Verifying Inevitability of Oscillation in Ring Oscillators Using the Deductive SOS-QE Approach

Hafiz ul Asad
City University London

Kevin D. Jones
Plymouth University

Editor's notes:

■ **ROs ARE AN** integral part of today's system-on-chip designs. They are used for many purposes, including, reference clock generation, phase interpolation, frequency translation, etc. Ideally, these oscillators should start oscillating from all possible initial node voltages. Unfortunately, such ideal oscillators are impossible to design and there are always states (voltages on nodes) from where they fail to oscillate [1]. Oscillations in an RO can be pictorially shown by functions varying periodically over time, somewhat similar to a "sin" function. An another useful representation of oscillation is in the state space where oscillatory behavior corresponds to a periodic set of states. These two types of representations are depicted in Figure 1. By varying design parameters, such as transistors widths and lengths, the shape and/or location of this periodic path is greatly varied in the state space, as shown in Figure 2. More importantly, this impacts the frequency/phase response of an RO. For an RO to have the desired frequency with little or no phase distortion, the trajectories must converge to the desired periodic region in the state space. A periodic set of states is said to be almost globally inevitable (AGI), if an RO eventually reaches this set, from all but a negligible dead set of voltages on its nodes. This is an important property, and in [2], researchers at Rambus identified the failure of an even stage RO to have the global inevitability property for a subset of initial conditions and parameters. Proving that an RO starts from almost all arbitrary initial states (voltages on nodes) is beyond the existing SPICE-based simulation capabilities. This is because it requires infinite number of simulations to be carried out for establishing global inevitability of states.

Recently, there have been several efforts of using formal reachability analysis for the verification of the global inevitability property.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.
Digital Object Identifier 10.1109/MDAT.2016.2573588
Date of publication: 00 Month 00.

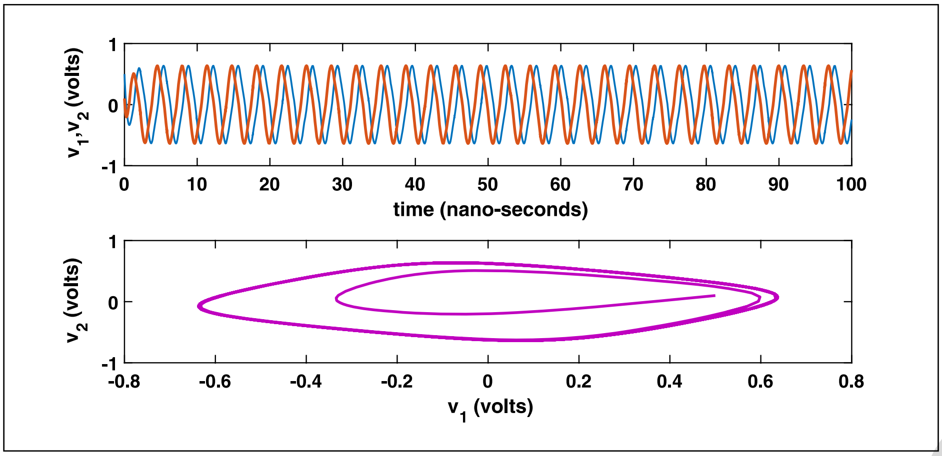

Figure 1. Different representation of RO oscillations.

Reachability tools model an RO as a continuous system, described by ordinary differential equations (ODEs), and use set-theoretic simulations to see whether a target set is reachable from an initial set. The inevitability property is verified by using reachability analysis iteratively. Reachability suffers from being of bounded-time nature, and since it relies on the over-approximate solutions of ODEs, is thus subjected to erroneous results. A survey of several such methods can be found in [3]. In [1], Yan et al. showed convergence to the oscillation in an even stage RO with probability one. They showed zero measure probability of the failure set using a cone argument. They further showed convergence to the desired limit cycle using reachability analysis. While the approach is comprehensive, it uses an expensive paper–pencil argument about the zero measure probability of the failure set. Then, they used the approximate but sound reachability computations, which is of bounded time nature and computationally very expensive.

In this paper, we present a deductive approach to verify the AGI of oscillations in an RO. Our work is inspired by the Lyapunov theory of stability for dynamical systems [4] and uses a certificate-based deductive approach to verify the inevitability of oscillations in ROs. We define the verification task as a conjunction of several subproperties whose verification is delegated to the existence of several Lyapunov-like certificates. Construction of these certificates can be posed as first-order formulas (FOFs) with quantifiers (universal, existential). We use a sound numeric-symbolic approach, called SOS-QE, for the verification of these FOFs. This is basically using a numeric, yet computationally efficient, SOS programming technique for the certificates construction, followed by the symbolic validation of these certificates by the QE technique. A similar technique has been used for nonlinear gain analysis in [5]. In [6], Harrison used SOS in HOL theorem prover to verify positivity of the universally quantified polynomials. Deductive and deductive-bounded approaches have been used for the inevitability verification of a charge pump phase lock loop in [7]. To the best of our knowledge, this is the first deductive approach for the solution of the research problem posed in [2]. Being deductive, our approach does not solve the ODEs and thus avoids the conservative approximation their solutions. Furthermore, once the inevitability property is verified, it stands

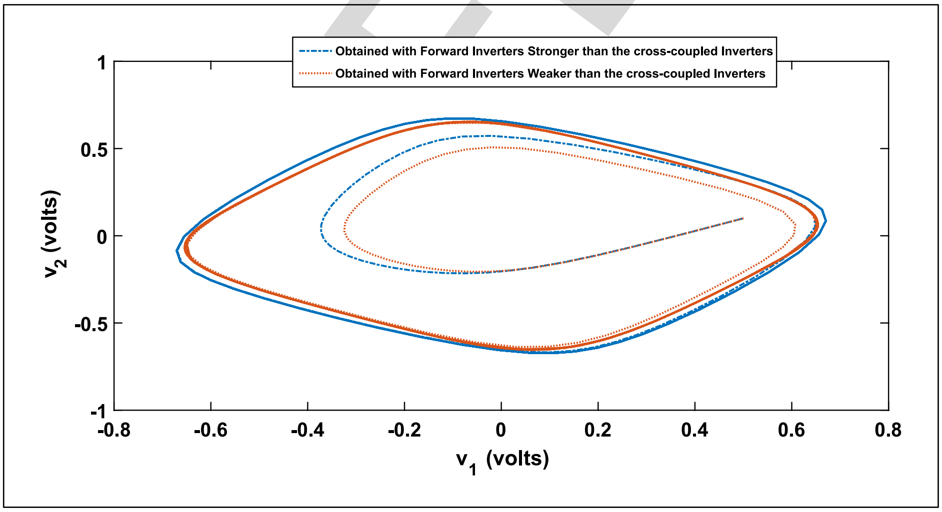

Figure 2. Parameter variation effect on the location of the periodic trajectory.

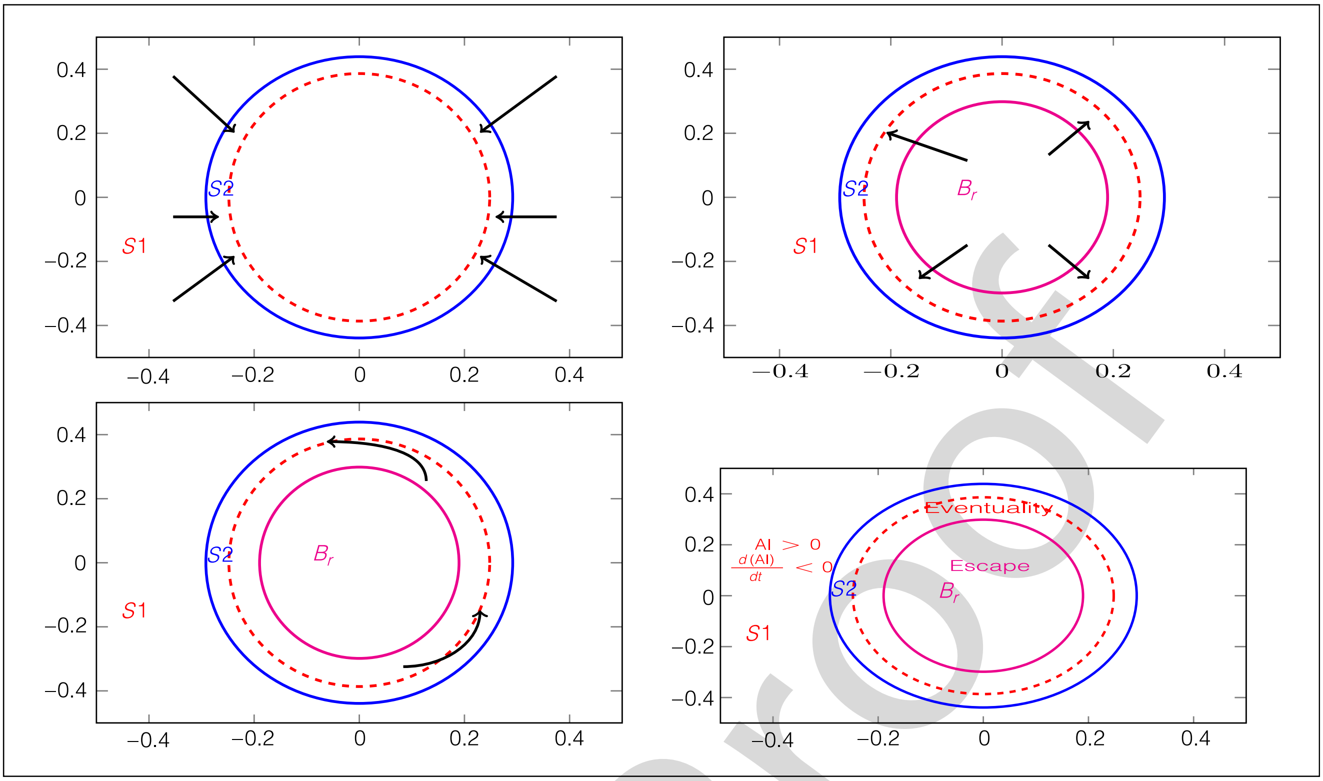

Figure 3. Verification strategy: Dividing the convergence of trajectories to the dashed Periodic set into several subtasks.

verified for the infinite time, unlike the bounded reachability analysis.

This article is organized as follows. First, we introduce the preliminaries of this article. Then, we illustrate verification of the inevitability of oscillation in RO, followed by the experimental results.

