

A subexponential construction of graph coloring for multiparty computation

Hassan Jameel Asghar, Yvo Desmedt, Josef Pieprzyk and
Ron Steinfeld

Communicated by Rainer Steinwandt

Abstract. We show the first deterministic construction of an unconditionally secure multiparty computation (MPC) protocol in the passive adversarial model over black-box non-Abelian groups which is both optimal (secure against an adversary who possesses any $t < \frac{n}{2}$ inputs) and has subexponential complexity of construction based on coloring of planar graphs. More specifically, following the result of Desmedt et al. (2012) that the problem of MPC over non-Abelian groups can be reduced to finding a t -reliable n -coloring of planar graphs, we show the construction of such a graph which allows a path from the input nodes to the output nodes when any t -party subset is in the possession of the adversary. Unlike the deterministic constructions from Desmedt et al. (2012) our construction has subexponential complexity and is optimal at the same time, i.e., it is secure for any $t < \frac{n}{2}$.

Keywords. Multiparty computation, graph coloring, non-Abelian group, planar graph.

2010 Mathematics Subject Classification. 94A60, 05C10, 05C15, 05C25.

1 Introduction

Secure multiparty computation (MPC), a topic first addressed by Yao as a generalization of his famous millionaires' problem in 1982 [16], enables two or more parties to securely compute a function on their individual secrets such that the parties involved obtain the correct output without revealing their secrets. Since Yao's germinal work, extensive research has been done in cryptography to construct protocols for secure MPC. Most protocols for unconditionally secure MPC, which is the adversarial model considered in this paper, involve performing multiplications and additions over a finite field. Some of these protocols have been generalized to work over rings; [7] presents an example. A natural extension of this trend is to realize MPC over groups. Recent years have seen a surge in interest in the cryptographic applications of non-Abelian groups [14, 15]. A result from

Barrington [2] that any function can be computed by the non-Abelian symmetric group S_5 (see [11]) arises further interest in the study of secure MPC over non-Abelian groups. Following the trend, we are interested in secure MPC of circuits over a finite non-Abelian group (G, \cdot) , where the group operations are performed by the circuit gates. These circuits are aptly named G -circuits. Our focus is limited to protocols that only require black-box access to G . This means that the only operations performed by the parties are group multiplication, group inverse and sampling a random element of the group.

Secure MPC over Abelian groups is easily realized through a well-known black-box protocol that uses only two rounds, based on the notion of homomorphic secret-sharing schemes [6]. It is secure against t passive (or equivalently, semi-honest) parties out of n , where t can be any number less than n . The communication complexity of the construction is $O(n^2)$ group elements. A homomorphic secret-sharing scheme has the property that if $\mathbf{v} = (v_1, v_2, \dots, v_n)$ is a vector of shares of the secret $s \in G$, and $\mathbf{w} = (w_1, w_2, \dots, w_n)$ is the corresponding share vector of another secret $s' \in G$, then the product vector $(v_1 \cdot w_1, v_2 \cdot w_2, \dots, v_n \cdot w_n)$ is the share vector of the secret $s \cdot s'$. In other words, just by knowing the individual shares of the two vectors the product of the two secrets can be computed. The MPC protocol based on such a scheme then works as follows. Each of the n -parties holds a unique input from the vector (x_1, x_2, \dots, x_n) . The goal is to securely compute the product of the inputs. In the first round, each party computes n shares of its input x_i and sends a unique share to each of the n parties. In the second round each party computes the product of all the n shares received from the parties. By the homomorphic property the computed product is a share vector for the product $x_1 \cdot x_2 \cdots x_n$ which can then be computed by the parties.

As soon as one enters the realm of non-Abelian groups the above construction fails. This is not surprising as it was shown that there is no homomorphic construction for the non-Abelian case [12]. Until recently, only non-black-box approaches for MPC of G -circuits over non-Abelian groups were known. But these constructions incur efficiency penalties, which we shall elaborate further while discussing related work. Note that unlike the setting of Abelian groups, a t -private protocol over a non-Abelian group should have an honest majority, i.e., $t < \frac{n}{2}$ (see [3]). A recent work from Desmedt et al. [11] showed for the first time the construction of black-box MPC of G -circuits over non-Abelian groups under the passive adversarial model. They reduce the problem of t -private n -party MPC protocol to a graph coloring problem over planar graphs. The result is a notion of t -reliable n -coloring of a planar graph which is secure against an adversarial access of any t -color subset I of the n colors. The first of the three constructions of graph colorings described in [11] is optimal, i.e., it can be used for any $t < \frac{n}{2}$, but only at the expense of exponential communication (construction) and round complexity;

$O(\binom{2t+1}{t}^2)$ and $O(\binom{2t+1}{t})$, respectively.¹ The same construction is used recursively to obtain a protocol that achieves polynomial complexity of construction for any $t \in O(n^{1-\epsilon})$ where ϵ is any positive constant. Notice that polynomial complexity is achieved here at the cost of optimality. The last construction is probabilistic and achieves optimal resilience, i.e., $t < \frac{n}{2}$, while maintaining polynomial construction complexity. By adjusting t , the complexity can be reduced to as low as $O(t^2)$ where $t \leq \frac{n}{2+\epsilon}$ for any positive constant ϵ .

In this paper we show a *deterministic* construction of a t -reliable n -coloring of planar graphs that is optimal ($t < \frac{n}{2}$) under the passive adversarial model with a subexponential complexity of construction $O(t^{2 \cdot \log_2 t})$. Unlike [11] where specific coloring constructions were given for small values of t , our construction is applicable to arbitrary t .

2 Related work

In accordance with the theme of the paper, our treatment of related work is restricted to t -private protocols for G -circuits over non-Abelian groups. The aforementioned non-black-box approach for constructing such protocols for any $t < \frac{n}{2}$ comprises of two methods, both based on Shamir's t -of- n secret-sharing scheme. The first method [3, 4] represents the G -circuit as a Boolean circuit and then uses Shamir's t -of- n secret sharing scheme over the field $\text{GF}(p)$ for some prime $p > 2t + 1$. The communication complexity of this protocol is $O(t^2 \log t)$, including a multiplicative factor equal to the number of AND gates. Due to its dependence on the number of AND gates of the circuit, the protocol is only efficient for a small circuit, and hence a small group G . Some later improvements on this bound have been achieved (cf. [8, 9]) but the communication complexity is still linearly dependent on the number of AND gates.

The second approach [1, 7] represents the G -circuit as an arithmetic circuit over a finite ring R . Shamir's secret-sharing scheme generalized to any finite ring is then used to complete the construction. The communication complexity of this protocol is $O(t^2 \log t \cdot N_M(C) \cdot l(R))$. Here $N_M(C)$ is the number of multiplications in the representation of the G -circuit over the ring R and $l(R)$ is the number of bits required to represent the elements of the ring, which satisfies $l(R) \geq \log |R|$. For a generic ring R , if the group G is 'embedded' in the ring so that the multiplication operation in R is the same as G , $l(R)$ is as big as $|G|$, i.e., the communication complexity is linearly dependent on the number of elements in G .

¹ For the sake of clarity a multiplicative factor, which represents the size of the G -circuit, is not shown in these and ensuing complexity measures.

To the best of our knowledge, the first constructions of black-box MPC of G -circuits over non-Abelian groups were shown in [11], where three different constructions are illustrated. The idea behind the constructions is to reduce the problem of constructing a t -private n -party MPC protocol to a t -reliable n -coloring of planar graphs. Informally, this means that if the adversary is in possession of a random t color subset I , then the graph is not blocked in the sense that there is at least one path from the inputs to the outputs that does not contain any element from I . The constructions in [11] are therefore illustrations of t -reliable n -colorings of planar graphs. Central to the constructions is a square planar graph $\mathcal{G}_{\text{tri}}(l, l)$ whose t -reliable n -coloring is demonstrated. Here the parameter l represents the number of x (left) and y (right) input nodes which is the same for a square graph. The first construction achieves optimal resilience with $t < \frac{n}{2}$ but at the cost of exponential complexity of construction, i.e., $l = \binom{n}{t}$. Recursive use of this construction leads to a construction with polynomial complexity but in which t is not a constant fraction of n . More specifically, the second construction requires $t = O(n^{1-\epsilon})$ for some positive constant ϵ . The third construction is probabilistic and simply assigns a random color from 1 to n to each node of the square graph $\mathcal{G}_{\text{tri}}(l, l)$. This probabilistic construction achieves optimal resilience while maintaining polynomial communication (construction) complexity.

Recently, Cohen et al. [5] have independently shown a construction of secure MPC over black-box non-Abelian groups in the passive model that achieves the asymptotically optimal bound of $\frac{1}{2} - \Omega(\frac{1}{n})$. The complexity of their construction is $n^{O(\log n)}$ which compares well with our construction. However, their construction is based on logarithmic depth threshold formulae as opposed to our construction which is based on graph coloring of non-planar graphs. Cohen et al. also show two polynomial time constructions [5]. The first construction is *almost* optimal, shying away from the optimal bound. More precisely it is secure against $\frac{1}{2} - 2^{-O(\sqrt{\log n})}$ fraction of passively corrupted parties. The second polynomial time construction achieves the asymptotically optimal bound described above, but only under the assumption of the so-called majority from majorities conjecture. Loosely speaking, this conjecture states the existence of a polynomial time algorithm in n , with n an odd integer, which generates a formula on n inputs of logarithmic depth, which consists only of 3-input majority gates (and no constants) and computes the majority function on n inputs [5]. At the time of this writing, no such algorithm is known.

Active adversaries. Although the focus of this paper is on security against a passive adversary, we nevertheless briefly describe the work on MPC over black-box non-Abelian groups in the active model for the sake of completeness. The first secure protocol under an active attack model was shown by Desmedt et al.

in [10]. The protocol is optimal in the sense that it satisfies the Q^3 property, which means that the adversary structure Δ does not contain any three subsets of players, the union of which is the entire set of players. Notice that this condition is necessary to achieve active security [13]. The construction from Desmedt et al. is quadratic in the number of maximal sets in the adversary structure Δ , which in general can be exponential in the number of players n . Recently, Cohen et al. [5] have improved on that result by showing a construction based on threshold formulae of logarithmic depth which is *almost* optimal, i.e., is secure against an active adversary that controls at most $\frac{1}{3} - \Omega(\frac{1}{\sqrt{\log n}})$ players.

3 Preliminaries, notations and definitions

Before proceeding to our construction of a t -reliable n -coloring of a planar graph, we recall some results from [11] which establish the link between secure MPC over G -circuits and t -reliable n -coloring of certain graphs. To this end, it is first shown in [11] that the problem of constructing t -private n -party MPC protocols over G -circuits can be reduced to the problem of constructing a t -private subprotocol for an n -party shared 2-product function, where the two inputs and the solitary output of this function are shared among the parties. In the second step, it is shown how to reduce the problem of a shared 2-product subprotocol to the problem of finding a t -reliable n -coloring of planar graphs. The details of these reductions together with the definitions of these terms can be found in [11]. For the sake of this paper, we shall restrict our scope to constructing t -reliable n -colorings of planar graphs, and take the results from [11] for granted which show how these constructions suffice to realize secure MPC over G -circuits. Notice that a separate result from [11] shows the reduction from MPC over arbitrary Boolean circuits to MPC over G -circuits using Barrington's result [2]. Thus, the construction shown here, and the ones described in [11], can be used for general secure MPC.

As already mentioned, in this paper we are going to study graph coloring structures. The underlying mathematical object of interest is a planar directed acyclic graph (PDAG) for which we have two well defined collections of nodes. The first one contains all input nodes (source) and the second collection comprises of all output nodes (sink). These two collections correspond to the players of an MPC protocol that receive the inputs and outputs. Each node in the graph is assigned a label (color) which indicates the player doing the computation. The edges represent elements of the group G that are transmitted to other players. The computation at each node is multiplication of group elements from all incoming edges, and resharing of the product using a k -of- k secret-sharing scheme along the outgoing edges. The k -of- k secret-sharing scheme follows from the following amended proposition from [11]:

Proposition 3.1. *Let (G, \cdot) be a finite group, and fix an element $g \in G$. Further fix integers k and $j \in [k]$. If $k - 1$ shares $\{s_g(i)\}_{i \in [k] \setminus \{j\}}$ are sampled uniformly and independently at random from G , and $s_g(j)$ is obtained as the unique element of G such that $g = s_g(1) \cdot s_g(2) \cdots s_g(k)$, then $(s_g(1), s_g(2), \dots, s_g(k))$ is a k -of- k sharing of g .*

We are now ready to precisely characterize the PDAGs relevant to our study.

Definition 3.2. A graph \mathcal{G} with set of nodes \mathcal{V} is called *triangle PDAG* if the following properties hold:

- The input and output nodes create a triangle. The sides of the triangle contain input nodes. The set \mathcal{L} includes all input nodes from the left-hand side, and the set \mathcal{R} all input nodes from the right-hand side. The base of the triangle, denoted by the set \mathcal{B} , is created by the output nodes.
- The intersection of the sets \mathcal{L} and \mathcal{R} consists of a single node (it can receive input from left and right).
- The intersections $\mathcal{L} \cap \mathcal{B}$ and $\mathcal{R} \cap \mathcal{B}$ contain single nodes that play double role of input and output nodes.
- $\mathcal{V} \supseteq \{\mathcal{L} \cup \mathcal{R} \cup \mathcal{B}\}$.

