

Fast Reliability Ranking of Matchstick Minimal Networks

Vlad-Florin Drăgoi, and Valeriu Beiu, *Senior Member, IEEE*

Abstract

In this article, we take a closer look at the reliability of large minimal networks constructed by repeated compositions of the simplest possible networks. For a given number of devices $n = 2^m$ we define the set of all the possible compositions of series and parallel networks of two devices. We then define several partial orders over this set and study their properties. As far as we know the ranking problem has not been addressed before in this context, and this article establishes the first results in this direction. The usual approach when dealing with reliability of two-terminal networks is to determine existence or non-existence of uniformly most reliable networks. The problem of ranking two-terminal networks is thus more complex, but by restricting our study to the set of compositions we manage to determine and demonstrate the existence of a poset.

Index Terms

Heaviside most reliable, minimal two-terminal network, poset of compositions, reliability polynomial, uniformly most reliable.

I. INTRODUCTION

One well-known problem in information processing is that of identifying schemes that would allow maximizing reliability, while keeping resources bounded (redundancy factors). Obviously, the design-for-reliability problem becomes more challenging as the system grows larger and is required to function without interruptions for longer times. Another aspect is that enhancing/maximizing reliability should be done with a limited amount of additional (redundant) components. The number of components is the simplest and most obvious cost function, but other cost functions (also known as *figures-of-merit*, or FoMs) have been proposed and used, e.g., the number of wires. It follows that *design-for-reliability* is a constraint optimization problem: *maximize system reliability given limited resources*. The problem permeates way beyond computers into most man-made systems, while nature also relies on reliability principles/schemes at different levels (an example here being the human brain, having 10^{11} neurons interconnected by 10^{15} synapses, working over many years).

In the following we shall restrict the scope of our discussions to computers. In this context, reliability was established by John von Neumann [1]. The focus was on how one could design reliable circuits/computers using unreliable logic gates. The schemes proposed have replicated gates followed by voting and/or multiplexing, and led to regular and repetitive building blocks. Another take on this topic was put forward by Edward F. Moore and Claude E. Shannon [2], [3]. The major difference was that instead of starting from gates, Moore and Shannon decided to pursue their analysis starting from relays (switching devices). Their results were much more encouraging than [1].

In this article, we analyze particular solutions for designing reliable and regular networks. One of the main motivations is that regular networks bode well with novel array-based designs, e.g., FinFETs [4], vertical FET, gate-all-around FET, and arrays of beyond CMOS devices [5]. These can be extrapolated to wireless sensor networks, vehicular/mobile ad hoc networks, and Internet of Things [6], [7]. The solution we are advocating here for growing larger and more reliable networks is by *combining smaller networks through compositions*. The basic building blocks we are going to use here are the smallest networks connected in series and in parallel. One of the main advantages of using series and parallel networks is that they are very easy to evaluate (as their reliability polynomials are easier to compute [8]), while compositions of series and parallel networks are inheriting this benefit.

a) Related work: Moore and Shannon were the first to propose the technique of “composition” for building complex networks [2]. They proved that when a network is composed with itself k times the resulting network is *significantly more reliable*. When k tends to infinity the reliability of the repeated compositions approaches a Heaviside step function θ .

Lately, compositions of series and parallel [9], as well as compositions of hammocks [10] were advocated and evaluated. The results reported in [9] are promising for several reasons.

Firstly, the reliability polynomials are efficiently computable (for compositions of series and parallel). Secondly, there are series and parallel compositions which are comparable to hammocks (with respect to several different metrics for reliability), and thirdly the reliability polynomials of compositions have compact forms and are sparser than the ones for hammocks.

One of the open questions stated in [9] was: *What is the most reliable composition given a fixed number of devices?* The trivial solution, which is the worst case scenario, is to generate all compositions of a given size n , to compute all the associated

V. Drăgoi is with the Faculty of Exact Sciences, “Aurel Vlaicu” University of Arad, 2-4 Elena Dragoi Str., 310330 Arad, Romania, and with Normandie Univ, France; UR, LITIS, F-76821 Mont-Saint-Aignan, France.

V. Beiu is with the Faculty of Exact Sciences, “Aurel Vlaicu” University of Arad, 2-4 Elena Dragoi Str., 310330 Arad, Romania.

reliability polynomials, and to compare them (by means of different FoMs). Here our aim is to give a non-trivial solution to this question by studying the relationships between compositions of series and parallel networks. For doing this we introduce several partial orders over the set of all compositions.

Recently, ordering the reliability polynomials of series and parallel compositions was investigated in [11] using simulations. Here, while tackling the same type of problems, we are advancing the theoretical foundation for explaining the simulation results of [11]. In particular, the main contributions of this article are:

- 1) We give here a theoretical tool based on poset theory, in order to mathematically explain and prove the existence of an ordering relation over the set of reliability polynomials of compositions of series and parallel.
- 2) We introduce a matrix representation for a particular class of networks (introduced by Moore and Shannon in [2]), that allows us to determine and prove several structural properties including duality of these networks.
- 3) We use the structure of the poset to answer fundamental questions regarding the reliability of compositions of series and parallel.

b) Application of the poset of compositions: Uniformly most reliable matchstick minimal networks The problem of finding *uniformly most reliable* (UMR) networks or graphs (both terms have been used interchangeably in the literature) is an interesting topic in reliability theory. This property is defined as follows: Among the set of all graphs with ω vertices and n edges, a graph is UMR if its reliability polynomial is greater than the reliability polynomials of all other graphs from the same set, for every $p \in [0, 1]$ (definition from [12], [13]). Many results are known in this sense. For the *all-terminal reliability* problem there are certain conditions for which UMR networks exist [13], [14], [15], [16], and conditions for which UMR networks do not exist [14], [17], [18]. For the *two-terminal reliability* problem even fewer results are known [12], [19].

This article will focus only on a subclass of two-terminal minimal networks known as *matchstick minimal networks* (MMNs), without restriction on the number of vertices ω . Hence, we will say that an MMN made of n edges/devices is UMR if its reliability polynomial is greater than or equal to the reliability polynomials of all MMNs of n edges/devices, for every $p \in [0, 1]$. By studying the properties of our posets we will show that the all-parallel composition network is UMR-MMN.

Heaviside most reliable Reliability as per Moore and Shannon's paper [2] should be understood not only as the connectivity (s, t -connectedness) but also as the non-connectivity (s, t -disconnectedness) of the network, as their networks were intended to replace switching devices (i.e., which have to connect and also to disconnect as needed). Hence, such networks should have their reliability polynomials close to 0 for some interval $[0, p_0)$, and close to 1 for the remaining interval $[p_0, 1]$. This implies that these networks should have their reliability polynomials as close as possible to a shifted Heaviside step function $\theta(p - p_0)$ with p_0 around $1/2$.

That is why, in this paper we define the concept of *Heaviside most reliable* (HMR). More precisely, we will say that an MMN for which the reliability polynomial is smaller than the reliability polynomials of all other MMNs for all $p \in [0, p_0)$, and greater than the reliability polynomials of all other MMNs for $p \in [p_0, 1]$, is HMR-MMN. Notice that the HMR for $p_0 = 0$ is UMR. With respect to this definition, we will prove that there are no HMR-MMNs for any $p_0 \in (0, 1)$.

Complexity of comparing MMNs Another possibly useful application of the results we are going to report here is that, when comparing MMNs by using the structural properties of the posets (i.e., symmetries, rank unimodality, etc.), we are able to reduce the computational complexity. More precisely, we show that results like those in [9] can be obtained by computing the reliability polynomials of a very small number of compositions. This fact brings a significant reduction of the computational complexity.

It is well-known that in general computing the reliability polynomial of a network is #P [20], [21]. Nevertheless, there are several subclasses of two-terminal networks for which this problem becomes tractable, such as particular ladder networks (e.g., Brech-Colbourn, fan, K_3 , K_4 cylinders, etc.). Still, little is known about the complexity of this problem for MMNs. For the moment, we know that this problem can be solved in polynomial time for compositions of series and parallel [9], and for series-parallel networks in general [22]. However, the complexity of computing the reliability polynomials for hammocks is not yet known [23]. That is why this study of posets reveals interesting relationships between MMNs, without computing their associated reliability polynomials.

This article is organized as follows. Section II starts with formal definitions of MMNs. We also define the main concepts, namely compositions of series and parallel, as well as their basic properties. In Section III we present structural properties of compositions, with emphasis on their duality property. Section IV is devoted to posets of reliability polynomials of compositions, while Section V describes the main characteristics of the most promising poset. In Section VI we illustrate two possible applications for UMR-MMNs and HMR-MMNs, before ending the paper with concluding remarks and future directions of research.

II. PRELIMINARIES

A. Minimal two-terminal networks

Definition 1. Let n be a strictly positive integer. We say that N is a two-terminal network of size n if \mathbf{N} is a circuit, made of n identical devices, that has two distinguished contacts/terminals: an input or source S , and an output or terminus T .

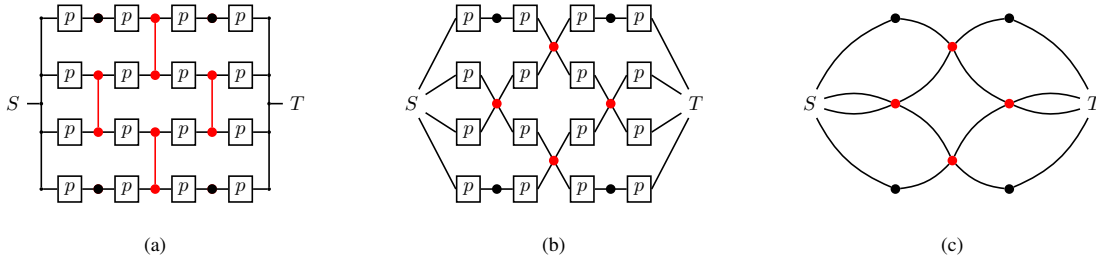


Fig. 1: A particular MMN, the hammock $H_{4,4}$: (a) brick-wall representation [2]; (b) hammock representation [3]; and (c) graph representation [2].

