Edge-Colored Graphs with Applications To Homogeneous Faults[☆]

Yongge Wang

University of North Carolina at Charlotte, USA

Yvo Desmedt

University College London, United Kingdom

Abstract

In this paper, we use the concept of edge-colored graphs to model homogeneous faults in networks. We then use this model to study the minimum connectivity (and design) requirements of networks for being robust against homogeneous faults within certain thresholds. In particular, necessary and sufficient conditions for most interesting cases are obtained. For example, we will study the following cases: (1) the number of colors (or the number of non-homogeneous network device types) is one more than the homogeneous fault threshold; (2) there is only one homogeneous fault (i.e., only one color could fail); and (3) the number of non-homogeneous network device types is less than five.

Keywords: graphs, network security, network reliability, homogeneous faults, fault tolerance

1. Background and edge-colored graph

In network communications, the communication could fail if some nodes or some edges are broken. Though the failure of a modem could be considered the failure of a node, we can model this scenario also as the failure of the communication link (the edge) attached to this modem. Thus it is sufficient to consider edge failures in communication networks. It is also important to note that several nodes (or edges) in a network could fail at the same time. For example, all brand X routers in a network could fail at the same time due to a platform dependent computer worm (virus) attack. In order to design survivable communication networks, it is essential to consider this kind of homogeneous faults for networks. Existing works on network quality of services have not addressed this issue in detail and there is no existing model to study network reliability in this aspect. In this paper, we use the edge-colored graphs which could be used to model homogeneous faults in networks. The model is then used to optimize the design of survivable networks and to study the minimum connectivity (and design) requirements of networks for being robust against homogeneous faults within certain thresholds.

Definition 1. *An edge-colored graph is a tuple $G(V,E,C,f)$, with V the node set, E the edge set, C the color set, and f a map from E onto C. The structure*

$$\mathcal{Z}_{C,t} = \{Z : Z \subseteq E \text{ and } |f(Z)| \le t\}.$$

*is called a t-color adversary structure. Let $A, B \in V$ be distinct nodes of G. A, B are called $(t+1)$-*color connected *for $t \ge 1$ if for any color set $C_t \subseteq C$ of size t, there is a path p from A to B in G such that the edges on p do not contain any color in C_t. An edge-colored graph G is $(t+1)$-*color connected *if and only if any two nodes A and B in G are $(t+1)$-color connected.*

The interpretation of the above definition is as follows. In a network, if two edges have the same color, then they could fail at the same time. This may happen when the two edges are designed with same technologies (e.g., with same operating systems, with same application software, with same hardware, or with same hardware and software). If an edge-colored network is $(t+1)$-color connected, then the network communication is robust against the failure of edges of any t colors

[☆]An extended abstract of this paper has appeared in the Proceedings to ICITS 2011.

Email addresses: yonwang@uncc.edu (Yongge Wang), y.desmedt@cs.ucl.ac.uk (Yvo Desmedt)

(that is, the adversary may tear down any t types of devices).

In practice, one communication link may be attached to different brands of network devices (e.g., routers, modems) on both sides. For this case, the edge can have two different colors. If any of these colors is broken, the edge is broken. Thus from a reliability viewpoint, if one designs networks with two colors on the same edge, the same reliability/security can be obtained by having only one color on each edge. In the following discussion, we will only consider the case with one color on each edge. Meanwhile, multiple edges between two nodes are not allowed either.

We are interested in the following practical questions. For a given number n of nodes in V (i.e., the number of network nodes), a given number γ of the colors (e.g., the number of network device types), and a given number t, how can we design a $(t+1)$-color connected edge-colored graph $G(V, E)$ with minimum number m of edges? In another word, how can we use minimum resources (e.g., communication links) to design a network that will keep working even if t types of devices in the network fail?

For practical network designs, one needs first to have an estimate on the number of homogeneous faults. For example, the number t of brands of routers that could fail at the same time. Then it is sufficient to design a $(t+1)$-color connected network with $\gamma = t+1$ colors (e.g., with $t+1$ different brands of routers). Necessary and sufficient conditions for this kind of network design will be obtained in this paper.

Another important issue that should be taken into consideration in practical network designs is that the number γ of colors (e.g., the number of brands for routers) is quite small. For example, γ is normally less than five. Necessary and sufficient conditions for network designs with $\gamma \leq 5$ and with optimized resources will be obtained in this paper. Note that for cases with small γ, we may have $\gamma > t+1$.

The outline of the paper is as follows. Section 3 describes the necessary and sufficient conditions for the case of $\gamma = t+1$ without optimizing the number of edges in the networks. Section 4 gives a necessary condition for edge-colored networks in terms of optimized number of edges. Section 5 shows that the necessary conditions in Section 4 are also sufficient for the most important three cases: (1) $\gamma = t+1$; (2) $t = 1$; and (3) $\gamma \leq 5$. Section 6 shows that it is **coNP**-hard to determine whether a given edge-colored graph is $(t+1)$-connected, and we conclude the paper by presenting a few resutls related to disjunct set systems in Section 7.

2. Related works

Though edge-colored graph is a new concept which we used to model network survivability issues, there are related research topics in this field. For example, edge-disjoint (colorful) spanning trees have been extensively studied in the literature (see, e.g., [1]). These results are mainly related to our discussion in the next section for the case of $\gamma = t+1$. An edge-colored graph G is *proper* if whenever two edges share an end point they carry different colors. A spanning tree for an edge-colored graph is called colorful if no two of its edges have the same color. Two spanning trees of a graph are edge disjoint if they do not share common edges. For a non-negative integer s, let K_s denote the complete graph on s vertices. A classical result from Euler (see [1]) shows that the edges of K_{2n} can be partitioned into n isomorphic spanning trees (paths, for example) and each of these spanning trees can easily be made colorful, but the resulting edge-colored graph usually fails to be proper.

Though it is important to design edge-colored graphs with required security parameters, for several scenarios it is also important to calculate the robustness of a given edge-colored graphs. Roskind and Tarjan [7] designed a greedy algorithm to find $(t+1)$ edge disjoint spanning trees in a given graph. This is related to the question of $(t+1)$-color connectivity for the case of $\gamma = t+1$. We are not aware of any approximate algorithms for deciding $(t+1)$-color connectivity of a given edge-colored graph. Indeed, we will show that this problem is **coNP**-hard.

