

Application Domain Specific Highly Reliable IT Solutions

SOFTWARE TESTING, PROTH NUMBERS

RESEARCH RESULTS BY
ATTILA KOVÁCS (0.5 FTE)



NATIONAL RESEARCH, DEVELOPMENT
AND INNOVATION OFFICE
HUNGARY

PROGRAM
FINANCED FROM
THE NRDI FUND

LEVELS OF TKP RESEARCH IN OUR FACULTY LIFE



Innovation



Research



Education

Σ = Thematic Excellence

DIGITAL SERVICES: QUALITY

Aims:

- (1) To promote the industrial applications of new, more efficient software testing methods developed by us
- (2) To develop an educational service



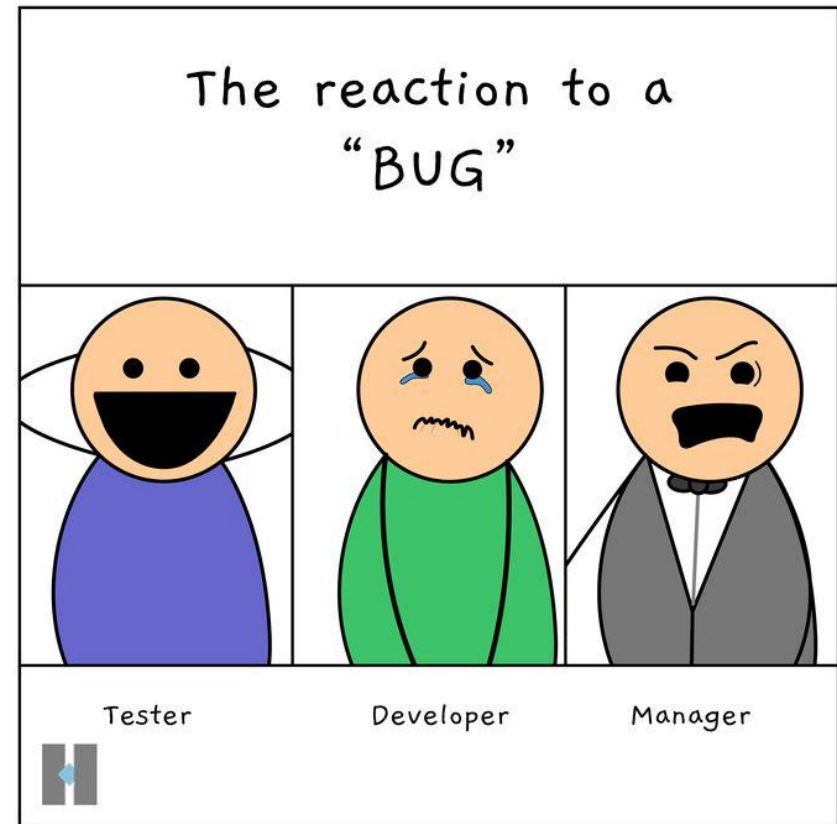
PRELIMINARIES

We have developed a new method called General Predicate Testing (GPT) for testing SW requirements

- We have shown that with our method, predicate errors made during development can be **detected with 100%** regardless of the programming language and constructs
- We have shown that the size of the test set is highly dependent on the appropriate functional and data decomposition

We have also developed a new method for testing the requirements that can be modelled with state machines (Action-State Testing)

- We have shown that the method has a more efficient error detection capability than before (e.g. use case testing, state-transition testing)



RESULTS

- **A service that tells us how effectively a tester can design tests has not been available in the world so far**
- We have prepared an educational material aimed at introducing the methods internationally and promoting their industrial applications
- The new methods were programmed, the adequacy of the tests could be measured with the help of reality-closed mutations, and the tests were automated. This way, the exercises can also tell what tests are missing
- We wrote blogs about the effectiveness of the methods. So far, 9 blog posts have been made

Remark: Negotiations are underway to test the methods at the industrial level (Bosch, GraphiSoft).



