Early Pioneers in Reversible Computation

Paweł Kerntopf[1], Radomir Stanković[2], Alexis De Vos[3] and Jaakko Astola[4]
[1] Department of Computer Science, Faculty of Physics and Applied Computer Science, University of Łódz, Łódz, Poland
[2]Department of Computer Science, Faculty of Electronics, University of Niš, Niš, Serbia
[3]Imec and Department of Electronics, Universiteit Gent, Gent, Belgium
[4]Tampere International Center for Signal Processing, Tampere University of Technology, Tampere, Finland
email: p.kerntopf@ii.pw.edu.pl, radomir.stankovic@gmail.com, alex@elis.ugent.be, jaakko.astola@tut.fi

***Abstract*—Reversible computation is one of the most intensively developing research areas nowadays. It has originated in 1960s and 1970s from pioneering works of Landauer, Bennett, Toffoli, Fredkin and Feynman on possible energy savings in logic circuits due to their reversibility and on quantum computation. However, the extensive research has been conducted independently during these decades on essentially the same notions but using different terminology. We present a survey of less known or forgotten papers to show that a transfer of ideas between these disciplines is possible.**

Index Terms – reversible computation, information lossless circuits, invertible Boolean functions

I. Introduction

A function is called reversible if it is a bijective mapping. A circuit is called reversible if it implements a reversible function, i.e. there is one-to-one correspondence between its inputs and outputs. Research on reversible logic circuits is motivated mainly by possible applications in many areas of computer science, e.g. quantum computation, low-power digital devices, nanotechnology, DNA computation, signal processing and image processing. Therefore, recently, design of reversible circuits and reversible computers has been intensively studied [1, 2].

Starting from the 1960s, due to the pioneering work of Landauer, Bennett, Fredkin, Toffoli, Feynman and many other physicists, the field of reversible computation has been developing very dynamically and has been widely recognized. However, another two independent directions of research started even earlier but used different terms for the same basic notions. One direction was initiated in 1954 by David A. Huffman (1925-1999) under the name *information lossless functions, circuits and machines* [3-5]. Another direction was using the name *invertible functions/circuits* instead of "reversible functions/circuits". It was initiated in 1962 by Charles S. Lorens (1928-2006) under the influence of two of his colleagues at the Jet Propulsion Laboratory, California Institute of Technology, Pasadena [6]. Both directions have been continued until now but seem to be unknown in the reversible computation community.

The Huffman's motivation was formulated as follows [4]: "*Information-lossless transducer is, roughly, one for which a knowledge of the output sequence of symbols is sufficient for the determination of the corresponding sequence of input symbols. Such transducers find application in the preparation of data for transmission through channels in which secrecy is important or in which the signals are subject to man-made or natural noise.*" His notion of *information losslessness* means exactly the same as *reversibility*. His contribution is cited in many publications on automata theory, error-correcting codes, cryptology, computability theory and number theory.

The Lorens' motivation for doing research in a similar direction is explained in [6]: *The initial interest in invertible Boolean functions originated with numerous discussions with R. M. Stewart [7] about logical nets and with S. W. Golomb on balanced functions.* In this paper Lorens deals with enumeration of equivalence classes of invertible (i.e. reversible) functions. His results on enumeration problems of Boolean functions were extended by M. A. Harrison in many papers and in his PhD dissertation, as well as by other researchers who also generalized them to multiple-valued functions. Recently, Lorens' results on linear and affine equivalences of Boolean functions are cited in "The On-line Encyclopedia of Integer Sequences" and in the context of cryptographically strong Boolean functions.

In this paper, we point out that there is an equivalence between the notion of reversibility and the two more notions used in the literature, namely information losslessness and invertibility. We show a bridge between these previously separated disciplines of research that makes possible a coordinated exploration and transfer of ideas between them. The main goal in this paper is to make these research communities aware of each other.

The paper is organized as follows. Section II is a brief survey on the development of the field of reversible computation. In Section III basic biographical data for D. A. Huffman and C. S. Lorens are provided. Sections IV and Section V summarize their main papers related to reversible computation. Section VI describes continuation of their work up to now. The paper is concluded in Section VII.

II. Development of Reversible Computation

Early pioneers experimented with reversible logic [4], reversible Turing machines [8], and reversible programming [9]. But the real trigger for wider interest came from the fundamental question: What is the minimum amount of energy needed for performing an elementary step of computation? People were convinced that this quantum was of the order of magnitude of kT (where k is equal to Boltzmann's constant and T is the temperature of the computing equipment). For finding the exact lower limit, a struggle with Boltzmann's demon was the usual approach. The scientific community had to wait for Rolf Landauer to find out that the actual amount necessary is zero, provided

one computes in a logically reversible way [9, 10]. The energy dissipation $kTln2$ is needed, not for performing an elementary computing step, but for erasing an elemental amount (say, bit) of information. Not the processing, but the loss of information creates entropy and therefore converts work into heat [12].

The April 1982 issue of the International Journal of Theoretical Physics, completely dedicated to the physics of computing, and subsequent issues of this journal in 1982, featuring contributions by *the founding fathers* Landauer, Bennett, Fredkin, Toffoli and Feynman [13-17], constituted the inevitable arrival of reversible computing in the scientific arena. The subsequent Bennett-Landauer paper [18] in the journal Scientific American (July 1985) reached a large audience and thus inspired many people.

