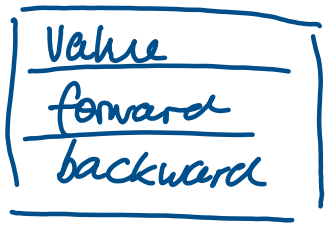
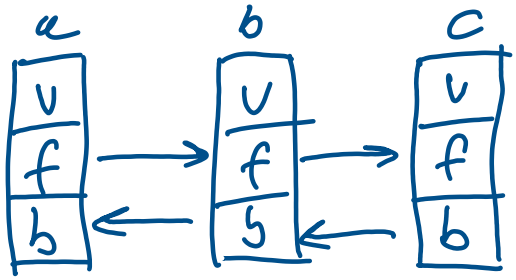
Unlinking

Dienstag, 30. Juni 2020 16:37

doubly linked list:



← linked list element



remove b:

$a.f = c$
$c.b = a$

remove b from b's perspective:

$$\underbrace{b.b}_{a}.f = \underbrace{b.f}_{c}$$

$$\underbrace{b.f}_{c}.b = \underbrace{b.b}_{a}$$

malloc terms:

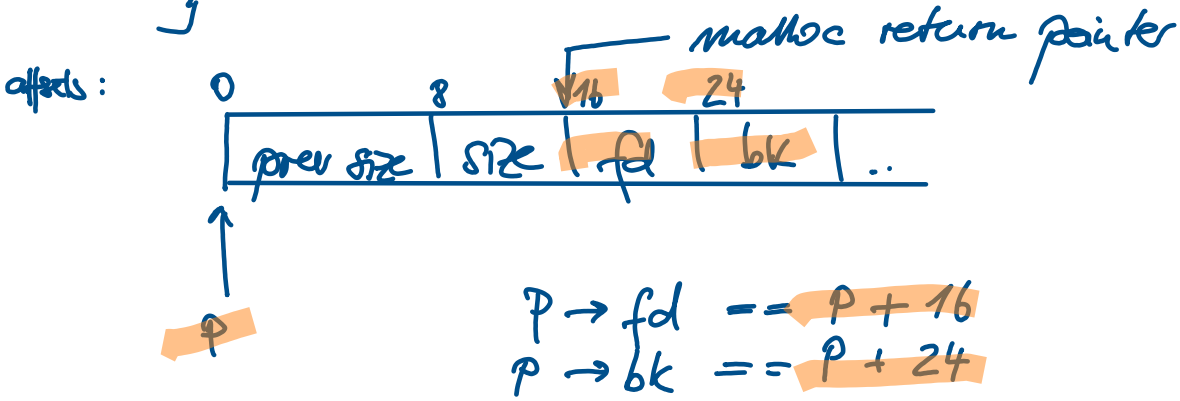
→ see malloc internals website

- unlinking:

chunk to be freed (b above)

```
#define unlink(P, BK, FD) {
    FD = P->fd
    BK = P->bk
    FD->bk = BK
    BK->fd = FD
}
```

(see malloc.c)



P is of type mchunkptr

Usable space starts at P+16 (when P in use, otherwise there will be fd and bk pointers)

Note: This issue has been fixed with additional sanity checks → see malloc.c and look for "corrupted double-linked list"

→ always check the libc version!