MATEC Web of Conferences **139**, 00204 (2017) DOI: 10.1051/matecconf/201713900204
ICMITE 2017

Strongly (k,d)-Graphical Labellings For Designing Graphical Passwords In Communication

Hui Sun[1], *Xiaohui* Zhang[1], and *Bing* Yao[1,2,⋆]

[1] *College of Mathematics and Statistics, Northwest of Normal University, Lanzhou 730070, CHINA*
[2] *School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, CHINA*

Abstract. The safety of the traditional text passwords is questioned by many users in the present information research. Graphical passwords become new research object of many researchers, who hope they can replace the existing text passwords and improve user account security. We are studying Topsnut-graphical passwords, which can be traced back to an idea of "topological structure plus number theory" proposed first by Hongyu Wang with her colleagues, and we found the equivalence between with Topsnut-graphics passwords of the trees having perfect matching. Through designing new parametric graphical labellings, we hope to enrich the variety of Topsnut-graphical passwords, and study the relationship between new parametric graphic labellings and existing labellings on trees having perfect matching. In addition, we also found, by two kinds of special operations, trees having perfect matching can be converted into paths perfect matching, and the nature of the original passwords remains unchanged. Our results can be provided to two or more banking users, and our method can easily be converted into polynomial time algorithms.

1 Introduction

Password have become an important part of human daily life, whether it is shopping or chatting and playing games, people use passwords. Your password can not only ensure the safety of personal privacy, but also provides a sense of security for the user.However, attacks to passwords appear in our daily life, and more by more. The safety of the traditional text passwords is questioned by many users in the present information research. Graphical passwords become new research object of many researchers, who hope they can replace the existing text passwords and improve user account security, because of graphical passwords are easy for users and difficult to be broken by attackers [1]. We call new graphical passwords as *Topsnut-graphical passwords* , denoted by Topsnut-GPWs, for distinguishing with other graphical passwords, since they are made by an idea of "topological structure plus number theory" (Topsnut) proposed firstly by Wang *et al.* in [2] and [3]. Studies have shown that humans remember pictures more than texts, and psychological research supports the hypothesis [4]. However, one of the biggest drawbacks in the existing graphical passwords in [1] is that they occupy large storage space, slow communication speed and lack of practicability.

We show an example for illustrating Topsnut-GPWs simply. Olaf goes to a bank to establish an account for his deposit. At first, Olaf are provided for making a password based

⋆e-mail: yybb918@163.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

 DOI: 10.1051/matecconf/201713900204

on six given small circles shown in Fig.1(a). At second, he connected by a straight line between small circles and drew a Chinese character with six small circles and seven sides – "day" in Fig.1(b). Next, he label numbers in these circles (see Fig.1(c)). Finally, label seven lines with particular numbers (see Fig.1(d)). We use $f(u)$ to indicate the label of a circle, and $f(uv)$ to be the label of an edge uv joining two circles u, v as its ends. Thus, $|f(u) - f(v)| = f(uv)$ holds true for each line uv. Thereby, we have made the desired password, called a *Topsnut-GPWs* in which the graphical structure is a graph without numbers labelled to the vertices and edges of the graph. If Olaf establishes multiple bank accounts at the same time, it is clear that it is not safe to share one password in multiple accounts, and it is not easy to memorize many different passwords. At this point, he can set up a parametric password to deal with this situation(see Fig.1(e)). When $k = 1, d = 1$, it is Fig.1(d). We will design more complicated parametric graphical passwords in this article.

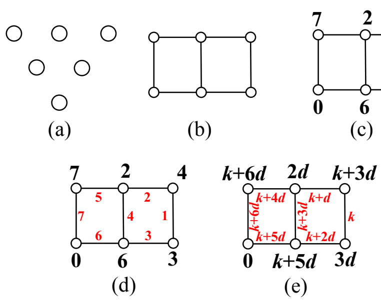

Figure 1. Olaf makes a graphical password.

