Towards Wave Digital Memcomputing with Physical Memristor Models

Karlheinz Ochs, Enver Solan, Dennis Michaelis, and Maximilian Herbrechter

Ruhr-University Bochum
Chair of Digital Communication Systems
Bochum, Germany
Email: {karlheinz.ochs, ever.solan, dennis.michaelis,
maximilian.herbrechter}@rub.de

***Abstract*—Self-organizing circuits are subject to current research, especially self-organizing logic gates (SOLGs). The self-organizing aspect enables the latter to be operated 'backwards', meaning that outputs can be used as inputs and vice versa. This makes SOLGs potential candidates to solve mathematically complex problems efficiently. Although SOLGs have been subject to up to date research, the investigated circuits center around purely mathematical models of memristors. In this work, we aim to solve the NP-complete subset sum problem with SOLGs based on a physical model of real memristors. The memristors of choice are RRAM-cells, as they provide a promising performance and a fast convergence due to their rapid switching behavior. For this purpose, we exploit the wave digital emulation technique which differs from many other emulation techniques by preserving passivity. It is shown that a simple subset sum problem is properly solved.**

I. Introduction

In modern times, most of the worldwide communication already occurs through the internet. Cybersecurity therefore is an aspect that will become more and more important in the future, since electronic eavesdropping of sensitive information is a massive threat for personal data and industrial spying alike. Modern cryptographic techniques mostly rely on so called one way functions, which are easy to compute in one direction yet finding their inverse functions is very challenging. One well-known example is the NP-hard problem of prime factorization which is widely used in today's cryptographic approaches.

However, the upcoming of quantum computing challenges current standards in cryptographic. The theoretical framework suggests that the prime factorization can be solved efficiently and therefore demand for new quantum proof cryptographic systems. One function often mentioned in this context is the subset sum problem, because it is mathematically more complex than the prime factorization and there currently is neither a standard nor quantum algorithm to solve this problem efficiently in its entirety [1], [2]. Hence, it is a candidate for post-quantum cryptosystems.

Another system challenging cryptographic techniques are memcomputers which are known to solve prime factorizations [3] and even the subset sum problem in polynomial time [4]. The approach involves finding a theoretical model of an analog circuit that represents the problem at hand. In that regards, so called self-organizing logic gates (SOLGs) have been constructed which can be operated 'backwards', meaning that input nodes can be used as output nodes and vice versa [5]. The central element in these approaches is a resistor with memory called a memristor [6].

While current investigations are promising, it is yet to be seen whether SOLGs can operate with real memristive devices. In general, resistive random access memory (RRAM) cells are promising real memristors that firstly have been applied in memory applications [7], [8]. Their fast switching behavior and the fact that they are well studied also makes them a candidate for applications in self-organizing circuits as well [9], [10]. Although the design and development process of RRAM-cells is costly, they are well suited for manufacturing. The current approach is to deploy emulators based on a mathematical model of a physical RRAM-cell as an intermediate step towards a hardware realization. The here utilized emulation technique is based on the wave digital concept since it is know to preserve passivity [11]. It has successfully been used for memristors in general [12], [13] and RRAM-cells in particular [14].

The paper is structured as follows. In Sec. II details on the deployed RRAM-cell is presented. The self-organizing logic gates (SOLGS) are briefly discussed in Sec. III before the wave digital model of a self-organizing logic and (SO-AND) gait with physical RRAM-cell models is established in Sec. IV. We then apply our model to solve the NP-complete subset sum problem in Sec. V. A final conclusion summarizes the main results and an outlook on future work is given.

II. RRAM-Cell

The memristor model we utilize in this work is based on the hafnium dioxide RRAM-cell investigated in [14]. Its underlying differential equation of the memory state z is

$$\begin{aligned}\dot{z} &= g(u)[\sigma(u)\sigma(z) + \sigma(-u)\sigma(1-z)],\\ g(u) &= S_{\mathrm{p}}\Sigma(u-U_{\mathrm{tp}}) + S_{\mathrm{n}}\Sigma(u-U_{\mathrm{tn}}),\end{aligned} \tag{1}$$

where $\sigma(\xi)$ is the Heaviside function, $\Sigma(\xi) = \int_0^{\xi} \sigma(\eta)\mathrm{d}\eta$, $z = 0$ and $z = 1$ describe the RRAM-cell in the low resistance state R_0 and high resistance state R_1, respectively, S_p and S_n describe the steepness of transitioning between the resistance states, and U_tn and U_tp are the negative and positive thresholds for the transitional behavior, respectively.
The voltage current relationship of the deployed RRAM-cell is described by

$$\begin{aligned} i(t) &= W(z,u)u(t) = M^{-1}(z,u)u(t), \\ M(z,u) &= R_0 + z(R_1(u) - R_0). \end{aligned} \tag{2}$$