GENERAL PREDICATE TESTING UI - SAMPLE

General predicate test description

```
isVIP(bool); price(num,0.01); discount(num,0.01)
true; (100,200]; >20
```

Requirements

```
IF isVIP = true AND price > 100 AND price <= 200 AND
discount > 20
```

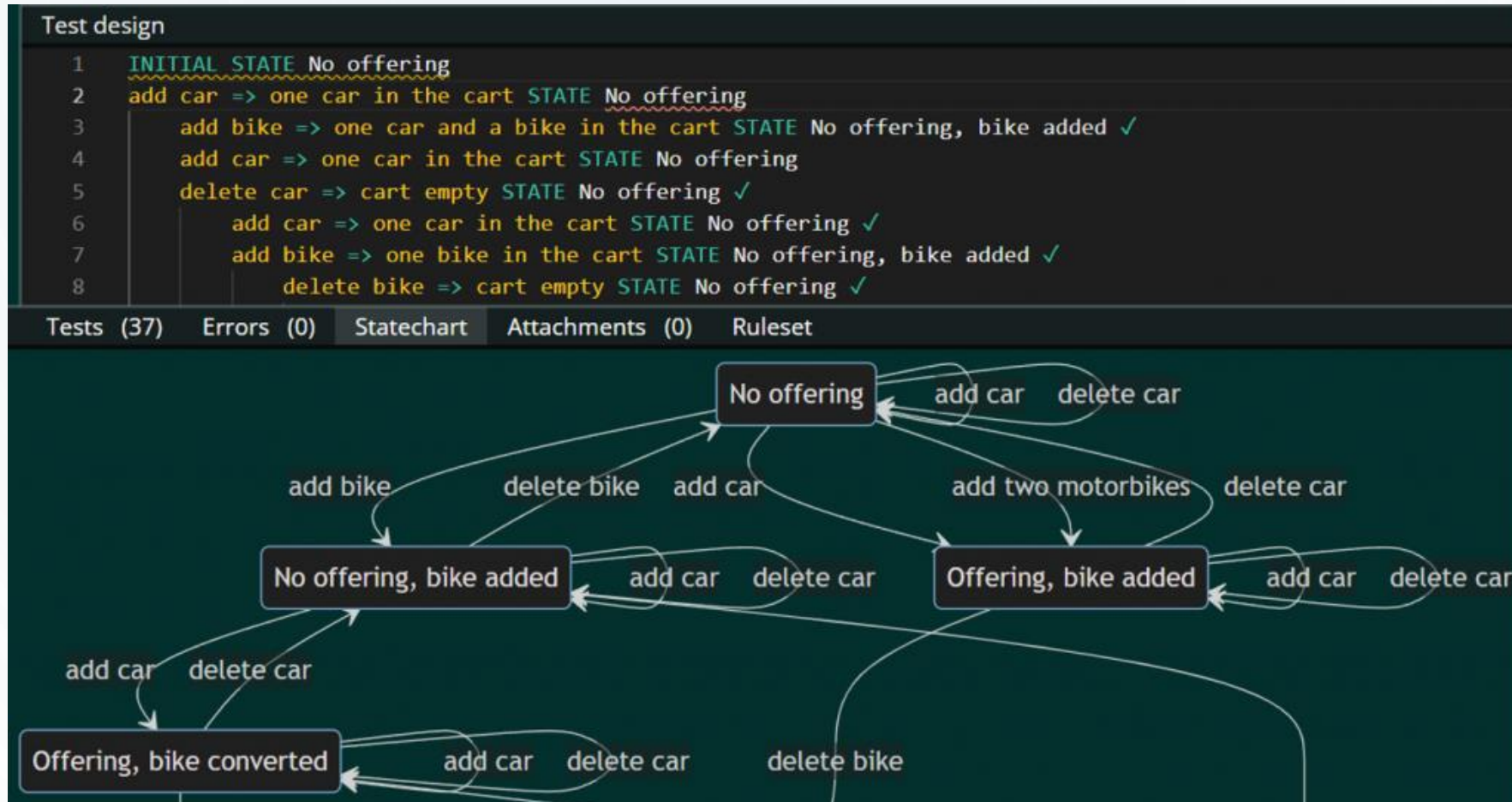
Generate TestsClose user guide

Generated test cases

☐ Show interval values

	isVIP	price	discount
T1	true	100.01	20.02
T2	true	200	20.01
T3	false	100.01	20.01
T4	true	200.02	20.01
T5	true	100	20.01
T6	true	200.01	20.01
T7	true	99.99	20.01
T8	true	100.01	19.99
T9	true	100.01	20