Preliminaries

Verification strategy

We use a divide-and-rule strategy and divide the verification task into several subtasks. To show that all trajectories converge with an arbitrarily small distance of the periodic trajectory, we do this in three phases as shown in Figure 3. In the first phase (top left), we show that trajectories from the set $\mathcal{S}1$ eventually reach $\mathcal{S}2$ and stay there forever. Note that the set $\mathcal{S}2$ is the area enclosed by the blue circular closed path whereas $\mathcal{S}1$ is the one outside it. In the second phase (top right), we show that almost all trajectories in the set $\mathcal{B}_r$, defined by the area enclosed by the magenta circular line, eventually reach an annular region defined by the set $\mathcal{S}2 \setminus \mathcal{B}_r$. In the second stage, we also show that none of the trajectories trap in the dead-set (from where RO fails to start). Finally, we show that all trajectories in the annular region (bottom left) converge to within an arbitrarily small distance of the desired periodic trajectory, shown by the dashed red circular path in Figure 3. For each of these three subtasks, we define three properties and state the AGI property as the conjunction of these three properties. Each of these subproperties specifies the long-term behavior of the trajectories of ROs in a specific subset of the state space which is verified by the existence of a certificate. These certificates, and their time derivatives, if exist, exhibit the characteristic of being positive (semipositive) or negative (seminegative) in their respective subsets. This scenario is depicted in the bottom right subfigure of Figure 3. As shown, we divide the space into three subsets: $\mathcal{S}1$, $\mathcal{S}2$, and $\mathcal{B}_r$. The dotted circle in the red shows the hypothetical location of the periodic trajectory (limit cycle) in the state space. The trajectories of an RO exhibit different long-term characteristics in these three different subsets. We use three different certificates called attractive invariance (AI), escape, and

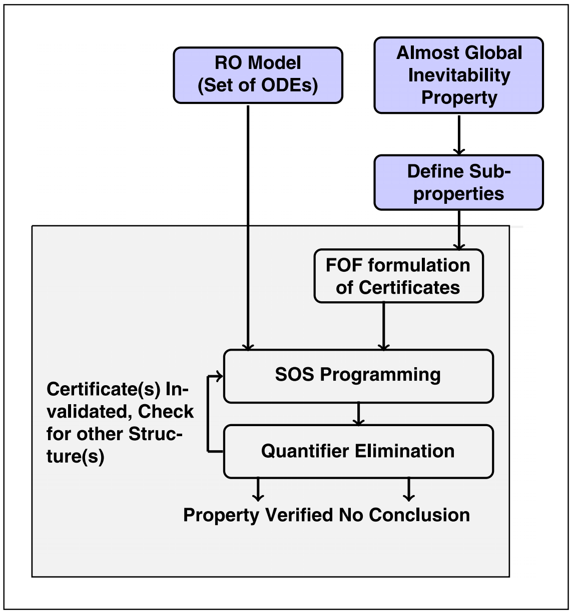

Figure 4. AGI property verification methodology.

eventuality to verify different subproperties. For illustration purposes, here we have depicted the positivity/negativity of the AI certificate in the set $\mathcal{S}1$. The existence of these certificates is formulated as verification of FOFs with universal–existential quantifiers over real polynomials. Verification of these FOFs is carried out using a numeric–symbolic technique of SOS programming and QE. The overall verification flow is shown in Figure 4. The existential quantification is solved by numerically finding different feasible certificates using SOS programming. To further validate these certificates, for their numerical imprecisions, symbolic analysis (QE) is carried out for each of the universally quantified formula. If a certificate is invalidated by the QE stage, a new search is made for a certificate(s) with a different structure this time. The output of our methodology results in either the AGI property being verified, or with no conclusion about its truthfulness, if a user-defined number of iterations have been exhausted.

Modeling of the ring oscillator

We model the RO shown in Figure 5 as a polynomial continuous dynamical system. Let us denote by x the vector of node voltages at the outputs of inverters. The continuous dynamical system model of an RO is a tuple $(\mathbf{X}, \mathcal{X}_{\text{initial}}, \mathbf{U}, f)$ where $\mathbf{X}$ is a set of state variables interpreted over $\mathbb{R}, \mathcal{X} = \mathbb{R}^{\mathbf{X}}$ is the set of all possible valuations of the variables, $\mathcal{X}_{\text{initial}} \subset \mathcal{X}$ is the set of initial conditions, $\mathbf{U}$ is the set of parameters (to model circuit capacitance, resistance, transistor parameters) interpreted over $\mathbb{R}$ with $U = \mathbb{R}^{\mathbf{U}}$ being the set of all possible parameter valuations, and

$$f : \mathcal{X} \times \mathcal{U} \rightarrow \mathcal{X} \tag{1}$$

the vector field characterizing the system. We assume that the vector field f is a polynomial function of $x \in \mathcal{X}$ called a polynomial vector field. Let us denote by $\Phi(x_0, t)$ the solution of equation $((d\Phi(X(t)))/dt) = f(\mathcal{X}, \mathcal{U}), X(0) = x_0 \in \mathcal{X}_{\text{init}}$.

Definition 1 (Equilibrium State). A state $x_e \in \mathcal{X}$ is called an equilibrium of the RO, iff $f(x_e) = 0$.

Definition 2 (Attractive Invariance of a Set). A set $\mathcal{X}_I$ is invariant iff $\forall x_0 : x_0 \in \mathcal{X}_I$, $\Phi(x_0, t) \in \mathcal{X}_I$ for all t. It is called attractive invariant (AI) iff $\forall x_0 : x_0 \in \mathcal{X} \setminus \mathcal{X}_I$, $\lim_{t \to b} \Phi(x_0, t)\mathcal{X}_I, b \in \mathbb{R}_{\geq 0}$.

Definition 3 (Limit Cycle). A set $\gamma \subset \mathcal{X}$ is called a limit cycle, iff $\forall x_0 : x_0 \in \gamma, \Phi(x_0, T) = x_0$ for $T > 0$, and for all $0 < t < T$, $\Phi(x_0, t) \neq x_0$. This is an invariant set.

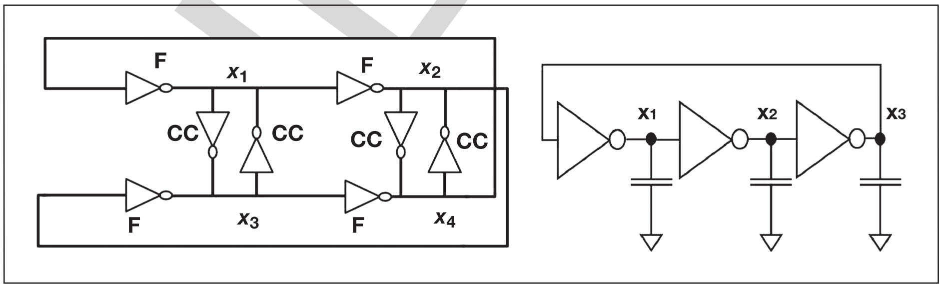

Figure 5. Two different topologies of ring oscillators. Left: Even stage RO. Right: Odd stage RO.

Definition 4 (Inevitability of the Limit Cycle). The limit cycle γ is said to be inevitable, iff $\forall x_0 : x_0 \in \mathcal{X}_{\text{initial}}, y \in \gamma, r > 0$, $b \in \mathbb{R}_{\geq 0}$

$$\lim_{t \to b} \|\Phi(x_0, t) - y\| \leq r. \tag{2}$$

Assumption 1. In this work, we assume that the location of γ in the state space is known.

For a practically feasible RO, there are states in $\mathbb{R}^n$ from where it fails to start and reaches the limit cycle γ [1]. For example, equilibrium is one such state from where an RO cannot start. We call the set of all such states the "dead set."

Definition 5 (Dead Set). A set of states is called a dead set denoted by $\mathcal{X}_{\text{dead}}$, such that $\forall x_0 : x_0 \in \mathcal{X}_{\text{dead}}$, $\lim_{t\to\infty} \|\Phi(x_0, t) - x_e\| = 0$. Here x_e is an equilibrium state.

Definition 6 (AGI of Oscillation in RO). The limit cycle $\gamma \subset \mathcal{X}$ is said to be "almost globally inevitable," iff $\forall x_0 : x_0 \in \{\mathcal{X} \setminus \mathcal{X}_{\text{dead}}\}, y \in \gamma, r > 0, b \in \mathbb{R}_{\geq 0}$

$$\lim_{t\to b} \|\Phi(x_0, t) - y\| \leq r. \quad (3)$$

In this paper, we consider two different topologies of ROs, i.e., the odd stage and the even stage RO as depicted in Figure 5. While we treat each individual node voltage as a state variable for the odd stage RO, we use the strategy suggested in [1] for the even stage RO, and divide its operation into differential and common modes. We denote the node voltages of the even stage RO by $x(0,j)$ and $x(1,j)$ for $j = 0, 1, \ldots, n-1$. Here n is the number of stages. For the even stage RO in Figure 5, $x(0,0) = \mathcal{X}_1, x(0,1) = \mathcal{X}_2, x(1,0) = \mathcal{X}_3, x(1,1) = \mathcal{X}_4$. The voltages $x(0,j)$ and $x(1,j)$ form the differential pair whose differential component is $x(0,j) - x(1,j)$, and the common mode component is $x(0,j) + x(1,j)$. The even stage RO, while operating normally, has its oscillation manifested in the differential mode, whereas the common mode settles to the constant zero value. If we assume that inverters are identical, then, $\forall j : j \in [0, n-1], \forall x : x \in \mathcal{X}$ such that $x(0,j) = x(1,j)$, we have $\Phi(x,t) = x_e$ as $t \to \infty$. This means that the set $\{x(0,j) = x(1,j), \forall j : j \in [0, n-1]\} \in \mathcal{X}_{\text{dead}}$. Similarly, for odd stage RO, if $x_1 = x_2 = x_3$, then $\lim_{t\to\infty} \Phi(x,t) = x_e$.

RO properties verification using Lyapunov-like certificates

To verify the AGI of the limit cycle γ, we use several Lyapunov-like certificates in different subsets of the state space of the RO, Figure 3. To show attractive invariance of a set, a Lyapunov-like certificate has been presented in [8].

Lemma 1. If there exist a polynomial with real coefficients $V : \mathcal{X} \to \mathbb{R}$, $\epsilon > 0$ and a minimum $\eta > 0$ such that

1) $V(x) > 0, \forall x \in \mathbb{R}^n \setminus 0$;
2) $\{V(x) = 1\} \subseteq \{q(x) \leq \eta\}$;
3) $\{V(x) \geq 1\} \subseteq \{(\partial V/\partial x)(x).f(x,u) \leq \epsilon\}$;

then the set $\mathcal{S}2 := \{V(x) \leq 1\}$ is an AI set for an RO with a vector field given in (1), and it is contained in the set $\{q(x) \leq \eta\}$ where $q : \mathcal{X} \to \mathbb{R}$.

Proof. See [8]. □

In the above Lemma 1, the set $\{q(x) = \eta\}$ is used for optimization purposes and the parameter η is minimized so that this set contains the desired AI set $\mathcal{S}2 := \{V(x) \leq 1\}$. Inside the AI set $\mathcal{S}2$, trajectories can reach either the dead set $\mathcal{X}_{\text{dead}}$ or to within a small distance of the limit cycle γ (shown in dotted red in Figure 3). Let us define a set $\mathcal{B}_r = V(x) \leq r$, $0 < r < 1$ (shown in magenta in Figure 3). To show that trajectories starting in the set $\mathcal{B}_r$ are not trapped in the dead set $\mathcal{X}_{\text{dead}}$, and eventually escape to the set $\mathcal{S}2 \setminus \mathcal{B}_r$, we introduce an escape certificate.