Note that the definition does not provide any details about the internal structure of the graph \mathcal{G} . The aim of this paper is to provide details about it.

Definition 3.3. A graph \mathcal{RG} over the set of nodes \mathcal{V} is called *rectangle PDAG* if the following properties hold:

- The input and output nodes create a rectangle. The input nodes are inserted on the top and the right-hand side of the rectangle and the sets of nodes are \mathcal{T} and \mathcal{R} , respectively. The output nodes create the left-hand side and the bottom of the rectangle. The sets of nodes are denoted by \mathcal{L} and \mathcal{B} , respectively.
- The nodes $\mathcal{T} \cap \mathcal{L}$ and $\mathcal{B} \cap \mathcal{R}$ play double role of input and output nodes.
- $\mathcal{V} \supseteq \{\mathcal{L} \cup \mathcal{R} \cup \mathcal{B} \cup \mathcal{T}\}$.

Definition 3.4. The function $C : \mathcal{V} \rightarrow [n]$ is a t -reliable n -coloring for triangle PDAG \mathcal{G} over the set of nodes \mathcal{V} if for each t -color subset $I \subset [n]$, there are three nodes $\{\ell, r, b\}$ such that

- $\ell \in \mathcal{L}, r \in \mathcal{R}$ and $b \in \mathcal{B}$ and $\{C(\ell) \cup C(r) \cup C(b)\} \cap I = \emptyset$;

- there is a path PATH_b^ℓ in \mathcal{G} from the input node $\ell \in \mathcal{L}$ to the output node $b \in \mathcal{B}$, such that none of the nodes in the path has a color in the subset I (the path is called I -avoiding);
- there is a path PATH_b^r in \mathcal{G} from the input node $r \in \mathcal{R}$ to the output node $b \in \mathcal{B}$, such that none of the nodes in the path has a color in the subset I .

Definition 3.5. The function $C : \mathcal{V} \rightarrow [n]$ is an (h, v) -reliable n -coloring for a rectangle PDAG \mathcal{RG} over the set of nodes \mathcal{V} , if

- for each h -color subset $I \subset [n]$, there are two nodes $\ell \in \mathcal{L}$ and $r \in \mathcal{R}$ such that there is a (horizontal) I -avoiding path PATH_ℓ^r from r to ℓ ;
- for each v -color subset $J \subset [n]$, there are two nodes $t \in \mathcal{T}$ and $b \in \mathcal{B}$ such that there is a (vertical) J -avoiding path PATH_b^t from t to b .

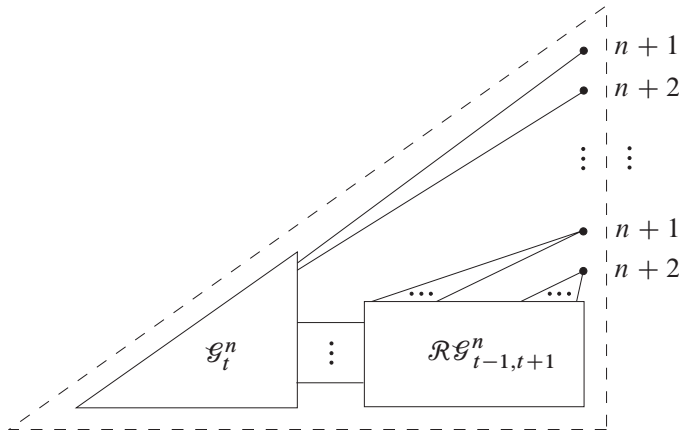
4 Overview of the constructions

Our construction shows how to build a family of triangle PDAG \mathcal{G}_{t+1}^{n+2} for which the corresponding $(t+1)$ -reliable $(n+2)$ -coloring exists, where $n = 2t+1$. The construction is recursive and uses the following two building blocks:

- a triangle PDAG \mathcal{G}_t^n with t -reliable n -coloring, and
- a rectangle PDAG $\mathcal{RG}_{(t-1, t+1)}^n$ with $(t-1, t+1)$ -reliable n -coloring, i.e., the rectangle graph provides a horizontal I -avoiding path as long as $|I| \leq t-1$ and a vertical I -avoiding path if $|I| \leq t+1$. Horizontal and vertical paths exist simultaneously if $|I| \leq t-1$. Note that only vertical paths exist if $|I| \in \{t, t+1\}$.

Note that apart from the two basic components \mathcal{G}_t^n and $\mathcal{RG}_{t-1, t+1}^n$, the construction applies a collection of vertices colored by either $(n+1)$ or $(n+2)$. Also, the coloring of the component graph $\mathcal{RG}_{t-1, t+1}^n$ uses the two additional ‘helper’ colors $n+1$ or $n+2$, in addition to the colors from $[n]$, but the analysis only requires the existence of paths for $I \in [n]$. All these components are depicted in Figure 1. Each vertex of the right-hand side of \mathcal{G}_t^n is connected to two vertices with colors $(n+1)$ and $(n+2)$. Assume that the set I consists of $(t+1)$ colors. The construction has to provide I -avoiding paths for the following three cases:

- Case 1: $|I \cap \{n+1, n+2\}| = 0$. This also means that the graph \mathcal{G}_t^n is blocked. However, an I -avoiding path can be constructed using the very top vertex with color $(n+2)$ (that accepts two inputs from left and right) and goes through all vertices with colors $(n+1)$ and $(n+2)$. The path also passes through the rectangle graph $\mathcal{RG}_{t-1, t+1}^n$, which supplies a vertical I -avoiding path within the component.

Figure 1. Construction of \mathcal{G}_{t+1}^{n+2} .

- Case 2: $|I \cap \{n+1, n+2\}| = 1$. The graph \mathcal{G}_t^n provides the $I \setminus \{n+1, n+2\}$ -avoiding path within itself. We will show that the right-hand path can be extended by using either one of the nodes with color $\{n+2, n+1\}$ or by using the rectangle graphs.
- Case 3: $|I \cap \{n+1, n+2\}| = 2$. The right-hand vertices with colors $(n+1)$ and $(n+2)$ are blocked. An I -avoiding path is going to be created from I -avoiding paths that exist in both \mathcal{G}_t^n and the copies of $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$.

The crux of the construction is the rectangle graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$ that extends the I -avoiding paths vertically and horizontally.

Figure 2 depicts the overall structure of the graph, assuming $n \equiv 1 \pmod{4}$, i.e., $n = 4t + 1$ colors for some $t \in \mathbb{N}$. Notice that this essentially means that t is a power of 2. The structure uses

- Triangle graphs \mathcal{G}_{t-1}^{2t-1} to facilitate the horizontal avoiding paths.
- Rectangle graphs $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$ and $\mathcal{R}\mathcal{G}_{t-1,t}^{2t}$. The second graph has one color less than the first. This is caused by the fact that the odd integer n cannot be split into halves.
- Two groups of vertices colored with $(n+1)$ or $(n+2)$. Figure 2 shows the color $(n+1)$. An important observation is that both colors $(n+1)$ and $(n+2)$ are not used in horizontal paths. They provide vertical avoiding paths in $\mathcal{R}\mathcal{G}_{2t-1,2t+1}^{4t+1}$.
- Two *bridging nodes* labelled b_1 and b_2 which connect two vertically adjacent copies of \mathcal{G}_{t-1}^{2t-1} .

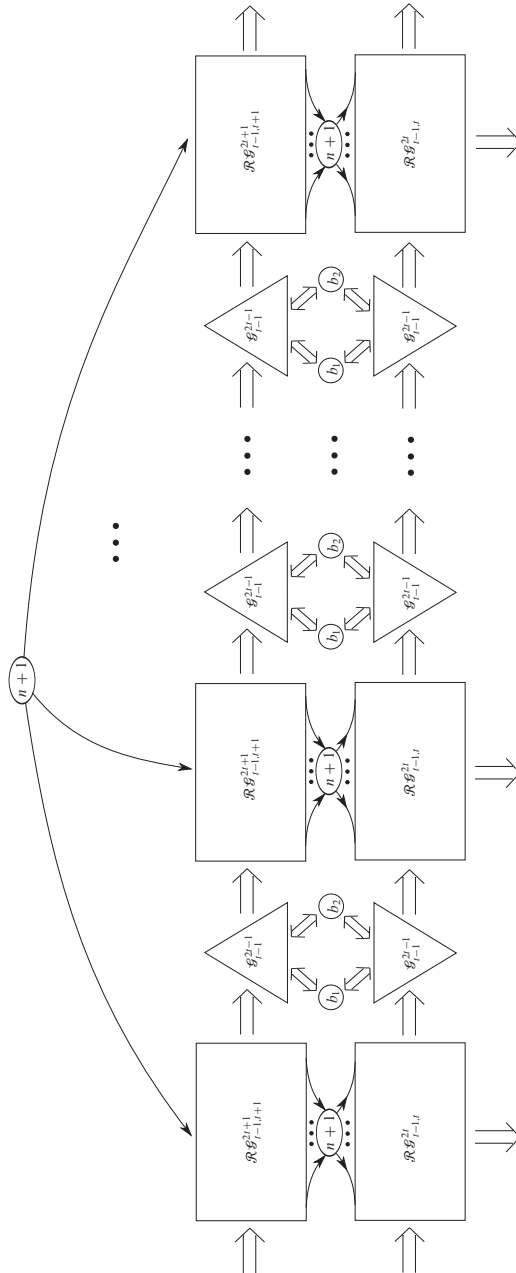
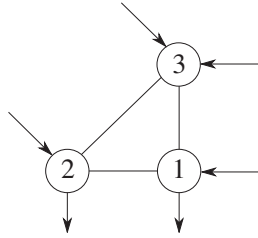


Figure 2. Generic construction of $\mathcal{RG}_{2t-1, 2t+1}^{4t+1}$. Figure 90° counter-clockwise rotated.

Figure 3. 1-reliable 3-coloring graph \mathcal{G}_1^3 .

As noted above, the above construction assumes that t is a power of 2 for some $t \in \mathbb{N}$. In the following section, we shall show the construction of rectangle graphs assuming t to be a power of 2. This enables us to show the construction of the graphs $\mathcal{RG}_{t-1,t+1}^{2t+1}$, $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$, $\mathcal{RG}_{4t-1,4t+1}^{8t+1}$, \dots in a straightforward manner. In case t is not a power of 2, the construction of $\mathcal{RG}_{t-1,t+1}^{2t+1}$ is somewhat different, which is explained in Appendix A.

5 Building elements

Triangle and rectangle graphs are relatively simple for small parameters n and t . For $n = 1$ and $t = 0$, the triangle graph \mathcal{G}_0^1 is a single vertex with color 1. For $n = 3$ and $t = 1$, the graph \mathcal{G}_1^3 with 1-reliable 3-coloring is shown in Figure 3. The structure of 2-reliable 5-coloring graph \mathcal{G}_2^5 is illustrated in Figure 4. It is built from a triangle graph \mathcal{G}_1^3 which is 1-reliable 3-coloring and a rectangle graph $\mathcal{RG}_{0,2}^3$ which is $(0, 2)$ -reliable 3-coloring. The rectangle graph $\mathcal{RG}_{0,2}^3$ is the smallest that can be defined. It allows a horizontal I -avoiding path only if $|I \cap \{1, 2, 3\}| = 0$. A vertical I -avoiding path in $\mathcal{RG}_{(0,2)}^3$ exists if $|I \cap \{1, 2, 3\}| = 2$.

The graphs can be made symmetric by using *mirror tricks*. An example is shown in Figure 5. The structure consists of two copies of the same graph, where one is a vertical reflection of the other. If we apply the trick once again but flipping the structure horizontally, we will get a graph that is fully symmetric that has the same number of inputs and outputs.

5.1 Analysis of rectangle graphs $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$ for vertical paths

Let us start from the simplest rectangle graph $\mathcal{RG}_{1,3}^5$ that can be built from \mathcal{G}_0^1 and $\mathcal{RG}_{0,2}^3$. The overall structure is shown in Figure 6. The rectangle graph $\mathcal{RG}_{0,1}^2$ is a modified copy of $\mathcal{RG}_{0,2}^3$, where one color is removed (or equivalently duplicated). This obviously means that the vertical paths in it can be blocked by the two vertices. The triangle graphs \mathcal{G}_0^1 are replaced by bullet points (but could be

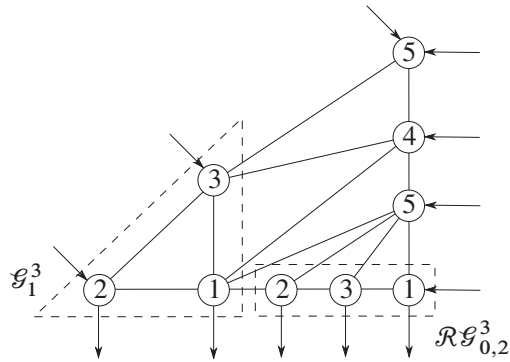


Figure 4. A 2-reliable 5-coloring graph \mathcal{G}_2^5 .

