

Quantum Random Active Element Machine

Michael Stephen Fiske

Aemea Institute, San Francisco, CA
mf@aemea.org

In [4], a computational procedure (Procedure 2) – combining quantum randomness and the active element machine (AEM) [5] – executes a universal Turing machine with Turing incomputable firing patterns. The procedure emulates any digital computer program so its computational steps are incomprehensible to an external observer. This procedure’s purpose is to hinder malware authors.

An AEM consists of computational primitives called *active elements* that simultaneously transmit and receive pulses to and from other active elements. Each pulse has an amplitude and a width, indicating how long the pulse amplitude lasts as input to the element receiving the pulse. If element E_i simultaneously receives pulses with amplitudes summing to a value greater than E_i ’s threshold and E_i ’s refractory period has expired, then E_i fires. If E_i fires at time t and a non-zero connection exists from E_i to E_k , a pulse reaches element E_k at time $t + \tau_{ik}$, where τ_{ik} is the transmission time. AEM programs are built from **element**, **connection**, **fire**, **program** and **meta** commands. A command explicitly specifies its execution time. Multiple commands can simultaneously execute. During AEM program execution, the **meta** command can self-modify the AEM.

These constructions are physically realizable; the AEM model and a quantum random number generator (QRNG) device [8] act as a single computational entity. The quantum randomness and the **meta** command can non-deterministically modify the AEM’s program. A theory of ideal QRNGs in [1] strives to certify the behavior of actual QRNG devices [2]. Given an ideal QRNG that never stops measuring 0’s and 1’s, the theory in [1] implies that the binary sequence $x_0x_1\dots$ is bi-immune. Set \mathcal{A} corresponds to $x_0x_1\dots$, where $k \in \mathcal{A}$ if and only if $x_k = 1$.

Set $\mathcal{A} \subset \mathbb{N}$ is *immune* if \mathcal{A} is infinite and $\forall \mathcal{B} \subset \mathbb{N}$, [\mathcal{B} is infinite and computably enumerable] $\implies \mathcal{B} \cap \overline{\mathcal{A}} \neq \emptyset$. \mathcal{A} is *bi-immune* if both \mathcal{A} and $\overline{\mathcal{A}}$ are immune. The following lemma helps prove theorem 1: Let $\mathcal{A} \oplus \mathcal{B} = (\mathcal{A} - \mathcal{B}) \cup (\mathcal{B} - \mathcal{A})$. If \mathcal{R} is computably enumerable and \mathcal{A} is bi-immune, then $\mathcal{A} \oplus \mathcal{R}$ is bi-immune.

Theorem 1. *Suppose the measurement, noncontextuality, eigenstate and elements of physical reality assumptions in [1] hold. Thus, in [4], the quantum random sequence used in procedure 2 is bi-immune. Hence, in procedure 2, the active element firing pattern (definition 3, page 79) – emulating the computation of a non-halting universal Turing machine – is a bi-immune sequence.*

Theorem 2. *If \mathcal{A} is a bi-immune set, created by a QRNG, and \mathcal{R} is Turing computable, then a quantum random AEM can compute bi-immune $\mathcal{A} \oplus \mathcal{R}$.*

Our constructions are motivated by the observations that a Gödel numbering is a special type of interpretation and a Turing machine is a discrete, autonomous, dynamical system. In [7], pages 26–29 describe an implicit *interpretation as-*

sumption in computability theory: e.g., a fixed Gödel numbering for the partial recursive functions is a Turing computable coding from sets of instructions to the integers. This assumption puts an unnecessary constraint on computation, illustrated in [4] as an incomputable firing interpretation to an external observer.

