ADFD+: An Automatic Technique for Finding and Presenting Failure domains

Mian Asbat Ahmad and Manuel Oriol

Abstract—**This paper presents Automated Discovery of Failure Domain+ (ADFD+), an upgraded version of ADFD technique with respect to algorithm and graphical presentation of failure domains. The new algorithm used in ADFD+ searches for the failure-domain around the failure in a given radius as against ADFD which limits the search between lower and upper bounds. The graphical output has been further improved in ADFD+ and provides labelled graphs to depict the results in easily understandable user friendly form. ADFD+ was compared with Randoop to find the comparative performance of the two techniques. The results indicate that ADFD+ is a promising technique for finding failure and failure domain efficiently and effectively. ADFD+ outperforms Randoop by taking two orders of magnitude less time to discover the failure domains showing higher efficiency. In addition, ADFD+ surpasses Randoop by identifying all failure domains in 50% or less number of test cases showing higher effectiveness. ADFD+ has the added advantage of presenting the failure domains in graphical form as against Randoop which lacks the ability of graphical presentation.**

Index Terms—**software testing, automated random testing, ADFD.**

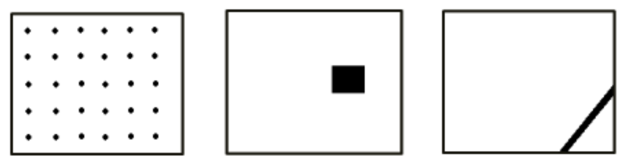
I. Introduction

Software testing is most widely used for verification and validation process. Efforts have been continuously made by researchers to make the testing process more and more effective and efficient. Testing is effective when it finds maximum number of faults in minimum number of test cases and it is efficient when maximum number of test cases are executed in minimum possible time. During up-gradation and development of testing techniques, focus is always on increasing the effectiveness by improving the algorithm and the efficiency by introducing partial or complete automation of the testing process.

A number of empirical evidence confirms that failure revealing test cases tend to cluster in contiguous regions across the input domain [6], [15], [16]. According to Chan et al. [3] the clusters are arranged in the form of point, block and strip failure domains. In the point domain the failure revealing inputs stand-alone and are evenly spread through out the input domain. In block domain the failure revealing inputs are contiguously clustered in one area. In strip domain the failure revealing inputs are clustered in one long elongated area. Figure 1 shows failure domains of the three types for two-dimensional program.

Manuscript received Feb 5, 2014; revised March 20, 2013. The authors are with the Department of Computer Science, University of York, YO10 5DD, UK (e-mail: mian.ahmad@york.ac.uk, manuel.oriol@york.ac.uk).

The paper describes ADFD+, an improved form of ADFD strategy developed previously by Ahmad and Oriol [2]. It is an automated framework which finds the failures and their domains within a specified range and present the results on a graphical chart. To evaluate the effectiveness and efficiency of the newly developed ADFD+ technique, its performance is compared with that of a mature random testing tool Randoop [12]. The results generated by ADFD+ and Randoop about failure domains in the error-seeded programs showed that ADFD+ outperform Randoop with respect to time and number of test cases to find a failure domain. Additionally ADFD+ presents the results graphically showing identified point block and strip domains visually.



(a) Point domain (b) Block domain (c) Strip domain

Fig. 1. Failure domains across input domain [3]

The rest of the paper is organized as follows: Section II describes the ADFD+ technique, its improvement over ADFD, workflow of ADFD+, implementation of ADFD+ and illustrate working of ADFD+ with the help of an example. Section III describes the random testing tool Randoop, Section V explains the experimental setup. Section VI reveals results of the experiments. Section VII discusses the results. Section **??** presents related work, Section X concludes the study and finally future work.

II. Automated Discovery of Failure Domain+

ADFD+ is an improved form of ADFD strategy developed previously by Ahmad and Oriol [2]. The technique automatically finds failures, failure domains and present the results in graphical form. In this technique, the test execution is initiated by random+ and continues till the first failure is found in the SUT. The technique then copies the values leading to the failure and the surrounding values to the dynamic list of interesting values. The resultant list provides relevant test data for the remaining test session and the generated test cases are more targeted towards finding new failures around the existing failures in the given SUT.
The improvements made in ADFD+ in comparison with ADFD strategy are stated as follows.