There followed a lot of activity on reversible logic design, aiming at the synthesis of a logic function, making use of exclusively reversible building blocks (NOT gates, Feynman gates, Toffoli gates, Fredkin gates, Peres gates, etc.) [2]. Both heuristic and deterministic algorithms for synthesis of reversible circuits were published. Meanwhile, computer scientists started to build the rules for reversible programming. Only recently, people from reversible circuits and people from reversible languages came together in an attempt to develop a unified approach. Recent books by De Vos (2010) [1], Wille and Drechsler (2010) [19], and Perumalla (2013) [20] go in that direction.

In parallel with these theoretical efforts, research groups worked on proofs-of-concept by buiding actual reversible circuits, both in standard micro- and nanotechnologies (CMOS electronics) [1, 21] and in innovative hardware (MEMS [22, 23] and superconducting SQUIDs [24]). These efforts ultimately lead to the long-awaited experimental confirmation of Landauer's theorem. Independently, in 2011-2012 two scientific teams [25-28] demonstrated in the lab that erasing a bit of information dissipates $kT\,ln2$ of energy, whereas reversible processing of a bit dissipates no energy. With these experimental results, reversible computation has come to maturity.

Additionally we observe cross-fertilisation between the field of (classical) reversible computing and the field of quantum computing. The application of *the square root of NOT* (also called *the V gate*) [29, 30] in the synthesis of reversible circuits is a good example. Another one is the design of various V-shaped ripple-adders/subtractors, multipliers, etc. [31, 32]

Today, reversible computers have become a full-fledged separate research topic in the framework of computer science. Already several hundreds of researchers are working in the field, leading to over 300 publications a year. Besides reversible-computing papers in major computer-science conferences (e.g. DAC, DATE, ASPDAC, ICCAD, ISMVL, MIXDES), a dedicated conference series on Reversible Computation has been established (Ischia 2005, York 2009, Bremen 2010, Gent 2011, Copenhagen 2012, Victoria 2013, Kyoto 2014). Besides many informal international collaborations, also official international research projects have been set up (e.g. the European multilateral Landauer project [33] and the bilateral MicroPower project, a current joint research project of Department of Computer Science at the University of Copenhagen, Denmark, and Electronics and Information Systems Department at Gent University, Belgium [34]).

Further development of the reversible-computing science has now the disposal of powerful tools, such as automatic synthesis and verification. Software tools such as RevKit [35] and SyReC [36] are available. Therefore, industrial applications are possible today. It seems that the day of the first commercial device is near.

III. Careers of D. A. Huffman and C. S. Lorens

In this section we provide essential facts about professional careers of David Alfred Huffman (Aug. 9, 1925 – Oct 7, 1999) and Charles Stanton Lorens (1928 – Jan. 14, 2006) who in 1950s and 1960s published pioneering works in reversible computation.

Huffman was born in Ohio and in 1944 received Bachelor's degree in electrical engineering at Ohio State University at the age of merely 18. Soon he became an officer in the destroyer that was clearing mines in Japanese and Chinese seas after World War II. After two years of service in US Navy Huffman returned to Ohio State University and in 1949 earned Master's degree in electrical engineering. Next he moved to MIT where, still as a PhD student, made the greatest achievement in his life. Namely, as a term paper in the class on information theory taught by professor Robert M. Fano he devised a method of binary coding [37] that was better than the best up-to-date Shannon-Fano coding invented three years earlier. Instead of building the frequency-sorted binary tree top down as Fano and Shannon did he constructed the tree bottom up obtaining the optimal lossless data compression. It was proved that the Huffman code is a minimum-length code in the sense that no other encoding has a shorter average length. Huffman said: "It was my luck to be there at the right time and also not have my professor discourage me by telling me that other good people had struggled with this problem". Due to this achievement Huffman's name is now known to almost all the computer science community. "Huffman code is one of the fundamental ideas that people in computer science and data communications are using all the time," wrote Donald E. Knuth, the famous author of the worldwide known multivolume series of books "The Art of Computer Programming".

In 1953 Huffman collected his PhD degree in electrical engineering at the MIT with the thesis "*The Synthesis of Sequential Switching Circuits*," (advisor: Samuel H. Caldwell) which was published next year in Journal of the Franklin Institute [38]. This pioneering effort had a great impact on the development of switching and automata theory. Already in 1955 Huffman was awarded the Louis E. Levy Medal from the Franklin Institute for his doctoral thesis. Later he got two more distinctions for the same work: in 1973 – W. Wallace McDowell Award from IEEE Computer Society "for his contributions to the solution of sequential circuit problems and coding theory, and for his leadership as a teacher", and in 1981 was Computer Pioneer

Charter Recipient from IEEE Computer Society "for Sequential Circuit Design".

His work on lossless data coding and design of sequential circuits lead him to studying lossless sequential machines. After presenting first concepts in [3, 4] he published a seminal paper [5] which will be briefly described in the next section.

Immediately after defending his PhD thesis Huffman got a teaching position MIT, where he conducted research on various problems in design of sequential circuits (among them highly cited papers [39, 40]). In his publications basic models for synchronous and asynchronous circuits were proposed which are used till now. In 1962 he got a position of a professor at MIT but five years later he moved to newly founded University of California, Santa Cruz where he organized the Department of Computer Science and became its first Chair.