We emphasize that the usual way of defining and studying the reliability of a two-terminal network is by graph theoretical models [24], [25]. Even though our definition might seem different, actually one can map any circuit onto a graph by establishing a bijection between any device of a circuit and the corresponding edge of the graph, see Fig. 1. In this paper we will consider that only devices/edges can fail with independent and identical probability $q = 1 - p$.

Any two-terminal network N can be characterized at least by three parameters: *width* (w), *length* (l), and *size* (n), where w is the size of a “minimal cut” separating S from T ; l is the size of a “minimal path” from S to T ; n is related to l and w as $n \geq wl$ (see Theorem 3 in [2]). If $n = wl$ we say that N is a minimal network.

In the following we will restrict our investigation to a subclass of minimal two-terminal networks, which we are calling MMNs. These should not be confused with matchstick graphs [26], which are different structures from geometric graph theory.

Definition 2. Let w and l be two strictly positive integers. A two-terminal network N is MMN if and only if it can be designed in one of the following two ways. Either start with a parallel-of-series (PoS) of width w and length l (as in Fig. 2 (a)) and place vertical matchsticks (wires) arbitrarily; or start with a series-of-parallel (SoP) of width w and length l (as in Fig. 2 (b)) and remove vertical matchsticks (wires) arbitrarily.

A matchstick is a short wire (red) connecting two vertically adjacent nodes as in Fig. 1 (a). By shrinking the matchsticks in Fig. 1 (a) down to a single node (red) we obtain the “ \times ”-crossing representation shown in Fig. 1 (b).

Definition 3. For any MMN N with $w, l \geq 2$, we define its matchsticks incidence matrix $M_N \in \mathcal{M}_{w-1, l-1}(\{0, 1\})$, as $M_N(i, j) = 1$ if there is a matchstick at position (i, j) and 0 elsewhere.

For example, the four MMNs in Fig. 2 have matchstick incidence matrices

$$M_{PoS} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad M_{SoP} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad M_{H_{4,4}} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad M_{H_{4,4}^+} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Convention 4. The convention that we adopt here is to start indexing the vectors and the matrices with 1, respectively $(1, 1)$. The elements of any set are ordered by lexicographic order, and (when the set contains integers) these are ordered with respect to the natural order on integers.

MMNs with $w = 1$ are called *all-series* and do not admit a matchstick incidence matrix. This fact also holds for *all-parallel* networks, that is to say MMNs with $l = 1$. The set of all MMNs of size $n = wl$ will be denoted \mathcal{N}_n , and we have $\mathcal{N}_n = \bigcup_{w|n} \mathcal{N}_{w, n/w}$ (see [9]).

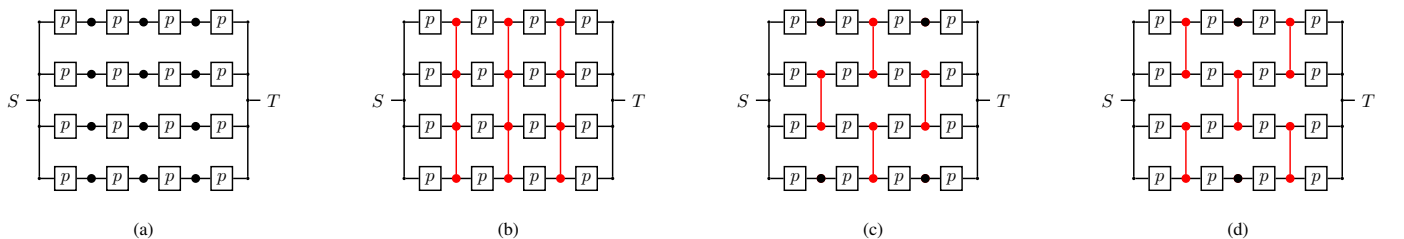


Fig. 2: Four representative MMNs with $w = l = 4$: (a) PoS (no matchsticks); (b) SoP (all possible matchsticks); (c) $H_{4,4}$; and (d) $H_{4,4}^+$.

Lemma 5. For any strictly positive w and l we have

$$|\mathcal{N}_{w,l}| = 2^{(w-1)(l-1)}. \quad (1)$$

Proof. By Definition 3 there is a one-to-one mapping between the set of MMNs of width w and length l and the set of binary matrices $\mathcal{M}_{w-1,l-1}(\{0,1\})$. From this fact the combinatorial result follows. \square

B. Hammocks and compositions of series and parallel

a) *Hammock networks:* MMNs with the well-known ‘‘brick-wall’’ pattern (see Fig. 1 (a)) are known as hammocks [2], [3], [23]. They can be generated starting from PoS [8] (see Fig. 2 (a)). If w and l are both even there are two solutions $\mathbf{H}_{w,l}$ and $\mathbf{H}_{w,l}^+$ (see Figs. 2 (c) and (d)), while otherwise we are left only with $\mathbf{H}_{w,l}$ (out of all the $2^{(w-1)(l-1)}$ MMNs given by eq. (1)).

b) *Compositions of series and parallel:* The composition of two MMNs N_1 and N_2 , denoted $N_1 \bullet N_2$ is obtained by replacing each device in N_1 by a copy of N_2 . In this article, we will consider only compositions where N_1 and N_2 are either two devices in series, or two devices in parallel. In order to be consistent with the existing notations from the literature we will denote two devices in series $C^{(0)}$, and two devices in parallel $C^{(1)}$. We generalize compositions of $C^{(0)}$ and $C^{(1)}$ to any m -length binary vector $\mathbf{u} = (u_1, \dots, u_m) \in \{0,1\}^m$ as

$$C^{\mathbf{u}} = C^{(u_1)} \bullet \dots \bullet C^{(u_m)}. \quad (2)$$

Notation 6. We will employ similar notations as for MMNs, namely, \mathcal{C}_{2^m} is a network from \mathcal{C}_{2^m} , the set of all 2^m -size compositions of $C^{(0)}$ and $C^{(1)}$.

We also remember two well-known concepts, for any binary vector $\mathbf{u} \in \{0,1\}^m$:

- $\text{Supp}(\mathbf{u})$, is the set of all indices corresponding to non-zero entries of \mathbf{u} ;
- $|\mathbf{u}|$ is the Hamming weight, i.e., the number of non-zero components of \mathbf{u} .

Notice that

$$|\mathbf{u}| = \#\text{Supp}(\mathbf{u}). \quad (3)$$

For example, $\mathbf{u} = (1, 1, 0, 1)$ has $\text{Supp}(\mathbf{u}) = \{1, 2, 4\}$ and $|\mathbf{u}| = 3$.

Proposition 7. Let w_1, w_2, l_2 and l_1 be integers strictly larger than 1, and let $N_1 \in \mathcal{N}_{w_1, l_1}$ and $N_2 \in \mathcal{N}_{w_2, l_2}$. Then the composition of N_1 and N_2 is $N = N_1 \bullet N_2 \in \mathcal{N}_{w_1 w_2, l_1 l_2}$, with matchstick incidence matrix

$$M_N = \begin{pmatrix} M_{N_2} & \mathbf{1}_{(w_2-1) \times 1} & \dots & \dots & M_{N_2} & \mathbf{1}_{(w_2-1) \times 1} & M_{N_2} \\ \mathbf{0}_{1 \times (l_2-1)} & M_{N_1}(1, 1) & \dots & \dots & \mathbf{0}_{1 \times (l_2-1)} & M_{N_1}(1, l_1 - 1) & \mathbf{0}_{1 \times (l_2-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{0}_{1 \times (l_2-1)} & M_{N_1}(w_1 - 1, 1) & \dots & \dots & \mathbf{0}_{1 \times (l_2-1)} & M_{N_1}(w_1 - 1, l_1 - 1) & \mathbf{0}_{1 \times (l_2-1)} \\ M_{N_2} & \mathbf{1}_{(w_2-1) \times 1} & \dots & \dots & M_{N_2} & \mathbf{1}_{(w_2-1) \times 1} & M_{N_2} \end{pmatrix}. \quad (4)$$

- When $w_1 = 1$ M_N is obtained as in (4) by tacking only the 1st block rows containing M_{N_2} .
- When $l_1 = 1$ M_N is obtained as in (4) by tacking only the 1st block column containing M_{N_2} .
- When $w_2 = 1$ M_N is obtained as in (4) by deleting the block rows containing M_{N_2} .
- When $l_2 = 1$ M_N is obtained as in (4) by deleting the block column containing M_{N_2} .

Proposition 8 ([9]). Let m be a strictly positive integer and $C^{\mathbf{u}} \in \mathcal{C}_{2^m}$. Then $C^{\mathbf{u}}$ is an MMN of size 2^m , length $l = 2^{m-|\mathbf{u}|}$ and width $w = 2^{|\mathbf{u}|}$. We have

$$\mathcal{C}_{2^m} = \bigcup_{i=0}^m \mathcal{C}_{2^i, 2^{m-i}}.$$

Proposition 9. Let $1 \leq i \leq m$ and $\mathbf{u} = (0^{m-i}, 1^i)$ and $\mathbf{v} = (1^i, 0^{m-i})$. Then $C^{\mathbf{u}}$ is a SoP of $w = 2^i$ and $l = 2^{m-i}$ and $C^{\mathbf{v}}$ is a SoP of $w = 2^i$ and $l = 2^{m-i}$.

III. DUALITY PROPERTIES OF MMNS

A fundamental notion mentioned in [2] is the dual of a network, denoted as N^\perp . In order to give our main theorem for duality we introduce the bitwise complement of a binary matrix $M_N \in \mathcal{M}_{w-1, l-1}(\{0,1\})$ as

$$\overline{M}_N = \mathbf{1}_{(w-1) \times (l-1)} \oplus M_N, \quad (5)$$

where $\mathbf{1}_{l \times w}$ is the all-ones matrix.

Theorem 10. Let N be a $l \times w$ MMN. If $l = 1$ or $w = 1$ then N and N^\perp are the all-parallel and all-series networks. If $w, l \geq 2$ and $M_N \in \mathcal{M}_{w-1, l-1}(\{0, 1\})$ then N^\perp is a $w \times l$ MMN

$$M_{N^\perp} = (\overline{M_N})^t.$$

In order to prove this theorem we will consider any MMN as an electrical circuit where we associate a resistance to each device, and S and T are connected as in Fig. 3. This is a resistor circuit which admits a dual that can be computed using Kirchoff's laws.