- ADFD+ generates a single Java file dynamically at run time to plot the failure domains as compared to one Java file per failure in ADFD. This saves sufficient time and makes the execution process quicker.
- ADFD+ uses (x, y) vector series to represent failure domains as opposed to the (x, y) line series in ADFD. The vector series allows more flexibility and clarity to represent failure and failure domains.
- ADFD+ takes a single value as range within which the strategy searches for a failure domain whereas ADFD takes two values as lower and upper bounds representing x and y-axis respectively.
- In ADFD+, the algorithm of dynamically generating Java file at run-time has been made simplified and efficient as compared to ADFD.
- In ADFD+, the failure domains generated in the output graph present a clear view of pass and fail domains with individually labelled points of failures as against a less clear view of pass and fail domains and lack of individually labelled points in ADFD.

A. *Workflow of ADFD+*

ADFD+ is a completely automatic technique requiring the user to specify program and domain range followed by clicking the $DrawFaultDomain$ button to execute testing. As soon as the button is clicked, YETI comes in to play with ADFD+ strategy to search for failures in the program under test. On finding a failure, the ADFD+ strategy creates a Java file which contains calls to the program on the failing and the surrounding values within the specified range. The Java file is executed after compilation and the results obtained are analysed to separate pass and fail values which are accordingly stored in the text files. At the end of test, all the values are plotted on the graph with pass values in blue and fail values in red colour as shown in Figure 3.

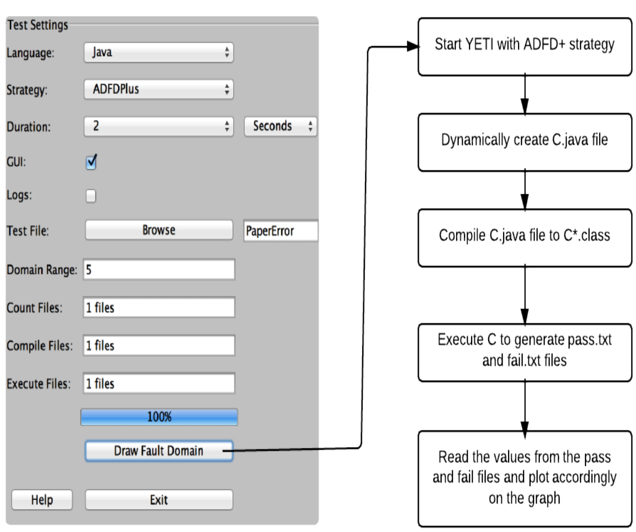


Fig. 2. Workflow of ADFD+

B. *Implementation of ADFD+*

The ADFD+ technique is implemented in YETI which is available in open-source at http://code.google.com/p/yeti-test/. A brief overview of YETI is given with the focus on parts relevant to implementation of ADFD+ strategy.

YETI is a testing tool developed in Java for automatic testing of programs using random strategies. YETI meta-model is language-agnostic which enables it to test programs written in functional, procedural and object-oriented languages. YETI consists of three main parts including core infrastructure for extendibility, strategies section for adjustment of multiple strategies and languages section for supporting multiple languages. Both strategies and languages sections have pluggable architecture to easily incorporate new strategies and languages making YETI a favourable choice to implement ADFD+ strategy. YETI is also capable of generating test cases to reproduce the failures found during the test session. The strategies section in YETI contains all the strategies including random, random+ and DSSR to be selected for testing according to specific needs.

C. *Example to illustrate working of ADFD+*

Suppose we have the following error-seeded class under test. It is evident from the program code that an $ArithmeticException$ (divison by zero) failure is generated when the value of variable x ranges between 5 to 8 and the value of variable y between 2 to 4.

```java
public class Error {
  public static void Error (int x, int y){
    int z;
    if (((x>=5)&&(x<=8))&&((y>=2)&&(y<=4)))
         {
              z = 50/0;
         }
    }
}
```

At the beginning of the test, ADFD+ strategy evaluates the given class with the help of YETI and finds the first failure at x = 6 and y = 3. Once a failure is identified ADFD+ uses the surrounding values around it to find a failure domain. The range of surrounding values is limited to the value set by the user in the $DomainRange$ variable. When the value of $DomainRange$ is set to 5, ADFD+ evaluates a total of 83 values of x and y around the found failure. All evaluated (x, y) values are plotted on a two-dimensional graph with red filled circles indicating fail values and blue filled circles indicating pass values. Figure 3 shows that the failure domain forms a block pattern and the boundaries of the failure are $(5, 2), (5, 3), (5, 4), (6, 2), (6, 4), (7, 2), (7, 4), (8, 2), (8, 3), (8, 4)$.

