ICS 期末部分题目梳理（2016—2022）

一、2016Final

总体评价：选择题质量差、难度中，汇编因为不是 x86-64 很反常规所以体感上很难，流水线送分，链接送分，ECF 答案有错误，虚存&Sys I/O 考察的很偏，计网难，并发比较简单。总体难度 A，难度中等。

1. 选择 T2-浮点数：TBD，过于恶心。

2. 选择 T3-避免缓冲溢出：分配再大的缓冲区数组，只要输入够大就无法根本避免。所以随机化栈偏移地址、存放 Canary Wharf、避免有风险库函数、设置不可执行区域都是有效办法。

3. 选择 T7-链接中的 static 特性：同时有 extern 声明的外部全局和本地 static 时，优先按照本地 static 解析。此时外部的函数如果对外部变量做修改，不影响本地 static 变量的值。

4. 选择 T8-链接中的内存分布：两个点，一是地址顺序：init<text<data<bss(包括 COMMON)；二是命令顺序，先编译的文件内存地址低。

5. 选择 T10-ECF 中的信号：A 选项新连接到达监听端口，当有新连接到达一个监听端口时，操作系统会将这个连接交给相应的进程，但这个过程不会直接导致信号发送给进程。B 选项 SIGSEGV，C 选项除零 SIGFPE（浮点数异常）。有点恶心人的意思。

6. 选择 T13-虚拟内存中的 Core i7 案例：错题。VPN=TLBT+TLBI，PPN 是 TLB 中取出的内容的一部分，B 错；本案例中各个 VPN 位数相等（这是 C 的原意），但是一定不是各个 VPN 相等，C 错。

7. 选择 T17-计网：A 选项服务器用 80 端口提供 Web 服务；B 选项，TCP 是基于 IP 的传输层传输 Stream 的可靠的连接且连接进程的协议，故正确。C 选项可以进行无连接通信；D 选项可以用网卡直接连（有点超纲）。

8. 选择 T18-计网：IP 已知就不需要 DNS（Domain Name System）来翻译。

9. 解答 T23-链接：第二小问，small 的值不会随着 f_int_void 返回而清空，本身 f2.c 也是个程序。

10. 解答 T24-ECF：PartI 第二小问，主进程 exit 不会导致其他进程完蛋，而是托管给 init，只是会成为孤儿进程，因此一定输出满 4 个字母。

11. 解答 T25-综合：同一个进程/Shared 不需要复制，Private&&不同进程执行 write 时需要单独复制。3.2 问 TBD。

12. 解答 T26-计网：Getaddinfo 完了需要 Freeaddinfo，销毁 listp；进程连接到服务器后需要关闭 listenfd——echo 丢给子进程 connfd——关闭父进程中的 connfd。

13. 解答 T27-并发：叙述竞争的时候需要详细到 Load、Update、Store 三阶段详细的顺序。

二、2018Final

总体评价：选择有错题但总体简单，流水线、链接送分，ECF&Sys I/O 非常经典质量高但是很困难，虚存质量高但是也很困难，计网送分，并发有部分空偏但总体适中，第八题不予置评，超纲。总体难度 S+，难度巅峰。

1. 选择 T4-链接：错题。A 选项，对全局符号的不恰当定义不会有任何报告（书链接章节开头引言，比较偏），A 错；B 选项超纲，课程范围内认为 B 错误。

2. 选择 T5-ECF：B 选项中宏连接需要用|来实现（一般都是或）；C 选项是课本原话。

3. 解答 T17-链接：extern 声明要写外部，有且仅有未初始化的全局变量放在 COMMON 中。绝对寻址是 r.symbol+r.addend，和当前的无关。

4. 解答 T19-虚拟内存（困难）

（1）页表大小计算。第一空，想清楚虚拟页中取出来的是物理页号（32 位），一个占掉 4 KB，需要虚拟 VPN=10，VPO=12，所以虚拟地址一共 22 位。进而，按照一个页大小 4KB =2^12Bytes 理解，总共需要 2^(22-12)=1024 页。第二空，图中已经完成了对齐（看黑线），需要二级=2+1+1；一级 1；共 4+1=5 页。