While in UCSC, Huffman continued publishing papers on switching theory [41, 42] and collaborated with the Stanford Research Institute, Menlo Park, CA (now SRI International) [43] and with Aerospace Research Laboratories, USAF [44]. Even after retirement in 1994 remained active in the department, teaching information theory and signal analysis courses. While at Santa Cruz he also switched to new problems, e.g. was one of the pioneers in the new field of computational origami – by studying mathematical properties of "zero curvature" surfaces he developed techniques for folding paper into unusual sculptured shapes [45].

At the end of 1990s he was honored with new awards for life-achievements: in 1998 – A Golden Jubilee Award for Technological Innovation from the IEEE Information Theory Society, for "*the invention of the Huffman minimum-length lossless data-compression code"*, and in 1999 – The IEEE Richard W. Hamming Medal "for design procedures of minimum redundancy (Huffman) codes and asynchronous sequential circuits, and contributions to analysis of visual imagery".

Lorens' career was not so brilliant as Huffman's but their ways crossed at MIT. He graduated from the University of Colorado, then went to MIT for an MS degree (1954) and for a PhD in electrical engineering (1956). The title of his PhD thesis was "Theory and applications of flow-graphs" (in 1964 he published a book on the same topic [46]). The earliest of his research reports were prepared for Bell Telephone Labs., N.Y. (1954) and for General Electric Company, Schenectady, N.Y. (1955). From 1957 till 1960 he was working at the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA. In 1961 he moved to Space-General Corporation and Aerospace Corporation (the latter is probably a new name of the previous corporation) in California in four locations: El Monte, El Segundo, Glendale and Los Angeles.

Among his colleagues in the above listed institutions were well known researchers working in the fields of switching theory and Boolean functions, Irving S. Reed and Solomon W. Golomb, with whom he coauthored papers. Probably due to these close relationships he gained a deep knowledge in these fields. The evidence for this can be seen in his pioneering report of 1962 [47] on enumeration of classes of invertible (i.e. reversible) Boolean functions under various groups over domain and range. Two years later he published its contents in IRE Transactions on Electronic Computers [6]. However, it seems that he has not published more papers on this topic. All other his publications, we were able to retrieve in the web, deal with research on communication systems for spacecrafts, guided missiles and satellites etc. In 1970s Lorens moved to U.S. Defense Communications Agency, Reston, Virginia, where he worked until retirement.

IV. Contribution of D. A. Huffman

Transducers are devices in which the energy of the input and output signals are in different forms. Thus, they convert the energy of one form into the energy of another form. Typically, these are electrical or electronic devices, meaning that various forms of energy are converted into electrical energy, i.e., devices such as for instance microphones and loudspeakers that convert sound waves into electrical signals and vice versa.

In [4], Huffman considered transducers that can be mathematically modelled by combinational and sequential logic circuits. For the practical applications, it was natural to consider information-lossless transducers. In the case of combinational circuits, the information-lossless transducers are defined as circuits *for which a knowledge of the output sequence of symbols is sufficient for the determination of the corresponding input symbols* [4].

This is obviously equivalent to the contemporary definition of reversible logic circuits. Further, in the example used to illustrate the definition of the information-lossless combinational circuit, Huffman emphasized that the circuit has the same number n of inputs and outputs, and the output n-tuples are permutation of these at the inputs.

Regarding sequential circuits, for simplicity, Huffman considered in [4] and [5] binary-input binary-output synchronous circuits, and remarked that generalizations to more general cases are straightforward.

As concisely stated in the review of [5] by A. J. Blikle [48],

Such a circuit is said to be information-lossless if there exist no two (not necessarily different) states s_i and s_f and no two different input sequences x and x' of equal length and output sequence y such that both x and x' lead from s_i to s_f and yield y.

In the original formulation by Huffman, the problem is the following. Given the transition table of the sequential circuit and knowing the sequence of output symbols, but having no direct knowledge of its input symbols or of its internal states, determine the corresponding input sequence. As explicitly stated by the author, all the related concepts were previously precisely defined, discussed, and illustrated by examples in [3].

In [4], Huffman considers two characteristic types of information-lossless sequential circuits, and remarked that

there are many lossless sequential circuits that cannot be classified into considered types. For this reason, it is proposed the general canonical form of such circuits (Figure 1) into which all information-lossless finite automata may be synthesized [4].

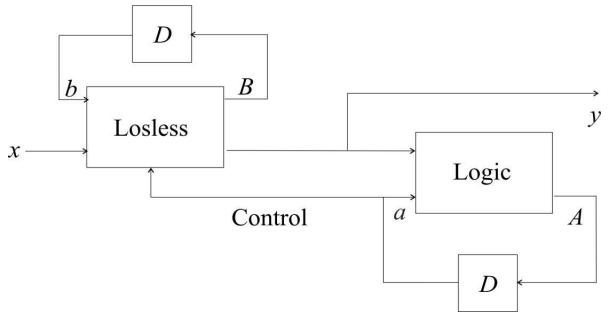

Figure 1. General canonical form into which every information-lossless finite-state circuit may be synthesized.

These block schemata are viewed as canonical forms for information-lossless sequential circuits. These forms as well as forms for inverses of such circuits are further discussed and elaborated in [5].

