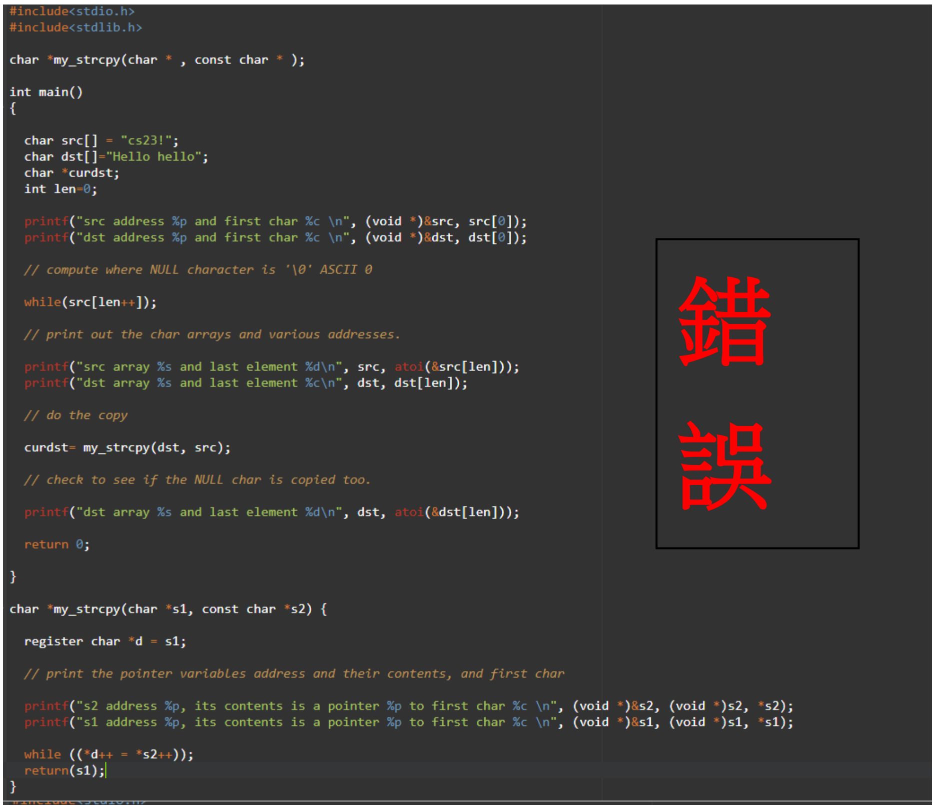
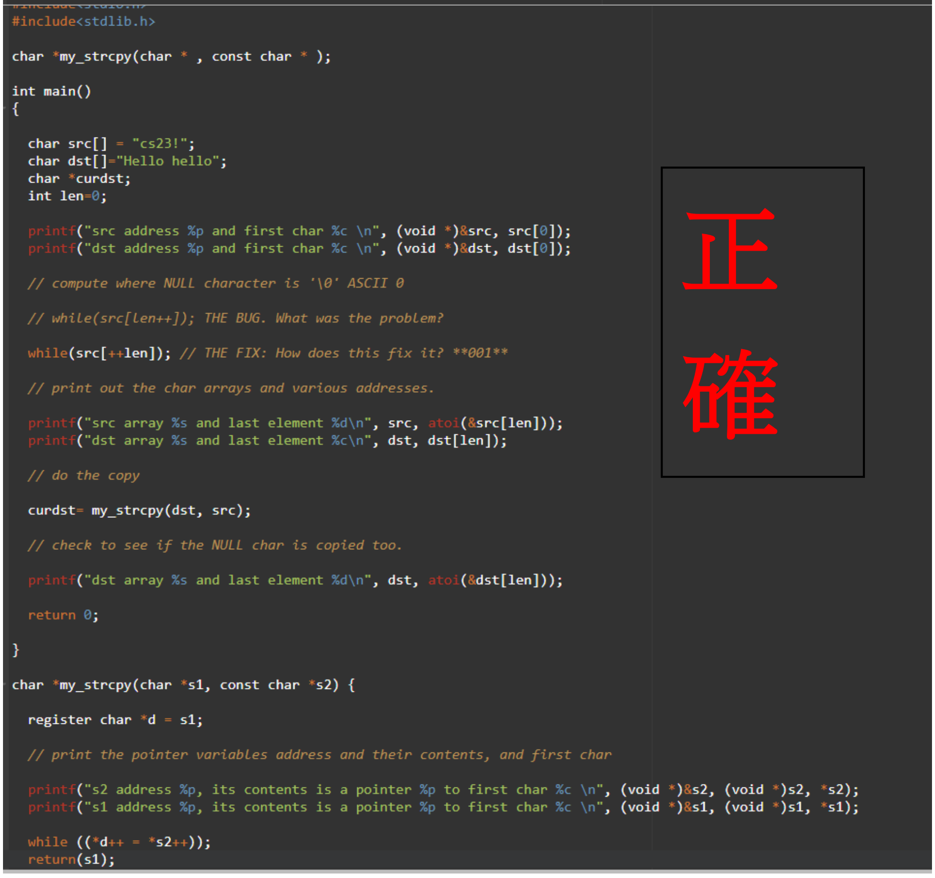
strcpy.c 觀察