Let states $Q = \{q_1, \dots, q_{|Q|}\}$, alphabet $A = \{a_1, \dots, a_{|A|}\}$, halt state h and program $\eta : Q \times A \rightarrow Q \cup \{h\} \times A \times \{-1, +1\}$ be a Turing machine. Define a 1–1 mapping ϕ from η to a finite set of affine functions. Set $B = |A| + |Q| + 1$. Set $\nu(h) = 0$, $\nu(a_i) = i$ and $\nu(q_i) = i + |A|$. ϕ maps right computational step $\eta(q, T_k) = (r, \alpha, +1)$ to affine $f(x, y) = (Bx - B^2\nu(T_k), \frac{1}{B}y + B\nu(r) + \nu(\alpha) - \nu(q))$. State q moves to r ; $\alpha \in A$ replaces T_k on tape square k . ϕ maps left step $\eta(q, T_k) = (r, \alpha, -1)$ to $g(x, y) = (\frac{1}{B}x + B\nu(T_{k-1}) + \nu(\alpha) - \nu(T_k), By + B\nu(r) - B^2\nu(q) - B\nu(T_{k-1}))$. ϕ maps configuration $(q, k, T) \in Q \times \mathbb{Z} \times A^{\mathbb{Z}}$ to $\phi(q, k, T) = (\sum_{j=-1}^{\infty} \nu(T_{k+j+1})B^{-j}, B\nu(q) + \sum_{j=0}^{\infty} \nu(T_{k-j-1})B^{-j})$ in the x - y plane.

Dynamical system $\frac{dx}{dt} = F(x, y), \frac{dy}{dt} = G(x, y)$ is *autonomous* if the independent variable t does not appear in F and G . The map $H(x, y) = (1 + y - \frac{7}{5}x^2, \frac{3}{10}x)$ is discrete and autonomous. Executing a Turing machine corresponds to iterating a discrete, autonomous system in the x - y plane, consisting of a finite number of affine functions, whose domains lie in distinct unit squares. If configuration (q, k, T) halts after n computational steps, then the orbit of $\phi(q, k, T)$ exits one of the unit squares on the n th iteration. If configuration (r, j, S) is immortal, then the orbit of $\phi(r, j, S)$ remains in these unit squares forever.

From these observations, a proof of the *Turing unsolvability of the halting problem* is reexamined. On pages 9–10 of [3], a proof by contradiction is used to define a “total, Turing computable” $g(x) = \begin{cases} 1 & \text{if } \Phi_x(x) \text{ does not halt} \\ \Phi_x(x) + 1 & \text{if } \Phi_x(x) \text{ halts} \end{cases}$ where $\Phi_x(y)$ represents a universal Turing machine. The existence of y with $g = \Phi_y$ and the resulting contradiction $g(y) = \Phi_y(y) + 1 = g(y) + 1$ depend upon the interpretation assumption as $\Phi_x(y)$ acts as an interpreter in the proof. No contradiction is necessarily reached from a Turing incomputable interpretation. Since the `meta` command uses quantum randomness to modify the AEM program, this can create a non-autonomous system. Non-autonomous systems exhibit dynamical behaviors that autonomous systems cannot produce [6].

References

1. Abbott, A.A., Calude, C.S., Conder, J., Svozil, K.: Strong Kochen-Specker theorem and incomputability of quantum randomness. *Phys. Rev. A* 86, 062109, 1–11 (2012)
2. Calude, C.S., Dinneen, M.J., Dumitrescu, M., Svozil, K.: Experimental Evidence of Quantum Randomness Incomputability. *Phys. Rev. A* 82, 022102, 1–8 (2010)
3. Downey, R., Hirschfeldt, D.: *Algorithmic Randomness and Complexity*. Springer (2010)
4. Fiske, M.S.: Turing Incomputable Computation. In: *Turing-100 Proceedings*. Alan Turing Centenary. EasyChair, vol. 10, pp. 66–91 (2012), <http://www.aemea.org/Turing100>
5. Fiske, M.S.: The Active Element Machine. In: Unger, H., Kyamakya, K., Kacprzyk, J. (eds.) *Autonomous Systems: Developments and Trends*. SCI, vol. 391, pp. 69–96. Springer, Heidelberg (2011)

6. Fiske, M.S.: Non-autonomous Dynamical Systems Applicable to Neural Computation. Northwestern University (1996)
7. Rogers Jr., H.: Theory of Recursive Functions and Effective Computability. MIT Press (1987)
8. Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L., Zbinden, H.: Optical quantum random number generator. *Journal of Modern Optics* 47, 595–598 (2000)

**Giancarlo Mauri
Alberto Dennunzio
Luca Manzoni
Antonio E. Porreca (Eds.)**

LNCS 7956

Unconventional Computation and Natural Computation

**12th International Conference, UCNC 2013
Milan, Italy, July 2013
Proceedings**



 **Springer**

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Giancarlo Mauri Alberto Dennunzio
Luca Manzoni Antonio E. Porreca (Eds.)