III. Randoop

Random tester for object oriented programs (Randoop) is a fully automatic tool, capable of testing Java classes and .Net binaries. It takes as input a set of classes, time limit or number of tests and optionally a set of configuration files to

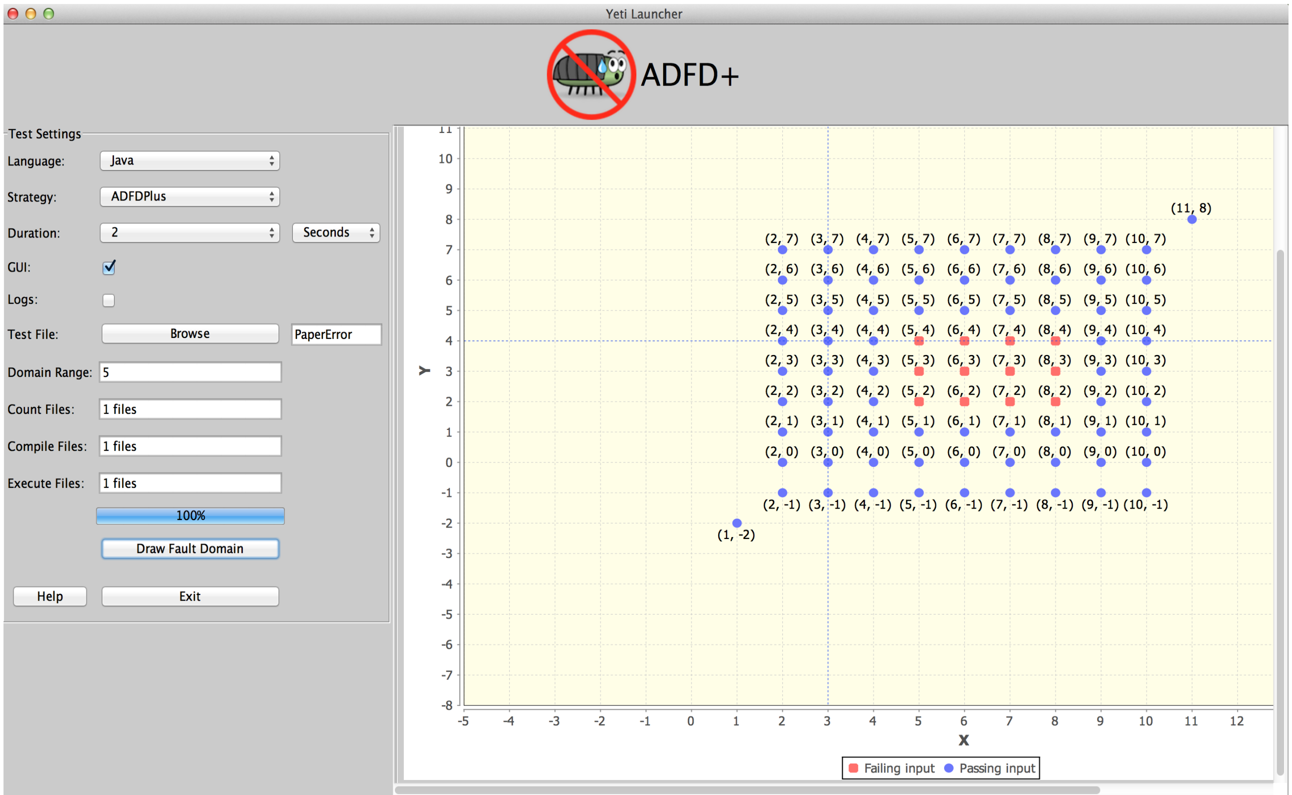


Fig. 3. The output of ADFD+ for the above code.

assist testing. Randoop checks for assertion violations, access violations and un-expected program termination in a given class. Its output is a suite of JUnit for Java and NUnit for .Net program. Each unit test in a test suite is a sequence of method calls (hereafter referred as sequence). Randoop builds the sequence incrementally by randomly selecting public methods from the class under test. Arguments for these methods are selected from the pre-defined pool in case of primitive types and as sequence of null values in case of reference type. Randoop uses feedback mechanism to filter out duplicate test cases.

