

ICS 35.080
CCS L 77



中华人民共和国国家标准

GB/T 45717—2025

信息技术 软件测量 软件质量测量 自动化的源代码质量测度

Information technology—Software measurement—Software quality
measurement—Automated source code quality measures

(ISO/IEC 5055:2021, MOD)

2025-05-30 发布

2025-12-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	III
引言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 质量测度所涉缺陷及对应元模型	3
6 自动化源代码质量测度缺陷说明	19
7 质量测度的计算	31
附录 A (资料性) 结构编号变化对照一览表	32
附录 B (资料性) 技术差异及其原因一览表	34
附录 C (资料性) 与 GB/T 25000(所有部分)的关系	36
附录 D (资料性) 缺陷密度测度	38
附录 E (资料性) 缺陷和检测模式及对应编程语言一览表	39
附录 F (资料性) 软件元素与 KDM 转换	54
附录 G (资料性) 缺陷模式要素	57
附录 H (资料性) 检测模式要素	74
附录 I (资料性) 自动化源代码质量测度案例	213
参考文献	220

前　　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件修改采用 ISO/IEC 5055:2021《信息技术 软件测量 软件质量测量 自动化的源代码质量测度》。

本文件与 ISO/IEC 5055:2021 相比，在结构上有较多调整。两个文件之间的结构编号变化对照一览表见附录 A。

本文件与“ISO/IEC 5055:2021”相比，存在较多技术差异，在所涉及的条款的外侧页边空白位置用垂直单线（|）进行了标示。这些技术差异及其原因一览表见附录 B。

本文件做了下列编辑性改动：

- 由于 ISO/IEC 5055:2021 的 6.1 概述了第 6 章内容，本文件将其标题由“目的”更改为“概述”；
- 本文件更改了 ISO/IEC 5055:2021 中 6.1 概述其他章条内容时错误引用的章条号：将 6.2、6.3、6.6 依次修正为 6.3、6.4、6.7；
- ISO/IEC 5055:2021 的 6.2 中“这些违规构成自动化源代码信息安全性测度中每个质量测度元素”仅针对信息安全性，本文件更改为“这些违规构成自动化源代码质量测度中每个质量测度元素”，覆盖所有质量特性；
- ISO/IEC 5055:2021 缩略语中已明确 SPMS 为结构化模式元模型标准，本文件将 5.10 标题由“软件模式元模型标准(SPMS)”更改为“结构化模式元模型标准”；
- ISO/IEC 5055:2021 的 6.10 将 6 种模式节错误地统计为 7 种，本文件删除了“参考链接”模式节，因此本文件保留 5 种模式节；
- 由于 ISO/IEC 5055:2021 中针对同一检测模式存在多个编号，本文件更改为针对同一检测模式仅对应一个编号。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：珠海南方软件网络评测中心、中国电子技术标准化研究院、国家应用软件产品质量检验检测中心、广东省科技基础条件平台中心、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）、复旦大学、道普信息技术有限公司、珠海优特电力科技股份有限公司、东信和平科技股份有限公司、远光软件股份有限公司、上海计算机软件技术开发中心、北京工业大学、广州番禺职业技术学院、哈尔滨工业大学、北京谷器数据科技有限公司、广东益安人防工程科技有限公司、南京大学、北京航空航天大学、广西达译科技有限公司、北京科技大学、山东山科数字经济研究院有限公司、华测检测认证集团股份有限公司、重庆市软件评测中心有限公司、北京轩宇信息技术有限公司、江苏赛西科技发展有限公司、北京北大软件工程股份有限公司、北京云起无垠科技有限公司、浪潮软件集团有限公司、深圳开源互联网安全技术有限公司、上海创景信息科技有限公司、浪潮通用软件有限公司、江苏汤谷智能科技有限公司、江苏南方信息技术有限公司、上海市软件评测中心有限公司、西南计算机有限责任公司、中国航天系统科学与工程研究院、北京高质系统科技有限公司、中国科学院微小卫星创新研究院（上海微小卫星工程中心）、上海浦东软件平台有限公司、上海安般信息科技有限公司、苏州洞察云信息技术有限公司、广东拓思软件科学园有限公司、湖南省佳策测评信息技术服务有限公司、北京中科卓信软件测评技术中心、中国航天科工集团第三研究院第三〇四研究所、北京软件和信息服务交易所有限公司、湖南云畅网络科技有限公司、广域铭岛数字科技有限公司、山东浪潮科学研究院有限公司、合肥天帷信息安

全技术有限公司、浙江德迅网络安全技术有限公司、广州淦源智能科技有限公司、深圳市欣中大自动化技术有限公司、全通金信控股(广东)有限公司、众智软件股份有限公司。

本文件主要起草人：侯建华、张旸旸、冯宽、王威、李军、刘健、吴毅坚、韩明军、李伟杰、黄小鹏、向万红、李文鹏、杨尚沅、王在炯、李幸、张瀚文、郭剑虹、周凌云、王宇、袁文强、李绍伟、汤中泽、毕伟、胡芸、刘潇健、张星星、邱旭东、杨鹏、马樱、石龙、王公韬、艾骏、许华寿、黄佳毅、周鸣乐、陈振宇、王亚涛、郑旭飞、高栋栋、高庆、陈安莹、孟建、王颉、凌纪来、朱金波、刘丹、曹骏、李利萍、董冠涛、福德鹏、严亮、施敏华、侯觅、强恺旻、严涵琦、张元元、王萍、颜龙荣、程超、吴俊爽、于铁强、胡艳平、李锐、武建双、叶德望、江淦源、胡大治、胡丙良、吴迪龙、阴玥、王洪秀、魏子重、丁伟。