Lemma 2. For a compact set $\mathcal{B}_r \subset \mathcal{S}2$, if there is a differentiable escape certificate, $\mathcal{E} : \mathcal{X} \to \mathbb{R}$, such that:

1) $\mathcal{E}(x) = 0 \ \forall x : x \in \mathcal{X}_{\text{dead}}$;
2) $\mathcal{E}(x) > 0 \ \forall x : x \in \mathcal{B}_r \setminus \mathcal{X}_{\text{dead}}$;
3) $(\partial \mathcal{E}/\partial x)(x).f(x,u) > 0 \ \forall x : x \in \mathcal{B}_r \setminus \mathcal{X}_{\text{dead}}$;

then $\forall x : x \in \{\mathcal{B}_r \setminus \mathcal{X}_{\text{dead}}\}, \lim_{t\to\infty} x(t) \notin \mathcal{B}_r$.

Proof. See [4, Ch. 4]. □

To show that trajectories in the set $\mathcal{S}2 \setminus \mathcal{B}_r$ eventually reach to within a close distance of the limit cycle γ, we use the eventuality certificate presented in [9]. Let us have a set $\mathcal{X}_{\text{LC}}$, such that $\|y - x\| \leq \alpha, \forall x \in \mathcal{X}_{\text{LC}}, y \in \gamma, \alpha > 0$.

Theorem 1. If there exists a differentiable certificate of eventuality $E : \mathcal{X} \to \mathbb{R}$ satisfying the following conditions:

1) $E(x) \leq 0 \ \forall x \in (\mathcal{S}2 \setminus \mathcal{B}_r) \setminus \mathcal{X}_{\text{dead}}$;
2) $E(x) > 0 \ \forall x \in Cl(\partial \mathcal{S}2 \setminus \partial \mathcal{X}_{\text{LC}})$;
3) $(\partial E/\partial x)(x).f(x,u) < 0 \ \forall x \in Cl(\mathcal{S}2 \setminus \mathcal{X}_{\text{LC}})$;

then for all initial conditions $x_0 \in \mathcal{S}2 \setminus \mathcal{B}_r$, the trajectory $x(t)$ satisfies $x(T) \in \mathcal{X}_{\text{LC}}$, for some $T \geq 0$ and for all $t \in [0, T]$, $x(t) \in X$. Here Cl and ∂ denote closure and boundary of a closed set, respectively.

Proof. See [9]. □

For the common mode of the even stage RO, we further show that common mode voltages settle down to zero in the steady state. We verify this using the Lyapunov certificate restated for the common mode in Theorem 2.

Theorem 2. For the continuous dynamical system with a vector field given in (1), and with the state vector replaced by $x = \{x(0,0) + x(1,0), x(0,1) + x(1,1), \ldots, x(0, n-1) + x(1, n-1)\}$, let us assume an invariant set $\mathcal{X}_{\text{com}}$, which we call the common-mode state space. Note that this set is invariant due to the fact that node voltages are bounded by the supply voltage. If there exists a Lyapunov certificate $\mathcal{L} : \mathcal{X} \to \mathbb{R}$ such that

$$\mathcal{L}(x) > 0,\ \forall x \in \{\mathcal{X}_{\text{com}} \setminus \{0\}\}, \mathcal{L}(0) = 0 \quad (4)$$

$$\frac{\partial L}{\partial x}(x).f(x,u) < 0,\ \forall x \in \{\mathcal{X}_{\text{com}} \setminus \{0\}\} \quad (5)$$

then the set $\{x = 0\}$ is asymptotically stable, and $\forall x \in \mathcal{X}_{\text{com}}$, $\lim_{t\to\infty} \Phi(x,t) = 0$.

Proof. Similar to [4]. □

SOS programming and QE

We formulate our verification methodology as a conjunction of several FOFs having polynomial equations, inequalities, quantifiers $\{\forall, \exists\}$ and boolean operators $\{\wedge, \vee, \neg, \to, \text{etc.}\}$. There are algorithms that can, in principle, generate quantifier-free formulas from a universal–existential quantified FOF over the real fields (see [6] and the references therein). However, they are complex and only work for small academic problems. Showing positivity of a real polynomial, SOS uses a sufficient but incomplete criterion of establishing the decomposition of the polynomial into a sum of squares of polynomials [10]. A sufficient condition for a multivariate polynomial $p(x)$ to be nonnegative everywhere is that it can be decomposed as a sum of squares of polynomials, i.e., $p(x) = \sum_{i=1}^{m} p_i^2(x), p_i(x) \in \mathcal{R}_n$. We denote the set of polynomials in n variables with real coefficients by $\mathcal{P}_n$. A subset of this set is the set of SOS polynomials in n variables denoted by $\mathcal{S}_n$.

Verification of AGI of oscillation in RO

Formulation of the verification problem

We formulate the verification of the AGI property as the conjunction of different subproperties, corresponding to the three subfigures in Figure 3, defined below.

Property 1. $\forall x(0) : x(0) \in \mathcal{S}1, \lim_{t\to b} x(t) \in \mathcal{S}2$, $b \in \mathbb{R}_{\geq 0}$.

Property 2. $\forall x(0) : x(0) \in \mathcal{B}_r, \lim_{t\to\infty}(x(t) \notin \mathcal{X}_{\text{dead}} \wedge x(t) \in \mathcal{S}2 \setminus \mathcal{B}_r)$.

Property 3. $\forall x(0) : x(0) \in \mathcal{S}2 \setminus \mathcal{B}_r, \lim_{t\to b} \|y - x(t)\| \leq \alpha, y \in \gamma, b \in \mathbb{R}_{\geq 0}, \alpha > 0$.

We define a fourth property characterizing the common mode behavior of the even stage RO in the invariant set $\mathcal{X}_{\text{com}}$.

Property 4. $\forall x(0) : x(0) \in \mathcal{X}_{\text{com}}, \lim_{t\to\infty} x(t) = 0$.

If we denote the almost global inevitability property by φ, Property 1 by $\varphi 1$, Property 2 by $\varphi 2$, Property 3 by $\varphi 3$, and Property 4 by $\varphi 4$, then $\varphi = \varphi 1 \wedge \varphi 2 \wedge \varphi 3$, for the odd stage RO, and, $\varphi = \varphi 1 \wedge \varphi 2 \wedge \varphi 3 \wedge \varphi 4$, for the even stage RO. A trajectory $x(t)$ of the odd stage RO satisfies φ, iff it satisfies $\varphi 1$ in $\mathcal{S}1$, $\varphi 2$ in $\mathcal{B}_r$, and $\varphi 3$ in $\mathcal{S}2 \setminus \mathcal{B}_r$, i.e., $\forall x : x \in \mathcal{X}, x \models \varphi \Longleftrightarrow (x \models \varphi 1\, \forall x : x \in \mathcal{S}1) \wedge (x \models \varphi 2\, \forall x : x \in \mathcal{S}2) \wedge (x \models \varphi 3\, \forall x : x \in \mathcal{S}2 \setminus \mathcal{B}_r)$.

Similarly, for en even stage RO, $\forall x : x \in \mathcal{X}, x \models \varphi \Longleftrightarrow (x \models \varphi 1\, \forall x : x \in \mathcal{S}1) \wedge (x \models \varphi 2\, \forall x : x \in \mathcal{B}_r) \wedge (x \models \varphi 3\, \forall x : x \in \mathcal{S}2 \setminus \mathcal{B}_r) \wedge (x \models \varphi 4\, \forall x : x \in \mathcal{X}_{\text{com}})$.

SOS-QE approach to verify AGI of oscillation

Here we present the formalization and verification of Property 1 using a SOS-QE approach and a similar approach is used for the verification of other subproperties. We define the conditions of Lemma 1 by the following FOF:

$$\psi_0 := \exists p^{\mathcal{P}} : \psi_1$$
$$\psi_1 := \forall x^{\mathcal{X}} : \psi_2$$
$$\psi_2 := \Big((x \neq 0 \Longrightarrow V(p,x) > 0)$$
$$\wedge \big\{ (1 - V(p,x) \geq 0) \Longrightarrow (\eta - q(x)) \geq 0 \big\}$$
$$\wedge \left\{ (V(p,x) - 1 \geq 0) \Longrightarrow \left(\frac{\partial V}{\partial x}(p,x).f(x,u) \leq -\epsilon \right) \right\} \Big).$$

Here $p \in \mathcal{P}$ represents the coefficients space of the certificate V. A sufficient condition for the verification of property $\varphi 1$ is stated in the following theorem.

Theorem 3. If there is a feasible certificate $V(x)$, fulfilling the conditions in Lemma. 1, then $(x \models \psi_0 \Longleftrightarrow x \models \varphi 1), \forall x(0) \in \mathcal{S}1$, and $\mathcal{S}2 = V(x) \leq 1$.

Following the sufficiency conditions in Theorem 3, we verify $\varphi 1$ using the mixed SOS-QE approach. We start with a SOS program searching for the AI certificate $V(x)$ such that it satisfies the conditions in Lemma. 1. Note that every condition on $V(x)$ in Lemma 1 is a positivity/negativity condition which can be formulated as a SOS condition. Furthermore, we need these conditions to be satisfied in different sets which are encoded using a sound mathematical technique called the S-procedure [10]. A SOS program incorporating these conditions is given as follows:

$$\begin{aligned} &\text{minimize} \quad \eta \\ &\text{subject to} \end{aligned}$$

(i) $V(0) = 0$

(ii) $(V(x) - \epsilon - \sum_{k=1}^{n} s_1^k(x) g_k(x)) \in \mathcal{S}_n$

(iii) $(\eta - q(x)) - s_2(x)(1 - V(x)) \in \mathcal{S}_n$

(iv) $((-\epsilon - (\partial V/\partial)(x).f(x,u)) - s_3(x)(V(x) - 1) - \sum_{k=1}^{n} s_4^k(x) g_k(x) - \sum_{j=1}^{m} s_5^j(x)\, a_j(u)) \in \mathcal{S}_n$, $\forall x \in \mathcal{X}, \{s_1^k, s_2, s_3, s_4^k, s_5^j\}\ \mathcal{S}_n, \forall k \in \{1, \ldots, n\}, \forall j \in \{1, \ldots, m\}, \epsilon > 0, \eta > 0.$

Here $V(x)$, $s_1^k, s_2, s_3, s_4^k, s_5^j$, are polynomials of degree d.

In this SOS program, constraint (ii) enforces positive definiteness on the certificate $V(x)$ by introducing a small positive number ϵ. This constraint has to be satisfied in the state space $\mathcal{X}$ defined as $\mathcal{X} = \{x \in \mathbb{R}^n : g_k(x) \geq 0, \text{for } k \in \{1, \ldots, n\}\}$. Constraint (iii) ensures that $\{V(x) \leq 1\} \subseteq \{q(x) \leq \eta\}$. Constraint (iv) incorporates the set inclusion $\{V(x) \geq 1\} \subseteq \{\partial V/\partial x.f(x,u) \leq \epsilon\}$. This constraint also ensures that parameters u belong to the set $\{a_j(u) \geq 0, \text{ for } j \in \{1, \ldots, m\}$. The above SOS program, if feasible, returns a certificate of attractive invariance $V(x)$ with its parameters $p \in \mathcal{P}$ fixed within a limited numerical precision. We further verify the validity of this certificate using symbolic QE. Note that in QE, coefficients are represented in $\mathbb{Q}^n$. Using QE, we check the truth value of the negation of the formula ψ_1, since the existential quantifier has already been eliminated by the SOS program. On refutation of $\neg\psi_1$, we conclude $(x \models \varphi 1 \Longleftrightarrow x \models \psi_0), \forall x \in \mathcal{S}1$. If either the SOS program is infeasible for a certificate $V(x)$, or the QE tool returns a true valuation for the formula $\neg\psi 1$, we repeat the process by increasing the degree of the certificate $V(x)$. If we still cannot get the desired certificate, we conclude inconclusiveness about the truth value of $\varphi 1$.