IV. Research Questions

The following research questions have been addressed in the study for evaluating ADFD+ strategy with respect to efficiency, effectiveness and presentation of failure domains:

1) How efficient is ADFD+ as compared to Randoop?
2) How effective is ADFD+ as compared to Randoop?
3) How failure domains are presented by ADFD+ as compared to Randoop?

V. Evaluation

For evaluating the effectiveness and efficiency, we compared ADFD+ with Randoop, following the common practice of comparison of the new tool with a mature random testing tool [8], [10], [17]. Testing of several error-seeded one and two dimensional numerical programs was carried out as per program code already published in the article [2]. The programs were divided in to set A and B containing one and two-dimensional programs respectively. Each program was injected with at least one failure domain of point, block or strip nature. The failure causing values are given in Table I. Every program was tested independently for 30 times by both ADFD+ and Randoop. Time taken and number of tests executed to find all failures were used as criteria for efficiency and effectiveness respectively. The external parameters were kept constant in each test. Due to the absence of contracts and assertions in the code under test, undeclared exceptions were taken as failures in accordance with the previous studies [2], [9].

A. Experimental setup

All experiments were conducted with a 64-bit Mac OS X Mountain lion version 10.8.5 running on 2.7 GHz Intel Core i7 with 16 GB (1600 MHz DDR3) of RAM. YETI runs on top of the Java^{TM}SE Runtime Environment [version 1.6.0_35]. The ADFD+ Jar file is available at https://code.google.com/p/yeti-test/downloads/list/ and Randoop at https://randoop.googlecode.com/files/randoop.1.3.3.zip.

The following two commands were used to run the ADFD+ and Randoop respectively. Both tools were executed with default settings, however, Randoop was provided with a seed value as well.

```
$ java -jar adfd_yeti.jar -------------(1)
```

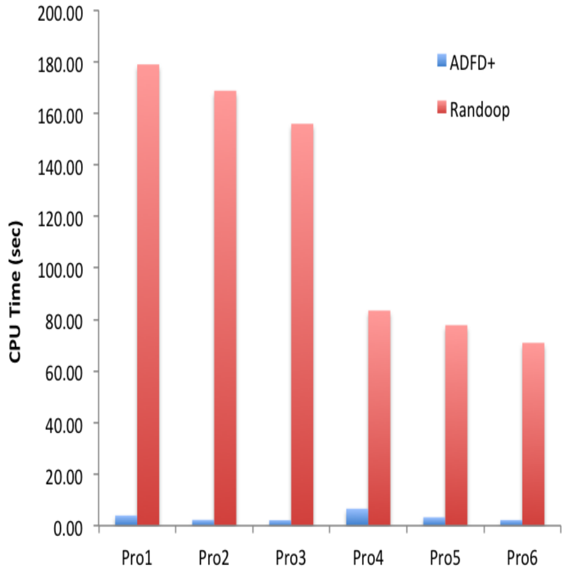


Fig. 4. Time taken to find failure domains

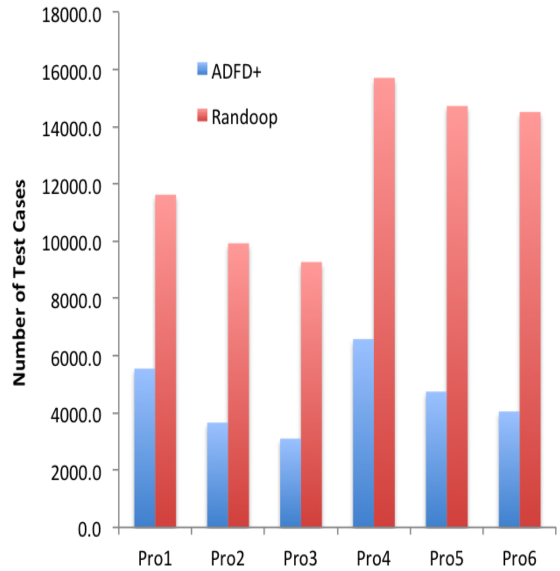


Fig. 5. Test cases taken to find failure domains

```
$ java randoop.main.Main gentests \
--testclass=OneDimPointFailDomain \
--testclass=Values --timelimit=100 ----(2)
```

VI. Experimental results

A. Efficiency

Figure 4 shows the comparative efficiency of ADFD+ and Randoop. The $x - axis$ represents one and two-dimensional programs with point, block and strip failure domains while the $y - axis$ represents average time taken by the tools to detect the failure domains. ADFD+ outperformed Randoop in the time taken to discover all forms of failure domains. The figure shows extra ordinary efficiency in case of ADFD+, amounting to two orders of magnitude or more.

