New Algebraic Groups Produced By Graphical Passwords Based On Colorings And Labellings

Hui Sun[1], *Xiaohui* Zhang[1], *Meimei* Zhao[3] 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
[3] College of Science, Gansu Agricultural University, Lanzhou 730070, CHINA

Abstract. Safety of plain text passwords has been questioned in current researching information passwords. Graphical passwords are another way for alternative text-based passwords and to improve the user account security. As we are constructing Topsnut-graphical passwords that can be traced to an idea of "Graph structure plus the number theory" proposed first by Hongyu Wang with her colleagues, we find that some of Topsnut-graphical passwords can be composed of algebraic groups under the principle of Abelian additive finite group. We apply the odd-elegant labelling of graph theory to produce Topsnut-graphical passwords, and verify our Topsnut-graphical passwords can form algebraic groups, called *labelling graphical groups*. Our results can provide those users who have business in two or more banks, and our methods are easily transformed into algorithms with polynomial times.

1 Introduction

Everyone in today's society has at least two or three passwords. Your password can not only ensure the safety of personal privacy, but also provide a sense of security for the user. The password is stolen and lost it, which is often seen in daily life. Safety of plain text password has been questioned. A graphical password is one of the ways to alternative for text-based passwords and to improve the user account security, because of graphical passwords are easy for users and difficult to be broken by attackers [1]. New graphical passwords can be made by the idea of "Graph structure plus the number theory" due to Wang *et al*. in [2] and [3], we call such new graphical passwords as *Topsnut-graphical passwords* for distinguishing with other graphical passwords. Studies have shown that humans remember pictures more than texts, and psychological research supports the hypothesis [4]. In addition, Topsnut-graphical passwords differ from those graphical passwords mentioned in [1], since they need less storage space and can be realize in communication quickly.

We show an example to introduce Topsnut-graphical pass-words simply. Alina goes to a bank for her business. First of all, she is given six topological structures (also, six graphs) shown in Fig.1, and is asked for selecting a graph for making a key. Secondly, she select the graph shown in Fig.1 (e) and Fig.2 (1) as the base of her key. Next, she labels each small circle of the graph shown in Fig.2 (2) with a positive integer, continuously, she labels each *edge* that joins two small circles with a positive integer, these two small circles are called the *ends* (also, vertices in graph theory) of the edge. Finally, she obtain her key shown in Fig.2 (3), this key is called a opsnut-graphical password. Observe the well-labelled graph Fig.2 (3), we can find that three numbers x,y,z on an edge labelled with number y and its two ends labelled with numbers x,z hold $x + z = y$ (mod 16), that is, $x + z = y$ if $x + z < 16$, and $x + z - 16 = y$ if $x + z \geq 16$.

Naturally, from the view of theoretical investigation and practice, we want to solve some basic problems: (i) Find all graphical passwords for the graph Fig.2(1)? (ii) Find connections among graphical passwords of the graph if the problem (i) are determined; (iii) Find all of graphs having 7 vertices and 8 edges. As known, many graph labellings can be used to other applications out of graph theory. We will apply operations, colorings and labellings of graph theory ([5], [6], [7]) to answer partially these three problems. In the following discussion, we will show an application of the odd-elegant labelling of graph theory.

* Corresponding author: yybb918@163.com

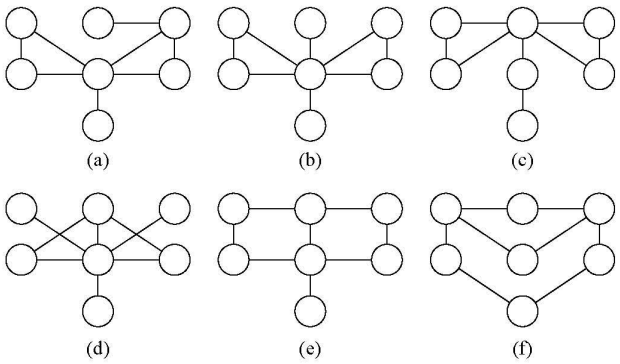

Fig. 1. Six topological structures.