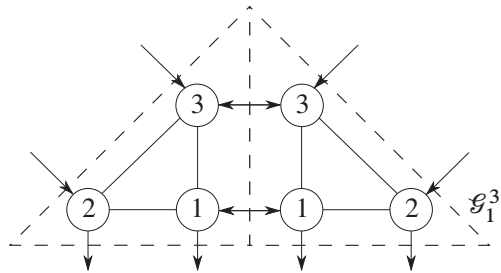


Figure 5. Mirror trick for \mathcal{G}_1^3 .

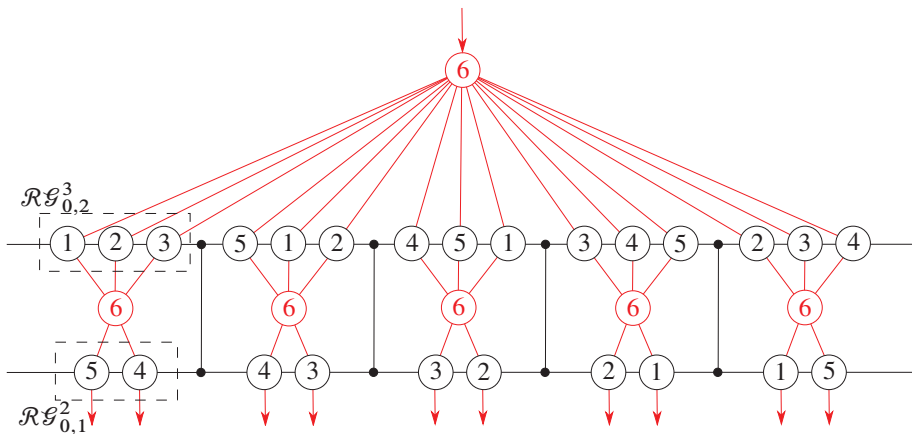


Figure 6. Rectangle graph $\mathcal{R}\mathcal{G}_{1,3}^5$.

replaced by a single vertex from either left or right side). One of the purposes of $\mathcal{RG}_{1,3}^5$ is to provide at least one vertical path from a top vertex with the color 6 that passes through the graph and ends up at one of the outputs (in red).

We claim that the graph $\mathcal{RG}_{1,3}^5$ provides at least one vertical I -avoiding path as long as $|I \cap [5]| = 3$. To prove this we need to consider all possible cases for the set I . There are $\binom{5}{3} = 10$ such subsets. For instance, if $I = \{1, 4, 5\}$, there is an I -avoiding path that starts from the top 6, 2, 6, 3 (in the second subgraph from the left) ending at the 3rd output (from the left). Note that there are 5 components $(\mathcal{RG}_{0,2}^3, \mathcal{RG}_{0,1}^2)$ and each pair is defined for vertices with 5 colors. The collection of colors in each component is a simple “rotation” of colors between the pairs.

Now we are ready to consider the vertical paths in the generic construction from Figure 2. We assume that the construction of $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$ consists of exactly $n = 4t + 1$ copies of $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$ connected by appropriate copies of \mathcal{G}_{t-1}^{2t-1} . We assume that for each component $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$, we split colors by a simple rotation of colors, i.e.,

- the first component $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$ gets assigned the colors

$$A_1 = \{1, 2, \dots, 2t + 1\} \quad \text{and} \quad B_1 = \{2t + 2, \dots, 4t + 1\},$$

respectively,

- the i -th component $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$ gets the colors A_i and B_i by rotating the colors as shown in Figure 7.

Theorem 5.1. *Given the rectangle graph $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$ built from n components $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$ and connected by the triangle graphs as shown in Figure 2. Assume that each component $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$ is assigned the sets of colors (A_i, B_i) as described in Figure 7. Then for an arbitrary I with $|I| \leq 2t + 1$, there is a vertical I -avoiding path in $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$.*

Proof. Assume we have a set I of $(2t + 1)$ colors that needs to be avoided. To create a path that avoids I , we need to find a component $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$ with (A_i, B_i) such that

$$|I \cap A_i| = t + 1 \quad \text{and} \quad |I \cap B_i| = t. \quad (5.1)$$

To see that this is possible, consider the ring of colors in Figure 7. We put the colors from the set I on the ring in their positions and then rotate the ring (or move from (A_i, B_i) to (A_{i+1}, B_{i+1})) until there is such pair which satisfies conditions (5.1). Note that this can always be done as a single step in rotation (move from (A_i, B_i) to (A_{i+1}, B_{i+1}) may increase or decrease the numbers in the intersections by 1). As the rotation is cyclic, there must be a pair of subsets (A_i, B_i) that contain the required number of colors of the vertical I -avoiding path. \square

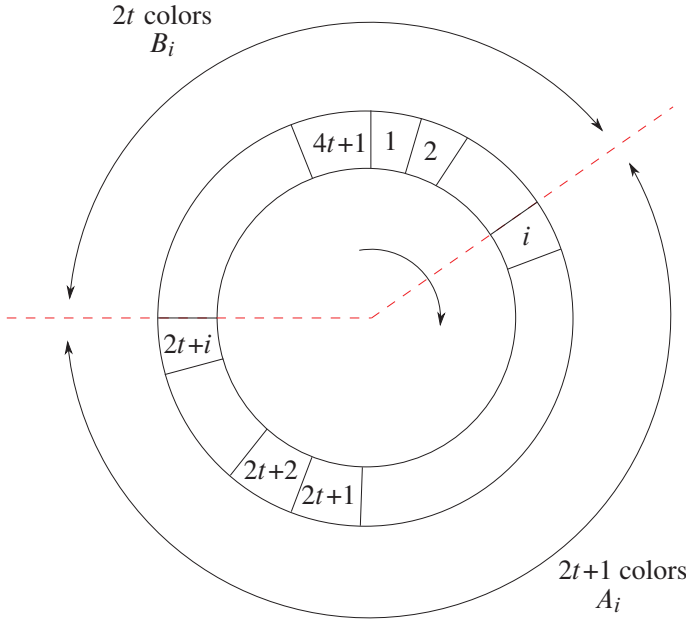


Figure 7. Assignment of colors to components $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,2t}^{2t})$.

5.2 Analysis of rectangle graphs $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$ for horizontal paths

We have proved that the rectangle graph $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$ provides vertical I -avoiding paths as long as $|I| \leq 2t + 1$ and it has to have $n = 4t + 1$ components $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,2t}^{2t})$. Now we have to show that $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$ permits horizontal I -avoiding paths as long as $|I| \leq 2t - 1$.

We start from the simplest case when $t = 1$ that is illustrated in Figure 6. To avoid confusion, the graph $\mathcal{RG}_{1,3}^5$ is redrawn without the vertices with the color $(n + 1) = 6$ in Figure 8. Note that the vertices with the color 6 are used to provide vertical paths only. It is easy to check that for all sets I with a single color, there is a horizontal path.

For $t = 2$, the rectangle graph $\mathcal{RG}_{3,5}^9$ consists of 9 copies of $(\mathcal{RG}_{1,3}^5, \mathcal{RG}_{1,2}^4)$, and enough copies of the triangle graph \mathcal{G}_1^3 to provide connections. The graph $\mathcal{RG}_{3,5}^9$ is shown in Figure 9.

Note also that the collection of colors for copies of \mathcal{G}_1^3 is chosen in such a way that the colors are present in both the left and right-hand side copies of the rectangle graphs. A justification for this choice is that this component can be blocked only if both copies of the rectangle graphs are blocked. The vertically adjacent

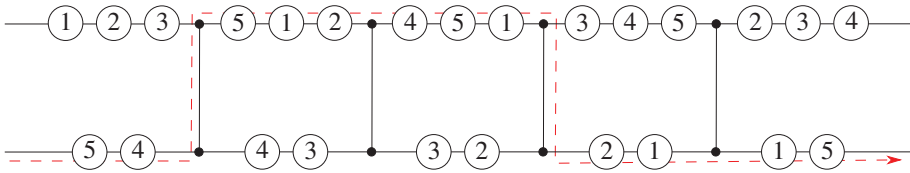


Figure 8. Rectangle graph $\mathcal{R}\mathcal{G}_{1,3}^5$ with a horizontal path in red that avoids $I = \{3\}$.

copies of \mathcal{G}_1^3 are connected via the bridging nodes. These nodes are assigned the two colors that are *swapped* between the diagonally adjacent rectangle graphs. For instance, in the first component in Figure 9, the colors 1 and 6 have been swapped between the two pairs of diagonal rectangle graphs ($\mathcal{R}\mathcal{G}_{1,3}^5$ and $\mathcal{R}\mathcal{G}_{1,2}^4$). These are then assigned to the bridging nodes. Notice that the triangle graph \mathcal{G}_1^3 has three nodes in its base (obtained using the mirror trick). The left (resp. right) bridging node connects with the two nodes in the base of the left (resp. right) image of the triangle graph \mathcal{G}_1^3 . This is made explicit in Figure 10, where a segment of the rectangle graph $\mathcal{R}\mathcal{G}_{3,5}^9$ is shown. As we shall see next, the vertical path through the triangle graphs is only used when exactly one of the two colors assigned to the bridging nodes is blocked. Thus, this connection ensures that the path between the two triangle graphs is not blocked when used for vertical traversing.

To prove that there is a horizontal I -avoiding path, where $|I| = 3$, it is enough to enumerate all possible subsets of 3 elements out of 9. There are $\binom{9}{3} = 84$ such cases. However, there is a better way to prove. This method can also be naturally extended for the general case. Because the structure is regular, it is enough to analyze transition of paths between two neighboring components as shown in Figure 11. Let I with $|I| = 3$ be an arbitrary set that needs to be avoided. The set splits in a natural way into two subsets $I_{A_1} = I \cap A_1$ and $I_{B_1} = I \cap B_1$ for the first component and also for the second one, i.e., $I_{A_2} = I \cap A_2$ and $I_{B_2} = I \cap B_2$. Let us have a closer look at the colors 1 and 6 that are switched between sets, the color 1 goes from A_1 to B_2 and 6 goes from B_2 to A_2 . There are the following four possibilities:

- The colors $1 \notin I$ and $6 \notin I$. Nothing is changing and the appropriate horizontal path can be extended (i.e., if the graph with colors from A_1 is blocked, then the graph with colors from A_2 is also blocked. Alternatively, if the graph with colors A_1 provided the horizontal avoiding path, then the graph with A_2 extends the path).
- The colors $1 \in I$ and $6 \in I$. The elements from I were swapped and the rectangle graphs provide an avoiding path by corresponding rectangle graphs.

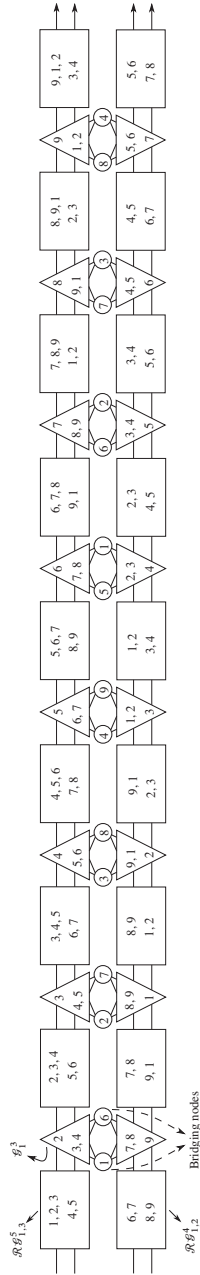


Figure 9. Rectangle graph $\mathcal{RG}_{3,5}^9$ without vertical nodes. Figure 90° counter-clockwise rotated.

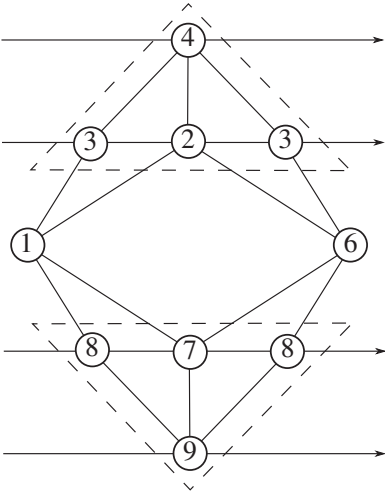


Figure 10. The vertical connection between two copies of the triangle graphs \mathcal{G}_1^3 via the bridging nodes 1 and 6 in $\mathcal{RG}_{3,5}^9$.

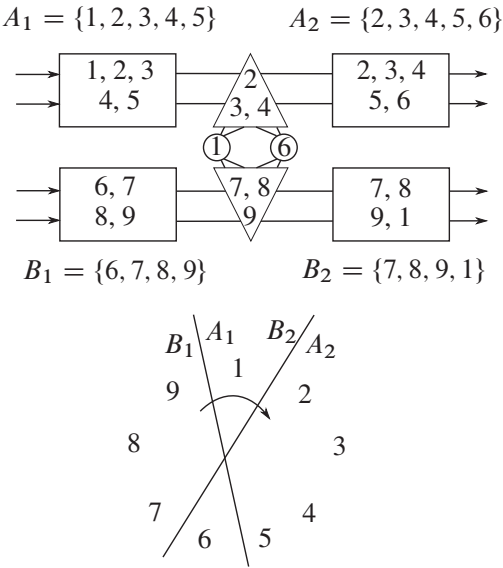


Figure 11. Two consecutive pairs of rectangle graphs.

