A fork() in the road

fork 状态机复制包括持有的操作系统对象
execve 重置状态机，但继承持有的所有操作系统对象.

文件描述符：一个指向操作系统内对象的"指针".
- 对象只能通过操作系统允许的方式访问.
- 从0开始编号(0,1,2分别是 stdin, stdout, stderr)
- 可以通过 open 取得，close 释放，dup 复制
- 对于数据文件，文件描述符会"记住"上次访问文件的位置.

文件描述符的"复制"、文件抽象的代价.
- 操作系统必须正确管理好偏移量.
  文件写入是原子性操作.
- dup() 的两个文件描述符是共享 offset.
- 状态机被复制，复制后内存都被共享.
  - "copy-on-write" 只有被写入的页面才会复制一份.
    - 被复制后，整个地址空间都被标记为"只读"
    - 操作系统捕获 Page Fault 后酌情复制页面.
    - fork-execve 效率得到提升.
  - 操作系统会维护每个页面的引用计数.

搜索并行化
加速状态空间搜索
每次搜索都 fork 一个新进程、无需回溯

跳过初始化
Zygote Process (Android)
- Java Virtual Machine 初始化涉及大量类加载.
- 一次加载，全员使用

Chrome site isolation (Chrome)
Fork server (AFL)

备份和容错
用 fork 做个快照.
- 主进程 crash 了，启动快照重新执行

fork(): UNIX 时代的遗产
在操作系统的演化过程中，为进程增加了更多的东西.
- 信号
- 线程
- 进程间通信
- ptrace

fork() 的七宗罪.
- fork is no longer simple
- fork doesn't compose
- fork isn't thread-safe
- fork is insecure 指针指向地址不变
- fork is slow
- fork doesn't scale
- fork encourages memory overcommit