Hindawi
Security and Communication Networks
Volume 2018, Article ID 9482345, 11 pages
https://doi.org/10.1155/2018/9482345

Research Article

A New Type of Graphical Passwords Based on Odd-Elegant Labelled Graphs

Hongyu Wang,[1] **Jin Xu**,[1] **Mingyuan Ma**,[1] **and Hongyan Zhang**[2]

[1]*School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*
[2]*School of Management Science and Engineering, Shandong Normal University, Jinan 250014, China*

Correspondence should be addressed to Hongyu Wang; why5126@pku.edu.cn

Received 11 January 2018; Accepted 1 March 2018; Published 11 April 2018

Academic Editor: Zheng Yan

Graphical password (GPW) is one of various passwords used in information communication. The QR code, which is widely used in the current world, is one of GPWs. Topsnut-GPWs are new-type GPWs made by topological structures (also, called graphs) and number theory, but the existing GPWs use pictures/images almost. We design new Topsnut-GPWs by means of a graph labelling, called odd-elegant labelling. The new Topsnut-GPWs will be constructed by Topsnut-GPWs having smaller vertex numbers; in other words, they are compound Topsnut-GPWs such that they are more robust to deciphering attacks. Furthermore, the new Topsnut-GPWs can induce some mathematical problems and conjectures.

1. Introduction and Preliminary

1.1. Researching Background. Graphical passwords (GPWs) have been investigated for over 20 years, and many important results can be found in three surveys [1–3]. GPW schemes have been proposed as a possible alternative to text-based schemes. However, the existing GPWs have (i) no mathematical computation; (ii) more storage space; (iii) no individuality; (iv) geometric positions; (v) slow running speed; (vi) vulnerable to attack; and (vii) no transformation from lower safe level to high security. However, QR code is a successful example of GPW' applications in mobile devices by fast, relatively reliable and other functions [4, 5]. GPWs may be accepted by users having mobile devices with touch screen [6, 7].

Wang et al. show an idea of "topological structures plus number theory" for designing new-type GPWs (abbreviated as Topsnut-GPWs, [8–10]). All topological structures used in Topsnut-GPWs can be stored in a computer through ordinary algebraic matrices. And Topsnut-GPWs have no requirement of geometric positions for users and allow users to make their individual passwords rather than learning more rules they do not like and so on.

How to quickly build up a large scale of Topsnut-GPWs from those Topsnut-GPWs having smaller vertex numbers? How to construct a one-key versus more-locks (one-lock versus more-keys) for some Topsnut-GPWs? And how to compute Topsnut-GPWs' space by the basic computing unit 2^n? Obviously, we need enough graphs and lots of graph coloring/labellings, and we can turn more things into Topsnut-GPWs. Let G_p be the number of graphs having p vertices. From [11], we know

p	G_p	bits
18	1787577725145611700547878190848	100
19	24637809253125004524383007491432768	114
20	645490122795799841856164638490742749440	129
21	32220272899808983433502244253755283616097664	145
22	3070846483094144300637568517187105410586657814272	161
23	559946939699792080597976380819462179812276348458981632	179
24	195704906302078447922174862416726256004122075267063365754368	197

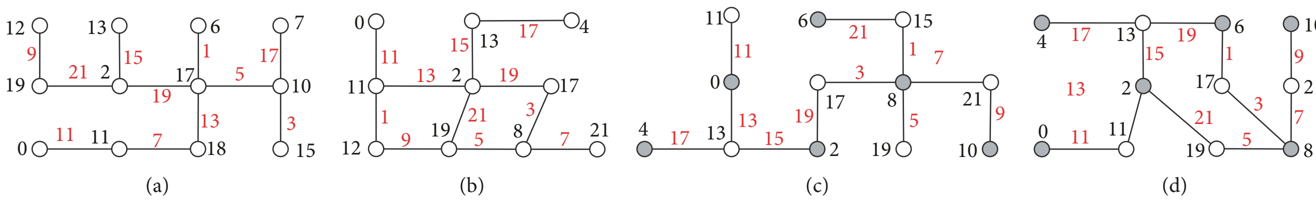


Figure 1: (a) An odd-elegant tree; (b) an odd-elegant graph; (c) a set-ordered odd-elegant tree; (d) a set-ordered odd-elegant graph.

where $G_p \approx 2^{\text{bits}}$ for $p = 18, 19, \dots, 24$. It means that adding various graph labellings enables us to design tremendous Topsnut-GPWs with huge topological structures and vast of graph coloring/labellings, since there are over 150 graph labellings introduced in [12]. As a fact, Topsnut-GPWs can generate alphanumeric passwords with longer units. As an example, we take a path $v_1 v_{10} v_{11} v_{20}$ in Figure 6(d) to produce an alphanumeric password

$$W = 1'1816141210201'10'11517211110'11'10202011'20'111579320' \tag{1}$$

by selecting the neighbors of each vertex of these four vertices v_1, v_{10}, v_{11}, and v_{20}. Clearly, such password W may have longer unit in a large scale of Topsnut-GPW for meeting the need of high level security.

In this article, we will apply a graph labelling called odd-elegant labelling [13]. And we will define some construction operations under odd-elegant labelling for designing our compound Topsnut-GPWs.

1.2. Preliminary. We use standard notation and terminology of graph theory. Graphs mentioned are loopless, with no multiple edges, undirected, connected, and finite, unless otherwise specified. Others can be found in [14]. Here, we will use A (p,q)-graph G which is one with p vertices and q edges; the symbol $[m,n]$ stands for an integer set $\{m, m+1, \dots, n\}$ for integers m and n with $0 \le m < n$; $[s,t]^o$ indicating an odd-set $\{s, s+2, \dots, t\}$, where s and t both are odd integers with $1 \le s < t$; and $[k,\ell]^e$ represents an even-set $\{k, k+2, \dots, \ell\}$, where k and ℓ are both even integers with respect to $0 \le k < \ell$.

Definition 1 (see [13]). Suppose that a (p,q)-graph G admits a mapping $f : V(G) \to [0, 2q-1]$ such that $f(u) \ne f(v)$ for distinct vertices $u, v \in V(G)$, and the label $f(uv)$ of every edge $uv \in E(G)$ is defined as $f(uv) = f(u) + f(v) \pmod{2q}$ and the set of all edge labels is equal to $[1, 2q-1]^o$. One considers f to be an *odd-elegant labelling* and G to be an *odd-elegant.*

Definition 2 (see [15]). Suppose that a bipartite graph G receives a labelling f such that $\max\{f(x) : x \in X\} < \min\{f(y) : y \in Y\}$, where (X, Y) is the bipartition of vertex set $V(G)$ of G. We call f a *set-ordered labelling* (So-labelling for short).

As shown in Figure 1, there are four different examples of Definitions 1 and 2.

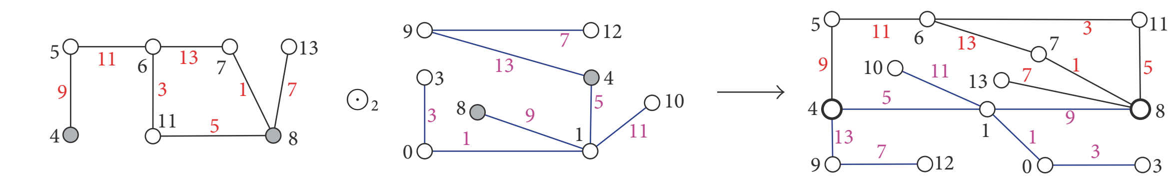
Definition 3. Let G_j be a (p_j, q_j)-graph with $j = 1, 2$. A graph G obtained by identifying each vertex $x_{i,1}$ of G_1 with a vertex $x_{i,2}$ of G_2 into one vertex $x_i = x_{i,1} \circ x_{i,2}$ with $i \in [1, m]$ is called an *m-identification graph* and denoted as $G = \odot_m \langle G_1, G_2 \rangle$; the vertices $x_1, x_2, \dots, x_m$ are called the *identification-vertices.*

Moreover, the m-identification graph $G = \odot_m \langle G_1, G_2 \rangle$ defined in Definition 3 has $p_1 + p_2 - m$ vertices and $q_1 + q_2$ edges. One can split each identification-vertex $x_i = x_{i,1} \circ x_{i,2}$ into two vertices $x_{i,1}$ and $x_{i,2}$ (called the *splitting-vertices*) for $i \in [1, m]$, such that G is split into two parts G_1 and G_2. For the purpose of convenience, the above procedure of producing am m-identification graph $G = \odot_m \langle G_1, G_2 \rangle$ is called an *m-identification operation*; conversely, the procedure of splitting $G = \odot_m \langle G_1, G_2 \rangle$ into two parts G_1 and G_2 is named as the *m-splitting operation.*

Definition 4. Let G_i be a connected (p_i, q)-graph with $i = 1, 2$, and let $p = p_1 + p_2 - 2$. If the 2-identification (p,q)-graph $G = \odot_2 \langle G_1, G_2 \rangle$ has a mapping $f : V(G) \to [0, q-1]$ holding the following: (i) $f(x) \ne f(y)$ for each pair of vertices $x, y \in V(G)$, (ii) f is an odd-elegant labelling of G_i with $i = 1, 2$, and (iii) $|f(V(G_1)) \cap f(V(G_2))| = 2$ and $f(V(G_1)) \cup f(V(G_2)) \subseteq [0, q-1]$, then one calls G a *twin odd-elegant graph* (a TOE-graph), f a *TOE-labelling*, G_1 a *TOE-source graph*, G_2 a *TOE-associated graph*, and (G_1, G_2) a *TOE-matching pair.*

We illustrate Definition 4 with Figure 2. In other words, a twin odd-elegant graph $G = \odot_2 \langle G_1, G_2 \rangle$ with its TOE-source graph G_1 and TOE-associated graph G_2, where (G_1, G_2) is a TOE-matching pair.

