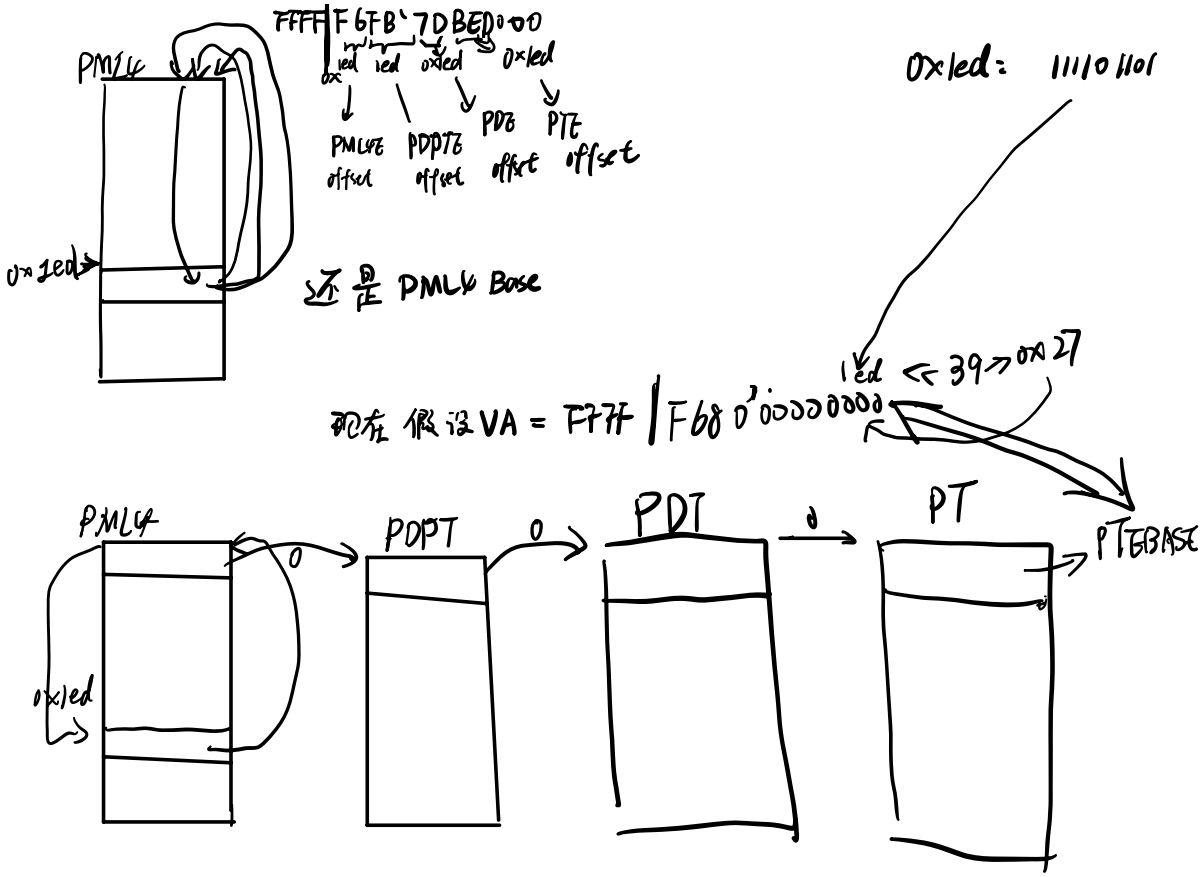

Win 加偏移随机化，不再是 1ed 为偏移，于是可以先找到此自映射偏移，通过 CR3 + 此偏移得到 PTE Base. (详见第二章代码)