Universidade Federal da Bahia
Instituto de Matemática

Programa de Pós-graduação em Ciência da Computação

CARACTERIZAÇÃO DA QUALIDADE INTERNA DE FERRAMENTAS DE ANÁLISE ESTÁTICA DE CÓDIGO FONTE

Joenio Marques da Costa
joenio@joenio.me

QUALIFICAÇÃO DE MESTRADO

Salvador
18 de maio de 2016

Universidade Federal da Bahia
Instituto de Matemática

Joenio Marques da Costa
joenio@joenio.me

CARACTERIZAÇÃO DA QUALIDADE INTERNA DE FERRAMENTAS DE ANÁLISE ESTÁTICA DE CÓDIGO FONTE

Trabalho apresentado ao Programa de Pós-graduação em Ciência da Computação do Instituto de Matemática da Universidade Federal da Bahia como requisito parcial para obtenção do grau de Mestre em Ciência da Computação.

Orientadora: Profa. Dra. Christina von Flach G. Chavez
Co-orientador: Prof. Dr. Paulo Roberto Miranda Meirelles

Salvador
18 de maio de 2016

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

CAPÍTULO 1

INTRODUÇÃO

(à fazer)

1.1 CONTRIBUIÇÕES ESPERADAS

(à fazer)

CAPÍTULO 2

FUNDAMENTAÇÃO TEÓRICA

2.1 ENGENHARIA DE SOFTWARE

Sistemas de software são utilizados em praticamente todas as áreas do conhecimento humano e têm exercido um papel essencial em nossa sociedade (MAFRA; TRAVASSOS, 2006). A dependência crescente de serviços oferecidos por tais sistemas evidencia a necessidade de produzir software de qualidade, contornando os desafios relacionados a funcionalidades incompletas ou incorretas, custos acima do esperado ou prazos não cumpridos.

Diante destes desafios, surge a Engenharia de Software, uma disciplina centrada no desenvolvimento de sistemas de software através de uma abordagem sistemática, disciplinada, e quantificável para o desenvolvimento, operação e manutenção (SOCIETY, 2014).

Nas últimas décadas, o foco em estudos empíricos na área de Engenharia de Software tem crescido significantemente (STOL; FITZGERALD, 2015), resultando no uso crescente de métodos como surveys, estudos de caso, experimentos e revisões sistemáticas de literatura. Através destes estudos empíricos, pesquisadores transformam a Engenharia de Software em uma disciplina mais científica e controlável – a Engenharia de Software Experimental – provendo meios para avaliar e validar métodos, técnicas, linguagens e ferramentas.

Não raro, muitos destes estudos criam novos sistemas de software, tais sistemas costumam ser utilizados como meio para atingir os resultados da pesquisa ou, em alguns casos, são o próprio fim do estudo realizado. Neste trabalho, tais ferramentas de software são nosso objeto de pesquisa e serão chamados de "software científico" – Portillo-Rodríguez et al. (2012) utiliza o termo "research tool"para designar este mesmo tipo de software.

2.2 SOFTWARE CIENTÍFICO

Softwares científicos são ferramentas de software desenvolvidas no decorrer de pesquisas científicas como parte de um estudo, podem ser pequenos scripts, protótipos, ou mesmo produtos de software completos que demonstram ou refletem os resultados de uma pesquisa. Em Engenharia de Software este tipo de software desempenha um papel essencial e sua importância pode ser notada através do grande número de conferências com sessões específicas sobre publicação de ferramentas.

Kon et al. (2011) em um estudo sobre como pesquisas em Engenharia de Software podem se beneficiar do ecosistema de Software Livre faz uma análise de 10 edições do SBES[1] e conclui que apesar do aumento do interesse por parte dos pesquisadores em

[1]Simpósio Brasileiro de Engenharia de Software

disponibilizar o código-fonte de suas ferramentas isto ainda é minoria. O que confirma a preocupação de Krishnamurthi e Vitek (2015) em um estudo sobre repetibilidade de pesquisas científicas, onde chamam atenção para o papel central que os artefatos de software possuem em pesquisas de ciência da computação e questionam: "Onde está o software nas pesquisas sobre linguagem de programação?".