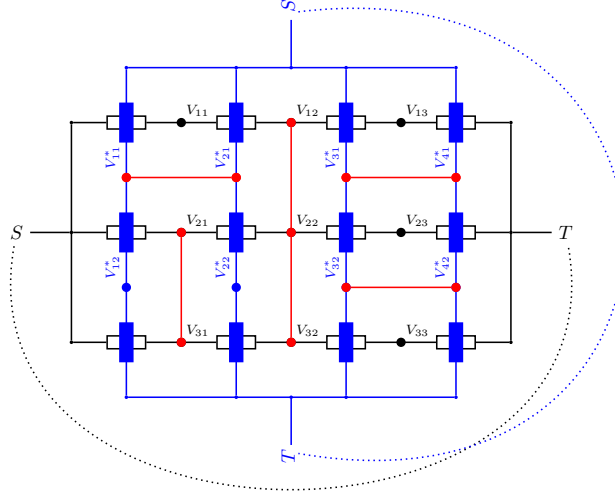


Fig. 3: An MMN (black) with vertical matchsticks (red), and its dual (blue) with horizontal matchsticks (also red).

Proof. Let N be an MMN of width w and length l . If $l = 1$ or $w = 1$ the result is trivial.

Consider that $l, w \geq 2$, i.e., N admits an M_N . A matchstick in N is a node in the electrical circuit and, as nodes become loops in N^\perp , we will show that whenever $M_N(i, j) = 1$ we have $M_{N^\perp}(j, i) = 0$. As loops become nodes in N^\perp , any sequence of zeros in M_N will translate into a sequence of ones in M_{N^\perp} .

Label the interior node of N by $V_{i,j}$ from left to right for j (or from S to T), and from top to bottom for i (see Fig. 3), where $1 \leq i \leq w$ and $1 \leq j \leq l - 1$. Notice that any vertically adjacent devices/resistors belong to a loop. All loops in N will become nodes in N^\perp . We will label these nodes V_{i^*, j^*}^* , where $1 \leq i^* \leq l$ and $1 \leq j^* \leq w - 1$, j^* being counted from top to bottom, and i^* from left to right. Therefore, N^\perp is a network of width l and length w .

For an arbitrary (i, j) suppose that there is a matchstick in N between $V_{i,j}$ and $V_{i+1,j}$, i.e., $M_N(i, j) = 1$. Since a matchstick corresponds to a node, this means that it will become a loop in N^\perp between V_{j^*, i^*}^* and $V_{(j+1)^*, i^*}^*$, i.e., $M_{N^\perp}(j^*, i^*) = 0$. Also, when there is no matchstick in N between $V_{i,j}$ and $V_{i+1,j}$, there is a matchstick in N^\perp between V_{j^*, i^*}^* and $V_{(j+1)^*, i^*}^*$. Since this holds for arbitrary i and j , the proof is concluded. \square

We can now determine the dual of the composition of two MMNs.

Lemma 11. Let N_1 and N_2 be two MMNs. Then we have $(N_1 \bullet N_2)^\perp = N_1^\perp \bullet N_2^\perp$.

This follows from Proposition 7 and Theorem 10.

Proposition 12. Let m be a strictly positive integer and $u \in \{0, 1\}^m$. Then $C^{\bar{u}}$ has width $w = 2^{m-|u|}$, length $l = 2^{|u|}$ and

$$(C^u)^\perp = C^{\bar{u}}. \quad (6)$$

Proof. Follows directly from Lemma 11 and Theorem 10. \square

IV. POSETS OF RELIABILITY

A. Reliability polynomials

The reliability of a two-terminal network is defined as the probability that the source S and the terminus T are connected (also known as s, t -connectness) [25]. A classical convention for the reliability polynomial is to use $\text{Rel}(p)$, where $p \in [0, 1]$ is the probability that a device is closed. Since the reliability polynomial is associated to a network N (H or C in particular), we shall use the notation $\text{Rel}(N; p)$, which gives $\text{Rel}(C; p)$ and $\text{Rel}(H; p)$ for compositions, and respectively hammocks.

Here, we are going to rely on the following form of the reliability polynomial

$$\text{Rel}(\mathbf{N}; p) = \sum_{i=0}^n N_i(\mathbf{N}) p^i (1-p)^{n-i}. \quad (7)$$

The coefficients $N_i(\mathbf{N})$ in eq. (7) are integers satisfying the relation $0 \leq N_i(\mathbf{N}) \leq \binom{n}{i}$ for any n -size network \mathbf{N} (see [25]), and additionally

Proposition 13. *Let \mathbf{N}_1 and \mathbf{N}_2 be arbitrary two-terminal networks of size n . If $N_i(\mathbf{N}_1) \leq N_i(\mathbf{N}_2)$, $\forall 0 \leq i \leq n$ then $\text{Rel}(\mathbf{N}_1; p) \leq \text{Rel}(\mathbf{N}_2; p)$.*

Computing $\text{Rel}(\mathbf{C}; p)$ can be done using the following theorem.

Theorem 14 ([9]). *Let m be a strictly positive integer and $\mathbf{u} = (u_1, \dots, u_m) \in \{0, 1\}^m$. Then:*

$$\text{Rel}(\mathbf{C}^{\mathbf{u}}; p) = \text{Rel}(\mathbf{C}^{(u_1)}) \circ \dots \circ \text{Rel}(\mathbf{C}^{(u_m)}; p), \quad (8)$$

where $\text{Rel}(\mathbf{C}^{(0)}; p) = p^2$ and $\text{Rel}(\mathbf{C}^{(1)}; p) = 1 - (1-p)^2$.

B. Partial orders

Inspired by basic techniques from order theory (see Chapter 3 in [27]) we will define several partial orders for \mathcal{C}_{2^m} . We recall that a *partially ordered set (poset)* is a set with a binary relation, which is *reflexive*, *transitive* and *antisymmetric*. Any pair of elements in a poset are either comparable (i.e., in relation to one another), or incomparable. In this subsection we will define several order relations for the set of compositions. For the relations that we define here it is straightforward to check reflexivity, transitivity and antisymmetry. When comparing two MMNs we say that \mathbf{N}_1 is *more reliable* than \mathbf{N}_2 if

$$\forall 0 \leq p \leq 1 \quad \text{Rel}(\mathbf{N}_2; p) \leq \text{Rel}(\mathbf{N}_1; p). \quad (9)$$

Using this convention we say that $\mathbf{C}^{\mathbf{u}}$ and $\mathbf{C}^{\mathbf{v}}$ are comparable, and simply write $\mathbf{u} \leq \mathbf{v}$ or $\mathbf{v} \leq \mathbf{u}$ if and only if for any $p \in [0, 1]$ we have either $\text{Rel}(\mathbf{C}^{\mathbf{u}}; p) \leq \text{Rel}(\mathbf{C}^{\mathbf{v}}; p)$ or $\text{Rel}(\mathbf{C}^{\mathbf{v}}; p) \leq \text{Rel}(\mathbf{C}^{\mathbf{u}}; p)$, i.e.,

$$\mathbf{u} \leq \mathbf{v} \Leftrightarrow \text{Rel}(\mathbf{C}^{\mathbf{u}}) \leq \text{Rel}(\mathbf{C}^{\mathbf{v}}). \quad (10)$$

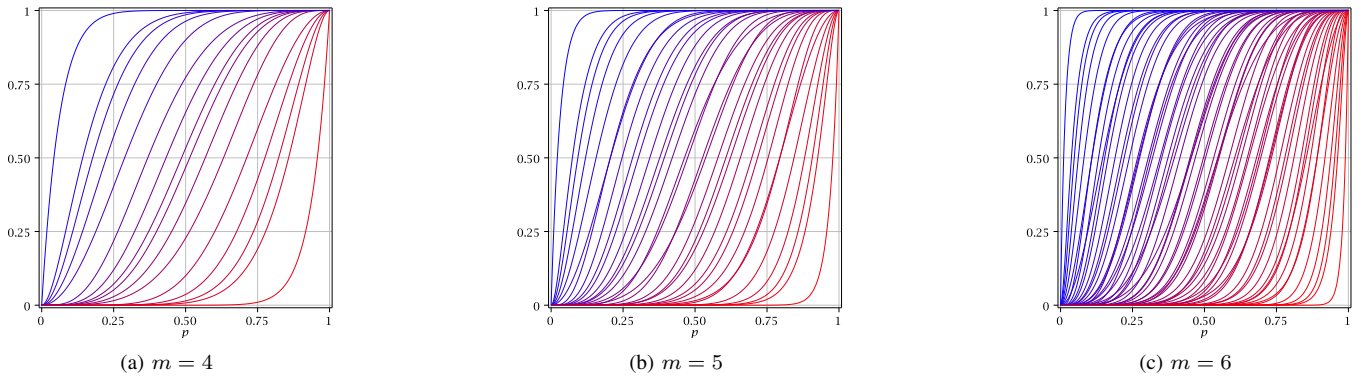


Fig. 4: Reliability polynomials for all compositions in \mathcal{C}_{2^m} .

1) Preliminary simulations: Our simulations have shown that the poset induced by the order given by eq. (10) does not look like any known poset. Moreover, there is no trivial algebraic relation over the set of binary vectors that obeys the aforementioned order. Figs. 4a and 4b plot the reliability polynomials for all the compositions when $m = 4$, and respectively $m = 5$. These simulations show that up to $m = 4$ the order on the compositions is total. Starting from $m = 5$ the order is partial, the compositions that are no longer comparable are $(0, 0, 0, 0, 1)$ with $(1, 1, 0, 0, 0)$, $(0, 0, 0, 1, 1)$ with $(1, 1, 0, 1, 0)$, and $(0, 0, 1, 0, 1)$ with $(1, 1, 1, 0, 0)$. As m grows the number of non-comparable compositions in the poset increases (see $m = 6$ in Fig. 4c).