RRAM-cells are a particular interesting candidate in self-organizing memristive circuits aiming to solve mathematically complex problems, e.g. SOLGs, due to their fast switching behavior. That is because a quick consensus is expected which would results in a low convergence time.

III. Self-Organizing Logic Gates

Due to lack of space, we cover the section on SOLG only briefly and refer the interested reader to [5]. Firstly, we set the convention that a logical 'true' is encoded by a voltage of 1V and a logical 'false' with a voltage of -1V. Fig. 1 shows the circuit of a self-organizing AND (SO-AND) gate. The SO-AND gate consists of three so called dynamic correction modules (DCMs) $\mathcal{S}_\mu$ that are interconnected through memristors M_4, M_5. Each DCM consists of two voltage-controlled voltage generators (VCVGs), a voltage-controlled differential current generator (VCDCG) and a memristor.

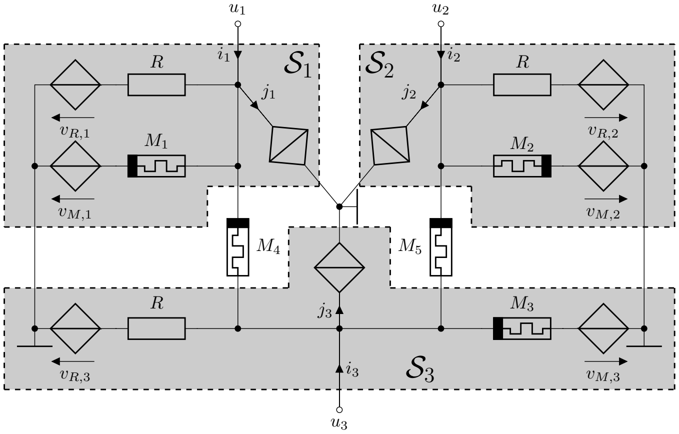

Fig. 1: Circuit based realization of a SO-AND gate with DCMs $\mathcal{S}_\mu$ consisting of resistive VCVGs $v_{R,\mu}$, memristive VCVGs $v_{M,\mu}$ and VCDCGs j_μ. They are connected through memristors M_4, M_5, respectively.

The VCVGs $v_{\lambda,\mu}$, where $\lambda = \{M, R\}, \mu = \{1, 2, 3\}$, inject a current in combination with a resistor or memristor into a gate to make configurations stable or unstable, depending on the desired functionality. In other words, they determine the equilibriums states of the circuit. The computation of generated voltage is a linear combination of input voltages u_μ at the terminals μ.

In case of an analog circuit, it might be that $u_\mu \neq \pm 1V$. If so, we currently obtain undesired stable states of the SO-AND gate, as there is a continuum of equilibrium states of the overall circuit. VCDCGs inject the currents j_μ into terminals μ, depending on the algebraic sign of the voltage present at the specific terminal. This forces the SOLG to reconfigure itself and eventually reach a stable configuration with a voltage level distinctly encoding a logic level.

As stated above, the logic states are encoded into the voltage. Consequently, a logical negation is simply realized by swapping the terminals. A SO-AND gate and negation element are the only essential tools to create a SO-OR and a SO-XOR gate, which is because $A \vee B = \neg[\neg A \wedge \neg B]$ and $A \oplus B = [A \vee B] \wedge \neg[A \wedge B]$. For the desired application of this work, these are all the necessary building blocks. It is furthermore assumed throughout this work that all logic gates are SOLGs.