引　　言

随着计算机在各领域的广泛应用,软件产品的质量受到了越来越多的关注。软件产品的质量不仅直接关系到业务的准确性,还可能对人身安全产生直接影响。因此,选择和开发值得信赖、可靠的软件产品显得至关重要。为了对软件产品的质量进行定量评估,需要明确定义软件产品的质量测度。因此,标准化软件产品的质量测度对于软件质量评估具有极其重要的意义。

近年来,国内软件开发生命周期逐渐在规范,用户从关注软件产品逐渐延伸至关注源代码层面的质量测量。尽管 GB/T 25000.23—2019 为 GB/T 25000.10—2016 中的质量特性定义了软件测度,但这些测度主要集中在软件行为层面,仅在源代码层面提供了一小部分测度,并没有充分定义在开发期间使用的源代码质量测度。因此,不同的合同中供应商对常见的源代码质量测度可能会有不同的解释和计算方法。本文件通过在源代码缺陷层面定义软件质量测度,对 GB/T 25000.23—2019 进行了补充,并增强了源代码层面的测量以支持 GB/T 25000 软件产品质量标准。本文件与 GB/T 25000 标准的关系见附录 C。

本文档旨在针对软件源代码的结构化质量特性进行量化评估。这些质量特性包括维护性、性能效率、可靠性和信息安全性。为此,本文件定义了四个自动化源代码质量测度(ASCQM),即自动化源代码维护性测度(ASCMM)、自动化源代码性能效率测度(ASCPEM)、自动化源代码可靠性测度(ASCRM)和自动化源代码信息安全性测度(ASCSM)。这些自动化源代码质量测度的定义符合 GB/T 25000.10—2016 中需要量化的质量特性的定义。每个测度根据源代码中影响被测量质量特性的缺陷数量来计算,即对源代码中违反良好体系结构和编码实践且可能导致不可接受的运行风险或过高的成本的行为进行检测和统计。

本文件的自动化源代码质量测度并非对上述四个质量特性的所有可能缺陷进行检测,而是专注于严重缺陷的检测和统计。本文件详细列举了 194 种严重缺陷,包括 29 种维护性缺陷、18 种性能效率缺陷、74 种可靠性缺陷以及 73 种信息安全性缺陷。然而,由于部分缺陷同时隶属于多个质量特性,实际上本文件仅包含 137 种独立的缺陷。

虽然国内的源代码静态质量分析自动化工具研发已经取得了一定的成果,但与国外相比,国内的源代码静态质量分析自动化工具在误报和漏报等方面仍存在一些问题,需要进一步完善和改进。目前,针对结构化质量缺陷的分析研究已确定了一系列常见的代码结构模式,这些模式主要依据代码是否符合特定的结构特征来判断其是否存在缺陷。每种缺陷都可以通过一种或多种检测模式来发现,同时,一种检测模式也可能适用于多种缺陷的检测。本文件包含了 135 种检测模式,这些检测模式可以为国内的源代码静态质量分析自动化工具开发提供指导。

本文件的正文部分采用结构化模式元模型标准(SPMs)表示每种缺陷和检测模式,并采用知识发现元模型(KDM)表示这些检测模式的代码元素。在使用四个自动化源代码质量测度对代码进行自动化测量时,本文件提供了针对每个质量测度分别计算缺陷和质量特性分值的两个公式。在评估不同软件的自动化源代码质量测度结果时,由于软件规模、用户对缺陷的关注重点不同等原因,相同的质量测度分值可能产生不同的评估结果。

随着软件工程技术的发展,传统在 IT 应用程序中实现的传统功能现在正转移到嵌入式软件/系统上,开展自动化源代码质量测度对于嵌入式系统、物联网等日渐普及且尤为重要。由于本文件规定的测度中包含的缺陷适用于所有形式的软件,因此本文件不单独描述嵌入式软件的缺陷。

本文件可能会由于新的严重缺陷的增加或模型中现有的缺陷因计算机技术的持续发展而不断升级完善,缺陷和检测模式相关数据会相应增加。因此,本文件将是一个适应计算技术变化的标准。

信息技术 软件测量 软件质量测量 自动化的源代码质量测度

1 范围

本文件规定了针对软件源代码结构化质量特性(维护性、性能效率、可靠性和信息安全性)进行量化评估的自动化的源代码质量测度。

本文件适用于软件的需方、供方和第三方机构利用自动化工具开展的源代码质量测量。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

子缺陷 contributing weakness

在软件中属于另一个缺陷的衍生实例的缺陷。

3.2

圈复杂度 cyclomatic complexity

分析软件单元内部的逻辑路线,计算出独立路径数量。

注: 圈复杂度数值反映了软件单元的逻辑复杂程度。

[来源: QB/T 5275—2018, 3.8, 有修改]

3.3

检测模式 detection pattern

一组已解析程序元素及其关系的抽象表示。

注: 检测模式用形式化表示语言描述,用于检测软件源代码中特定缺陷。

3.4

维护性 maintainability

产品或系统能够被预期的维护人员修改的有效性和效率的程度。

[来源: GB/T 25000.10—2016, 4.3.2.7]

3.5

父缺陷 parent weakness

在软件中有多个衍生实例的缺陷。

3.6

性能效率 performance efficiency

性能与在指定条件下所使用的资源量有关。

注: 资源可包括其他软件产品、系统的软件和硬件配置,以及原材料(如打印纸和存储介质)。

[来源: GB/T 25000.10—2016, 4.3.2.2]