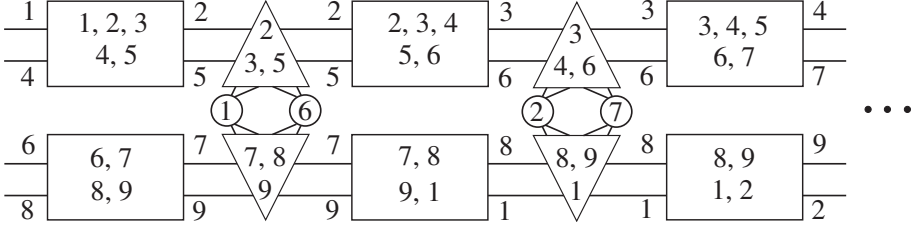


Figure 12. Assignment of colors to inputs and outputs in first few components of $\mathcal{RG}_{3,5}^9$.

- The colors $1 \in I$ and $6 \notin I$. This also means that $|I_{A_2}| = |I_{A_1}| - 1$ and $|I_{B_2}| = |I_{B_1}| + 1$. The switch between two rectangle graphs happens if the top graph with colors A_1 was blocked by two colors (i.e., $|I_{A_1}| = 2$) as the graph with colors from A_2 is now providing horizontal avoiding path as $|I_{A_2}| = 1$. Clearly the graph with colors B_2 has been blocked. For example, assume that $I = \{1, 2, 7\}$, the graph \mathcal{RG}_{A_1} is blocked and \mathcal{RG}_{B_1} provides a horizontal avoiding path. The graph \mathcal{RG}_{A_2} extends the avoiding path (via the copies of \mathcal{G}_1^3) while \mathcal{RG}_{B_2} is blocked. Thus, a vertical transition has to be made through the triangle graphs. Since the bridging node with color 1 is blocked, the transition between the two triangle graphs is provided by the bridging node with color 6. Note however that the switch will not happen if $|I_{A_1}| = 3$ as the graph with colors from A_2 is blocked.
- The colors $1 \notin I$ and $6 \in I$. This case is similar to the previous one.

We did not consider how the rectangle graphs are to be connected to triangle graphs \mathcal{G}_1^3 . This can be done by taking 3 vertices with colors from the intersection between the colors of the neighboring rectangle graphs. The assignment of colors to inputs and outputs for a part of the graph $\mathcal{RG}_{3,5}^9$ is given in Figure 12. Note that the triangle graphs \mathcal{G}_1^3 have the same colors on both sides. This can be done using the mirror trick. The top and bottom copies of \mathcal{G}_1^3 are connected via the bridging nodes each one of which is connected to two of the three nodes in the base of the triangle graphs (this is the result of the mirror trick); see Figure 10.

Consider the general case for horizontal avoiding paths in $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$ for $n = 4t + 1$, as shown in Figure 13. The vertices with the color $n + 1 = 4t + 2$ are not shown as they are used in vertical avoiding paths only. The graph $\mathcal{RG}_{2t-1,2t+1}^{4t+1}$ applies n copies of pairs $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$ that are connected by appropriate copies of the graph \mathcal{G}_{t-1}^{2t-1} ; see Figure 2. The copies $(\mathcal{RG}_{t-1,t+1}^{2t+1}, \mathcal{RG}_{t-1,t}^{2t})$ are labelled by the colors (A_i, B_i) ; $i = 1, \dots, n$. The following colors are assigned

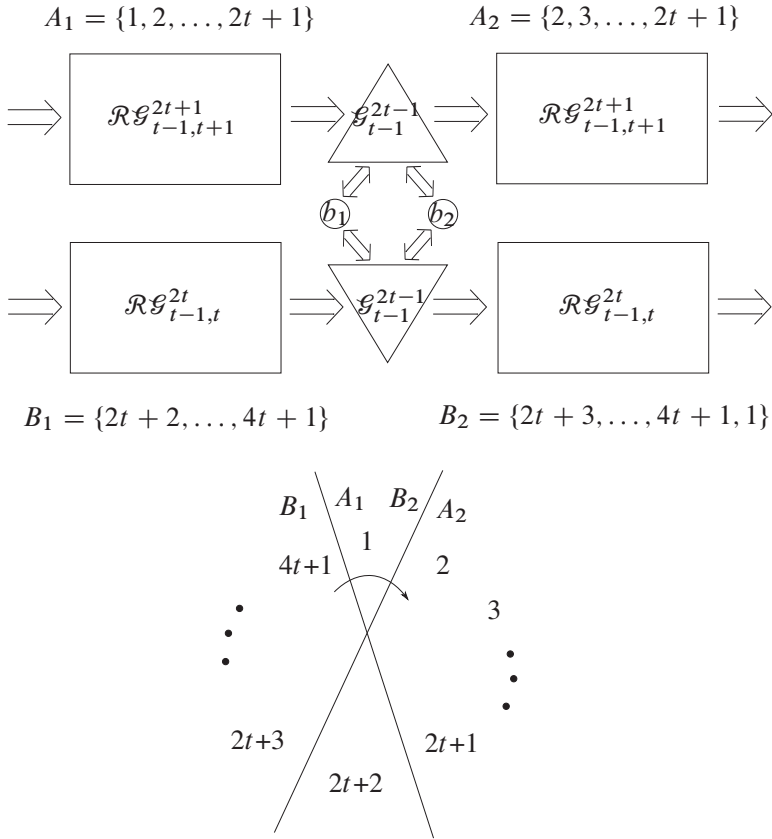


Figure 13. Two first components of the graph $\mathcal{RG}_{2t-1, 2t+1}^{4t+1}$.

to the pair (A_1, B_1) :

$$A_1 = \{1, \dots, 2t+1\} \quad \text{and} \quad B_1 = \{2t+2, \dots, 4t+1\},$$

and the pair (A_i, B_i) is obtained from (A_{i-1}, B_{i-1}) by rotation of colors by one; see Figure 13. Without loss of generality, we consider the horizontal paths between two components shown in Figure 13. Given an arbitrary set I with $|I| = 2t-1$ that needs to be avoided. The set splits in a natural way into two subsets $I_{A_1} = I \cap A_1$ and $I_{B_1} = I \cap B_1$ for the first component and also for the second one, i.e., $I_{A_2} = I \cap A_2$ and $I_{B_2} = I \cap B_2$. Let us have a closer look at the colors 1 and $2t+2$ that are switched between sets, the color 1 goes from A_1 to B_2 and $2t+2$ goes from B_1 to A_2 . There are the following four possibilities:

- The colors $1 \notin I$ and $2t + 2 \notin I$. Nothing is changing and the appropriate horizontal path can be extended (i.e., if the graph with colors from A_1 is blocked, then the graph with colors from A_2 is also blocked. Alternatively, if the graph with colors A_1 provided the horizontal avoiding path, then the graph with A_2 extends the path).
- The colors $1 \in I$ and $2t + 2 \in I$. The elements from I were swapped. If there is an avoiding path in the graphs $(\mathcal{RG}_{A_1}, \mathcal{RG}_{B_1})$, then it can be extended in the graphs $(\mathcal{RG}_{A_2}, \mathcal{RG}_{B_2})$.
- The colors $1 \in I$ and $2t + 2 \notin I$. This also means that $|I_{A_2}| = |I_{A_1}| - 1$ and $|I_{B_2}| = |I_{B_1}| + 1$. The switch between two rectangle graphs happens if the top graph with colors A_1 is blocked by t colors (i.e., $|I_{A_1}| = t$) and the bottom graph with colors B_1 provides a horizontal avoiding path (as $|I_{B_1}| = t - 1$). The graph with colors from A_2 provides a horizontal avoiding path as $|I_{A_2}| = t - 1$. Clearly the graph with colors B_2 has been blocked. The switch is made possible through the triangle graphs via the bridging node with color $2t + 2$. Note however that the switch will not happen if $|I_{A_1}| > t$ as the graph with colors from A_2 remains blocked.
- The colors $1 \notin I$ and $2t + 2 \in I$. This case is similar to the previous one.

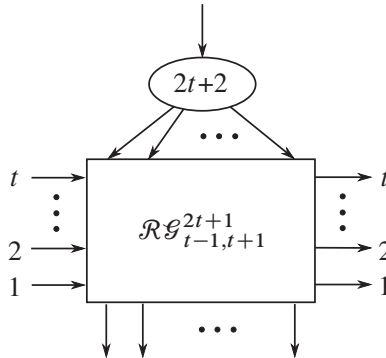
To facilitate the switch the triangle graphs must provide appropriate extension of avoiding paths. Note that the triangle graph between \mathcal{RG}_{A_1} and \mathcal{RG}_{A_2} is labelled by $2t - 1$ colors that are in both sets A_1 and A_2 . This also means that the triangle graph is blocked only if both graphs \mathcal{RG}_{A_1} and \mathcal{RG}_{A_2} are blocked. A similar remark applies for the triangle graph between \mathcal{RG}_{B_1} and \mathcal{RG}_{B_2} .

5.3 Rectangle graphs $\mathcal{RG}_{t-1,t+1}^{2t+1}$ for arbitrary t

The design of the rectangle graphs discussed so far is limited to t being a power of 2. For an arbitrary t , the construction of the rectangle graph $\mathcal{RG}_{t-1,t+1}^{2t+1}$ is slightly different. Appendix A details how to obtain such a rectangle graph. Thus, we assume from now on that we have a rectangle graph $\mathcal{RG}_{t-1,t+1}^{2t+1}$ that is horizontally I -avoiding and vertically J -avoiding as long as $|I| \leq t - 1$ and $|J| \leq t + 1$ and $I, J \subseteq [n]$. The graph is illustrated in Figure 14. Note that horizontal input and output vertices preserve colors by using the mirror trick.

6 Construction for \mathcal{G}_t^{2t+1}

The triangle graph \mathcal{G}_{t+1}^{n+2} for $n = 2t + 1$, where $t = 2, 3, 4, \dots$, is constructed by the following five steps (see Figure 15):

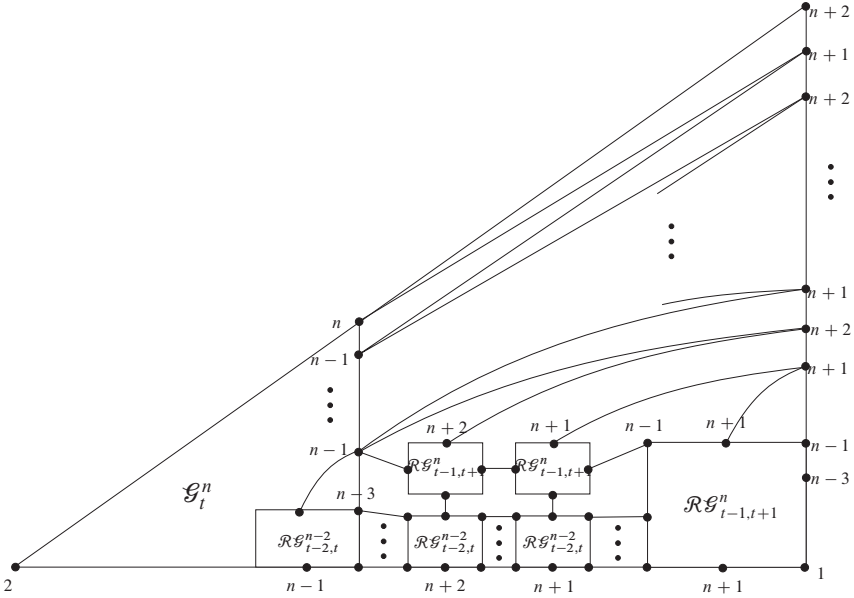
Figure 14. Rectangle graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$.

- Take a triangle graph \mathcal{G}_t^n that is t -reliable n -coloring and a rectangle graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$, where the graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$ is $(t-1, t+1)$ -reliable n -coloring and with the structure as shown on Figure 14. The structure applies three copies of $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$ and two copies of $\mathcal{R}\mathcal{G}_{t-2,t}^{n-2}$.
- A single node (with color $n+2$) is added as the top node of \mathcal{G}_{t+1}^{n+2} . This node belongs to both the top left and right sides of the graph and accepts inputs from both directions.
- The right-hand side of the triangle graph \mathcal{G}_{t+1}^{n+2} consists of a collection of nodes colored alternately by two colors $n+2$ and $n+1$ together with the nodes from the right side of the bottom copy of the rectangle graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$. Each node with colors $\{n, n-1\}$ is connected by two edges to their corresponding nodes of the right side of the triangle graph \mathcal{G}_{t+1}^{n+2} with colors $(n+2)$ and $(n+1)$.
- The rectangle graph that is the component of \mathcal{G}_t^n is connected to its two copies and the last copy is connected to the bottom copy of $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$.
- Two copies of $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$ are used to connect the bottom node of \mathcal{G}_t^n with color $(n-1)$ to the very top of the bottom copy of $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$.