Furthermore, if each G_i with $i = 1, 2$ is a connected graph in Definition 4, and the TOE-source G_1 is a bipartite connected graph having its own bipartition (X_1, Y_1) and a labelling f satisfying Definition 2, we call the 2-identification graph $G = \odot_2 \langle G_1, G_2 \rangle$ a *set-ordered twin odd-elegant graph* (So-TOE-graph) and f a *set-ordered twin odd-elegant labelling* (So-TOE-labelling). Notice that the source graph G_1 is a set-ordered odd-elegant graph by Definitions 1 and 2. In vivid speaking, a source graph and its associated graph



(a) G_1 (b) G_2 (c) G

Figure 2: The formation process of Definition 4.

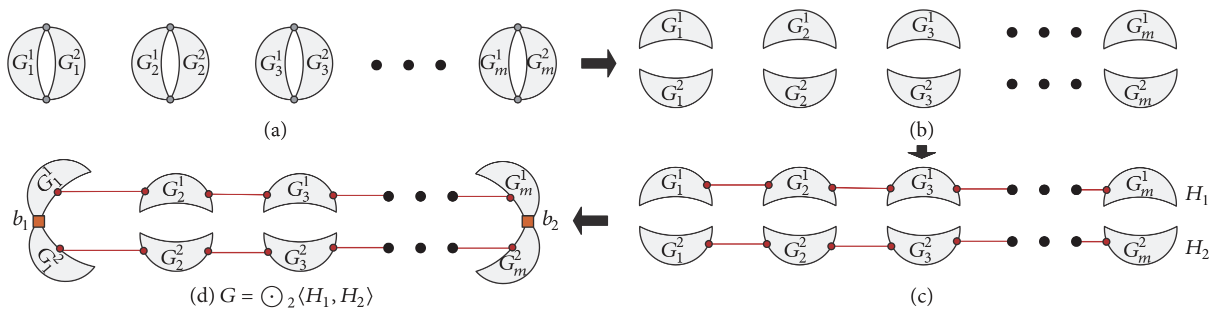


Figure 3: A scheme of the edge-series operation.

defined in Definition 4 can be called a *TOE-lock-model* and a *TOE-key-model* ([10]), respectively.

1.3. Techniques for Constructing 2-Identification Graphs. The following three operations, *CA-operation, edge-series operation, and base-pasted operation*, will be used in this article.

(O-1) CA-Operation. Suppose each graph G_k has an odd-elegant labelling f_k and $V(G_k) = \{x^k_l : l = 1, 2, \ldots, |V(G_k)|\}$ with $k \in [1, m]$. Clearly, for $a \neq b$ with $a, b \in [1, m]$, there are vertices $x^a_i \in V(G_a)$ and $x^b_j \in V(G_b)$ such that $f_a(x^a_i) = f_b(x^b_j)$. For example, some G_k has a vertex x^k_i such that the label $f_k(x^k_i) = 0$ with $k \in [1, m]$. We can combine those vertices that have the same labels into one vertex, which gives us a new graph, denoted by $G = \bigodot_\epsilon\langle G_1, G_2, \ldots, G_m\rangle$. This process is called a *CA-operation* on $G_1, G_2, \ldots, G_m$.

(O-2) Edge-Series Operation. Given two groups of disjoint trees $G^r_1, G^r_2, \ldots, G^r_m$ with $r = 1, 2$ there are vertices $x^r_k, y^r_k \in V(G^r_k)$ with $k \in [1, m]$. Joining the vertex y^r_j with the vertex x^r_{j+1} by an edge for $j \in [1, m-1]$ produces a tree H_r (denoted by $H_r = \ominus^m_{k=1} G^r_k$) with $r = 1, 2$; next we let one vertex $u^1_s \in V(H_1)$ coincide with one vertex $v^2_s \in V(H_2)$ into one vertex $a_s = u^1_s \circ v^2_s$ with $s = 1, 2$. The resulting graph $\bigodot_2\langle H_1, H_2\rangle$ is just a 2-identification graph.

(O-3) Base-Pasted Operation. Given two disjoint trees T_r (called *base-trees*) having vertices $x^r_1, x^r_2, \ldots, x^r_m$ and two groups of disjoint trees $G^r_1, G^r_2, \ldots, G^r_m$ with $r = 1, 2$, we let a vertex $u^r_k \in V(G^r_k)$ coincide with the vertex $x^r_k \in V(T_r)$ into one vertex $u^r_k \circ x^r_k$ for $k \in [1, m]$ such that the resulting tree F_r (i.e., $F_r = T_r \bigodot^m_{k=1} G^r_k$) has $V(F_r) = \bigcup^m_{k=1} V(G^r_k)$, $E(F_r) = (\bigcup^m_{k=1} E(G^r_k)) \cup E(T_r)$ for $r = 1, 2$. We overlap one vertex $w^1_s \in V(F_1)$ with one vertex $z^2_s \in V(F_2)$ into one vertex $b_s = w^1_s \circ z^2_s$ with $s = 1, 2$ to build up a 2-identification graph $F = \bigodot_2\langle F_1, F_2\rangle$ holding $V(F_1) \cap V(F_2) = \{a_1, a_2\}$ and $E(F) = E(F_1) \cup E(F_2)$.

In the following, we give the diagrams with $m = 2$ for edge-series operation and base-pasted operation, shown in Figures 3 and 4, respectively.

2. Main Results and Their Proofs

Lemma 5. *Each star $K_{1,n}$ is a TOE-source tree of a So-TOE-tree.*

Proof of Lemma 5 is shown in Figure 5. It describes the construction process of the So-TOE-tree $\bigodot\langle K_{1,n}, K_{1,n}\rangle$ by any TOE-source tree $K_{1,n}$.

Theorem 6. *Every set-ordered odd-elegant graph being not a star is a So-TOE-source graph of at least two So-TOE graphs.*

Proof. Suppose that (p_1, q)-graph G_1 having vertex bipartition is (X, Y), where $X = \{x_i : i \in [1, s]\}$, $Y = \{y_j : j \in [1, t]\}$, $s + t = p_1$, and $\min\{s, t\} \geq 2$. By the hypothesis of the theorem, G_1 has a set-ordered odd-elegant labelling f_1 defined by $f_1(x_i) + 2 \leq f_1(x_{i+1})$, $i \in [1, s-1]$; $f_1(y_1) = f_1(x_s) + 1$, $f_1(y_j) + 2 \leq f_1(y_{j+1})$, $i \in [1, t-1]$; $f_1(y_t) \leq 2q - 1$. Hence, $f_1(E(G_1)) = \{f_1(xy) = f_1(x) + f_1(y) \pmod{2q} : xy \in E(G_1)\} = [1, 2q-1]^o$. It is not difficult to observe that $f_1(V(G_1)) \subset \{0, 2, \ldots, f_1(x_s), f_1(y_1), \ldots, 2q-1\}$; that is, $f_1(X)/2 \subset \mathbb{N}$ and $(f_1(Y) + 1)/2 \subset \mathbb{N}$.

Case 1. We construct a labelling f_2 of a new tree T_2 having $q+1$ vertices by the labelling f_1 such that $f_2(V(T_2)) = [1, f_1(x_s) + 1]^o \cup [f_1(y_1) - 1, 2q-2]^e$, such that $f_2(E(T_2)) = \{f_2(uv) = f_2(u) + f_2(v) \pmod{2q} : uv \in E(T_2)\} = [1, 2q-1]^o$, where $f_2(u) \neq f_2(v)$ for $u, v \in V(T_2)$. This tree T_2 can be built up in the following way: a bipartition (U_1, V_1) with $U_1 = \{u_i :$

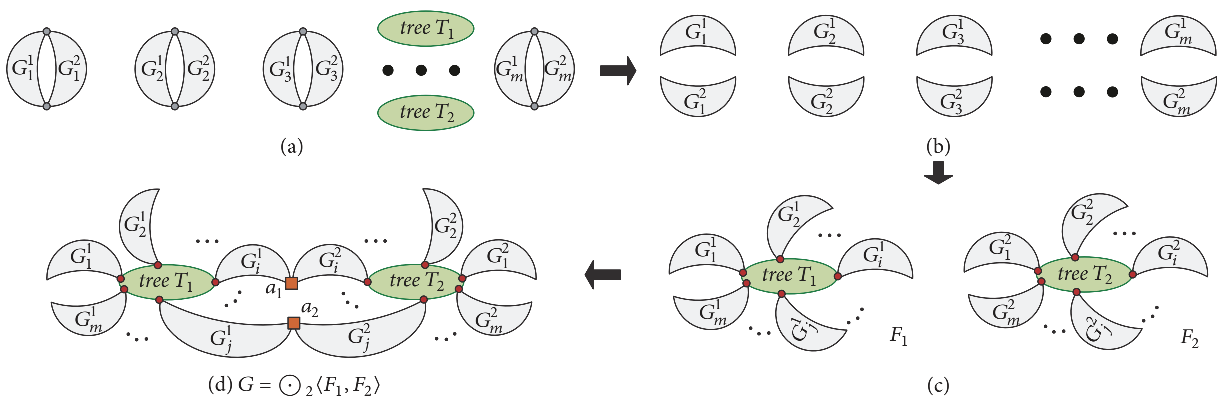


FIGURE 4: A scheme of the base-pasted operation.