ACTION STATE TESTING UI - SAMPLE



EXISTING EXERCISES

Stateless applications with compound predicates:

Practice	Complexity	Author
Price calculation	2	Forgács & Kovács
Online book store	3	Forgács & Kovács
Paid vacation days	5	Forgács & Kovács
University grade system	6	Forgács & Kovács

Stateful applications:

Practice	Complexity	Author
Car rental	4	Forgács & Kovács
Tour competition	9	Forgács & Kovács
Pizza ordering	7	Forgács & Kovács
Extra holiday	5	Forgács & Kovács



SAMPLE EXERCISE

Read the specification below carefully. Add the test cases one by one. A test case ends with 'Calculate result'. You can continue adding test cases after 'Show my result'. 'Try again' starts a new test design session. You can use the [GPT algorithm](#) to partly automate test design.

University course grade system

R1 A university course grade system evaluates grades based on the following ingredients:

- blackboard exercises (BE) in the range from 0 to 50 points,
- laboratory exercises (LE) in the range from 0 to 50 points,
- written part (WP), also in the range of 0 - 50 points,

R2 The sum of partial grades $SUM = (BE + LE + WP)$ is calculated and the final grade follows the following rules:

R2-1 If any of BE, LE, WP is under 25 points - failed.

R2-2 SUM is less than 76 points – failed.

R2-3 SUM is 76 - 100 points - satisfactory.

R2-4 SUM is 101 - 125 points – good.

R2-5 SUM is greater than 125 points - very good.

The output is the result set, i.e., failed/satisfactory/good/very good.

blackboard exercises: laboratory exercises: written part: course result: - Number of test cases: 0

TECHNICAL DEBT REPRODUCIBILITY

Question: How reproducible the measurement results in the scientific publications?

Objective: The goal was to investigate the scientific publications presented at the premier Technical Debt conferences by understanding how reproducible the reported findings are

Method: We conducted a systematic literature review of **135** unique papers published at the “International Workshop on Managing Technical Debt” and the “International Conference on Managing Technical Debt” scientific conference series on Technical Debt



Results: Only 44 of the investigated papers presented numerical evidence, and only **5** papers listed the tools, the availability of the tools, and the version of the tools used. For the rest of the papers additional information would have been needed for the potential reproducibility.

One of the published papers even referred to a pornographic site as a source of a toolset for empirical research [2]



DIGITAL SERVICES: CYBERSECURITY

Lattice-based cryptography

- **Aims:** Lattice-based cryptography is a promising post-quantum cryptography family, both in terms of foundational properties as well as in its application to both traditional and emerging security problems such as encryption, digital signature, key exchange, and homomorphic encryption.
 - **Result:** A toolset for supporting the research of lattice based number expansions [3]
- 
- 

GNS

Definition

The triple (Λ, M, D) is called a *number system* (GNS) if every element x of Λ has a unique, finite representation of the form $x = \sum_{i=0}^{\lambda} M^i d_i$, where $d_i \in D$ and $\lambda \in \mathbb{N}$

- ▶ A GNS satisfies the *unique representation property*.
- ▶ M is called the *base* and D is the *digit set*
- ▶ λ is the *length of the expansion*

GNS

- ▶ If two elements of Λ are in the same coset of the factor group $\Lambda/M\Lambda$ then they are said to be congruent modulo M

Theorem

If (Λ, M, D) is a number system then

- 1. D must be a full residue system modulo M*
- 2. M must be expansive (Vince, 1993)*
- 3. $\det(I - M) \neq \pm 1$ (unit condition)*

If a system fulfills the first two conditions then it is called a radix system.