In his review of [5], Blikle remarked that this paper is more interesting for engineers than mathematicians. This is quite understandable, since the review appeared in the *Journal of Symbolic Logic*, a rather mathematically oriented journal, while the paper was published in the engineering focussed journal (in the Special Supplement to both *IRE Transactions on Circuit Theory and IRE Transactions on Information Theory*).

Importance of the topic discussed by Huffman can be estimated by the way of presenting it as can be seen from the references [3], [4], [5]. The basic concepts were first reported and discussed at a conference, then presented in a technical report for the staff of MIT, and further studied and elaborated in two journal papers, and later also in a chapter of an edited book (see remarks in the reference [5]).

V. Contribution of C. S. Lorens

The notion of reversible logic functions and related concepts can be found under the term *invertible Boolean functions* in the work of C. S. Lorens [6]. In this paper, Lorens discussed functions f: $\{0,1\}^n \rightarrow \{0,1\}^n$, i.e., Boolean functions with the same number of inputs and outputs, without imposing any restriction on the ordering of the n-tuples. Therefore, the outputs can be all possible permutations of the inputs and Lorens studied them from the combinatorial point of view.

The set of all $(2^n)!$ invertible Boolean functions of n variables is classified into equivalence classes, where the equivalence relation is defined as follows.

Denote by G and H the groups of permutations acting on the inputs and outputs of invertible Boolean functions, respectively. For an input n-tuple x, two functions $f_1(x)$ and $f_2(x)$ are equivalent if there is a $g \in G$ and an $h \in H$ such that $f_1(x)=h(f_2(g(x)))$. Thus are defined equivalence classes, in group theory known as double cosets [1].

In [6], Lorens studied the case when G and H are identical groups. In this respect, as pointed in [49], his work can be viewed as a particular case of the work by de Bruijn [50] and Harrison [51], [52], who both considered the case when these permutation groups are different. In the similar context, it can be noted that Lorens did a generalization of the work by Pólya, who considered the restricted case of groups acting solely on the inputs [53].

H. S. Stone commented in [49] that the formula of the number of classes is interesting for small values of n, since the number of equivalence classes asymptotically approaches $(2^n)!/|G|^2$, where $|G|$ is the order of G. The enumeration technique used by Lorens is a special case of the technique by de Bruijn, which is a generalization of the enumeration theory used by Pólya. The work of Lorens motivated further investigations on the topic by Harrison [54].

Another pioneering work in reversible logic can be found in [7] and the motivation was preliminary introduced in [55]. In this correspondence, R.M. Stewart discussed various structures of logic networks, under the term structure meaning the topology of logic networks, i.e., the placement of logic gates and interconnections among them. A special attention was paid to structures corresponding to three dimensional regular lattices, and consisting of elementary components, and simple interconnections, preferably just between the neighboring components. The components located on the periphery of the network are connected to the inputs and outputs of the entire network.

These preliminary discussions were elaborated in [7], where it was pointed out that the composite structures (interconnections of simpler substructures) can be realized by reversible transformations. The term transformation refers to 24 two-input two-output circuits built from NOT and CNOT reversible gates [7]. This work inspired Lorens as he admitted in [6]. However, Lorens used the term *invertible* in contrast to Stewart's term *reversible*.

VI. Continuations of the Work of Huffman and Lorens

Huffman's paper [5] on information lossless machines has been cited in over 100 publications. His basic notions were immediately generalized in many ways by numerous researchers and these efforts had been continued for 40 years approximately [56-75]. Soon after [5] was published as well as more recently they were presented in textbooks on automata theory [76-80]. Paper [5] was also cited in papers on error-correcting codes [81], cryptology [82-83], computability theory [84], Latin squares [85] and number theory [86].

Although the topic of the Lorens' paper [6] was narrower than the problem treated by Huffman in [5] it also found many followers. His results on enumeration of equivalence classes of invertible/reversible functions were extended by M. A. Harrison in many papers and in his PhD dissertation, as well as by other researchers who also generalized them to multiple-valued functions [87-93]. Recently, it appeared that

Lorens' results are cited in a broader context of linear and affine equivalences of Boolean functions by researchers working in the field of cryptographically strong Boolean functions [94-99].

Some of the Lorens' results are cited in all N. J. A. Sloane's collections of integer sequences [100-102]. For example, in "The On-line Encyclopedia of Integer Sequences" founded by N. J. A. Sloane in 1964:

- the entry A000722 gives the number of invertible Boolean functions of *n* variables (it is interesting that the term 'reversible' is not mentioned in the "Encyclopedia"!),
- the entry A000652 gives the number of equivalence classes of invertible Boolean functions of *n* variables under action of permutation and complementation of variables on domain and range.
- the entry A001038 gives the number of invertible Boolean functions of *n* variables with GL(*n*, 2) acting on the domain ad range.

Above mentioned entries cite Lorens' paper and no papers on reversible functions.

In Google Scholar paper [6] has merely 18 citations. However, even now there is a public interest in this publication. Namely, by using the option "Metrics" in the webpage IEEE Xplore one can become assured that Lorens' paper is "still alive": up to now there were 85 downloads of PDF file of Lorens' paper or views of its HTML version in the period starting from Jan. 2011 (27 in 2011, 26 in 2012, 30 in 2013 and 2 in 2014)!

