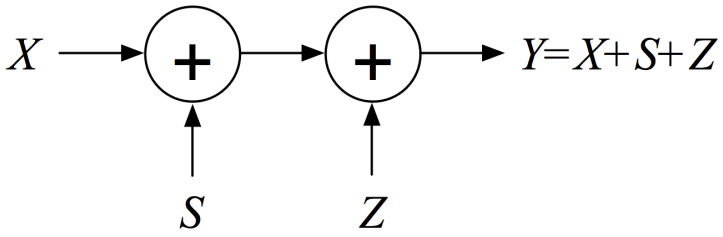
$$\Pr\{x^n \in A_\epsilon^{(n)}\} \to 1.$$

Επομένως, για $n \to \infty$,

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

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

Θεωρούμε μετάδοση σε Γκαουσιανό Κανάλι με ισχύ $\mathbb{E}[X^2] = P$. 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 $0$;

Απάντηση:

Δεδομένου ότι οι $S$ και $Z$ είναι ανεξάρτητες, το κανάλι είναι Γκαουσιανό με θόρυβο $\mathcal{N}(0, N_z + N_s)$. Συνεπώς,

$$R_1 = \frac{1}{2}\log\left(1 + \frac{P}{N_z + N_s}\right) \text{ bits ανά χρήση καναλιού.}$$

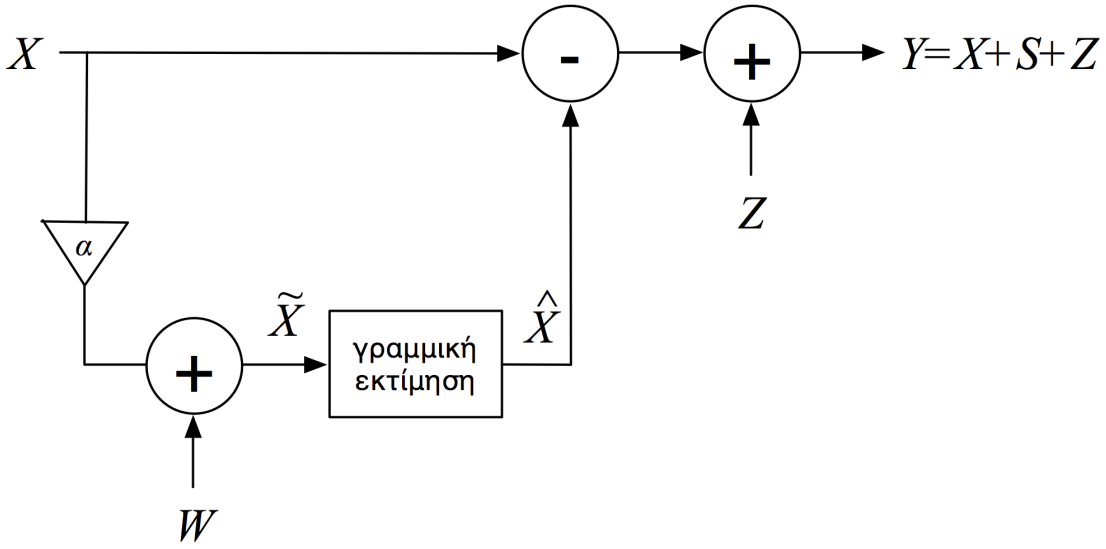
Ο ρυθμός μετάδοσης είναι πάντοτε μεγαλύτερος από το $0$ αν και για πολύ μεγάλο $N_s$ τείνει στο $0$.

(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)

Απάντηση:

Με πράξεις,

$$\begin{aligned} Y &= X + S + Z \\ &= X + \hat{X} + Z \\ &= X - \frac{\alpha P}{\alpha^2 P + N_w}\tilde{X} + Z \\ &= X - \frac{\alpha P}{\alpha^2 P + N_w}\alpha X + \frac{\alpha P}{\alpha^2 P + N_w} W + Z \\ &= \frac{N_w}{\alpha^2 P + N_w} X + \frac{\alpha P}{\alpha^2 P + N_w} W + Z. \end{aligned}$$

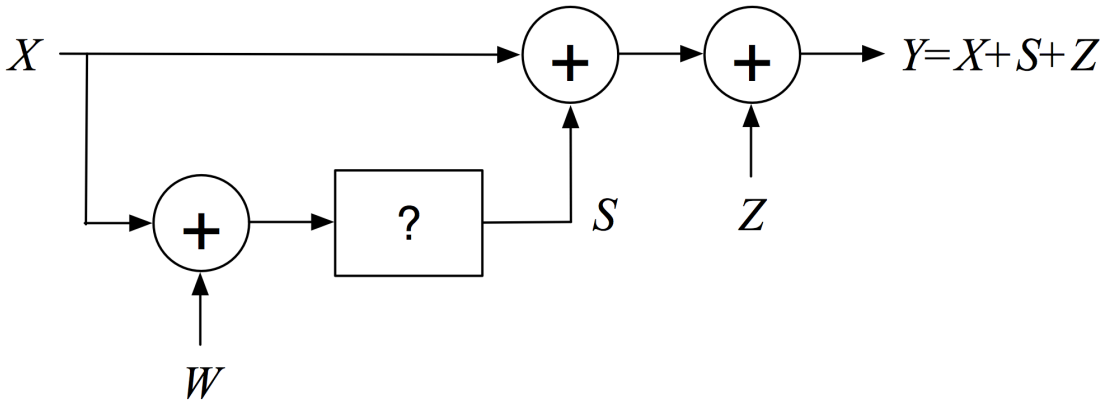
Επομένως, το κανάλι ισοδυναμεί με Γκαουσιανό κανάλι με ισχύ πομπού $\frac{N_w^2}{(\alpha^2 P + N_w)^2} P$ και διασπορά (Γκαουσιανού) θορύβου ίση με $N_z + \frac{\alpha^2 P^2}{(\alpha^2 P + N_w)^2} N_w$. Συνεπώς,