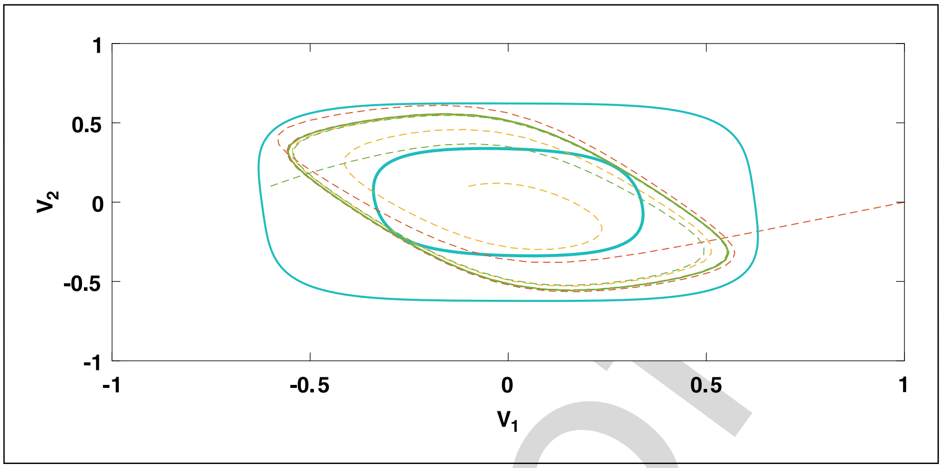

Figure 6. Odd RO AI set $\{r <= V <= 1\}$: Annular region between solid green plots, trajectories: dashed plots.

Experimental evaluation

We used a degree-7 least-square polynomial model characterizing the input–output nonlinear

Table 1 Odd RO inevitability verification time.

Certificate	YALMIP-SOS Time (Sec)	REDLOG-QE Time (Sec)
Attractive Invariants	824.8 (Degree 4)	Clause 1 = 0.219 Clause 2 = 0.047 Clause 3 = 8.222
Escape	6.3 (Degree 2)	Clause 1 = 0.060 Clause 2 = 0.026 Clause 3 = 0.320
Eventuality	31.5 (Degree 4)	Clause 1 = 0.070 Clause 2 = 0.025 Clause 3 = 0.636

Table 2 Even RO inevitability verification time.

Certificate	YALMIP-SOS Time (Sec)	REDLOG-QE Time (Sec)
Attractive Invariants	6127.6 (Degree 10)	Clause 1 = 5.24 Clause 2 = 0.33 Clause 3 = 1.56
Escape	320.6757 (Degree 4)	Clause 1 = 0.01 Clause 2 = 0.30 Clause 3 = 2.50
Eventuality	4128.8 (Degree 6)	Clause 1 = 0.349 Clause 2 = 0.300 Clause 3 = 0.615
Lyapunov	55.24 (Degree 4)	Clause 1 = 0.02 Clause 2 = 0.75 Clause 3 = 0.57

behavior of an inverter. We obtained this approximation of the inverter model by running MATLAB simulation using the Schichman–Hodges MOS transistor models. Note that, in this model, we take into account the effect of transistor widths/lengths on the slope of the inverter output. We used YALMIP [11] solver within MATLAB for SOS programming, and REDLOG [12], for QE on a 2.6-GHZ Intel Core i5 machine with 4 GB of memory. For an odd RO, we were able to compute a degree-4 AI certificate. The AI set, marked by the level set $V(x) \leq 1$, is shown in Figure 6. Inside the AI set, we showed trajectories escape the set $V \leq r$, by computing a degree-2 escape certificate. Similarly, the convergence of the trajectories to within a small distance of the limit cycle has been shown by computing a degree-4 eventuality certificate in the set $\{V \leq 1 \wedge V \geq r\}$. Time taken by the SOS solver to compute these certificates is listed in the second column of Table 1. Verification of these certificates in REDLOG, given its ability of how large a formula it can handle, has been divided into the verification of the individual clauses of the FOFs benefiting from its disjunctive normal form (DNF). Since we were interested in the negation of FOFs in the DNF, we verified whether each clause was "false." The verification times of the QE are listed in the third column of Table 1. For AI and escape certificates, REDLOG successfully verified the negation of their universally quantified FOFs. A timeout was reported by the REDLOG tool for all clauses of the eventuality FOF of the odd RO. The reason for these timeouts is the set, an intersection of two level curves of the AI certificate, that puts an additional burden on the solver resulting in its timeout. To overcome this issue, we instead conservatively over-underapproximate the set $\{V \leq 1 \wedge V \geq r\}$, by a quadratic polynomial, and construct the eventuality certificate for this new set. This solved our problem and REDLOG has been able to verify the eventuality certificate in this conservative approximation of the set $\{V \leq 1 \wedge V \geq r\}$. Note that this conservatism is to approximate the annular set $\{V \leq 1 \wedge V \geq r\}$ and does not add to the overall conservatism of our methodology.

Similarly, for the even stage RO, we computed a degree-10 AI, a degree-4 escape, a degree-6 eventuality, and a degree-4 Lyapunov certificate. Computation times are given in Table 2 and the AI set is shown in Figure 7.

Though verifying the property, using SOS-QE approach, needs user input, it offers a comparable computation time to [1]. Yan et al. have reported approximately 22000 s for the complete verification of the even stage RO, whereas our accumulative time for the even stage RO is approximately 6500 s. Even if we add the time of all the instances for which we received an infeasible certificate, our computation time is still not more than half of what has been reported in [1]. This is in addition to our methodology being less conservative and applicable to an infinite horizon.

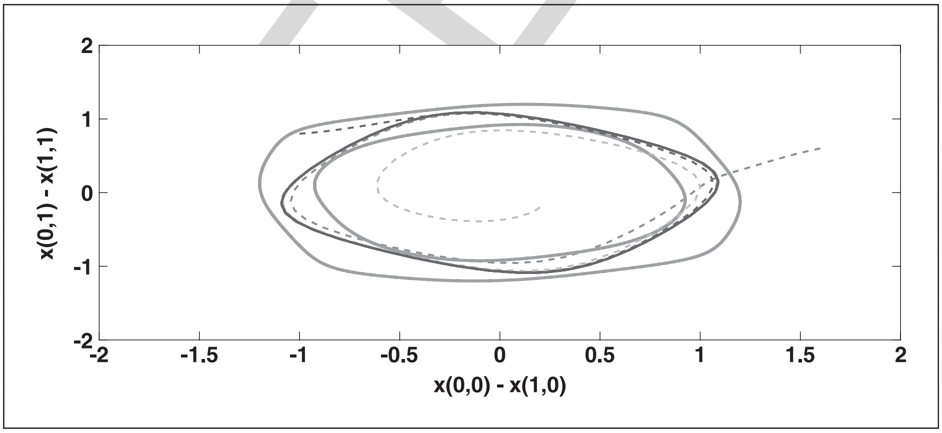

Figure 7. Even RO AI set $\{r <= V <= 1\}$: Annular region between solid green plot, trajectories: dashed.

RESULTS SHOW THE effectiveness of our approach to verifying the complex AGI property of a real-world analog circuit. We have verified the AGI using the Lyapunov-based deductive method which is not only applicable to infinite time, but also avoids explicitly solving ODEs and is thus less conservative than the reachability approaches. ■

References

[1] C. Yan, M. R. Greenstreet, and S. Yang, "Verifying global start-up for a Möbius ring-oscillator," *Formal Methods Syst. Design*, vol. 45, no. 2, pp. 246–272, 2014.

[2] K. D. Jones, J. Kim, and V. Konrad, "Some real world problems in the analog and mixed signal domains," in *Designing Correct Circuits*, 2008.

[3] M. H. Zaki, S. Tahar, and G. Bois, "Formal verification of analog and mixed signal designs: A survey," *Microelectron. J.*, vol. 39, no. 12, pp. 1395–1404, 2008.

[4] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.

[5] H. Ichihara and H. Anai, "An SOS-QE approach to nonlinear gain analysis for polynomial dynamical systems," *Math. Comput. Sci.*, vol. 5, no. 3, pp. 303–314, 2011.

[6] J. Harrison, "Verifying nonlinear real formulas via sums of squares," in *Theorem Proving in Higher Order Logics*, vol. 4732, Lecture Notes in Computer Science, pp. 102–118, Berlin, Germany: Springer-Verlag, 2007.

[7] H. Asad and K. D. Jones, "Verifying inevitability of phase-locking in a charge pump phase lock loop using sum of squares programming," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf.*, 2015, pp. 295–300.

[8] W. Tan, "Nonlinear control analysis and synthesis using sum-of-squares programming," PhD dissertation, Univ. California Berkeley, Berkeley, CA, USA, 2006.

[9] S. Prajna and A. Rantzer, "Convex programs for temporal verification of nonlinear dynamical systems," *SIAM J. Control Optim.*, vol. 46, no. 3, pp. 999–1021, 2007.

[10] S. Prajna and A. Papachristodoulou, "Analysis of switched and hybrid systems-beyond piecewise quadratic methods," in *Proc. Amer. Control Conf.*, vol. 4, 2003, pp. 2779–2784.

[11] J. Lofberg, "Yalmip: A toolbox for modeling and optimization in matlab," in *Proc. IEEE Int. Symp. Comput. Aided Control Syst. Design*, 2004, pp. 284–289.

[12] A. Dolzmann and T. Sturm, "Redlog: Computer algebra meets computer logic," *ACM SIGSAM Bull.*, vol. 31, no. 2, pp. 2–9, 1997.

Hafiz ul Asad is a Research Assistant at the Center for Software Reliability, City University London, London, U.K. His research interests include hardware verification, dynamical systems, and formal methods. ul Asad has a PhD in electrical engineering from City University London.

Kevin D. Jones is the Executive Dean at the Faculty of Science and Engineering, University of Plymouth, Plymouth, U.K. His research interests include hardware verification, formal methods, and cyber security. Jones has a PhD in computing science from Manchester, Manchester, U.K. He is a Senior Member of the IEEE, and a Fellow of IET and BCS. AQ1

■ Direct questions and comments about this article to Hafiz ul Asad, City University London, EC1V 0HB London U.K.; hafiz.ul-asad.1@city.ac.uk.

AUTHOR QUERY

AUTHOR PLEASE ANSWER QUERY

AQ1 = Please define IET and BCS.

