

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2014 年 11 月 13 日 (13.11.2014)



WIPO | PCT



(10) 国际公布号
WO 2014/180107 A 1

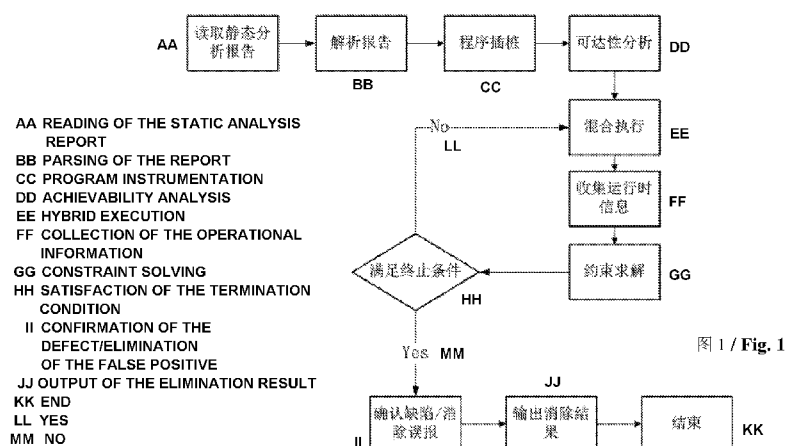
- (51) 国转 利分类号 :
G06F 19/00 {2011.0}
- (21) 国际申请号 : PCT/CN20 13/086993
- (22) 国际申请日 : 2013 年 11 月 13 日 (13.11.2013)
- (25) 申 饰 言 : 中文
- (26) 公布语言 : 中文
- (30) 优先权 :
2013 10165634. 8 2013 年 5 月 8 日 (08.05.2013) CN
- (71) 申请人 : 南京大学 (NANJING UNIVERSITY)
[CN/CN]; 中国江苏省南京市鼓楼区汉口路 22 号, Jiangsu 210093 (CN)。
- (72) 发明人 王林章 (WANG, Linzhang); 中国江苏省南京市鼓楼区汉口路 22 号 Jiangsu 210093 (CN)。李孟宸 (LI, Mengchen); 中国江苏省南京市鼓楼区汉口路 22 号, Jiangsu 210093 (CN)。李宣东 (LI, Xuandong); 中国江苏省南京市鼓楼区汉口路 22 号, Jiangsu 210093 (CN)。陈志 (CHEN, Zhi); 中国江苏省南京市鼓楼区汉口路 22 号, Jiangsu 210093 (CN)。

- (74) 代理人 : 南京瑞弘专利商标事务所 (普通合伙)
(NANJING RUIHONG PATENT AND TRADEMARK OFFICE(GENERAL PARTNERSHIP)); 中国江苏省南京市玄武区太平门街 1 号 304 室, Jiangsu 210016 (CN)。
- (81) 指定国 除另有指明, 要求每一种可提供的国家保护) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, ML, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 除另有指明, 要求每一种可提供的地区保护) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,

[见续页]

(54) Title: TEST-BASED STATIC ANALYSIS FALSE POSITIVE ELIMINATION METHOD

(54) 发明名称 : 一种基于测试的静态分析误报消除方法



(57) Abstract: Provided in the present invention is a test-based static analysis false positive elimination method, allowing for enhanced usability for a software static analysis technology, and for reduced time and labor costs for manual confirmation and checking of a static analysis report. Program information is collected when in operation by utilizing a testing technology and is verified against a related target path and target defect in the static analysis report, and, either a defect is confirmed or a false positive is eliminated. The present invention, a static analysis report file saved in a metadata exchange format based on the Extensible Markup Language is read first, and information on a target defect is parsed from the file; for a static analysis alert of each specific defect, a hybrid execution concept is employed for continued specific execution, symbolic execution, and constraint solving for a program, a model is established during this process on the basis of features of different defects, and operational information is collected; the operational information acquired in the preceding step is used to determine whether or not the defect occurred, or to determine that the static analysis alert is a false positive; and, iteration until all static analysis alerts are processed.