2 Graphical passwords

2.1 Preliminary

All graphs mentioned here are undirected, finite, and no multiple-edges and loops, and they are called *simple graphs*. We use standard terminology and notation of graph theory, other undefined concepts or definitions can be found in [5] and [6]. Additional notations are: the symbol $[m, n]$ indicates a set $\{m, m+1, \dots, n\}$ with integers m, n respect to $0 \leq m < n$; the $[s, t]^o$ denotes an *odd-integer set* $\{s, s+2, \dots, t\}$ with odd integers s, t maintaining $1 \leq s < t$; and the notation $[a, b]^e$ stands up an *even-integer set* $\{a, a+2, \dots, b\}$ with even integers a, b falling into $2 \leq a < b$. $|X|$ is the *cardinality* of elements of a set X. A (p, q)-graph G has p vertices and q edges. The set of all vertices adjacent to a vertex v in G is denoted as $N(x) = \{v : xv \in E(G)\}$, called the *neighborhood* of the vertex x. And the *degree* $\deg(u)$ of a vertex u is equal to $\deg(u) = |N(u)|$. A vertex of degree one is called a *leaf* here. We restate the definitions of well-known graph labellings as follows:

Definition 1 *[5, 7] Suppose that a connected (p, q)-graph G admits a mapping $\psi : V(G) \rightarrow \{0, 1, 2, \dots\}$. The induced edge label is defined as $\psi(xy) = |\psi(x) - \psi(y)|$ for each edge $xy \in E(G)$. Write $\psi(V(G)) = \{\psi(u) : u \in V(G)\}$, $\psi(E(G)) = \{\psi(xy) : xy \in E(G)\}$. There are the following constraints:*

(1) $|\psi(V(G))| = p$.

(2) $|\psi(E(G))| = q$.

(3) $\psi(V(G)) \subseteq [0, q]$, $\min \psi(V(G)) = 0$.

(4) $\psi(V(G)) \subset [0, 2q-1]$, $\min \psi(V(G)) = 0$.

(5) $\psi(E(G)) = \{\psi(xy) : xy \in E(G)\} = [1, q]$.

(6) $\psi(E(G)) = \{\psi(xy) : xy \in E(G)\} = \{1, 3, 5, \dots, 2q-1\}$.

(7) G is a bipartite graph with the bipartition (X, Y) such that $\max\{\psi(x) : x \in X\} < \min\{\psi(y) : y \in Y\}$ ($\psi(X) < \psi(Y)$ for short).

(8) G is a tree having a perfect matching M such that $\psi(x) + \psi(y) = q$ for each matching edge $xy \in M$.

(9) G is a tree having a perfect matching M such that $\psi(x) + \psi(y) = 2q - 1$ for each matching edge $xy \in M$.

A graceful labelling *ψ holds (1), (3) and (5) true; a* set-ordered graceful labelling *ψ holds (1), (3), (5) and (7) true; a* strongly graceful labelling *ψ satisfies (1), (3), (5) and (8); a* strongly set-ordered graceful labelling *ψ holds (1), (3), (5), (7) and (8) true. An* odd-graceful labelling *ψ holds (1), (4) and (6) true; a* set-ordered odd-graceful labelling *ψ holds (1), (4), (6) and (7) true; a* strongly odd-graceful labelling *ψ satisfies (1), (4), (6) and (9); a* strongly set-ordered odd-graceful labelling ψ *holds (1), (4), (6), (7) and (9) true, simultaneously.*

In [8], the authors show: *A connected bipartite graph H admits a (strongly) set-ordered graceful labelling if and only if H admits a (strongly) set-ordered odd-graceful labelling.* We will use the graph labellings defined in Definition 2 in this article.

Definition 2 *Let G be a (p,q)-graph, and let $S_{k,d} = \{k, k+d, \dots, k+(q-1)d\}$ for integers $k \geq 1$ and $d \geq 1$.*

(1) [9] A (k,d)-graceful labelling *f of G holds $f(V(G)) \subseteq [0, k+(q-1)d]$, $f(x) \neq f(y)$ for distinct $x, y \in V(G)$ and $f(E(G)) = \{|f(u) - f(v)|;\ uv \in E(G)\} = S_{k,d}$. Especially, a $(k,1)$-graceful labelling is also a k-graceful labelling.*