END OF QUERY

Verifying Inevitability of Oscillation in Ring Oscillators Using the Deductive SOS-QE Approach

Hafiz ul Asad
City University London

Kevin D. Jones
Plymouth University

Editor's notes:

■ **ROs are an** integral part of today's system-onchip designs. They are used for many purposes, including, reference clock generation, phase interpolation, frequency translation, etc. Ideally, these oscillators should start oscillating from all possible initial node voltages. Unfortunately, such ideal oscillators are impossible to design and there are always states (voltages on nodes) from where they fail to oscillate [1]. Oscillations in an RO can be pictorially shown by functions varying periodically over time, somewhat similar to a "sin" function. An another useful representation of oscillation is in the state space where oscillatory behavior corresponds to a periodic set of states. These two types of representations are depicted in Figure 1. By varying design parameters, such as transistors widths and lengths, the shape and/or location of this periodic path is greatly varied in the state space, as shown in Figure 2. More importantly, this impacts the frequency/phase response of an RO. For an RO to have the desired frequency with little or no phase distortion, the trajectories must converge to the desired periodic region in the state space. A periodic set of states is said to be almost globally inevitable (AGI), if an RO eventually reaches this set, from all but a negligible dead set of voltages on its nodes. This is an important property, and in [2], researchers at Rambus identified the failure of an even stage RO to have the global inevitability property for a subset of initial conditions and parameters. Proving that an RO starts from almost all arbitrary initial states (voltages on nodes) is beyond the existing SPICE-based simulation capabilities. This is because it requires infinite number of simulations to be carried out for establishing global inevitability of states.

Recently, there have been several efforts of using formal reachability analysis for the verification of the global inevitability property.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/MDAT.2016.2573588
Date of publication: 00 Month 00.

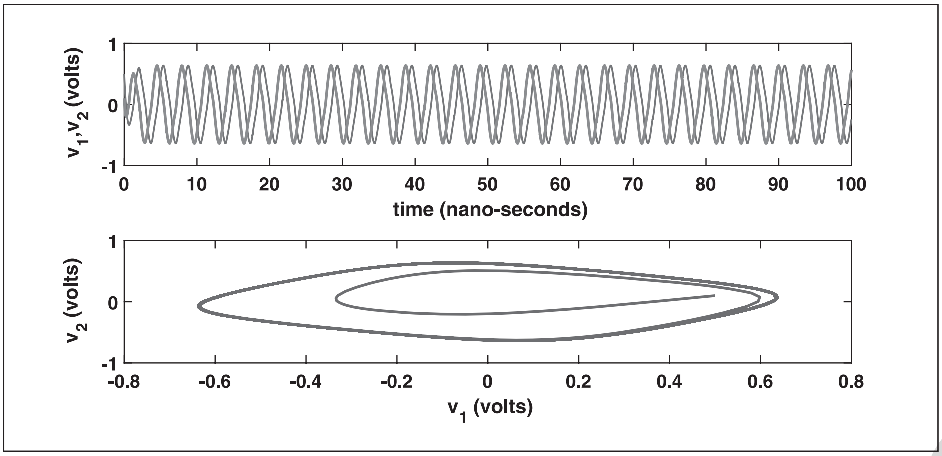

Figure 1. Different representation of RO oscillations.

Reachability tools model an RO as a continuous system, described by ordinary differential equations (ODEs), and use set-theoretic simulations to see whether a target set is reachable from an initial set. The inevitability property is verified by using reachability analysis iteratively. Reachability suffers from being of bounded-time nature, and since it relies on the over-approximate solutions of ODEs, is thus subjected to erroneous results. A survey of several such methods can be found in [3]. In [1], Yan et al. showed convergence to the oscillation in an even stage RO with probability one. They showed zero measure probability of the failure set using a cone argument. They further showed convergence to the desired limit cycle using reachability analysis. While the approach is comprehensive, it uses an expensive paper–pencil argument about the zero measure probability of the failure set. Then, they used the approximate but sound reachability computations, which is of bounded time nature and computationally very expensive.

In this paper, we present a deductive approach to verify the AGI of oscillations in an RO. Our work is inspired by the Lyapunov theory of stability for dynamical systems [4] and uses a certificate-based deductive approach to verify the inevitability of oscillations in ROs. We define the verification task as a conjunction of several subproperties whose verification is delegated to the existence of several Lyapunov-like certificates. Construction of these certificates can be posed as first-order formulas (FOFs) with quantifiers (universal, existential). We use a sound numeric-symbolic approach, called SOS-QE, for the verification of these FOFs. This is basically using a numeric, yet computationally efficient, SOS programming technique for the certificates construction, followed by the symbolic validation of these certificates by the QE technique. A similar technique has been used for nonlinear gain analysis in [5]. In [6], Harrison used SOS in HOL theorem prover to verify positivity of the universally quantified polynomials. Deductive and deductive-bounded approaches have been used for the inevitability verification of a charge pump phase lock loop in [7]. To the best of our knowledge, this is the first deductive approach for the solution of the research problem posed in [2]. Being deductive, our approach does not solve the ODEs and thus avoids the conservative approximation their solutions. Furthermore, once the inevitability property is verified, it stands

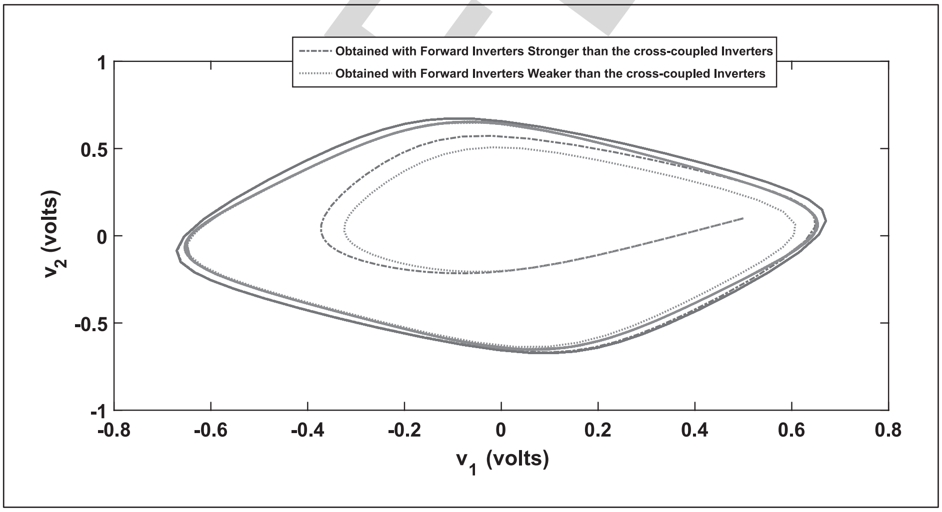

Figure 2. Parameter variation effect on the location of the periodic trajectory.

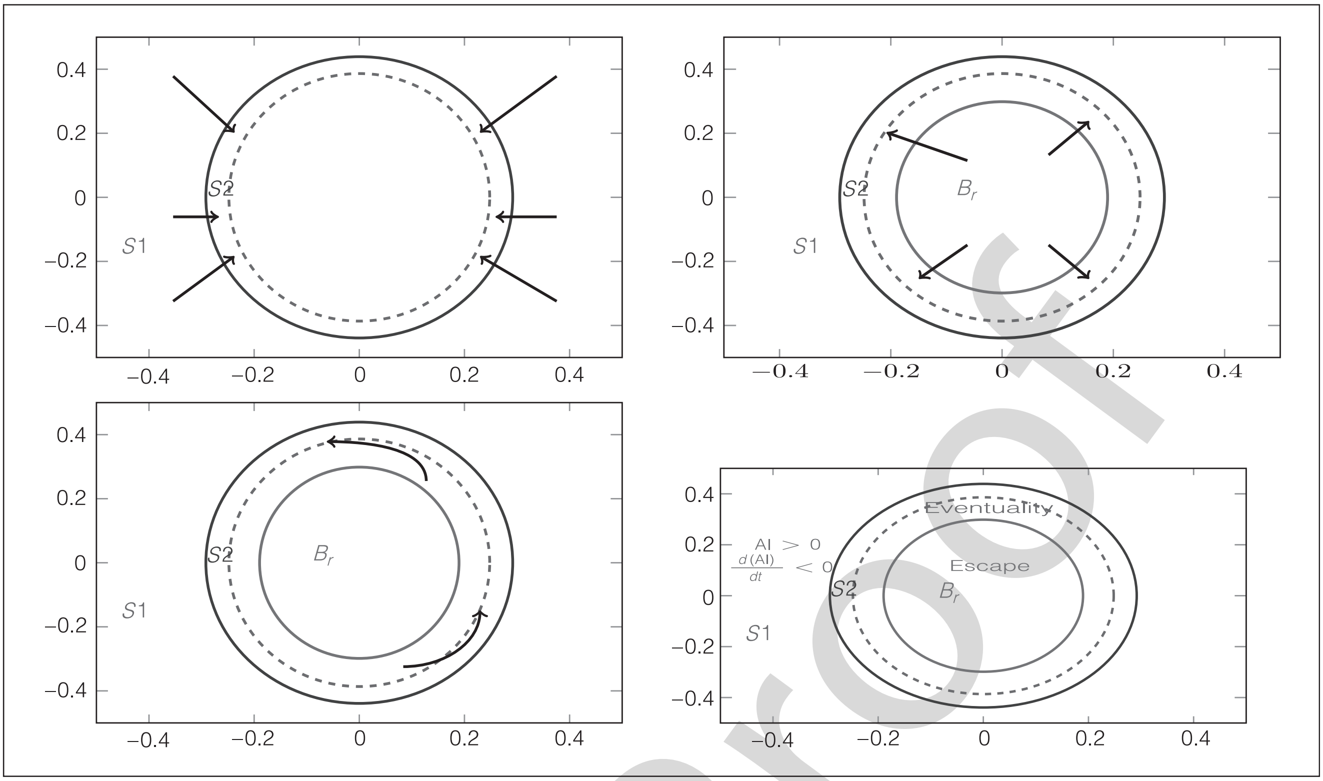

Figure 3. Verification strategy: Dividing the convergence of trajectories to the dashed Periodic set into several subtasks.

verified for the infinite time, unlike the bounded reachability analysis.

This article is organized as follows. First, we introduce the preliminaries of this article. Then, we illustrate verification of the inevitability of oscillation in RO, followed by the experimental results.