（2）虚存类型：无大页、超大页；有 TLB、权限位；二级页表。仔细阅读题目中的提示，要求我们可能修改后 7 位。

对于地址 0xD7416560：VPO=0x560，TLB=0xD7416，拆分可知（一定记得挖去后三位 TLBI！！！）TLBT=1101011101000010=0x1AE82，观察 valid=1 知 TLB 命中，取出的内容是带有权限位的 PPN，挖掉后面 12 位（只能理解题中后 8～12 位指代的是第 7～11 位）于是得到 PPN，与 VPO 拼接得到物理地址 PA=0x00A23560。坑点来了，此时 TLB 需要修改 Dirty 位——写过了必须改！后三位变为 067，故完成写后该项 TLB 为 0x00A23067（没改让你写啥？）。最后，根据 VPN1=0x35D，乘 4 得到 0x00C24800，不存在于题目信息中，二级那空写“\”。

对于地址 0x0401369B，同理计算发现 TLB 未命中，启动常规翻译即可。重点在于最后的写回，后三位应为 0x067（Dirty 要修改），前面是 PPN=0x00BA4（物理地址前 20 位），所以填 0x00BA4067。

（3）第一空显然是 5，最下面那个。第二空需要注意到 volatile 意味着用内存存储变量，所以根据 COW 机制，需要写 1+2+4+8=15 次，即修改 15 次。

5. 解答 T20-计网：再次回顾以下内容

a. IP 是网络层协议，给每台电脑分配一个唯一的 32 位 IP 地址，并传送 Datagram（数据包）到正确的地址，是不可靠的（不保证数据包一定到达目的地，不重传），是主机到主机之间，无连接也非面向连接。

b. UDP 是传输层协议，建立在 IP 协议上，允许 Datagram 在不同的进程之间传送，不可靠，是进程到进程之间，无连接也非面向连接。

c. TCP 也是传输层协议，建立在 IP 协议上，使得 Stream（字节流）在不同的连接的进程之间（即进程对之间）传送，可靠，连接也面向连接。特别的还是全双工的。

d. （事先写出来，方便比对复习，且确实常考，但教材上 http 不在此处出现）

HTTP 是应用层协议，建立在 TCP 协议上，在 Web 客户端和服务器之间传输 Web Content（超文本数据，如 HTML 文档、图片、视频等），可靠，连接也面向连接。

6. 解答 T21-并发：（1）为什么要写 acd 仍然 TBD。（2）对于 c 要注意到 i++，j++顺序相反，所以一定有各一次无法抵消，至少是 1001，1001。（3）改成 2 相当于让信号失效，事实上只需要一个信号就可以。

7. 解答 T22-综合：不予置评。

三、2019Final

总体评价：选择考察点偏且难，流水线送分，链接送分，ECF&Sys I/O 送分，虚存有难度，但是是逻辑推理上的难，不是本身机制的难，计网做过往年题就是送分，并发送分。总体难度 C+，比较简单。

1. 选择 T4-汇编之 RISC/CISC：回顾如下内容，可知选 C。

指令集	CISC	RISC
传参+regs	寄存器少，可以用栈传参	寄存器多，不可用栈传参
寻址方式	多样，不需专门访存指令	只能使用特定指令访存
有无 CC	使用 CC	无 CC
指令种类	多	少
执行时间	长	短
指令长度	短（便于执行）	长（为了性能）

能耗	高	低（常用于嵌入式系统、手机 ARM）

2. 选择 T5-存储：DRAM 常常组织成一个矩阵族，整行访问时效率比较高，B 错误。SSD 设备擦写的时间会比读取要高一个数量级。一般来说，SRAM 使用比较多的晶体管，而 DRAM 晶体管很少，主要基于电容，SSD 是闪存，晶体管也不会很多，因此后二者的存储密度相对高。