(2) [5] A felicitous labelling *f of G holds $f(V(G)) \subseteq [0,q]$, $f(x) \neq f(y)$ for distinct $x, y \in V(G)$ and $f(E(G)) = \{f(uv) = f(u) + f(v) \pmod q : uv \in E(G)\} = [0, q-1]$; and furthermore, f is* super *if $f(V(G)) = [0, p-1]$.*

(3) [5] An edge-magic total labelling *f of G holds $f(V(G) \cup E(G)) = [1, p+q]$ such that for any edge $uv \in E(G)$ and $f(u) + f(v) + f(uv) = c$, where the magic constant c is a fixed integer; and furthermore f is* super *if $f(V(G)) = [1, p]$.*

(4) [5] An edge-magic graceful labelling *f of G holds $f(V(G) \cup E(G)) = [1, p+q]$ such that for any edge $uv \in E(G)$, $|\ f(u) + f(v) - f(uv) = c\ |$ where the magic constant c is a fixed integer; and furthermore f is* super *if $f(V(G)) = [1, p]$.*

(5) [10] A labeling f of G is said to be (k,d)-arithmetic *if $f(V(G)) \subseteq [0, k+(q-1)d]$, $f(x) \neq f(y)$ for distinct $x, y \in V(G)$ and $\{f(uv) = f(u) + f(v) : uv \in E(G)\} = S_{k,d}$.*

(6) [11] An odd-elegant labelling *f of G holds $f(V(G)) \subset [0, 2q-1]$, $f(u) \neq f(v)$ for distinct $u, v \in V(G)$, and $f(E(G)) = \{f(uv) = f(u) + f(v) \pmod{2q} : uv \in E(G)\} = \{1, 3, 5, \dots, 2q-1\}$.*

By the definition of a (k,d)-graceful labelling, we know that the graph having a (k,d)-graceful labelling must be bipartite, and this property can be obtained by odd-graceful graphs [8]. Guo *et al.* [12] defined a *strongly* (k,d)*-graceful labelling* as: *Let a (p,q)-graph G has a (k,d)-graceful labelling f and a perfect matching M. If $f(u) + f(v) = k + (q-1)d$ for each edge $uv \in M$, then f is called a strongly (k,d)-graceful labelling of G, and G is called a strongly (k,d)-graceful graph.* When $(k,d) = (1,1)$, f is just a strongly graceful labelling of G; as $(k,d) = (1,2)$, f is a strongly odd-graceful labelling of G [5]. We show the examples shown in Fig.2 for understanding Definition 1,2. Three new labellings are defined in Definition 3.

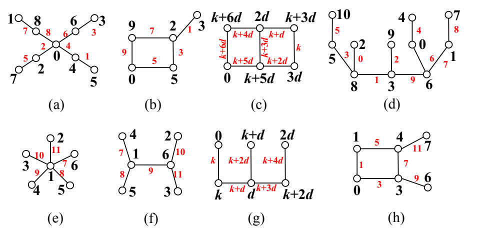

Figure 2. An example for illustrating Definition 1,2 (a) A strongly graceful labelling; (b) a set-ordered odd-graceful labelling; (c) a (k,d)-graceful labelling; (d) a felicitous labelling; (e) a super edge-total graceful labelling; (f) a super edge-magic graceful labelling; (g) a (k,d)-arithmetic labelling; (h) an odd-elegant labelling.

2.2 New graphical passwords

Definition 3 *Let T be a (p,q)-tree having a perfect matching M, and let $S_{k,d} = \{k, k+d, \dots, k+(q-1)d\}$, $S'_{k,d} = \{k, k+2d, \dots, k+2(q-1)d\}$, $S''_{k,d} = \{k, k+d, \dots, k+(p+q-1)d\}$ for integers $k \geq 1$ and $d \geq 1$. Suppose that each leaf of T is an end of some matching edge of M, so $M(L)$ is the set of all leaves of T, and furthermore the graph $T - M(L)$ obtained by deleting all leaves of T is a tree having $c = |V(T - M(L))|$ vertices. AM is the abbreviation of arithmetic matching.*

(1) An AM-(k,d)-totally odd/even graceful labelling *f of G holds $f(V(G)) \subseteq [0, k+2(q-1)d]$, $f(x) \neq f(y)$ for distinct $x, y \in V(G)$ and $f(E(G)) = \{|f(u) - f(v)| : uv \in E(G)\} = S'_{k,d}$. Meanwhile, $f(u) + f(v) = k + 2(q-1)d$ for each edge $uv \in M$.*