A partir daí podemos afirmar que softwares científicos são peça fundamental para que pesquisadores independentes possam reproduzir, validar ou expandir os resultados encontrados em estudos anteriores e assim aumentar o rigor e a qualidade científica de tais pesquisas (VITEK; KALIBERA, 2011).

2.3 REPRODUTIBILIDADE

Reprodutibilidade é a habilidade de replicar um experimento ou estudo em sua totalidade a fim de confirmar suas hipóteses e resultados, apesar de ser uma prática central do método científico ainda é um grande obstáculo em muitos estudos. Enquanto pesquisadores publicam artigos descrevendo e divulgando seus resultados, é raro que façam o mesmo com toda a produção gerada durante a pesquisa. A maioria dos componentes necessários para a reprodução dos resultados de uma pesquisa – por exemplo, código-fonte e dados – usualmente permanecem não publicados.

Isto se configura como uma barreira para a reprodutibilidade, e consequentemente para a repetição, replicação e variação de estudos (FEITELSON, 2015) já que a disponibilidade de código-fonte é o mínimo necessário para que isto ocorra, como pode ser visto no espectro de reprodutibilidade de Peng (2011) reproduzido aqui na Figura 2.1.

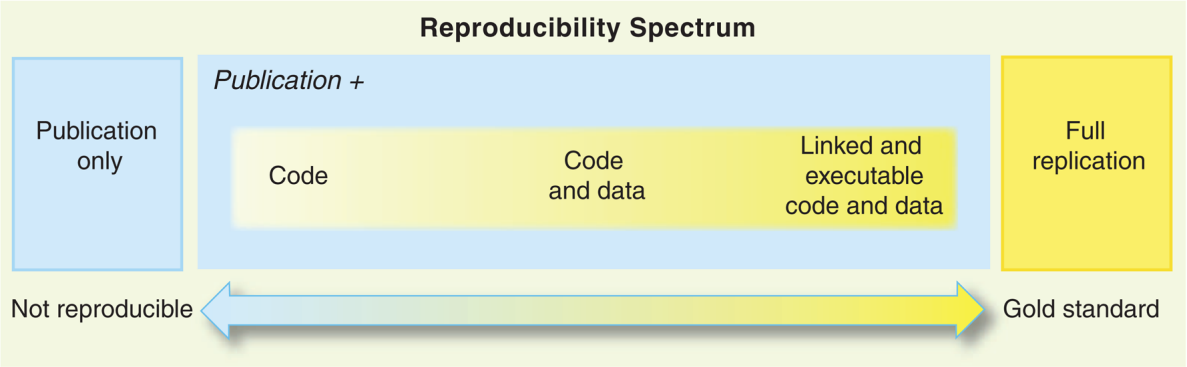

Figura 2.1 The spectrum of reproducibility(PENG, 2011)

Dentro deste contexto, e considerando que muitos estudos ainda sofrem com dificuldades de repetição (KAZMAN, 2016), surge a preocupação de avaliar a qualidade dos softwares científicos a partir de métodos adequados, especialmente em relação a sua manutenabilidade e disponibilidade por serem problemas comuns enfrentados pelos pesquisadores (PRLIć; PROCTER, 2012).

2.4 QUALIDADE DE SOFTWARE

Qualidade de software diz respeito à quão bem um software é projetado e o quanto este software está em conformidade com o projeto, embora existam inúmeras definições há um concenso de que existem duas dimensões básicas para medir a qualidade de um software, estas dimensões estão relacionadas à características de qualidade interna e de qualidade externa.

Segundo McConnell (2004), qualidade interna são aquelas características que preocupam o desenvolvedor, como: manutenabilidade, flexibilidade, portabilidade, reusabilidade, legibilidade, testabilidade e compreensão. São questões relacionadas ao código-fonte e em como o software foi construído, como design e boas práticas por exemplo.

Qualidade externa são aquelas características que afetam o usuário, como por exemplo: exatidão, usabilidade, eficiência, confiabilidade, integridade, adaptabilidade, acurácia e robustez. Estas características impactam extritamente no uso do software e não em como o software foi construído.

Segundo a ISO/IEC 25010 (ISO, 2011) estas características podem ser divididas em subcaracterísticas. A característica usabilidade por exemplo é dividida nas seguintes subcaracterísticas: capacidade de compreensão, capacidade de aprendizado, operabilidade, atratividade e conformidade. Esta característica está relacionada, por exemplo, a facilidade com que usuários aprendem e utilizam um sistema, e passa por questões como facilidade de instalação, aprendizado, e uso.