(57) 摘要:

[见续页]



RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, 本国际公布,
CM, G^A, GN, G⁴, GW, KM, ML, MR, NE, SN, TD, — 包括国际检索报告(条约第 21 条(3))。
TG)。

本发明给出一种基于测试的静态分析误报消除方法，能够增强软件静态分析技术的可用性，降低人工确认和检查静态分析报告的时间和人力成本。利用测试技术来在运行时收集程序信息，与静态分析报告中涉及的目标路径和目标缺陷相互印证，确认缺陷或消除误报。本发明首先读取以基于可扩展标记语言的元数据交换格式保存的静态分析报告文件，从中解析出目标缺陷的信息；对每一条特定缺陷的静态分析警报，采用混合执行的思想对程序进行持续的具体执行、符号执行以及约束求解，在这一过程中根据不同缺陷的特征建模，收集运行时信息；使用上一步获取的运行时信息确认是否发生该缺陷，或判断该静态分析警报是一个误报；迭代直到所有静态分析警报被处理完毕。

一种基于测试的静态分析误报消除方法

技术领域

本发明涉及利用测试方法削减静态分析结果中误报数目的技术，主要利用符号执行和具体执行相结合的动态测试技术验证静态分析的结果，实现对软件静态分析结果中误报的判断和消除，属于软件工程、软件测试、软件动静态分析相结合的技术领域。

背景技术

静态分析与动态分析技术都被用于在 C/C++ 程序中发现程序缺陷。静态分析技术通常将不同类型的软件缺陷检测过程形式化为特定的匹配问题，即在目标分析程序中匹配某种缺陷的特征或模式。因为软件缺陷常常在特定的控制流路径上发生，大部分的静态分析技术同时也是路径敏感的，或在静态分析的结果中会给出疑似发生缺陷的路径，所以静态分析技术能在不实际运行程序的情况下发现程序中的潜在缺陷，从而避免额外的运行时开销。基于以上特性，静态分析技术在研究界和工业界中都广受重视。然而，静态分析工具可能会牺牲精确性以获得更好的扩展性，从而导致对许多重要的程序属性建模并不准确，比如堆内存单元等。另外，由于缺少运行时信息，静态分析工具常常报告出大量的未经确认的警报，而真实的内存泄漏隐藏其中。这严重限制了实际开发中静态分析工具的可用性，即使是一款成熟的商用静态分析工具，也可能在分析中等规模的程序时报告较多的警报。人工检查所有这些警报并从中找到真实的缺陷是一项艰巨、沉闷和耗时耗力的工作。

软件测试技术实际执行待测程序，可以在运行时确认软件缺陷是否发生。实际触发缺陷的一个测试用例及其执行时信息将是确认静态分析警报的有效方式。软件测试的结果可以帮助确认静态分析结果的正确性，从而消除其中的误报。软件测试需要充分和高质量的测试用例集，生成程序测试输入的方法有很多，具体执行和符号执行是其中重要的技术。

混合执行技术是符号执行和具体执行结合的技术。具体执行就是使用具体的变量值输入到程序中，驱动程序的执行。符号执行指的是使用符号变量代替具体变量，根据程序中的变量之间相互关系及控制流，得到符号表达式和符号约束条件，从而将程序执行状态符号化；其通常与约束满足问题求解方法一同使用。混合执行技术是一种对同时进

行具体执行和符号执行的混合程序测试技术。

发明内容

技术问题：软件静态分析技术可以在开发早期阶段发现软件缺陷，因而被广泛使用，但由于静态分析结果中包含不同数量的误报，从而降低了静态分析在实际中的可用性。本发明的目的是提供一种基于测试的静态分析误报消除方法，根据运行时的信息确认真实的软件缺陷，并消除静态分析结果中的误报，增强软件静态分析技术的可用性，降低人工确认和检查静态分析报告的时间和人力成本。

技术方案：本发明首先读取并解析静态分析工具产生的包含缺陷信息的软件报告，从中抽取出目标缺陷的信息，包括静态分析工具报告的缺陷发生点和可能导致缺陷的程序路径；对每一条特定缺陷的静态分析警报，采用混合执行的思想对程序进行持续的具具体执行、符号执行以及约束求解，在这一过程中根据不同缺陷的特征建模，收集运行时信息，直到停止条件满足时结束该过程；使用上一步获取到的运行时信息确认是否发生该缺陷，或判断该静态分析警报是否是一个误报；迭代执行以上步骤直到所有静态分析警报被处理完毕。