IV. Wave Digital Representation

To create an emulator based on the wave digital algorithm we first transform voltage u and current i to the voltage waves a and b through

$$a = u + Ri, \qquad b = u - Ri, \tag{3}$$

with the port resistance $R > 0$. By observing the structure of the DCMs in Fig. 1, it can be seen that they consists of the parallel interconnection of a resistive VCVG, a memristive VCVG and a VCDCG. First, the wave digital representations of these two ports will be derived before we connect them through a parallel adaptor which accounts for their interconnection.
Firstly, the memristive voltage source of Fig. 3 can be written in wave quantities through (3)

$$u = v - Mj \quad \Leftrightarrow \quad a = \rho_M b + [1 - \rho_M]v, \tag{4}$$

with $\rho_M = \frac{M - R_M}{M + R_M}$, and $M = M(z, u_M)$ being the RRAM-cell discussed in Sec. II. Note that the role of a and b reverse in case of a source. The resistive voltage source is a special case of (4) in which $M(z, u_M) = R_M = R$. Therefore,

$$u = v - Rj \quad \Leftrightarrow \quad a = v. \tag{5}$$

Note that a VCDCG j_μ and a resistive VCVG $v_{R,\mu}$ can be combined into one resistive VCVG with $v = v_{R,\mu} + Rj_\mu$. With these wave digital representations we can model the DCMs $\mathcal{S}_\mu$ in the wave digital domain as pictured in Fig. 4 (left), where the middle element is a 4-port reflection free parallel adaptor, described by

$$\boldsymbol{b} = \boldsymbol{S}\boldsymbol{a} \quad \text{with} \quad \boldsymbol{S} = \boldsymbol{e}\boldsymbol{\gamma}^T - \mathbf{1} \quad \text{and} \quad \boldsymbol{\gamma}^T = \frac{2\boldsymbol{e}^T\boldsymbol{G}}{\boldsymbol{e}^T\boldsymbol{G}\boldsymbol{e}},$$

where $\boldsymbol{S}$ is the scattering matrix, $\boldsymbol{e} = [1, \ldots, 1]^T$, $\mathbf{1}$ is the identity matrix, $\boldsymbol{G} = \mathrm{diag}(G_\mu, G_{\mathcal{S},\mu}, G_M, \tilde{G}_{\mathcal{S},\mu})$, $\tilde{G}_{\mathcal{S},\mu} = G_\mu + G_{\mathcal{S},\mu} + G_M$ and $G_\nu = R_\nu^{-1}$. For more details we refer to [11].
As for the memristive interconnection of DCMs through

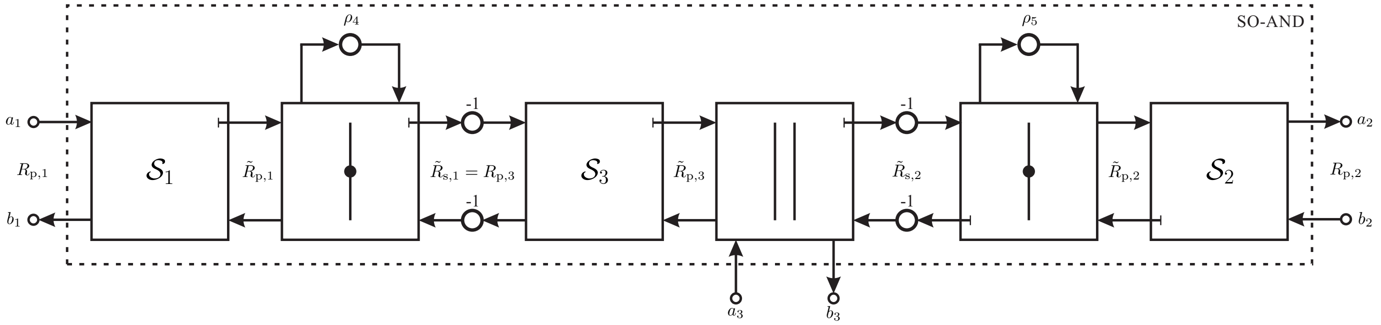
SO-AND
a_1
$R_{\mathrm{p},1}$
b_1
$\mathcal{S}_1$
ρ_4
$\tilde{R}_{\mathrm{p},1}$
-1
$\tilde{R}_{\mathrm{s},1} = R_{\mathrm{p},3}$
-1
$\mathcal{S}_3$
$\tilde{R}_{\mathrm{p},3}$
-1
$\tilde{R}_{\mathrm{s},2}$
-1
ρ_5
$\tilde{R}_{\mathrm{p},2}$
$\mathcal{S}_2$
$R_{\mathrm{p},2}$
a_2
b_2
a_3
b_3

Fig. 2: Wave digital model of the SO-AND gate in Fig. 1.

