**סמסטר ב', מועד א', תשע"ה**
**0368-4435-01**
**תאריך הבחינה: 26 ביולי 2015**

**<u>מבחן בית בקורס הסקה אוטומטית לצורך ניתוח תוכניות</u>**
**<u>פרופ' מולי שגיב</u>**

משך הבחינה 10 ימים מיום קבלתה.
הבחינה היא בחינת כבוד. הינך מתבקש לחתום על ההצהרה הבאה:
"אני מצהיר/ה שביצעתי הבחינה בעצמי וללא עזרה מגורם כלשהוא". על החתום_____.
הבחינה היא עם חומר פתוח. מותר להיעזר בכל חומר רלבנטי.
בכל הסעיפים חשוב לנמק את הסיבה עם הסבר, הוכחה ו/או דוגמא
**בהצלחה!**

**יש לענות על 5 מתוך 6 השאלות הבאות. משקל כל השאלות שווה.**

## <u>שאלה 1 (shape analysis)</u>

א. נאמר ששני מצביעים (pointers) p ו- q הם שווים בהחלט (must-alias) בנקודה l בתוכנית, אם בכל ביצוע של התוכנית מתקיים שבנקודה l, p ו-q מצביעים לאותה כתובת.
הסבר כיצד ניתן לקרוא מן התוצאה של TVLA אם p ו- q הם must-alias בנקודה l.
ב. תן דוגמא לתוכנית עבורה p ו- q הם must-alias בנקודה מסוימת, אבל TVLA לא תצליח לגלות זאת. האם יתכן מצב הפוך, כלומר ש- TVLA תדווח ש- p ו- q הם must-alias אפילו שהדבר אינו נכון?
ג. נאמר ששני מצביעים (pointers) p ו- q יתכן שהם שווים (may-alias) בנקודה l בתוכנית, אם קיים ביצוע של התוכנית שבו בנקודה l, p ו-q מצביעים לאותה כתובת.
הסבר כיצד ניתן לקרוא מן התוצאה של TVLA אם p ו- q הם may-alias בנקודה l.
ד. האם קיימת דוגמא עבורה p ו- q הם may-alias בנקודה מסוימת, אבל TVLA לא תצליח לגלות זאת?
ה. האם ניתן להשתמש ב- TVLA כדי לגלות תוכניות שמבצעות פעמיים ברצף שחרור זיכרון (קריאה ל- free)?
ו. האם יתכנו שתי תוכניות שקולות שבאחת מהן TVLA מצליחה להוכיח שהתוכנית אינה מבצעת null-dereference ובשנייה TVLA נכשלת?
ז. האם TVLA תצליח להוכיח שהתוכנית הבאה תחזיר false כאשר startNode מצביע על רשימה לא מעגלית:

```
boolean hasLoop(Node startNode) {
    Node slowNode = startNode;
    Node fastNode1 = startNode;
    Node fastNode2 = startNode;
    while (slowNode &&
           fastNode1 = fastNode2.next() &&
           fastNode2 = fastNode1.next()) {
        if (slowNode == fastNode1 || slowNode == fastNode2)
            return true;
        slowNode = slowNode.next();
    }
    return false;
}
```

## שאלה 2 (SMT)

1. פרטי צעד-אחר-צעד את פעולת תהליך Nelson-Oppen כדי למצוא האם הנוסחה הבאה ספיקה, מעל תאוריית הרשימות (lists) ה integers וה uninterpreted functions:

$$x \le y \wedge y \le x + car(cons(0,z)) \wedge f(h(x)-h(y))=1 \wedge f(0)=0$$

2. הסבירי את כל המקרים בהם תהליך Nelson-Oppen אינו שלם ותני דוגמה לכל אחד מהמקרים.

## שאלה 3 (concolic exectution)

הדגימי ביצוע קונקולי (concolic execution) של הפונקציה h בקוד הבא (הניחי שבהרצה הראשונה, שני הפרמטרים מקבלים את הערך אפס). האם השגיאה תתגלה?

```
int f(int x) {return 2 * x;}
01 int h(int x, int y) {
02     if (x != y)
03         if (f(x) == x + 10)
04             error();
05     return 0;
06 }
```

## שאלה 4 (WP)

1. הרחיבי את כללי ה WP לתוכניות עם שגרות פנימיות (פרוצדורות). הניחי שלכל שגרה נתונים pre-condition ו post-condition, שמשתמשים בפרמטרים הפורמליים ובערך החזרה כדי להגדיר מה השגרה מניחה על ערכי הפרמטרים ומה היא מבטיחה על ערך החזרה.

2. הדגימי הוכחה בעזרת הכללים על התכנית הבאה:

```
bool is_even(unsigned int n) {
    if (n == 0)return true;
    else {unsigned int m; m = n - 1; return is_odd(m); }
}
bool is_odd(unsigned int n) {
    if (n == 0) return false;
    else {unsigned int m; m = n - 1; return is_even(m); }
}
void main() {
    unsinged int x;
    assert ((is_even(x) &&  !is_odd(x)) ||
            (!is_even(x) && is_odd(x)));
}
```

**שאלה 5 (SAT)**

1. תני דוגמא לנוסחה פסוקית שעבורה non-chronological-backtracking מוביל לחיסכון משמעותי במספר האיטרציות של האלגוריתם.

2. תני דוגמא לנוסחה פסוקית שעבורה אלגוריתם DPLL מבצע מספר איטרציות גדול ככל האפשר (בשאיפה: אקספוננציאלי בגודל הנוסחה).

**שאלה 6 (points to analysis)**

השאלה מתייחסת לאנליזת may-points-to שנלמדה בכיתה, שמוצאת האם משתנה אחד יכול להצביע למשתנה אחר.

א. האם ההגדרה הבאה למשמעות האבסטרקטית של ההשמה p:=NULL* היא מונוטונית?
$[*p=NULL]\#\ (pt) = pt - \{(x,y) \mid (p,x) \in pt\}$

ב .האם ההגדרה בסעיף א. היא נאותה ,כלומר משמרת את הסמנטיקה הקונקרטית?

ג. נתבונן בהגדרה הבאה:
$[*p=NULL]\#\ (pt) = pt - \{(x,y) \mid (p,x) \in pt, \forall z: (p, z) \in pt \rightarrow z=x \}$
האם ההגדרה היא מונוטונית ?

ד. האם היא נאותה ?

ה. האם היא אופטימלית, כלומר induced ע"י האבסטרקציה ?

ו. האם קיימת דוגמא לתוכנית שבה יש הבדל בין אנליזת flow-sensitive ו- flow-insensitive ?
תזכורת: אנליזה flow-insensitive אינה מבצעת הורדות ומתעלמת ממשפטי בקרה.

**בהצלחה!**
**מולי ועודד**