#### 变异测试应用研究综述

**摘要：**

**关键词：**

**1.引言**

（变异测试简介）

（内容简介）

**2.文献检索**

（检索方法）

（文献筛选）

（文献分类）

**3.变异测试应用**

3.1优化回归测试：

（论文的工作和贡献 xxx等人提出了xxx，干了xxx，结果为xxx）

（总结以上工作，共性，差异，问题）·

优化回归测试

回归测试是软件开发和维护过程中保障软件质量的一种重要手段，用于保障代码修改的正确性，并避免代码修改对被测程序的其他模块造成副作用。目前常见的回归测试技术包括：失效测试用例的识别和修复技术、测试用例选择技术、测试用例优先级排序技术、测试用例集约简技术和测试用例集扩充技术等。

变异测试的主要作用在于评估已有的测试用例在被测程序上的充分性。一个变异体(mutant)就是在原被测程序中人为地用变异算子（mutation operator）引入差错，以生成相对于原程序的变异。如果一个测试用例在测试原被测程序和测试变异程序时结果不一致，那么我们说这个测试用例“杀死”了这个变异体；如果一个测试用例未能“杀死”变异体，可能就要考虑这个测试用例对于被测程序的充分性来说是不足的。一个测试用例的充分性得分就是它能够杀死的变异体的数量。

变异测试可以用于优化回归测试。

Goran等人1考察了一个使用突变测试的工业应用程序，涉及3万多名开发人员和190万更改集，用4种编程语言编写。他们指出，使用生产突变的突变测试不会给软件开发过程增加显著的开销，并且报告了开发人员所感知到的突变测试的好处。他们还量化了非有效的突变的成本，结果表明，实现突变充分性既不实际也不理想。Rudolf等人2调查了突变测试在提高安全关键软件系统中单元测试质量方面的适用性和实用性。在改进测试时，在代码中发现了两个新的错误。针对突变体的测试执行需要超过4000小时的计算时间，总的时间大约是半年。他们所研究系统的一个重要特性是它在单元测试中100%的MC/DC覆盖率，这是安全标准所推荐的。这一覆盖水平满足认证要求。他们调查了突变测试在此背景下的适用性和有用性，以评估现有测试的故障检测有效性，并识别测试中的缺陷。他们还调查并量化了在研究的真实世界软件系统中应用突变测试所涉及的工作和成本。他们的结果表明，突变分析对于改进安全关键软件的验证是潜在的有用的。突变测试能够评估已经达到100%覆盖率的测试套件的质量。此外，突变测试提供了测试用例中很难发现的缺陷的提示。这些反馈可以直接用于修改和增强测试。

突变测试依赖于确定性测试行为(对每个突变取模)来确定突变是否被杀死。Maik等人3发现，即使测试始终通过，它们仍然可以在代码覆盖级别上表现出细粒度的不确定性，导致测试不确定地执行突变的代码。这些因素可以解释目前现有的突变测试工具无法检测到的总体突变评分中(平均)4个百分点的变化。他们提出了通过改进的覆盖收集来检测和管理突变测试中的这种flakiness的技术，以确保从测试到它们所覆盖的突变的更可靠的映射，并在突变没有覆盖它们时重新运行测试，直到获得可靠的结果。他们的实验结果表明，这种技术将未知突变体的比例降低了79.4%。

测试用例优先级(TCP)是回归测试的一个重要组成部分，允许更早地检测到错误或帮助减少测试时间和成本。虽然以往研究中存在几种TCP方法，但越来越多的研究对它们进行了针对合成软件缺陷(称为突变体)的评估。因此，目前还不清楚在多大程度上，突变体上的TCP性能可以代表在实际故障上实现的性能。为了回答这个问题，Qi等人4 进行了一次实证研究，比较TCP技术应用于现实世界和突变故障的性能。他们研究的背景包括八个经过充分研究的TCP方法，35k+突变错误，以及在defect ts4j数据集中来自五个Java系统的357个真实的错误。他们的研究结果表明，所研究的TCP技术在突变体上的相对性能可能与在真实故障上的性能没有很强的相关性，这取决于主题程序的属性。这表明，在某些情况下，在一组突变体上表现最好的技术在实际应用到实际故障时可能并不是最好的技术。他们还说明了这些相关性对于由不同算子产生的突变体是不同的，这取决于所选择的算子是否反映了主题程序的典型错误。这突出了为特定程序域开发突变运算符的重要性，尤其是对TCP而言。