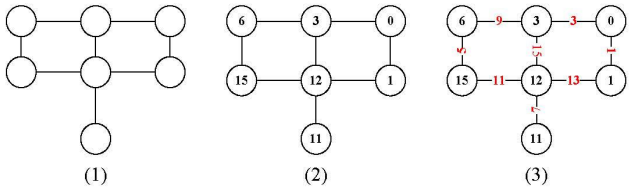

Fig. 2. Alina makes a graphical password.

2 Graphical groups

2.1 Preliminary

The shorthand notation $[m,n]$ to indicate a set $\{m,m+1,...,n\}$ with integers m,n respect to $0 \le m < n$; the symbol $[s,t]^o$ denotes an odd number set $\{s,s+2,...,t\}$ with odd numbers s,t keeping $1 \le s < t$; the notation $[\alpha,\beta]^e$ stands up an even number set $\{\alpha,\alpha+2,...,\beta\}$ with even numbers α, β falling into $2 \le \alpha < \beta$; $|X|$ is the cardinality of elements of a set X. All graphs mentioned here are undirected, finite, no multiple-edges and no loops, and we call them *simple graphs*. A (p,q)-graph G has its vertex set $V(G)$ of cardinality p and edge set $E(G)$ of cardinality q. Another two notations will be used in this article are $N(x) = \{v : v \in V(G)\}$ (the set of all vertices adjacent to a vertex v in G, called the *neighborhood* of x) and $N_e(x) = \{xv : v \in N(x)\}$ (called the *edge-neighborhood* of x). The symbol $\deg(x)$ stands for the degree of a vertex x, also, $\deg(x) = |N(x)|$.

Definition 1. Let X be a non-empty set, and let $\odot$ be a 2-element operation on X. We call the algebraic structure $\Gamma = (X,\odot)$ as a group if it holds:

(1) *Uniqueness and Closure*: $x \odot y \in X$ holds for any pair of elements $x,y \in X$;

(2) *Unit element* (*zero element*): There exists an element $e \in X$ such that $e \odot x = x \odot e = x$ for each element $x \in X$;

(3) *Inverse element*: Any element $x \in X$ corresponds another element $y \in X$ such that $x \odot y = y \odot x = x$, we call y the inverse element of x, denoted as $y = x^{-1}$;

(4) *Associative law*: Any triple $x,y,z \in X$ holds $(x \odot y) \odot z = x \odot (y \odot z)$.

Furthermore, $\Gamma = (X,\odot)$ is called an *Abelian group* (a *commutative group*) if the 2-element operation $\odot$ holds the commutative law true.

3 Graphical groups based on graph labellings

3.1 A graphical group obtained from the graph odd-elegant labelling

Let $f_1: V(H_1) \to [0,q]$ be an odd-elegant labelling such that $f_1(E(H_1)) = [1,2q-1]$ for a (p,q)-graph H_1. Define a *modular labelling* $f_k(x) = f_1(x) + (k-1) \pmod{2q}$ with $x \in V(G)$ and $k \in [1,2q]$. Notice that $F(H_{2q+1}) = F(H_1)$. As $k \in [2,2q]$, each copy of the (p,q)-graph H_1 is written as H_k, and $F(H_k)$ is the graph labelled the vertices of H_k by the labelling f_k. Define a 2-element operation $F(H_i) \oplus_k F(H_j)$ on a set $O_{dde}(H) = \{F(H_k): k \in [1,2q]\}$ by $[f_i(x) + f_j(x) - f_k(x)]_{(\mathrm{mod}\ 2q)}$ with $x \in V(G) = V(H_i) = V(H_j) = V(H_k)$, where $[f_i(x) + f_j(x) - f_k(x)]_{(\mathrm{mod}\ 2q)}$ means that

$$[f_i(x) + f_j(x) - f_k(x)]_{(\mathrm{mod}\ 2q)} = 2q - [f_i(x) + f_j(x) - f_k(x)] \quad (1)$$

if $f_i(x) + f_j(x) - f_k(x) < 0$ or $f_i(x) + f_j(x) - f_k(x) \ge 2q$, otherwise,

$$[f_i(x) + f_j(x) - f_k(x)]_{(\mathrm{mod}\ 2q)} = f_i(x) + f_j(x) - f_k(x) \quad (2)$$

We call this particular operation as the *odd-elegant additive-sum* of graphs.