B1029034 林奕安

下方是本次作業中程式碼裡有 bug 的程式與修正過後的程式，

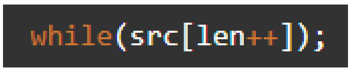


```c
#include<stdio.h>
#include<stdlib.h>

char *my_strcpy(char * , const char * );

int main()
{

  char src[] = "cs23!";
  char dst[]="Hello hello";
  char *curdst;
  int len=0;

  printf("src address %p and first char %c \n", (void *)&src, src[0]);
  printf("dst address %p and first char %c \n", (void *)&dst, dst[0]);

  // compute where NULL character is '\0' ASCII 0

  while(src[len++]);

  // print out the char arrays and various addresses.

  printf("src array %s and last element %d\n", src, atoi(&src[len]));
  printf("dst array %s and last element %c\n", dst, dst[len]);

  // do the copy

  curdst= my_strcpy(dst, src);

  // check to see if the NULL char is copied too.

  printf("dst array %s and last element %d\n", dst, atoi(&dst[len]));

  return 0;

}

char *my_strcpy(char *s1, const char *s2) {

  register char *d = s1;

  // print the pointer variables address and their contents, and first char

  printf("s2 address %p, its contents is a pointer %p to first char %c \n", (void *)&s2, (void *)s2, *s2);
  printf("s1 address %p, its contents is a pointer %p to first char %c \n", (void *)&s1, (void *)s1, *s1);

  while ((*d++ = *s2++));
  return(s1);
}
```

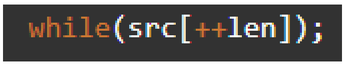


```c
#include<stdio.h>
#include<stdlib.h>

char *my_strcpy(char * , const char * );

int main()
{

  char src[] = "cs23!";
  char dst[]="Hello hello";
  char *curdst;
  int len=0;

  printf("src address %p and first char %c \n", (void *)&src, src[0]);
  printf("dst address %p and first char %c \n", (void *)&dst, dst[0]);

  // compute where NULL character is '\0' ASCII 0

  // while(src[len++]); THE BUG. What was the problem?

  while(src[++len]); // THE FIX: How does this fix it? **001**

  // print out the char arrays and various addresses.

  printf("src array %s and last element %d\n", src, atoi(&src[len]));
  printf("dst array %s and last element %c\n", dst, dst[len]);

  // do the copy

  curdst= my_strcpy(dst, src);

  // check to see if the NULL char is copied too.

  printf("dst array %s and last element %d\n", dst, atoi(&dst[len]));

  return 0;

}

char *my_strcpy(char *s1, const char *s2) {

  register char *d = s1;

  // print the pointer variables address and their contents, and first char

  printf("s2 address %p, its contents is a pointer %p to first char %c \n", (void *)&s2, (void *)s2, *s2);
  printf("s1 address %p, its contents is a pointer %p to first char %c \n", (void *)&s1, (void *)s1, *s1);

  while ((*d++ = *s2++));
  return(s1);
```