GNS

- ▶ The *decision problem* for (Λ, M, D) asks if they form a GNS or not
- ▶ The *classification problem* means finding all cycles (witnesses)
- ▶ The *parametrization problem* means finding families of GNS (like CNS)
- ▶ The *construction problem* aims constructing a digit set D to M for which (Λ, M, D) is GNS. In general, construct a digit set D to M such that (Λ, M, D) satisfies a given signature

FURTHER RESULTS

- We investigated the question of how the structural imprints of number system constructions can be calculated algorithmically (in the most common base) in the ring of real quadratic fields (as a lattice) with canonical digits.
- The complexity of the general case is not known, we suspect it is a “difficult problem” (which is why we are investigating it).
- The results so far show that in our case we can give a significantly more efficient method than the previously known (general) algorithms. We are still working on calculating the exact runtime of the algorithm. So far, there are 18 pages in the LaTeX template for the relevant publication. Readiness: 80%

CYBERSECURITY – PROTH PRIMES

Rank ↕	Number	Discovered ↕	Digits ↕	Form	Ref
1	$2^{82589933} - 1$	2018-12-07	24,862,048	Mersenne	[1]
2	$2^{77232917} - 1$	2017-12-26	23,249,425	Mersenne	[17]
3	$2^{74207281} - 1$	2016-01-07	22,338,618	Mersenne	[18]
4	$2^{57885161} - 1$	2013-01-25	17,425,170	Mersenne	[19]
5	$2^{43112609} - 1$	2008-08-23	12,978,189	Mersenne	[20]
6	$2^{42643801} - 1$	2009-06-04	12,837,064	Mersenne	[21]
7	$2^{37156667} - 1$	2008-09-06	11,185,272	Mersenne	[20]
8	$2^{32582657} - 1$	2006-09-04	9,808,358	Mersenne	[22]
9	$10223 \times 2^{31172165} + 1$	2016-10-31	9,383,761	Proth	[23]
10	$2^{30402457} - 1$	2016-01-07	9,182,931	Mersenne	[24]

PAPER ON PROTH NUMBERS AND PRIMES

ABSTRACT. Computing the reciprocal sum of sparse integer sequences with tight upper and lower bounds is far from trivial. In case of Carmichael numbers or twin primes even the first decimal digit is unknown. For accurate bounds the exact structure of the sequences needs to be unfolded. In this paper we present explicit bounds for the sum of reciprocals of Proth primes with nine decimal digit precision. We show closed formulae for calculating the n^{th} Proth number F_n , the number of Proth numbers up to n , and the sum of the first n Proth numbers. We give an efficiently computable analytic expression with linear order of convergence for the sum of the reciprocals of the Proth numbers involving the Ψ function (the logarithmic derivative of the gamma function). We disprove two conjectures of Zhi-Wei Sun regarding the distribution of Proth primes.

Research at present: all the above results can be generalized to the primes. (Proth means $p = 2$)

DISSEMINATION

Conference participation, conference organization:

- HUSTEF 2021 International Conference Lecture: The New Efficient Test Design Technique, co-author: István Forgács

Academic collaborations:

- Charles University, Prague, Czech Republic

Industrial collaborations:

- Ericsson Magyarország Kft.
- Robert Bosch Kft.
- GraphiSoft Kft.
- Eötvös Loránd University Competence Center

PhD students involved in the research:

- Borsos, Bertalan
- Farkas, Ingrid Izabella
- Hudoba, Péter

Supervised diploma theses:

- Mohammed Jamal: Cutting-Edge technologies of E2E Test Automation applied on scalable Cloud-Based Services and DevOps at IBM
- Ayshan Yariyeva: Dealing with the new concept of use case testing
- Bitar Naief: Combinatorial techniques in software testing
- Ádám Garai: Presentation of cyber security tasks

PUBLICATIONS (APPEARED/TO APPEAR)

- [1] Borsos, Kovács, Tihanyi: Tight upper and lower bounds for the reciprocal sum of Proth primes, *Ramanujan Journal*, to appear, 2022.
- [2] Szabados, Farkas, Kovács: Reproducibility in the Technical Dept domain, *Acta Sapientia*, Vol. 13, No. 2, p. 335-360, 2021, DOI: 10.2478/ausi-2021-00016
- [3] Hudoba, Kovács: Toolset for Supporting the Research of Lattice Based Number Expansions, *Acta Cybernetica*, 25(2), 271-284, 2021, <https://doi.org/10.14232/actacyb.289524>

THANK
YOU



NATIONAL RESEARCH, DEVELOPMENT
AND INNOVATION OFFICE
HUNGARY

PROGRAM
FINANCED FROM
THE NRDI FUND



AVAILABLE AT

attila.kovacs@inf.elte.hu