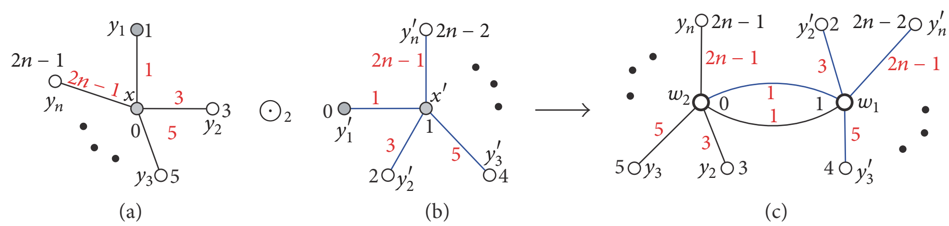


FIGURE 5: An example of illustrating Lemma 5.

$i \in [1, s_1]\}$ and $V_1 = \{v_j : j \in [1, t_1]\}$, where $s_1 + t_1 = q + 1$, such that $f_2(u_i) = 2i - 1$, $i \in [1, s_1]$; $f_2(v_j) = 2(s_1 - 2 + j)$, $j \in [1, t_1]$. Any edge $u_iv_j \in E(T_2)$ satisfies $f_2(u_iv_j) = f_2(u_i) + f_2(v_j) \pmod{2q}$ with $i \in [1, s_1]$ and $j \in [1, t_1]$. We construct the edge set of T_2 as $\{u_1v_j, u_iv_{t_1} : i \in [1, s_1], j \in [1, t_1 - 1]\}$ such that the edge labels are $f_2(u_iv_{t_1}) = 2i - 3$, $f_2(u_1v_j) = 2j + 2s_1 - 3 \pmod{2q}$ for $i \in [1, s_1]$ and $j \in [1, t_1 - 1]$. Observe that $f_2(E(T_2)) = [1, 2q - 1]^o$, $f_1(y_1) = f_2(u_{s_1})$, and $f_1(x_s) = f_2(v_1)$.

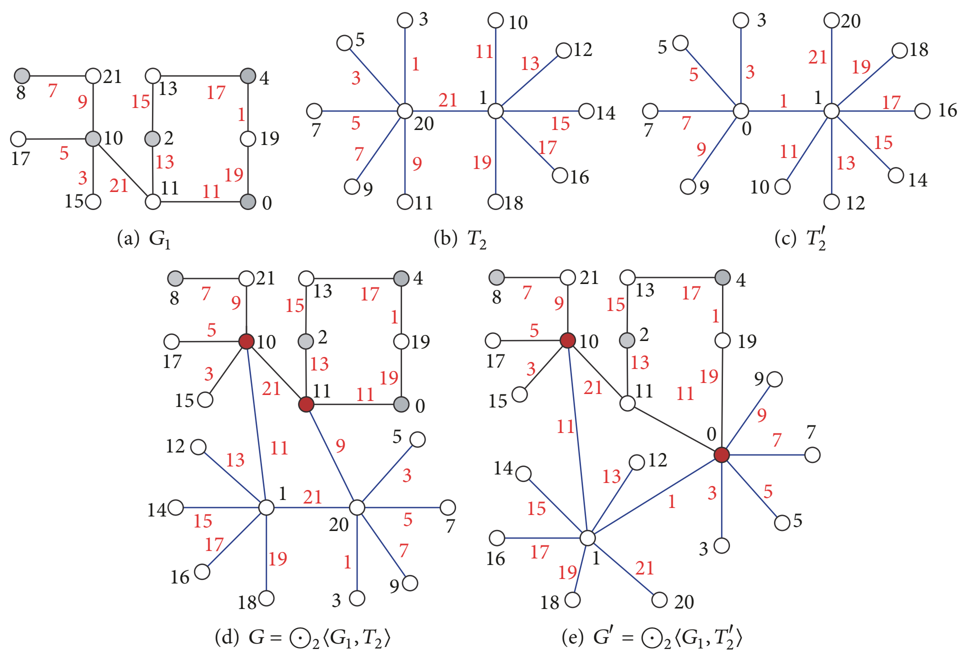
Now, we can combine the vertex y_1 and x_s of G_1 with the vertex u_{s_1} and v_1 of T_2 into one (two identification-vertices) w_1 and w_2, respectively, so we obtain the desired graph $G = \odot_2\langle G_1, T_2\rangle$. And G has a labelling f defined as $f(x_i) = f_1(x_i), i \in [1, s-1]$; $f(y_j) = f_1(y_j), i \in [2, t]$; $f(u_k) = f_2(u_k)$, $k \in [1, s_1 - 1]$, $f(v_l) = f_2(v_l)$, $l \in [2, t_1]$, $f(w_1) = f_1(y_1)$, and $f(w_2) = f_1(x_s)$. Clearly, any pair of two vertices of G are assigned different numbers. According to Definition 4, G is an So-TOE-graph having the source graph G_1. Examples that illustrate Case 1 of Theorem 6 are shown by Figures 6(a), 6(b), and 6(d).

Case 2. Similarly to Case 1, we can get the following results: let $f_2(V(T_2')) = [1, f_1(x_s) - 1]^o \cup [f_1(y_1) - 1, 2q - 2]^e \cup \{0\}$, $f_2(E(T_2')) = [1, 2q - 1]^o$, and furthermore $f_2(u) \neq f_2(v)$ for $u, v \in V(T_2')$. This tree T_2' can be built up in the following way: a bipartition (U_2, V_2) with $U_2 = \{u_i : i \in [1, s_1 - 1]\}$ and $V_2 = \{v_j : j \in [1, t_1 + 1]\}$, such that $f_2(u_i) = 2i - 1$, $i \in [1, s_1 - 1]$; $f_2(v_j) = 2(s - 2 + j)$, $j \in [1, t_1]$, $f_2(v_{t_1+1}) = 0$. Any edge $u_iv_j \in E(T_2')$ satisfies $f_2(u_iv_j) = f_2(u_i) + f_2(v_j) \pmod{2q}$ with $i \in [1, s_1 - 1]$ and $j \in [1, t_1 + 1]$. We construct the edge set of T_2' as $\{u_1v_j, u_iv_{t+1} : i \in [2, s_1 - 1], j \in [1, t_1]\}$ such that the edge labels are $f_2(u_iv_{t+1}) = 2i - 1$, for $i \in [1, s_1 - 1]$, and $f_2(u_1v_j) = 2(s + j) - 3$, for $j \in [1, t_1]$. Observe that $f_2(E(T_2')) = [1, 2q - 1]^o$, $f_1(x_1) = f_2(v_{t_1+1})$, and $f_1(x_s) = f_2(v_1)$.

Now, we can combine the vertex x_1 and x_s of T_1 with the vertex v_{t_1+1} and v_1 of T_2' into one (the identified vertex) w_1 and w_2, so we obtain the desired tree $G' = \odot_2\langle G_1, T_2'\rangle$. And G' has a labelling f defined as $f(x_i) = f_1(x_i)$, $i \in [2, s - 1]$; $f(y_j) = f_1(y_j)$, $i \in [1, t]$; $f(u_k) = f_2(u_k)$, $k \in [1, s_1 - 1]$, $f(v_l) = f_2(v_l)$, $l \in [2, t_1]$, $f(w_1) = 0$, and $f(w_2) = f_1(x_s)$. Clearly, any pair of two vertices of G' are assigned different numbers. According to Definition 4, G' is a So-TOE-graph having the source graph G_1. An example for illustrating Case 2 of Theorem 6 is given by Figures 6(a), 6(c), and 6(e). □

Theorem 7. *Suppose that $G_k = \odot_2\langle G_k^1, G_k^2\rangle$ is a So-TOE-graph, where each G_k^1 is a source tree for $k \in [1, m]$. Then $G = \odot_2\langle H_1, H_2\rangle$ obtained by the edge-series operation has a So-TOE-labelling.*

Proof. By the hypothesis of the theorem, every $(p_k^1 + p_k^2 - 2, 2q_k)$-graph G_k has a set-ordered odd-elegant source-(p_k^1, q_k)-graph G_k^1 and an associated-(p_k^2, q_k)-graph G_k^2 for $k \in [1, m]$. Let $V(G_k^1) \cap V(G_k^2) = \{w_k^1, w_k^2\}$; the vertex set of each graph G_k^r can be partitioned into (X_k^r, Y_k^r) with $r = 1, 2$, where $X_k^r = \{x_{k,i}^r : i \in [1, s_k^r]\}$, $Y_k^r = \{y_{k,j}^r : j \in [1, t_k^r]\}$, and $s_k^r + t_k^r = p_k^r$ for $k \in [1, m]$ and $r = 1, 2$. By Definition 4, every G_k has a So-TOE-labelling θ_k with $k \in [1, m]$ such that $\theta_k(x_{k,1}^r) \geq r - 1$; $\theta_k(x_{k,i}^r) + 2 \leq \theta_k(x_{k,i+1}^r)$ with $i \in [1, s_k^r]$; $\theta_k(y_{k,1}^r) = \theta_k(x_{k,s_k^r}^r) - (-1)^r$; $\theta_k(y_{k,j}^r) + 2 \leq \theta_k(y_{k,j+1}^r)$ for $i \in [1, t_k^r]$; and $\theta_k(y_{t_k^r}^r) \leq 2q_k - r$.