而仔細觀察過後，可以發現 2 個程式碼有不同的地方:

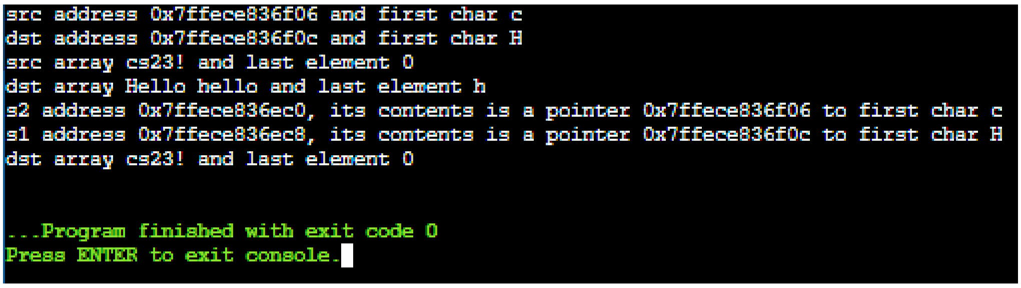


```
while(src[len++]);
```

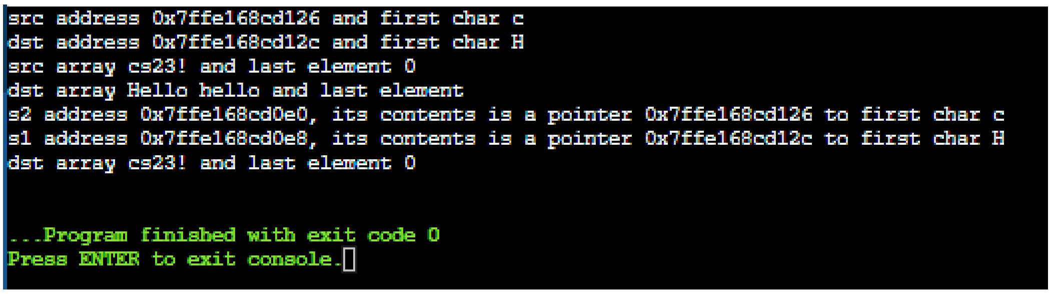


```
while(src[++len]);
```

這個會造成輸出上的不同:



```
src address 0x7ffece836f06 and first char c
dst address 0x7ffece836f0c and first char H
src array cs23! and last element 0
dst array Hello hello and last element h
s2 address 0x7ffece836ec0, its contents is a pointer 0x7ffece836f06 to first char c
s1 address 0x7ffece836ec8, its contents is a pointer 0x7ffece836f0c to first char H
dst array cs23! and last element 0


...Program finished with exit code 0
Press ENTER to exit console.
```



```
src address 0x7ffe168cd126 and first char c
dst address 0x7ffe168cd12c and first char H
src array cs23! and last element 0
dst array Hello hello and last element
s2 address 0x7ffe168cd0e0, its contents is a pointer 0x7ffe168cd126 to first char c
s1 address 0x7ffe168cd0e8, its contents is a pointer 0x7ffe168cd12c to first char H
dst array cs23! and last element 0


...Program finished with exit code 0
Press ENTER to exit console.
```

根據調查，這與 strcpy 的性質有關。Strcpy 會有 2 個引數，1 個是指向目標陣列的第一個元素的 pointer，另 1 個是指向源字串的第一個元素的 pointer，分別對應了 dst 跟 src。由於++在前與在後的性質不一樣，在後會使 src 本身產生改變而在前不會影響 src 本身，這就導致了最終輸出上的不同。