Sabe-se que, em algum nível, as caractarísticas de qualidade interna afetam as características de qualidade externa (MCCONNELL, 2004), softwares que não possuem boa manutenabilidade por exemplo afetam a habilidade de correção de defeitos, que por sua vez afetam as características de exatidão e confiabilidade.

Dito isto podemos perceber que é possível inferir características de qualidade externa de um software a partir de suas qualidades internas, o que pode ser realizado a partir da análise de suas métricas de código-fonte.

2.5 MÉTRICAS DE CÓDIGO-FONTE

Uma métrica, segundo a definição da ISO/IEC 25010 (ISO, 2011), é a composição de procedimentos para a definição de escalas e métodos para medidas, em engenharia de software estas métricas podem ser classificadas em três categorias: métricas de produto, métricas de processo e métricas de projeto.

Métricas de produto são aquelas que descrevem as características de artefatos do desenvolvimento, como documentos, diagramas, código-fonte e arquivos binários. Métricas de processo medem atributos relacionados ao ciclo de desenvolvimento do software. Métricas de projeto são aquelas que descrevem as características dos recursos disponíveis ao desenvolvimento.

Neste trabalho nosso interesse estão nas métricas de produto, que podem ser classificadas entre internas ou externas, ou seja, aquelas que medem propriedades visíveis apenas aos desenvolvedores ou que medem propriedades visíveis aos usuários, respectivamente. Iremos extrair propriedades dos softwares científicos a fim de medir a sua qualidade in-

terna através de um conjunto de métricas previamente definido, este conjunto tomará como base o trabalho realizado por Meirelles (2013) onde foi realizado um estudo associando qualidade de software à qualidade de código-fonte através da observação de métricas de código-fonte. E será realizado através de ferramentas de análise estática de código-fonte.

2.6 FERRAMENTAS DE ANÁLISE ESTÁTICA DE CÓDIGO-FONTE

Ferramentas de análise estática de código-fonte são ferramentas capazes de realizar a leitura de código-fonte de um projeto de software de forma automatizada ou semi-automatizada e extrair daí informações sobre as entidades do software, como módulos, classes, funções, métodos, variáveis, seus relacionamentos, suas características e diversas outras informações possíveis de serem exraídas diretamente do código-fonte que seja útil ao engenheiro de software.

Estas informaçoes costumam ser aplicadas à tarefas comuns da engenharia de software, como por exemplo, recuperação arquitetural, localização de falhas, manutenção, refatoração, compreensão, análise de performance, visualização, entre outras.

Segundo Kirkov e Agre (2010) estas ferramentas possuem uma anatomia comum, composta de quatro componentes básicos - construção de modelos; algoritmos de análise e reconhecimento de padrões; base de conhecimento de padrões; e representação final.

A construção de modelos de um programa é o primeiro passo e é feito por um parser de código-fonte (BINKLEY, 2007). A base de conhecimento de padrões é usada para representar e armazenar informações sobre potenciais problemas encontrados no código-fonte. O objetivo do algoritmo de análise e reconhecumento de padroes é classificar as informações encontradas no modelo a partir da base de conhecumento de padroes. A representação final é um relatório ou outro tipo de visualização apresentada através de uma interface de usuário apropriada.

Esta representação final pode ser por exemplo um relatório contendo os valores de métricas calculadas para o software sendo analisado, e é esta caractarística das ferramentas de análise estática de código-fonte que será utilizada neste trabalho para recuperar métricas de produto de software que reflitam os atributos de qualidade dos software científicos estudados.

CAPÍTULO 3

METODOLOGIA

Será feito um levantamento de softwares científicos e softwares da indústria do domínio *análise estática de código-fonte*. Este domínio foi selecionado com base na experiência do pesquisador nesta área, o que facilita encontrar fontes sobre ferramentas, bem como analisar e estudar tais softwares. O foco em um domínio se justifica pela necessidade de reduzir o escopo do estudo a fim de viabilizar o trabalho dentro do tempo previsto em um programa de mestrado.