Theorem 6.1. *Given*

- (i) *a rectangle graph $\mathcal{R}\mathcal{G}_{(t-1,t+1)}^n$ that is $(t-1, t+1)$ -reliable n -coloring and*
- (ii) *the triangle graph \mathcal{G}_t^n ,*

the triangle graph \mathcal{G}_{t+1}^{n+2} generated by the recursive construction described above is $(t+1)$ -reliable $(n+2)$ -coloring.

Figure 15. The recursive construction of \mathcal{G}_{t+1}^{n+2} .

Proof. Before we start our proof, we introduce some useful notations. As the construction uses a sequence of related rectangle graphs, we denote by I_t the set of colors that need to be avoided in the graph \mathcal{G}_t^n , where $t = 1, 2, \dots$ and $n = 2t + 1$. Observe that any particular pattern of colors I_t has to satisfy the relation

$$I_1 \subseteq I_2 \subseteq \dots \subseteq I_t \subseteq I_{t+1}.$$

This relation is enforced by the construction.

We have to argue that for an arbitrary set I_{t+1} of $(t + 1)$ colors, where $I_{t+1} \subset [n + 2]$, the graph \mathcal{G}_{t+1}^{n+2} contains three nodes $\ell \in \mathcal{L}$, $r \in \mathcal{R}$ and $b \in \mathcal{B}$ such that the two paths PATH_b^ℓ and PATH_b^r are I_{t+1} -avoiding. We consider three possible cases for the set I_{t+1} , namely

- (i) $|I_{t+1} \cap [n]| = t + 1$ and $|I_{t+1} \cap \{n + 1, n + 2\}| = 0$,
- (ii) $|I_{t+1} \cap [n]| = t$ and $|I_{t+1} \cap \{n + 1, n + 2\}| = 1$,
- (iii) $|I_{t+1} \cap [n]| = t - 1$ and $|I_{t+1} \cap \{n + 1, n + 2\}| = 2$.

The proof proceeds by induction. It is easy to verify that the triangle \mathcal{G}_1^3 is 1-reliable 3-coloring. It takes a bit more effort (by trivial exhaustive search) to establish that the triangle \mathcal{G}_2^5 is 2-reliable 5-coloring.

The induction step: we assume that the triangle \mathcal{G}_t^n is t -reliable n -coloring and that the rectangle graphs are providing appropriate horizontal and vertical avoiding paths. Assume that the set I_{t+1} contains $t + 1$ colors taken from the set $[n + 2]$. We also assume that \mathcal{G}_t^n has the following property:

Property A. If $|I_t| \leq t$ and the colors $n - 1$ and n are not both in I_t , then there exists an I_t -avoiding path in \mathcal{G}_t^n that enters via one of the input nodes of color $n - 1$ or n on the top right-hand side of \mathcal{G}_t^n .

This property is evident from the way the triangle graph is connected, and is preserved by the recursion. We also assume that the horizontal I -avoiding paths in the rectangle graphs are symmetric (they enter and exit at the same node position r from the bottom) and moreover that the following property holds for the rectangle graphs:

Property B. If $|I_t| = t - 1$ and $\{2k, 2k + 1\} \notin I_t$ for some $k \leq t$, then for $k + 1 < \alpha \leq t$, the I_t -avoiding paths via $\mathcal{RG}_{\alpha-2,\alpha}^{2\alpha-1}$ all go via the same input/output node position r (and thus can be extended from one rectangle to the next).

The above property is justified through the way the rectangle graphs in \mathcal{G}_{t+1}^{n+2} are connected as shown in Appendix B.

Case 1: $|I_{t+1} \cap [n]| = t + 1$ and $|I_{t+1} \cap \{n + 1, n + 2\}| = 0$. The case is illustrated in Figure 16. As both colors $n + 2$ and $n + 1$ do not belong to I_{t+1} , the I_{t+1} -avoiding path exists if we select the top node that belongs to both sets \mathcal{L} and \mathcal{R} or in other words $\ell = r$. In fact, we have a single path that takes inputs from both the left and right sides. This path includes all nodes with colors $\{n + 2, n + 1\}$; in Figure 16 the path is depicted by a thick line. The last node with color $n + 1$ is connected to the nodes of the rectangle graph $\mathcal{RG}_{(t-1,t+1)}^n$ that completes the path. Note that the color $n + 1$ is used internally in the rectangle graph to provide a path, and property A of \mathcal{G}_t^n has been preserved in \mathcal{G}_{t+1}^{n+2} , as required. Further notice that we have not used the induction assumption here.

Case 2: $|I_{t+1} \cap [n]| = t$ and $|I_{t+1} \cap \{n + 1, n + 2\}| = 1$. In the proof, we are going to show the existence of I_{t+1} -avoiding paths. We assume that there is a I_t -avoiding path in \mathcal{G}_t^n . There are the following two possible cases:

Case 2a: The avoiding path in \mathcal{G}_t^n starts from one of the nodes with colors in the set $\{n, n - 1\}$. By construction this path can be extended as each node with a color from $\{n, n - 1\}$ is connected to two nodes with a color from $\{n + 2, n + 1\}$. This scenario is illustrated in Figure 17.

Case 2b: The avoiding path in \mathcal{G}_t^n starts from one of the nodes in the rectangle graph $\mathcal{RG}_{t-2,t}^{n-2}$ at the bottom of the graph. The two copies of $\mathcal{RG}_{t-2,t}^{n-2}$ extend this path horizontally until the graph $\mathcal{RG}_{t-1,t+1}^n$ which is horizontally blocked



Note that property A of \mathcal{G}_t^n has been preserved in \mathcal{G}_{t+1}^{n+2} , as required.

$$\{1, 2, 3\}; \{4, 5\}; \dots; \{n-1, n\}; \{n+1, n+2\}.$$

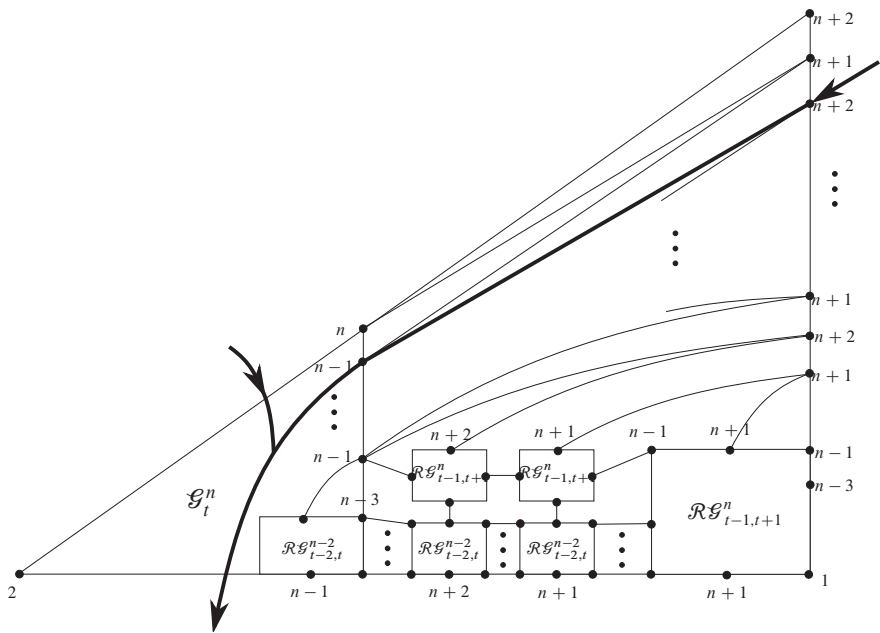


Figure 17. A I_{t+1} -avoiding path in \mathcal{G}_{t+1}^{n+2} – Case 2a.

As the last collection includes two colors from I_{t+1} , this means that at least one subset (partition) from the collection

$$\{1, 2, 3\}; \{4, 5\}; \dots; \{n - 1, n\}$$

must have two colors that do not belong to I_{t+1} (if we have t urns and $t - 1$ balls and we put balls into urns, then at least one urn must be empty). Consider the partition $\{2k, 2k + 1\}$ that does not have any color from I_{t+1} , where $k \leq t$ and all other partitions $\{2\alpha, 2\alpha + 1\}$ for $t \geq \alpha > k$ have at least one color in I_{t+1} . Note that in this case the last partition $\{n + 1, n + 2\}$ contains both elements in I_{t+1} . Thus, the partition of colors has to be of the following form:

$$\underbrace{\{1, 2, 3\}}_1 \underbrace{\{4, 5\}}_2 \dots \underbrace{\{2k - 2, 2k - 1\}}_{k-1} \underbrace{\{2k, 2k + 1\}}_k \underbrace{\{2k + 2, 2k + 3\}}_{k+1} \\ \dots \underbrace{\{2t, 2t + 1\}}_t \underbrace{\{2t + 2, 2t + 3\}}_{t+1},$$

where

- $|\{2k, 2k + 1\} \cap I_{t+1}| = 0$ and
- $|\{2\alpha, 2\alpha + 1\} \cap I_{t+1}| \neq 0$ for all α with $k < \alpha \leq t + 1$.

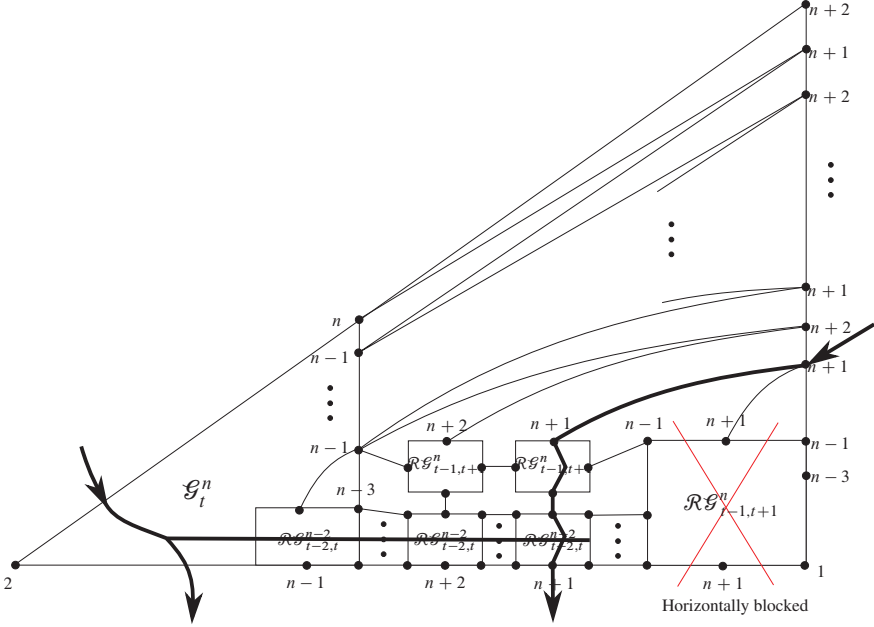


Figure 18. A I_{t+1} -avoiding path in \mathcal{G}_{t+1}^{n+2} – Case 2b.

The conclusion from the above reasoning is that it is enough to consider the “worst” scenario when two colors $\{n, n-1\} \notin I_t$, where $|I_t| = t-1$ as $|I_{t+1}| = t+1$. Being more specific there are other cases, that are equivalent to this one. For all these cases, two colors $2k+2, 2k+3 \notin I_{t+1}$ are followed by a sequence of single colors belonging to I_{t+1} , i.e.,

$$|\{2\alpha, 2\alpha+1\} \cap I_{t+1}| = 1 \quad \text{for } \alpha = k+1, \dots, t,$$

where colors $2t+2, 2k+3 \in I_{t+1}$. In all these cases the rectangle graphs $\mathcal{R}\mathcal{G}_{t-2,t}^{n-2}$ can be used to provide the horizontal path together with the rightmost rectangle graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$. The existence of this path follows from property B mentioned before which is justified via the connection of the rectangle graphs as shown in Appendix B.