(2) An AM-(k,d)-felicitous labelling *f of G holds $f(V(G)) \subseteq [0, k+(q-1)d]$, $f(x) \neq f(y)$ for distinct $x, y \in V(G)$ and $f(E(G)) = \{f(uv) = f(u) + f(v) \pmod{qd} : uv \in E(G)\} = S_{k,d}$; and*

 DOI: 10.1051/matecconf/201713900204

furthermore, f is super *if $f(V(G)) = [0, (\frac{p}{2} - 1)d] \cup [k + \frac{p}{2}d, k + (p - 1)d]$. Meanwhile, $|f(u) - f(v)| = k + cd$ for each edge $uv \in M$.*

(3) An AM-(k, d)-edge-magic total labelling *f of G holds $f(V(G) \cup E(G)) \subseteq [0, k+(p+q-1)d]$ such that for any edge $uv \in E(G)$ and $f(u) + f(v) + f(uv) = a$, where the magic constant a is a fixed integer; and furthermore, f is* super *if $f(V(G)) = [1, \frac{p}{2}d] \cup [k + \frac{p}{2}d, k + qd]$. Meanwhile, $|f(u) - f(v)| = k + (c - 1)d$ for each edge $uv \in M$ and the elements of $f(E(T))$ yield an arithmetic progression having $|M|$ terms and the first term $k + 2(p - 1)d$ and the common difference $-2d$.*

(4) An AM-(k, d)-edge-magic graceful labelling *f of G holds $f(V(G) \cup E(G)) \subseteq [0, k + (p + q - 1)d]$ such that for any edge $uv \in E(G)$, $| f(u) + f(v) - f(uv) |= a$ where the magic constant a is a fixed integer; and furthermore, f is* super *if $f(V(G)) = [1, \frac{p}{2}d] \cup [k + \frac{p}{2}d, k + qd]$. Meanwhile, $|f(u) - f(v)| = k + (c - 1)d$ for each edge $uv \in M$ and the elements of $f(E(T))$ yield an arithmetic progression having $|M|$ terms and the first term $k + pd$ and the common difference $2d$.*

(5) Suppose that T has a (k, d)-arithmetic f. If $|f(u) - f(v)| = k$ for each edge $uv \in M$, and the elements of $f(E(T))$ produce an arithmetic progression having $|M|$ terms and the first term k and the common difference $2d$. Then we call f an AM-(k, d)-arithmetic labelling *of T.*

(6) An AM-(k, d)-totally odd/even-elegant labelling *f of G holds $f(V(G)) \subset [0, k + 2(q - 1)d]$, $f(u) \neq f(v)$ for distinct $u, v \in V(G)$, and $f(E(G)) = \{f(uv) = f(u) + f(v) (\mathrm{mod}\ k + 2qd) : uv \in E(G)\} = S'_{k,d}$. Meanwhile, $|f(u) - f(v)| = k$ for each edge $uv \in M$ and the elements of $f(E(T))$ yield an arithmetic progression having $|M|$ terms and the first term k and the common difference $4d$.*

Remark. The parity of AM-(k, d)-totally odd/even graceful labelling is related to the value of k, if $k = odd/even$, then it is AM-(k, d)-totally odd/even graceful labelling.

Eight examples shown in Fig.3 are for understanding Definition 1,2 and 3.