(a) G_1 (b) T_2 (c) T_2'

(d) $G = \bigodot_2\langle G_1, T_2\rangle$ (e) $G' = \bigodot_2\langle G_1, T_2'\rangle$

Figure 6: Examples of Theorem 6.

Therefore, $\theta_k(E(G_k^r)) = \{\theta_k(xy) = \theta_k(x) + f_k^r(y) \pmod{2q_k} : xy \in E(G_k^r)\} = [1, 2q_k - 1]^o$, where $\theta_k(x) \neq \theta_k(y)$ for distinct vertices $x, y \in V(G_k)$, which means $\theta_k(x^1_{k,s_k}) = \theta_k(y^2_{k,1}) = \theta_k(w^1_k)$ and $\theta_k(y^1_{k,1}) = \theta_k(x^2_{k,s_k}) = \theta_k(w^2_k)$. Clearly, the labels of other vertices of $G^1_k \cup G^2_k$ differ from each other.

Firstly, we split G_k into two parts G^1_k and G^2_k, that is, doing a 2-splitting operation on every G_k with $k \in [1, m]$. Secondly, our discussion focuses on G^1_k and G^2_k with $k \in [1, m]$. We construct a graph by joining the vertex y^r_{k,t_k} with the vertex $x^r_{k+1,1}$ by an edge, where $k \in [1, m-1]$ and $r = 1, 2$, called H_r. For the purpose of convenience, we set $S(a, b) = \sum_{l=a}^{b} \theta_l(x^1_{l,s^1_l}) + 2$, $Q(1, t) = 2\sum_{l=1}^{t}(q_l + 1)$, $Q_m = 2\sum_{l=1}^{m}(q_l + m - 1)$, $S(1, 0) = 0$, and $Q(1, 0) = 0$. For $r = 1, 2$, $i \in [1, s^r_k]$, and $j \in [1, t^r_k]$, we define a new labelling f as follows:

(T-1) $f(x^r_{k,i}) = \theta_k(x^r_{k,i}) + S(1, k-1)$;

(T-2) $f(y^r_{k,j}) = \theta_k(y^r_{k,j}) + Q(1, k-1) + S(k+1, m)$;

(T-3) $f(x^r_{k,i}y^r_{k,j}) = f(x^r_{k,i}) + f(y^r_{k,j}) \pmod{Q_m}$;

(T-4) $f(y^r_{k,t_k}x^r_{k+1,1}) = f(x^r_{k+1,1}) + f(y^r_{k,t_k}) \pmod{Q_m}$.

By the labelling forms (T-1) and (T-2) above, we can verify $f(x^1_{k,i}) \in [0, f(x^1_{m,s_m})]^e = [0, S(1, m) - 2]^e$ with $k \in [1, m]$ and have the following properties: (i) $f(x^2_{k,i}) \in [1, f(x^2_{m,s_m})]^o = [1, S(1, m) - 1]^o$; (ii) $f(y^1_{k,j}) \in [f(y^1_{1,1}), f(y^1_{m,t_m})]^o = [S(1, m) - 1, Q_m - 1]^o$; and (iii) $f(y^2_{k,j}) \in [f(y^2_{1,1}), f(y^2_{m,t_m})]^e = [S(1, m) - 2, Q_m - 2]^e$.

Computing the labelling forms (T-3) and (T-4) enables us to obtain $f(E(H_r)) = [1, Q_m - 1]^o$ for $r = 1, 2$. Now, we combine the vertex x^1_{m,s_m} with the vertex $y^2_{1,1}$ into one vertex and then combine the vertex $y^1_{1,1}$ with the vertex x^2_{m,s_m} into one vertex. (i.e., do the 2-identification operation). Thus the labelling f is a So-TOE-labelling of $G = \bigodot_2\langle H_1, H_2\rangle$; therefore, G is a So-TOE-graph too. □

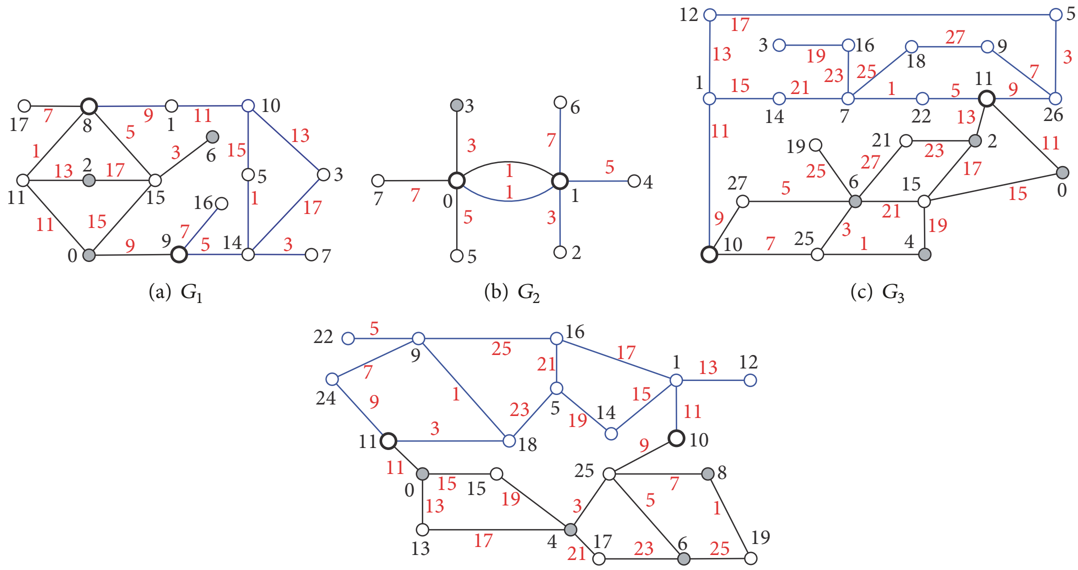
See Figures 7, 8 and 9 for understanding Theorem 7.

In experiments, for each arrangement $G^r_{k_1}, G^r_{k_2}, \ldots, G^r_{k_m}$ of $G^r_1, G^r_2, \ldots, G^r_m$, there are many possible constructions of $G = \bigodot_2\langle H_1, H_2\rangle$ for holding Theorem 7 (as shown in Figure 9).

Theorem 8. *Suppose that* $G_k = \bigodot_2\langle G^1_k, G^2_k\rangle$ *is a So-TOE-graph, where each* G^1_k *is a source graph for* $k \in [1, p]$. *Then* $G = \bigodot_2\langle S_1, S_2\rangle$ *obtained by the base-pasted operation has a So-TOE-labelling if two base-trees* T_1 *and* T_2 *are set-ordered.*

Proof. By the hypothesis of the theorem, every $(p^1_k + p^2_k - 2, 2q)$-graph $G_k = \bigodot_2\langle G^1_k, G^2_k\rangle$ has a set-ordered odd-elegant source-(p^1_k, q)-graph G^1_k and an associated-(p^2_k, q)-graph G^2_k for $k \in [1, p]$. Let $G^1_k \cap G^2_k = \{w^1_k, w^2_k\}$; the vertex set of each graph G^r_k can be partitioned into (X^r_k, Y^r_k) with $r = 1, 2$, where $X^r_k = \{x^r_{k,i} : i \in [1, s^r_k]\}$, $Y^r_k = \{y^r_{k,j} : j \in [1, t^r_k]\}$, $s^r_k \le t^r_k$, and $s^r_k + t^r_k = p^r_k$ for $k \in [1, p]$ and $r = 1, 2$. Every G_k, by Definition 4, has a So-TOE-labelling π_k with $k \in [1, p]$, and π_k has the following properties: $\pi_k(x^r_{k,1}) = r - 1$; $\pi_k(x^r_{k,i}) + 2 \le \pi_k(x^r_{k,i+1})$ for $i \in [1, s^r_k]$; $\pi_k(x^r_{k,s_k}) = M - 1 + r$; $\pi_k(y^r_{k,1}) = \pi_k(x^r_{k,s^r_k}) - (-1)^r = M - 1 + r - (-1)^r$; $\pi_k(y^r_{k,j}) + 2 \le \pi_k(y^r_{k,j+1})$ with $i \in [1, t^r_k]$; $\pi_k(y^r_{t^r_k}) = 2q - r$; and $\pi_k(x^r_{k,i}y^r_{k,j}) = \pi_k(x^r_{k,i}) + \pi_k(y^r_{k,j}) \pmod{2q}$.