Preliminaries

Verification strategy

We use a divide-and-rule strategy and divide the verification task into several subtasks. To show that all trajectories converge with an arbitrarily small distance of the periodic trajectory, we do this in three phases as shown in Figure 3. In the first phase (top left), we show that trajectories from the set $\mathcal{S}1$ eventually reach $\mathcal{S}2$ and stay there forever. Note that the set $\mathcal{S}2$ is the area enclosed by the blue circular closed path whereas $\mathcal{S}1$ is the one outside it. In the second phase (top right), we show that almost all trajectories in the set $\mathcal{B}_r$, defined by the area enclosed by the magenta circular line, eventually reach an annular region defined by the set $\mathcal{S}2 \setminus \mathcal{B}_r$. In the second stage, we also show that none of the trajectories trap in the dead-set (from where RO fails to start). Finally, we show that all trajectories in the annular region (bottom left) converge to within an arbitrarily small distance of the desired periodic trajectory, shown by the dashed red circular path in Figure 3. For each of these three subtasks, we define three properties and state the AGI property as the conjunction of these three properties. Each of these subproperties specifies the long-term behavior of the trajectories of ROs in a specific subset of the state space which is verified by the existence of a certificate. These certificates, and their time derivatives, if exist, exhibit the characteristic of being positive (semipositive) or negative (seminegative) in their respective subsets. This scenario is depicted in the bottom right subfigure of Figure 3. As shown, we divide the space into three subsets: $\mathcal{S}1$, $\mathcal{S}2$, and $\mathcal{B}_r$. The dotted circle in the red shows the hypothetical location of the periodic trajectory (limit cycle) in the state space. The trajectories of an RO exhibit different long-term characteristics in these three different subsets. We use three different certificates called attractive invariance (AI), escape, and

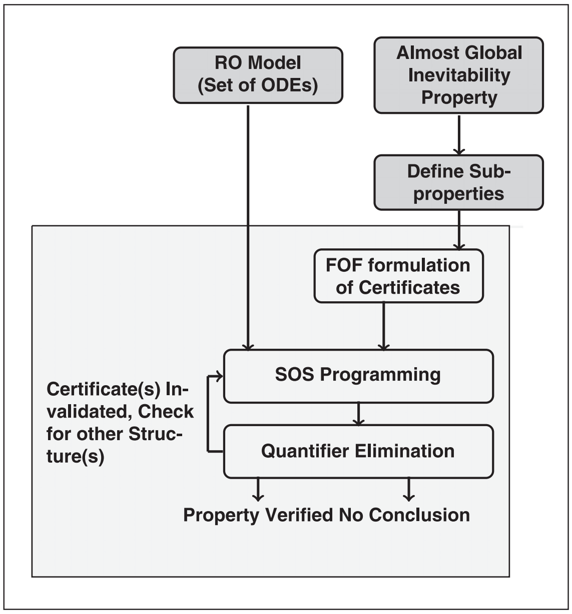

Figure 4. AGI property verification methodology.

eventuality to verify different subproperties. For illustration purposes, here we have depicted the positivity/negativity of the AI certificate in the set $\mathcal{S}1$. The existence of these certificates is formulated as verification of FOFs with universal–existential quantifiers over real polynomials. Verification of these FOFs is carried out using a numeric–symbolic technique of SOS programming and QE. The overall verification flow is shown in Figure 4. The existential quantification is solved by numerically finding different feasible certificates using SOS programming. To further validate these certificates, for their numerical imprecisions, symbolic analysis (QE) is carried out for each of the universally quantified formula. If a certificate is invalidated by the QE stage, a new search is made for a certificate(s) with a different structure this time. The output of our methodology results in either the AGI property being verified, or with no conclusion about its truthfulness, if a user-defined number of iterations have been exhausted.

Modeling of the ring oscillator

We model the RO shown in Figure 5 as a polynomial continuous dynamical system. Let us denote by x the vector of node voltages at the outputs of inverters. The continuous dynamical system model of an RO is a tuple $(\mathbf{X}, \mathcal{X}_{\text{initial}}, \mathbf{U}, f)$ where $\mathbf{X}$ is a set of state variables interpreted over $\mathbb{R}$, $\mathcal{X} = \mathbb{R}^{\mathbf{X}}$ is the set of all possible valuations of the variables, $\mathcal{X}_{\text{initial}} \subset \mathcal{X}$ is the set of initial conditions, $\mathbf{U}$ is the set of parameters (to model circuit capacitance, resistance, transistor parameters) interpreted over $\mathbb{R}$ with $U = \mathbb{R}^{\mathbf{U}}$ being the set of all possible parameter valuations, and

$$f : \mathcal{X} \times \mathcal{U} \to \mathcal{X} \tag{1}$$

the vector field characterizing the system. We assume that the vector field f is a polynomial function of $x \in \mathcal{X}$ called a polynomial vector field. Let us denote by $\Phi(x_0, t)$ the solution of equation $((d\Phi(X(t)))/dt) = f(\mathcal{X}, \mathcal{U}), X(0) = x_0 \in \mathcal{X}_{\text{init}}$.

Definition 1 (Equilibrium State). A state $x_e \in \mathcal{X}$ is called an equilibrium of the RO, iff $f(x_e) = 0$.

Definition 2 (Attractive Invariance of a Set). A set $\mathcal{X}_I$ is invariant iff $\forall x_0 : x_0 \in \mathcal{X}_I$, $\Phi(x_0, t) \in \mathcal{X}_I$ for all t. It is called attractive invariant (AI) iff $\forall x_0 : x_0 \in \mathcal{X} \setminus \mathcal{X}_I$, $\lim_{t \to b} \Phi(x_0, t)\mathcal{X}_I, b \in \mathbb{R}_{\geq 0}$.

Definition 3 (Limit Cycle). A set $\gamma \subset \mathcal{X}$ is called a limit cycle, iff $\forall x_0 : x_0 \in \gamma, \Phi(x_0, T) = x_0$ for $T > 0$, and for all $0 < t < T$, $\Phi(x_0, t) \neq x_0$. This is an invariant set.

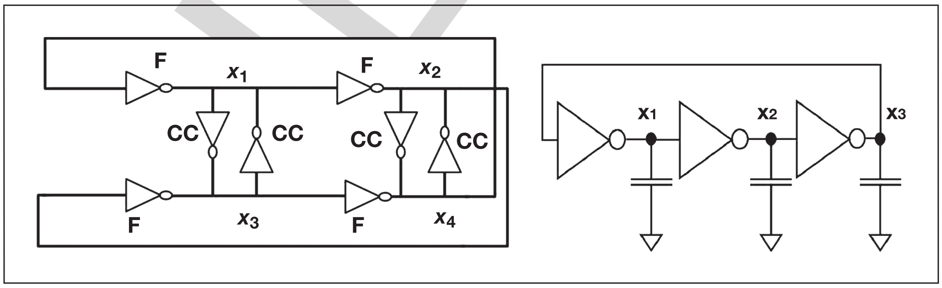

Figure 5. Two different topologies of ring oscillators. Left: Even stage RO. Right: Odd stage RO.

Definition 4 (Inevitability of the Limit Cycle). The limit cycle γ is said to be inevitable, iff $\forall x_0 : x_0 \in \mathcal{X}_{\text{initial}}, y \in \gamma, r > 0$, $b \in \mathbb{R}_{\geq 0}$

$$\lim_{t \to b} \|\Phi(x_0, t) - y\| \leq r. \tag{2}$$

Assumption 1. In this work, we assume that the location of γ in the state space is known.

For a practically feasible RO, there are states in $\mathbb{R}^n$ from where it fails to start and reaches the limit cycle γ [1]. For example, equilibrium is one such state from where an RO cannot start. We call the set of all such states the "dead set."

Definition 5 (Dead Set). A set of states is called a dead set denoted by $\mathcal{X}_{\text{dead}}$, such that $\forall x_0 : x_0 \in \mathcal{X}_{\text{dead}}$, $\lim_{t\to\infty} \|\Phi(x_0, t) - x_e\| = 0$. Here x_e is an equilibrium state.

Definition 6 (AGI of Oscillation in RO). The limit cycle $\gamma \subset \mathcal{X}$ is said to be "almost globally inevitable," iff $\forall x_0 : x_0 \in \{\mathcal{X} \setminus \mathcal{X}_{\text{dead}}\}, y \in \gamma, r > 0, b \in \mathbb{R}_{\geq 0}$

$$\lim_{t\to b} \|\Phi(x_0, t) - y\| \leq r. \tag{3}$$

In this paper, we consider two different topologies of ROs, i.e., the odd stage and the even stage RO as depicted in Figure 5. While we treat each individual node voltage as a state variable for the odd stage RO, we use the strategy suggested in [1] for the even stage RO, and divide its operation into differential and common modes. We denote the node voltages of the even stage RO by $x(0,j)$ and $x(1,j)$ for $j = 0, 1, \ldots, n-1$. Here n is the number of stages. For the even stage RO in Figure 5, $x(0,0) = \mathcal{X}_1, x(0,1) = \mathcal{X}_2, x(1,0) = \mathcal{X}_3, x(1,1) = \mathcal{X}_4$. The voltages $x(0,j)$ and $x(1,j)$ form the differential pair whose differential component is $x(0,j) - x(1,j)$, and the common mode component is $x(0,j) + x(1,j)$. The even stage RO, while operating normally, has its oscillation manifested in the differential mode, whereas the common mode settles to the constant zero value. If we assume that inverters are identical, then, $\forall j : j \in [0, n-1], \forall x : x \in \mathcal{X}$ such that $x(0,j) = x(1,j)$, we have $\Phi(x, t) = x_e$ as $t \to \infty$. This means that the set $\{x(0,j) = x(1,j), \forall j : j \in [0, n-1]\} \in \mathcal{X}_{\text{dead}}$. Similarly, for odd stage RO, if $x_1 = x_2 = x_3$, then $\lim_{t\to\infty} \Phi(x, t) = x_e$.

RO properties verification using Lyapunov-like certificates

To verify the AGI of the limit cycle γ, we use several Lyapunov-like certificates in different subsets of the state space of the RO, Figure 3. To show attractive invariance of a set, a Lyapunov-like certificate has been presented in [8].

Lemma 1. If there exist a polynomial with real coefficients $V : \mathcal{X} \to \mathbb{R}$, $\epsilon > 0$ and a minimum $\eta > 0$ such that

1) $V(x) > 0, \forall x \in \mathbb{R}^n \setminus 0$;
2) $\{V(x) = 1\} \subseteq \{q(x) \leq \eta\}$;
3) $\{V(x) \geq 1\} \subseteq \{(\partial V/\partial x)(x).f(x,u) \leq \epsilon\}$;

then the set $\mathcal{S}2 := \{V(x) \leq 1\}$ is an AI set for an RO with a vector field given in (1), and it is contained in the set $\{q(x) \leq \eta\}$ where $q : \mathcal{X} \to \mathbb{R}$.

Proof. See [8]. □

In the above Lemma 1, the set $\{q(x) = \eta\}$ is used for optimization purposes and the parameter η is minimized so that this set contains the desired AI set $\mathcal{S}2 := \{V(x) \leq 1\}$. Inside the AI set $\mathcal{S}2$, trajectories can reach either the dead set $\mathcal{X}_{\text{dead}}$ or to within a small distance of the limit cycle γ (shown in dotted red in Figure 3). Let us define a set $\mathcal{B}_r = V(x) \leq r$, $0 < r < 1$ (shown in magenta in Figure 3). To show that trajectories starting in the set $\mathcal{B}_r$ are not trapped in the dead set $\mathcal{X}_{\text{dead}}$, and eventually escape to the set $\mathcal{S}2 \setminus \mathcal{B}_r$, we introduce an escape certificate.