3. 选择 T10-虚拟内存：Cache 总是指向物理地址，无论如何切换都不需要刷新。从用户态切换到内核态只改变访问权限，不改变映射方式，不刷新；换进程则由于不同进程有独立的虚拟内存空间，映射方式可能不同，所以需要刷新（考点在这）。故 A。

4. 选择 T12-虚拟内存：模拟要点：1.块对齐指的是算上头脚等杂七杂八的一起对齐到 16 字节。2.模拟时记得添加/取消 prev&next 指针再对齐。3.p5 后 free(p3)完了必须要记得合并！最容易出错的一步。最后发现把 56 刚好能放在合并出来的块里。空闲的 16Bytes=4header+4prev+4next+4footer，没有有效 load，选 D。

5. 选择 T13-虚拟内存：运气最好=TLB 一次命中，Cache 也命中，0 次。最坏的：TLB 没中，每次查找页表项也没中，最后翻译出的物理地址也不在 SRAM Cache 中（注意 Cache 也会存储一部分物理信息），题目要求访问虚拟内存地址，意思是要取出物理内存中的数据。所以是 5 次，选 B。

6. 选择 T16-计网：GET 请求的参数用?来分隔，A 错误。

7. 解答 T21-汇编与流水线：Trailing Cycle=4 周期，基础周期=指令数，罚时：load-use=1 周期，mis-pred=2 周期，ret=3 周期。末尾的 mis-pred 一般不惩罚。

8. 解答 T22-链接：一定看清楚对于外部的符号，写当前模块的节还是原来模块的节。总结就是慢慢读题。

9. 解答 T23-Sys I/O：open=再开一个文件表（位置独立），dup=把这个导到已有的文件表，小心 O_APPEND 宏即可。

10. 解答 T24-虚拟内存：“倒推法”——给的是不完整的东西，读可能是一级读二级，二级读物理地址；写可能是写到写到物理地址/二级页表，这是因为一级到二级的翻译过程没有必要修改。现在，由于读出来的 0x80AA32C4 和写入地址 0x00AA3AD0 是抛去权限位、有效位、VPO 后均为 AA3 的，可以大胆推测 0x00AA3 是二级页表起始地址，所以 0x67F 对应一级，C3F 是物理页。据此可以推理。

四、2020Final

总体评价：选择难，T2、T9 仍然悬而未决，T23、T25 硬整烂活，质量也差。流水线中等但估计很多人（包括我）已经忘得差不多，需要记住 load-use、mis-predict、ret 分别罚时 1、2、3 个周期，链接有一个小坑，需要读懂哪个变量在哪就送分了，ECF&Sys I/O 需要仔细但是也不难。重量级的来了，这个虚存和虚存就没什么关系，特别是最后一问纯粹为了恶心人和 Cache 硬整的烂活，耗时还容易算错。并发也是重量级，考了哲学家就餐问题的变种，但是总归靠感觉可以填出来大部分。总体难度由于选择一个 2 分+虚存极其容易直接暴毙，给到 S。

1. 选择 T1-汇编：A 为 Arthals 博客中专门画篇幅讲述的，B 正确（P118），C 前半句没问题，但是%rbp 会作为可变栈帧的指针使用，错误。D 正确，archlab 的 writeup 中提及。

2. 选择 T2-Cache：圈 1：利用 C=SEB 计算的时候，没有考虑 tag、valid。两位 tag、一位 valid，至少是 1.75 倍，错误。圈 2 正确，模拟即可。圈 3 错误，模拟即可。圈 4 错误，哪怕忘了，从圈 3 也能看出来是空间局部性差的时候是半斤八两的，实际上是空间局部性良好的时候 A 模式更好地利用 Cache。因此选 B。

3. 选择 T9-ECF：缓冲区应该是类似于 MAP_PRIVATE 的数组，每个进程缓冲区，第一次后是 1 个-，第二次后是 2 个-，因此 2*9=18，选 B。