基于测试的静态分析误报消除方法包括以下步骤：

步骤 1： 读取静态分析结果报告。

从磁盘文件读取以基于可扩展标记语言的元数据交换格式保存的静态分析报告文件。

步骤 2： 对读入的静态分析报告进行解析，得到待验证警报列表。

分别从静态分析报告中解析出静态分析警报信息，包括疑似缺陷路径和特定缺陷发生点，形成待验证警报列表。

步骤 3： 程序插桩

采用程序插桩技术在程序源代码中插入标记语句，程序插桩插入的程序语句与原程序同步编译、链接为可执行程序。

所述插入标记语句的工作包括：

① 将待验证警报列表中的警报信息标记于源代码中，也就是标记静态分析警报的路径片段中的分支语句和缺陷相关语句，在其前/后插入标记语句，为后续步骤中计算路径片段可达性和运行时标记路径服务。

② 插桩标记符号变量和符号表达式、约束条件，为混合执行中的符号执行服务；

③ 根据不同的缺陷特征，插桩标记内存分配，字符串拷贝等特定缺陷的特征语句，以运行时收集信息，辅助判断缺陷是否发生。

所述程序插桩或者插桩是在保证被测程序原有逻辑完整性的基础上在程序中插入额外的标记语句（称为探针），通过探针的执行并抛出程序运行的特征数据，通过对这些数据的分析，获得程序的控制流和数据流信息，得到逻辑覆盖等动态信息，实现测试。

步骤 4：可达性分析

以在程序源代码中插入的静态分析警报的路径片段为目标，在控制流图上计算程序中每一个分支在执行时是否可能到达标记路径片段。

所述控制流图是一个有向图，程序源代码中的每个语句对应图中的一个节点，图中节点之间的路径表示程序代码之间的控制关系。

所述可达性分析是一个直观的控制流图遍历和计算过程，将过程内的控制流计算与过程间的调用图结合即可实现。

步骤 5：利用混合执行测试方法生成测试用例，对程序进行测试。

利用混合执行测试方法生成测试用例，在运行时验证静态分析警报是否是误报，具体处理过程如下：

步骤 51) 以一个初始输入做具体执行，在第一次执行中收集符号表达式和符号约束条件。

步骤 52) 根据收集到的符号约束条件中的分支点，形成对当前执行路径的一个约束组合，满足所有这些约束条件的具体值集合按照此程序路径执行。

步骤 53) 在运行时收集与特定缺陷相关的程序信息。

步骤 54) 对收集到的约束条件集合中的约束条件逐一取反求解。

步骤 55) 在每一轮执行中或执行结束前，判断是否当前执行覆盖到目标路径片段。如果执行到疑似缺陷路径，则生成此次运行时缺陷是否触发的一个临时结果，此结果的集合将用于最终确定静态分析警报是否是一个真实的缺陷或误报。

步骤 56) 利用约束求解得到的新值作为新的输入，重复步骤 51) 的过程，直到满足混合执行停止条件，或达到测试执行迭代次数的上界。

所述混合执行测试方法是符号执行和具体执行结合的测试方法；符号执行指的是使用符号变量代替具体变量，不执行程序的前提下模拟程序执行来进行相关测试分析的技术。

术，一般与约束满足问题求解方法一同使用；具体执行就是指使用具体的变量值输入到程序中，驱动程序的正常执行进行测试；混合执行是一种对程序交替进行具体执行和符号执行的混合软件程序测试技术。

步骤 6: 根据测试执行中每一覆盖到目标路径片段时记录的结果集合，判断特定缺陷的静态分析警报是否是一个得到确认的缺陷，如果不是，认为其是误报。报告上述确认/误报消除结果。

步骤 7: 对于测试执行始终无法覆盖执行到的静态分析警报，将其归为一类无法确定的警报，并提醒开发者或测试人员人工处理。

有益效果：本发明所述的基于测试的静态分析误报消除方法实现了对静态分析结果报告的解析，对静态分析报告的缺陷特征在测试运行时加以收集和确认，并消除静态分析警报中的错误报告。具体来说，本发明所述的方法具有如下的有益效果：