This may be partially attributed to the very fast processing of YETI, integrated with ADFD+. YETI is capable of executing 10^6 test calls per minute on Java code. To ignore the contribution of YETI and assess the performance of ADFD+ by itself, the effectiveness of ADFD+ was compared with Randoop in terms of the number of test cases required to identify the failure domains without giving any consideration to the time consumed for completing the test session. The results are presented in the following section.

B. Effectiveness

Figure 5 shows the comparative effectiveness of ADFD+ and Randoop. The $x - axis$ represents one and two-dimensional programs with point, block and strip failure domains while the $y - axis$ represents average number of test cases used by the tools to detect the failure domains. The figure shows higher effectiveness in case of ADFD+, amounting to 100% or more. The better effectiveness of ADFD+ may be attributed to its working mechanism in comparison with Randoop for identifying failures. ADFD+ changes its algorithm to exhaustive testing in a specified range around the failure as against Randoop which uses the same random algorithm for searching failures.

C. Failure Domains

The comparative results of the two tools with respect to presentation of the identified failure domains reveal better performance of ADFD+ by providing the benefit of presenting the failure domains in graphical form as shown in Figure 6 and 7. The user can also enable or disable the option of showing the failing values on the graph. In comparison Randoop lacks the ability of graphical presentation and the option of showing the failure domains separately, instead it provides the results scattered across the textual files.

VII. Discussion

The results indicated that ADFD+ is a promising technique for finding failure and failure domain effectively and efficiently. It has the added advantage of showing the results in graphical form. The pictorial representation of failure domains facilitates the debuggers to easily identify the underlying failure domain and its boundaries for troubleshooting.

As revealed in the results ADFD+ outperformed Randoop by two orders of magnitude or more in the time taken to discover the failure domains. This was partially attributed to the very fast processing of YETI integrated with ADFD+. To counter the effect of YETI the comparative performance of ADFD+ and Randoop was determined in terms of the number of test cases required to identify the failure domains giving no consideration to the time taken for completing the test session. As shown in the results in Figure 5, ADFD+ outperformed

Randoop by identifying all failure domains in 50% or less number of test cases.

The ADFD+ was found quite effective and efficient in case of block and strip domains but not so in case of point domains where the failures lie away from each other as shown in the following code. This limitation of ADFD+ may be due to the search in vain for new failures in the neighbourhood of failures found requiring the additional test cases resulting in increases overhead.

```
public class Error {
  public static void Error (int x, int y){
    int z;
    if (x == 10000)
         {   z = 50/0;    }

    if (y == -2000)
         {   z = 50/0;    }
   }
}
```

The number of test cases to be undertaken in search of failures around the previous failure found is set in the range value by the user. The time taken by test session is directly proportional to the range value. Higher range value leads to larger graphical output requiring zoom feature which has been incorporated in ADFD+ for use when the need arise.

VIII. Threats to validity

The study faces threats to external and internal validity. The external threats are common to most of the empirical evaluations. It includes, to what degree the programs under test, the generation tools and the nature of seeded errors are representative of the true practice. The present findings will serve as a foundation for future research studies to be undertaken with several types of classes, test generation tools and diversified nature of seeded errors in order to overcome the threats to external validity. The internal threat to validity includes the use of error-seeded classes in our experiments. Internal threat may be avoided by taking real classes and failures in the experiments. Moreover, testing a higher number of classes will also increase the validity of the results.

IX. Related Work

The increase in complexity of programs poses new challenges to researchers for finding more effective and efficient ways of software testing. Adaptive Random Testing [4], Proportional random testing [3], feedback directed random testing [13] are few of the most common upgraded version of random testing aim towards increasing performance. Automated random testing is simple to implement and capable of finding hitherto bugs in complex programs [5], [11]. ADFD+ is an upgraded version of ADFD [2] technique technique to find a failure and using it can effectively and efficiently detect the whole failure domain.

Few of the Identification, classification and visualisation of pass and fail domains have been proposed in the past [14], [1], [7]. This includes Hierarchical Multi Dimension Scaling (HMDS), which describe a semi-automated procedure of classifying and plotting the faults [14]. Xslice [1] is used to differentiates the execution slices of passing and failing part of a test in a visual form. Another tool called Tarantula uses colour coding to track the statements of a program during and after the execution of the test suite [7]. A serious limitation of the above mentioned tools is that they are not fully automated and require human intervention during execution. Moreover these tools need require existing test cases to work on where as ADFD+ strategy generates test cases, discovers failures, identifies pass and fail domains and visualises the results in a graphical form operating in fully automated manner.