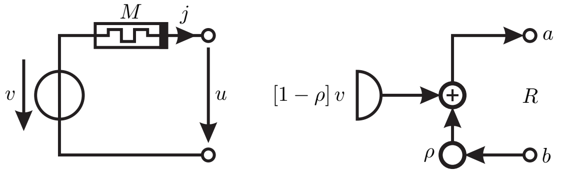

Fig. 3: Memristive voltage source (left) and its wave digital representation (right).

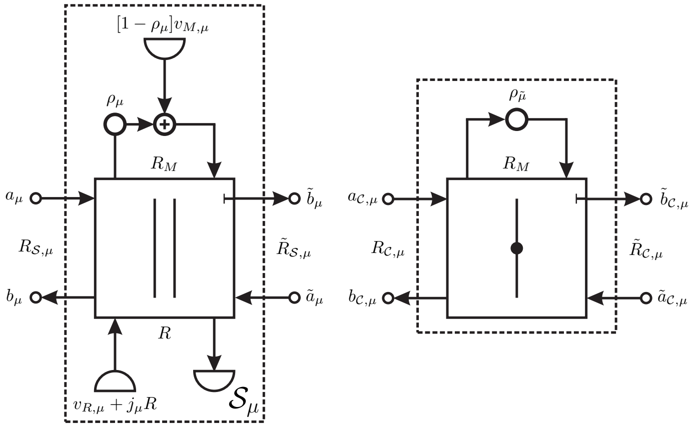

Fig. 4: Dynamic correction modules $\mathcal{S}_\mu$ (left) deployed for every input/output port μ and its wave digital representation (right).

memristors M_4, M_5, a memristor is also special case of (4) with $v = 0$, leading to

$$u = -Mj \quad \Leftrightarrow \quad b = \rho_M a. \tag{6}$$

The wave digital representation of the memristive interconnection of the DCMs $\mathcal{S}_\mu$ is shown in Fig. 4 (right), where the middle element is a 3-port reflection-free series adaptor with

$$\boldsymbol{b} = \boldsymbol{S}\boldsymbol{a} \quad \text{with} \quad \boldsymbol{S} = \boldsymbol{1} - \boldsymbol{\gamma}\boldsymbol{e}^T \quad \text{and} \quad \gamma = \frac{2\boldsymbol{R}\boldsymbol{e}}{\boldsymbol{e}^T\boldsymbol{R}\boldsymbol{e}},$$

where $\boldsymbol{R} = \mathrm{diag}(\tilde{R}_{c,\mu}, R_M, \tilde{R}_{c,\mu}), \tilde{R}_{c,\mu} = \tilde{R}_{c,\mu} + R_M$.

Complete wave digital model of the SO-AND gate can be obtained through a proper port-wise interconnection of the models in Fig. 4. Consequently, the complete wave digital model of the circuit in Fig. 1 is depicted in Fig. 2. We like to highlight to the implicit relationships that can be observed at the three memristors of the DCMs and the two connection memristors which can be dealt with iterator elements [15].

V. The Subset Sum Problem

The general subset-sum problem is known to be

$$\max_{c_\mu \in \{0,1\}} \quad \sum_{\mu=1}^{n} c_\mu w_\mu \leq s,$$

with w_μ are integer number and s is the upper bound to the sum. We are specifically interested in the application in cryptography [1] and therefore trying to solve the problem with equality

$$s = \sum_{\mu=1}^{n} c_\mu w_\mu, \tag{7}$$

assuming that it is uniquely solvable. In order to obtain a circuit which is able to solve (7), we require self-organizing half-adders (SO-HA), self-organizing full-adders (SO-FA) to model the summations, and self-organizing toggle units (SO-TU) to represent binary variables c_μ deciding whether w_μ is part of the solution. It is known that HAs can be realized by properly interconnecting one XOR-gate and one AND-gate, while a FA can be build from two AND-gates, two XOR-gates and one OR-gate. Fig. 5 shows the setup to solve (7) for $n = 3$, with w_μ being 3-bit numbers and s is a 5-bit number. Their representation in the binary system is noted by

$$w_\mu = \sum_{\nu=0}^{2} w_{\mu\nu} 2^\nu, \quad s = \sum_{\nu=0}^{4} s_\nu 2^\nu. \tag{8}$$

One of the SO-TUs is diplayed in the top box, where the results of the SO-AND gates are $w_\mu\nu$ if c_μ is a logical 1 and the results are logical 0 otherwise.