Após o levantamento e seleção das ferramentas será feita a caracterização inicial e posteriormente análise estática do seu código-fonte, onde teremos métricas para cada ferramenta e possivelmente valores referência para ferramentas de análise estática, estes valores de referência darão origem a recomendações de refatoração para ferramentas deste domínio.

Por final traçaremos um paralelo entre caracteristicas de qualidade externa e valores de métricas de qualidade interna, especialmente em relação à portabilidade e usabilidade respondendo as seguintes questões:

- O software pode ser instalado facilmente? (Portability: Installability)
  - O software possui alguma instrução de instalação? (understandability ou learnability)
  - O software é facilmente encontrado para obtenção? (download, requisito para operability)
- O usuário consegue utilizar o sistema sem muito esforço? (Usability: Operability)
  - O software ao ser instalado devidamente executa suas funções mínimas sem erros? (compliance)

As seções à seguir descrevem em detalhes as atividades de cada etapa da metodologia.

3.1 HIPÓTESES

São hipóteses deste estudo:

H1: *Existem publicações sobre ferramentas de análise estática com disponibilidade de código-fonte*

H2: *Existem ferramentas de análise estática disponíveis livremente na indústria com disponibilidade de código-fonte*

H3: *Existem valores de referência para métricas de código-fonte para ferramentas de análise estática*

H4: *Ferramentas da indústria possuem melhores valores de métricas de código-fonte*

H5: *É possível relacionar a característica de qualidade externa usabilidade à valores de métricas de qualidade interna*

3.2 PLANEJAMENTO DO ESTUDO

3.2.1 Seleção das métricas

Meirelles (2013) realizou uma série de estudos onde associou características da qualidades de produto de software à características de qualidade de código-fonte através de métricas como indicador para o sucesso de projetos de software livre. Em um destes estudos um dos critérios utilizados para a seleção de métricas foi escolher aquelas que medem aspectos relevantes à manutenibilidade do software.

Nós iremos aqui utilizar a mesma seleção de métricas utilizadas por Meirelles (2013) a fim de caracterizar a qualidade interna das ferramentas de análise estática previamente selecionadas.

LOC *Número total de linhas de código*

NM *Número total de módulos*

CBO *Média do acoplamento entre objetos*

LCOM4 *Média da falta de coesão entre métodos*

SC *Complexidade estrutural*

3.2.2 Seleção da ferramenta de análise estática de código-fonte

Para realizar a caracterização das ferramentas e extrair suas métricas de código-fonte será necessário uma ferramenta que permita automatizar este processo, neste trabalho utilizaremos a ferramenta de análise estática Analizo (KON, 2010).

Analizo é um *toolkit* livre, multi-linguagem e extensível para análise de código-fonte, é uma ferramenta mantida constantemente, com desenvolvedores ativos, eu sou um dos desenvolvedores dessa ferramenta o que me dá a capacidade de realizar atualizações ou correção de problemas ao longo deste estudo caso isto venha a ser necessário.

3.2.3 Seleção das fontes de ferramentas de análise estática

Para ser possível validar as hipóteses aqui levantadas é necessário realizar uma busca por ferramentas de análise estática desenvolvidas no contexto da academia e da indústria, para isso, será feito um planejamento detalhado para realizar a seleção de ferramentas em cada um destes contextos.

No contexto acadêmica a busca por ferramentas será feita através de artigos publicados em conferências que tenham histórico de publicação sobre ferramentas de análise estática de código fonte. Estes artigos serão analisados e aqueles com publicação de ferramenta de análise estática serão selecionados.

Na indústria a busca por ferramentas será feita a partir de referências encontradas na internet, algumas organizações mantém listas de ferramentas para análise de código-fonte, a Wikipedia também mantém uma lista de ferramentas, estas referências serão utilizadas como ponto de partida e cada ferramenta será analisada a fim de validar se são da indústria ou surgiram em contexto acadêmico.

Uma vez que as ferramentas tenham sido selecionadas inicia-se a extração de seus atributos de qualidade interna.

3.3 COLETA DE DADOS

A partir das fontes selecionadas na etapa anterior serão realizadas duas atividades para identificar e mapear as ferramentas de análise estática com código-fonte disponível, uma atividade relacionada ao levantamento de ferramentas da academia, outra atividade relacionada ao levantamento de ferramentas da indústria.