X. Conclusion

The newly developed Automated Discovery of Failure Domain+ (ADFD+) is distinct from other random testing techniques because it not only identify failures but also identify failure domains and provides the result output in easily understandable graphical form. The paper highlights the improved features of ADFD+ in comparison with ADFD technique previously developed by our team [2]. The paper then analyses and compares the experimental results of ADFD+ and Randoop for the point, block and strip failure domains. The ADFD+ surpassed Randoop in terms of effectiveness by identifying the failure domains in 50% or less number of test cases and demonstrated extra ordinary improvement to the tune of two orders of magnitude or more in efficiency measured as time taken to discover the failure domains. The better performance of ADFD+ may be attributed mainly to its ability to change algorithm to exhaustive testing in a specified range around the first identified failure as against Randoop which uses the same random algorithm continuously for searching failures.

XI. Future Work

The ADFD+ strategy is capable of testing numerical programs and needs to be extended for testing of non numerical and reference data types to enable it to test all types of data. ADFD+ has the capability of graphical presentation of results for one and two-dimensional numerical programs. It is worthwhile to extend the technique to enable it to present the results of multi-dimensional numerical and non numerical programs in the graphical form.

XII. Acknowledgments

The authors thank the Department of Computer Science, University of York for its financial support with the Departmental Overseas Research Scholarship (DORS) award. We also thanks to Richard Page for his valuable help and generous support.

REFERENCES

[1] H. Agrawal, J. R. Horgan, S. London, and W. E. Wong. Fault localization using execution slices and dataflow tests. In *Software Reliability Engineering, 1995. Proceedings., Sixth International Symposium on*, pages 143–151. IEEE, 1995.

[2] M. A. Ahmad and M. Oriol. Automated discovery of failure domain. *Lecture Notes on Software Engineering*, 03(1):289–294, 2013.

[3] F. Chan, T. Y. Chen, I. Mak, and Y.-T. Yu. Proportional sampling strategy: guidelines for software testing practitioners. *Information and Software Technology*, 38(12):775–782, 1996.

[4] T. Y. Chen. Adaptive random testing. *Eighth International Conference on Qualify Software*, 0:443, 2008.

[5] C. Csallner and Y. Smaragdakis. Jcrasher: An automatic robustness tester for Java. *Software—Practice & Experience*, 34(11):1025–1050, Sept. 2004.

[6] G. B. Finelli. Nasa software failure characterization experiments. *Reliability Engineering & System Safety*, 32(1):155–169, 1991.

[7] J. A. Jones, M. J. Harrold, and J. Stasko. Visualization of test information to assist fault localization. In *Proceedings of the 24th international conference on Software engineering*, pages 467–477. ACM, 2002.

[8] C. Oriat. Jartege: a tool for random generation of unit tests for java classes. In *Quality of Software Architectures and Software Quality*, pages 242–256. Springer, 2005.

[9] M. Oriol. Random testing: Evaluation of a law describing the number of faults found. In *Software Testing, Verification and Validation (ICST), 2012 IEEE Fifth International Conference on*, pages 201 –210, april 2012.

[10] C. Pacheco and M. D. Ernst. *Eclat: Automatic generation and classification of test inputs*. Springer, 2005.

[11] C. Pacheco and M. D. Ernst. Eclat: Automatic generation and classification of test inputs. In *In 19th European Conference Object-Oriented Programming*, pages 504–527, 2005.

[12] C. Pacheco and M. D. Ernst. Randoop: feedback-directed random testing for java. In *Companion to the 22nd ACM SIGPLAN conference on Object-oriented programming systems and applications companion*, pages 815–816. ACM, 2007.

[13] C. Pacheco, S. K. Lahiri, M. D. Ernst, and T. Ball. Feedback-directed random test generation. In *Proceedings of the 29th international conference on Software Engineering*, ICSE '07, pages 75–84, Washington, DC, USA, 2007. IEEE Computer Society.

[14] A. Podgurski, D. Leon, P. Francis, W. Masri, M. Minch, J. Sun, and B. Wang. Automated support for classifying software failure reports. In *Software Engineering, 2003. Proceedings. 25th International Conference on*, pages 465–475. IEEE, 2003.

