Συναρτήσεις & Κέρματα

1. Η Πέππα και η Σούζυ έχουν δύο κέρματα, ένα σωστά φτιαγμένο (με πιθανότητα να φέρει 1 ίση με $p = \frac{1}{2}$), και ένα ελατωματικό, με πιθανότητα να φέρει 1 ίση με πιθανότητα $q \neq \frac{1}{2}$. Δυστυχώς, καθώς έπαιζαν, τα δύο κέρματα μπλέχτηκαν ώστε δεν μπορούν πλέον να ξεχωρίσουν ποιό είναι ποιό. Υπάρχει τρόπος ώστε να διεξάγουν ρίψεις ώστε το αποτέλεσμα να είναι ίσο με 1 με πιθανότητα ακριβώς $\frac{1}{2}$;

   Λύση: Έστω $\Pr[b_A = 1] = p$ και $\Pr[b_B = 1] = q$.

   Από τον πίνακα αληθείας της αποκλειστικής διάζευξης έχουμε ότι $\Pr[b = 1] = \Pr[b_A = 1 \wedge b_B = 0] + \Pr[b_A = 0 \wedge b_B = 1]$. Άρα: $\Pr[b = 1] = p \cdot (q-1) + (p-1) \cdot q = p \cdot q - p + p \cdot q - q = 2p \cdot q - p - q$.

2. Σε μία συσκευή υπάρχει μια γεννήτρια τυχαίων αριθμών η οποία σε κάθε κλήση επιστρέφει ένα τυχαίο bit. Στις προδιαγραφές της συσκευής, η γεννήτρια επιστρέφει 1 με πιθανότητα $\frac{1}{2}$.

   Δυστυχώς, για λόγους κόστους, ο Βασίλης προμηθεύτηκε συσκευές Β΄ διαλογής, στις οποίες η γεννήτρια επιστρέφει 1 με πιθανότητα $\frac{1}{2} + \delta$, όπου $0 < \delta < \frac{1}{2}$.

   (α΄) Ο Βασίλης πιστεύει ότι μπορεί να βελτιώσει την συμπεριφορά της γεννήτριας εάν κάθε φορά που χρειάζεται ένα bit καλεί τη γεννήτρια δύο φορές και κάνει XOR τα αποτελέσματα. Εξηγήστε τι σημαίνει «βελτιώσει» τη συμπεριφορά, και εξετάστε (αυστηρά) αν η διαίσθηση του Βασίλη είναι σωστή.

   (α΄) Η συμπεριφορά θα «βελτιωθεί» αν το αποτέλεσμα της διαδικασίας εμφανίζει μικρότερη "απόσταση" (στα επόμενα μαθήματα θα ορίσουμε τυπικά τη στατιστική απόσταση) από την ομοιόμορφη από το δ που πετύχαμε με την απλή χρήση της γεννήτριας. Άρα θα υπολογίσουμε την απόσταση από την ομοιόμορφη κατανομή της ιδέας του Βασίλη, και θα τη συγκρίνουμε με το δ.
   Έστω Y μια μεταβλητή που ακολουθεί την κατανομή της (Β' διαλογής) γεννήτριας (πέρα από την X που ορίσαμε ήδη). Θεωρήσαμε δύο διαφορετικές μεταβλητές για να αναπαραστήσουμε τις δύο διαφορετικές κλήσεις που θα γίνουν στη γεννήτρια. Η πρόταση του Βασίλη είναι ισοδύναμη με το να χρησιμοποιήσει τη μεταβλητή $Z := X \oplus Y$. Μένει να υπολογίσουμε τις πιθανότητες $\Pr[Z = 0], \Pr[Z = 1]$ και να υπολογίσουμε την απόσταση από την ομοιόμορφη οπως παραπάνω. Έχω:

$$
\begin{aligned}
&\Pr[Z = 0] = \Pr[((X = 0) \cap (Y = 0)) \cup ((X = 1) \cap (Y = 1))] \\
=&\Pr[(X = 0) \cap (Y = 0)] + \Pr(X = 1) \cap (Y = 1), \text{ αφού τα δύο γεγονότα είναι ξένα.} \\
=&\Pr[X = 0] \cdot \Pr[Y = 0] + Pr[X = 1] \cdot \Pr[Y = 1], \text{ αφού τα γεγονότα είναι ανεξάρτητα.} \\
=&\left(\frac{1}{2} - \delta\right)^2 + \left(\frac{1}{2} + \delta\right)^2 \\
=&\frac{1}{4} - \delta + \delta^2 + \frac{1}{4} + \delta + \delta^2 \\
=&\frac{1}{2} + 2\delta^2
\end{aligned}
$$

   Προφανώς, $\Pr[Z = 1] = 1 - \frac{1}{2} + 2\delta^2 = \frac{1}{2} - 2\delta^2$.
   Άρα, η ιδέα του Βασίλη, επιστρέφει 1 με απόκλιση $2\delta^2$ από το ιδανικό, αντί δ που είχαμε αρχικά. Στην σκέψη αυτή μας βοηθά ότι για την παραγωγή ενός bit, υπάρχουν μόνο δύο ενδεχόμενα τα οποία αναγκαστικά είναι συμπληρωματικά. Άρα, αρκεί να μελετήσουμε το ένα από αυτά (π.χ. την πιθανότητα να παραχθεί το 1).
   Μένει να συγκρίνουμε το δ με το $2\delta^2$. Γνωριζουμε από την εκφώνηση ότι $0 < \delta < \frac{1}{2}$ άρα αφού δ θετικό $\delta^2 < \frac{1}{2}\delta$ άρα $2\delta^2 < \delta$, οπότε η πρόταση του Βασίλη είναι βάσιμη.

