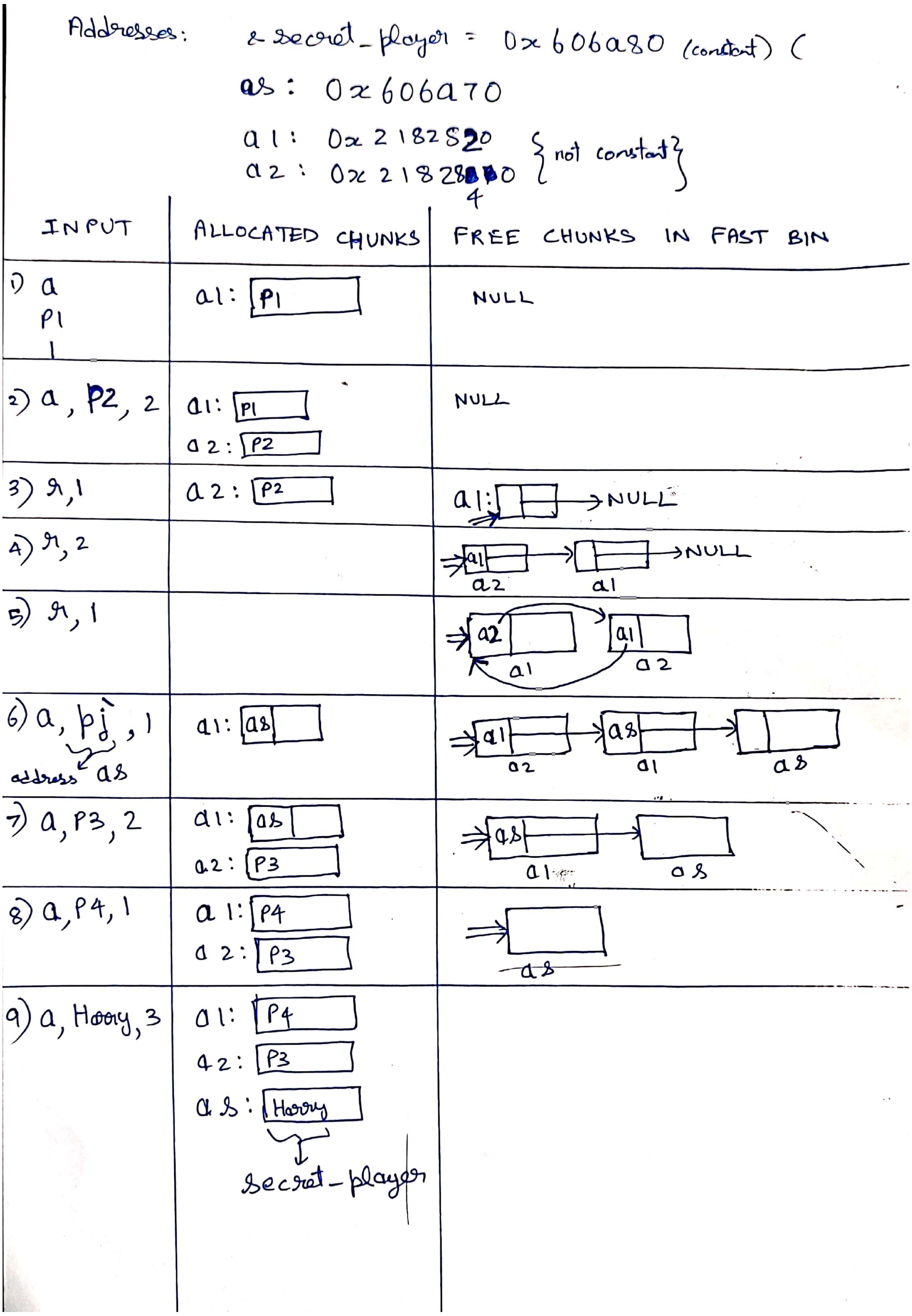
CS6570 Assignment 5b - Report

Rachit Tibrewal (CS16B022)
E Santhosh Kumar (CS16B107)



Addresses: &secret_player = 0x 606a80 (constant) (
as : 0x 606a70
a1 : 0x 2182820
a2 : 0x 21828[illegible]0
4
{not constant}

INPUT	ALLOCATED CHUNKS	FREE CHUNKS IN FAST BIN
1) a P1 1	a1: P1	NULL
2) a, P2, 2	a1: P1 a2: P2	NULL
3) r,1	a2: P2	a1: → NULL
4) r, 2		→ a1 → → NULL a2 a1
5) r, 1		→ a2 a1 a1 a2
6) a, pj, 1 address as	a1: as	→ a1 → as → a2 a1 as
7) a, P3, 2	a1: as a2: P3	→ as → a1 as
8) a, P4, 1	a1: P4 a2: P3	→ as
9) a, Harry, 3	a1: P4 a2: P3 as: Harry secret_player	

Figure 1: Fast Bin state after every command

Refer to typescript for an example execution of the attack. The attached image shows the state of the fast bin linked list after every command. Each malloc and free is of the same small size and happens on the same stack.

- We find address of $secret_player$ using gdb. It is a constant and is 0x606a80.
- We use double free attack to make the linked list a cycle.
- Now we malloc and put the value 0x606a70 = 0x606a80 - 0x10 in the new chunk.
- This chunk which is also present in the free linked list (due to the cyclicity) has the same value 0x606a70. However, it is now interpreted as the next address.
- After two more mallocs, the chunk at 0x606a70 is interpreted as the next free chunk.
- Now we add a new player Harry who gets added at location 0x606a80 ($secret_player$).