3. Necessary and sufficient conditions for special cases

In this section, we show necessary and sufficient conditions for some special cases.

Lemma 2. *An edge-colored graph $G(V, E, C, f)$ is $(t+1)$-color connected if and only if, for all i_1, i_2, ..., $i_{\gamma-t} \leq \gamma$, $(V, E_{i_1} \cup E_{i_2} \cup \cdots \cup E_{i_{\gamma-t}})$ is a connected graph, where $E_1, E_2, \ldots, E_\gamma$ is a partition of E under the γ different colors.*

As we have mentioned in the previous section, the Euler's result claims that K_{2n} can be partitioned into n spanning trees. Thus, by Lemma 2, we have the following theorem.

Theorem 3. *(Euler) For $n = 2\gamma$, there is a coloration $G(V, E, C, f)$ of K_n such that G is $(\gamma - 1)$-color connected.*

In the following, we extend Theorem 3 to the general case of $n \geq 2\gamma$.

Lemma 4. *For $n \geq 2\gamma$ and $\gamma \geq 2$, there exists a graph $G(V,E)$ with $|V| = n, |E| = \gamma(n-1)$, and $E = E_1 \cup E_2 \cup \cdots \cup E_\gamma$ such that the following conditions are satisfied:*

1. *$G(V, E_i)$ is a connected graph for all $0 < i \leq \gamma$;*
2. *$E_i \cap E_j = \emptyset$ for all $i \neq j \leq \gamma$.*

Proof. We prove the Lemma by induction on n and γ. For $n = 2$ and $\gamma = 1$, the Lemma holds obviously. Assume that the Lemma holds for $n_0 \geq 2\gamma_0$.

In the following, we show that the Lemma holds for $n = n_0 + 1, \gamma = \gamma_0$ and for $n = n_0 + 2, \gamma = \gamma_0 + 1$. Let $G(V_0, E_0)$ be the graph with $|V_0| = n_0, |E_0| = \gamma_0(n_0 - 1)$, and $E_0 = E_1^0 \cup E_2^0 \cup \cdots \cup E_{\gamma_0}^0$ such that the conditions in the Lemma are satisfied.

For the case of $n = n_0 + 1$ and $\gamma = \gamma_0$, let $V = V_0 \cup \{u\}$ where u is a new node that is not in V_0, and let $E_1 = E_1^0 \cup \{(u, u_1)\}$, $E_2 = E_2^0 \cup \{(u, u_2)\}$, $\ldots$, $E_{\gamma_0} = E_{\gamma_0}^0 \cup \{(u, u_{\gamma_0})\}$ where $u_1, u_2, \ldots, u_{\gamma_0}$ are distinct nodes from V_0. It is straightforward to show that $|V| = n, |E| = \gamma(n-1)$, $G(V, E_i)$ is a connected graph, and $E_i \cap E_j = \emptyset$ for all $i \neq j \leq \gamma$. Thus the Lemma holds for this case.

For the case of $n = n_0 + 2$ and $\gamma = \gamma_0 + 1$, let $V = V_0 \cup \{u, v\}$ where u, v are new nodes that are not in V_0, and define $E_1, \ldots, E_\gamma$ as follows.

1. Set $E_\gamma = \emptyset$ and $U = \emptyset$, where U is a temporary variable.
2. Define E_1:
   (a) Select an edge $(v_1, v_2) \in E_1^0$.
   (b) Let $E_1 = \left(E_1^0 \setminus \{(v_1, v_2)\}\right) \bigcup \{(v_1, u), (u, v), (v, v_2)\}$.
   (c) Let $E_\gamma = E_\gamma \cup \{(v, v_1), (v_1, v_2), (v_2, u)\}$ and $U = U \cup \{v_1, v_2\}$.
3. Define E_i for $2 \leq i \leq \gamma_0$:
   (a) Select $v_{2i-1}, v_{2i} \notin U$.
   (b) Let $E_i = E_i^0 \cup \{(u, v_{2i-1}), (v, v_{2i})\}$.
   (c) Let $E_\gamma = E_\gamma \cup \{(v, v_{2i-1}), (u, v_{2i})\}$ and $U = U \cup \{v_{2i-1}, v_{2i}\}$.

It is straightforward to show that $|V| = n, |E_i| = (n - 1)$ (thus $|E| = \gamma(n-1)$), $G(V, E_i)$ is a connected graph, and $E_i \cap E_j = \emptyset$ for all $i \neq j \leq \gamma$. This completes the proof of the Lemma. Q.E.D.

Theorem 5. *Given n, γ, t with $\gamma = t + 1$, there exists a $(t + 1)$-color connected edge-colored graph $G(V, E, C, f)$ with $|V| = n$ and $|C| = \gamma$ if and only if $n \geq 2\gamma$.*

Proof. By Lemma 2, a $(t + 1)$-color connected edge-colored graph $G(V, E, C, f)$ with $|V| = n$ and $|C| = \gamma = t + 1$ contains at least $\gamma(n - 1)$ edges. Meanwhile, $G(V, E, C, f)$ contains at most $n(n-1)/2$ edges. Thus for $n < 2\gamma$, we have $n(n - 1)/2 < \gamma(n - 1)$. In other words, for $n < 2\gamma$, there is no $(t + 1)$-color connected edge-colored graph $G(V, E, C, f)$ with $|V| = n$ and $|C| = \gamma = t + 1$. Now the theorem follows from Lemmas 2 and 4. Q.E.D

4. Necessary conditions for general cases

First we note that for an edge-colored graph G to be $(t + 1)$-color connected, each node must have a degree of at least $t+1$. Thus the total degree of an n-node graph should be at least $n(t + 1)$. This implies the following lemma.

Lemma 6. *For $\gamma \geq t+1 > 1$, and a $(t+1)$-color connected edge-colored graph $G(V, E, C, f)$ with $|V| = n$, $|E| = m$, and $|C| = \gamma$, we have $2m \geq (t + 1)n$.*

In the following, we use cover free family concepts to study the necessary conditions for edge-colored graphs connectivity.