3.3.1 Ferramentas da academia

A seleção de ferramentas será relizada através de uma revisão estruturada dos artigos selecionados a partir das seguintes conferências:

- ASE - Automated Software Engineering[1]
- CSMR[2] - Conference on Software Maintenance and Reengineering[3]
- SCAM - Source Code Analysis and Manipulation Working Conference[4]
- ICSME - International Conference on Software Maintenance and Evolution[5]

Chamamos de revisão estruturada um processo disciplinado para seleção de artigos a partir de critérios bem definidos de forma que seja possível a reprodução do estudo por parte de pesquisadores interessados. Alguns resultados preliminares podem ser consultados na Tabela 4.1 da Seção 4.1.

3.3.2 Ferramentas da indústria

A seleção de ferramentas da indústria será feita a partir de uma busca manual em fontes encontradas na Internet sobre ferramentas de análise estática.

[1] http://ase-conferences.org

[2] A conferência CSMR tornou-se SANER - Software Analysis, Evolution, and Reengineering a partir da edição 2015.

[3] http://ansymore.uantwerpen.be/csmr-wcre

[4] http://www.ieee-scam.org

[5] http://www.icsme.org

O projeto SAMATE[6] - *Software Assurance Metrics and Tool Evaluation* disponível em NIST (2016) mantém uma lista de ferramentas de análise estática mantida, mais sobre o projeto SAMATE pode ser encontrado em Ribeiro (2015).

O software Spin mantém em seu site uma lista de ferramentas comerciais e de pesquisa para análise estática de código-fonte para C em Spin (2016).

O Instituto de Engenharia de Software do CERT mantém uma lista de ferramentas de análise estática em CERT (2016).

O software Flawfinder oferece em seu site um link com referências para inúmeras ferramentas livres, proprietárias, gratuitas mas não-livres de ferramentas de análise estática e outros tipos de análise em Wheeler (2015).

Uma outra fonte contendo uma relação expressiva de ferramentas é mantida na Wikipedia em Wikipedia (2016).

Estas fontes serão pesquisadas manualmente em busca de ferramentas de análise estática que tenham sido desenvolvidas no contexto da indústria, algums resultados preliminares podem ser encontrados nas Tabelas 4.3 e 4.2.

3.3.3 Caracterização dos artigos

Os artigos selecionados a partir da revisão estruturada serão avaliados a fim de caracterizar se se tratam de publicação de ferramenta de análise estática de código-fonte, esta revisão será realizada de forma semi-automatizada com base num script[7] que fará o primeiro filtro dos artigos a partir de uma busca no conteúdo a partir dos seguintes termos:

```
"tool"; E
"download" OU "available"; E
"http" OU "ftp"; E
"static analysis" OU "parser".
```

Caracterização dos papers analisados na revisão estruturada e caracterização teórica do ecosistema das ferramentas da academia.

3.3.4 Caracterização das ferramentas

Será realizada uma caracterização prática das ferramentas, tanto acadêmica quando da indústria, através da análise e extração de métricas de código-fonte das mesmas.

3.4 EXEMPLO DE USO

Por fim, os valores de métricas de referência encontradas serão utilizadas como guia para refatorar a ferramenta Analizo.

(ler o TCC "Código Limpo e seu Mapeamento para Métricas de Código Fonte"onde foi feito trabalho similar)

[6] http://samate.nist.gov

[7] http://github.com/joenio/dissertacao-ufba-2016/blob/master/revisao-estruturada/filter

CAPÍTULO 4

CONCLUSÃO

4.1 RESULTADOS PRELIMINARES

A Tabela 4.1 apresenta um resumo do número de artigos em cada edição do SCAM e quantos artigos trazem publicação de ferramenta de análise estática com código fonte disponível.

As Tabelas 4.3 e 4.2 apresentam ferramentas do NIST após avaliação inicial sobre disponibilidade do código-fonte. Das 54 ferramentas apenas 19 tinham código fonte disponível.

Assim, temos um total de 19 ferramentas da indústria com código-fonte disponível e ??? da academia com código fonte disponível, é preciso avaliar em qual linguagem de programação foi escrita cada ferramentas pois só iremos analisar aquelas em C, C++ ou Java que são suportadas pelo Analizo.