Lemma 2. For a compact set $\mathcal{B}_r \subset \mathcal{S}2$, if there is a differentiable escape certificate, $\mathcal{E} : \mathcal{X} \to \mathbb{R}$, such that:

1) $\mathcal{E}(x) = 0 \ \forall x : x \in \mathcal{X}_{\text{dead}}$;
2) $\mathcal{E}(x) > 0 \ \forall x : x \in \mathcal{B}_r \setminus \mathcal{X}_{\text{dead}}$;
3) $(\partial\mathcal{E}/\partial x)(x).f(x,u) > 0 \ \forall x : x \in \mathcal{B}_r \setminus \mathcal{X}_{\text{dead}}$;

then $\forall x : x \in \{\mathcal{B}_r \setminus \mathcal{X}_{\text{dead}}\}, \lim_{t\to\infty} x(t) \notin \mathcal{B}_r$.

Proof. See [4, Ch. 4]. □

To show that trajectories in the set $\mathcal{S}2 \setminus \mathcal{B}_r$ eventually reach to within a close distance of the limit cycle γ, we use the eventuality certificate presented in [9]. Let us have a set $\mathcal{X}_{\text{LC}}$, such that $\|y - x\| \leq \alpha, \forall x \in \mathcal{X}_{\text{LC}}, y \in \gamma, \alpha > 0$.

Theorem 1. If there exists a differentiable certificate of eventuality $E : \mathcal{X} \to \mathbb{R}$ satisfying the following conditions:

1) $E(x) \leq 0 \ \forall x \in (\mathcal{S}2 \setminus \mathcal{B}_r) \setminus \mathcal{X}_{\text{dead}}$;
2) $E(x) > 0 \ \forall x \in Cl(\partial\mathcal{S}2 \setminus \partial\mathcal{X}_{\text{LC}})$;
3) $(\partial E/\partial x)(x).f(x,u) < 0 \ \forall x \in Cl(\mathcal{S}2 \setminus \mathcal{X}_{\text{LC}})$;

then for all initial conditions $x_0 \in \mathcal{S}2 \setminus \mathcal{B}_r$, the trajectory $x(t)$ satisfies $x(T) \in \mathcal{X}_{\text{LC}}$, for some $T \geq 0$ and for all $t \in [0, T]$, $x(t) \in X$. Here Cl and ∂ denote closure and boundary of a closed set, respectively.

Proof. See [9]. □

For the common mode of the even stage RO, we further show that common mode voltages settle down to zero in the steady state. We verify this using the Lyapunov certificate restated for the common mode in Theorem 2.

Theorem 2. For the continuous dynamical system with a vector field given in (1), and with the state vector replaced by $x = \{x(0,0) + x(1,0), x(0,1) + x(1,1), \ldots, x(0, n-1) + x(1, n-1)\}$, let us assume an invariant set $\mathcal{X}_{\text{com}}$, which we call the common-mode state space. Note that this set is invariant due to the fact that node voltages are bounded by the supply voltage. If there exists a Lyapunov certificate $\mathcal{L} : \mathcal{X} \to \mathbb{R}$ such that

$$\mathcal{L}(x) > 0,\ \forall x \in \{\mathcal{X}_{\text{com}} \setminus \{0\}\}, \mathcal{L}(0) = 0 \quad (4)$$

$$\frac{\partial L}{\partial x}(x).f(x,u) < 0,\ \forall x \in \{\mathcal{X}_{\text{com}} \setminus \{0\}\} \quad (5)$$

then the set $\{x = 0\}$ is asymptotically stable, and $\forall x \in \mathcal{X}_{\text{com}}$, $\lim_{t\to\infty} \Phi(x,t) = 0$.

Proof. Similar to [4]. □

SOS programming and QE

We formulate our verification methodology as a conjunction of several FOFs having polynomial equations, inequalities, quantifiers $\{\forall, \exists\}$ and boolean operators $\{\wedge, \vee, \neg, \rightarrow, \text{etc.}\}$. There are algorithms that can, in principle, generate quantifier-free formulas from a universal–existential quantified FOF over the real fields (see [6] and the references therein). However, they are complex and only work for small academic problems. Showing positivity of a real polynomial, SOS uses a sufficient but incomplete criterion of establishing the decomposition of the polynomial into a sum of squares of polynomials [10]. A sufficient condition for a multivariate polynomial $p(x)$ to be nonnegative everywhere is that it can be decomposed as a sum of squares of polynomials, i.e., $p(x) = \sum_{i=1}^{m} p_i^2(x), p_i(x) \in \mathcal{R}_n$. We denote the set of polynomials in n variables with real coefficients by $\mathcal{P}_n$. A subset of this set is the set of SOS polynomials in n variables denoted by $\mathcal{S}_n$.

Verification of AGI of oscillation in RO

Formulation of the verification problem

We formulate the verification of the AGI property as the conjunction of different subproperties, corresponding to the three subfigures in Figure 3, defined below.

Property 1. $\forall x(0) : x(0) \in \mathcal{S}1, \lim_{t\to b} x(t) \in \mathcal{S}2$, $b \in \mathbb{R}_{\geq 0}$.

Property 2. $\forall x(0) : x(0) \in \mathcal{B}_r, \lim_{t\to\infty}(x(t) \notin \mathcal{X}_{\text{dead}} \wedge x(t) \in \mathcal{S}2 \setminus \mathcal{B}_r)$.

Property 3. $\forall x(0) : x(0) \in \mathcal{S}2 \setminus \mathcal{B}_r, \lim_{t\to b} \|y - x(t)\| \leq \alpha, y \in \gamma, b \in \mathbb{R}_{\geq 0}, \alpha > 0$.

We define a fourth property characterizing the common mode behavior of the even stage RO in the invariant set $\mathcal{X}_{\text{com}}$.

Property 4. $\forall x(0) : x(0) \in \mathcal{X}_{\text{com}}, \lim_{t\to\infty} x(t) = 0$.

If we denote the almost global inevitability property by φ, Property 1 by $\varphi 1$, Property 2 by $\varphi 2$, Property 3 by $\varphi 3$, and Property 4 by $\varphi 4$, then $\varphi = \varphi 1 \wedge \varphi 2 \wedge \varphi 3$, for the odd stage RO, and, $\varphi = \varphi 1 \wedge \varphi 2 \wedge \varphi 3 \wedge \varphi 4$, for the even stage RO. A trajectory $x(t)$ of the odd stage RO satisfies φ, iff it satisfies $\varphi 1$ in $\mathcal{S}1$, $\varphi 2$ in $\mathcal{B}_r$, and $\varphi 3$ in $\mathcal{S}2 \setminus \mathcal{B}_r$, i.e., $\forall x : x \in \mathcal{X}, x \models \varphi \Longleftrightarrow (x \models \varphi 1\, \forall x : x \in \mathcal{S}1) \wedge (x \models \varphi 2\, \forall x : x \in \mathcal{S}2) \wedge (x \models \varphi 3\, \forall x : x \in \mathcal{S}2 \setminus \mathcal{B}_r)$.

Similarly, for en even stage RO, $\forall x : x \in \mathcal{X}, x \models \varphi \Longleftrightarrow (x \models \varphi 1\, \forall x : x \in \mathcal{S}1) \wedge (x \models \varphi 2\, \forall x : x \in \mathcal{B}_r) \wedge (x \models \varphi 3\, \forall x : x \in \mathcal{S}2 \setminus \mathcal{B}_r) \wedge (x \models \varphi 4\, \forall x : x \in \mathcal{X}_{\text{com}})$.

SOS-QE approach to verify AGI of oscillation

Here we present the formalization and verification of Property 1 using a SOS-QE approach and a similar approach is used for the verification of other subproperties. We define the conditions of Lemma 1 by the following FOF:

$$\psi_0 := \exists p^{\mathcal{P}} : \psi_1$$
$$\psi_1 := \forall x^{\mathcal{X}} : \psi_2$$
$$\psi_2 := \Bigg((x \neq 0 \Longrightarrow V(p,x) > 0)$$
$$\wedge \left\{ (1 - V(p,x) \geq 0) \Longrightarrow (\eta - q(x)) \geq 0 \right\}$$
$$\wedge \left\{ (V(p,x) - 1 \geq 0) \Longrightarrow \left(\frac{\partial V}{\partial x}(p,x).f(x,u) \leq -\epsilon \right) \right\} \Bigg).$$

Here $p \in \mathcal{P}$ represents the coefficients space of the certificate V. A sufficient condition for the verification of property $\varphi 1$ is stated in the following theorem.

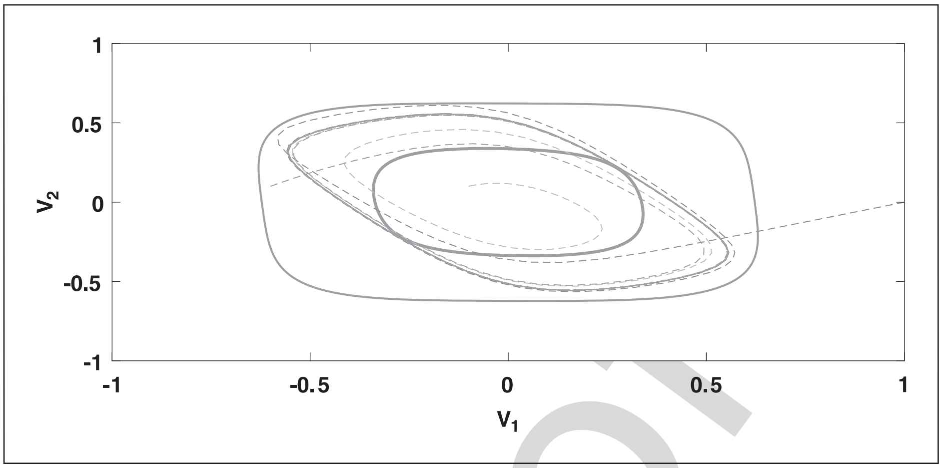

Figure 6. Odd RO AI set $\{r <= V <= 1\}$: Annular region between solid green plots, trajectories: dashed plots.

Theorem 3. If there is a feasible certificate $V(x)$, fulfilling the conditions in Lemma. 1, then $(x \models \psi_0 \Longleftrightarrow x \models \varphi 1), \forall x(0) \in \mathcal{S}1$, and $\mathcal{S}2 = V(x) \leq 1$.

Following the sufficiency conditions in Theorem 3, we verify $\varphi 1$ using the mixed SOS-QE approach. We start with a SOS program searching for the AI certificate $V(x)$ such that it satisfies the conditions in Lemma. 1. Note that every condition on $V(x)$ in Lemma 1 is a positivity/negativity condition which can be formulated as a SOS condition. Furthermore, we need these conditions to be satisfied in different sets which are encoded using a sound mathematical technique called the S-procedure [10]. A SOS program incorporating these conditions is given as follows:

$$\begin{aligned} &\text{minimize} \quad \eta \\ &\text{subject to} \end{aligned}$$

(i) $V(0) = 0$
(ii) $(V(x) - \epsilon - \sum_{k=1}^{n} s_1^k(x) g_k(x)) \in \mathcal{S}_n$
(iii) $(\eta - q(x)) - s_2(x)(1 - V(x)) \in \mathcal{S}_n$
(iv) $((-\epsilon - (\partial V/\partial)(x).f(x,u)) - s_3(x)(V(x) - 1) - \sum_{k=1}^{n} s_4^k(x) g_k(x) - \sum_{j=1}^{m} s_5^j(x)\, a_j(u)) \in \mathcal{S}_n$, $\forall x \in \mathcal{X}, \{s_1^k, s_2, s_3, s_4^k, s_5^j\}\ \mathcal{S}_n, \forall k \in \{1,\ldots,n\}, \forall j \in \{1,\ldots,m\}, \epsilon > 0, \eta > 0.$

Here $V(x)$, $s_1^k, s_2, s_3, s_4^k, s_5^j$, are polynomials of degree d.