[15] C. Schneckenburger and J. Mayer. Towards the determination of typical failure patterns. In *Fourth international workshop on Software quality assurance: in conjunction with the 6th ESEC/FSE joint meeting*, pages 90–93. ACM, 2007.

[16] L. J. White and E. I. Cohen. A domain strategy for computer program testing. *Software Engineering, IEEE Transactions on*, (3):247–257, 1980.

[17] T. Xie, D. Marinov, W. Schulte, and D. Notkin. Symstra: A framework for generating object-oriented unit tests using symbolic execution. In *Tools and Algorithms for the Construction and Analysis of Systems*, pages 365–381. Springer, 2005.

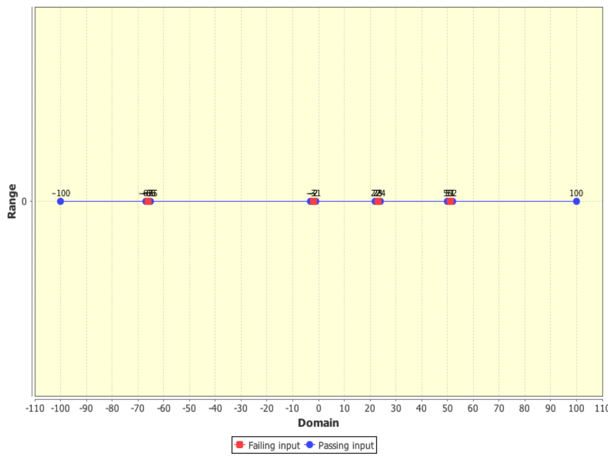
Mian Asbat Ahmad is a PhD scholar at the Department of Computer Science, the University of York, UK. He completed his M(IT) and MS(CS) from Agric. University Peshawar, Pakistan in 2004 and 2009 respectively. His research interests include new automated random software testing strategies.

Manuel Oriol is a lecturer at the Department of Computer Science, the University of York, UK. He completed his PhD from University of Geneva and an MSc from ENSEEIHT in Toulouse, France. His research interests include software testing, software engineering, middleware, dynamic software updates, software architecture and real-time systems.

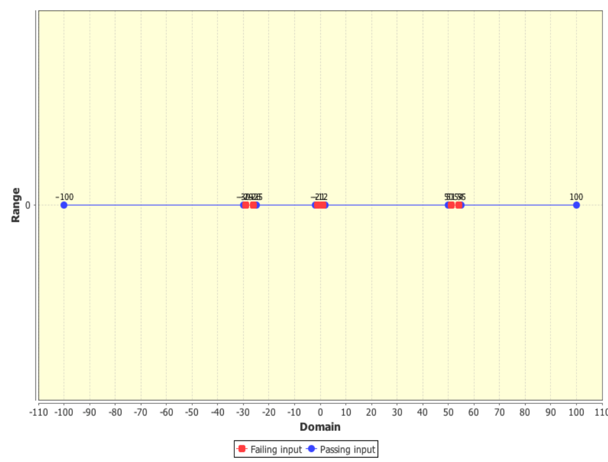
Appendix

TABLE I
TABLE DEPICTING VALUES OF X AND Y ARGUMENTS FORMING POINT, BLOCK AND STRIP FAILURE DOMAIN IN FIGURE 6(A), 6(B), 6(C) AND FIGURE 7(A), 7(B), 7(C) RESPECTIVELY