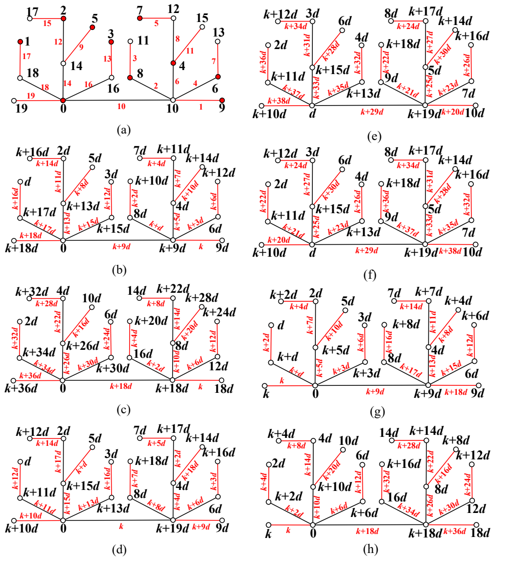

Figure 3. Eight examples for illustrating Definition 1,2 and 3. (a) A strongly set-ordered graceful labelling; (b) a strongly (k, d)-graceful labelling; (c) an AM-(k, d)-totally odd/even graceful labelling; (d) an AM-(k, d)-super felicitous labelling; (e) an AM-(k, d)-super edge-magic total labelling; (f) an AM-(k, d)-super edge-magic graceful labelling; (g) an AM-(k, d)-arithmetic labelling (h) an AM-(k, d)-totally odd/even-elegant labelling.

3 Main results on trees having perfect matching

3.1 Connections of strongly (k, d)-graphical labellings on trees having perfect matching

Lemma 1 *Let T be a tree having n (≥ 4) vertices and a perfect matching M, and let (X, Y) be its bipartition. Let $S_{k,d} = \{k, k + d, \ldots, k + (n - 2)d\}$ for integers $k \geq 1$ and $d \geq 1$. If each edge of the perfect matching M has an end of degree one, then we have the following pairwise equivalent assertions:*

(1) T admits a strongly set-ordered graceful labelling;

(2) T admits a strongly (k, d)-graceful labelling;

(3) T admits an AM-(k, d)-totally odd/even graceful labelling;

DOI: 10.1051/matecconf/201713900204

(4) T admits an AM-(k,d)-super felicitous labelling;

(5) T admits an AM-(k,d)-super edge-magic total labelling;

(6) T admits an AM-(k,d)-super edge-magic graceful labelling;

(7) T admits an AM-(k,d)-arithmetic labelling;

(8) T admits an AM-(k,d)-totally odd/even-elegant labelling.

Lemma 2 *Suppose that a tree T containing a perfect matching $M(T)$ admits a strongly graceful labelling f. Then*

(i) *(Edge-exchanging operation) T admits another strongly graceful labelling g defined as $g(u) = f(v)$ and $g(v) = f(u)$ for each edge $uv \in M(T)$.*

(ii) *(Leaf-decreasing operation) Suppose that an edge $uv \in M(T)$ holds $\deg_T(v) = 1$ and $N(u) = \{v, u_i : i \in [1, d_u - 1]\}$, where $d_u = \deg_T(u) \geq 3$. The tree H obtained by deleting edges uu_j and joining v with u_j for $j \in [s+1, d_u - 1]$, where $0 \leq s < d_u - 1$, is strongly graceful too, and H has a perfect matching $M(H)$ such that $|L(T) \cap V(M(T))| - 1 = |L(H) \cap V(M(H))|$.*

(iii) *(Leaf-increasing operation) Suppose that an edge $uv \in M(T)$ holds $\deg_T(u) \geq 2$ and $\deg_T(v) \geq 2$. We have a strongly graceful tree G obtained by deleting the edge uv from T, identifying u with v into one vertex, denoted as u_0, and joining a new vertex v_0 with u_0, and furthermore G has a perfect matching $M(G) = \{u_0v_0\} \cup (M(T) \setminus \{uv\})$ such that $|L(T) \cap V(M(T))| + 1 = |L(G) \cap V(M(G))|$.*

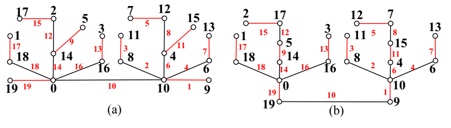

Figure 4. An example for understanding the results of Lemma 2. The strongly graceful tree (a) has ten leaves greater than that of the strongly graceful tree (b) obtained by Lemma 2.

