内核通过一个红黑树来记录了空闲的内存，malloc就是从树中查找一块大小适合的内存并把地址给你，然后把这个节点从树中摘除，避免被别人分配到产生冲突。这个内存现在归你一个人用了。

free函数是把你的这个内存重新放回到红黑树中，让别人可以申请到这个内存。从逻辑上来说，你现在不能在使用这个内存了，因为它已经不属于你。但是系统的实现上目前没有做到，所以你还是能访问这个地址。

另外，系统也不会帮你覆盖……