VII. Conclusions

We presented that, at the approximately the same time, Charles S. Lorens and David A. Huffman, as well as Rolf Landauer and his followers invented the same notion independently, motivated by completely different reasons. Unfortunately, it seems that Lorens and Huffman altogether published only a few papers in this direction and then switched to another fields of research. Moreover, they might not know that their results were soon extended and generalized. Nevertheless, all these three research areas has been evolving till today. However, the three communities are separated – they know nothing about each other. It is somewhat strange that in the span of almost 50 years these communities never found a meeting point. Thus the main goal of this paper is to make these research communities aware of each other.

References

[1] A. De Vos, Reversible Computing: Fundamentals, Quantum Computing, and Applications. Weinheim: Wiley-VCH Verlag, 2010.

[2] M. Saeedi and I. L. Markov, "Synthesis and optimization of reversible circuits: a survey," ACM Computing Surveys, vol. 45, no. 2, pp. 21:1-34, 2013.

[3] D. A. Huffman, "Information conservation and sequence transducers," in Proceedings of the Symposium on Information Networks, April 12-14, 1954, J. Fox, Ed., New York: Polytechnic Institute of Brooklyn, 1955, pp. 291-307.

[4] D. A. Huffman, "Notes on information lossless finite-state automata," Nuovo Cimento, Series 10, vol. 13, no. 2 (Supplement), pp. 397-405, 1959.

[5] D. A. Huffman, "Canonical forms for information lossless finite-state logical machines," IRE Trans. on Circuit Theory, vol. 6 (Special Supplement), May 1959, pp. 41-59, and IRE Trans. on Information Theory, vol. 5 (Special Supplement), May 1959, pp. 41-59. [Also published as Technical Report 349, Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA, 21 pages, March 25, 1959 (Reprinted from the Transactions of the 1959 International Symposium on Circuit and Information Theory). A revised version of the Huffman's paper appeared in the book: Sequential Machine: Selected Papers, E. F. Moore, Ed., Reading, Mass.: Addison-Wesley, pp. 132-156, 1964].

[6] C. S. Lorens, "Invertible Boolean functions," IEEE Trans. on Electronic Computers, vol. EC-13, pp. 529-541, Oct. 1964.

[7] R. M. Stewart, "Theory of structurally homogeneous logic nets," in Biological Prototypes and Synthetic Systems, Proc. 2nd Annual Bionics Symposium, E. E. Bernard and M. R. Care, Eds., vol. 1, pp. 370-380, New York: Plenum Press, 1962.

[8] Y. Lecerf, "Machines de Turing réversibles", Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, vol. 257, pp. 2597-2600, 1963.

[9] C. Lutz and H. Derby, "Janus: a time-reversible language," California Institute of Technology, Pasadena, unpublished report, 1982.

[10] R. Landauer, "Irreversibility and heat generation in the computing process, IBM Journal of Research and Development, vol. 3, 1961, pp. 183-191.

[11] R. W. Keyes and R. Landauer, "Minimal energy dissipation in logic," IBM Journal of Research and Development, vol. 14, pp. 152-157, 1970.

[12] C. H. Bennett, "Logical reversibility of computation," IBM Journal of Research and Development, vol. 6, pp. 525-532, 1973.

[13] T. Toffoli, "Physics and computation," International Journal of Theoretical Physics, vol. 21, no. 3-4, pp. 165-175, 1982.

[14] E. Fredkin and T. Toffoli, "Conservative logic," International Journal of Theoretical Physics, vol. 21, no. 3-4, pp. 219-253, 1982.

[15] R. Landauer, "Uncertainty principle and minimal energy dissipation in the computer," International Journal of Theoretical Physics, vol. 21, no. 3-4, pp. 283-297, 1982.

[16] R. Feynman, "Simulating physics with computers," International Journal of Theoretical Physics, vol. 21, no. 6-7, pp. 467-488, 1982.

[17] C. H. Bennett, "The thermodynamics of computation—a review," International Journal of Theoretical Physics, vol. 21, no. 12, pp. 905–940, 1982.

[18] C. H. Bennett and R. Landauer, "The fundamental physical limits of computation," Scientific American, vol. 253, pp. 38-46, 1985.

[19] R. Wille and R. Drechsler, Towards a Design Flow for Reversible Logic. Dordrecht: Springer, 2010.

[20] K. S. Perumalla, Introduction to Reversible Computing. Boca Raton, USA: Chapman&Hall/CRC Press, 2013.

[21] A. De Vos, Reversible Computer Hardware, Electronic Notes in Theoretical Computer Science, vol. 253, no. 6, 2010, pp. 17–22.

[22] S. Houri, A. Valentin, and H. Fanet, "Comparing CMOS-based and NEMS-based adiabatic logic circuits," Reversible Computation, RC 2013, G. Dueck and D. Miller, Eds., LNCS, vol. 7948, pp. 36-45, Heidelberg: Springer, 2013.

[23] J. Wenzler, T. Dunn, T. Toffoli, and P. Mohanty, "Logically reversible nanomechanical logic gate," (submitted) nano.bu.edu/Computing.html

[24] J. Ren and V. K. Semenov, "Progress with physically and logically reversible superconducting digital circuits. IEEE Trans. on Applied Superconductivity, vol. 21, pp. 780—786, 2011.