(1) 本发明所述的基于测试的静态分析误报消除方法中，通过在运行时收集与静态分析警报相关的程序信息和缺陷特征信息，利用测试技术不断覆盖静态分析警报的疑似路径片段和目标缺陷位置，从而在运行中或运行结束时确认静态分析警报的特定缺陷是否真实发生，并消除错误的警报，降低了人工处理静态分析报告的工作量和时间成本。

(2) 结合了可达性分析和混合执行测试，形成了一套对静态分析报告的解析、插桩、动态分析技术和结果分类系统，通过对不同特征的软件缺陷建模，将可以适用于消除不同类型缺陷的静态分析报告。

附图说明

图 1 是基于测试的静态分析误报消除方法流程图。

具体实施方式

下面对本发明的具体实施方式作更详细的描述。

一. 读取与解析静态分析结果报告

在具体实施中，从磁盘文件获取以基于可扩展标记语言的元数据交换格式保存的静态分析报告文件。基于可扩展标记语言的数据格式已经有成熟的信息查找方法及查询语言，但不同缺陷需要在静态分析报告中查询不同的信息，而不同的静态分析工具产生的数据格式也并不统一，需要对应地了解使用的静态分析工具生成的报告数据格式，并编

写简单的缺陷信息查找程序获取静态分析警报。

要得到待验证的静态分析警报列表，需要在读取静态分析报告同时做特定于缺陷类型的数据处理和组织。静态分析报告中解析出的信息，应该包括并不限于疑似缺陷路径和缺陷发生点，对于特定的缺陷类型，与缺陷相关的其他信息一起组织为警报列表，比如内存泄漏的一条静态分析警报可以组织为三元组 $\langle a, p, e \rangle$ ，其中 a 表示疑似泄漏内存的分配位置， p 为疑似缺陷路径， e 为疑似泄漏点。一条缓冲区溢出警报可以组织为三元组 $\langle p, e, len \rangle$ ，其中 p 为疑似缺陷路径， e 为静态分析给出导致缓冲区溢出的语句， len 为可能导致溢出的缓冲区长度。

二. 程序源代码预处理

在具体实施中，对程序的源代码做两项预处理工作：程序插桩和控制流图可达性分析

在具体实施中，采用程序插桩技术在程序源代码中插入需要的语句，程序插桩插入的程序语句与原程序同步编译、链接为可执行程序，程序插桩的主要步骤为：

(程序插桩 1) 依次读取待验证列表的警报信息，对每条警报信息中的疑似路径片段做插桩，即将路径片段中的分支语句插入程序中的正确位置；

(程序插桩 2) 对每条警报信息中的缺陷相关语句插桩，插桩的语句应该包含缺陷相关的信息，如内存分配位置或缓冲区溢出长度等；

(程序插桩 3) 根据程序语法插桩行为语句，以在运行时收集符号变量和符号表达式、约束条件等；

(程序插桩 4) 根据不同的缺陷特征，插桩信息收集语句，如内存分配操作，字符串拷贝操作等，应在对应语句后插桩信息收集操作，以便运行时收集信息，辅助判断缺陷是否发生。

在具体实施中，控制流图上的可达性分析计算程序中每一个分支在执行时是否可能到达标记路径片段，主要步骤为：

(可达性分析 1) 计算源代码控制流图 G 并存储；

(可达性分析 2) 对源代码控制流图求反，即节点不变，图的边指向反转，得到图 G' ；

(可达性分析 3) 在反控制流图 G' 上，以一条静态分析警报的疑似路径片段作为起点，对 G' 做遍历；

(可达性分析 4) 在遍历过程中，每到达一个 G 的分支路径，标记该分支路径为到

当前警报的路径片段可达；

(可达性分析 5) 不断重复 (可达性分析 3) 和 (可达性分析 4) 知道所有警报的路径片段都完成可达性分析；

三. 采用路径指导策略的混合执行测试消除误报

混合执行是具体执行、符号执行两种执行操作相结合的一种方法。在具体实施中，程序执行时即实现了具体执行，而符号执行通过预处理中插桩的符号执行操作同步进行。

在具体实施中，深度优先的遍历策略是在对条件约束进行取反时，依次选取路径条件栈栈顶的条件出来进行取反，该策略不断遍历所有遇到的分支，在已有静态分析警报和控制流图的可达性分析条件下，可以进一步优化为路径指导的遍历策略。利用混合执行测试方法生成测试用例，消除误报的步骤：