The path avoiding I_t starts from the top node of the graph \mathcal{G}_t^n with the color n and goes vertically through the rectangle $\mathcal{R}\mathcal{G}_{t-2,t}^{n-2}$ on the left-hand side; see Figure 19. The bottom node with the color $n-1$ is connected via three copies of the rectangle graphs $\mathcal{R}\mathcal{G}_{t-1,t+1}^n$ to the node $n-1$ on the right-hand side of the graph \mathcal{G}_{t+1}^{n+2} . Note that the rectangle graphs provide the horizontal avoiding paths. \square

Using the above relation, we can write

$$\begin{aligned}
 G(t) &\leq G(t-1) + 5T(t-1) + 2t, \\
 G(t) &\leq G(t-2) + 5T(t-2) + 5T(t-1) + 2(t-1) + 2t, \\
 G(t) &\leq G(t-3) + 5T(t-3) + 5T(t-2) + 5T(t-1) + 2(t-2) \\
 &\quad + 2(t-1) + 2t, \\
 &\vdots \\
 G(t) &\leq G(1) + 5 \sum_{i=1}^{t-1} T(i) + 2 \sum_{i=1}^{t-1} (i+1).
 \end{aligned}$$

If we replace $T(i)$ by $(4i+2)T(\frac{i}{2}) + 4iG(\frac{i}{2}) + 4i$, we get

$$\begin{aligned}
 G(t) &\leq G(1) + 5 \sum_{i=1}^{t-1} \left((4 \cdot i + 2) \cdot T\left(\frac{i}{2}\right) + 4 \cdot i \cdot G\left(\frac{i}{2}\right) \right) + 2 \sum_{i=1}^{t-1} (i+1) \\
 &\leq G(1) + 5 \sum_{i=1}^{t-1} \left((4 \cdot i + 2) \cdot T\left(\frac{t}{2}\right) + 4 \cdot i \cdot G\left(\frac{t}{2}\right) \right) + 2 \sum_{i=1}^{t-1} (i+1) \\
 &= G(1) + 5T\left(\frac{t}{2}\right) \sum_{i=1}^{t-1} (4 \cdot i + 2) + 20G\left(\frac{t}{2}\right) \sum_{i=1}^{t-1} i + 2 \sum_{i=1}^{t-1} (i+1) \\
 &= G(1) + 10(t^2 - 1)T\left(\frac{t}{2}\right) + 20 \frac{t(t-1)}{2} G\left(\frac{t}{2}\right) + t^2 + t - 2 \\
 &\leq G(1) + 10t^2 T\left(\frac{t}{2}\right) + 10t^2 G\left(\frac{t}{2}\right) + t^2 + t - 2 \\
 &= C \cdot t^2 \cdot T\left(\frac{t}{2}\right) + C \cdot t^2 \cdot G\left(\frac{t}{2}\right) + C \cdot t^2.
 \end{aligned}$$

Now, replacing

$$T\left(\frac{t}{2}\right) = (2t+2)T\left(\frac{t}{4}\right) + 2tG\left(\frac{t}{4}\right) + 2t$$

and

$$G\left(\frac{t}{2}\right) \leq \frac{Ct^2}{4} T\left(\frac{t}{4}\right) + \frac{Ct^2}{4} G\left(\frac{t}{4}\right) + \frac{Ct^2}{4},$$

we obtain

$$\begin{aligned}
 G(t) &\leq Ct^2 \left(2t + 2 + \frac{Ct^2}{4} \right) T\left(\frac{t}{4}\right) + Ct^2 \left(2t + \frac{Ct^2}{4} \right) G\left(\frac{t}{4}\right) \\
 &\quad + Ct^2 \left(2t + \frac{Ct^2}{4} \right).
 \end{aligned}$$

We repeat the substitution

$$T\left(\frac{t}{4}\right) = (t+2)T\left(\frac{t}{8}\right) + tG\left(\frac{t}{8}\right) + t$$

and

$$G\left(\frac{t}{4}\right) \leq \frac{Ct^2}{16}T\left(\frac{t}{8}\right) + \frac{Ct^2}{16}G\left(\frac{t}{8}\right) + \frac{Ct^2}{16},$$

and get

$$\begin{aligned} G(t) &\leq Ct^2\left(2t+2+\frac{Ct^2}{4}\right)T\left(\frac{t}{4}\right) + Ct^2\left(2t+\frac{Ct^2}{4}\right)G\left(\frac{t}{4}\right) \\ &\quad + Ct^2\left(2t+\frac{Ct^2}{4}\right) \\ &= Ct^2\left(2t+2+\frac{Ct^2}{4}\right)\left(t+2+\frac{Ct^2}{16}\right)T\left(\frac{t}{8}\right) + Ct^2\left(2t+\frac{Ct^2}{4}\right) \\ &\quad \cdot \left(t+\frac{Ct^2}{16}\right)G\left(\frac{t}{8}\right) + Ct^2\left(2t+\frac{Ct^2}{4}\right)\left(t+\frac{Ct^2}{16}\right). \end{aligned}$$

If we continue substituting complexities of $T(n/2^i)$ and $G(n/2^i)$ by $T(n/2^{i+1})$ and $G(n/2^{i+1})$, then in some point we hit the stopping case $T(1)$ and $G(1)$. This is to say that the number of terms is upper bounded by $\log_2 t$ or

$$\begin{aligned} G(t) &\leq \underbrace{Ct^2\left(2t+2+\frac{Ct^2}{4}\right)\left(t+2+\frac{Ct^2}{16}\right)}_{\log_2 t \text{ times}} \cdots T(1) \\ &\quad + \underbrace{Ct^2\left(2t+\frac{Ct^2}{4}\right)\left(t+\frac{Ct^2}{16}\right)}_{\log_2 t \text{ times}} \cdots G(1) \\ &\quad + \underbrace{Ct^2\left(2t+\frac{Ct^2}{4}\right)\left(t+\frac{Ct^2}{16}\right)}_{\log_2 t \text{ times}} \cdots. \end{aligned}$$

The number of replacements is upper bounded by $\log_2 t$. This also means that

$$G(t) = O(t^{2 \cdot \log_2 t}).$$

Now assume that t is odd, then the rectangle graph $\mathcal{R}_{t-1,t+1}^n$ has the following

recursive relation:

$$\begin{aligned}
 T(t) &= (2t + 1) \cdot T\left(\left\lceil \frac{t}{2} \right\rceil\right) + (2t + 1) \cdot T\left(\left\lceil \frac{t}{2} \right\rceil - 1\right) + 2 \cdot t \cdot G\left(\left\lceil \frac{t}{2} \right\rceil\right) \\
 &\quad + 2 \cdot t \cdot G\left(\left\lceil \frac{t}{2} \right\rceil - 1\right) + 4 \cdot t \\
 &\leq (4t + 2) \cdot T\left(\left\lceil \frac{t}{2} \right\rceil\right) + 4 \cdot t \cdot G\left(\left\lceil \frac{t}{2} \right\rceil\right) + 4 \cdot t,
 \end{aligned}$$

which is the same expression as the case when t is a power of 2. (Note that if t is a power of 2, then $\lceil \frac{t}{2} \rceil = \frac{t}{2}$.) This leads us to the same complexity evaluation. If t is neither odd nor a power of 2, then the recursive relation for $\mathcal{RG}_{t-1,t+1}^n$ is the same as in the case when t is a power of 2 until an odd value is encountered during recursion. In this case, we can substitute the (bounded) recursive relation obtained above for an odd t . Thus, the complexity evaluation holds in this case as well.

Concluding remarks

We cannot say for certain whether the construction of a t -reliable n -coloring triangle PDAG is the best that can be achieved and if it is possible to improve on the subexponential complexity of the specific construction shown in this paper. It remains an open problem to show a deterministic construction that is optimal and has polynomial complexity of construction. Indeed an MPC protocol over non-Abelian groups with black-box access does not necessarily have to be a t -reliable n -coloring of a planar graph. It could employ some other mathematical structure. One such construction was shown recently by Cohen et al. [5] using threshold log-depth formulae as building blocks. Such possibilities are likely to incite further interest in this topic.

A Rectangle graphs $\mathcal{RG}_{t-1,t+1}^{2t+1}$ for arbitrary t

The purpose of this appendix is to show how to reduce the construction of rectangle graphs $\mathcal{RG}_{t-1,t+1}^{2t+1}$ for arbitrary t , to smaller rectangle graphs $\mathcal{RG}_{t'-1,t'+1}^{2t'+1}$ and $\mathcal{RG}_{t''-1,t''}^{2t''}$ of the same form, with $t' < t$ and a triangle graph $\mathcal{G}_{t'-1}^{2t'-1}$. Together with the recursion for \mathcal{G}_t^{2t+1} shown in Section 6, this gives a construction of the graphs \mathcal{G}_t^{2t+1} , $\mathcal{RG}_{t-1,t+1}^{2t+1}$ for any t .

Recall that, in Section 6, we only showed the construction of $\mathcal{RG}_{t-1,t+1}^{2t+1}$ when t is a power of 2. We first show the construction of $\mathcal{RG}_{t-1,t+1}^{2t+1}$ when t is odd. We will then show how the case when t is even and not a power of 2 can be reduced to this case.

A.1 Analysis of rectangle graphs $\mathcal{RG}_{t-1,t+1}^{2t+1}$ with odd t for horizontal paths

The smallest of the rectangle graphs of the form $\mathcal{RG}_{t-1,t+1}^{2t+1}$ with odd t is the rectangle graph $\mathcal{RG}_{0,2}^3$ ($t = 1$) which can be trivially drawn as three connected nodes. We therefore consider the rectangle graph $\mathcal{RG}_{2,4}^7$, corresponding to $t = 3$, shown in Figure 20. It consists of 7 pairs of rectangle graphs $(\mathcal{RG}_{1,3}^5, \mathcal{RG}_{0,1}^2)$. Adjacent copies of $\mathcal{RG}_{1,3}^5$ are connected via the triangle graph \mathcal{G}_1^3 . The triangle graph \mathcal{G}_0^1 (which consists of a single node) connects neighboring copies of $\mathcal{RG}_{0,1}^2$. The triangle graph \mathcal{G}_0^1 also connects adjacent copies of $\mathcal{RG}_{0,1}^2$. The triangle graph \mathcal{G}_0^1 is colored with the common color of the adjacent rectangle graphs $\mathcal{RG}_{0,1}^2$. The colors of \mathcal{G}_1^3 are chosen such that they are present in both the left- and right-hand rectangle graph $\mathcal{RG}_{1,3}^5$. This ensures that this triangle graph is blocked only if both copies of rectangle graphs $\mathcal{RG}_{1,3}^5$ are blocked.

The triangle graphs \mathcal{G}_1^3 and \mathcal{G}_0^1 are connected via two nodes which are labelled “bridging nodes” in the figure. Each bridging node is assigned the color which is swapped between the diagonal rectangle graphs. For instance, in the first component in Figure 20, the colors 1 and 6 have been swapped between the two pairs of diagonal rectangle graphs $(\mathcal{RG}_{1,3}^5$ and $\mathcal{RG}_{0,1}^2)$. These are then assigned to the bridging nodes. Notice that the triangle graph \mathcal{G}_1^3 has three nodes in its base (obtained using the mirror trick). The left (resp. right) bridging node connects with the two nodes in the base of the left (resp. right) image of the triangle graph \mathcal{G}_1^3 . This is made explicit in Figure 21, where a segment of the rectangle graph $\mathcal{RG}_{2,4}^7$ is shown. Recall that the vertical path through the triangle graphs is only used when exactly one of the two colors assigned to the bridging nodes is blocked. Thus, this connection ensures that the path between the two triangle graphs is not blocked when used for vertical traversing. The graph $\mathcal{RG}_{2,3}^6$ is the same as $\mathcal{RG}_{2,4}^7$ except that the rectangle graphs $\mathcal{RG}_{1,3}^5$ are replaced by $\mathcal{RG}_{1,2}^4$.

To show that the given construction provides a horizontal I -avoiding path, we consider the example of the rectangle graph $\mathcal{RG}_{4,6}^{11}$ which corresponds to $t = 5$. One way is to check all $\binom{11}{2} = 55$ possible paths. But as before, we can utilize the regularity of the structure to analyze the path between two neighboring components. Figure 22 shows a segment of these components.

This graph is constructed with the help of pairs of the rectangle graphs $\mathcal{RG}_{2,4}^7$ and $\mathcal{RG}_{1,2}^4$. Adjacent copies of $\mathcal{RG}_{2,4}^7$ are connected through \mathcal{G}_2^5 whereas those of $\mathcal{RG}_{1,2}^4$ are linked via \mathcal{G}_1^3 . The figure illustrates how the two triangle graphs are connected vertically via the bridging nodes. The triangle graph \mathcal{G}_2^5 has 9 nodes in its base as a result of the mirror trick. The left image of this graph is connected to the left bridging node (colored 1), and the right image is connected to the right bridging node (colored 8). Notice that the two images have one base node in com-

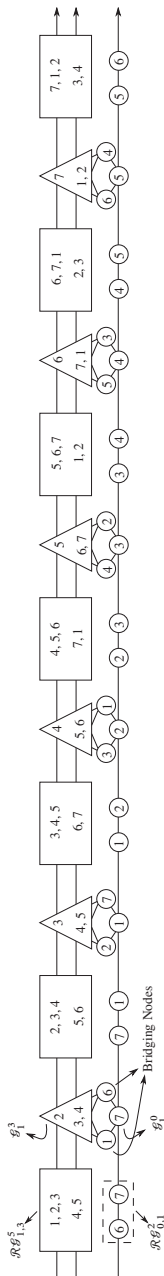


Figure 20. Rectangle graph $\mathcal{RG}_{2,4}^7$ without vertical nodes. Figure 90° counter-clockwise rotated.