The normal, trivial operating mode of the circuit would be to have c_μ as inputs and s_ν as outputs. The goal of the self-organizing structure in this application is to reverse these roles, such that s_ν is the input and c_μ the desired output. The emulation results for $w_1 = 2, w_2 = 1, w_3 = 5$ and $s = 7$ are shown in Fig. 6. It can be seen that after $t \approx 50\mathrm{ms}$ the wave digital emulation converges to $c_1 = c_3 = 1\mathrm{V}$ (logical 'true') and $c_3 = -1\mathrm{V}$ (logical 'false'). This result is indeed correct as $1 \cdot w_1 + 0 \cdot w_2 + 1 \cdot w_3 = s$, confirming that physical RRAM-cells

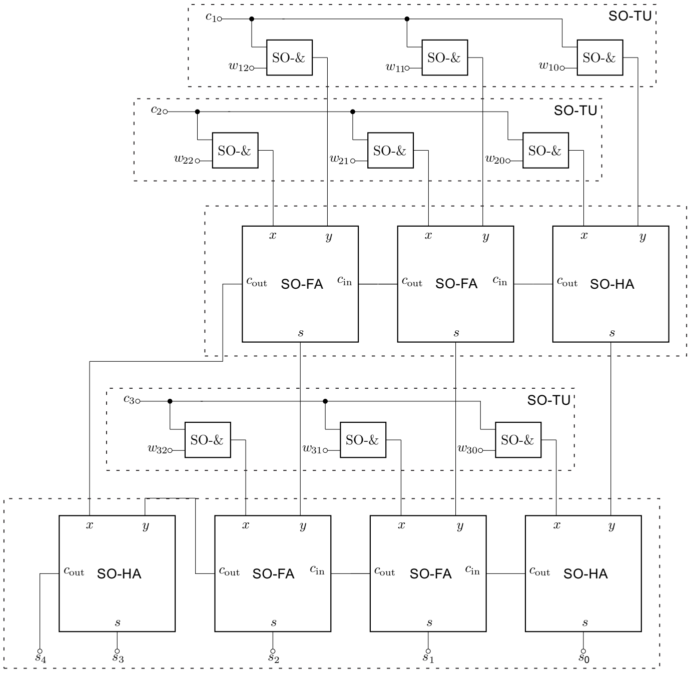

Fig. 5: Graphical representation of a SO 3-bit subset-sum problem solver consisting of SO toggle units (top box) and SO half- and full-adders (bottom box), used to solve (7) for three 3-bit numbers $w_1, \ldots, w_3$ and a 5-bit number s.

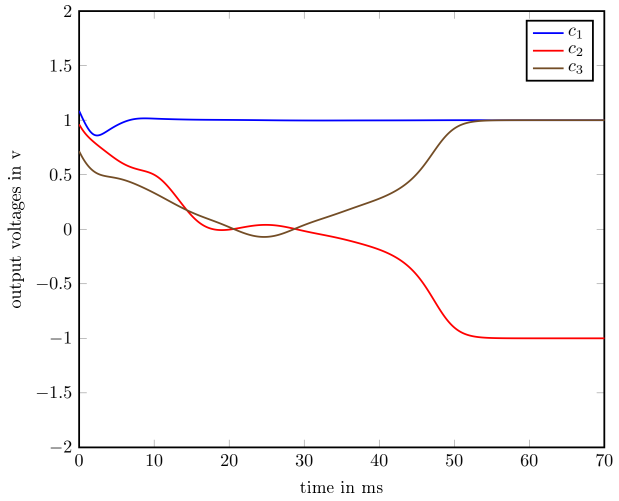

Fig. 6: Emulation results show a fast convergence of 50ms to the subset-sum problem of (7) with $w_1 = 2, w_2 = 1, w_3 = 5$ and $s = 7$.

can be deployed in order to solve the NP-complete problem of the subset sum.