Definition 7. *Let X be a finite set with $|X| = m$ and $\mathcal{F}$ be a set of mutually disjoint subsets of X with $|\mathcal{F}| = \gamma$. Then $(X, \mathcal{F})$ is called an (m, γ)-partition of X if $X = \bigcup_{P \in \mathcal{F}} P$. Let n, t be positive integers. An (m, γ)-partition $(X, \mathcal{F})$ is called a $(t; n-1)$-cover free family (or $(t; n - 1)$-CFF(m, γ)) if, for any t elements $B_1, \ldots, B_t \in \mathcal{F}$, we have that*

$$\left| X \setminus \left(\bigcup_{i=1}^{t} B_i \right) \right| \geq n - 1 \text{ or } \left| \bigcap_{i=1}^{t} (X \setminus B_i) \right| \geq n - 1$$

It should be noted that our above definition of cover-free family is different from the generalized cover-free family definition for set systems in the literature. In [8], a set system $(X, \mathcal{F})$ is called a $(w, t; n - 1)$-cover free family if for any w blocks $A_1, \ldots, A_w \in \mathcal{F}$ and any t blocks $B_1, \ldots, B_t \in \mathcal{F}$, one has $\left|\left(\cap_{j=1}^{w} A_j\right) \setminus \left(\cup_{i=1}^{t} B_i\right)\right| \geq n - 1$. Specifically, there are two major differences between our (m, γ)-partition system and the set systems in the literature.

1. For a set system $(X, \mathcal{F})$, $\mathcal{F}$ may contain repeated elements.
2. For a set system $(X, \mathcal{F})$, the elements in $\mathcal{F}$ are not necessarily mutually disjoint.

It is straightforward to show that an edge-colored graph G is $(t+1)$-color connected if and only if for any color set $C_t \subseteq C$ of size t, after the removal of edges in G with colors in C_t, G remains connected. Assume that G contains n nodes. Then a necessary condition for connectivity is that G contains at least $n-1$ edges. From this discussion, we get the following lemma.

Lemma 8. *For an edge-colored graph $G(V,E,C,f)$, with $|V|=n$, $|E|=m$, $|C|=\gamma$, a necessary condition for $G(V,E,C,f)$ to be $(t+1)$-color connected is that the (m,γ)-partition $(X,\mathcal{F})$ is a $(t;n-1)$-CFF(m,γ) with $X=E$ and $\mathcal{F}=\{E_c : c\in C\}$ where $E_c=\{e : f(e)=c, e\in E\}$.*

In the following, we analyze lower bounds for the number m of edges for the existence of a $(t;n-1)$-CFF(m,γ). For a set partition $(X,\mathcal{F})$ and a positive integer t, let

$$\mu(X,\mathcal{F};t)=\min\left\{\left|X\setminus\left(\bigcup_{i=1}^{t}B_i\right)\right| : B_1,\ldots,B_t\in\mathcal{F}\right\}$$

It is straightforward to see that a (m,γ)-partition $(X,\mathcal{F})$ is a $(t;n-1)$-CFF(m,γ) if and only if $\mu(X,\mathcal{F};t)\geq n-1$.

Given positive integers m,γ,t, let

$$\mu(m,\gamma;t)=\max_{(m,\gamma)\text{-partition }(X,\mathcal{F})}\mu(X,\mathcal{F};t)$$

From the above discussion and Lemma 6, we have the following theorem.

Theorem 9. *Let m,γ,t be given positive integers. $\mu(m,\gamma;t)\geq n-1$ and $2m\geq(t+1)n$ are necessary conditions for the existence of a $(t+1)$-color connected edge-colored graph $G(V,E,C,f)$, with $|V|=n$, $|E|=m$, $|C|=\gamma$.*

Theorem 10. *Let m,γ,t be given positive integers. We have*

1. *if $t\geq m-\lfloor\frac{m}{\gamma}\rfloor\cdot\gamma$, then $\mu(m,\gamma;t)=(\gamma-t)\cdot\lfloor\frac{m}{\gamma}\rfloor$*
2. *if $t<m-\lfloor\frac{m}{\gamma}\rfloor\cdot\gamma$, then $\mu(m,\gamma;t)=(\gamma-t)\cdot\lfloor\frac{m}{\gamma}\rfloor+\Big(m-\lfloor\frac{m}{\gamma}\rfloor\cdot\gamma-t\Big)$.*

Proof. For a given (m,γ)-partition $(X,\mathcal{F})$, let $B_1,\ldots,B_\gamma$ be an enumeration of elements in $\mathcal{F}$ such that $|B_i|\leq|B_{i+1}|$ for all $i<\gamma$. It is straightforward to show that $\mu(X,\mathcal{F};t)=\sum_{i=1}^{\gamma-t}|B_i|$. Thus $\mu(m,\gamma;t)$ takes the maximum value if $\sum_{i=1}^{\gamma-t}|B_i|$ is maximized. It is straightforward to show that this value is maximized when the (m,γ)-partition $(X,\mathcal{F})$ satisfies the following conditions:

1. $|B_i|=\lfloor\frac{m}{\gamma}\rfloor$ for $i\leq\gamma-\Big(m-\lfloor\frac{m}{\gamma}\rfloor\cdot\gamma\Big)$, and
2. $|B_i|=\lfloor\frac{m}{\gamma}\rfloor+1$ for $\gamma\geq i>\gamma-\Big(m-\lfloor\frac{m}{\gamma}\rfloor\cdot\gamma\Big)$.

The theorem follows from the above discussion. Q.E.D.

Example 1. *For $n=7, m=10, \gamma=5$, and $t=2$, we have $\mu(10,5;2)=6=n-1$. However, $2m=20<(t+1)n=21$. This shows that the condition $2m\geq(t+1)n$ in Theorem 9 is not redundant.*

Example 2. *There are no $(t+1)$-color connected edge-colored graph $G(V,E,C,f)$ for the following special cases:*

1. $\gamma=2, t=1, n=3$.
2. $\gamma=4, t=2, n=4$.
3. $\gamma=3, t=2, n\leq 5$.

Proof. Before we consider the specific cases, we observe that, when γ and t are fixed, the function μ is non-decreasing when m increases.

1. In this case, the maximum value that m could take is 3. Thus $\mu(3,2;1)=1<n-1=2$. That is, there is no $(1;2)$-CFF$(3,2)$, which implies the claim. Note that this result also follows from Theorem 5.