[25] B. Lambson, D. Carlton, and J. Bokor, "Exploring the thermodynamic limits of computation in integrated systems: magnetic memory, nanomagnetic logic, and the Landauer limit," Physical Review Letters, vol. 107, no. 1, 010604, 4 pp., 2011.

[26] G. L. Snider, E. P. Blair, G. P. Boechler, C. C. Thorpe, N. W. Bosler, M. J. Wohlwend, J. M. Whitney, C. S. Lent, and A. O. Orlov, "Minimum energy for computation, theory vs. experiment," Proc. 11th IEEE Int'l Conf. on Nanotechnology, pp. 478-481, 2011.

[27] A. Berut, A. Arakelyan, A. Petrosyan, S. Ciliberto, R. Dillenschneider, and E. Lutz, "Experimental verification of Landauer's principle linking information and thermodynamics," Nature, vol. 483, pp. 187-189, 2012.

[28] A. O. Orlov, C. S. Lent, C. C. Thorpe, G. P. Boechler, and G. L. Snider, "Experimental test of Landauer's principle at the sub-kT level," Japanese Journal of Applied Physics, vol. 51, pp. 06FE10:1-5, 2012.

[29] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," Physical Review A, vol. 52, no. 5, pp. 3457-3467, 1995.

[30] A. De Vos and S. De Baerdemacker, "The roots of the NOT gate," Proc. 42nd IEEE International Symposium on Multiple-Valued Logic, pp. 167-172, 2012.

[31] S. Cuccaro, T. Draper, S. Kutin, and D. Moulton, "A new quantum ripple-carry addition circuit," Proc. 8th Workshop on Quantum Information Processing, 9 pages, 2005.

[32] S. Burignat and A. De Vos, "A review on performances of reversible ripple-carry adders," International Journal of Electronics and Telecommunications, vol. 58, no. 3, pp. 205-212, 2012.

[33] Landauer: Operating ICT basic switches below the Landauer limit http://www.landauer-project.eu/

[34] H.B. Axelsen, R. Glück, A. De Vos, and M. K. Thomsen, "MicroPower: Towards Low-Power Microprocessors with Reversible Computing," ECRIM NEWS, 2010, http://ecrim-news.ecrim.eu/en79/special-theme/micropower-towards-low-power-microprocessors-with-reversible-computing

[35] M. Soeken, S. Frehse, R. Wille, and R. Drechsler, "RevKit: An open source toolkit for the design of reversible circuits," Reversible Computation, RC 2011, A. De Vos and R. Wille, Eds., LNCS, vol. 7165, pp. 64-76, Heidelberg: Springer, 2012.

[36] R. Wille, S. Offermann, and R. Drechsler, "SyReC: A programming language for synthesis of reversible circuits," System Specification and Design Languages, Lecture Notes in Electrical Engineering, vol. 106, pp. 297-222, New York: Springer, 2012.

[37] D. A. Huffman, "A method for the construction of minimum-redundancy codes", Proc. IRE, vol. 40, no. 9, pp. 1098–1101, 1952.

[38] D. A. Huffman, "The synthesis of sequential switching circuits," Journal of the Franklin Institute, vol. 257, pp. 161-190, March 1954; pp. 275-303, April, 1954.

[39] D. A. Huffman, "The synthesis of linear sequential coding networks," Information Theory, Transactions of the Third London Symposium on Information Theory, 1954, C. Cherry, Ed., pp. 77-95, New York: Academic Press, 1956.

[40] D. A. Huffman, "The design and use of hazard-free switching networks," Journal of the ACM, vol. 4, no. 1, pp. 47-62, 1957.

[41] D. A. Huffman, "Logical design with one NOT-element," Proceedings of the Second Hawaii International Conference of Systems Science, pp. 735-738, 1969.

[42] D. A. Huffman, "Combinational circuits with feedback," in: A. Mukhopadhyay (ed.), Recent Developments in Switching Theory, pp. 27-55, Academic Press, New York and London 1971.

[43] D. A. Huffman, "Testing for faults in cellular logic arrays," SRI Project 8487, Final technical report 1 January 1970 - 6 January 1972, Stanford Research Institute, Menlo Park, CA, 83 pages, January 1972.

[44] D. J. Hall, R. O. Duda, D. A. Huffman, and D. E. Wolf, "Development of new pattern-recognition methods," ARL 73-0153, Aerospace Research Laboratories, Air Force Systems Command, United States Air Force, Wright-Patterson Air Force Base, Ohio. XII, 223 pages, 1973.

[45] D. A. Huffman, "Curvature and creases: A primer on paper," *IEEE Trans. on Computers*, vol. 25, no. 10, pp. 1010-1019, 1976.

[46] C. S. Lorens, "Flowgraphs: For the Modeling and Analysis of Linear Systems," McGraw-Hill Monographs in Modern Engineering Science, New York: McGraw-Hill, 1964.

[47] C. S. Lorens, "*Invertible Boolean Functions*," Space-General Corp., El Monte, CA, Research Memorandum No. 21; January 25, 1962 and July 1, 1962.

[48] A. J. Blikle, "Review of 'Canonical forms for information-lossless finite-state logical machines' by D. A. Huffman," Journal of Symbolic Logic, vol. 32, no. 3, p. 389, 1967.

[49] H. S. Stone, "Review of 'Invertible Boolean functions' by C. S. Lorens, " Journal of Symbolic Logic, vol. 36, no. 2, p. 347-348, 1971.