VI. Conclusion and Outlook

In this work, the subset sum problem was investigated in order to find its inverse operation through circuits on the basis of self-organizing logic gates with physical models of RRAM-cells. The intrinsic parallelism of electrical quantities makes these approaches suitable candidates to solve mathematically complex problems efficiently. We developed an emulator based on the wave digital algorithm and confirmed the proper functioning of SOLGs with RRAM-cells through our emulation results.

For future research it is interesting to investigate if the setup works for large amounts of numbers, as they would be practically used in cryptographic approaches to cybersecurity. Emulators like ours will aid this research by enabling live sensitivity analyses or parameter optimization to enhance convergence speed [16]. Additionally, different algorithms for the protection of sensible data, possibly on the basis of mathematically even more complex problems, need to be developed for post-memcomputing cryptosystems.

Acknowledgment

The financial support by the German Research Foundation (Deutsche Forschungsgemeinschaft - DFG) through FOR 2093 and DFG-404291403 is gratefully acknowledged.

References

[1] A. Kate *et al.*, "Generalized Cryptosystems Based on the Subset Sum Problem," *International Journal of Information Security*, vol. 10, no. 3, pp. 189 – 199, Jun. 2011.

[2] A. Daskin, "A Quantum Approach to Subset-Sum and Similar Problems," *arXiv:1707.08730v4*, Sep. 2017.

[3] F. Traversa *et al.*, "Polynomial-time Solution of Prime Factorization and NP-hard Problems with Digital Memcomputing Machines," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 27, no. 2, p. 023107, 2017.

[4] F. Traversa *et al.*, "Memcomputing NP-complete Problems in Polynomial Time using Polynomial Resources and Collective States," *Science Advances*, vol. 1, no. 6, Jul. 2015.

[5] Y. Bearden *et al.*, "Instantons in Self-Organizing Logic Gates," *Physical Review Applied*, vol. 9, pp. 034 029 1 – 8, 2018.

[6] L. Chua, "Everything You Wish to Know About Memristors But Are Afraid to Ask," *International Journal of Circuit Theory and Applications*, vol. 24, no. 2, pp. 319 – 368, Jun. 2015.

[7] V. Thangamani, "Memristor-Based Resistive Random Access Memory: Hybrid Architecture for Low Power Compact Memory Design," *Control Theory and Informatics*, vol. 4, no. 7, pp. 7–14, 2014.

[8] R. Waser *et al.*, "Redox-Based Resistive Switching Memories - Nanoionic Mechanisms, Prospects, and Challenges," *Advanced Materials*, vol. 21, no. 25-26, pp. 2632–2663, Jul. 2009.

[9] S. Dirkmann *et al.*, "Understanding Filament Growth and Resistive Switching in Hafnium Oxide Memristive Devices," *ACS Applied Materials and Interfaces*, vol. 17, no. 10, pp. 14 857 – 14 868, Mar. 2018.

[10] E. Bailey *et al.*, "Understanding Synaptic Mechanisms in SrTiO$_2$ RRAM Devices," *IEEE Transactions on Electron Devices*, pp. 1 – 7, 2018.

[11] A. Fettweis, "Wave Digital Filters: Theory and Practice," *Proceedings of the IEEE*, vol. 74, no. 2, pp. 270–327, Feb. 1986.

[12] K. Ochs *et al.*, "Wave Digital Emulation of Charge- or Flux-Controlled Memristors," *IEEE 59th International Midwest Symposium on Circuits and Systems*, pp. 1–4, Aug. 2016.

[13] E. Solan *et al.*, "Wave Digital Emulation of General Memristors," *International Journal of Circuit Theory and Applications*, pp. 1–17, Jul. 2018.

[14] E. Solan *et al.*, "Wave Digital Emulation of a TiN/Ti/HfO2/TiN RRAM Cell Based on a Semi-Physical Model," *submitted to International Journal of Circuit Theory and Applications*.

[15] T. Schwerdtfeger *et al.*, "A Multidimensional Approach to Wave Digital Filters with Multiple Nonlinearities," *22nd European Signal Processing Conference*, Sep. 2014.

[16] K. Ochs *et al.*, "Sensitivity Analysis of Memristors Based on Emulation Techniques," *IEEE 59th International Midwest Symposium on Circuits and Systems, Abu Dhabi, UAE*, pp. 1 – 4, Oct. 2016.