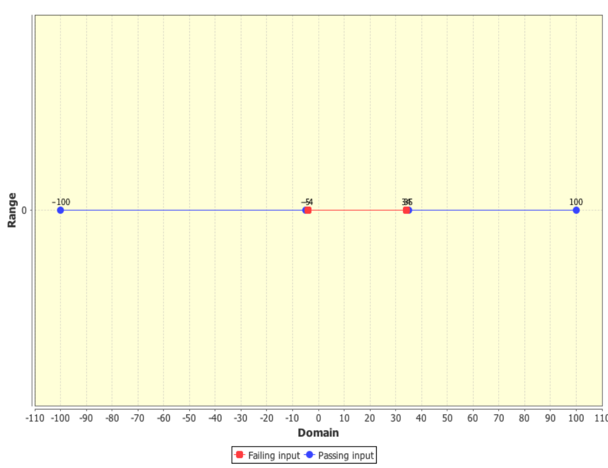
Dim	Point failure	Block failure	Strip failure
One	x = -66	x = -1, 0, 1	x = -4 – 34
	x = -2	x =-26 – -29	
	x= 51	x = 51 – 54	
	x= 23		
Two	x=2, y=10	x = 5, y = 2	x = 7, y = 0
	x=4, y=10	x = 6, y = 2	x = 8, y = 0
	x=7, y=10	x = 7, y = 2	x = 8, y = 1
	x=9, y=10	x = 8, y = 2	x = 9, y = 1
		x = 5, y = 3	x = 9, y = 2
		x = 6, y = 3	x = 10, y = 2
		x = 7, y = 3	x = 10, y = 3
		x = 8, y = 3	x = 11, y = 3
		x = 5, y = 4	x = 11, y = 4
		x = 6, y = 4	x = 12, y = 4
		x = 7, y = 4	x = 12, y = 5
		x = 8, y = 4	x = 13, y = 6
			x = 14, y = 6
			x = 14, y = 7



(a) Point failure domain in one-dimension

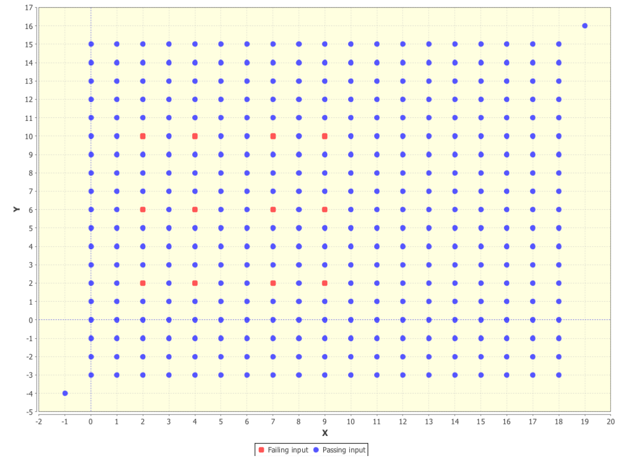


(b) Block failure domain in one-dimension

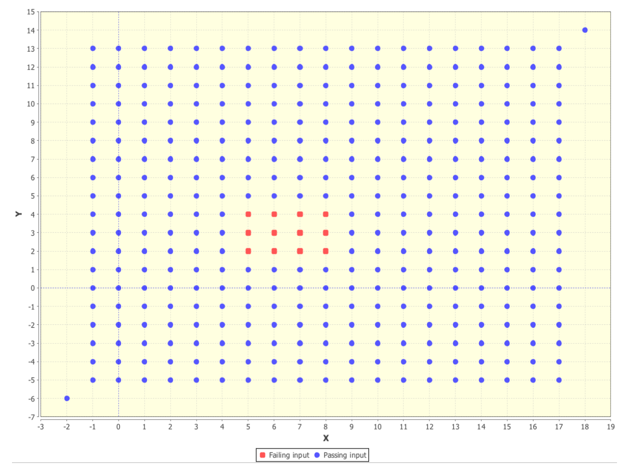


(c) Strip failure domain in one dimension

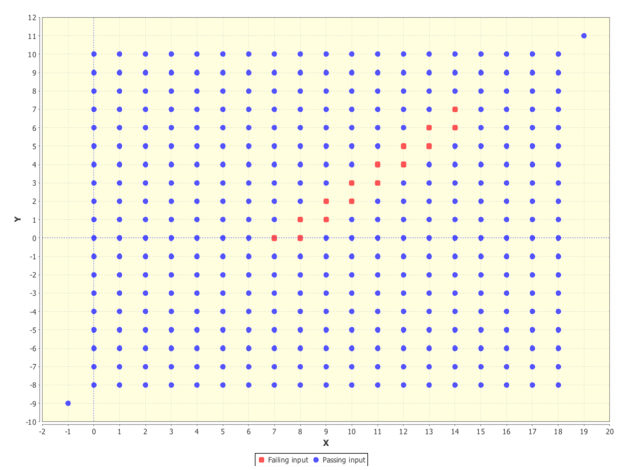
Fig. 6. Pass and fail values of plotted by ADFD+ in three different cases of two-dimension programs



(a) Point failure domain in two-dimension



(b) Block failure domain in two-dimension



(c) Strip failure domain in two-dimension

Fig. 7. Pass and fail values of plotted by ADFD+ in three different cases of two-dimension programs