(消除误报步骤 1) 混合执行测试以一个初始输入做具体执行，从而在第一次执行中收集到符号表达式和符号约束条件。

(消除误报步骤 2) 根据收集到的分支点符号条件，可以形成对当前执行路径的一个约束集合，满足所有这些约束条件的具体值集合按照此程序路径执行。

(消除误报步骤 3) 在具体执行时收集与特定缺陷相关的程序信息，例如，对于缓冲区溢出缺陷，需要收集运行时程序中的缓冲区信息，包括缓冲区的大小，当前使用情况等；对于内存分配和释放操作，收集分配是否成功，内存单元的大小和地址等。

(消除误报步骤 4) 采用路径指导的遍历策略，根据预处理步骤中的控制流图可达性分析，在收集到的路径约束条件集合中，选择到静态分析警报路径片段可达性最优的路径分支，进行取反求解。由于避免了对所有分支取反求解，减少了需要遍历的程序路径空间。

(消除误报步骤 5) 在每一轮执行中或执行结束前，判断当前执行是否覆盖到目标路径片段。如果执行到了疑似缺陷路径，则生成此次运行时缺陷是否触发的一个临时结果，此结果的集合将用于最终确定静态分析警报是否是一个真实的缺陷或误报。

(消除误报步骤 6) 利用约束求解得到的新值作为新的输入，重复 (消除误报步骤 1) 至 (消除误报步骤 6) 的过程，直到满足混合执行停止条件，或达到测试执行迭代次数的上界。

(消除误报步骤 7) 根据测试执行中每一覆盖到目标路径片段的的结果集合，确认特定缺陷是否发生，如果覆盖到警报路径的结果集合中全部没有出发特定缺陷，认为其是误

报。报告上述消除结果。

(消除误报步骤 8) 对于测试执行始终无法覆盖执行到的静态分析警报，将其归为一类无法确定的警报，并提醒开发者或测试人员人工处理。

权 利 要 求 书

1. 一种基于测试的静态分析误报消除方法，其特征在于该方法所包含的步骤为：

步骤 1) 从磁盘文件读取以基于可扩展标记语言的元数据交换格式保存的静态分析报告文件，

步骤 2) 分别从静态分析报告中解析出静态分析警报信息，包括疑似缺陷路径和特定缺陷发生点，形成待验证警报列表，

步骤 3) 采用程序插桩技术在程序源代码中插入标记语句，程序插桩插入的程序语句与原程序同步编译、链接为可执行程序；所述程序插桩或者插桩是在保证被测程序原有逻辑完整性的基础上在程序中插入额外的标记语句，称为探针，通过探针的执行并抛出程序运行的特征数据，通过对这些数据的分析，获得程序的控制流和数据流信息，得到逻辑覆盖等动态信息，实现测试，

步骤 4) 以在程序源代码中插入的静态分析警报的路径片段为目标，在控制流图上计算程序中每一个分支在执行时是否可能到达标记路径片段，所述控制流图是一个有向图，程序源代码中的每个语句对应图中的一个节点，图中节点之间的路径表示程序代码之间的控制关系，

步骤 5) 利用混合执行测试方法生成测试用例，在运行时验证静态分析警报是否是误报，所述混合执行测试方法是符号执行和具体执行结合的测试方法；符号执行指的是使用符号变量代替具体变量，不执行程序的前提下模拟程序执行来进行相关测试分析的技术，与约束满足问题求解方法一同使用；具体执行就是指使用具体的变量值输入到程序中，驱动程序的正常执行进行测试；混合执行是一种对程序交替进行具体执行和符号执行的混合软件程序测试技术，