2. In this case, the maximum value that m could take is 6. Thus $\mu(6,4;2)=2<n-1=3$.

3. We only show this for the case $\gamma=3, t=2, n=5$. In this case, the maximum value that m could take is 10. Thus $\mu(10,3;2)=3<n-1=4$. Note that this result also follows from Theorem 5. Q.E.D

The following theorem is a variant of Theorem 9.

Theorem 11. *For $\gamma-1>t>0$, a necessary condition for the existence of a $(t+1)$-color connected edge-colored graph $G(V,E,C,f)$ with $|V|=n$, $|E|=m$, and $|C|=\gamma$ is that $2m\geq(t+1)n$ and the following conditions are satisfied:*

- *If $n=(\gamma-t)k$ for some integer $k>0$, then $m\geq\gamma k-1$.*
- *If $n=(\gamma-t)k+1$ for some integer $k>0$, then $m\geq\gamma k$.*
- *If $n=(\gamma-t)k+2$ for some integer $k>0$, then $m\geq\gamma k+t+1$.*
- $\cdots\cdots$
- *If $n=(\gamma-t)k+\gamma-t-1$ for some integer $k>0$, then $m\geq\gamma k+\gamma-2$.*

Proof. For $\gamma > t+1$, by Theorem 10, we have

$$\mu(m,\gamma;t) = \begin{cases} (\gamma-t)k' & m=\gamma k'+i \\ (\gamma-t)k'+1 & m=\gamma k'+t+1 \\ \cdots\cdots & \\ (\gamma-t)k'+\gamma-t-1 & m=\gamma k'+\gamma-1 \end{cases}$$

where $0 \le i \le t$.

Thus the necessary condition $\mu(m,\gamma;t) \ge n-1$ in Theorem 9 can be interpreted as the following conditions:

$$k' \ge \begin{cases} \frac{n-1}{\gamma-t} & \text{if } m=\gamma k'+i \text{ for } 0\le i\le t \\ \frac{n-2}{\gamma-t} & \text{if } m=\gamma k'+t+1 \\ \cdots\cdots & \\ \frac{n-\gamma+t}{\gamma-t} & \text{if } m=\gamma k'+\gamma-1 \end{cases}$$

In other words, for a $(t+1)$-color connected edge-colored graph $G(V,E,C,f)$, one of the following $\gamma-t$ conditions is satisfied:

- $|V|=n, |E| \ge \gamma \left\lceil \frac{n-1}{\gamma-t} \right\rceil$, and $|C|=\gamma$.
- $|V|=n, |E| \ge \gamma \left\lceil \frac{n-2}{\gamma-t} \right\rceil + t+1$, and $|C|=\gamma$.
- $\cdots\cdots$
- $|V|=n, |E| \ge \gamma \left\lceil \frac{n-\gamma+t}{\gamma-t} \right\rceil + \gamma-1$, and $|C|=\gamma$.

By distinguishing the cases for $n=(\gamma-t)k$, $n=(\gamma-t)k+1$, $\cdots$, and $n=(\gamma-t)k+\gamma-t-1$, and by reorganizing the above lines, these necessary conditions can be interpreted as the following $\gamma-t$ conditions:

- $n=(\gamma-t)k$ and $m \ge \gamma k-1$ for some $k>0$. Note that this follows from the last line of the above conditions (one can surely take other lines, but then the bound for m would be larger). This comment applies to the following cases too.
- $n=(\gamma-t)k+1$ and $m \ge \gamma k$ for some $k>0$.
- $n=(\gamma-t)k+2$ and $m \ge \gamma k+t+1$ for some $k>0$.
- $\cdots\cdots$
- $n=(\gamma-t)k+\gamma-t-1$ and $m \ge \gamma k+\gamma-2$ for some $k>0$.

Q.E.D.

5. Necessary and sufficient conditions for practical cases (with small γ and t)

Generally we are interested in the question whether the necessary condition in Theorems 9 and 11 are also sufficient. In the following, we show that this is true for several important practical cases.

Theorem 12. *The necessary conditions in Theorem 9 are sufficient for the case of* $\gamma = t+1$.

Proof. Since $m - \lfloor \frac{m}{\gamma} \rfloor \cdot \gamma$ is the remainder of m divided by γ, we trivially have $t = \gamma - 1 \ge m - \lfloor \frac{m}{\gamma} \rfloor \cdot \gamma$. Now assume that $\gamma > \frac{n}{2}$. By Theorem 10, we have $\mu(m,\gamma;t) = \lfloor \frac{m}{\gamma} \rfloor \le \lfloor \frac{n(n-1)}{2\gamma} \rfloor < n-1$. The rest follows from Theorem 5. Q.E.D.

Before we show that the necessary conditions in Theorems 9 and 11 are sufficient for the case of $t=1$, we first present two lemmas whose proofs are straightforward.

Lemma 13. *For* $n=\gamma=m\ge 3$ *and* $t=1$*, the following* γ*-node circle graph is* $(1+1)$*-color connected:*

$$\{(v_1,v_2),(v_2,v_3),\ldots,(v_\gamma,v_1)\}$$

with $f(v_i,v_{i+1})=c_i$ *for* $i<\gamma$ *and* $f(v_\gamma,v_1)=c_\gamma$.

Lemma 14. *For* $t=1$, $\gamma\ge 3$, *and* $\gamma<n\le 2\gamma-2$, *the graph in Figure 1 with the edges:*

$$\{(v_1,v_2),(v_2,v_3),\ldots,(v_\gamma,v_1)\}\cup \\ \{(v_\gamma,v_{\gamma+1}),(v_{\gamma+1},v_{\gamma+2}),\ldots,(v_n,v_1)\}$$

and colors defined by

$$\begin{aligned} f(v_i,v_{i+1}) &= c_i & \text{for } 1\le i\le\gamma-1 \\ f(v_\gamma,v_1) &= c_\gamma & \\ f(v_{\gamma+i-1},v_{\gamma+i}) &= c_i & \text{for } 1\le i\le n-\gamma \\ f((v_n,v_1)) &= c_{n-\gamma+1} & \end{aligned}$$

is $(1+1)$*-color connected.*

Before we show that the necessary conditions in Theorem 9 are also sufficient for the case of $t=1$, we first prove this for $\gamma=3$.