In the next subsection, we will introduce partial orders less fine than the pointwise order, i.e., the orders to be defined here are such that if $\mathbf{u} \leq \mathbf{v}$ then $\mathbf{u} \leq \mathbf{v}$.

2) *A general order:* The first partial order that naturally comes to mind when dealing with the reliability of MMNs results from their incidence matrices.

Definition 15. Let N_1 and N_2 be two MMNs having the same w and l . We say that $N_1 \preceq_M N_2$ if and only if

$$\forall 1 \leq i \leq w-1, 1 \leq j \leq l-1 \quad M_{N_1}(i, j) \leq M_{N_2}(i, j).$$

The meaning of \preceq_M is that whenever there is a matchstick at a position (i, j) in N_1 there has to be a matchstick at the same position in N_2 . Therefore, N_2 has at least the same number of matchsticks as N_1 and can also be understood as “the matchsticks of N_1 perfectly overlap those of N_2 .”

Lemma 16. Let N_1 and N_2 be two MMNs having the same w and l such that $N_1 \preceq_M N_2$. Then we have

$$\forall 0 \leq i \leq wl \quad N_i(N_1) \leq N_i(N_2).$$

Theorem 17. Let N_1 and N_2 be two MMNs having the same w and l such that $N_1 \preceq_M N_2$. Then

$$\text{Rel}(N_1) \leq \text{Rel}(N_2).$$

Proof. The proof follows from Lemma 16 and Proposition 13. \square

Notice that in [2], the authors pointed out that hammocks are “midway” between a PoS and a SoP with respect to the number of matchsticks (see Fig. 2). This implies the following ordering among hammocks, PoS and SoP.

Proposition 18. Let $m \geq 2$ and let $1 \leq i \leq m-1$. We have

$$\text{Rel}\left(\mathcal{C}^{(1^i 0^{m-i})}\right) \leq \text{Rel}\left(\mathbf{H}_{2^i, 2^{m-i}}\right) \leq \text{Rel}\left(\mathcal{C}^{(0^{m-i} 1^i)}\right).$$

Proof. By Proposition 8 we check that the networks $\mathcal{C}^{(1^i 0^{m-i})}$ (PoS) and $\mathcal{C}^{(0^{m-i} 1^i)}$ (SoP) have the same dimensions as $\mathbf{H}_{2^i, 2^{m-i}}$, while afterwards we use $M_{\mathbf{H}_{2^i, 2^{m-i}}}$, $M_{\mathcal{C}^{(0^{m-i} 1^i)}}$ and $M_{\mathcal{C}^{(1^i 0^{m-i})}}$ in Theorem 17 to prove the result. \square

An even tighter inequality can be established.

Proposition 19. For $m \geq 3$ and $2 \leq i \leq m-2$ we have

$$\text{Rel}\left(\mathcal{C}^{(1^{i-1} 0^{m-i-1} 10)}\right) \leq \text{Rel}\left(\mathbf{H}_{2^i, 2^{m-i}}\right).$$

The proof is similar to the previous one.

If some MMNs with identical w and l can easily be compared by means of \preceq_M , what happens in the case of MMNs having different parameters? Our simulations show that several particular cases of MMNs, although having different parameters, are comparable. In particular, compositions of series and parallel are such cases.

C. Partial orders for compositions

Definition 20. Let \mathbf{u} and \mathbf{v} be two binary vectors of size m . We define $\mathbf{u} \preceq_S \mathbf{v}$ if and only if $\text{Supp}(\mathbf{u}) \subseteq \text{Supp}(\mathbf{v})$. Equality holds only for $\mathbf{u} = \mathbf{v}$.

Definition 21. Let $l \leq m$ be two strictly positive integers and \mathbf{u}, \mathbf{v} be two binary vectors of size m such that $|\mathbf{u}| = |\mathbf{v}| = l$. Let $\text{Supp}(\mathbf{u}) = \{s_1, \dots, s_l\}$ and $\text{Supp}(\mathbf{v}) = \{t_1, \dots, t_l\}$, with $s_1 < \dots < s_l$ and $t_1 < \dots < t_l$. We define $\mathbf{u} \preceq_H \mathbf{v}$ if and only if $\forall 1 \leq i \leq l, s_i \leq t_i$.

We combine \preceq_S and \preceq_H in a natural manner and define the order “ \preceq_{SH} ” as being equal to

- \preceq_S when comparing vectors with different Hamming weights;
- \preceq_H when comparing vectors having the same Hamming weight.

The orders that we define and prove here (i.e., \preceq_S , \preceq_H and \preceq_{SH}) have also been used in other fields [28], [29]. The first one (\preceq_S) was proposed in the context of Boolean functions [30], more precisely for computing the Algebraic Normal Form of a Boolean function using the Fast Mobius Transform [30, Section 2.1]. In a completely different field, \preceq_S was used to tighten the bounds on the error block probability of a polar code designed for a binary erasure channel ([31, Section VI]). In [32], [28], [33], \preceq_{SH} was used to prove degradation of communication channels for polar codes, while in [34] and [29], it was used to optimize construction of polar codes for different type of channels. In [35], Gordon, Miller and Ostapenko used \preceq_{SH} for solving the closest pair problem in large datasets by means of optimal hash functions. The order \preceq_{SH} was also used in a cryptographic application [36].

Now, we are ready to introduce one of our main results.

Theorem 22. Let u and v be two binary vectors of size m . Then we have

$$u \preceq_{SH} v \Rightarrow u \leq v.$$

The proof of this theorem is given in Appendix A. This was already state without proof in [11]. The poset of compositions will be shorthand as $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ and, for convenience, we will use u instead of C^u .

V. PROPERTIES OF THE POSET

In order to give the structural properties of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ we remember several fundamental concepts from poset theory. A quick bibliographic search shows that this poset is isomorphic to a well-known one, denoted as $M(n)$ in [37, Section 4.1.2], where it is called *partitions into distinct summands*. This poset has the following main properties: *rank unimodal*, *rank symmetric* and *Sperner property*.

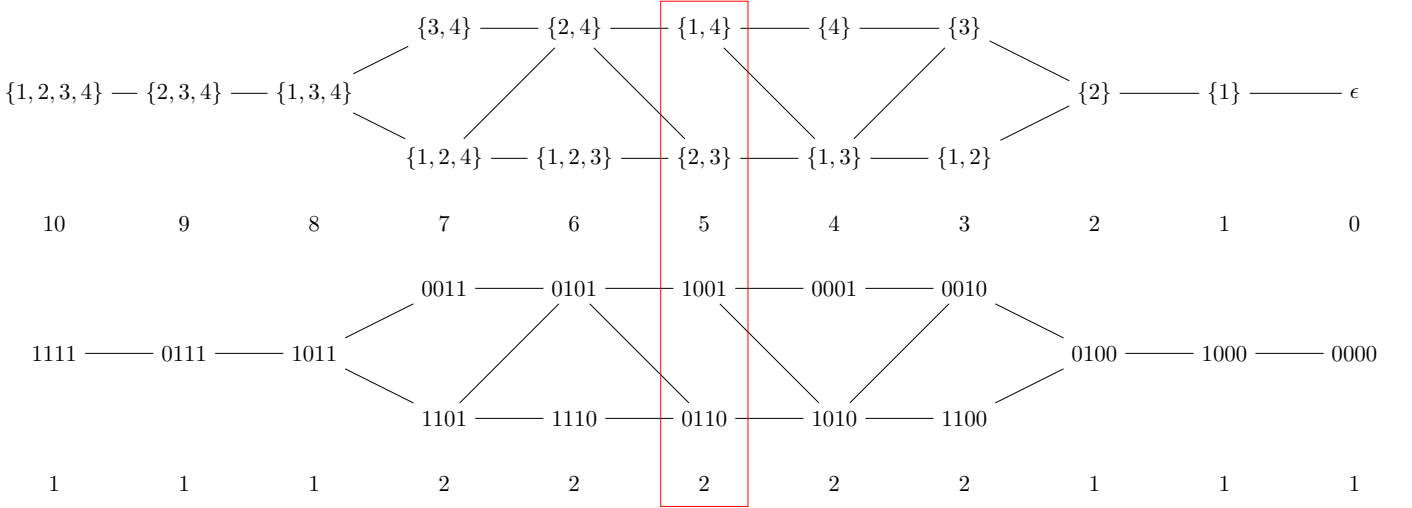


Fig. 5: The Hasse diagram for $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ for $m = 4$, the rank values for each level of the poset, and $\#\mathcal{P}_i$.

A. Preliminaries

Definition 23. Let \mathcal{P} be a poset. We call any subset of \mathcal{P} a *chain*, if and only if it is totally ordered. Any subset of \mathcal{P} is called an *antichain* if no pair of elements in it are comparable.

For example, for $m = 4$ we have that $\{(0101), (1110)\}$ and $\{(1110), (1001)\}$ are two antichains, while $\{(0010), (1010), (0110), (0101), (0011), (1011)\}$ is a chain (see Fig. 5).

Definition 24. A poset \mathcal{P} is *bounded from above/below* if there is an element x of \mathcal{P} such that any other element of \mathcal{P} is smaller/larger than x . When \mathcal{P} admits both an upper and a lower bound we simply say that \mathcal{P} is *bounded*.

Definition 25. Let \mathcal{P} be a poset. We say that \mathcal{P} is *graded* if \mathcal{P} can be equipped with a (rank) function $\rho : \mathcal{P} \rightarrow \mathbb{N}$ that satisfies:

- if x is minimal then $\rho(x) = 0$.
- if y covers x then $\rho(y) = \rho(x) + 1$.

Any graded poset \mathcal{P} can be partitioned into $\mathcal{P} = \bigcup_{i=1}^r \mathcal{P}_i$, where \mathcal{P}_i is the rank i of \mathcal{P} . This implies that any maximal length chain in \mathcal{P} passes through exactly one element in each \mathcal{P}_i . Any \mathcal{P}_i is also an antichain, since all the elements of \mathcal{P}_i have rank i and thus are not comparable. For a graded poset \mathcal{P} the maximum number of elements in an antichain is lower bounded by the maximum of $\#\mathcal{P}_i$.