步骤 6: 根据测试执行中每一覆盖到目标路径片段时记录的结果集合，判断特定缺陷的静态分析警报是否是一个得到确认的缺陷，如果不是，认为其是误报，报告上述确认/误报消除结果，

步骤 7: 对于测试执行始终无法覆盖执行到的静态分析警报，将其归为一类无法确定的警报，并提醒开发者或测试人员人工处理。

2. 根据权利要求 1 所述的基于测试的静态分析误报消除方法，其特征在于，所述的利用混合执行测试方法生成测试用例，在运行时验证静态分析警报是否是误报，具体处理过程如下：

步骤 51) 以一个初始输入做具体执行，在第一次执行中收集符号表达式和符号约束

条件，

步骤 52) 根据收集到的符号约束条件中的分支点，形成对当前执行路径的一个约束组合，满足所有这些约束条件的具体值集合按照此程序路径执行，

步骤 53) 在运行时收集与特定缺陷相关的程序信息，

步骤 54) 对收集到的约束条件集合中的约束条件逐一取反求解，

步骤 55) 在每一轮执行中或执行结束前，判断是否当前执行覆盖到目标路径片段；如果执行到疑似缺陷路径，则生成此次运行时缺陷是否触发的一个临时结果，此结果的集合将用于最终确定静态分析警报是否是一个真实的缺陷或误报，

步骤 56) 利用约束求解得到的新值作为新的输入，重复步骤 51) 的过程，直到满足混合执行停止条件，或达到测试执行迭代次数的上界。

3. 根据权利要求 1 所述的基于测试的静态分析误报消除方法，其特征在于，所述插入标记语句的工作包括：

① 将待验证警报列表中的警报信息标记于源代码中，也就是标记静态分析警报的路径片段中的分支语句和缺陷相关语句，在其前/后插入标记语句，为后续步骤中计算路径片段可达性和运行时标记路径服务，