A ferramenta utilizada para identificar a linguagem de programação em que estes softwares foram escritos foi a sloccount, uma ferramenta livre para contagem de linhas de código fonte, onde se calcula em quais linguagens de programação um software foi escrito.

Após analise ficamos com um total de 25 ferramentas, 15 da indústria e 10 da academia, a Tabela 4.4 traz um resumo de todos as ferramentas analisadas.

4.2 CRONOGRAMA

(à fazer)

Tabela 4.1 Total de artigos analisados por edições do SCAM

Edição	Total de artigos	Artigos com ferramenta
SCAM 2001	23	-
SCAM 2002	18	-
SCAM 2003	21	-
SCAM 2004	17	-
SCAM 2005	19	-
SCAM 2006	22	2
SCAM 2007	23	1
SCAM 2008	29	-
SCAM 2009	20	-
SCAM 2010	21	1
SCAM 2011	21	1
SCAM 2012	22	4
SCAM 2013	24	-
SCAM 2014	35	1
SCAM 2015	?? (pendente)	?
Total	315	10

Tabela 4.2 Lista de ferramentas do SAMATE - NIST com código fonte não disponível

Ferramenta	Avaliacao
ABASH	código não disponível
ApexSec Security Console	código não disponível
Astrée	código não disponível
bugScout	código não disponível
C/C++test®	código não disponível
dotTEST™	código não disponível
Jtest®	código não disponível
HP Code Advisor (cadvise)	código não disponível
Checkmarx CxSAST	código não disponível
CodeCenter	código não disponível
CodePeer	código não disponível
CodeSecure	site offline
CodeSonar	código não disponível
Coverity SAVE™	código não disponível
Csur	código não disponível
DoubleCheck	código não disponível
Fluid	código não disponível
Goanna Studio and Goanna Central	código não disponível
HP QAInspect	código não disponível
Insight	código não disponível
ObjectCenter	código não disponível
Parfait	código não disponível
PLSQLScanner 2008	código não disponível
PHP-Sat	link para código offline
PolySpace	código não disponível
PREfix and PREfast	código não disponivel
QA-C, QA-C++, QA-J	código não disponível
Qualitychecker	código não disponível
Rational AppScan Source Edition	código não disponível
Resource Standard Metrics (RSM)	código não disponível
SCA	código não disponível
SPARK tool set	código não disponível
TBmisra®, TBsecure®	código não disponível
PVS-Studio	código não disponível
xg++	código não disponível

Tabela 4.3 Lista de ferramentas do SAMATE - NIST com código fonte disponível

Ferramenta	Avaliacao
BOON	código disponível
Clang Static Analyzer	código disponível
Closure Compiler	código disponível
Cppcheck	código disponível
CQual	código disponível
FindBugs	código disponível
FindSecurityBugs	código disponível
Flawfinder	código disponível
Jlint	código disponível
LAPSE	código disponível
Pixy	código disponível
PMD	código disponível
pylint	codigo disponivel
RATS (Rough Auditing Tool for Security)	código disponível
Smatch	código disponível
Splint	código disponível
UNO	código disponível
Yasca	código disponível
WAP	código disponível

Tabela 4.4 Lista com total de ferramentas a serem analisadas

Ferramenta	Linguagem	Fonte
BOON	ansic	industria
CQual	ansic	industria
RATS	ansic	industria
Smatch	ansic	industria
Splint	ansic	industria
UNO	ansic	industria
Clang Static Analyzer	cpp	industria
Cppcheck	cpp	industria
Jlint	cpp	industria
WAP	java	industria
Closure Compiler	java	industria
FindBugs	java	industria
FindSecurityBugs	java	industria
Pixy	java	industria
PMD	java	industria
Indus	java	academia
TACLE	java	academia
JastAdd	java	academia
WALA	java	academia
error-prone	java	academia
AccessAnalysis	java	academia
Bakar Alir	java/ada/python	academia
InputTracer	ansic	academia
srcML	cpp/cs (cs = C# ?)	academia
Source Meter	java	academia

REFERÊNCIAS BIBLIOGRÁFICAS

BINKLEY, D. Source code analysis: A road map. In: IEEE COMPUTER SOCIETY. *2007 Future of Software Engineering*. [S.l.], 2007. p. 104–119.