针对测试用例优先级，Donghwan等人5  提出了一种新的测试用例优先化技术，它结合了基于变异和基于多样性的方法。他们的基于多样性感知的突变技术依赖于突变区分的概念，该概念旨在将一个突变的行为与另一个突变区别开来，而不是与原始程序区别开来。他们以352个实际故障和553477个开发者编写的测试案例，实证研究了基于突变的优先排序技术（即，使用传统的突变杀灭和拟定的突变区分）的相对成本和有效性。实证评估考虑了各种环境下的传统和多样性感知突变标准：单目标贪婪、混合和多目标优化。 结果表明，基于突变的优先级排序至少在88.9%和77.8%的故障上比随机优先级排序和基于覆盖的优先级排序更有效或同样有效。在贪婪、混合和多目标优化策略中，使用仅杀死和多样性意识突变充分性标准，没有一个更好的测试用例优先化技术。有趣的是，虽然仅杀死突变和多样性意识突变充分性标准之间没有优势，但它们的联合使用提高了优先级排序的有效性。对于多目标优化问题，Pareto前沿排序的有效性与排序目标之间没有稳定的相关性。多目标技术的优先级执行时间大约需要37分钟，而贪婪和混合技术需要不到8秒。他们的研究结果有几点启示。例如，尽早识别和杀死突变体比尽早覆盖语句更有效。

将变异用于优化回归测试的案例已经屡见不鲜。比如Coles等人6 开发了Java使用的变异测试工具PIT。PIT十分迅速，因为它直接操纵字节码，并且优化了变异体的执行。它也十分的鲁棒并且在生产工具中得到了很好的继承，它可以在命令行界面、ANT或者MAVEN这样的包管理器中被调用。Just等人7开发了Java的变异测试工具Major。Major提供了集成于OpenJDK编译器中的变异器，并且为JUnit提供了变异测试的分析工具。Major支持常见的变异算子，如二元运算符置换、单元运算符置换（取反等）、常量置换（数值型和字符串型）、分支条件操纵、删除语句（比如删除一行函数调用）。

基于JavaScript的变异测试工具相对较少，对于NodeJS后端运行环境的变异测试工具更少了。但是随着NPM的使用者越来越多、其上的模块也越来越多，一个模块上的bug可能会导致巨大的影响。Rodríguez-Baquero等人8 开发了面向NodeJS的变异测试工具，并将其用到了NPM最热门的且自带测试用例的前20个模块中的12个。

也有研究指出了当前常见的变异测试工具的不足，并提出了改进。Kintis等人9对Java的三种变异测试框架进行了比较。也测量了生成的等价变异体的百分比。得出的结论是Major，MuJava 和 PIT 均不能包含彼此，即每个工具都还有改进的余地，主要是通过扩展它们所支持的变异种子。测试结果表明，这三种工具并不像预期地那样有效。这也揭示了关于变异测试的理论研究日渐成熟，但是常见的变异测试工具并不能满足研究范式的事实。Laurent等人10指出，大部分的变异测试工具仅使用了少量的且严格的变异算子。由于变异测试的可靠性很大程度上依赖于变异算子的选择，因此这样的现象是令人担忧的。他们使用了扩展的变异算子然并在PIT上进行了实现。在真实的项目中，PIT原有的变异算子产生的变异体更容易被杀死，它们平均比扩展的变异算子生成的评分低了35%到75%。

3.2引导测试生成：

引导测试生成

在软件测试中，测试用例可以定义为一组输入，并开发执行先决条件来验证特定需求是否得到满足，能够满足测试目标的测试用例集称为有效测试套件。手动生成测试用例是一项复杂而又昂贵的任务，自动测试用例生成被认为是手动测试用例生成的一种替代方法，因为它可以减少过程中涉及的成本和时间。