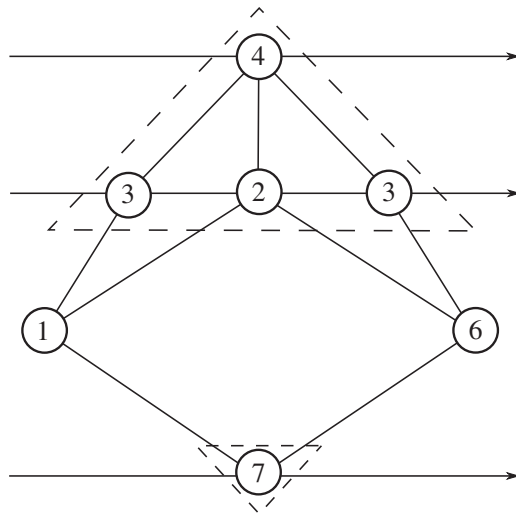


Figure 21. The vertical connection between the triangle graphs \mathcal{G}_1^3 and \mathcal{G}_0^1 via the bridging nodes 1 and 6 in $\mathcal{R}\mathcal{G}_{2,4}^7$.

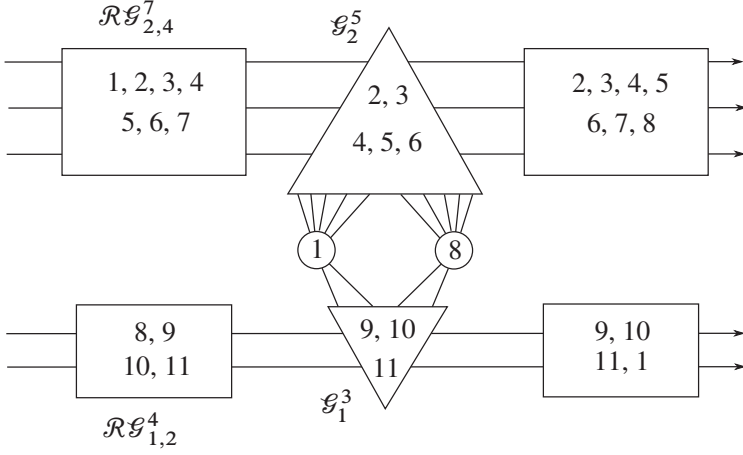
mon (the middle base node). The two mirror images of the triangle graph \mathcal{G}_1^3 are connected similarly to the bridging nodes.

Now given an avoiding set I , where $|I| = 4$, we need to show that there is a horizontal I -avoiding path between two neighboring components. Without loss of generality, we consider the first component as shown in Figure 22. Let us represent the colors of the four rectangle graphs by the following sets:

$$\begin{aligned} A_1 &= \{1, 2, 3, 4, 5, 6, 7\}, & A_2 &= \{2, 3, 4, 5, 6, 7, 8\}, \\ B_1 &= \{8, 9, 10, 11\}, & B_2 &= \{9, 10, 11, 1\}. \end{aligned}$$

Let $\mathcal{R}\mathcal{G}_{A_1}$, $\mathcal{R}\mathcal{G}_{A_2}$, $\mathcal{R}\mathcal{G}_{B_1}$ and $\mathcal{R}\mathcal{G}_{B_2}$ represent rectangle graphs with colors from the sets A_1 , A_2 , B_1 and B_2 , respectively. Given an arbitrary set I , we can split it into subsets $I_{A_1} = I \cap A_1$ and $I_{A_2} = I \cap A_2$ in a straightforward way. The sets I_{B_1} and I_{B_2} are defined likewise. There are four possible scenarios if we consider the colors switched between the two rectangles, i.e., 1 and 8 (these are also the colors of the bridging nodes):

- The colors $1 \notin I$ and $8 \notin I$. The horizontal paths are provided by the rectangle graphs $\mathcal{R}\mathcal{G}_{A_i}$ or $\mathcal{R}\mathcal{G}_{B_i}$. For instance, if the rectangle graph $\mathcal{R}\mathcal{G}_{B_1}$ is blocked then so is $\mathcal{R}\mathcal{G}_{B_2}$. On the contrary, if $\mathcal{R}\mathcal{G}_{B_1}$ allows a horizontal path then so does $\mathcal{R}\mathcal{G}_{B_2}$. The same is true for $\mathcal{R}\mathcal{G}_{A_1}$ and $\mathcal{R}\mathcal{G}_{A_2}$.

Figure 22. A section of the rectangle graph $\mathcal{RG}_{4,6}^{11}$.

- The colors $1 \in I$ and $8 \in I$. The colors are swapped between the rectangles, and the horizontal path is provided by either the rectangle graphs \mathcal{RG}_{A_i} or \mathcal{RG}_{B_i} .
- The colors $1 \in I$ and $8 \notin I$. This implies that $|I_{A_2}| = |I_{A_1}| - 1$ and $|I_{B_2}| = |I_{B_1}| + 1$. Now, there will be a switch between the two types of rectangle graphs if \mathcal{RG}_{A_1} is blocked by three nodes, i.e., $|I_{A_1}| = 3$. This means that a horizontal path exists through \mathcal{RG}_{B_1} as $|I_{B_1}| = 1$. However, \mathcal{RG}_{B_2} is blocked because $|I_{B_2}| = 2$. Thus, a vertical transition has to be made through the triangle graphs. Since the bridging node with color 1 is blocked, the transition between the two triangle graphs is provided by the bridging node with color 8. The horizontal path is then completed through \mathcal{RG}_{A_2} since $|I_{A_2}| = 2$. In case \mathcal{RG}_{A_1} is not blocked by three nodes, a switch is not required.
- The colors $1 \notin I$ and $8 \in I$. This is similar to above, except now the bridging node with color 8 is blocked and therefore the vertical connection between the two triangle graphs is provided through the bridging node colored 1.

Let $t' = \lceil \frac{t}{2} \rceil$. To generalize, for any odd t we see that $\mathcal{RG}_{t-1,t+1}^{2t+1}$ can be constructed using $2t + 1$ pairs of the rectangle graphs $\mathcal{RG}_{t'-1,t'+1}^{2t'+1}$ and $\mathcal{RG}_{t'-2,t'-1}^{2t'-2}$. Adjacent copies of $\mathcal{RG}_{t'-1,t'+1}^{2t'+1}$ are connected through the triangle graph $\mathcal{G}_{t'-1}^{2t'-1}$. The neighboring copies of the rectangle graph $\mathcal{RG}_{t'-2,t'-1}^{2t'-2}$ are connected via the triangle graph $\mathcal{G}_{t'-2}^{2t'-3}$. This is shown in Figure 23. The vertical connection between the two triangle graphs is established through the two bridging nodes la-

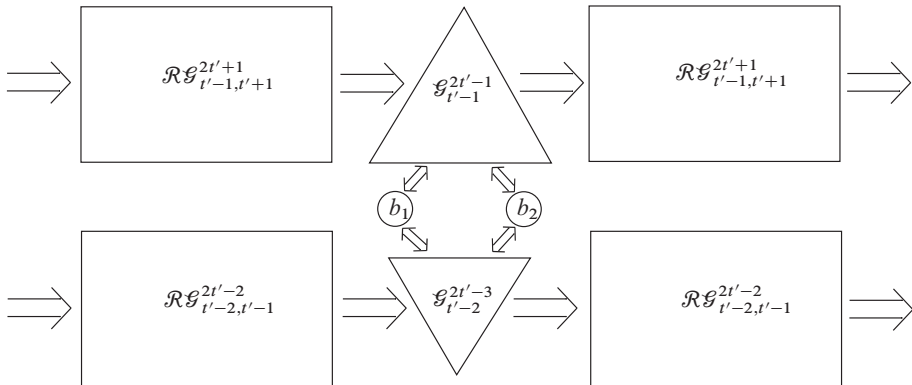


Figure 23. The general construction of the rectangle graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$ for an odd t .

belled b_1 and b_2 in the figure. As before, the left mirror images of the two triangle graphs are connected to b_1 and the right mirror images to b_2 . The color assignment to the rectangle graph is shown in Figure 24, where the sets A_i and B_i represent the colors assigned to the i th rectangle graph $\mathcal{R}\mathcal{G}_{t'-1,t'+1}^{2t'+1}$ and $\mathcal{R}\mathcal{G}_{t'-2,t'-1}^{2t'-2}$, respectively, where $i \in \{1, 2, \dots, 2t+1\}$. The i th pair of bridging nodes is assigned the colors $(i, 2t'+i+1)$, since this is the pair of colors swapped between the diagonal rectangle graphs. The triangle graphs are assigned colors which are common to the two copies of rectangle graphs that are attached to them.

We have the following theorem for vertical paths in $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$ for an odd t .

Theorem A.1. *Suppose t is odd and let $t' = \lceil \frac{t}{2} \rceil$. Let $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$ be the rectangle graph built from the set of $2t+1$ rectangle graph components $\mathcal{R}\mathcal{G}_{t'-1,t'+1}^{2t'+1}$ and $\mathcal{R}\mathcal{G}_{t'-2,t'-1}^{2t'-2}$ connected via the triangle graphs $\mathcal{G}_{t'-1}^{2t'-1}$ and $\mathcal{G}_{t'-2}^{2t'-3}$ along with the bridging nodes b_1 and b_2 as shown in Figure 23. Let the component rectangle graphs be assigned colors from the sets (A_i, B_i) as illustrated in Figure 24. Then for any set of colors I , where $|I| \leq t-1$, there is a horizontal I -avoiding path in $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$.*

Proof. The proof is a straightforward generalization of the case for rectangle graph $\mathcal{R}\mathcal{G}_{4,6}^{11}$. \square

A.2 Analysis of rectangle graphs $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$ with odd t for vertical paths

The rectangle graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$ has to provide a vertical path from a top (external) vertex with a color different from the $2t+1$ colors of the rectangle graph. The

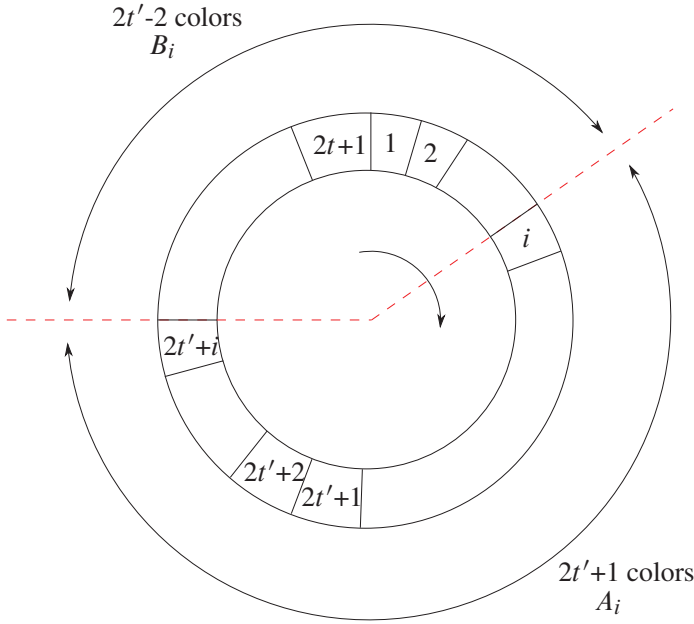
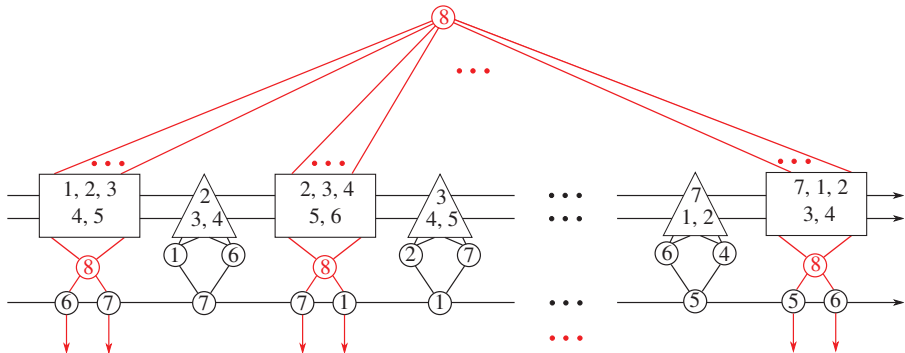


Figure 24. The assignment of colors to the rectangle graphs $\mathcal{RG}_{t'-1, t'+1}^{2t'+1}$ and $\mathcal{RG}_{t'-2, t'-1}^{2t'-2}$.

path should pass through $\mathcal{RG}_{t-1, t+1}^{2t+1}$ and end up at one of its output nodes. To show that the graph allows a vertical I -avoiding path, with $|I| \leq t + 1$, we once again begin with the example of $\mathcal{RG}_{2,4}^7$, which corresponds to $t = 3$. Figure 25 shows an abbreviated snapshot of this graph.

The node colored 8, which is external to the graph, connects to all the copies of the component rectangle graphs $\mathcal{RG}_{1,3}^5$. These components are then connected to another node, again colored 8, which in turn connects to the respective copies of the rectangle graph $\mathcal{RG}_{0,1}^2$. As before, let us denote the set of colors assigned to the rectangle graphs $\mathcal{RG}_{1,3}^5$ by A_1, A_2, \dots, A_7 . Similarly, B_1, B_2, \dots, B_7 denote the set of colors of the rectangle graphs $\mathcal{RG}_{0,1}^2$. Given an avoiding path I , with $|I| \leq 4$, we need to find a pair of colors (A_i, B_i) such that $I_{A_i} = I \cap A_i$ has cardinality less than or equal to 3, and $I_{B_i} = I \cap B_i$ has cardinality less than or equal to 1. Since $\mathcal{RG}_{1,3}^5$ provides a vertical I -avoiding path with $|I| \leq 3$ and $\mathcal{RG}_{0,1}^2$ provides a vertical I -avoiding path with $|I| \leq 1$, such a partition will guarantee a vertical I -avoiding path with $|I| \leq 4$ in $\mathcal{RG}_{2,4}^7$.