Thus, the properties of each So-TOE-labelling π_k induce $\pi_k(E(G^r_k)) = \{\pi_k(xy) = \pi_k(x) + f^r_k(y) \pmod{2q} : xy \in E(G^r_k)\}$, and also



(a) G_1 (b) G_2 (c) G_3 (d) G_4

Figure 7: Four So-TOE-graphs G_k with $k \in [1, 4]$ described in the proof of Theorem 7.

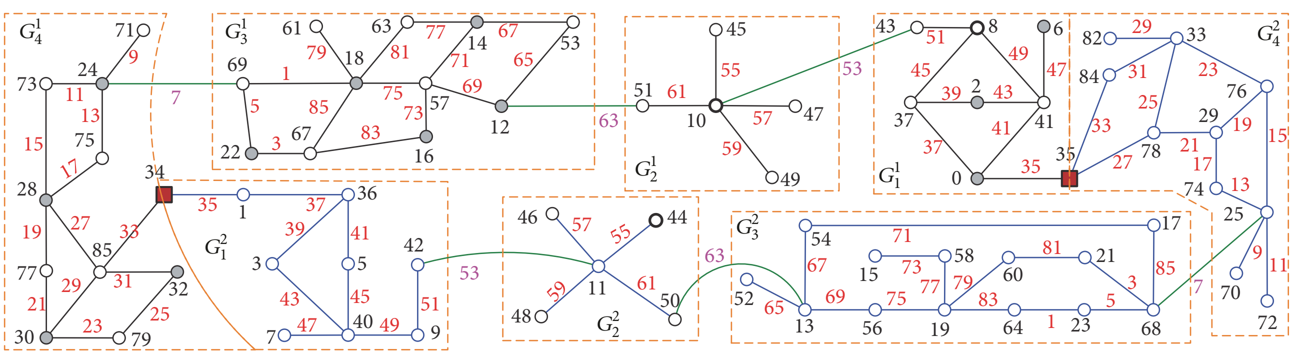


Figure 8: A So-TOE-graph made by the graphs shown in Figure 7 for illustrating Theorem 7.

$$\pi_k\left(E\left(G_k^r\right)\right) = \left[\pi_k\left(x_{k,1}^r\right)+\pi_k\left(y_{k,1}^r\right), \pi_k\left(x_{k,s_k^r}^r\right)+\pi_k\left(y_{k,t_k^r}^r\right)\right] \cdot (\bmod 2q) = [1, 2q-1]^o, \quad (2)$$

where $\pi_k(x) \neq \pi_k(y)$ if $x \neq y$ and $x, y \in V(G_k)$. In other words, we have $\pi_k(x_{k,s_k}^1) = \pi_k(y_{k,1}^2) = \pi_k(w_k^1)$ and $\pi_k(y_{k,1}^1) = \pi_k(x_{k,s_k}^2) = \pi_k(w_k^2)$. The labels of other vertices of $G_k^1 \cup G_k^2$ differ from each other.

Let $V(T_r) = \{z_1^r, z_2^r, \ldots, z_p^r\}$, such that there exists a set-ordered odd-elegant labelling $f_{T_r}^{oe}$, satisfying $f_{T_r}^{oe}(z_i^r) < f_{T_r}^{oe}(z_{i+1}^r)$ with $i \in [1, p-1]$, and the bipartition (U_r, V_r) of vertex set of T_r satisfies $|U_r| \leq |V_r|$ for $|U_r| = l$ and $r = 1, 2$.

Next, we discuss all graphs G_k^1 and G_k^2 with $k \in [1, p]$ by the parity of positive integer p in the following two cases.

Case 1. For considering the case $p = 2\beta + 1$ and $r = 1, 2$, we define a new labelling f with $i \in [1, s_k^r]$ and $j \in [1, t_k^r]$ in the following way:

(C-1) $f(x_{2k-1,i}^r) = \pi_{2k-1}(x_{2k-1,i}^r) + 2(q+1)(k-1)$ with $k \in [1, \beta+1]$;

(C-2) $f(x_{2k,i}^r) = \pi_{2k}(x_{2k,i}^r) + 2(q+1)(\beta+k) - 2 - (-1)^r$ with $k \in [1, \beta]$;

(C-3) $f(y_{2k-1,j}^r) = \pi_{2k-1}(y_{2k-1,j}^r) + 2(q+1)(\beta+k-1)$ with $k \in [1, \beta+1]$;

(C-4) $f(y_{2k,j}^r) = \pi_{2k}(y_{2k,j}^r) + 2(q+1)(k-1) + 2 + (-1)^r$ with $k \in [1, \beta]$;

(C-5) $f(x_{k,i}^r y_{k,j}^r) = f(y_{k,j}^r) + f(x_{k,i}^r) \pmod{2p(q+1)-2}$.

Based upon the labelling forms (C-1)–(C-4), we compute

$$\left(\bigcup_{k=1}^{\beta+1} f\left(X_{2k-1}^1\right)\right) \cup \left(\bigcup_{k=1}^{\beta} f\left(Y_{2k}^1\right)\right) = \left[0, 2(q+1)\beta + M\right]^e;$$

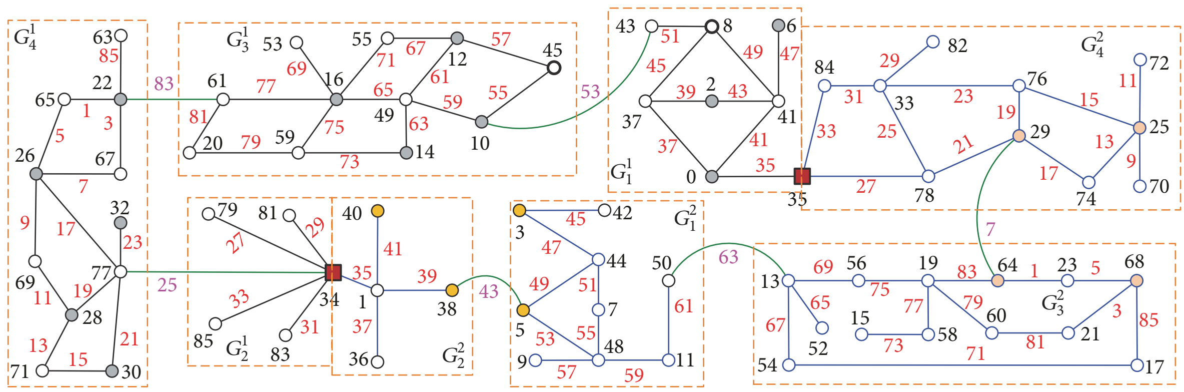


Figure 9: Another So-TOE-graph made by the graphs shown in Figure 7 for illustrating Theorem 7.

$$\begin{aligned}
&\left(\bigcup_{k=1}^{\beta+1} f\left(Y^1_{2k-1}\right)\right)\cup\left(\bigcup_{k=1}^{\beta} f\left(X^1_{2k}\right)\right)\\
&\quad=\left[2(q+1)\beta+M+1,2p(q+1)-3\right]^o,\\
&\qquad\qquad\qquad\qquad r=1,\\
&\left(\bigcup_{k=1}^{\beta+1} f\left(X^2_{2k-1}\right)\right)\cup\left(\bigcup_{k=1}^{\beta} f\left(Y^2_{2k}\right)\right)\\
&\quad=\left[1,2(q+1)\beta+M+1\right]^o;\\
&\left(\bigcup_{k=1}^{\beta+1} f\left(Y^2_{2k-1}\right)\right)\cup\left(\bigcup_{k=1}^{\beta} f\left(X^2_{2k}\right)\right)\\
&\quad=\left[2(q+1)\beta+M,2p(q+1)-4\right]^e,\\
&\qquad\qquad\qquad\qquad r=2.
\end{aligned} \tag{3}$$

Thereby, we have shown that $\bigcup_{r=1}^{2}\bigcup_{k=1}^{p} f(V(G^r_k)) \subset [0, 2p(q+1)-3]$ and

$$\left(\bigcup_{r=1}^{2}\bigcup_{k=1}^{p} f\left(E\left(G^r_k\right)\right)\right)\cup\left(\bigcup_{r=1}^{2} f\left(E\left(T_r\right)\right)\right) = \left[1,2p(q+1)-3\right]^o, \tag{4}$$

and furthermore the labels of vertices, except $f(x^1_{p,s}) = f(y^2_{1,1})$ and $f(x^2_{p,s}) = f(y^1_{1,1})$, differ from each other, and the labels of edges differ from each other.

