

Ομάδες & 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 ελαττωματικό, 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 ποιο είναι ποιο. 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. 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 μήνυμά του, και αναλόγως να προστεθεί ένας τέταρτος γύρος στον οποίο «ανοίγει» τη δεσμευσή του.

Είναι ασφαλής η παραλλαγή του Βασίλη;

3. Να δείξετε ότι το σύνολο των συμβολοσειρών μήκους 2 bit (“00”, “10”, “01”, “11”), με πράξη το XOR κατά συντεταγμένη, αποτελεί ομάδα.

Λύση Ελέγχουμε ότι οι ιδιότητες της ομάδας ισχύουν:

- Έστω ένα ζεύγος συμβολοσειρών “ab”, “cd”. Το αποτέλεσμα της πράξης μεταξύ τους θα είναι “ef” όπου $e = a \text{ XOR } c$ και $f = b \text{ XOR } d$. Με έλεγχο του πίνακα τιμών της XOR επιβεβαιώνουμε ότι το XOR δύο bits είναι bit, οπότε θα ισχύει ότι το e και το f είναι bits.
- Η μεταθετικότητα της ομάδας προκύπτει από το ότι το XOR είναι μεταθετικό, και η ιδιότητα διατηρείται κάνοντας πράξεις ανα συντεταγμένη (όπως παραπάνω)
- Υπάρχει ουδέτερο στοιχείο και είναι το “00”, αφού ισχύει ότι $a \text{ XOR } 0 = a$, και η ιδιότητα διατηρείται κάνοντας πράξεις ανα συντεταγμένη (όπως παραπάνω).

4. Μελετήστε τον ορισμό της μεταθετικότητας και κυκλικότητας από τις σημειώσεις. Να δείξετε ότι η παραπάνω ομάδα είναι μεταθετική αλλά όχι κυκλική.

Λύση

- Η μεταθετικότητα της ομάδας προκύπτει από το ότι το XOR είναι μεταθετικό.
 - Η ομάδα δεν είναι κυκλική: για κάθε συμβολοσειρά bits ισχύει ότι το XOR με τον εαυτό της παράγει μηδενικά. Άρα κάθε στοιχείο έχει τάξη το πολύ 2 $\neq 4$, οπότε δεν υπάρχει στοιχείο που να παράγει την ομάδα.
5. Έστω ομάδα $(\mathbb{G}, *)$ τάξης q , όπου το q έχει μήκος λ bits. Για ένα στοιχείο της ομάδας a , γράφουμε $a^2 := a * a$ κ.ο.κ. Για οποιοδήποτε $x \in \mathbb{Z}_q$, δείξτε ότι μπορούμε να υπολογίσουμε το a^x σε χρόνο πολυωνυμικό ως προς το λ .

Γράφουμε το ανάπτγμα του x στο δυαδικό:

$$x = \sum_{i=0}^{i=\lambda-1} 2^i \cdot x_i, \text{ όπου } x_i \in \{0, 1\}$$

Αντίστοιχα, μπορούμε να αναλύσουμε το g^x :

$$g^x = \prod_{i=0}^{i=\lambda-1} a^{2^i \cdot x_i}, \text{ όπου } x_i \in \{0, 1\}$$

Επιπλέον, παρατηρούμε ότι $a^{2^i \cdot x_i} = a^{2^i}$ όταν $x_i = 1$ και $a^{2^i \cdot x_i} = \epsilon$ όταν $x_i = 0$.

Άρα, για να υπολογίσουμε το δεξί μέλος αρκεί:

- Να υπολογίσουμε τους όρους $a^2, a^4, \dots, a^{2^{\lambda-1}}$. Αυτό επιτυγχάνεται με $\lambda - 1$ εφαρμογές της πράξης της ομάδας (μία για κάθε τετραγωνισμό).
- Να υπολογίσουμε τους όρους $a^{2^i \cdot x_i}$ έχοντας διαθέσιμα τα a^{2^i} . Αυτό επιτυγχάνεται χωρίς επιπλέον υπολογισμό.
- Να πολλαπλασιάσουμε τους όρους που δεν είναι ουδέτεροι. Αυτοί θα είναι το πολύ λ όροι, ενώ για τυχαίο x θα είναι κατα μέσο όρο $\frac{\lambda}{2}$.

Συνολικά, χρειαζόμαστε το πολύ $2\lambda - 2$ πολλαπλασιασμούς, και σε μια μέση περίπτωση $\frac{3\lambda}{2}$.

Σημείωση: Δεν είναι αποτελεσματικό να πολλαπλασιάσουμε το a με τον εαυτό του x φορές: ένας αριθμός με μήκος λ bits έχει στη γενική περίπτωση τιμή $\approx 2^\lambda$, το οποίο είναι εκθετικό στο λ , και άρα υπολογιστικά απαγορευτικό.

6. 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.

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:

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