CERT. *Secure Coding Tools*. 2016. [Online; acessado 23 Abril de 2016]. Disponível em: ⟨http://www.cert.org/secure-coding/tools/index.cfm⟩.

FEITELSON, D. G. From repeatability to reproducibility and corroboration. *ACM SIGOPS Operating Systems Review*, ACM, v. 49, n. 1, p. 3–11, 2015.

ISO, I. Iec25010: 2011 systems and software engineering–systems and software quality requirements and evaluation (square)–system and software quality models. *International Organization for Standardization*, p. 34, 2011.

KAZMAN, A. T. R. On the worthiness of software engineering research. 2016. Disponível em: ⟨http://shidler.hawaii.edu/sites/shidler.hawaii.edu/files/users/kazman/se_research_worthiness.pdf⟩.

KIRKOV, R.; AGRE, G. Source code analysis - an overview. *Cybernetics and Information Technologies*, v. 10, n. 2, p. 60–77, 2010.

KON, A. T. J. C. J. M. P. M. L. R. R. L. A. C. C. F. Analizo: an extensible multi-language source code analysis and visualization toolkit. p. 6, 2010.

KON, F. et al. Free and open source software development and research: Opportunities for software engineering. In: *SBES*. [s.n.], 2011. p. 82–91. Disponível em: ⟨http://dblp.org/db/conf/sbes/sbes2011.html\\#KonMLTCM11⟩.

KRISHNAMURTHI, S.; VITEK, J. The real software crisis: Repeatability as a core value. *Communications of the ACM*, ACM, v. 58, n. 3, p. 34–36, 2015.

MAFRA, S. N.; TRAVASSOS, G. H. Estudos primários e secundários apoiando a busca por evidência em engenharia de software. 2006.

MCCONNELL, S. *Code Complete*. 2nd. ed. [S.l.]: Microsoft Press, 2004.

MEIRELLES, P. R. M. *Monitoramento de métricas de código-fonte em projetos de software livre*. Tese (Doutorado) — Universidade de São Paulo, São Paulo, Brazil, 2013.

NIST. *SAMATE - Source Code Security Analyzers*. 2016. [Online; acessado 20 Abril de 2016]. Disponível em: ⟨http://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html⟩.

PENG, R. D. Reproducible research in computational science. *Science (New York, Ny)*, NIH Public Access, v. 334, n. 6060, p. 1226, 2011.

PORTILLO-RODRíGUEZ, J. et al. Tools used in global software engineering: A systematic mapping review. p. 663–685, 2012. Disponível em: ⟨http://dblp.org/db/journals/infsof/infsof54.html\\#Portillo-RodriguezVPB12⟩.

PRLIć, A.; PROCTER, J. B. Ten simple rules for the open development of scientific software. *PLoS Computational Biology, vol. 8, issue 12, p. e1002802*, v. 8, p. 2802, dec 2012.

RIBEIRO, A. C. Análise estática de código-fonte com foco em segurança: Metodologia para avaliação de ferramentas. 2015.

SOCIETY, I. C. *Guide to the Software Engineering Body of Knowledge*. Version 3.0. [S.l.], 2014.

SPIN. *Static Source Code Analysis Tools for C*. 2016. [Online; acessado 23 Abril de 2016]. Disponível em: ⟨http://www.spinroot.com/static⟩.

STOL, K.-J.; FITZGERALD, B. A holistic overview of software engineering research strategies. In: *3rd International Workshop on Conducting Empirical Studies in Industry*. [S.l.: s.n.], 2015. p. 8.

VITEK, J.; KALIBERA, T. Repeatability, reproducibility, and rigor in systems research. In: ACM. *Proceedings of the ninth ACM international conference on Embedded software*. [S.l.], 2011. p. 33–38.

WAKIL, M. M. E. Software metrics - a taxonomy. 1994.

WHEELER, D. A. *Static analysis tools for security*. 2015. [Online; acessado 23 de Abril de 2016]. Disponível em: ⟨http://www.dwheeler.com/essays/static-analysis-tools.html⟩.

WIKIPEDIA. *List of tools for static code analysis*. 2016. [Online; acessado 23 Abril de 2016]. Disponível em: ⟨https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis⟩.