Definition 26. Let \mathcal{P} be a graded poset with $\mathcal{P} = \bigcup_{i=1}^r \mathcal{P}_i$. We say that

- \mathcal{P} is *rank symmetric* if $\#\mathcal{P}_i = \#\mathcal{P}_{r-i}$, for all i ;
- \mathcal{P} is *rank unimodal* if the sequence $\{\#\mathcal{P}_i\}_{1 \leq i \leq r}$ is unimodal;
- \mathcal{P} is *Sperner* if $\max_A \#A = \max_i \#\mathcal{P}_i$, where A runs through the set of all antichains.

Hence, in a *Sperner* poset the largest rank provides an antichain of maximum cardinality. Notice that there may exist other antichains of maximum cardinality as well. So, if \mathcal{P} is rank symmetric, rank unimodal, and *Sperner*, then $\max_A \#A = \#\mathcal{P}_{r/2}$ when r is even, and $\max_A \#A = \#\mathcal{P}_{\lfloor r/2 \rfloor} = \#\mathcal{P}_{\lceil r/2 \rceil}$ when r is odd.

B. Applications to compositions

1) General properties of the poset of compositions:

Proposition 27. $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is bounded, where $\mathbf{u} = (0, \dots, 0)$ and $\mathbf{v} = (1, \dots, 1)$ are the minimum, and respectively the maximum elements.

Proof. This follows directly from the definition of the order \preceq_{SH} . \square

We can also prove that $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is graded by specifying a rank function.

Proposition 28. Let m be a strictly positive integer. $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is graded, where

$$\forall \mathbf{u} \in \{0, 1\}^m \quad \rho(\mathbf{u}) = \sum_{i \in \text{Supp}(\mathbf{u})} i.$$

Proof. First, notice that the minimum element of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is the all-zeros vector, which implies that $\rho(0, \dots, 0) = 0$. For the second condition we need to check that if \mathbf{v} covers \mathbf{u} then $\rho(\mathbf{v}) = \rho(\mathbf{u}) + 1$. For any \mathbf{u} in the poset, \mathbf{v} might cover \mathbf{u} either by \preceq_S or by \preceq_H .

- Suppose that \mathbf{v} covers \mathbf{u} and $\mathbf{u} \preceq_H \mathbf{v}$, and let $\text{Supp}(\mathbf{u}) = \{s_1, \dots, s_l\}$ and $\text{Supp}(\mathbf{v}) = \{t_1, \dots, t_l\}$. This implies that $\exists 1 \leq i_0 \leq l$ such that $s_{i_0} + 1 = t_{i_0}$ and $\forall 1 \leq i \neq i_0 \leq l, s_i = t_i$. Hence we have $\rho(\mathbf{v}) = \rho(\mathbf{u}) + 1$.
- Suppose that \mathbf{v} covers \mathbf{u} and $\mathbf{u} \preceq_S \mathbf{v}$. By definition we have $\text{Supp}(\mathbf{u}) \subset \text{Supp}(\mathbf{v})$. Notice that unless $1 \notin \text{Supp}(\mathbf{u})$, \mathbf{v} can not cover \mathbf{u} by \preceq_S . We will prove this claim by contradiction. Suppose that $1 \in \text{Supp}(\mathbf{u})$ and $\exists \mathbf{v}$ that covers \mathbf{u} by \preceq_S . We distinguish two cases:
 - 1) The first case is when $\text{Supp}(\mathbf{u}) = \{1, 2, \dots, l\}$. This implies that $\{1, \dots, l\} \subset \text{Supp}(\mathbf{v})$ and the smallest \mathbf{v} which satisfies this condition is such that $\text{Supp}(\mathbf{v}) = \{1, \dots, l+1\}$. Now, by letting \mathbf{w} be such that $\text{Supp}(\mathbf{w}) = \{2, 3, \dots, l+1\}$, $\mathbf{u} \preceq_H \mathbf{w} \preceq_S \mathbf{v}$, which is impossible since \mathbf{v} covers \mathbf{u} .
 - 2) The second case is when the elements in $\text{Supp}(\mathbf{u})$ are not necessarily consecutive integers from 1 to l . This implies that there are at least two elements in $\text{Supp}(\mathbf{u})$, s_i and s_{i+1} , such that s_i is the smallest element satisfying $s_i \leq s_{i+1} - 2$. The smallest \mathbf{v} that is $\mathbf{u} \preceq_S \mathbf{v}$ satisfies $\text{Supp}(\mathbf{v}) = \text{Supp}(\mathbf{u}) \cup \{s_i + 1\}$. Now let \mathbf{w} be such that $\text{Supp}(\mathbf{w}) = \{2, \dots, s_i + 1\} \cup \{s_{i+1}, \dots, s_l\}$. Obviously, we have $\mathbf{u} \preceq_H \mathbf{w} \preceq_S \mathbf{v}$, which is impossible.

Since $1 \notin \text{Supp}(\mathbf{u})$ and 1 is the smallest element that one could add to $\text{Supp}(\mathbf{u})$ in order to obtain an element \mathbf{v} such that $\mathbf{u} \preceq_S \mathbf{v}$, the proof is concluded. \square

Theorem 29 ([37]). Let m be a strictly positive integer. Then the set of compositions ordered by \preceq_{SH} is rank unimodal, rank symmetric and Sperner.

For example, when $m = 4$ (see Fig. 5) the sequence of $\#\mathcal{P}_i$ is 1, 1, 1, 2, 2, 2, 2, 1, 1, 1, which is rank symmetric and rank unimodal.

In the following we will answer four natural questions related to $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$:

- Which is the maximum length of a chain?
- How to construct a chain of maximum length?
- Which is the middle of the poset?
- How to identify at least one element from the middle of the poset?

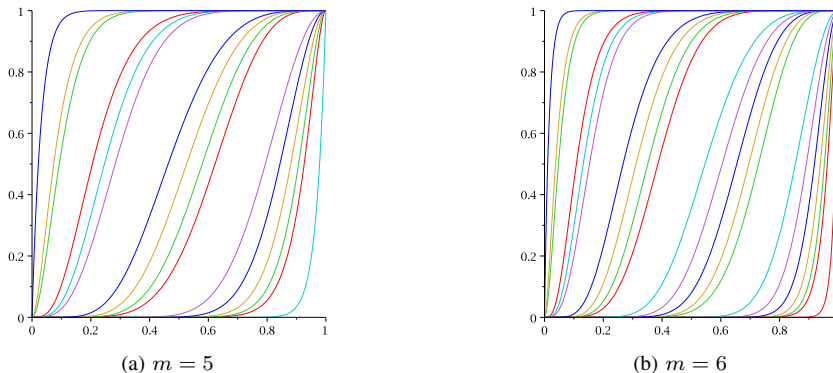


Fig. 6: $\text{Rel}(\mathcal{C}^{\mathbf{u}})$ for $\mathbf{u} \in \mathcal{S}$, constructed using the algorithm from Proposition 31.

2) *Maximum length chain of the poset:*

Corollary 30. *Let m be a strictly positive integer. Then the maximum length of a chain in $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ equals $\binom{m+1}{2}$.*

Proof. First, notice that any chain can traverse any rank i at most once. Hence, the maximum length chain has to traverse each rank once and only once, meaning that it starts at rank 0 (given by $\mathbf{u} = (0, \dots, 0)$) and walks through one element in each rank i till it reaches the maximum element (which is $\mathbf{u} = (1, \dots, 1)$).

Second, in order to compute the length of this chain we use the rank function ρ for the maximum element, $\rho(1, \dots, 1) = \sum_{i=1}^m i = \binom{m+1}{2}$. \square

Proposition 31. *Define the following algorithm*

Input : A strictly positive integer m
Output: A maximum length chain \mathcal{S} for $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$
 $\mathcal{S} = \{\}$;
 $k = 0$;
for j *from* 1 *to* m **do**
 for i *from* 0 *to* $m - j$ **do**
 $\mathcal{S} = \mathcal{S} \cup \{k + 2^i\}$;
 end
 $k = k + 2^{m-j}$;
end
Return \mathcal{S} in binary;

This algorithm constructs a maximum length chain \mathcal{S} for $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$.

Proof. This algorithm builds a set $\mathcal{S} = \bigcup_{j=1}^m \mathcal{S}_j$, where $\mathcal{S}_j = \{k_j + 2^i \mid 0 \leq i \leq m - j\}$, with $k_j = \sum_{l=1}^j 2^{m-l+1} \pmod{2^m}$. The first set \mathcal{S}_1 is the set of all possible powers of 2. The second set is the set of all integers that can be written as sum of 2^{m-1} plus any other power of 2, and so on. Notice that the sets \mathcal{S}_j are pairwise disjoint. By simple inspection of the sets \mathcal{S}_j we have

$$\forall 1 \leq j \leq m \quad \#\mathcal{S}_j = m + 1 - j. \quad (11)$$

Hence, we obtain

$$\#\mathcal{S} = \sum_{j=1}^m \#\mathcal{S}_j = \sum_{j=1}^m (m + 1 - j) = \binom{m+1}{2}.$$

We still need to check whether \mathcal{S} is a chain in $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$. If we expand each element in \mathcal{S}_j for any fixed j , we notice that they are totally ordered with respect to \preceq_H . On top of that, the first element of \mathcal{S}_{j+1} is larger than the last element of \mathcal{S}_j with respect to the order \preceq_S , which concludes the proof. \square

3) *The middle of the poset:*

Corollary 32. *Let m be a strictly positive integer. Then the middle of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is either $\binom{m+1}{2}/2$ (when m is a multiple of 4), or $\lfloor \binom{m+1}{2}/2 \rfloor$ and $\lceil \binom{m+1}{2}/2 \rceil$ (otherwise).*

The middle of the poset corresponds to the sequence of maximum numbers of subsets of $\{1, 2, \dots, m\}$ that share the same sum (A025591 in [38]) :

$$1, 1, 1, 2, 2, 3, 5, 8, 14, 23, 40, \dots$$

Proposition 33. *Let k and m be strictly positive integers with $\mathbf{u} \in \{0, 1\}^m$ such that*

$$\mathbf{u} = \begin{cases} (0^k & 1^{2k} & 0^k) & m = 4k \\ (0^{k+1} & 1^{2k} & 0^k) & m = 4k + 1 \\ (0^k & 1^{2k} & 0^{k+1} & 1) & m = 4k + 2 \\ (0^k & 1^{2k+2} & 0^{k+1}) & m = 4k + 3 \end{cases}.$$

Then, both \mathbf{u} and $\bar{\mathbf{u}}$ are middle rank elements of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$.

