Lab2文档

原始代码存在问题1

错误概述：

这版bbuddy_pfree核心逻辑实际上是强制将释放的内存碎片化，而不是将其合并，从而背离了伙伴算法的初衷，并带来严重的内存碎片问题

错误分析：

考虑下面的代码片段

代码块

```
        while(nr_page_left) {
                freed_ch = (chunk_head_t *)obj;
                //..........
                 /*在这里硬性将空闲块的Level编码成0*/
                freed_ch->level = 0;
                /*空闲块强行插入level=0的空闲链表头部*/
                freed_ch->next = b->free_head[0];
                //.......
                b->free_head[0] = freed_ch;
                nr_page_left--;
                //......
        }
```

假定释放一个order=3的8页内存块，正确的实现应该将这个其作为一个整体，并尝试寻找它的其余8页伙伴以合并成order=4的更大块，如条件不满足也应将其插入空闲链表；而现有代码的逻辑是将其拆分为8个order=0的小块并全部加入order=0的空闲链表中，导致随着内存分配与释放，系统内存日趋碎片化，最终几乎所有内存都变为order=0的小片段（即使它们在物理空间上是连续的），从而无法满足大内存分配需求。

原始代码存在问题2

错误概述：

退一万步讲，哪怕真希望在运行过程中让内存逐渐碎片化，`obj = (char *) freed_ct + 1`的错误指针运算逻辑也会导致空闲链表与内存的损坏，并使后续某次内存分配中由于返回非页对齐的无效地址触发灾难性故障。

错误分析：

考虑下面的代码：

代码块

```
        freed_ct = (chunk_tail_t *)((char *)obj
                    + (1UL << __PAGE_SHIFT)) - 1;
        //..........
        obj = (char *) freed_ct + 1;
```

`obj = (char *) freed_ct + 1` 的原始意图是计算出下一个order=0 块的起始地址，以便在下一次循环可以进行处理；但实际上，freed_ct指向的是（[下一页起始地址]-chunk_tail_t结构体大小）的位置，只有添加一个chunk_tail_t结构体大小才可以得到页对齐的地址，但是代码实现中将其强制转换为了char类型的指针，导致obj实际变为了一个非页对齐的、指向上一页末尾元数据内部的无效地址。在下一次循环迭代中，该错误会导致空闲链表整体损坏，并在某次内存分配中因返回未对齐指针而导致系统崩溃

代码修改思路

见foo.c中的代码及其对应注释

修改前后结果对比

（1）修改前，执行malloc(4096)前和free后，空闲链表状态不一致，且free后空闲链表实际上已经损坏。具体表现为free list在level 1层级为空而level 0层级有两个独立入口；空闲链表中出现0x40192ffd-0x40193ffd这种起始地址十分逆天的东西，且两个level 0内存块在0x40192ffd-0x40193000居然有重叠部分！

代码块

```
[    2.587571] ERR: [libukallocbbuddy] <bbuddy.c @ 305> Dumping current state of the free list:
[    2.587768] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 0 is empty.
[    2.587923] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 1 (Order 1):
[    2.588082] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40192000, end: 0x40194000, level: 1
```

代码块

```
[    2.611768] ERR: [libukallocbbuddy] <bbuddy.c @ 305> Dumping current state of the free list:
[    2.612060] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 0 (Order 0):
[    2.612322] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40192ffd, end: 0x40193ffd, level: 0
[    2.612560] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address:
```

```
[    2.588300] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 2 (Order 2):
[    2.588463] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44104000, end: 0x44108000, level: 2
[    2.588700] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40194000, end: 0x40198000, level: 2
[    2.588914] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40014000, end: 0x40018000, level: 2
[    2.589135] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 3 (Order 3):
[    2.589295] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44108000, end: 0x44110000, level: 3
[    2.589535] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40198000, end: 0x401a0000, level: 3
[    2.589758] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40018000, end: 0x40020000, level: 3
[    2.589983] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 4 (Order 4):
[    2.590139] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44110000, end: 0x44120000, level: 4
[    2.590378] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 5 is empty.
```

```
0x40192000, end: 0x40193000, level: 0
[    2.612798] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 1 is empty.
[    2.612992] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 2 (Order 2):
[    2.613223] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44104000, end: 0x44108000, level: 2
[    2.613541] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40194000, end: 0x40198000, level: 2
[    2.613884] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40014000, end: 0x40018000, level: 2
[    2.614232] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 3 (Order 3):
[    2.614452] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44108000, end: 0x44110000, level: 3
[    2.614781] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40198000, end: 0x401a0000, level: 3
[    2.615126] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40018000, end: 0x40020000, level: 3
[    2.615490] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 4 (Order 4):
[    2.615721] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address:
```

```
[    2.590531] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 6 (Order 6):
[    2.590693] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44140000, end: 0x44180000, level: 6
[    2.590913] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x401c0000, end: 0x40200000, level: 6
[    2.591144] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40040000, end: 0x40080000, level: 6
[    2.591371] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 7 (Order 7):
[    2.591524] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44180000, end: 0x44200000, level: 7
[    2.591751] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40080000, end: 0x40100000, level: 7
[    2.591975] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 8 is empty.
[    2.592132] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 9 (Order 9):
[    2.592295] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44200000, end: 0x44400000, level: 9
[    2.592519] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40200000, end: 0x40400000, level: 9
```

```
0x44110000, end: 0x44120000, level: 4
[    2.616079] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 5 is empty.
[    2.616323] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 6 (Order 6):
[    2.616561] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44140000, end: 0x44180000, level: 6
[    2.616912] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x401c0000, end: 0x40200000, level: 6
[    2.617262] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40040000, end: 0x40080000, level: 6
[    2.617528] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 7 (Order 7):
[    2.617773] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44180000, end: 0x44200000, level: 7
[    2.618130] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40080000, end: 0x40100000, level: 7
[    2.618438] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 8 is empty.
[    2.618678] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 9 (Order 9):
[    2.618915] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44200000, end: 0x44400000, level: 9
[    2.619242] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40200000, end: 0x40400000, level: 9
```