Theorem 1. *The set $O_{dde}(H)$ based on a (p,q)-graph H_1 forms an Abelian group, we call $O_{dde}(H)$ a labelling graphical group (labelling graphical Abelian group) based on the graph G hereafter. Furthermore, $f_k(uv) = f_1(uv) + 2(k-1)$ with $k \in [1,2q]$.*

Proof. First of all, the equation

$$F(H_i) \oplus_k F(H_j) = F(H_{i+j-k}) \quad (3)$$

with $i + j - k \pmod{2q} \in [1,2q]$ follows the equation

$$[f_i(x) + f_j(x) - f_k(x)]_{(\mathrm{mod}\ 2q)} = f_1(x) + (i + j - k - 1) \pmod{2q} = f_{i+j-k}(x)$$

with $x \in V(G) = V(H_i) = V(H_j) = V(H_k)$. We are ready to show five principles for a standard group in the following.

(1) *Zero element*. The zero element of $O_{dde}(H)$ is $F(H_1)$ as $k = 1$ in the equation (3).

(2) *Inverse element*. The inverse of each element $H_i \in O_{dde}(H)$ is the element $H_{2q+2-i} \in O_{dde}(H)$. In fact,

$$F(H_1) \oplus_1 F(H_{2q+2-i}) = F(H_{2q+1}) = F(H_1).$$

(3) *Uniqueness and Closure*. $F(H_i) \oplus_k F(H_j) \in O_{dde}(H)$ follows the equation (3).

(4) *Associative law*.

$[F(H_i) \oplus_k F(H_j)] \oplus_k F(H_l) = F(H_i) \oplus_k [F(H_j) \oplus_k F(H_l)]$.

Since

$[F(H_i) \oplus_k F(H_j)] \oplus_k F(H_l) = F(H_{i+j-k}) \oplus_k F(H_l) = F(H_{i+j+l-2k})$, and

$F(H_i) \oplus_k [F(H_j) \oplus_k F(H_l)] = F(H_i) \oplus_k F(H_{j+l-k}) = F(H_{i+j+l-2k})$, so the associative law holds true.

(5) *Commutative law.*

$$F(H_i) \oplus_k F(H_j) = F(H_j) \oplus_k F(H_i).$$

Since $F(H_i) \oplus_k F(H_j) = F(H_{i+j-k}) = F(H_{j+i-k}) = F(H_j) \oplus_k F(H_i)$.

We conclude that $O_{dde}(H)$ is an odd-elegant graphical group. Next, we determine a connection between $f_1(uv)$ and $f_k(uv)$ with $k \in [1,2q]$ in the following.

Notice that $f_1(E(H_1)) = [1,q]$. Consider the labelled graph H_k, take an edge $uv \in E(H_k)$, we have

$f_k(uv) = f_k(u) + f_k(v) = [f_1(u) + (k-1)] \pmod{2q} + [f_1(v) + (k-1)] \pmod{2q}$,

and there are the following cases:

$$\begin{aligned} f_k(uv) &= f_k(u) + f_k(v) \\ &= [f_1(u) + (k-1)] + [f_1(v) + (k-1)] \\ &= f_1(u) + f_1(v) + 2(k-1) \\ &= f_1(uv) + 2(k-1); \end{aligned}$$

The proof of this theorem is complete.

