QEMU System Emulator 源码学习

1. 调用结构
   主入口在 /softmmu/main.c

```
// 系统主入口
int main(int argc, char **argv, char** envp)
  // qemu 初始化函数
  qemu_init(argc, argv, envp)
  // qemu 工作函数
  qemu_main_loop()
  // qemu 清理函数
  qemu_cleanup()
```

2. 初始化过程
   入口在 /softmmu/vl.c

```
void qemu_init(int argc, char** argv, char **envp)
  //? 可能是初始化块设备选项队列
  BlockdevOptionsQueue bdo_queue = QSIMPLEQ_HEAD_INITIALIZER(bdo_queue)
  //? 可能是初始化接口队列
  QemuPluginList plugin_list = QTA
  ILQ_HEAD_INITIALIZER(plugin_list)
  // 设置buffer
  os_set_line_buffering()
```

3. 主要数据结构

```
enum QemuOptType {
    QEMU_OPT_STRING = 0,  // no parsing (use string as-is)
    QEMU_OPT_BOOL,        // on/off
    QEMU_OPT_NUMBER,      // simple number
    QEMU_OPT_SIZE,        // size, accepts (K)ilo, (M)ega, (G)iga, (T)era
postfix
};

typedef struct QemuOptDesc {
    const char *name;
    enum QemuOptType type;
    const char *help;
    const char *def_value_str;
} QemuOptDesc;

struct QemuOptsList {
    const char *name;
    const char *implied_opt_name;
    bool merge_lists;  // Merge multiple uses of option into a single list?
    QTAILQ_HEAD(, QemuOpts) head;st
    QemuOptDesc desc[];
};
```

```
#define QTAILQ_HEAD(name, type)                                         \
  union name {                                                          \
    struct type *tqh_first; /* first element */                         \
    QTailQLink tqh_circ;    /* link for circular backwards list */ \
  }
```