אלגוריתמיקה - סמסטר 2006ב - פתרון שאלות נבחרות מתוך ממ"ן 15

פתרון שאלה 1

א. נסמן ב-n את מספר הצמתים בגרף הקלט.

קיימות 3^n צביעות אפשריות, ולכן האלגוריתם ישתמש ב- 3^n מעבדים ובמערך בגודל 3^n. (אפשר למַספר את צמתי הגרף ואת שלושת הצבעים, וכך למַספר את 3^n הצביעות. נניח למשל שבגרף יש ארבעה צמתים ושלושת הצבעים הם אדום, כחול וצהוב. מעבד מס' 1233 יבדוק את הצביעה שבה הצומת v_1 צבוע באדום, v_2 צבוע בכחול, v_3 צבוע בצהוב ו- v_4 צבוע גם-כן בצהוב.)

האלגוריתם יתבצע בשני שלבים:

בשלב הראשון תיבדק חוקיות הצביעות. המעבד ה-i יבדוק אם הצביעה ה-i היא חוקית וירשום את תוצאת הבדיקה במקום ה-i במערך. הזמן שיידרש לביצוע שלב זה הוא $O(n^2)$, מפני שכדי לבדוק אם צביעה מסוימת היא חוקית צריך לעבור על כל קשתות הגרף, ולבדוק אם שני הצמתים שבקצות הקשת צבועים בצבעים שונים.

בשלב השני צריך לבדוק אם אחד המעבדים מצא צביעה חוקית. נשים לב, שלפי תנאֵי השאלה אין שיתוף בכתיבה ולכן אי אפשר להשתמש במשתנה משותף. כלומר, מעבד שמצא צביעה חוקית לא יוכל פשוט להחזיר True. לכן, כדי לבדוק אם אחד המעבדים מצא צביעה חוקית, האלגוריתם "יבנה" עץ בינרי, שהעלים שלו הם הערכים הבולאניים הכתובים במערך. בשלב זה האלגוריתם יפעל כמו אלגוריתם סיכום המשכורות המתואר בספר (פרט לכך שהאופרטור שיופעל על כל זוג צמתים בעץ יהיה OR ולא +). קיימת צביעה חוקית של הגרף בשלושה צבעים אם ורק אם ערכו של שורש העץ יהיה True. הזמן שיידרש לביצוע שלב זה הוא $\log_2 3^n = n \cdot \log_2 3 = O(n)$.

לפיכך, זמן הריצה הכולל של האלגוריתם יהיה $O(n) + O(n^2) = O(n^2)$.

ב. נניח שקיים אלגוריתם מקבילי R הפותר איזושהי בעיה NP-שלמה בזמן פולינומיאלי ובאמצעות מספר פולינומיאלי של מעבדים. ניתן לבצע סימולציה של R באמצעות אלגוריתם סדרתי. כלומר, מעבד אחד יכול לבצע (בסדר המתאים) את תפקידיהם של כל המעבדים שבהם משתמש R.

מכיוון שמספר מעבדים שבהם משתמש R הוא פולינומיאלי וזמן הריצה הכולל של R הוא פולינומיאלי, ברור שזמן הריצה של האלגוריתם הסדרתי יהיה גם כן פולינומיאלי.

כלומר, האלגוריתם הסדרתי פותר בעיה NP-שלמה בזמן פולינומיאלי, ומכך נובע ש- P = NP.

פתרון שאלה 4

א. המנגנון של חתימה אלקטרונית במערכת מפתח-ציבורי מוסבר בפרוטרוט בעמ' 316 בספר.

ב. הדרישות ממנגנון של חתימה אלקטרונית:

1. רק מקבל ההודעה יוכל לפענח אותה;
2. מקבל ההודעה יהיה בטוח באותנטיות של החתימה;
3. השולח לא יוכל להתכחש לחתימה;
4. מקבל ההודעה לא יוכל לחתום על הודעות אחרות בשם השולח;
5. מקבל ההודעה לא יוכל לשנות את ההודעה החתומה;
6. מקבל ההודעה לא יוכל לשלוח את ההודעה החתומה לצד ג'.

דרישות 1-5 מתמלאות במערכת של מפתח-ציבורי (זה נובע ישירות מאופן פעולת מנגנון החתימה).
כדי שגם דרישה 6 תתמלא, השולח צריך לרשום בגוף ההודעה שהיא מיועדת לנמען הספציפי.

פתרון שאלה 5

בועז יקנה שני עטים – עט ירוק ועט אדום.
הוא יציג בפני איה את אחד משני העטים ויבקש ממנה לומר מה צבעו.
אם איה איננה עיוורת-צבעים, היא תענה את התשובה הנכונה בוודאות.
לעומת זאת, אם היא עיוורת-צבעים, יש לה סיכוי של 50% לנחש נכון.
כדי שבועז ישתכנע בהסתברות הגדולה מ- 0.999 שאיה איננה עיוורת-צבעים, עליו לחזור על הניסוי 10 פעמים (לכל היותר). בכל פעם הוא יחליט איזה עט להציג בפני איה באופן אקראי (באמצעות הטלת מטבע).
אם איה תטעה באחת הפעמים, אז ברור שהיא עיוורת-צבעים. לעומת זאת, אם איה תצליח לנחש את צבע העט בכל הפעמים, אז הסיכוי שהיא עיוורת צבעים הוא $\left(\frac{1}{2}\right)^{10}$, כי הניסויים הם בלתי תלויים.
לכן, אם איה תצליח לנחש את צבע העט בכל הפעמים, הסיכוי שהיא איננה עיוורת צבעים הוא

$$1-\left(\frac{1}{2}\right)^{10}=1-\frac{1}{1024}>1-\frac{1}{1000}=0.999.$$