Fig.4 is for understanding Lemma 2. By Lemmas 1 and 2, we get the main result of this article as follows:

Theorem 1 *The eight assertions in Lemma 1 on a tree having a perfect matching are equivalent to each other.*

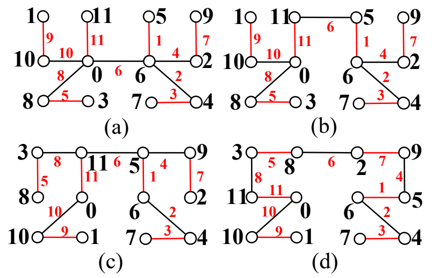

Figure 5. From (a) to (d) is the process trees having perfect matching can be converted into paths perfect matching in turn.

3.2 Trees having perfect matching can be converted into paths perfect matching

By studying the three operations of lemma 2, we define the following operation:

Definition 4 *Suppose that a (p,q)-graph G having perfect matching M have a strongly labelling f, if $f(xy) = f(uv), uv \in M, xy \notin E(G)$, then delete the edge uv and add the edge xy, this operation is called* mismatched edge transfer operation.

By mismatched edge transfer operation and operations of lemma 2, trees having perfect matching will be converted into paths having perfect matchings.

4 Conclusion

We have introduced six new graph labellings for trees having perfect matchings discovered by our working on researching graphical passwords, and show the equivalencies of eight graph labellings of trees having perfect matchings in lemma 1 and theorem 1. Moreover, by mismatched edge transfer operation and operations of lemma 2, trees having perfect matching will be converted into paths perfect matching, and the nature of the original passwords remains unchanged. Clearly, our results can help designers to produce Topsnut-GPWs quickly. On the other hands, our methods in the proofs of our rusults can be easily transformed into feasible and effective algorithms having polynomial complex. Thereby, our methods on dealing with Topsnut-GPWs can yield Topsnut-GPWs having high security level by polynomial algorithms. Moreover, by our experience working on graph labellings, we propose the following conjecture for further studying Topsnut-GPWs: *Trees with perfect matchings admit each one of six new labellings defined in Definition 3.*

Exploring the topological structure of some kind of graphs, finding its more intrinsic properties, and providing theoretical help for new graphical cryptography are indispensable. [13] and [14] explore the Equivalent Definitions Of Cactus Graphs and Euler graphs respectively. [15] and [16] explore odd-graceful labeling and odd-elegant labeling on ring computer networks.

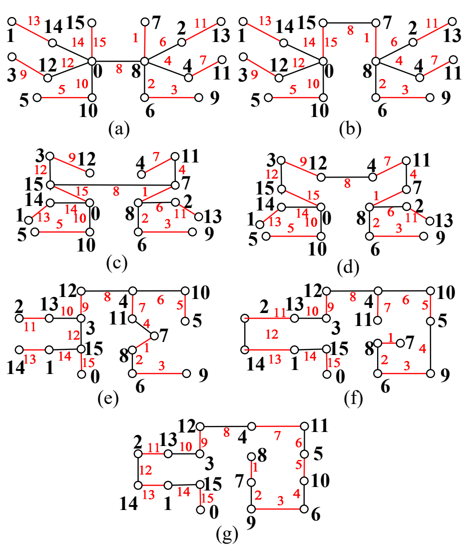

Figure 6. From (a) to (g) is the process trees having perfect matching can be converted into paths perfect matching in turn.

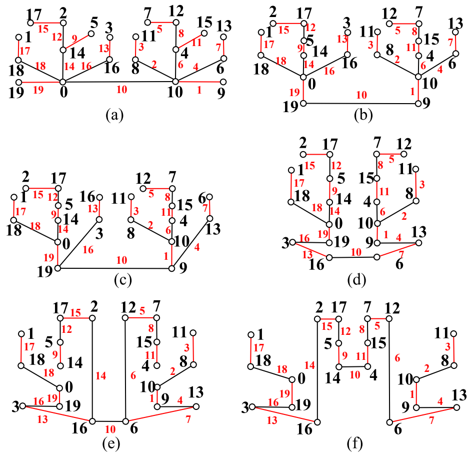

Figure 7. From (a) to (f) is the process trees having perfect matching can be converted into paths perfect matching in turn.