Theorem 15. *The necessary conditions in Theorem 9 are sufficient for the case of* $\gamma=3$ *and* $t=1$.

Proof. For $\gamma=3$ and $t=1$, we have

$$\mu(m,\gamma;t) = \begin{cases} 2k' & \text{if } m=3k' \text{ or } m=3k'+1 \\ 2k'+1 & \text{if } m=3k'+2 \end{cases}$$

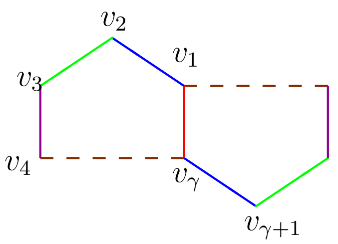

Figure 1: The Graph for Lemma 14

By the condition $\mu(m, \gamma; t) \geq n - 1$, the necessary condition is converted to the following conditions:

$$k' \geq \begin{cases} \frac{n-1}{2} & \text{if } m = 3k' \text{ or } m = 3k' + 1 \\ \frac{n-2}{2} & \text{if } m = 3k' + 2 \end{cases}$$

Thus in order to prove the theorem, it is sufficient to construct a $(1+1)$-color connected edge-colored graph $G(V, E, C, f)$ for each of the following two conditions:

- $|V| = n, |E| = 3\left\lceil \frac{n-1}{2} \right\rceil$, and $|C| = 3$.
- $|V| = n, |E| = 3\left\lceil \frac{n-2}{2} \right\rceil + 2$, and $|C| = 3$.

By distinguishing the cases for $n = 2k$ and $n = 2k + 1$, it is sufficient to construct the required edge-colored graph for each of the following two conditions:

- $n = 2k$, $m = 3k - 1$, and $\gamma = 3$.
- $n = 2k + 1$, $m = 3k$, and $\gamma = 3$.

For the case of $n = 2k$, let

$$\begin{array}{lcl} V & = & \{v_1, \cdots, v_{2k}\}, \\ E_1 & = & \{(v_1, v_{2i}) : 1 \leq i < k\} \\ E_2 & = & \{(v_1, v_{2i+1}) : 1 \leq i < k\} \cup \{(v_1, v_{2k})\} \\ E_3 & = & \{(v_{2i}, v_{2i+1}) : 1 \leq i < k)\} \cup \{(v_2, v_{2k})\} \\ E & = & E_1 \cup E_2 \cup E_3 \end{array}$$

For each $e \in E_i$ $(i \leq 3)$, let $f(e) = c_i$. Then it is straightforward to check that the edge-colored graph $G(V, E, C, f)$ is $(1+1)$-color connected, $|V| = n$, and $|E| = 3k - 1$.

For the case of $n = 2k + 1$, let

$$\begin{array}{lcl} V & = & \{v_1, \cdots, v_{2k+1}\}, \\ E_1 & = & \{(v_1, v_{2i}) : 1 \leq i \leq k\} \\ E_2 & = & \{(v_1, v_{2i+1}) : 1 \leq i \leq k\} \\ E_3 & = & \{(v_{2i}, v_{2i+1}) : 1 \leq i \leq k)\} \\ E & = & E_1 \cup E_2 \cup E_3 \end{array}$$

For each $e \in E_i$ $(i \leq 3)$, let $f(e) = c_i$. Then it is straightforward to check that the edge-colored graph $G(V, E, C, f)$ is $(1+1)$-color connected, $|V| = n$, and $|E| = 3k$, Q.E.D.

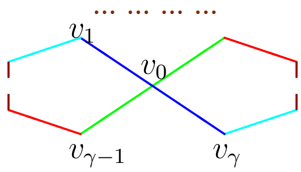

Figure 2: Graph for the case $n = (\gamma - 1)k + 1$, $m \geq k\gamma$

Corollary 16. *For $\gamma = 3$, $t = 1$, and $n, m > 0$, there exists a $(1+1)$-color connected edge-colored graph $G(V, E, C, f)$ with $|V| = n$ and $|E| = m$ if and only if $m \geq \min\left\{3\left\lceil \frac{n-1}{2} \right\rceil, 3\left\lceil \frac{n-2}{2} \right\rceil + 2\right\}$.*

Now let us prove the theorem for the general case of $t = 1$.

Theorem 17. *The necessary conditions in Theorems 9 and 11 are sufficient for the case of $t = 1$.*

Proof. For the case of $\gamma = 2$ and $t = 1$, it follows from Theorem 12. Now assume that $\gamma > 2$ and $t = 1$. In this special case, the necessary conditions in Theorem 11 are as follows:

- $n = (\gamma - 1)k$ and $m \geq \gamma k - 1$ for some $k > 0$.
- $n = (\gamma - 1)k + 1$ and $m \geq \gamma k$ for some $k > 0$.
- $n = (\gamma - 1)k + 2$ and $m \geq \gamma k + 2$ for some $k > 0$.
- $\cdots\cdots$
- $n = (\gamma - 1)k + \gamma - 2$ and $m \geq \gamma k + \gamma - 2$ for some $k > 0$.

In the following we first show that the condition "$n = (\gamma - 1)k + 1$ and $m \geq k\gamma$" is sufficient. Let the graph in Figure 2 be defined as follows:

$$\begin{array}{lcl} V & = & \{v_0, v_1, \cdots, v_{(\gamma-1)k}\}, \\ E_1 & = & \{(v_0, v_{(\gamma-1)i+1}) : 0 \leq i \leq k - 1\} \\ E_j & = & \{(v_{(\gamma-1)i+j-1}, v_{(\gamma-1)i+j}) : 0 \leq i \leq k - 1\} \\ & & \quad \text{for } 2 \leq j \leq \gamma - 1 \\ E_\gamma & = & \{(v_{(\gamma-1)i}, v_0) : 1 \leq i \leq k\} \\ E & = & E_1 \cup E_2 \cup \cdots \cup E_\gamma \end{array}$$

For each $e \in E_j$ with $j \leq \gamma$, let $f(e) = c_j$. Then it is straightforward to check that the edge-colored graph $G(V, E, C, f)$ is $(1+1)$-color connected, $|V| = (\gamma - 1)k + 1$, and $|E| = \gamma k$.

