My analysis:

The are some mismatches between call and ret instructions especially in some complex applications because:

- Programmers uses some branches, exceptions, goto statements, longjumps, signals in their codes

- Compilers has changed the flow of the program: It uses a ret instruction to generate a jump, it means using push <add> instruction and then ret instruction.Compilers uses this way in the situation the number of available register are rare.

Almost all mismatches that my Pintool have recorded are form longjmp function from Libc library. The basic idea behind using setjmp and longjmp is implementing an exception handling scheme to save CPU state whenever you encounter a try keyword and then do a longjmp whenever you throw an exception. If there are few try blocks in the program, like small programs, the frequency of the mismatches is not high. However, often in complex application like gedit there are a lot of try blocks. As a result, the frequency of the mismatches is high.