4. 选择 T14-虚拟内存：计算 VPN 大小的时候，除 4 还是除 8 要看地址位数。32=4，64=8。

5. 选择 T15-虚拟内存：最优连续页——1024 物理页，其中每页存放 1KB/4Bytes=256 个 PTE，因此需要 4 个三级页表，从而一、二级页表各 1 页，4+1+1=6，故最优 6KB。最坏全部不连续，需要 2^20 页，即 2^20 个 PTE，注意，这里在计算三级页表时也要尽可能的分散，而不是三级页表紧凑的排列。计算知每级 VPN=8，VPO=10（刚好对应 16G 虚拟地址空间），于是三级页表最多 2^8*2^8，二级 2^8，一级 1，总计 65536+256+1=65793，选 B。

6. 选择 T18-Sys I/O：错题。对等线程没有写时复制的概念，因为根本没有独立虚拟地址，A 错误；COW 机制课本只提及了私有区域，课程范围内 D 错误（但如果把共享区域理解成共享库，则 D 正确）。因此答案选 A 更好。

7. 选择 T23-并发：无意义的烂题，算逆序数即可。本题应该出现在《数据结构与算法 A》的试卷上，不知道为什么跑到此处了。选 C。

8. 选择 T24-并发：选项 A 需要注意，如果以 pthread_exit 则只会让主线程退出，exit、return 才会导致一起结束。

9. 选择 T25-并发：错题，ABC 都正确。

10. 解答 T26-流水线：再次强调公式=4 Trailing Cycles+执行指令数*1 Cycles+罚时。load-use=1、mis-pred=2、ret=3。末尾的罚时需要慎重考虑，本题中就不需要计末尾的罚时。

11. 解答 T27-链接：看清楚问的外部是写定义他的模块中的节还是当前模块的节，每年不一样，仔细读题。

12. 解答 T29-虚拟内存&Cache（伪困难）：不要被题目吓到！题目只在说一件事情：页号的 TLB，和第六章中 data 的 TLB 是不一样的。分析容易发现，前面 3 行不会导致替换（根本用不完），所以只看页数即可（此时的 miss 只有冷不命中）。由于一开始页都在硬盘中，所以页数=Page Fault 次数。所以计算方法：ceil(3*2^(n-9))。于是前三行分别填写 1、2、24（每列内容相同）。第四行第一空同理计算可知为 1536，后面需要模拟 TLB 进行 LRU 驱逐的过程。由于过于复杂，不再计算，考场上建议放弃。

13. 解答 T30-并发（困难）：第一问很容易猜到是死锁，原理是每个人都这么拿，到最后有可能每个哥们就拿了左边那个哥们的手机，每个人都拿不到右边的，就卡在这里了，上不去下不来的。第二问阅读后模拟一下，马上发现本质上是第一个执行外的其他进程会被卡死在 sem[0]处，所以只需要写 0（1～25 都行）。第三问先教你怎么猜：不拿自己的——不填 num，只用到圈 1 圈 2，由于进行了 if-else 的特判，所以一定是反着的，答案 1221 或 2112 均可，直接到手。原理在于确保不要让最后一个人跟着拿，破掉这个环即可。第四问比较困难，首先观察 28、29 行很容易猜到 DE 分别填写 32，A 很容易填出是 1，其余三空 TBD。

五、2021Final

总体评价：除链接大题外题目质量高、有深度、反押题，是所有 ICS 试卷里质量和难度都最佳的一套之一。选择题总体平稳比较简单，Cache 大题难度高，需要小心地进行 FIFO 模拟，最后难的空可以战略性放弃，链接大题有争议且表述不规范，全卷唯一瑕疵，ECF 大题难度高，再次强调了信号处理程序只打断收到信号的，发送者可能并行执行，虚拟内存大题总体平稳比较简单，并发编程也比较平稳，基本可以拿到 13-14 分。缺憾之处在于链接质量一般，Cache 作为第一个大题难度过高阅读量过大，是本试卷的问题所在。总体难度给到 S+。