Next, after computing the labelling forms (C-5) with $k \in [1, p]$, we obtain

$$\begin{aligned}
&f\left(E\left(G^r_{2k-1}\right)\right) = \left[A(2), B(1)\right]^o, \quad k \in [1,\beta+1];\\
&f\left(E\left(G^r_{2k}\right)\right) = \left[A(1), B(0)\right]^o, \quad k \in [1,\beta].\\
&\qquad\qquad\qquad (\bmod\ 2p(q+1)-2),
\end{aligned} \tag{5}$$

where $A(x) = M+1+2(q+1)(\beta+2k-x)$ and $B(y) = M-3+2(q+1)(\beta+2k-y)$. By the above deduction, we can know that

$$\bigcup_{k=1}^{p} f\left(E\left(G^r_k\right)\right) = \left[1,2p(q+1)-3\right]^o \setminus F, \tag{6}$$

where $F = \{M-1+2(q+1)(\beta+1+k), M+1+2(q+1)k : k = 0,1,2,\dots,\beta-1\}$. Next, for each vertex $z^r_k \in V(T_r)$ with $k \in [1, p]$ and $r = 1, 2$, we set

$$\begin{aligned}
&f\left(z^1_k\right) = f\left(x^1_{2k-1,s^1_{2k-1}}\right),\\
&f\left(z^2_k\right) = f\left(y^2_{2(\beta+k-l)+1,1}\right),\\
&\qquad\qquad k \in [1,l];\\
&f\left(z^1_{l+k}\right) = f\left(x^1_{2k,1}\right),\\
&f\left(z^2_{\beta+1+k}\right) = f\left(y^2_{2k,t^2_{2k}}\right),\\
&\qquad\qquad k \in [1,\beta];\\
&f\left(z^1_{l+\beta+k}\right) = f\left(x^2_{2k-1,1}\right),\\
&f\left(z^2_{l+k}\right) = f\left(y^1_{2(l+k)-1,t^2_{2(l+k)-1}}\right),\\
&\qquad\qquad k \in [1,\beta+1-l].
\end{aligned} \tag{7}$$

According to formula (7), we obtain $f(z^r_i z^r_j) = f(z^r_i) + f(z^r_j) \in F$ with $i \in [1,l]$, $j \in [l+1,p]$, and $r = 1,2$, which means

$$f\left(E\left(T_r\right)\right) = F. \tag{8}$$

Doing a *CA-operation* on G^r_k and T_r having labelling f for $k \in [1,p]$ produces a new graph S_r with $r = 1,2$. Now, we combine the vertex x^1_{p,s^1_p} with the vertex $y^2_{1,1}$ into one vertex $w_1 = x^1_{p,s^1_p} \circ y^2_{1,1}$ and moreover identify the vertex $y^1_{1,1}$ with the vertex x^2_{p,s^2_p} into one vertex $w_2 = y^1_{1,1} \circ x^2_{p,s^2_p}$ (i.e., do a 2-identification operation).

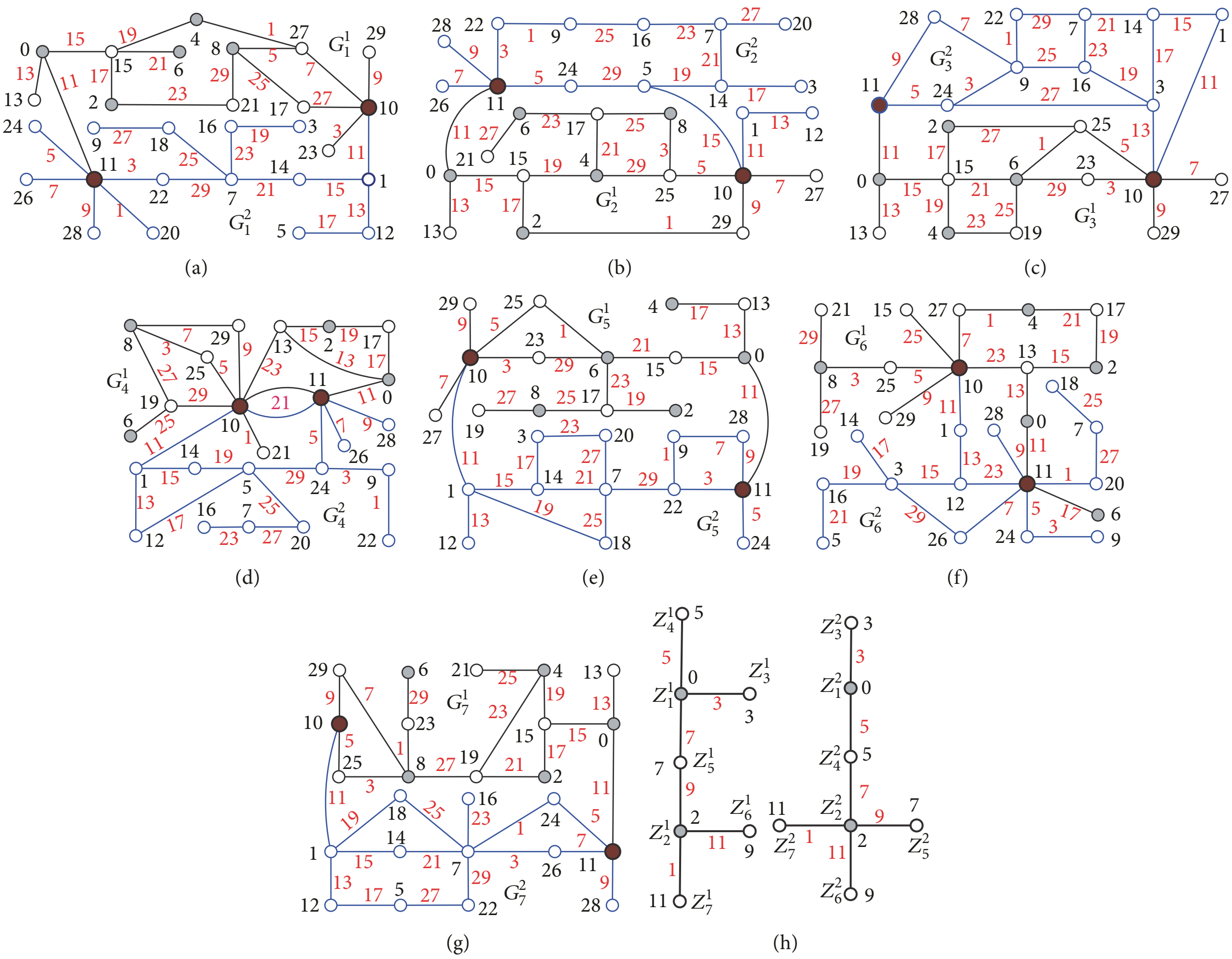


Figure 10: Seven So-TOE-graphs G_k with $k \in [1, 7]$ and two base-trees T_1 and T_2 described in the proof of Case 1 of Theorem 8.

By Definitions 2 and 4 and formulae (3)–(8), the labelling f is a So-TOE-labelling of $G = \odot_2\langle S_1, S_2\rangle$. Hence, G is a So-TOE-graph. Here, we have proven Case 1. For understanding Case 1, see Figures 10 and 11.

Case 2. We, for the case $p = 2\beta$ and $r = 1, 2$, define a new labelling f for $i \in [1, s^r_k]$ and $j \in [1, t^r_k]$ in the following way:

(L-1) $f(x^r_{2k-1,i}) = \pi_{2k-1}(x^r_{2k-1,i}) + 2(q+1)(k-1)$ with $k \in [1, \beta]$;

(L-2) $f(x^r_{2k,i}) = \pi_{2k}(x^r_{2k,i}) + 2(q+1)(\beta+k) - M - 4 - (-1)^r$ with $k \in [1, \beta]$;

(L-3) $f(y^r_{2k-1,j}) = \pi_{2k-1}(y^r_{2k-1,j}) + 2(q+1)(\beta+k-1) - M - 2$ with $k \in [1, \beta]$;

(L-4) $f(y^r_{2k,j}) = \pi_{2k}(y^r_{2k,j}) + 2(q+1)(k-1) + 2 + (-1)^r$ with $k \in [1, \beta]$;

(L-5) $f(x^r_{k,i}y^r_{k,j}) = f(y^r_{k,j}) + f(x^r_{k,i}) \pmod{2p(q+1)-2}$.

From the above labelling forms (L-1)–(L-4), we can compute

$$\left(\bigcup_{k=1}^{\beta} f\left(X^1_{2k-1}\right)\right) \cup \left(\bigcup_{k=1}^{\beta} f\left(Y^1_{2k}\right)\right) = [0, 2(q+1)\beta - 2]^e;$$

$$\left(\bigcup_{k=1}^{\beta} f\left(Y^1_{2k-1}\right)\right) \cup \left(\bigcup_{k=1}^{\beta} f\left(X^1_{2k}\right)\right) = [2(q+1)\beta - 1, 2p(q+1) - 3]^o, \quad r = 1,$$

$$\left(\bigcup_{k=1}^{\beta} f\left(X^2_{2k-1}\right)\right) \cup \left(\bigcup_{k=1}^{\beta} f\left(Y^2_{2k}\right)\right) = [1, 2(q+1)\beta - 1]^o;$$

$$\left(\bigcup_{k=1}^{\beta} f\left(Y^2_{2k-1}\right)\right) \cup \left(\bigcup_{k=1}^{\beta} f\left(X^2_{2k}\right)\right)$$