Now we show that the condition "$n = (\gamma - 1)k + j$ and $m \geq k\gamma + j$ for $2 \leq j \leq \gamma - 1$" is sufficient. Let $G(V, E, C, f)$ be the edge-colored graph that we have just constructed with $|V| = (\gamma - 1)k + 1$, and $|E| = \gamma k$.

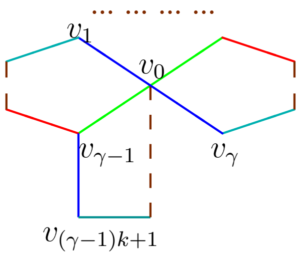

Figure 3: Graph for the case $n = (\gamma-1)k + j$, $m \geq k\gamma + j$

Let $V' = V \cup \{v_{(\gamma-1)k+1}, \ldots, v_{(\gamma-1)k+j-1}\}$. Define a new edge-colored graph $G(V', E', C, f')$ (see Figure 3) by attaching the following edges to the γ-node circle $\{(v_0, v_1), (v_1, v_2), \ldots, (v_{\gamma-1}, v_0)\}$:

$$\{(v_{\gamma-1}, v_{(\gamma-1)k+1}), (v_{(\gamma-1)k+1}, v_{(\gamma-1)k+2}), \ldots, (v_{(\gamma-1)k+j-1}, v_0)\}$$

The colors for the new edges are defined by letting $f'(v_{(\gamma-1)k+i}, v_{(\gamma-1)k+i+1}) = c_{i+1}$ for $0 \leq i \leq j-2$ and $f'(v_{(\gamma-1)k+j-1}, v_0) = c_j$ (note that $f = f'$ when restricted to E). It is straightforward to check that $G(V', E', C, f')$ is $(1+1)$-color connected, $|V| = (\gamma-1)k + j$, and $|E| = \gamma k + j$. Q.E.D.

Corollary 18. *For $t = 1$ and γ, $n, m > 1$, there exists a $(1+1)$-color connected edge-colored graph $G(V, E, C, f)$ with $|V| = n$ and $|E| = m$ if and only if m is larger than or equal to the minimum of the following values:*

$$\gamma\left\lceil\frac{n-1}{\gamma-1}\right\rceil, \gamma\left\lceil\frac{n-2}{\gamma-1}\right\rceil + 2, \ldots, \gamma\left\lceil\frac{n-\gamma+1}{\gamma-1}\right\rceil + \gamma - 1$$

Proof. It follows from the proof of Theorem 17. Q.E.D

Theorem 19. *The conditions in Theorems 9 and 11 are sufficient for the case of $\gamma = 4, t = 2$.*

Proof. It is sufficient to show that both of the conditions "$n = (\gamma-t)k+1$ and $m \geq k\gamma$" and "$n = (\gamma-t)k+2$ and $m \geq \gamma k + t + 1$" are sufficient (note that $\gamma = 4$ and $t = 2$). In the following we first show that the condition "$n = (\gamma-t)k+1$ and $m \geq k\gamma$" is sufficient by induction on k.

For the case of $k = 2$, we have $n = 5, m = 8, \gamma = 4$, and $t = 2$. Let the graph G_1 in Figure 4 be defined by the edges

$$\{(v_1, v_2)_1, (v_2, v_3)_2, (v_3, v_4)_1, (v_4, v_5)_3, (v_5, v_1)_2, (v_1, v_3)_3, (v_1, v_4)_4, (v_2, v_5)_4\}$$

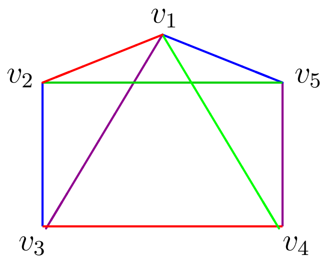

Figure 4: Graph for the case $n = 5, \gamma = 4, t = 2$

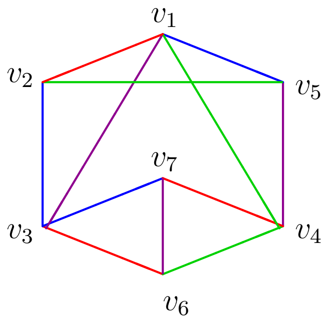

Figure 5: Graph for the case $n = 7, \gamma = 4, t = 2$

where $(v, v')_i$ means that the edge (v, v') takes color c_i. It is straightforward to check that G_1 is $(2+1)$-color connected.

For the case of $k = 3$, we have $n = 7, m = 12, \gamma = 4$, and $t = 2$. Let the graph G_2 in Figure 5 be defined as

$$\{(v_1, v_2)_1, (v_2, v_3)_2, (v_4, v_5)_3, (v_5, v_1)_2, (v_1, v_3)_3, (v_1, v_4)_4, (v_2, v_5)_4, (v_3, v_6)_1, (v_6, v_7)_3, (v_7, v_4)_1, (v_4, v_6)_4, (v_3, v_7)_2\}$$

where $(v, v')_i$ means that the edge (v, v') takes color c_i. It is straightforward to check that G_2 is $(2+1)$-color connected.

Now for $k = 2r$ ($r \geq 2$), we have $n = (\gamma-t)k+1 = 4r+1$ and $m = k\gamma = 8r$. If we glue the v_1 node of r copies of G_1, we get a $(t+1)$-color connected edge-colored graph G with $n = 4r+1$ and $m = 8r$. Thus the condition for the case of $k = 2r$ holds.

For $k = 2r+1$ ($r \geq 2$), we have $n = (\gamma-t)k+1 = 4r+3$ and $m = k\gamma = 8r+4$. If we glue the v_1 node of $r-1$ copies of G_1 and one copy of G_2, we get a $(t+1)$-color connected edge-colored graph G with $n = 4(r-1)+1+6 = 4r+3$ and $m = 8(r-1)+12 = 8r+4$. Thus the condition for the case of $k = 2r+1$ holds. This completes the induction.