如何生成高效的变异体和测试用例是变异测试研究中的一大方向。变异测试存在一大难点，即难以甄别出与被测程序等价的变异体。等价的变异体是指那些在语法上与被测程序不同，但是在语义上与被测程序相同的变异体。这些变异体不能被测试用例杀死（因为测试用例在等价变异体和被测程序上的行为是一致的，因此无法杀死这些变异体），但是还是要占据相当多的时间和成本去执行这些等价的变异体。Mirshokraie等人11指出，在过往的研究中发现，变异体生成阶段生成的变异体中，生成的10%~40%的变异体均与原程序等价。识别出等价变异体是一项繁杂耗时的人工工作，并且过往的研究集中在如何在变异体生成阶段之后发现等价变异体。Mirshokraie等人提出了一套通用的先验性规则，用于指导变异体生成器生成更少的等价变异体。简单来说，就是结合静态和动态程序分析技术，找出那些更易出错的代码和对程序行为有着显著影响的代码，并优先在这些代码上生成变异体。

变异测试生成的另一大难点是生成的变异体数量庞杂，测试成本高昂。Zhang等人12使用对变异体设置优先级和精简用到的变异体的方法，以快速地找出被杀死的和未被杀死的变异体，从而降低了所需生成的变异体的数量。

在过去，大多数关于变异测试的研究工作都集中在寻找非科学软件中的缺陷。所提出的方法旨在借助生物启发算法来改进过程，以识别科学代码中的变异体。科学软件依赖于输出的准确性而不是正确性。因此，一般的变异测试不足以发现错误，因为科学软件即使对小的舍入误差也很敏感。Nishtha等人13提出一种新的算法。他们使用的基于搜索的技术是一种改进的Crow Search Algorithm（CSA）用于生成测试数据。 在CSA中，搜索模式取决于称为飞行长度的独立参数。这可能导致搜索解决方案被困在本地区域内的问题。因此，提出的改进的ICSA方法为每个测试用例生成柯西随机数，以防止搜索陷入局部搜索，因此解决了CSA中的一些限制。

3.3缺陷定位：

在整个调试活动中，缺陷定位一直是一个代价昂贵的阶段。传统的人工定位需要测试者努力理解被测程序的复杂内部逻辑，以及测试通过和失败的运行之间的差异，这无疑是一个耗时耗力的工程，特别是对经验不足的开发者而言。

由此，自动缺陷定位技术得到了广泛的研究，目前最流行的方法是基于频谱的缺陷定位（SBFL）。该方法使用程序谱（即测试套件执行的信息概要），根据预测的包含缺陷的风险对程序语句进行排序。然后，开发人员将按照给定排名中语句的顺序检查被测程序，希望在排名顶部附近会遇到错误语句。但是这样的方法消耗较多程序运行时间成本和资源成本，且测试用例的数量和质量对缺陷定位性能影响较大。此外，此方法因为使用的模型（排名的线性检验）不具备足够的现实性和较低的准确性，也一直受到批评。

因此，有很多人开始考虑其他方法的缺陷定位，基于变异测试思想的缺陷定位正是目前许多人的研究方向。

Mike Papadakis等人考虑了一种基于变异分析的缺陷定位方法，通过人为地向代码中注入缺陷来探索程序的行为，并获得一些可用于自动故障定位的信息，该方法与现有的基于频谱的缺陷定位方法进行比较，结果显示明显优于后者。又由于应用变异分析需要消耗大量的计算资源，他们将选择性变异技术应用到缺陷定位问题，并确定了故障定位背景下具有代表性的变异算子集，来减少变异体数量。最终实验的结果表明，该方法能够将涉及的突变体数量减少80%，而不会损失故障定位精度。

Yves Le Traon等人提出了一种基于变异分析的故障定位方法——Metallaxis，其创新之处在于它使用了变异体，并将它们与错误的程序位置联系起来。因此，大部分因测试失败而死亡的变异体提供了一个关于故障位置的良好指示。使用Metallaxis的实验表明，它比基于语句的方法更有效。即使在有助于降低变异成本的技术（如变异采样）的情况下，这也是正确的。此外，受控实验的结果表明，使用变异作为测试技术有利于缺陷定位过程。因此，通过使用基于变异的测试套件而不是基于块或基于分支的测试套件，可以显著改进缺陷定位。他们还证明了Metallaxis具有良好的可扩展性。

Seokhyeon Moon等人提出了一种新的基于变异测试的故障定位技术——MUSE，MUSE使用变异分析来唯一地捕捉单个程序语句和观察到的故障之间的关系，而不受来自块结构的共享排名的强制影响。其基本思想是，由于错误的程序可以通过修改错误的语句来修复，因此修改错误的语句将使更多失败的测试用例通过。相比之下，由于改变正确的语句会引入新的错误语句，因此改变正确的语句将使更多通过的测试用例失败。

