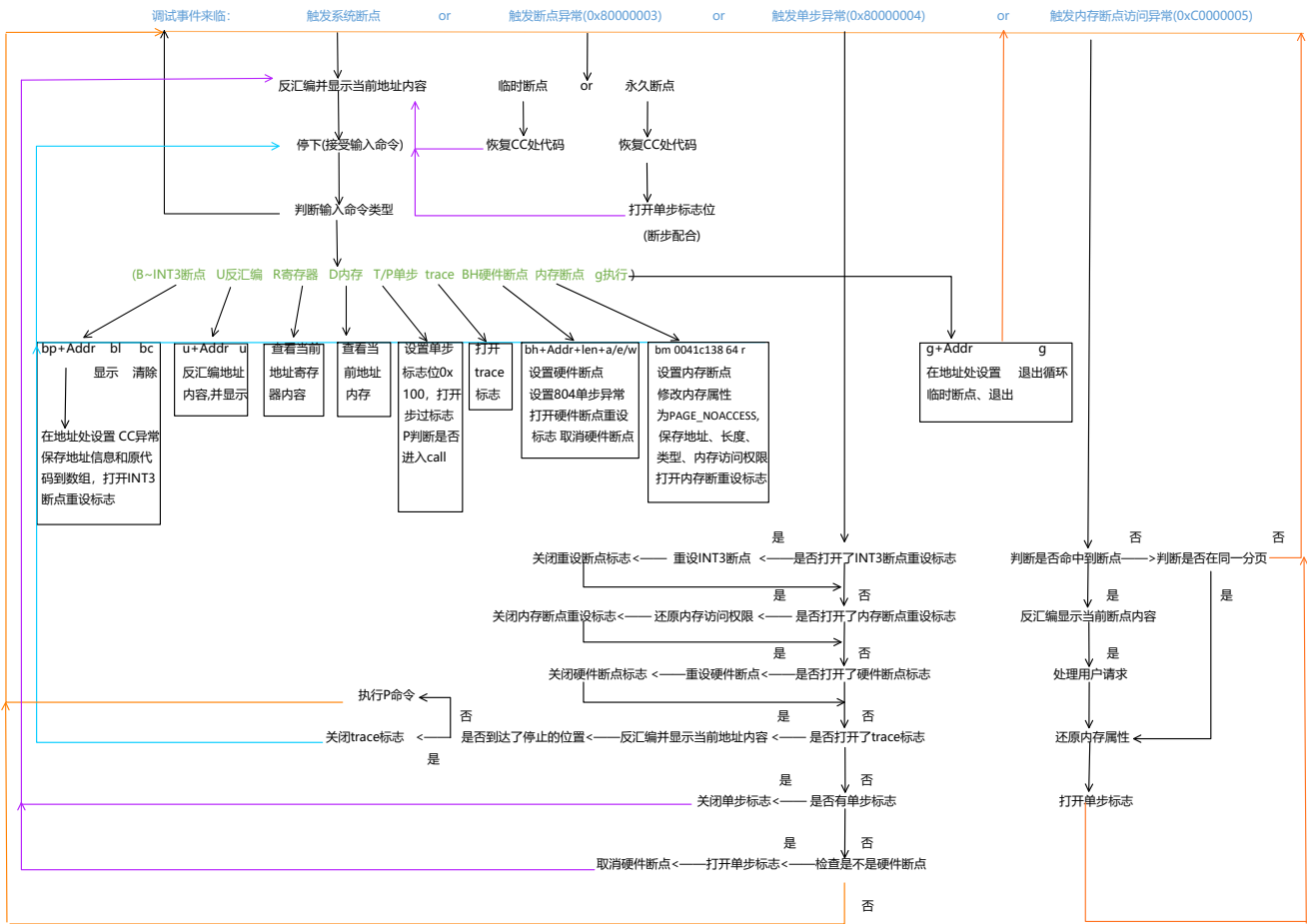


调试器执行流程

2021年6月27日 12:30

调试器的执行过程:

加载进程→建立调试会话→循环等待调试事件→退出调试事件



通过把相关内存页属性设置为PAGE_NOACCESS取消相应权限的, 则会触发EXCEPTION_ACCESS_VIOLATION(0xC0000005)异常
而硬件断点(包括单步和DrX)都会触发STATUS_SINGLE_STEP(0x80000004)异常
而使用int 3进行中断则会触发EXCEPTION_BREAKPOINT(0x80000003)异常