(Draft 3)

เรื่องน่าอับอายของข้อสอบ สอวน. คอมพิวเตอร์ ศูนย์กรุงเทพฯ

โดย sleeepntsheep และ ccsleep

Permalink: https://firefly.gchan.moe/overflow.pdf

ข้อสอบภาคทฤษฎี กลางค่ายหนึ่ง 2567 ข้อที่สอง โจทย์ว่าไว้ดังนี้

จงหาผลลัพธ์จากโปรแกรมดังต่อไปนี้

```c
#include <stdio.h>

int main() {
  int y = 0;
  int sum =0;
  for (int x=0; x>-100; x--) {
    if(x%3==0)
      y=sum+x;
    sum +=y;
  }
  printf("%d", sum);
}
```

ขอการันตีคำตอบเลยว่า **อะไรก็ได้**!

ตามหลักมาตรฐานภาษาซีที่ defined ไว้ล่าสุด (C17 ตาม ISO/IEC9899:2017) กล่าวไว้ดังนี้

*“If an exceptional condition occurs during the evaluation of an expression (that is, if the result is not mathematically defined or not in the range of representable values for its type), the behavior is **undefined**.”*

ในเคสของ `int` ซึ่งเป็น signed integer การเกิด overflow นั้นไม่มีการ define ไว้อย่างแน่นอน เช่น

```c
#include <stdio.h>

main() {
  int x = 2147483647;
  x++; // should have been 2147483648
  printf("%d", x); // undefined!
}
```

กล่าวคือไม่สามารถเขียนจำนวน `2147483648` ใน integer ได้ เพราะเกิน range ของ signed integer ไปแล้ว (`-2147483648 <= x <= 2147483637`)

ดังนั้นเขาถือว่าเป็น undefined behavior นั่นคือ

undefined behavior

*behavior, upon use of a nonportable or erroneous program construct or of erroneous data, for which this International Standard **imposes no requirements**.*

แปลง่าย ๆ คือ **ทำอะไรก็ได้** เช่น ไม่ทำอะไรเลย ปริ้นตัวเลขตัวหนังสือมั่ว ๆ ออกมา ทำโปรแกรมให้ Crash หรืออาจปริ้น diagnostics ออกมาหรือไม่ก็ได้ (ไม่ได้กำหนดไว้เลย)

ดังนั้นจึงแนะนำให้ร้องเรียน เนื่องจากโจทย์นี้คำตอบตามหลัก C Standard มีไว้อย่างชัดเจนแล้ว คือตอบยังไงก็ถูก ส่งกระดาษเปล่า ๆ ไปก็ต้องให้ถูก

ข้อสอบไล่โค้ดที่ออกโดย อ.ธีรวัฒน์ มีลักษณะผิดอย่างร้ายแรง ไม่ว่าจะเป็น

- การไม่ใส่ `#include <stdio.h>` (โค้ดรันไม่ได้)
- การ access out-of-bound array (ถือว่าเป็น undefined behavior)

ตัวอย่างข้อสอบปี 2561

```
#include "stdio.h"
#include "conio.h"
int AB[3][3] = {1, 5, 7, 12, 4, 1, 6, 9, 2};

int funct1(int n) {
int x;
x = n * n + 1;
return x;
}

main() {
  int i, j, N = 5, L;
  char *p;
  char str[] = "COMPUTERILOVEYOU";
  p = str;
  for (i = 0; i <= 3; i++) {
    for (j = 0; j < 3; j++) {
      L = AB[i][j];
      if (L > (N + i + j))
        L = L % (N + 1) + 1;
      printf("%c", *p + L);
      p++;
    }
    printf("\n");
  }
  getch();
}
```

- signed integer overflow (ถือว่า undefined)

เพิ่มเติม

อนึ่ง unsigned integer หากตัวเลขเกิน ถูก define ไว้ใน standard ของ C ว่าเป็นมอดุโลของ 2^N เมื่อ N คือจำนวนบิตของประเภทข้อมูลนั้น (จึงไม่มีการ overflow)

```
#include <stdio.h>
main() {
  unsigned int x = 4294967295;
  x++;
  printf("%d", x); // defined as 0
}
```

เช่นนี้จึงจะบังคับว่าตอบ `0` ได้เลย