[50] N. G. de Bruijn, "Generalization of Pólya's fundamental theorem in enumerative combinatorial analysis," Proc. Koninklijke Nederlandse Akademie van Wetenschappen, series A, vol. 62, no. 2, pp. 59-69, 1959, also: Indagationes mathematicae, vol. 21, pp. 59-69, 1959.

[51] M. A. Harrison, ""On the classification of Boolean functions by the general linear and affine group," Journal of the Society for Industrial and Applied Mathematics, vol. 12, pp. 284-299, 1964.

[52] M. A. Harrison, "Combinatorial problems in Boolean algebras and applications to the theory of switching," PhD Thesis, Dept. of Electrical Engineering, University of Michigan, USA, 1963.

[53] G. Pólya, "Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemische Verbindungen", Acta Mathematica, vol. 68, pp. 145-253, 1937.

[54] M. A. Harrison, "The number of classes of invertible Boolean functions", Journal of ACM, vol. 10, pp. 25-28, 1963.

[55] R.M. Stewart, "Notes on the structure of logic nets," Proceedings of I.R.E., vol. 49, no. 8, pp. 1322-1323, 1961.

[56] S. Even, "Generalized automata and their information losslessness," Proc. 3rd Annual Symposium on Switching Circuit Theory and Logical Design, Chicago, Ill., Oct. 7-12, pp. 143-148, 1962.

[57] S. Even, "On information lossless automata," PhD thesis, Harvard University, Cambridge, Mass., January 1963 [Also: Sperry Rand Research Center Report, No. 63-1].

[58] S. Even, "On information lossless automata of finite order," IEEE Transactions on Electronic Computers, vol. EC-14, pp 561-569, 1965.

[59] V. I. Levenshtein, "Inversion of finite automata," Dokl. Akad. Nauk SSSR, vol. 147, no. 6, pp. 1300–1303, 1962.

[60] J. L. Massey and M. K. Sain, "Inverses of Linear Sequential Circuits," IEEE Transactions on Computers, vol. C-17, April 1968, pp. 330-337. (See also "Postscript to Inverses of Linear Sequential Circuits," IEEE Transactions on Computers, vol. C-17, pp. 1177, 1968).

[61] R. R. Olson, "Note on feedforward inverses for linear sequential circuits," Report No. 684, University of Notre Dame, Department of Electrical Engineering, April 1, 1968.

[62] R. R. Olson, "On the invertibility of finite state machines," Report No. EE-703 (PhD dissertation), Department of Electrical Engineering, University of Notre Dame, Notre Dame, Indiana, USA, July 23, 1970.

[63] Y. Kambayashi and S. Yajima, "Finite memory sequential machines and information lossless sequential machines," Report A-6, Data Processing Center, Kyoto University, 1971.

[64] Y. Kambayashi and S. Yajima, "The upper bound of K in K-lossless sequential machines," Information and Control, vol. 19, no. 5, pp. 432-438, 1971.

[65] R. A. Thompson and T. L. Booth, "Encoding of probabilistic context-free languages," Theory of Machines and Computations, Proc. International Symposium on the Theory of Machines and Computations, Haifa, Israel, Aug. 16-19, 1971, Z. Kohavi and A. Paz, Eds., New York and London: Academic Press, pp. 169-178, 1971.

[66] Z. Kohavi and J. Winograd, "Bounds on the length of synchronizing sequences and the order of information losslessness," Theory of Machines and Computations, Proc. International Symposium on the Theory of Machines and Computations, Haifa, Israel, Aug. 16-19, 1971, Z. Kohavi and A. Paz, Eds., pp. 197-206, New York and London: Academic Press, 1971.

[67] D. V. Speranskii, "Essentially information-lossless automata," Avtomatika i Telemekhanika, no. 10, pp. 181–184, 1971.

[68] D. V. Speranskii, "On essentially information-lossless automata of finite order," Avtomatika i Telemekhanika, no. 6, pp. 90–95, 1972.

[69] E. E. Mills, "K-lossless sequential machines of maximum order," Proceedings of the Annual ACM Conference, p. 440, 1973.

[70] Z. Kohavi and J. Winograd, "Establishing bounds concerning finite automata," Journal of Computer and System Sciences, vol. 7, no. 3, pp. 288–299, 1973.

[71] E. A. Primenko and E. F. Skvortsov, "On the conditions of regularity for finite autonomous automata," Discrete Mathematics and Applications, vol. 1, no. 4, pp. 385–390, 1991 [Originally published in Diskretnaya Matematika, vol. 2, no.1, pp. 26-30, 1990].

[72] D. V. Speranskii, "Generalized information lossless automata. I," Kibernetika i Sistemnyi Analiz, no. 3, pp. 63–69, 1994 [English translation: Cybernetics and Systems Analysis, vol. 30, no. 3, pp. 365-370, May-June 1994].