Notice that Proposition 33 can be restated in an equivalent form by using $\text{Supp}(\mathbf{u})$. For example, when $m = 4k$ one would rather say that a middle rank element of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is \mathbf{u} with $\text{Supp}(\mathbf{u}) = \{k + 1, \dots, 2k\}$. One can check that \mathbf{u} is a middle rank element simply by computing the sum of the elements in $\text{Supp}(\mathbf{u})$.

Proof. We prove each possible case separately.

- $m = 4k$ with $k \geq 1$. In this case the middle rank equals $k(4k + 1) = 4k^2 + k$. The rank of $\mathbf{u} = 0^k 1^{2k} 0^k$ is

$$\sum_{i=k+1}^{3k} i = 2k^2 + 2k(2k + 1)/2 = 4k^2 + k.$$

- $m = 4k + 1$ with $k \geq 1$. The middle rank equals $(4k + 1)(4k + 2)/4 = 4k^2 + 3k + 1/2$. So we have two cases, either $4k^2 + 3k$ or $4k^2 + 3k + 1$. The rank of $\mathbf{u} = 0^{k+1} 1^{2k} 0^k$ is

$$\sum_{i=k+2}^{3k+1} i = 4k^2 + 3k.$$

- $m = 4k + 2$ with $k \geq 1$. The middle rank equals $(4k + 2)(4k + 3)/4 = 4k^2 + 5k + 3/2$. So we have two cases, either $4k^2 + 5k + 1$ or $4k^2 + 5k + 2$. The rank of $\mathbf{u} = 0^k 1^{2k} 0^{k+1} 1$ is

$$4k + 1 + \sum_{i=k+1}^{3k} i = 4k^2 + 5k + 1.$$

- $m = 4k + 3$ with $k \geq 1$. The middle rank equals $(4k + 3)(4k + 4)/4 = 4k^2 + 7k + 3$. The rank of $\mathbf{u} = 0^k 1^{2k+2} 0^{k+1}$ is

$$\sum_{i=k+1}^{3k+2} i = 4k^2 + 7k + 3.$$

The fact that $\bar{\mathbf{u}}$ is also an element of the middle of the poset follows from $\text{Supp}(\mathbf{u}) + \text{Supp}(\bar{\mathbf{u}}) = \binom{m+1}{2}$. \square

4) *Maximum length antichain:* Because $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is *Sperner*, the maximum length of an antichain is given by the maximum of $\#\mathcal{P}_i$, which is achieved by the middle rank.

Using a well-known theorem by Dilworth [39], we are able to determine the minimum number of chains in which $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ can be partitioned.

Theorem 34 ([39]). *The minimum number of chains in which the elements of a poset \mathcal{P} can be partitioned is equal to the maximum number of elements of an antichain of \mathcal{P} .*

Example 35. *Maximum antichains.*

- $m = 5$

$$\mathcal{P}_7 = \{[4, 2, 1], [4, 3], [5, 2]\} \quad \text{and} \quad \mathcal{P}_8 = \{[4, 3, 1], [5, 2, 1], [5, 3]\}.$$

- $m = 6$

$$\mathcal{P}_{10} = \{[4, 3, 2, 1], [5, 3, 2], [5, 4, 1], [6, 3, 1], [6, 4]\} \quad \text{and} \quad \mathcal{P}_{11} = \{[5, 3, 2, 1], [5, 4, 2], [6, 3, 2], [6, 4, 1], [6, 5]\}.$$

- $m = 7$

$$\mathcal{P}_{14} = \{[5, 4, 3, 2], [6, 4, 3, 1], [6, 5, 2, 1], [6, 5, 3], [7, 4, 2, 1], [7, 4, 3], [7, 5, 2], [7, 6, 1]\}.$$

- $m = 8$

$$\mathcal{P}_{18} = \{[6, 5, 4, 2, 1], [6, 5, 4, 3], [7, 5, 3, 2, 1], [7, 5, 4, 2], [7, 6, 3, 2], [7, 6, 4, 1], [7, 6, 5], [8, 4, 3, 2, 1], [8, 5, 3, 2], [8, 5, 4, 1], [8, 6, 3, 1], [8, 6, 4], [8, 7, 2, 1], [8, 7, 3]\}.$$

A consequence of Theorem 34 is that the minimum number of chains in which $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ can be partitioned equals $\#\mathcal{P}_{\binom{m+1}{2}}$. Now, since $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is isomorphic to $M(n)$ (see [37]), in order to determine the elements of $\mathcal{P}_{\binom{m+1}{2}}$ we can use an algorithm that generates subsets of $\{1, \dots, m\}$, such that the sum of their elements equals $\binom{m+1}{2}$. Example 35 illustrates this for several values of m . Notice that, the compositions \mathbf{u} given by Proposition 33 are also elements of these antichains.

VI. MOST RELIABLE MMNS

A. Uniformly most reliable networks

Definition 37. We say that $N^* \in \mathcal{N}_n$ is UMR-MMN if for any $N \in \mathcal{N}_n$ we have

$$\text{Rel}(N^*) \geq \text{Rel}(N) \quad \forall p \in [0, 1]. \quad (12)$$

This definition is not identical to that of Boesch et al. [13], as although eq. (12) is the same, the set of networks is different. For Boesch et al. the domain is represented by the set of simple graphs with n edges and w vertices, while in our case the domain is \mathcal{N}_n .

Theorem 38. Let m be a positive integer. Then C^u , with $u = (1, \dots, 1) \in \{0, 1\}^m$, is UMR-MMN in \mathcal{N}_{2^m} .

Proof. This follows directly from the fact that $u = (1, \dots, 1) \in \{0, 1\}^m$ is the supremum of $\mathcal{P}(C_{2^m}, \preceq_{SH})$. \square

B. Heaviside most reliable networks

Definition 39. We say that $N^* \in \mathcal{N}_n$ is HMR-MMN with $p_0 \in (0, 1)$ if for any $N \in \mathcal{N}_n$ we have

$$\text{Rel}(N^*) \leq \text{Rel}(N) \quad \forall p \in [0, p_0] \quad (13)$$

and

$$\text{Rel}(N^*) \geq \text{Rel}(N) \quad \forall p \in [p_0, 1]. \quad (14)$$

This means that an MMN is an HMR-MMN if it is very close to both the minimum of the poset, for a particular range of values, as well as to the maximum of the poset, for the remaining range of values.

Lemma 40. Let m be a strictly positive integer. For any $N \in \mathcal{N}_{2^m}$ we have

$$\text{Rel}(C^{(0, \dots, 0)}) < \text{Rel}(N) \quad \forall p \in (0, 1];$$

$$\text{Rel}(N) < \text{Rel}(C^{(1, \dots, 1)}) \quad \forall p \in [0, 1).$$

Theorem 41. Let m be a strictly positive integer. Then there is no HMR-MMN for $p_0 \in (0, 1)$.

Proof. By Lemma 40 we have that the only composition that satisfies eq. (13) is $C^{(0, \dots, 0)}$. We also have that the only composition that satisfies eq. (14) is $C^{(1, \dots, 1)}$. Unless $C^{(0, \dots, 0)}$ equals $C^{(1, \dots, 1)}$, it is impossible to have an MMN that satisfies both eq. (13) and eq. (14). So unless $m = 0$ there is no HMR-MMN. \square

C. Optimality of MMNs

1) *Motivations:* Since HMR-MMNs do not exist, we re-define optimality as follows: establish how close $\text{Rel}(N; p)$ is to $\theta(p - p_0)$. We restrict our search only to square MMNs ($w = l = \sqrt{n} = 2^{m/2}$), and support this choice by several arguments.

One argument is given in [9], [10], where the authors have proposed several FOMs such as: the steepness of the reliability polynomials, and their variation in a symmetric interval with respect to $p_0 = 0.5$. Those simulations, as well as our own simulations, have shown that square MMNs come ‘‘closer’’ to $\theta(p - 0.5)$ than non-square MMNs. Still, these have been verified only for small values of l and w .

Another argument is a combinatorial one. Suppose that one would randomly choose from the set of all MMNs of size n . The question one should ask is: Do square MMNs appear with higher probability?

Proposition 42. Let m be a strictly positive integer. Then we have

$$\lim_{m \rightarrow \infty} \frac{\#\mathcal{N}_{2^{m/2}, 2^{m/2}}}{\#\mathcal{N}_{2^m}} = 1. \quad (15)$$

Proof. Using a known result about the cardinality of the two sets we have

$$\begin{aligned} \frac{\#\mathcal{N}_{2^{m/2}, 2^{m/2}}}{\#\mathcal{N}_{2^m}} &= \frac{2^{(2^{m/2}-1)(2^{m/2}-1)}}{\sum_{i=0}^m 2^{(2^i-1)(2^{m-i}-1)}} \geq \frac{2^{(2^{m/2}-1)^2}}{2^{(2^{m/2}-1)^2} + m \cdot 2^{(2^{m/2}-1)(2^{m/2+1}-1)}} \\ \frac{\#\mathcal{N}_{2^{m/2}, 2^{m/2}}}{\#\mathcal{N}_{2^m}} &\geq \frac{1}{1 + m \cdot 2^{2^{m/2}-2^{m/2}-1-2^{m/2+1}+2^{m/2}}} = \frac{1}{1 + \frac{m}{2^{m/2-1}}}. \end{aligned}$$

We used here the fact that the sum can be upper bounded by the middle term plus m times the previous term. In order to verify this, one has to check whether

$$\forall 0 \leq i \leq \frac{m}{2} - 1, \quad 2^{(2^i-1)(2^{m-i}-1)} \leq 2^{(2^{m/2-1}-1)(2^{m/2+1}-1)}. \quad (16)$$

Tacking logarithms of both sides and expanding we obtain

$$\forall 0 \leq i \leq \frac{m}{2} - 1, 2^{m-i} + 2^i - 2^{m/2-1} - 2^{m/2+1} \geq 0. \quad (17)$$

The left part of the inequality can be viewed as an increasing function of i . Since for $i = 0$ this is positive, as long as $m \geq 2$, the proof is concluded. \square

2) *Theoretical results for square MMNs*: A first result that we prove involves square PoS, square hammocks and square SoP.