1. 选择 T8-讲座：当年讲座题，不具备参考价值，选 D。

2. 选择 T11-链接：动态链接中的 PLT 和 GOT 不在 24Fall 的教学计划内，选 B。

3. 选择 T14-Sys I/O：知识点都正确，模拟错误，选 D。O_TURNC=若文件存在则清空，O

_CRATE=若文件不存在则创建。

4. 选择 T18-计网：A 选项，根据 TCP 套接字是一个五元组，由连接双方的 ip, port 以及协议名唯一标识可知正确。B 选项，书 P654 中可以看到 connect 传递的参数 addr 是服务器的套接字，错误。C 选项，显然不能立刻读写，还没转化。D 选项，这个事是 listen 干的，bind 把 sockfd 与 addr 中的服务器套接字地址连接起来。

5. 解答 T21-Cache：（1）模拟时务必小心，是 FIFO，时刻做好标记。C1miss9 次，C2miss10 次，所以填“<”。（2）第 c 问，战略性放弃。

6. 解答 T22-链接：Part A 的 iter，由于 COMMON 中的变量由链接器分配空间，链接完成后进入.bss，所以填写.bss；count 对应 static int count，填写“否”的原因 TBD，与往年答案自相矛盾。PartB 需要搞清楚表述方式，TBD。PartC 超出本年度授课范围，不予置评。

7. 解答 T23-ECF：PartA 白给。解答 PartB 的核心要点在于：信号处理程序打断的是接收到信号的进程，和发送者没什么关系。据此可以立即判断出，由于子进程可能先执行完毕，导致可能出现很多种的可能性，并且由于可能是同时发送了多次，导致信号堆积只被处理一次，同时还要考虑 printf 和 fflush 执行可能交替，因此第三问中 CC12 也是有可能的。只有进入“嵌套式”信号处理程序才能让顺序唯一。因此答案选择（3）BCD（4）A，画进程图就可以。前面两问要记住，接受是内核把进程从 Kernel Mode 转化到 User Mode 时候干的事情，而一种信号最多被处理一次，因此选（1）C（2）A。

8. 解答 T24-虚拟内存：除了最后两分前面基本属于白送。前面需要注意的部分只有 y 地址具有的权限指的是物理地址，想清楚：在虚拟内存系统中，权限位通常存储在页表项 PTE 中，而不是直接存储在虚拟地址或物理地址中。于是取出 TLB 后再看权限位。倒数第二空意义不明，自己信心也不足——都推理出来了 n 是负数也没敢写！这是因为 A、x 肯定不是空指针，n 也不是 0，矩阵大小也合适（以上信息由函数内部没有引发错误得出），所以只能是 n 错误，那 n>0 肯定不会出错，又不是 0，就只能是 n<0 了。回忆 calloc（初始化为 0）与 malloc 的行为，当 n<0 时返回 nullptr 而不报错，因此如果你试图取 y[0]自然就相当于*y，访问空指针直接引起 segmentation fault。最后一空，建议用排除法，圈 1 说的是 CPU 内核态代码段用户态，当然可以执行，别搞反了！圈 2 很明显错的，那只能是圈 3。

9. 解答 T25-并发：第一问模版题，还没背熟，需要牢记。mutex 只有在需要保护全局变量时才上锁，因此尽量后上；需要注意的是 full 不代表是否满，而是代表有多少个东西（一定记住，信号量不只是 0 和 1，可以是很多非负正数），empty 也不是代表是不是空，而是代表空位，因此看清楚题目含义才可以做题，并发编程务必小心阅读注释。第二问是新题，但

阅读注释（注释啊！！又白白丢分）可立即判断出，初始化为 0。后两空的没时间做法：一律填写同一个选项，保底拿 1 分。正确做法：按照 mutex 的最小需要原则，尽可能晚地使用、尽可能早地释放，因此很容易判断出来先 D 后 C。很容易想出来如果一个线程在等待信号量 waiting_producer 另一个在等待 mutex，那立马会造成死锁。由于 PV 操作的原子性，先 V 后 P 不会导致错误，即便他们中间可能进行了别的线程的别的操作。最后一空，快速做法：肯定有问题啊！要不然浪费那么多资源干等干啥，选 A。正确做法：TBD。

六、2022Final：一个字评价——史。总体难度：A。

具体题目不予置评。

七、2013Final——页表自映射（需要记忆）