GDB disassemble

[1条回复](http://zhiwei.li/text/2008/10/09/gdb-disassemble/#comments)

前面几篇谈GDB调试程序的帖子，都对反汇编语焉不详。这里详细讨论一下disassemble/disass命令

反汇编一个函数  
disass func\_name

反汇编一段内存地址, 第1个参数是起始地址，第2个是终止地址  
disassemble 0x0 0x10

先看看文档 [Debugging with GDB](http://sourceware.org/gdb/download/onlinedocs/gdb.html)

源码和机器码  
可以使用 info line 命令来映射一个源码行到程序地址,然后使用命令disassemble显示一个地址范围的机器指令。  
比如，我要查看main函数从哪里开始

(gdb) info line main  
Line 34 of “rank.c” starts at address 0x804847f  
and ends at 0x8048493 .  
(gdb) info line \*0x804847f  
Line 34 of “rank.c” starts at address 0x804847f  
and ends at 0x8048493 .  
并且,info line会修改 x/i 命令的默认的起始地址

disassemble 不带参数，默认的反汇编范围是 所选择帧的pc附近的函数  
单个参数, 就是pc, 当然也可以是函数名，因为函数名 也是一个 地址; 这样范围就是该pc附近的函数  
两个参数，就是内存地址范围

set disassembly-flavor intel  将汇编指令格式 设置为intel格式，默认是att  
(gdb) show disassembly-flavor  
The disassembly flavor is “att”.

查看 反汇编指令的另一个方法就是使用x  
x/3i $pc  
显示pc开始的3条指令