3. Στο παράδειγμα που εξετάσαμε στο μάθημα, θεωρήσαμε ότι αρκεί μονάχα η Αλίκη να χρησιμοποιήσει σχήμα δέσμευσης για το μηνυμά της –αφού μιλάει πρώτη, ενώ ο Βασίλης δεν χρειάζεται.

   Ο Βασίλης προτείνει για λόγους συμμετρίας να στέλνει και αυτός μια δέσμευση αντί για το αρχικό μήνυμα του, και αναλόγως να προστεθεί ένας τέταρτος γύρος στον οποίο «ανοίγει» τη δεσμευσή του.

   Είναι ασφαλής η παραλλαγή του Βασίλη;

   Υπόδειξη. Θεωρήστε ότι η Αλίκη κερδίζει το παιχνίδι όταν το αποτέλεσμα είναι 1.

   Σημείωση. Ακόμα δεν έχουμε δει αυστηρά τη σύνταξη ενός σχήματος δέσμευσης, οπότε μπορείτε να χρησιμοποιήσετε ένα απλουστευμένο υποθετικό σχήμα όπου το $Com(a) \to (c, r)$ παράγει μια δέσμευση c στην τιμή a και μια απόδειξη r, ενώ το $Ver(a, c, r) \to \{0, 1\}$ ελέγχει εάν πράγματι το c περιέχει το a με βάση το r.

4. Έστω f, g δύο αμελητέες συναρτήσεις (βλ. ορισμό 2.6.3). Δείξτε ότι οι συναρτήσεις $h_1 := f + g$ και $h_2 := f \cdot g$ είναι επίσης αμελητέες. Επίσης, εάν το $q(x)$ είναι πολυώνυμο, δείξτε ότι η συνάρτηση $q \cdot f$ είναι και αυτή αμελητέα.

   Λύση

   Από τον ορισμό, μια συνάρτηση f είναι αμελητέα εάν για κάθε c υπάρχει n_0 ώστε για κάθε $n > n_0$:

   $$f(n) \leq \frac{1}{n^c}$$

   - Για την $f \cdot g$. Έστω κάποιο c_*, θα βρούμε κατάλληλο n_* ώστε για κάθε $n > n_*$:

     $$f(n) \leq \frac{1}{n^c}$$

     Για το συγκεκριμένο c_*, αφού η f είναι αμελητέα υπάρχει n_f τέτοιο ώστε για κάθε $n > n_*$:

     $$f(n) \leq \frac{1}{n^c}$$

     Επίσης, η g είναι αμελητέα, οπότε για $c = 0$ υπάρχει n_g ώστε για κάθε $n > n_g$:

     $$g(n) \leq \frac{1}{n^0}$$
     $$g(n) \leq 1$$

     Από τα προηγούμενα έχουμε ότι για $n_* = \max\{n_g, n_f\}$ ισχύει ότι για κάθε $n > n_*$:

     $$f(n) \cdot g(n) \leq \frac{1}{n^c} \cdot 1$$

   - Για την $f + g$:
     Έστω κάποιο c_p, θα βρούμε κατάλληλο n_p.
     Θεωρούμε το $c_p + 1$, και προσδιορίζουμε κατάλληλα n_f, n_g ώστε για $n > \max\{n_f, n_g\}$:

     $$f(n) \leq \frac{1}{n^{c_p+1}}$$
     $$g(n) \leq \frac{1}{n^{c_p+1}}$$

     Θέτουμε $n_{max} = \max(n_f, n_g, 2)$. Τότε έχουμε για όλα τα $n > n_{max}$:

     $$f(n) \leq \frac{1}{2 \cdot n^{c_p}}$$

$$g(n) \leq \frac{1}{2 \cdot n^{c_p}}$$

και άρα:

$$f(n) + g(n) \leq \frac{1}{n^{c_p}}$$

- Για την $f \cdot q$:
  Έστω κάποιο c'', θα βρούμε κατάλληλο n''.
  Το q θα έχει κάποιο βαθμό d, άρα για μεγάλα n (μεγαλύτερα από κάποιο n_s) θα ισχύει:

$$\forall n > n_q : q(n) < n^{d+1}$$

  Αφού f αμελητέα, για το $n^{c''+d+1}$ θα υπάρχει n_s τέτοιο ώστε:

$$\forall n > n_s : f(n) < \frac{1}{n^{c''+d+1}}$$

  Οπότε, για $n'' = \max\{n_q, n_s\}$ έχουμε:

$$\forall n > n'' : f(n) \cdot q(n) < \frac{n^{d+1}}{n^{c''+d+1}}$$