

Application Domain Specific Highly Reliable IT Solutions

SOFTWARE, QUALITY, RELIABILITY

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

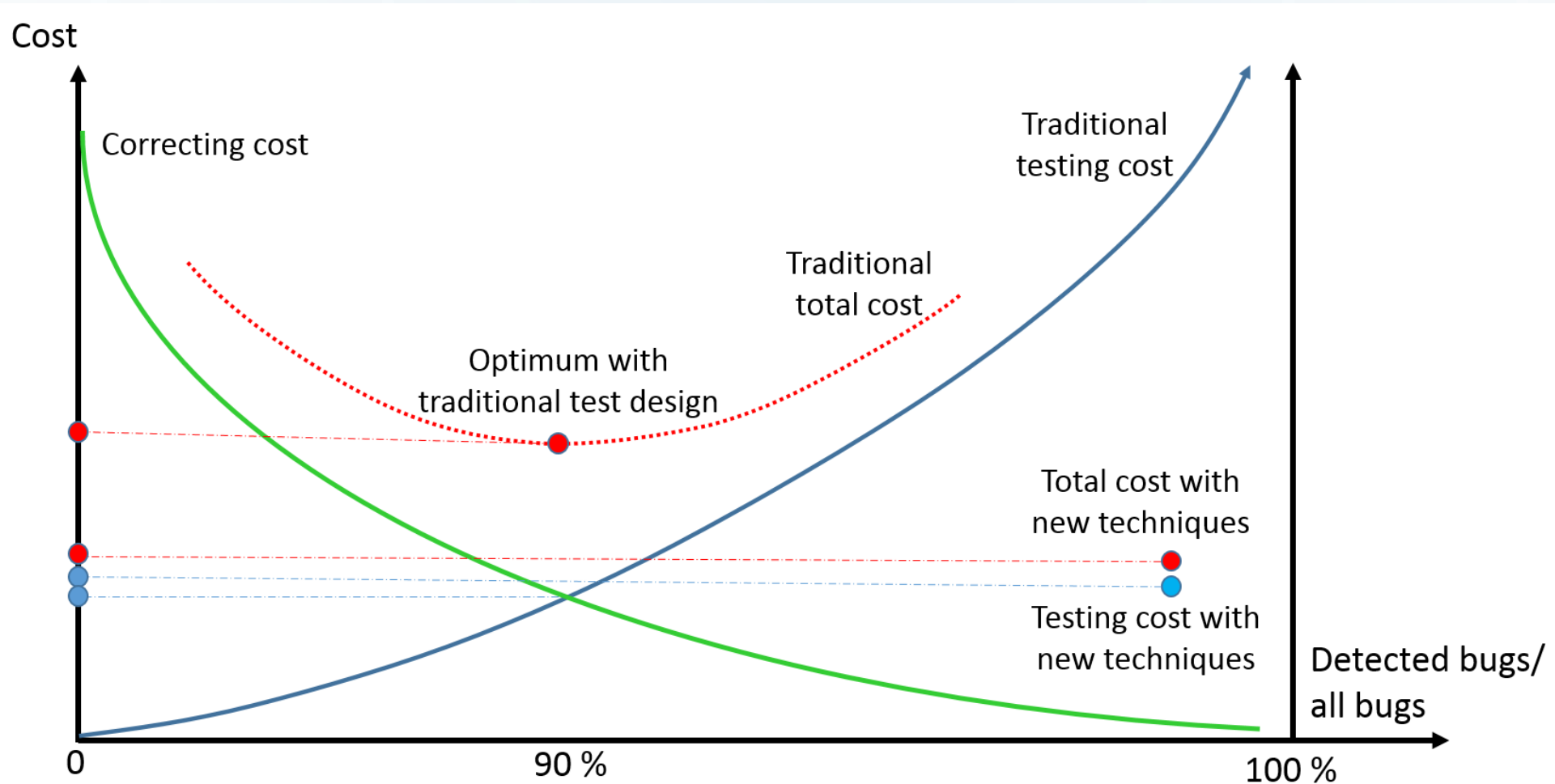


Innovation

Research

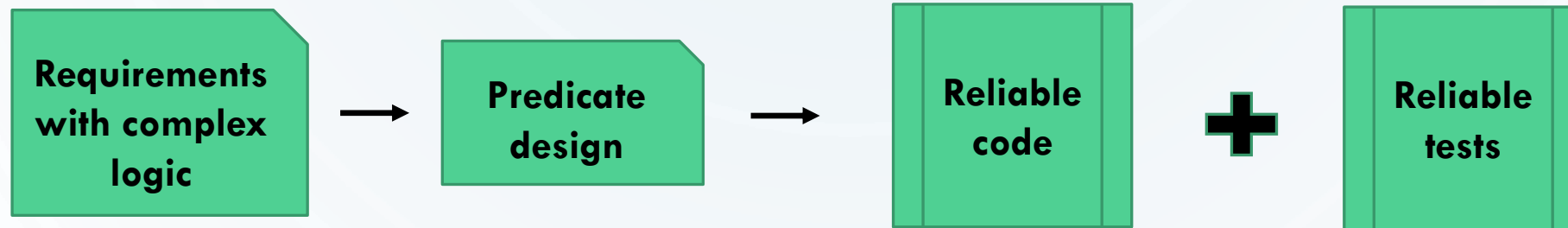
Education

SOFTWARE TESTING COST AND QUALITY



NEW TECHNIQUE NR1: GENERAL PREDICATE TESTING

- CPH and single (data or predicate) faults are assumed
- Before development:

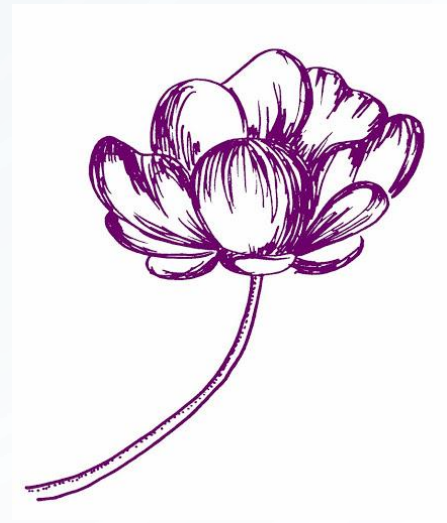


- Tests are „optimal” and linear (in the number of clauses)
- After development:
 - White-box case: suggestions for refactoring (minimizing the predicate set)
 - Black-box case or risky requirements: larger (and reliable) test set

There is a variant against tester's faults

NEW TECHNIQUE NR2: EVENT-STATE MODELING

- Given: requirements of a stateful system
- Traditional testing methods: Use case testing or state-transition testing
- Three main problems: model building, graph traversing, test case number explosion
- Our solution overcomes these issues.
- Our solution supports **codeless test automation**



CYBER SECURITY – LATTICE-BASED ALGORITHMS

- Why?
- 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 tool is developed for further research
- Paper to appear: Toolset for supporting the research of lattice based number expansions (with Péter Hudoba), Acta Cybernetica

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

CYBER SECURITY – 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	$2^{30402457} - 1$	2016-09-05	9,182,931	Mersenne	[24]

PROTH PRIMES


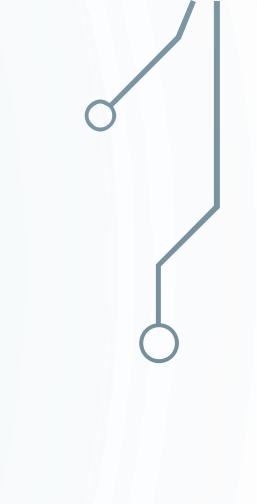
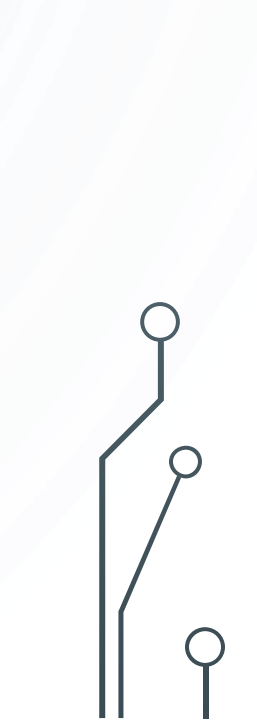
ABSTRACT. Computing the reciprocal sum of sparse integer sequences with tight upper and lower bounds is far from trivial. In case of Carmichael numbers or twin primes even the first decimal digit is unknown. For accurate bounds the exact structure of the sequences needs to be unfolded. In this paper 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 AND EDUCATION

- Albert Csongor Zsolt: Videójátékok felépítése és fejlesztése kis- és nagyvállalati környezetben
- Albírt Mátyás: Állapottartó modellek tesztelése
- Eszter Gábor: Sérülékenység elemző szoftver függőségi kontrollja egy telepítő részeként
- Firas Bou Karroum: Cloud computing quality and data assurance: complying with general data protection regulation (GDPR)
- Fonyódi Balázs: End-to-end Test Automation Framework for a Complex Telecommunication System
- Galgán Diána: Sérülékenység vizsgálati eredmények adatbázisának kialakítása és adatok feldolgozása,
- Korpa Bence: Entrópia deformáció vizsgálata általánosított számrendszerekkel
- Kristyori Dezső: UI tesztautomata optimalizációs lehetőségei
- Marczinus Dávid: Unit tesztek kódlefedettség-vizsgálata a szoftververziókban
- Rózsár Balázs: Tömörítés lehetőségeinek vizsgálata általánosított számrendszerekkel
- Tóth Attila: Tesztelhetőség vizsgálata különböző program implementációkban
- Vecsernyés Márk: Szoftver minőségi paramétereinek meghatározására szolgáló protokoll
- Végh Attila: End-to-end encryption implementation with vulnerability analysis
- Vásáros Máté: Ipari tesztautomata .Net keretrendszerben



SUMMARY

- 2 accepted journal papers
 - 2 submitted journal papers
 - 14 thesis supervision
 - PhD students are involved into the research
- 
- 
- 



THANK
YOU



NATIONAL RESEARCH, DEVELOPMENT
AND INNOVATION OFFICE
HUNGARY

PROGRAM
FINANCED FROM
THE NRDI FUND

AVAILABLE AT

attila.kovacs@inf.elte.hu