[73] D. V. Speranskii, "Finite order generalized information lossless automata. II," Kibernetika i Sistemnyi Analiz, no. 4, pp. 174–177,

1994 [English translation: Cybernetics and Systems Analysis, vol. 30, no. 4, pp. 619-622, July-August 1994].
[74] D. V. Speranskii, "Generalized linear information-lossless automata," Journal of Computer and Systems Sciences, vol. 37, no. 1, pp. 159-164, 1998 [English translation from Tekhnicheskaya Kibernetika].
[75] D. V. Speranskii and I. D. Speranskii, "On a problem for networks of linear automata without loss of information," Automation and Remote Control, vol. 60, no. 1, pp. 112-117, 1999.
[76] A. Gill, "Introduction to the Theory of Finite State Machines," New York: McGraw-Hill, 1962.
[77] M. A. Harrison, "Introduction to Switching and Automata Theory," New York: McGraw-Hill Book Co., 1965.
[78] T. L. Booth, "Sequential Machines and Automata Theory," New York: John Wiley & Sons, 1967.
[79] F. Hennie, "Finite State Models for Logical Machines," New York: John Wiley & Sons, 1968.
[80] Z. Kohavi, "Switching and Finite Automata Theory," New York: McGraw-Hill Book Co., 1970 [see also: Zvi Kohavi, Niraj K. Jha, "Switching and Finite Automata Theory," 3rd edition, Cambridge, UK: Cambridge University Press, 2010].
[81] P. G. Neumann, "Error-limiting coding using information-lossless sequential machines," IEEE Transactions on Information Theory, vol. IT-10, no. 2, pp. 108–115, 1964.
[82] R. Tao, "Finite Automata and Application to Cryptography," Springer 2009.
[83] P.Wayner, "Disappearing Cryptography: Information Hiding: Steganography and Watermarking," Burlington, MA: Morgan Kaufmann Publishers, 3rd ed., 2009.
[84] D. Doty and P. Moser, "Feasible Depth," Computation and Logic in the Real World, Proceedings of the Third Conference on Computability in Europe, CiE 2007, Siena, Italy, June 18-23, 2007, S. Barry Cooper, Benedikt Löwe, and Andrea Sorbi, Eds., Lecture Notes in Computer Science, pp. 228-237, Springer 2007.
[85] V. A. Nosov, "Constructing Families of Latin Squares over Boolean Domains," Boolean Functions in Cryptology and Information Security, Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security, Zvenigorod, Moscow region, Russia, 8–18 September 2007, NATO Science for Peace and Security Series, Sub-Series D: Information and Communication Security, B. Preneel and O. A. Logachev Eds., vol. 18, pp. 200-207 , IOS Press, 2008
[86] V. Becher and P. A. Heiber, Normal numbers and finite automata, Theoretical Computer Science, vol. 477, pp. 109-116, 2013.
[87] C. S. A. Edwards, "Subgroups of the group G_n," PhD dissertation, University of Illinois at Urbana Champaign, 1973.
[88] I. E. Strazdins, "On the number of types of invertible binary networks," Avtomatika & Vychislitelnaya Tekhnika, no. 1, pp. 30-34, 1974.
[89] E. A. Primenko, "Invertible Boolean functions and fundamental groups of transformations of algebras of Boolean functions," Avtomatika & Vychislitelnaya Tekhnika, no. 3, pp. 17-21, 1976.
[90] E. A. Primenko, "On the number of types of invertible Boolean functions," Avtomatika & Vychislitelnaya Tekhnika, no. 6, pp. 12-14, 1977.
[91] E. A. Primenko, "On the number of types of invertible transformations in multivalued logic," Kibernetika, no. 5, pp. 27-29, 1977.
[92] E. A. Primenko, "On the number of equivalence classes of with respect to certain subgroups of a symmetric group," Kibernetika, no. 6, pp. 19-22, 1979.
[93] E. A. Primenko, "Equivalence classes of invertible Boolean functions," Kibernetika, no. 6, pp. 1-5, 1984.
[94] A. Biryukov, C. De Cannière, A. Braeken, and B. Preneel, "A toolbox for cryptanalysis: linear and affine equivalence algorithms," Advances in Cryptology - EUROCRYPT 2003, E. Binham, Ed., LNCS, vol. 2656, pp. 33-50, Springer, 2003.
[95] L. Breveglieri, A. Cherubini, and M. Macchetti, "On the generalized linear equivalence of functions over finite fields," Advances in Cryptology - ASIACRYPT 2004, P. J. Lee, Ed., LNCS, vol. 3329, pp. 79-89, 2004.
[96] M. Macchetti, M. Caironi, L. Breveglieri, and A. Cherubini, "A complete formulation of generalized affine equivalence," Theoretical Computer Science, ICTCS 2005, M. Coppo, E. Lodi, and G. M. Pinna, Eds., LNCS, vol. 3701, pp. 338-347, Springer, 2005.
[97] G. Leander and A. Poschmann, "On the classification of 4 bit S-boxes," Arithmetic of Finite Fields, LNCS, vol. 4547, pp. 159-176, Springer, 2007.
[98] G. Leander, "Numerical results on Boolean functions with applications in cryptography," Brussels Contact Forum, 2007.
[99] C. De Cannière, "Analysis and design of symmetric encryption algorithms," PhD dissertation, Katholieke Universiteit Leuven, Belgium, 2007.
[100] N. J. A. Sloane, A Handbook of Integer Sequences, New York: Academic Press, 1973.
[101] N. J. A. Sloane and S. Plouffe, The Encyclopedia of Integer Sequences, New York: Academic Press, 1995.
[102] N. J. A. Sloane, "The On-line Encyclopedia of Integer Sequences," http://oeis.org