To see that this can be achieved, suppose $|I| = 4$ and observe Figure 24. We start with the initial configuration, i.e., $i = 1$, and rotate the “disk” clockwise until

Figure 25. Vertical path in the rectangle graph $\mathcal{R}\mathcal{G}_{2,4}^7$.

we reach a state where $|I_{A_i}| = 3$ and $|I_{B_i}| = 1$. Since the assignment of colors is cyclic, this can always be achieved. The case when $|I| < 4$ then follows, since if $\mathcal{R}\mathcal{G}_{2,4}^7$ allows an I -avoiding path with cardinality 4, then it also provides a path with a lesser cardinality.

In general, we have the following theorem.

Theorem A.2. Suppose t is odd and let $t' = \lceil \frac{t}{2} \rceil$. Let $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$ be the rectangle graph built from the set of $2t + 1$ rectangle graph components $\mathcal{R}\mathcal{G}_{t'-1,t'+1}^{2t'+1}$ and $\mathcal{R}\mathcal{G}_{t'-2,t'-1}^{2t'-2}$ connected via the triangle graphs $\mathcal{G}_{t'-1}^{2t'-1}$ and $\mathcal{G}_{t'-2}^{2t'-3}$ along with the bridging nodes b_1 and b_2 as shown in Figure 23. Let the component rectangle graphs be assigned colors from the sets (A_i, B_i) as illustrated in Figure 24. Then for any set of colors I , where $|I| \leq t + 1$, there is a vertical I -avoiding path in $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$.

Proof. Given an I -avoiding set, we need to find a partition of colors (A_i, B_i) , such that the respective intersections have cardinalities less than or equal to $t' + 1$ and $t' - 1$, respectively. This can be done by rotating the disk in Figure 24 until such a partition is encountered. Since the assignment of colors is cyclic, such a partition can always be obtained. \square

This shows that there exists a rectangle graph $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$, which is horizontally I -avoiding and vertically J -avoiding, where t is odd, $|I| \leq t - 1$ and $|J| \leq t + 1$. Note that the “reduced” graph $\mathcal{R}\mathcal{G}_{t-1,t}^{2t}$ can be obtained from $\mathcal{R}\mathcal{G}_{t-1,t+1}^{2t+1}$ by replacing the rectangle graphs $\mathcal{R}\mathcal{G}_{t'-1,t'+1}^{2t'+1}$ with $\mathcal{R}\mathcal{G}_{t'-1,t'}^{2t'}$, where $t' = \lceil \frac{t}{2} \rceil$, and removing the last triangle and rectangle graphs (since this graph has one color less).

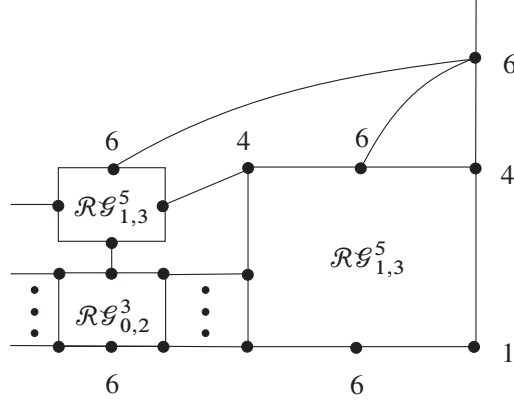


Figure 26. Connection of $\mathcal{RG}_{1,3}^5$ with $\mathcal{RG}_{0,2}^3$ and $\mathcal{RG}_{1,3}^5$ in \mathcal{G}_3^7 .

A.3 Construction of $\mathcal{RG}_{t-1,t+1}^{2t+1}$ for arbitrary t

We are now ready to show that for any $t \in \mathbb{N}$, there is a rectangle graph $\mathcal{RG}_{t-1,t+1}^{2t+1}$ which is horizontally I -avoiding and vertically J -avoiding, where $|I| \leq t-1$ and $|J| \leq t+1$.

Theorem A.3. *For any $t \in \mathbb{N}$, there exists a rectangle graph $\mathcal{RG}_{t-1,t+1}^{2t+1}$ which is horizontally I -avoiding and vertically J -avoiding, where $|I| \leq t-1$ and $|J| \leq t+1$.*

Proof. We discuss three mutually exclusive but collectively exhaustive cases.

- t is a power of 2. Let m be the power of 2, such that $2t+1 = 2 \cdot 2^m + 1$. Then, $2t'+1 = 2 \cdot \frac{t}{2} + 1$ can be written as $2 \cdot \frac{2^m}{2} + 1 = 2^m + 1$. Thus, the rectangle graph $\mathcal{RG}_{t-1,t+1}^{2t+1}$ can be recursively constructed, since its constituent rectangle graphs $\mathcal{RG}_{t'-1,t'+1}^{2t'+1}$ are of the form $T+1$ where T is a power of 2. We have already shown this construction in detail.
- t is odd. We have shown in this section how to construct the rectangle graph $\mathcal{RG}_{t-1,t+1}^{2t+1}$ for an odd t .
- t is even but not a power of 2. We can write t as $2m$, where m is some positive integer. Then, $2t'+1 = 2 \cdot \frac{t}{2} + 1$ can be written as $2 \cdot \frac{2m}{2} + 1 = 2m + 1$. If m is odd, then this leads us to the second case. If, however, m is even we recurse until an odd value of $m(i)$ is encountered for some recursion level i . The construction is then the same as the second case. The intermediate constructions before an odd value of $m(i)$ is encountered are the same as when t is a power of 2. \square

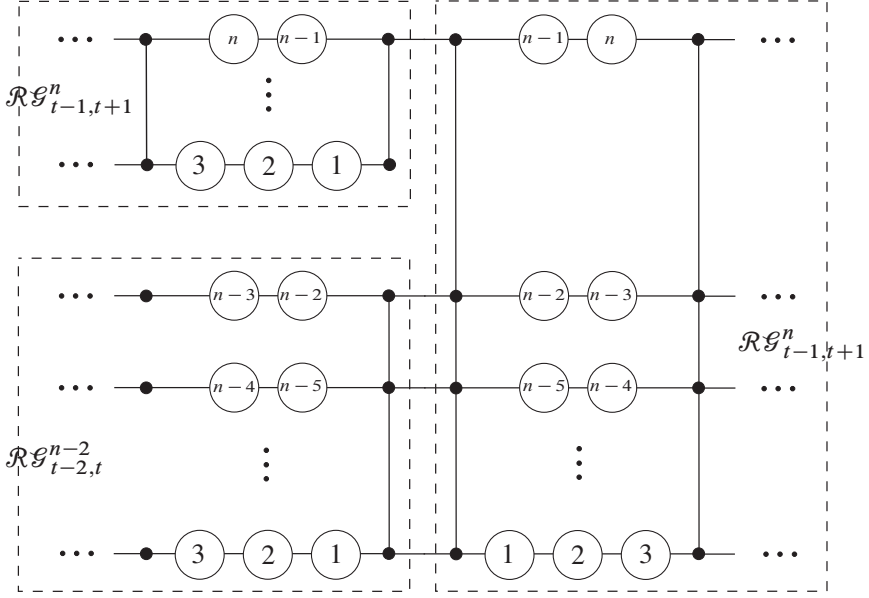


Figure 28. The connection of $\mathcal{RG}_{t-1,t+1}^n$ with $\mathcal{RG}_{t-2,t}^{n-2}$ and $\mathcal{RG}_{t-1,t+1}^n$ in \mathcal{G}_{t+1}^{n+2} .

angle graph $\mathcal{RG}_{t-1,t+1}^n$ with the same layer in the neighboring rectangle graph $\mathcal{RG}_{t-1,t+1}^n$. The remaining $n - 2$ colors are connected with the rectangle graph $\mathcal{RG}_{t-2,t}^{n-2}$ layer by layer to preserve colors on both sides in a straightforward manner. This is depicted in Figure 28. The external node $n + 1$ is not shown in the figure for clarity. The correctness of the connection follows from the way the rectangle graphs $\mathcal{RG}_{t-1,t+1}^n$ are constructed.

In light of this connection, we can assume that the horizontal I -avoiding paths in the rectangle graphs are symmetric, i.e., they enter and exit at the same node position r from the bottom.

Bibliography

- [1] J. Bar-Ilan and D. Beaver, Non-cryptographic fault-tolerant computing in constant number of rounds of interaction, in: *Proceedings of the 8th Annual ACM Symposium on Principles of Distributed Computing (PODC'89)*, ACM, New York (1989), 201–209.
- [2] D. A. Barrington, Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1 , in: *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC'86)*, ACM, New York (1986), 1–5.

- [3] M. Ben-Or, S. Goldwasser and A. Wigderson, Completeness theorems for non-cryptographic fault-tolerant distributed computation, in: *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, (STOC'88), ACM, New York (1988), 1–10.
- [4] D. Chaum, C. Crépeau and I. Damgård, Multiparty unconditionally secure protocols, in: *Proceedings of the 20th Annual ACM Symposium on Theory of Computing* (STOC'88), ACM, New York (1988), 11–19.
- [5] G. Cohen, I. B. Damgård, Y. Ishai, J. Kölker, P. B. Miltersen, R. Raz and R. D. Rothblum, Efficient multiparty protocols via log-depth threshold formulae (extended abstract), in: *Proceedings of the 33rd Annual International Cryptology Conference on Advances in Cryptology* (CRYPTO'13), Lecture Notes in Comput. Sci. 8043, Springer, Berlin (2013), 185–202.
- [6] J. Cohen Benaloh, Secret sharing homomorphisms: keeping shares of a secret secret, in: *Proceedings of the 6th Annual International Cryptology Conference on Advances in Cryptology* (CRYPTO'86), Springer, London (1987), 251–260.
- [7] R. Cramer, S. Fehr, Y. Ishai and E. Kushilevitz, Efficient multi-party computation over rings, in: *Proceedings of the 22nd International Conference on Theory and Applications of Cryptographic Techniques* (EUROCRYPT'03), Springer, Berlin (2003), 596–613.
- [8] I. Damgård, Y. Ishai and M. Krøigaard, Perfectly secure multiparty computation and the computational overhead of cryptography, in: *Proceedings of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques* (EUROCRYPT'10), Springer, Berlin (2010), 445–465.
- [9] I. Damgård and J. B. Nielsen, Scalable and unconditionally secure multiparty computation, in: *Proceedings of the 27th Annual International Cryptology Conference on Advances in Cryptology* (CRYPTO'07), Springer, Berlin (2007), 572–590.
- [10] Y. Desmedt, J. Pieprzyk and R. Steinfeld, Active security in multiparty computation over black-box groups, in: *Proceedings of the 8th International Conference on Security and Cryptography for Networks* (SCN'12), Springer, Berlin (2012), 503–521.
- [11] Y. Desmedt, J. Pieprzyk, R. Steinfeld, X. Sun, C. Tartary, H. Wang and A. C.-C. Yao, Graph coloring applied to secure computation in non-Abelian groups, *J. Cryptology* **25** (2012), no. 4, 557–600.
- [12] Y. Frankel, Y. Desmedt and M. Burmester, Non-existence of homomorphic general sharing schemes for some key spaces (extended abstract), in: *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology* (CRYPTO'92), Springer, Berlin (1992), 549–557.
- [13] M. Hirt and U. Maurer, Complete characterization of adversaries tolerable in secure multi-party computation (extended abstract), in: *Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing* (PODC'97), ACM, New York (1997), 25–34.

- [14] S. S. Magliveras, D. R. Stinson and T. van Trung, New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups, *J. Cryptology* **15** (2002), no. 4, 285–297.
- [15] S.-H. Paeng, K.-C. Ha, J. H. Kim, S. Chee and C. Park, New public key cryptosystem using finite non Abelian groups, in: *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology* (CRYPTO'01), Springer, London (2001), 470–485.
- [16] A. C. Yao, Protocols for secure computations, in: *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science* (SFCS'82), IEEE Computer Society, Washington (1982), 160–164.

Received October 11, 2013; revised June 26, 2014; accepted July 4, 2014.

Author information

Hassan Jameel Asghar, National ICT Australia (NICTA), Sydney, Australia.
E-mail: hassan.asghar@nicta.com.au

Yvo Desmedt, Department of Computer Science, University College London, UK;
and Department of Computer Science, University of Texas at Dallas, USA.
E-mail: yvo.desmedt@utdallas.edu

Josef Pieprzyk, School of Electrical Engineering and Computer Science,
Science and Engineering Faculty, Queensland University of Technology,
Brisbane, QLD 4000, Australia.
E-mail: josef.pieprzyk@qut.edu.au

Ron Steinfeld, Clayton School of Information Technology,
Faculty of Information Technology, Monash University, Clayton, Australia.
E-mail: ron.steinfeld@monash.edu