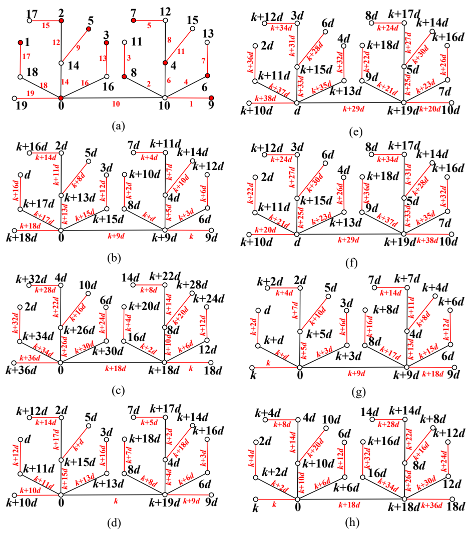

Figure 8. Eight examples for illustrating Definition 1,2 and 3. (a) A strongly set-ordered graceful labelling; (b) a strongly (k, d)-graceful labelling; (c) an AM-(k, d)-totally odd/even graceful labelling; (d) an AM-(k, d)-super felicitous labelling; (e) an AM-(k, d)-super edge-magic total labelling; (f) an AM-(k, d)-super edge-magic graceful labelling; (g) an AM-(k, d)-arithmetic labelling (h) an AM-(k, d)-totally odd/even-elegant labelling.

Acknowledgment

This project was supported by the National Natural Science Foundation of China under grant No. 61163054, No. 61363060 and No. 61662066.

References

[1] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, Graphical Passwords: A Survey. In Annual Computer Security Applications Conference (ACSAC), December 2005: 463-472. DOI: 10.1109/CSAC.2005.27 Source: DBLP

[2] Hongyu Wang, Jin Xu,Bing Yao. The Key-models And Their Lock-models For Designing New Labellings Of Networks.Proceedings of 2016 IEEE Advanced Information Management, Communicates,Electronic and Automation Control Conference (IMCEC 2016) pp565-5568.

[3] Hongyu Wang, Jin Xu,Bing Yao. Exploring New Cryptographical Construction Of Complex Network Data. IEEE First International Conference on Data Science in Cyberspace. IEEE Computer Society, (2016):155-160.

[4] R. N. Shepard, Recognition memory for words, sentences, and pictures, Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.

[5] Joseph A. Gallian. A Dynamic Survey of Graph Labeling. The Electronic Journal Of Combinatorics, 17 (2014), # DS6. (308 pages, 1693 reference papers)

[6] Bondy J. A. and Murty U. S. R. Graph Theory. Springer, ISBN: 978-1-84628-969-9, e-ISBN: 978-1-84628-970-5, DOI: 10. 1007/978-1-84628-970-5, 2008.

[7] Bing Yao, Xia Liu and Ming Yao. Connections between labellings of trees. Bulletin of the Iranian Mathematical Society, ISSN: 1017-060X (Print) ISSN: 1735-8515 (Online), Vol. **43** (2017): 275-283.

[8] Xiangqian Zhou, Bing Yao, Xiang-en Chen and Haixia Tao. A proof to the odd-gracefulness of all lobsters. Ars Combinatoria **103** (2012), 13-18.

[9] S.M. Hegde. On (k,d)-graceful graphs. Journal of Combinatorics, Information and System Sciences, Vol. **25** (1-4) (2000), 255-265.

[10] B. D. Acharya and S. M. Hegde. Arithmetic graphs. *J. Graph Theory*, **14** (1990), 275-299.

[11] Xiangqian Zhou, Bing Yao, Xiang'en Chen. Every Lobster Is Odd-elegant. Information Processing Letters **113** (2013), 30-33.

[12] Jinxia Guo, Bing Yao, Jiajuan Zhang. On Generalized Gracefulness Of Edge-Symmetri Trees. Journal Of Southwestern University (in Chinese), 2013, **35** (2): 62-68.

[13] Hui Sun, Bing Yao. On Equivalent Definitions Of Cactus Graphs. 2017 submitted.

[14] Hui Sun, Bing Yao. Exploring equivalent definitions of Euler graphs. 2017 submitted.

[15] Hui Sun, Bing Yao. Exploring the Odd Gracefulness of Cyclic-Dragon Graphs. 2017 submitted.

[16] Hui Sun, Bing Yao. On the odd-elegant quality of cyclic-dragon graphs. 2017 submitted.