For the condition "$n = (\gamma-t)k+2$ and $m \geq \gamma k + t + 1$", one can add one node to the graph for the case "$n = (\gamma-t)k+1$ and $m \geq k\gamma$" with 3 edges (with

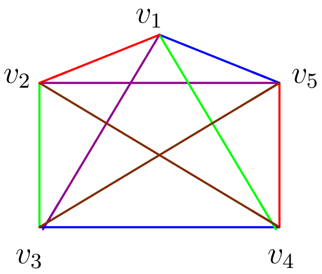

Figure 6: Graph for the case $n = 5, \gamma = 5, t = 3$

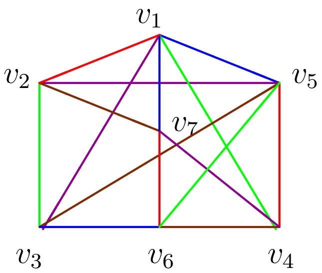

Figure 7: Graph for the case $n = 7, \gamma = 5, t = 3$

distinct colors) to any three nodes. The resulting graph meets the requirements. Q.E.D.

Theorem 19 could be extended to the case of $\gamma = 5$ and $t = 3$.

Theorem 20. *The conditions in Theorems 9 and 11 are sufficient for the case of $\gamma = 5$ and $t = 3$.*

Proof. It is sufficient to show that both of the conditions "$n = (\gamma - t)k + 1$ and $m \geq k\gamma$" and "$n = (\gamma - t)k + 2$ and $m \geq \gamma k + t + 1$" are sufficient (note that $\gamma - t = 2$). In the following we first show that the condition "$n = 2k + 1$ and $m \geq k\gamma$" is sufficient by induction on k and γ.

For $\gamma = 5$ and $k = 2$, we have $n = 5, m = 10$. The graph in Figure 6 shows that the condition is sufficient also. For the case of $k = 3$, we have $n = 7, m = 15$. The graph in Figure 7 shows that the condition is sufficient also.

For $k = 2r$ ($r \geq 2$), the condition becomes $n = (\gamma - t)k + 1 = 4r + 1$ and $m = k\gamma = 10r$. If we glue the v_1 node of r copies of $G_{5,1}$, we get a $(t + 1)$-color connected edge-colored graph G with $n = 4r + 1$ and $m = 10r$. Thus the condition for the case of $k = 2r$ holds.

For $k = 2r + 1$ ($r \geq 2$), the condition becomes $n = (\gamma - t)k + 1 = 4r + 3$ and $m = k\gamma = 10r + 5$. If we glue the v_1 node of $r - 1$ copies of $G_{5,1}$ and one copy of $G_{5,2}$, we get a $(t + 1)$-color connected edge-colored graph G with $n = 4(r - 1) + 1 + 6 = 4r + 3$ and $m = 10(r - 1) + 15 = 10r + 5$. Thus the condition for the case of $k = 2r + 1$ holds. This completes the induction.

For the condition "$n = (\gamma - t)k + 2$ and $m \geq \gamma k + t + 1$", we have $n = 2k + 2$ and $m \geq 5k + 4$. We can add one node to the graph for the case "$n = (\gamma - t)k + 1$ and $m \geq k\gamma$" with 4 edges (with distinct colors) to any four nodes. The resulting graph meets the requirements. Q.E.D.

Open Question: We showed in this section that the conditions in Theorems 9 and 11 are sufficient for practical cases. It would be interesting to show that these conditions are also sufficient for general cases.

6. Hardness results

We have given necessary and sufficient conditions for $(t + 1)$-color connected edge-colored graphs. It is also important to determine whether a given graph is $(t + 1)$-color connected. Unfortunately, the following Theorem shows that the problem is **coNP**-complete. The ceConnect problem is defined as follows.

INSTANCE: An edge-colored graph $G = G(V, E, C, f)$, two nodes $A, B \in V$, and a positive integer $t \leq |C|$.
QUESTION: Are A and B $(t + 1)$-color connected?

Before we prove the hardness result, we first introduce the concept of a color separator. For an edge-colored graph $G = G(V, E, C, f)$, a color separator for two nodes A and B of the graph G is a color set $C' \subseteq C$ such that the removal of all edges with colors in C' from the graph G will disconnect A and B. It is easy to observe that A and B are $(t + 1)$-color connected if and only there is no t-size color separator for A and B.

Theorem 21. *The problem ceConnect is* **coNP**-*complete.*

Proof. It is straightforward to show that the problem is in **coNP**. Thus it is sufficient to show that it is **coNP**-hard. The reduction is from the Vertex Cover problem. The VC problem is as follows (definition taken from [6]):

INSTANCE: A graph $G = (V, E)$ and a positive integer $t \leq |V|$.
QUESTION: Is there a vertex cover of size t or less for G, that is, a subset $V' \subseteq V$ with $|V'| \leq t$ and, for each edge $(u, v) \in E$, at least one of u and v belongs to V'?

For a given instance $G = (V, E)$ of VC, we construct a edge-colored graph $G_c = (V_c, E_c, f, C)$ as follows.

First assume that the vertex set V is ordered as in $V = \{v_1, \ldots, v_n\}$. Let

$$\begin{array}{rcl} V_c & = & \{A, B\} \bigcup \{e_{(v_i,v_j)} : (v_i, v_j) \in E \text{ and } i < j\} \\ E_c & = & \{(A, e_{(v_i,v_j)}), (e_{(v_i,v_j)}, B) : (v_i, v_j) \in E\} \\ C & = & \{c_v : v \in V\} \\ f & = & \{f(A, e_{(v_i,v_j)}) = c_{v_i}, f(e_{(v_i,v_j)}, B) = c_{v_j} : \\ & & (v_i, v_j) \in E, i < j\} \end{array}$$

In the following, we show that there is a vertex cover of size t in G if and only if there is a t-color edge separator for G_c.

Without loss of generality, assume that $V' = \{v'_1, \ldots, v'_k\}$ is a vertex cover for G. Then it is straightforward that $C' = \{c_{v'_i} : v'_i \in V'\}$ is a color separator for G_c since each incoming path for B in G_c contains two colors corresponding to one edge (v_i, v_j) in G.