$$\begin{aligned} R_2 &= \frac{1}{2} \log \left( 1 + \frac{\frac{N_w^2}{(\alpha^2 P + N_w)^2} P}{N_z + \frac{\alpha^2 P^2}{(\alpha^2 P + N_w)^2} N_w} \right) \\ &= \frac{1}{2} \log \left( 1 + \frac{N_w^2 P}{N_z (\alpha^2 P + N_w)^2 + \alpha^2 P^2 N_w} \right) \text{ bits ανά χρήση καναλιού.} \end{aligned}$$

Για $\alpha \to \infty$ (ή εάν $N_w \to 0$), $R_2 \to 0$. Το αποτέλεσμα είναι λογικό. Όσο καλύτερη είναι η εκτίμηση του $X$ τόσο καλύτερα μπορούμε να το αφαιρέσουμε από το κανάλι. Στο όριο, αφαιρούμε το $X$ και απομένει μόνο θόρυβος.

(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.

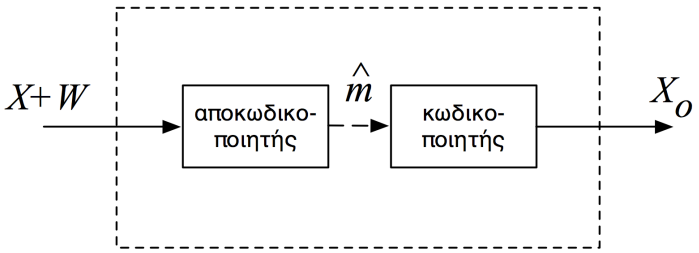
• Ο παρεμβολέας είναι τέλεια συγχρονισμένος με τον πομπό, δηλαδή γνωρίζει πότε ξεκινά η μετάδοση κάθε κωδικής λέξης.

• 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.

Απάντηση:

Ο πομπός μεταδίδει με ρυθμό μετάδοσης $\leq \frac{1}{2}\log\left(1+\frac{P}{N_w}\right)$. Επομένως, από το σήμα $X+W$, για κάθε $n$ σύμβολα, μπορούμε να βρούμε ποιο είναι το μήνυμα που μετέδωσε ο πομπός. Στη συνέχεια, επανακωδικοποιούμε το μήνυμα. Αυτό έχει ως αποτέλεσμα η έξοδος του κουτιού να είναι ακριβώς ίδια με το . Επομένως, θέτουμε $S = X_o$, όπου $X_o$ είναι η έξοδος του κωδικοποιητή καναλιού του κουτιού (ο οποίος είναι ο ίδιος με τον κωδικοποιητή που χρησιμοποιεί ο πομπός). Τελικά, ο δέκτης λαμβάνει $Y = Z$, με αποτέλεσμα να έχουμε $R_3 = 0$. Τα παραπάνω απεικονίζονται στο Σχήμα 4.




Σχήμα 4: Υλοποίηση συστήματος.

Παρατηρήστε ότι, σε αντίθεση με το προηγούμενο ερώτημα, επιτυγχάνουμε $R_3$ ακριβώς ίσο με $0$ παρόλο που οι μετρήσεις που έχουμε (τα $X+W$) είναι ενθόρυβες. Ωστόσο, δεν είναι περισσότερο ενθόρυβες από το $Y$, με αποτέλεσμα ο παρεμβολέας να μπορεί να δράσει ως δέκτης.

Εναλλακτική λύση (από συναδέλους σας)!

Μια ακόμα πιο απλή λύση είναι να αντιστρέψουμε την είσοδο του κουτιού! Δηλαδή, $S = (-1)\cdot(X+W)$! Με αυτόν τον τρόπο, $Y = W + Z$, δηλαδή η έξοδος, $Y$, περιέχει μόνο θόρυβο.

Εκ πρώτης όψεως φαίνεται περίεργο που ένας τόσο απλός τρόπος είναι εξίσου αποδοτικός με τον τρόπο που συνδυάζει αποκωδικοποίηση και επανακωδικοποίηση. Ωστόσο, σε αυτό το πρόβλημα δε μας ενδιαφέρει να βρούμε το $X$. Μας αρκεί να βλάψουμε τον πομπό. Στο Ερώτημα (β) προσπαθούμε να βρούμε όσο το δυνατόν καλύτερα το $X$ (χωρίς να χρησιμοποιήσουμε γνώση του βιβλίου κωδίκων). Ο εκτιμητής είναι βελτιστοποιημένος ως προς το κριτήριο της ελαχιστοποίησης του

μέσου τετραγωνικού σφάλματος μεταξύ του $X$ και της εκτίμησης του παρεμβολέα. Ωστόσο, στο συγκεκριμένο πρόβλημα, κριτήριό μας δεν είναι να βρούμε το σωστό $X$, αλλά να το απαλείψουμε. Με την απλή αντιστροφή του $X + W$ δεν μπορούμε μεν να εκτιμήσουμε το $X$ εξίσου καλά με το Ερώτημα (β), αλλά επιτυγχάνουμε το στόχο μας, ο οποίος είναι να απαλείψουμε πλήρως το $X$ από την έξοδο $Y$.

**Η ΣΕΛΙΔΑ ΑΥΤΗ ΕΙΝΑΙ ΚΕΝΗ ΕΣΚΕΜΜΕΝΑ**