

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 $\frac{1}{2}$;
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.
3. Στο παράδειγμα που εξετάσαμε στο μάθημα, θεωρήσαμε ότι αρκεί μονάχα η Αλίκη να χρησιμοποιήσει σχήμα δέσμευσης για το μήνυμά 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 μήνυμά 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 $Com(a) \rightarrow (c, r)$ παράγει μια δέσμευση c στην τιμή a και μια απόδειξη r , ενώ το $Ver(a, c, r) \rightarrow \{0, 1\}$ 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.