For the other direction, assume that $C' = \{c_{v'_i} : i = 1, \ldots, t\}$ is a t-color separator for G_c. Let $V' = \{v'_i : c_{v'_i} \in C'\}$. By the fact that C' is a color separator for G_c, for each edge $(v_i, v_j) \in E$ in G, the path $(A, e_{(v_i,v_j)}, B)$ in G_c contains at least one color from C'. Since this path contains only two colors c_{v_i} and c_{v_j}, we know that v_i or v_j or both belong to V'. In another word, V' is a t-size vertex cover for G. This completes the proof of the Theorem. Q.E.D.

7. Disjunct systems

We conclude our paper with some observations on the relationship between disjunct system and cover free families. Incidence matrix is usually used to describe set systems. Let $(X, \mathcal{F})$ be a (m, γ)-partition of X with $X = \{x_1, \ldots, x_m\}$ and $\mathcal{F} = \{B_1, \ldots, B_\gamma\}$. Then the incidence matrix of $(X, \mathcal{F})$ is the $m \times \gamma$ matrix $(a_{i,j})$ where $a_{i,j} = 1$ if $x_i \in B_j$ and $a_{i,j} = 0$ otherwise. If A is an incidence matrix of a set system, then A^T (the transpose of A) is an extended incidence matrix of a disjunct system. Note that by extended incidence matrix, we mean, after consolidating repeated columns of the matrix we get the incident matrix of a disjunct system.

Definition 22. *Let Y be a set of γ elements, and $\mathcal{B}$ be a set of m subsets of Y. Then the set system $(Y, \mathcal{B})$ is called a $(t; n-1)$-disjunct system (or $(t; n-1)$-DS(γ, m)) if for any $P \subseteq Y$ such that $|P| \leq t$, there exist at least $n-1$ blocks $B \in \mathcal{B}$ such that $P \cap B = \emptyset$.*

Theorem 23.
1. *If there exists a $(t; n-1)$-CFF(m, γ) then there exists a $(t; n'-1)$-DS(γ, m') for some $1 < n' \leq n$ and $m' \leq m$.*
2. *If there exists a $(t; n-1)$-DS(γ, m), then there exists a $(t; n-1)$-CFF(m', γ) for some $0 < m' \leq m$.*

Proof. Assume that $(X, \mathcal{F})$ is a $(t; n-1)$-CFF(m, γ) with incidence matrix A. Let $Y = \mathcal{F}$ and $\mathcal{B} = \{[x] : x \in X\}$ where $[x] = \{P : x \in P \text{ and } P \in \mathcal{F}\}$. In the following, we show that $(Y, \mathcal{B})$ is a $(t; n'-1)$-DS(γ, m') with extended incidence matrix A^T for some $1 < n' \leq n$ and $m' \leq m$. By the fact that $(X, \mathcal{F})$ is a $(t; n-1)$-CFF(m, γ), for any $P = \{B_1, \ldots, B_t\} \subseteq Y$, there exist distinct $x_1, \ldots, x_{n-1} \in X \setminus (\cup_{i=1}^{t} B_i)$. That is, for any $i \leq n-1$ and $j \leq t$, we have $x_i \notin B_j$ which means $B_j \notin [x_i]$. Thus $P \cap [x_i] = \emptyset$ for all $i \leq n-1$. Note that for $i \neq j$, we may have $[x_i] = [x_j]$. Thus the above arguments only guarantee that there exists $n' > 1$ such that $(Y, \mathcal{B})$ is a $(t; n'-1)$-DS(γ, m').

For the other direction, assume that $(Y, \mathcal{B})$ is a $(t; n-1)$-DS(γ, m) with incidence matrix A. Let $X = \mathcal{B}$ and $\mathcal{F} = \{[y] : y \in Y\}$ where $[y] = \{P : y \in P \text{ and } P \in \mathcal{B}\}$. In the following, we show that $(X, \mathcal{F})$ is a $(t, n-1)$-CFF(m, γ) with incidence matrix A^T. For any t blocks $[y_1], \ldots, [y_t] \in \mathcal{F}$, let $P = \{y_1, \ldots, y_t\}$. By the fact that $(Y, \mathcal{B})$ is a $(t, n-1)$-DS(γ, m), there exist distinct blocks $B_1, \ldots, B_{n-1} \in \mathcal{B}$ such that $P \cap B_i = \emptyset$. That is, for each $i \leq t$ and $j \leq n-1$, we have $y_i \notin B_j$ which means $B_j \notin [y_i]$. Thus $\{B_1, \ldots, B_{n-1}\} \in X \setminus (\cup_{i=1}^{t} [y_t])$. It follows that $(X, \mathcal{F})$ is a $(t, n-1)$-CFF(m, γ). Q.E.D.

Acknowledgment

The first author would like to thank Professors Doug Stinson and Ruizhong Wei for some discussions on cover-free families, and thank the anonymous reviewers for several valuable comments.

References

[1] G. Constantine. Colorful isomorphic spanning trees in complete graphs. *Annals of Combinatorics* **9**:163–167, 2005.

[2] Y. Desmedt and Y. Wang. Perfectly Secure Message Transmission Revisited. In *Proc. EuroCrypt'02*, pages 502-517. LNCS 2332, Springer-Verlag

[3] Y. Desmedt, Y. Wang, and M. Burmester. A complete characterization of tolerable adversary structures for secure point-to-point transmissions without feedback. In *Proc. ISAAC 2005*, pages 277–287. LNCS 3827. Springer Verlag.

[4] Y. Desmedt, Y. Wang, R. Safavi-Naini, and H. Wang. Radio networks with reliable communications. In *Proc. COCOON*, pages 156-166, LNCS 3595, 2005.

[5] K. Engel. Interval packing and covering in the boolean lattice. *Combin. Probab. Comput.* **5**:373–384, 1995.

[6] M.R. Garey and D.S. Johnson. *Computers and Intractability: A Guide to the Theory of* **NP**-*Completeness*. W. H. Freeman and Company, San Francisco, 1979.

[7] J. Roskind and R. Tarjan, A note on finding minimum-cost edge-disjoint spanning trees. *Math. Oper. Res.* **10**:701–708, 1985.

[8] D. Stinson and R. Wei. Generalized cover-free families. *Discrete Math.* **279**:463–477, 2004.

[9] Y. Wang and Y. Desmedt. Secure communication in multicast channels. *Journal of Cryptology* **14**(2):121–135, 2001.