Unconventional Computation and Natural Computation

12th International Conference, UCNC 2013
Milan, Italy, July 1-5, 2013
Proceedings

Volume Editors

Giancarlo Mauri

Alberto Dennunzio

Luca Manzoni

Antonio E. Porreca

Università degli Studi di Milano-Bicocca

Dipartimento di Informatica, Sistemistica e Comunicazione

Viale Sarca 336/14, 20126 Milan, Italy

E-mail: {mauri, dennunzio, luca.manzoni, porreca}@disco.unimib.it

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-39073-9

e-ISBN 978-3-642-39074-6

DOI 10.1007/978-3-642-39074-6

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013940604

CR Subject Classification (1998): F.1, F.2, I.1-2, C.1.3, C.1, J.2-3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

© Springer-Verlag Berlin Heidelberg 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Author Index

- Adamatzky, Andrew 79
Adorna, Henry N. 259
Ahmed, Saif 244
Alam Anik, Md. Tanvir 244
Alhazov, Artiom 246
Allerdißen, Merle 232
Aman, Bogdan 248
Arroyo, Fernando 255
Asiedu, Isaac Kobina 162
- Bakaoukas, Anastasios G. 250
Beggs, Edwin 6
Bianchi, Maria Paola 19
Boian, Elena 246
Bournez, Olivier 31
Bringsjord, Selmer 102
- Cabarle, Francis George C. 259
Calude, Cristian S. 43
Ciobanu, Gabriel 248
Cojocaru, Svetlana 246
Colesnicov, Alexandru 246
Costa, José Félix 6
Csuhaj-Varjú, Erzsébet 55
- de Lacy Costello, Ben 79
- Ehrenfeucht, Andrzej 3
- Fernau, Henning 67
Fiske, Michael Stephen 252
Formenti, Enrico 1
Foughmand-Araabi, Mohammad-Hadi 90
Freund, Rudolf 67
- Gale, Ella 79
Goliaei, Sama 90
Gómez Canaval, Sandra 255
Govindarajulu, Naveen Sundar 102
Greiner, Rinaldo 232
Grigoriev, Dima 113
- Hegedüs, László 257
Hernandez, Nestine Hope S. 259
- Ivanov, Sergiu 67
- Juayong, Richelle Ann B. 259
- Kari, Lila 125
Kopecki, Steffen 125
Krithivasan, Kamala 186
- Lefèvre, Jonas 31
Licato, John 102
- Makowiec, Danuta 138
Malahov, Ludmila 246
Manzoni, Luca 150
Mereghetti, Carlo 19
Mizuki, Takaaki 162
- Nagy, Benedek 257
- Padilla, Jennifer E. 174
Palano, Beatrice 19
Patitz, Matthew J. 174
Pena, Raul 174
Petic, Mircea 246
Poças, Diogo 6
Porreca, Antonio E. 150
- Ramanujan, Ajeesh 186
Richter, Andreas 232
Rogozhin, Yurii 246
Rozenberg, Grzegorz 3
Russell, Benjamin 198, 209
- Sánchez, José Ramón 255
Schmid, Markus L. 67
Schweller, Robert T. 174
Seeman, Nadrian C. 174
Seki, Shinnosuke 220
Sheline, Robert 174
Shpilrain, Vladimir 113
Simjour, Amirhossein 125
Sone, Hideaki 162
Stepney, Susan 198, 209

Subramanian, K.G. 67
Summers, Scott M. 174

Tadaki, Kohtaro 43
Tucker, John V. 6

Vaszi, György 55
Voigt, Andreas 232

Zhong, Xingsi 174