Seokhyeon Moon等人还为缺陷定位技术提出了一种新的评估指标，LIL（位置信息损失），其利用信息理论，通过定位技术测量断层的真实位置和预测位置之间的信息损失。LIL可以应用于任何故障定位技术，并描述任意数量缺陷的定位。最终，使用传统的消耗指标和提出的LIL指标，针对五个真实世界程序的14个错误版本评估MUSE。结果表明，平均而言，MUSE比目前最先进的SBFL技术Op2准确约25倍

。

通过对这些文献的深入分析，可以发现将变异分析引入缺陷定位问题，在准确性上都明显优于目前主流的基于频谱的缺陷定位技术（SBFL）。然而两种方法都会消耗大量的计算资源，对于基于变异分析的缺陷定位，这是由于变异测试本身要求生成大量变异体（其中大部分都为无效的等价变异体）所造成的，因此研究人员也在积极探究使用各种技术，如使用选择性变异技术，来降低变异分析的资源消耗。

3.4 AI测试：

根据寻找到的文献进行分析和比对，变异测试在AI测试的应用主要有以下几个方面：（1）用于检测和评估DNN的鲁棒性；（2）用于检测DNN受到的对抗样本攻击；

3.5其他应用：

**4.总结：**

（总结前文）

（现有研究的不足）

（对未来研究的看法）

**参考文献**

[1] G. Petrovic, M. Ivankovic, B. Kurtz, P. Ammann and R. Just, "An Industrial Application of Mutation Testing: Lessons, Challenges, and Research Directions," 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 2018, pp. 47-53, doi: 10.1109/ICSTW.2018.00027.

[2] Rudolf Ramler, Thomas Wetzlmaier, and Claus Klammer. 2017. An empirical study on the application of mutation testing for a safety-critical industrial software system. In Proceedings of the Symposium on Applied Computing (SAC '17). Association for Computing Machinery, New York, NY, USA, 1401–1408.

[3] Betka M, Wagner S. Towards practical application of mutation testing in industry—Traditional versus extreme mutation testing[J]. Journal of Software: Evolution and Process, 2022: e2450.

[4] Luo Q, Moran K, Poshyvanyk D, et al. Assessing test case prioritization on real faults and mutants[C]//2018 IEEE international conference on software maintenance and evolution (ICSME). IEEE, 2018: 240-251.

[5] Shin D, Yoo S, Papadakis M, et al. Empirical evaluation of mutation‐based test case prioritization techniques[J]. Software Testing, Verification and Reliability, 2019, 29(1-2): e1695.

[6] Coles, Henry, et al. "Pit: a practical mutation testing tool for java." Proceedings of the 25th international symposium on software testing and analysis. 2016.

[7] Just, René. "The Major mutation framework: Efficient and scalable mutation analysis for Java." Proceedings of the 2014 international symposium on software testing and analysis. 2014.

[8] Rodríguez-Baquero, Diego, and Mario Linares-Vásquez. "Mutode: generic javascript and node. js mutation testing tool." Proceedings of the 27th ACM SIGSOFT International Symposium on Software Testing and Analysis. 2018.

[9] Kintis, Marinos, et al. "Analysing and comparing the effectiveness of mutation testing tools: A manual study." 2016 IEEE 16th International Working Conference on Source Code Analysis and Manipulation (SCAM). IEEE, 2016.

[10] Laurent, Thomas, et al. "Assessing and improving the mutation testing practice of pit." 2017 IEEE International Conference on Software Testing, Verification and Validation (ICST). IEEE, 2017.

[11] Mirshokraie, Shabnam, Ali Mesbah, and Karthik Pattabiraman. "Efficient JavaScript mutation testing." 2013 IEEE Sixth International Conference on Software Testing, Verification and Validation. IEEE, 2013.

[12] Zhang, Lingming, Darko Marinov, and Sarfraz Khurshid. "Faster mutation testing inspired by test prioritization and reduction." Proceedings of the 2013 International Symposium on Software Testing and Analysis. 2013.

[13] Jatana, Nishtha; Suri, Bharti (2020). An Improved Crow Search Algorithm for Test Data Generation Using Search-Based Mutation Testing. Neural Processing Letters, (), –. doi:10.1007/s11063-020-10288-7