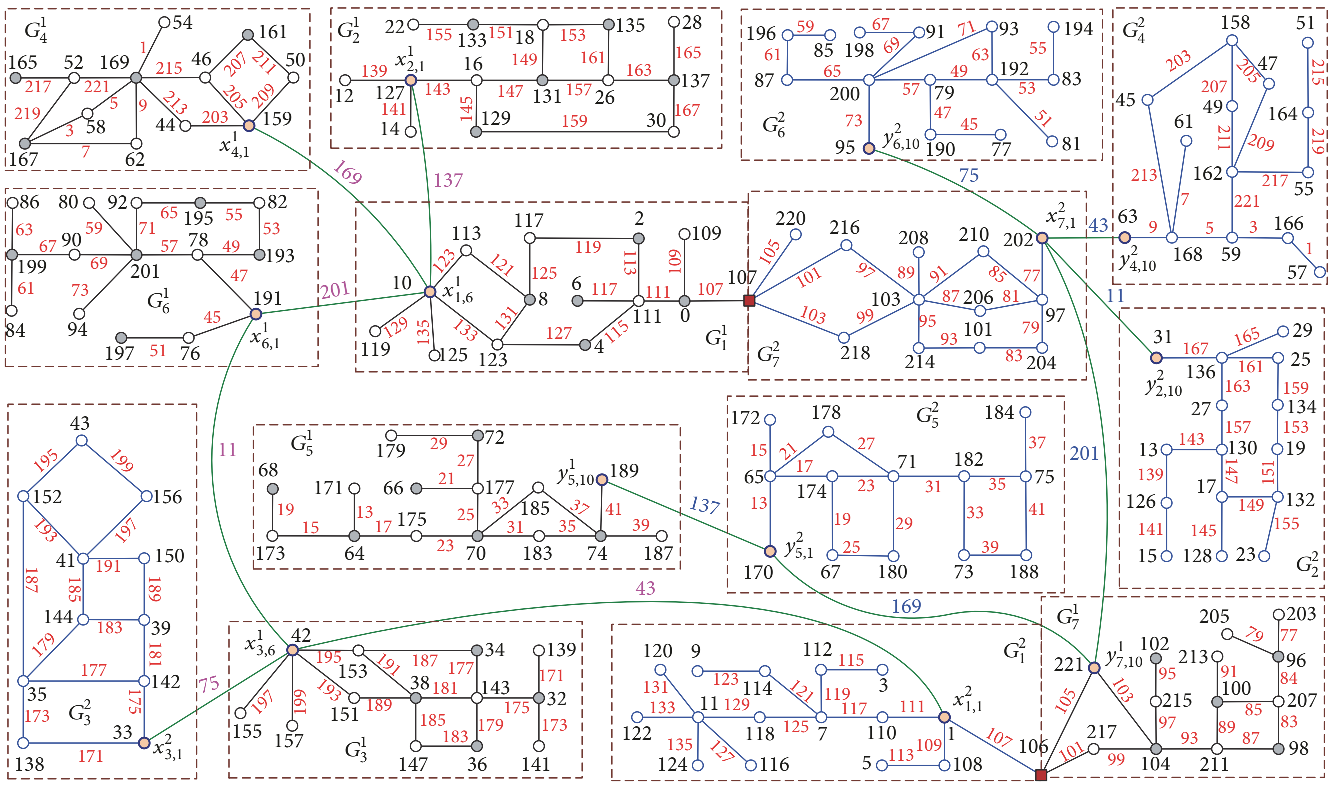


Figure 11: A So-TOE-graph $\odot_2\langle S_1, S_2\rangle$ made by the graphs shown in Figure 10 for understanding the proof of Case 1 of Theorem 8.

$$= [2(q+1)\beta - 2, 2p(q+1) - 4]^e, \qquad r = 2. \tag{9}$$

Thereby, we conclude that $\bigcup_{r=1}^{2}\bigcup_{k=1}^{p} f(V(G_k^r)) = [0, 2p(q+1)-3]$ and

$$\left[\bigcup_{r=1}^{2}\bigcup_{k=1}^{p} f(E(G_k^r))\right] \cup \left[\bigcup_{r=1}^{2} f(E(T_r))\right] = [1, 2p(q+1)-3]^o, \tag{10}$$

in which the labels of vertices and edges, except $f(y^1_{p,t^1_p}) = f(y^2_{1,1})$ and $f(y^2_{p,t^2_p}) = f(y^1_{1,1})$, differ from each other, respectively.

Again, by computing the labelling form (L-5) for each $k \in [1, p]$, we obtain

$$\begin{aligned} f(E(G^r_{2k-1})) &= [\alpha(2), \beta(1)]^o; \\ f(E(G^r_{2k})) &= [\alpha(1), \beta(0)]^o, \\ &\quad (\bmod 2p(q+1)-2), \quad k \in [1, \beta], \end{aligned} \tag{11}$$

where $\alpha(x) = 2(q+1)(\beta + 2k - x) - 1$ and $\beta(y) = 2(q+1)(\beta + 2k - y) - 5$.

Synthesizing the above argument, we get $\bigcup_{k=1}^{p} f(E(G_k^r)) = [1, 2p(q+1)-3]^o \setminus F'$, where the set $F' = \{2(q+1)(\beta + k) - 3 \ (\bmod 2p(q+1)-2) : k \in [1, 2\beta - 1]\}$. For each vertex $z_k^r \in T_r$ with $\in [1, p]$ and $r = 1, 2$, we set

$$\begin{aligned} f(z_k^1) &= f(x^1_{2k-1,1}), \\ f(z_k^2) &= f\left(x^2_{2(\beta+k-l),s^2_{2(\beta+k-l)}}\right), \\ &\qquad k \in [1, l]; \\ f(z^1_{l+k}) &= f\left(x^1_{2k,s^1_{2k}}\right), \\ f(z^2_{\beta+k}) &= f(x^2_{2k-1,1}), \\ &\qquad k \in [1, \beta]; \\ f(z^1_{l+\beta+k}) &= f\left(y^2_{2k,t^2_{2k}}\right), \\ f(z^2_{l+k}) &= f\left(y^1_{2(l+k)-1,1}\right), \\ &\qquad k \in [1, \beta - l]. \end{aligned} \tag{12}$$

The above formula (12) enables us to obtain $f(z_i^r z_j^r) = f(z_i^r) + f(z_j^r) \in F'$ with $i \in [1, l]$, $j \in [l+1, p]$, and $r = 1, 2$. Thereby, we have shown

$$f(E(T_r)) = F'. \tag{13}$$

After performing a *CA-operation* on G_k^r and T_r having labelling f for $k \in [1, p]$, then we obtain a new graph S_r with

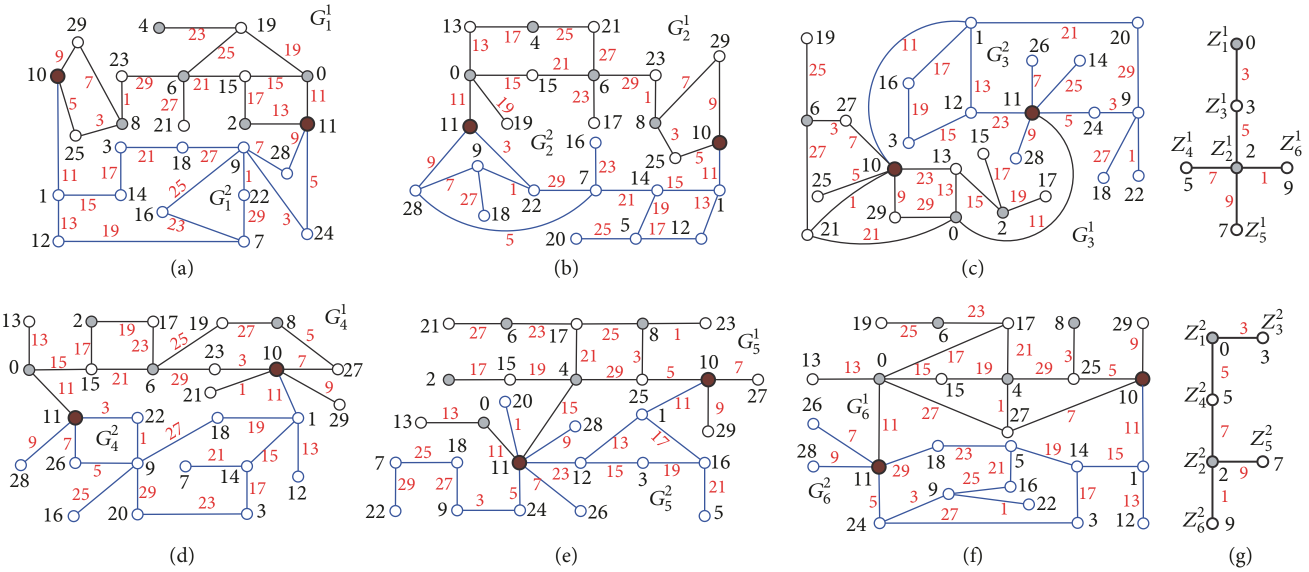


Figure 12: Six So-TOE-graphs G_k with $k \in [1,6]$ and two base-trees T_1 and T_2 described in the proof of Case 2 of Theorem 8.

$r = 1, 2$. Now, we overlap the vertex y^1_{p,t^1_p} with the vertex $y^2_{1,1}$ into one vertex $w'_1 = y^1_{p,t^1_p} \circ y^2_{1,1}$ and overlap the vertex $y^1_{1,1}$ with the vertex y^2_{p,t^2_p} into one vertex $w'_2 = y^1_{1,1} \circ y^2_{p,t^2_p}$ (i.e., do a 2-identification operation) in order to obtain $G' = \odot_2\langle S_1, S_2\rangle$. Furthermore, by Definitions 2 and 4 and formulae (9)–(13), the labelling f is a So-TOE-labelling of G', which implies that G' is a So-TOE-graph.

