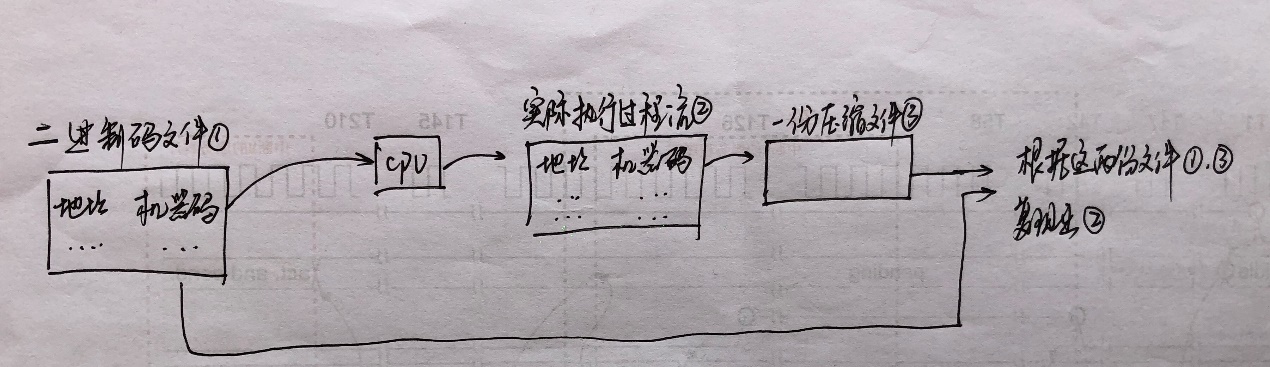
如下图，文件1是一个程序二进制码，去掉无关信息以后就只单纯包含（地址+机器）码两项内容了。程序二进制码丢给处理器执行以后会有一个实际的执行过程，这个过程不是完全按照程序二进制码一条一条顺序执行的，是有分支跳转的。文件2就是实际的执行过程流，也就是原始的程序二进制码在处理器中将分支跳转展开以后的一条一条地址。这个真实的执行流信息会被压缩处理，处理以后得到文件3，现在要根据文件1、3来复现实际的执行过程流，存入新文件4，最终得到的文件4应和文件2一致。

文件3内容包含四种格式的消息：  
1、header1（2bit 00）

2、header2（2bit 01）+index（4bit）

3、header3（2bit 10）+length（4bit）

4、header4（2bit 11）+address（32bit）+length（4bit）

所有的header，index，length，address都是以二进制呈现的

为了便于人工阅读文件3，可以将其内容作如下划分，||将消息一个一个分隔开，每个消息与上述格式对应

11 000000000000000000010000000000

00 0010 ||11 100000000000000000000000

00000000 0001|| 10 1111 || 10 1010|| 10 0010|| 01

0101|| 01 0101|| 00 ||00