Corollary 43 ([11]). *Let m be an even positive integer. We have*

$$\text{Rel} \left(\mathcal{C}^{(1^{m/2} 0^{m/2})} \right) \leq \text{Rel} \left(\mathbf{H}_{2^{m/2}, 2^{m/2}} \right) \leq \text{Rel} \left(\mathcal{C}^{(0^{m/2} 1^{m/2})} \right)$$

while there are $m^2/2$ ranks in $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ between the square PoS and the square SoP.

This follows directly from Proposition 18 by taking $i = m/2$.

Corollary 44. *Let m be an even positive integer, then*

$$\text{Rel} \left(\mathcal{C}^{(1^{m/2-1} 0^{m/2-1} 10)} \right) \leq \text{Rel} \left(\mathbf{H}_{2^{m/2}, 2^{m/2}} \right). \quad (18)$$

This is a direct consequence of Proposition 19 for $i = m/2 - 1$. The result represents an improvement, as it reduces the number of ranks to be analyzed from $m^2/2$ to $m^2/2 - m/2 - 1$. This is still a large number of elements. On one hand, since $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ is unimodal and symmetric it follows that the maximum cardinality rank is given by the middle of the poset. On the other hand, for $\mathbf{u} = (1^{m/2} 0^{m/2} 10)$ we have $\rho(\mathbf{u}) < \binom{m+1}{2}/2 < \rho(\bar{\mathbf{u}})$.

All of these arguments are supporting our choice to analyze only square compositions in the middle of the poset.

Theorem 45 ([40]). *Let m be a strictly positive integer. The middle of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$, has cardinality*

$$\#\mathcal{P}_{\binom{m+1}{2}} = \sqrt{\frac{6}{\pi}} \frac{2^m}{m^{3/2}} (1 + o(1)), \text{ when } m \rightarrow \infty. \quad (19)$$

A direct consequence of Theorem 45 is that searching for HMR compositions requires computing the reliability polynomials for only $n/\log^{3/2}(n)$ compositions. Here, since we restricted the study to square MMNs, we need to determine how many compositions in the middle of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ are square.

Our simulations are supporting the intuition that all the compositions in the middle of the poset are either square or close to square. This was verified for $6 \leq m \leq 13$. The simulations also showed that roughly half of the compositions in the middle of the poset are square. We conjecture this to be true in general.

Corollary 46. *Let m be a strictly positive integer. When $m \rightarrow \infty$ we have*

$$\frac{\#\left(\mathcal{P}_{\binom{m+1}{2}} \cap \mathcal{C}_{2^{m/2}, 2^{m/2}}\right)}{\#\mathcal{C}_{2^{m/2}, 2^{m/2}}} = \sqrt{\frac{3}{4}} \frac{1}{m} \left(1 + O\left(\frac{1}{m}\right)\right). \quad (20)$$

Proof. To estimate the numerator we use Theorem 45 with the assumption that half of the elements in the middle of the poset are square MMNs. For the denominator, when $m \rightarrow \infty$ we have

$$\binom{m}{m/2} = \sqrt{\frac{2}{m\pi}} 2^m \left(1 - O\left(\frac{1}{m}\right)\right),$$

\square

A straightforward interpretation of Corollary 46 is that the ratio of the number of square compositions in the middle of the poset over the number of all square compositions decreases as $\log(n)$.

3) *Simulation results*: For several even values of m we have computed the cardinality of the following sets:

- the set of compositions;
- the set of square compositions;
- the middle of the $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$;
- the set of square compositions in the middle of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$.

These results can be seen in Table I. Our successive optimizations have reduced the cardinality of the sets to be analyzed, in particular, when $m = 12$ there are 58 square compositions in the middle of the poset out of:

- 4096 possible compositions ($\sim 1.4\%$);
- 924 square compositions ($\sim 6.2\%$);
- 124 compositions in the middle of the poset ($\sim 46.7\%$).

We can use duality in order to decrease even further the size of the sets by a factor of 2. More exactly, if $\mathbf{u} \in \mathcal{P}_i$ then we know that $\bar{\mathbf{u}} \in \mathcal{P}_{n-i}$. With all of these optimizations at hand we have computed all the square compositions in the middle of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ for $m = 6$. We selected half of them by duality, and have recovered the same results as in [9]. These were obtained by computing the reliability polynomials of only 3 MMNs instead of 64 as in [9].

TABLE I: Cardinality of the set of compositions, square compositions, the middle of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$, square compositions in the middle of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$, and the ratio of square compositions in the middle of $\mathcal{P}(\mathcal{C}_{2^m}, \preceq_{SH})$ over all square compositions.

m	$\#\mathcal{C}_{2^m}$	$\#\mathcal{C}_{2^{m/2}, 2^{m/2}}$	$\#\mathcal{P}_{\binom{m+1}{2}/2}$	$\#\left(\mathcal{P}_{\binom{m+1}{2}/2} \cap \mathcal{C}_{2^{m/2}, 2^{m/2}}\right)$	$\frac{\#\left(\mathcal{P}_{\binom{m+1}{2}/2} \cap \mathcal{C}_{2^{m/2}, 2^{m/2}}\right)}{\#\mathcal{C}_{2^{m/2}, 2^{m/2}}}$
4	16	6	2	2	1
6	64	20	{5, 5}	{3, 3}	0.3
8	256	70	14	8	0.11
10	1024	252	{40, 40}	{20, 20}	0.16
12	4096	924	124	58	0.06

VII. CONCLUSIONS AND PERSPECTIVES

In this article, we have described the structure of a poset on the set of compositions of series and parallel two-terminal networks. We have used this structure to derive results on the existence of UMR-MMNs and HMR-MMNs.

There are several directions for extending and improving on the results reported here. The first one is related to the poset of reliability for the set of all MMNs. We have set up here the starting point by defining \preceq_M . By means of this large poset we are working on a formal proof that hammocks are the closest MMNs to $\theta(p - 0.5)$. The second one pertains to other forms of symmetries that could potentially reduce the computations for finding those network closest to $\theta(p - 0.5)$. It is to be mentioned that different networks might lead to identical reliability polynomials, e.g., if we swap the two terminals we obtain different networks having identical polynomials. Also a finer ordering of the reliability polynomials of the compositions would enable a more efficient algorithm for finding the optimal networks.

APPENDIX

Proposition 47. *Let \mathbf{u} and \mathbf{v} be two binary vectors of size m . Then we have $\mathbf{u} \preceq_S \mathbf{v} \Rightarrow \mathbf{u} \leq \mathbf{v}$.*

In order to prove this proposition we need the following lemma.

Lemma 48. *Let s be a strictly positive integer and for $i \in \{1, \dots, s\}$, let l_i, l_i^* be increasing functions from $[0, 1] \rightarrow [0, 1]$ such that $\forall p \in [0, 1], l_i^*(p) \leq l_i(p)$. Let $f = l_1 \circ \dots \circ l_s$ and $f^* = l_1^* \circ \dots \circ l_s^*$, then $\forall p \in [0, 1], f^*(p) \leq f(p)$.*

This lemma can be easily proved by induction. With this result at hand we can prove Proposition 47.

Proof of Proposition 47. First notice that $\text{Rel}(\mathbf{C}^{(0)}) \leq \text{Rel}(\mathbf{C}^{(1)})$. Then let \mathbf{u} and \mathbf{v} such that $\text{Supp}(\mathbf{u}) \subset \text{Supp}(\mathbf{v})$. By Lemma 48 the result holds. \square

Proposition 49. *Let \mathbf{u} and \mathbf{v} be two binary vectors of size m with $|\mathbf{u}| = |\mathbf{v}|$. Then we have $\mathbf{u} \preceq_H \mathbf{v} \Rightarrow \mathbf{u} \leq \mathbf{v}$.*

We will first prove a slightly weaker claim which provides a building block for the final proof.

Lemma 50. *Let $1 \leq s < m$ and $\mathbf{u} \in \{0, 1\}^m$ be such that $\text{Supp}(\mathbf{u}) = \{j_1, \dots, j_s\}$ with $1 \leq j_1 < \dots < j_s \leq m$. Now let \mathbf{u}^* be such that $\text{Supp}(\mathbf{u}^*) = \{j_1, \dots, j_i, j_{i+1}^*, j_{i+2}, \dots, j_s\}$ with $j_i \leq j_{i+1}^* \leq j_{i+1}$. Then $\mathbf{u}^* \preceq_H \mathbf{u}$ and $\mathbf{u}^* \leq \mathbf{u}$.*

Proof. From Theorem 14 we have

$$\begin{aligned} \text{Rel}(\mathbf{C}^{\mathbf{u}}) &= f_1 \circ \text{Rel}(\mathbf{C}^{(0)})^{j_{i+1}-j_{i+1}^*} \circ \text{Rel}(\mathbf{C}^{(1)}) \circ f_2 \\ \text{Rel}(\mathbf{C}^{\mathbf{u}^*}) &= f_1 \circ \text{Rel}(\mathbf{C}^{(1)}) \circ \text{Rel}(\mathbf{C}^{(0)})^{j_{i+1}-j_{i+1}^*} \circ f_2 \end{aligned}$$

where $f_1 = \text{Rel}(\mathbf{C}^{(0)})^{j_1} \circ \text{Rel}(\mathbf{C}^{(1)}) \circ \dots \circ \text{Rel}(\mathbf{C}^{(0)})^{j_i-j_{i-1}-1} \circ \text{Rel}(\mathbf{C}^{(1)}) \circ \text{Rel}(\mathbf{C}^{(0)})^{j_{i+1}^*-j_i-1}$ and $f_2 = \text{Rel}(\mathbf{C}^{(0)})^{j_{i+2}-j_{i+1}-1} \circ \text{Rel}(\mathbf{C}^{(1)}) \circ \dots \circ \text{Rel}(\mathbf{C}^{(0)})^{m-j_s-1}$.