Hence, the proof of Case 2 is finished, and illustrating this case is given in Figures 12 and 13.

The proof of the theorem is complete. □

3. Conclusion and Further Research

There are new Topsnut-GPWs having twin odd-elegant labellings introduced here. We define the twin odd-elegant labelling and investigate the 2-identification graph $G = \odot_2\langle G_1, G_2\rangle$, called twin odd-elegant graph. We think that finding all possible TOE-matching pairs (G, H) defined in Definition 4 may be interesting for a given TOE-graph G with an odd-elegant labelling g. Let

$$M_{\mathrm{TOE}}(G, g) = \{H : (G, H) \text{ is a TOE-matching pair}\} \tag{14}$$

be the set of all TOE-associated graphs H, so, we have a *TOE-book* $B(G, g) = \bigcup_{H \in M_{\mathrm{TOE}}(G,g)} \odot_2\langle G, H\rangle$ with *book-back* G and *book-pages* $H \in M_{\mathrm{TOE}}(G, g)$.

We should pay attention to the following problems:

(i) Since $G = \odot_2\langle G, H\rangle \cap \odot_2\langle G, H'\rangle$ for any pair of book-pages $H, H' \in M_{\mathrm{TOE}}(G, g)$, does $V(G) = \bigcup_{H \in M_{\mathrm{TOE}}(G,g)}(V(G) \cap V(H))$?

(ii) Suppose that G has m pairwise different odd-elegant labellings $g_1, g_2, \ldots, g_m$. Find some possible relationships among TOE-books $B(G, g_i)$ with $i \in [1, m]$.

For the future researching work on Topsnut-GPWs, we propose the following.

Conjecture 9. *Let each $\odot_2\langle G^1_k, G^2_k\rangle$ be a TOE-graph for $k \in [1, m]$ with $m \geq 2$. The 2-identification graph $G = \odot_2\langle H_1, H_2\rangle$ obtained by the edge-series operation (resp., the base-pasted operation) admits a TOE-labelling. r*

Conjecture 10. *Every simple and connected TOE-graph admits an odd-elegant labelling.*

Conjecture 11. *Each connected graph is the TOE-source graph of a certain TOE-graph.*

A more interesting problem is to design super Topsnut-GPWs such that each super Topsnut-GPW will not be deciphered by attacks of nonquantum computers, since (i) our methods introduced here can construct quickly large scale of Topsnut-GPWs having hundreds vertices; (ii) the space of the Topsnut-GPWs given in Theorem 8 is quite tremendous; (iii) the 2-identification graphs $\odot_2\langle H_1, H_2\rangle$ of Theorem 7 and $\odot_2\langle S_1, S_2\rangle$ of Theorem 8 are the compound type of Topsnut-GPWs based on smaller scale of Topsnut-GPWs $G_k = \odot_2\langle G^1_k, G^2_k\rangle$ with $k \in [1, m]$, and they induce the TOE-books $B(H_1, f)$ and $B(S_1, g)$; it may be guessed that there is no polynomial algorithm for determining the TOE-books; and (iv) no polynomial algorithm was reported for finding all odd-elegant labellings of a given graph.

Thereby, we hope to discover such super Topsnut-GPWs which can be used in the era of quantum information.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

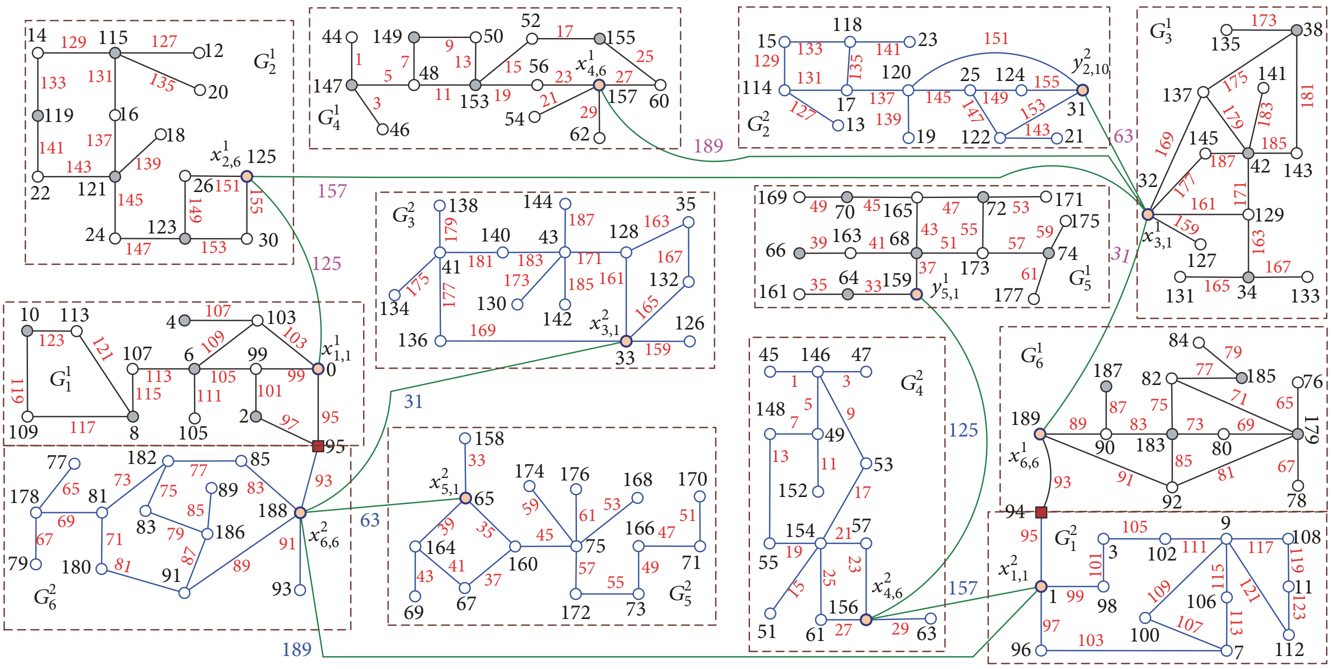


FIGURE 13: A So-TOE-graph $\odot_2\langle S_1, S_2\rangle$ made by the graphs shown in Figure 12 for understanding the proof of Case 2 of Theorem 8.

Acknowledgments

This work was supported by the National Key R&D Program of China (no. 2016YFB0800700) and the National Natural Science Foundation of China (nos. 61572046, 61502012, 61672050, 61672052, 61363060, and 61662066).

References

[1] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: a survey," in *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC '05)*, pp. 463–472, Tucson, Ariz, USA, December 2005.

[2] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: learning from the first twelve years," *ACM Computing Surveys*, vol. 44, no. 4, Article 19:1-41. Technical Report TR-09-09, School of Computer Science, Carleton University, Ottawa, Canada. 2009. (25 pages, 145 reference papers), 2012.

[3] H. Gao, W. Jia, F. Ye, and L. Ma, "A survey on the use of graphical passwords in security," *Journal of Software*, vol. 8, no. 7, pp. 320–329, 2013.

[4] "QR Code Essentials". Denso ADC. 2011. Retrieved 12 March 2013.

[5] "QR Code features". Denso-Wave. Archived from the original on 2013-01-29. Retrieved 3 October 2011.

[6] X. Suo, "A Study of Graphical Password for Mobile Devices," in *Mobile Computing, Applications, and Services*, vol. 130 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 202–214, Springer International Publishing, Cham, 2014.

[7] B. Yao, H. Sun, X. Zhang, H. Wang, J. Li, and G. Yan, "Graph theory towards designing graphical passwords for mobile devices," in *Proceedings of the 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 1640–1644, Chengdu, China, December 2017.

[8] H. Wang, J. Xu, and B. Yao, "Exploring new cryptographical construction of complex network data," in *Proceedings of the 1st IEEE International Conference on Data Science in Cyberspace, DSC 2016*, pp. 155–160, June 2016.

[9] H. Wang, J. Xu, and B. Yao, "The key-models and their lock-models for designing new labellings of networks," in *Proceedings of the 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2016*, pp. 565–568, October 2016.

[10] H. Wang, J. Xu, and B. Yao, "Twin Odd-graceful Trees Towards Information Security," in *Proceedings of the 7th International Congress of Information and Communication Technology, ICICT 2017*, pp. 15–20, Elsevier Science Publishers B. V., February 2017.

[11] F. Harary and E. M. Palmer, *Graphical enumeration*, Academic Press, 1973.

[12] J. A. Gallian, "A Dynamic Survey of Graph Labeling," *The Electronic Journal of Combinatorics*, vol. 17, DS6. (440 pages, 2265 reference papers), 2013.

[13] X. Zhou, B. Yao, and X. Chen, "Every lobster is odd-elegant," *Information Processing Letters*, vol. 113, no. 1-2, pp. 30–33, 2013.

[14] J. A. Bondy and U. S. R. Murty, *Graph Theory*, Springer, London, UK, 2008.

[15] B. Yao, H. Cheng, M. Yao, and M. Zhao, "A note on strongly graceful trees," *Ars Combinatoria*, vol. 92, pp. 155–169, 2009.