In this SOS program, constraint (ii) enforces positive definiteness on the certificate $V(x)$ by introducing a small positive number ϵ. This constraint has to be satisfied in the state space $\mathcal{X}$ defined as $\mathcal{X} = \{x \in \mathbb{R}^n : g_k(x) \geq 0, \text{for } k \in \{1,\ldots,n\}\}$. Constraint (iii) ensures that $\{V(x) \leq 1\} \subseteq \{q(x) \leq \eta\}$. Constraint (iv) incorporates the set inclusion $\{V(x) \geq 1\} \subseteq \{\partial V/\partial x.f(x,u) \leq \epsilon\}$. This constraint also ensures that parameters u belong to the set $\{a_j(u) \geq 0,\ \text{for } j \in \{1,\ldots,m\}$. The above SOS program, if feasible, returns a certificate of attractive invariance $V(x)$ with its parameters $p \in \mathcal{P}$ fixed within a limited numerical precision. We further verify the validity of this certificate using symbolic QE. Note that in QE, coefficients are represented in $\mathbb{Q}^n$. Using QE, we check the truth value of the negation of the formula ψ_1, since the existential quantifier has already been eliminated by the SOS program. On refutation of $\neg\psi_1$, we conclude $(x \models \varphi 1 \Longleftrightarrow x \models \psi_0), \forall x \in \mathcal{S}1$. If either the SOS program is infeasible for a certificate $V(x)$, or the QE tool returns a true valuation for the formula $\neg\psi 1$, we repeat the process by increasing the degree of the certificate $V(x)$. If we still cannot get the desired certificate, we conclude inconclusiveness about the truth value of $\varphi 1$.

Experimental evaluation

We used a degree-7 least-square polynomial model characterizing the input–output nonlinear

Table 1 Odd RO inevitability verification time.

Certificate	YALMIP-SOS Time (Sec)	REDLOG-QE Time (Sec)
Attractive Invariants	824.8 (Degree 4)	Clause 1 = 0.219 Clause 2 = 0.047 Clause 3 = 8.222
Escape	6.3 (Degree 2)	Clause 1 = 0.060 Clause 2 = 0.026 Clause 3 = 0.320
Eventuality	31.5 (Degree 4)	Clause 1 = 0.070 Clause 2 = 0.025 Clause 3 = 0.636

Table 2 Even RO inevitability verification time.

Certificate	YALMIP-SOS Time (Sec)	REDLOG-QE Time (Sec)
Attractive Invariants	6127.6 (Degree 10)	Clause 1 = 5.24 Clause 2 = 0.33 Clause 3 = 1.56
Escape	320.6757 (Degree 4)	Clause 1 = 0.01 Clause 2 = 0.30 Clause 3 = 2.50
Eventuality	4128.8 (Degree 6)	Clause 1 = 0.349 Clause 2 = 0.300 Clause 3 = 0.615
Lyapunov	55.24 (Degree 4)	Clause 1 = 0.02 Clause 2 = 0.75 Clause 3 = 0.57

behavior of an inverter. We obtained this approximation of the inverter model by running MATLAB simulation using the Schichman–Hodges MOS transistor models. Note that, in this model, we take into account the effect of transistor widths/lengths on the slope of the inverter output. We used YALMIP [11] solver within MATLAB for SOS programming, and REDLOG [12], for QE on a 2.6-GHZ Intel Core i5 machine with 4 GB of memory. For an odd RO, we were able to compute a degree-4 AI certificate. The AI set, marked by the level set $V(x) \leq 1$, is shown in Figure 6. Inside the AI set, we showed trajectories escape the set $V \leq r$, by computing a degree-2 escape certificate. Similarly, the convergence of the trajectories to within a small distance of the limit cycle has been shown by computing a degree-4 eventuality certificate in the set $\{V \leq 1 \wedge V \geq r\}$. Time taken by the SOS solver to compute these certificates is listed in the second column of Table 1. Verification of these certificates in REDLOG, given its ability of how large a formula it can handle, has been divided into the verification of the individual clauses of the FOFs benefiting from its disjunctive normal form (DNF). Since we were interested in the negation of FOFs in the DNF, we verified whether each clause was "false." The verification times of the QE are listed in the third column of Table 1. For AI and escape certificates, REDLOG successfully verified the negation of their universally quantified FOFs. A timeout was reported by the REDLOG tool for all clauses of the eventuality FOF of the odd RO. The reason for these timeouts is the set, an intersection of two level curves of the AI certificate, that puts an additional burden on the solver resulting in its timeout. To overcome this issue, we instead conservatively over-underapproximate the set $\{V \leq 1 \wedge V \geq r\}$, by a quadratic polynomial, and construct the eventuality certificate for this new set. This solved our problem and REDLOG has been able to verify the eventuality certificate in this conservative approximation of the set $\{V \leq 1 \wedge V \geq r\}$. Note that this conservatism is to approximate the annular set $\{V \leq 1 \wedge V \geq r\}$ and does not add to the overall conservatism of our methodology.

Similarly, for the even stage RO, we computed a degree-10 AI, a degree-4 escape, a degree-6 eventuality, and a degree-4 Lyapunov certificate. Computation times are given in Table 2 and the AI set is shown in Figure 7.

Though verifying the property, using SOS-QE approach, needs user input, it offers a comparable computation time to [1]. Yan et al. have reported approximately 22000 s for the complete verification of the even stage RO, whereas our accumulative time for the even stage RO is approximately 6500 s. Even if we add the time of all the instances for which we received an infeasible certificate, our computation time is still not more than half of what has been reported in [1]. This is in addition to our methodology being less conservative and applicable to an infinite horizon.

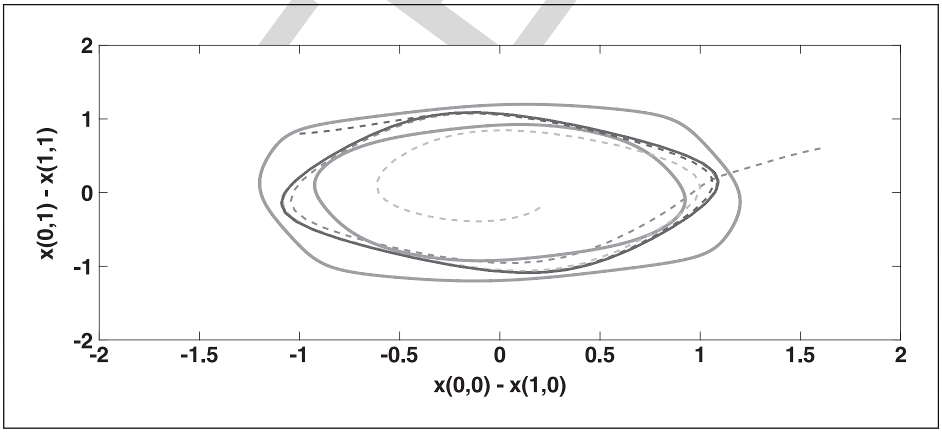

Figure 7. Even RO AI set $\{r <= V <= 1\}$: Annular region between solid green plot, trajectories: dashed.

Results show the effectiveness of our approach to verifying the complex AGI property of a real-world analog circuit. We have verified the AGI using the Lyapunov-based deductive method which is not only applicable to infinite time, but also avoids explicitly solving ODEs and is thus less conservative than the reachability approaches. ■

■ References

[1] C. Yan, M. R. Greenstreet, and S. Yang, "Verifying global start-up for a Möbius ring-oscillator," *Formal Methods Syst. Design*, vol. 45, no. 2, pp. 246–272, 2014.

[2] K. D. Jones, J. Kim, and V. Konrad, "Some real world problems in the analog and mixed signal domains," in *Designing Correct Circuits*, 2008.

[3] M. H. Zaki, S. Tahar, and G. Bois, "Formal verification of analog and mixed signal designs: A survey," *Microelectron. J.*, vol. 39, no. 12, pp. 1395–1404, 2008.

[4] H. K. Khalil, *Nonlinear Systems*, 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.

[5] H. Ichihara and H. Anai, "An SOS-QE approach to nonlinear gain analysis for polynomial dynamical systems," *Math. Comput. Sci.*, vol. 5, no. 3, pp. 303–314, 2011.

[6] J. Harrison, "Verifying nonlinear real formulas via sums of squares," in *Theorem Proving in Higher Order Logics*, vol. 4732, Lecture Notes in Computer Science, pp. 102–118, Berlin, Germany: Springer-Verlag, 2007.

[7] H. Asad and K. D. Jones, "Verifying inevitability of phase-locking in a charge pump phase lock loop using sum of squares programming," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf.*, 2015, pp. 295–300.

[8] W. Tan, "Nonlinear control analysis and synthesis using sum-of-squares programming," PhD dissertation, Univ. California Berkeley, Berkeley, CA, USA, 2006.

[9] S. Prajna and A. Rantzer, "Convex programs for temporal verification of nonlinear dynamical systems," *SIAM J. Control Optim.*, vol. 46, no. 3, pp. 999–1021, 2007.

[10] S. Prajna and A. Papachristodoulou, "Analysis of switched and hybrid systems-beyond piecewise quadratic methods," in *Proc. Amer. Control Conf.*, vol. 4, 2003, pp. 2779–2784.

[11] J. Lofberg, "Yalmip: A toolbox for modeling and optimization in matlab," in *Proc. IEEE Int. Symp. Comput. Aided Control Syst. Design*, 2004, pp. 284–289.

[12] A. Dolzmann and T. Sturm, "Redlog: Computer algebra meets computer logic," *ACM SIGSAM Bull.*, vol. 31, no. 2, pp. 2–9, 1997.

Hafiz ul Asad is a Research Assistant at the Center for Software Reliability, City University London, London, U.K. His research interests include hardware verification, dynamical systems, and formal methods. ul Asad has a PhD in electrical engineering from City University London.

Kevin D. Jones is the Executive Dean at the Faculty of Science and Engineering, University of Plymouth, Plymouth, U.K. His research interests include hardware verification, formal methods, and cyber security. Jones has a PhD in computing science from Manchester, Manchester, U.K. He is a Senior Member of the IEEE, and a Fellow of IET and BCS. AQ1

■ Direct questions and comments about this article to Hafiz ul Asad, City University London, EC1V 0HB London U.K.; hafiz.ul-asad.1@city.ac.uk.

AUTHOR QUERY

AUTHOR PLEASE ANSWER QUERY

AQ1 = Please define IET and BCS.

END OF QUERY