Notice that $\text{Rel}(\mathbf{C}^{(0)})^{j_{i+1}-j_{i+1}^*} \circ \text{Rel}(\mathbf{C}^{(1)})$ and $\text{Rel}(\mathbf{C}^{(1)}) \circ \text{Rel}(\mathbf{C}^{(0)})^{j_{i+1}-j_{i+1}^*}$ are the reliability polynomials of a SoP, respectively a PoS of $w = 2$ and $l = 2^{j_{i+1}-j_{i+1}^*}$. Hence by Theorem 17 we have $\text{Rel}(\mathbf{C}^{(1)}) \circ \text{Rel}(\mathbf{C}^{(0)})^{j_{i+1}-j_{i+1}^*} \leq \text{Rel}(\mathbf{C}^{(0)})^{j_{i+1}-j_{i+1}^*} \circ \text{Rel}(\mathbf{C}^{(1)})$. Using Lemma 48 applied to $\text{Rel}(\mathbf{C}^{\mathbf{u}})$ and $\text{Rel}(\mathbf{C}^{\mathbf{u}^*})$ we obtain the desired result. \square

Proof of Proposition 49. Let $\mathbf{u} \preceq_H \mathbf{v}$ with $\text{Supp}(\mathbf{u}) = \{j_1, \dots, j_s\}$ and $\text{Supp}(\mathbf{v}) = \{k_1, \dots, k_s\}$. Define for $i = 0, \dots, s$ the binary vectors $\mathbf{u}^{(*i)}$ such that $\text{Supp}(\mathbf{u}^{(*i)}) = \{j_1 \dots j_i, k_{i+1} \dots k_s\}$. We have $\mathbf{u}^{(*0)} = \mathbf{v}$, $\mathbf{u}^{(*s)} = \mathbf{u}$, and $\mathbf{u}^{(*i+1)} \preceq_H \mathbf{u}^{(*i)}$ verify the hypotheses of the previous lemma. Applying the previous lemma s times, we get $\text{Rel}(\mathbf{C}^{\mathbf{u}}) \leq \text{Rel}(\mathbf{C}^{\mathbf{v}})$. \square

ACKNOWLEDGEMENTS

Research supported in part by the EU through the European Research Development Fund under the Competitiveness Operational Program (*BioCell-NanoART = Novel Bio-inspired Cellular Nano-architectures*, POC-A1-A1.1.4-E-2015 nr. 30/01.09.2016).

REFERENCES

- [1] J. von Neumann, "Probabilistic logics and the synthesis of reliable organisms from unreliable components," *Automata Studies*, pp. 43–98, 1956.
- [2] E. F. Moore and C. E. Shannon, "Reliable circuits using less reliable relays - Part I," *Journal of the Franklin Institute*, vol. 262, no. 3, pp. 191–208, Sep. 1956.
- [3] —, "Reliable circuits using less reliable relays - Part II," *Journal of the Franklin Institute*, vol. 262, no. 4, pp. 281–297, Oct. 1956.
- [4] L. Geppert, "The amazing vanishing transistor act," *IEEE Spectrum*, vol. 39, no. 10, pp. 28–33, Oct. 2002.
- [5] R. Courtland, "The next high-performance transistor," *IEEE Spectrum*, vol. 53, no. 10, pp. 11–12, Oct. 2016.
- [6] R. S. Raji, "Smart networks for control," *IEEE Spectrum*, vol. 31, no. 6, pp. 49–55, Jun. 1994.
- [7] F. H. Qusay, *Internet of Things A to Z: Technologies and Applications*. Hoboken, NJ: John Wiley & Sons, 2018.
- [8] W. Kuo and Z. Ming, *Optimal Reliability Modeling: Principles and Applications*. Hoboken, NJ: John Wiley & Sons, 2003.
- [9] V. Dragoi, S. R. Cowell, V. Beiu, S. Hoara, and P. Gaspar, "How reliable are compositions of series and parallel networks compared with hammocks?" *International Journal of Computers Communications & Control*, vol. 13, no. 5, pp. 772–791, Oct. 2018.
- [10] V. Beiu, S. R. Cowell, V. Drăgoi, S. Hoara, and P. Gaspar, "Hammocks versus hammock," in *Proc. International Conference on Computers Communications and Control (ICCCC)*, Oradea, Romania, May 2018, pp. 119–123.
- [11] V. Dragoi, S. Cowell, and V. Beiu, "Ordering series and parallel compositions," in *Proc. IEEE International Conference on Nanotechnology (IEEE-NANO)*, Cork, Ireland, Jul. 2018.
- [12] H. Bertrand, O. Goff, C. Graves, and M. Sun, "On uniformly most reliable two-terminal graphs," *Networks*, vol. 72, no. 2, pp. 200–216, Feb. 2017.
- [13] F. T. Boesch, X. Li, and C. Suffel, "On the existence of uniformly optimally reliable networks," *Networks*, vol. 21, no. 2, pp. 181–194, Mar. 1991.
- [14] A. K. Kelmans, "On graphs with randomly deleted edges," *Acta Mathematica Academiae Scientiarum Hungarica*, vol. 37, no. 1-3, pp. 77–88, Mar. 1981.
- [15] G. Wang, "A proof of Boesch's conjecture," *Networks*, vol. 24, no. 5, pp. 277–284, Aug. 1994.
- [16] F. Ath and M. Sobel, "Some conjectured uniformly optimal reliable networks," *Probability in the Engineering and Informational Sciences*, vol. 14, no. 3, pp. 375–383, Jul. 2000.
- [17] J. I. Brown and D. Cox, "Nonexistence of optimal graphs for all terminal reliability," *Networks*, vol. 63, no. 2, pp. 146–153, Oct. 2014.
- [18] W. Myrvold, K. H. Cheung, L. B. Page, and J. E. Perry, "Uniformly-most reliable networks do not always exist," *Networks*, vol. 21, no. 4, pp. 417–419, Jul. 1991.
- [19] H. Bertrand, O. Goff, C. Graves, and M. Sun, "On uniformly most reliable two-terminal graphs," *Networks*, vol. 72, no. 2, pp. 200–216, 2018.
- [20] L. Valiant, "The complexity of enumeration and reliability problems," *SIAM Journal on Computing*, vol. 8, no. 3, pp. 410–421, Jul. 1979.
- [21] M. O. Ball, "Computational complexity of network reliability analysis: An overview," *IEEE Transactions on Reliability*, vol. 35, no. 3, pp. 230–239, Aug. 1986.
- [22] A. Satyanarayana and R. K. Wood, "Polygon-to-chain reductions and network reliability," Operations Research Center, University of California, Berkeley, CA, Tech. Rep. ORC 82-4, Mar. 1982.
- [23] S. R. Cowell, V. Beiu, L. Dăuș, and P. Poulin, "On the exact reliability enhancements of small hammock networks," *IEEE Access*, vol. 6, pp. 25411–25426, Apr 2018.
- [24] M. O. Ball, C. J. Colbourn, and J. S. Provan, "Network reliability," in *Handbook of Operations Research: Network Models*. North-Holland, Amsterdam: Elsevier, 1995, ch. 11, pp. 673–762.
- [25] C. J. Colbourn, *The Combinatorics of Network Reliability*. New York, NY: Oxford University Press, 1987.
- [26] H. Harborth, "Match sticks in the plane," in *The lighter side of mathematics. Proceedings of the Eugne Strens Memorial Conference on Recreational Mathematics and its History*, 1994, pp. 281–288.
- [27] R. P. Stanley, *Enumerative Combinatorics*. Cambridge, NY: Cambridge University Press, 2012.
- [28] M. Bardet, V. Dragoi, A. Otmani, and J. Tillich, "Algebraic properties of polar codes from a new polynomial formalism," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 230–234.
- [29] M. Mondelli, S. H. Hassani, and R. Urbanke, "Construction of polar codes with sublinear complexity," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 1853–1857.
- [30] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Cambridge, NY: Cambridge University Press, 2010, ch. 8, pp. 257–397.
- [31] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Seoul, South Korea, Jun. 2009, pp. 1496–1500.
- [32] C. Schürch, "A partial order for the synthesized channels of a polar code," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 220–224.
- [33] V. Dragoi, "Algebraic approach for the study of algorithmic problems coming from cryptography and the theory of error correcting codes," PhD Thesis, Normandie Université, Jul. 2017. [Online]. Available: <https://hal.archives-ouvertes.fr/tel-01627324>
- [34] G. He, J. Belfiore, I. Land, G. Yang, X. Liu, Y. Chen, R. Li, J. Wang, Y. Ge, R. Zhang, and W. Tong, "Beta-expansion: A theoretical framework for fast and recursive construction of polar codes," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Singapore, Singapore, Dec. 2017, pp. 1–6.

- [35] D. M. Gordon, V. S. Miller, and P. Ostapenko, "Optimal hash functions for approximate matches on the n -cube," *IEEE Transactions on Information Theory*, vol. 56, no. 3, pp. 984–991, Mar. 2010.
- [36] M. Bardet, J. Chaulet, V. Dragoi, A. Otmani, and J. Tillich, "Cryptanalysis of the McEliece public key cryptosystem based on polar codes," in *Proc. 7th International Workshop on Post-Quantum Cryptography (PQCrypto)*, Fukuoka, Japan, Feb. 2016, pp. 118–143.
- [37] R. P. Stanley, "Some applications of algebra to combinatorics," *Discrete Applied Mathematics*, vol. 34, no. 1-3, pp. 241–277, Nov. 1991.
- [38] N. J. A. Sloane, "The on-line encyclopedia of integer sequences." [Online]. Available: <http://oeis.org>
- [39] R. P. Dilworth, *A Decomposition Theorem for Partially Ordered Sets*. Boston, MA: Birkhäuser, 1987, pp. 139–144.
- [40] B. D. Sullivan, "On a conjecture of Andrica and Tomescu," *Journal of Integer Sequences*, vol. 16, no. 3, art. 13.3.1, pp. 1–6, Mar. 2013.