（2）修改后内存分配结果，执行palloc前（左）和free后（右）内存状态完全一致

代码块

```
[    2.418651] ERR: [libukallocbbuddy] <bbuddy.c @ 305> Dumping current state of the free list:
[    2.418816] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 0 is empty.
[    2.418983] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 1 (Order 1):
[    2.419149] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40192000, end: 0x40194000, level: 1
[    2.419362] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 2 (Order 2):
[    2.419517] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44104000, end: 0x44108000, level: 2
[    2.419736] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40194000, end: 0x40198000, level: 2
[    2.419953] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40014000, end: 0x40018000, level: 2
[    2.420172] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 3 (Order 3):
```

代码块

```
[    2.441137] ERR: [libukallocbbuddy] <bbuddy.c @ 305> Dumping current state of the free list:
[    2.441371] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 0 is empty.
[    2.441561] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 1 (Order 1):
[    2.441758] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40192000, end: 0x40194000, level: 1
[    2.442038] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 2 (Order 2):
[    2.442232] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44104000, end: 0x44108000, level: 2
[    2.442496] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40194000, end: 0x40198000, level: 2
[    2.442781] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40014000, end: 0x40018000, level: 2
[    2.443061] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 3 (Order 3):
```

```
[    2.420336] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44108000, end: 0x44110000, level: 3
[    2.420554] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40198000, end: 0x401a0000, level: 3
[    2.420776] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40018000, end: 0x40020000, level: 3
[    2.420996] ERR:  [libukallocbbuddy] <bbuddy.c @ 322> Free list 4 (Order 4):
[    2.421155] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44110000, end: 0x44120000, level: 4
[    2.421376] ERR:  [libukallocbbuddy] <bbuddy.c @ 320> Free list 5 is empty.
[    2.421530] ERR:  [libukallocbbuddy] <bbuddy.c @ 322> Free list 6 (Order 6):
[    2.421677] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44140000, end: 0x44180000, level: 6
[    2.421905] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x401c0000, end: 0x40200000, level: 6
[    2.422137] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40040000, end: 0x40080000, level: 6
[    2.422358] ERR:  [libukallocbbuddy] <bbuddy.c @ 322> Free list 7 (Order 7):
```

```
[    2.443256] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44108000, end: 0x44110000, level: 3
[    2.443527] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40198000, end: 0x401a0000, level: 3
[    2.443800] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40018000, end: 0x40020000, level: 3
[    2.444053] ERR:  [libukallocbbuddy] <bbuddy.c @ 322> Free list 4 (Order 4):
[    2.444246] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44110000, end: 0x44120000, level: 4
[    2.444519] ERR:  [libukallocbbuddy] <bbuddy.c @ 320> Free list 5 is empty.
[    2.444703] ERR:  [libukallocbbuddy] <bbuddy.c @ 322> Free list 6 (Order 6):
[    2.444880] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44140000, end: 0x44180000, level: 6
[    2.445096] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x401c0000, end: 0x40200000, level: 6
[    2.445355] ERR:  [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40040000, end: 0x40080000, level: 6
[    2.445611] ERR:  [libukallocbbuddy] <bbuddy.c @ 322> Free list 7 (Order 7):
```

```
[    2.422517] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44180000, end: 0x44200000, level: 7
[    2.422738] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40080000, end: 0x40100000, level: 7
[    2.422960] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 8 is empty.
[    2.423112] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 9 (Order 9):
[    2.423257] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44200000, end: 0x44400000, level: 9
[    2.423470] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40200000, end: 0x40400000, level: 9
```

```
[    2.445819] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44180000, end: 0x44200000, level: 7
[    2.446094] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40080000, end: 0x40100000, level: 7
[    2.446369] ERR: [libukallocbbuddy] <bbuddy.c @ 320> Free list 8 is empty.
[    2.446559] ERR: [libukallocbbuddy] <bbuddy.c @ 322> Free list 9 (Order 9):
[    2.446751] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x44200000, end: 0x44400000, level: 9
[    2.447024] ERR: [libukallocbbuddy] <bbuddy.c @ 326>   Entry at address: 0x40200000, end: 0x40400000, level: 9
```