② 插桩标记符号变量和符号表达式、约束条件，为混合执行中的符号执行服务，

③ 根据不同的缺陷特征，插桩标记内存分配，字符串拷贝等特定缺陷的特征语句，以运行时收集信息，辅助判断缺陷是否发生。

附图

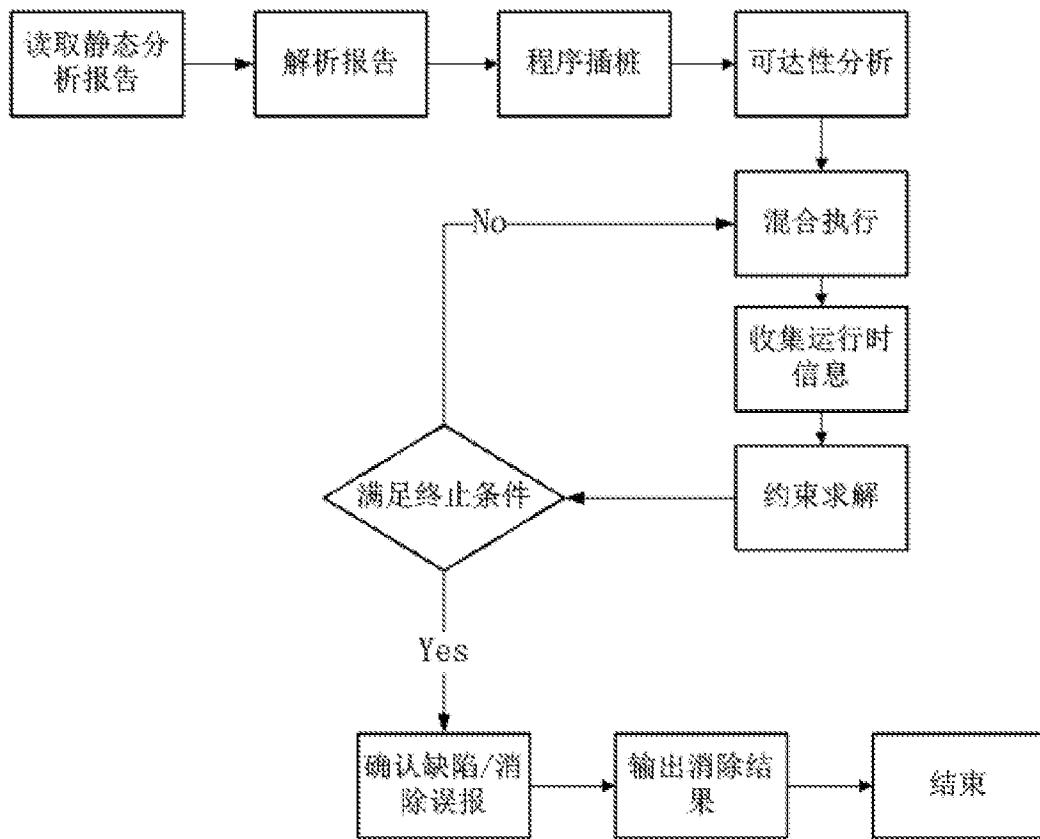


图 1

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN20 13/086993

A. CLASSIFICATION OF SUBJECT MATTER

G06F 19/00 (2011.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, WPI, EPODOC, CNKI, IEEE: concolic w test???, statically w analyz???, alarm???, defect?, statica+, eliminate+, false alarm, instrumentat+, concolic w test???, mixed w execute

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103294594 A (UNIV NANJING) 11 September 2013 (11.09.2013) see the whole document	1-3
X	CUI Zhan-QI, Target-Directed Concolic Testing, CHINESE JOURNAL OF COMPUTERS, June 2011, Vol. 34 No. 6, pages 953-964 see part 4 target-directed concolic testing, figure 2	1-3
A	YU Li-Qian, Combined Static and Dynamic Immutability Analysis of Java Program, CHINESE JOURNAL OF COMPUTERS, April 2010, Vol. 33 No. 4, pages 736-745 see the whole document	1-3
A	CN 102819490 A (UNIV BEIJING POSTS&TELECOM) 12 December 2012 (12.12.2012) see the whole document	1-3
A	CN 102323906 A (UNIV HARBIN ENG) 18 January 2012 (18.01.2012) see the whole document	1-3

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 11 February 2014 (11.02.2014)	Date of mailing of the international search report 06 March 2014 (06.03.2014)
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer SHI, Zhixin Telephone No. (86-10) 62411826

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN201 3/086993

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103294594 A	11.09.2013	None	
CN 102819490 A	12.12.2012	None	
CN 102323906 A	18.01.2012	None	

A. 主题的分类

G06F 19/00 (201 1.01) ;

按照国际专利分类(IPC) 或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06F/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词 (如使用))

CNPAT, WPI, EPODOC,CNKI, IEEE

静态分析, 警报, 误报, 插桩, 消除, 测试, 混合执行, concolic w test???, statically w analyz???, alarm???, defect?, ,

statica+,eliminate+

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 103294594 A (南京大学)11.9 月 2013 (11.09.2013) 参见全文	1-3
X	崔展齐, 一种目标制导的混合执行测试方法, 计算机学报 6 月 201 1,34 卷第 6 期, 第 953-964 页 参见第 4 部分 目标制导的混合执行测试、图 2	1-3
A	于利前, 静动态结合的 Java 程序不变性分析方法, 计算机学报 4 月 2010,33 卷第 4 期, 第 736-745 页 参见全文	1-3
A	CN 102819490 A (北京邮电大学)12.12 月 2012 (12.12.2012) 参见全文	1-3
A	CN 102323906 A (哈尔滨工程大学)18.1 月 2012 (18.01.2012) 参见全文	1-3

☐ 其余文件在 c 栏的续页中列出。

☐ 因 见同族专利附件。

* 引用文件的具体类型:

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的 3/4 之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期

11.2 月 2014 (11.02.2014)

国际检索报告邮寄日期

06.3 月 2014 (06.03.2014)

ISA/CN 的名称和邮寄地址:

中华人民共和国国家知识产权局

中国北京市海淀区蓟门桥西土城路 6 号 100088

传真号: (86-10)62019451

受权官员

石志昕

电话号码: (86-10) 62411826

国际检索报告

关于同族专利的信息

国际申请号

PCT/CN2013/086993

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 103294594 A	11.09.2013	无	
CN 102819490 A	12. 12.2012	无	
CN 102323906 A	18.01.2012	无	