A *dual labelling* $\overline{f_k}$ of a modular labelling f_k is defined by $\overline{f_k}(x) = 2q - f_k(x)$ with $x \in V(G)$. Let $\overline{O}_{dde}(H)$ be the set of graphs H_k, where each H_k is a labelled H by the dual labelling $\overline{f_k}$ *of* the modular labelling $f_k(x)$ with $x \in V(H)$ and $k \in [1,2q]$. We have

Corollary 2. *The set* $\overline{O}_{dde}(H)$ *forms a labelling graphical group* (*labelling graphical Abelian group*) *based on the* (*p,q*)*-graph H.*

3.2 Examples for illustrating Theorem 1

We show an example in Fig.3 for illustrating Theorem 1.

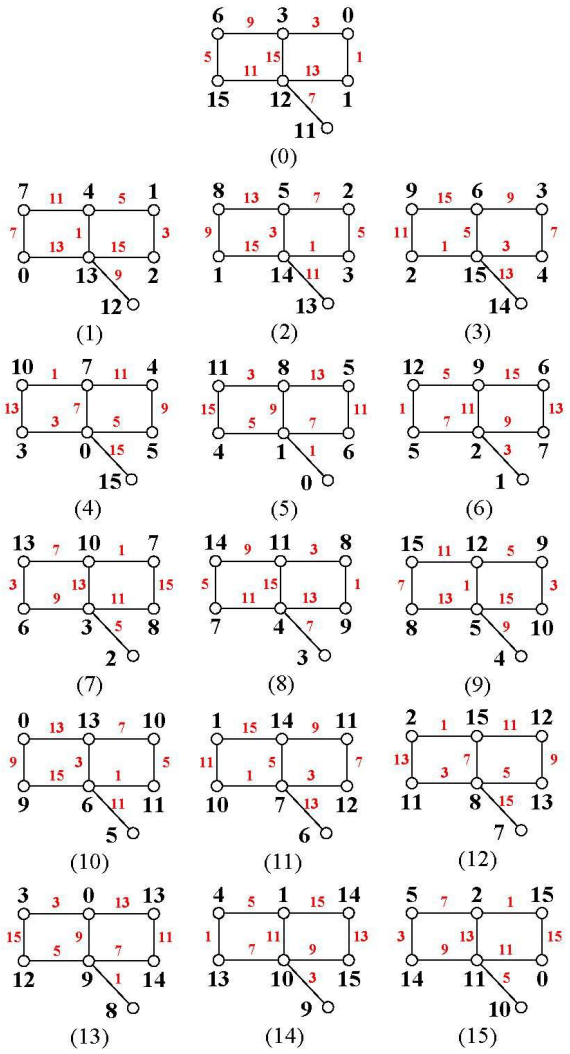

Fig. 3. A labelling graphical group for illustrating Theorem 1.

3.3 A new graph labelling

We, based on the previous results and examples, define a new labelling of graphs as follows:

Definition 2. A labelling h of a (p,q)-graph G is called a ***2q-modular odd-elegant labelling*** if $h : V(G) \to [0,2q-1]$, and $h(E(G)) = \{[h(u) + h(v)] \pmod{2q} : uv \in E(G)\} = [1,2q-1]^o$.

According to Definition 2 we can define a negative-labelling (see Fig.4), or a mixed-labelling for a graph G (see Fig.3 and Fig.4).

3.4 A mixed labelling graphical group

In fact, we can generalize our coloring/ labelling/operation graphical quasi-groups/groups. A labelling graphical group Hroup is formed by two collections A and B shown in Fig.3 and 4. It is not hard to define a 2-element operation on Hroup defined by

$[g_i(x)+g_j(x)-g_k(x)]_{(\mathrm{mod}\ 2q)}$, $[h_i(x)+h_j(x)-h_k(x)]_{(\mathrm{mod}\ 2q)}$,

$[g_i(x)+g_j(x)-h_k(x)]_{(\mathrm{mod}\ 2q)}$, $[h_i(x)+h_j(x)-g_k(x)]_{(\mathrm{mod}\ 2q)}$,

$[h_i(x)+g_j(x)-h_k(x)]_{(\mathrm{mod}\ 2q)}$ and $[g_i(x)+h_j(x)-g_k(x)]_{(\mathrm{mod}\ 2q)}$.

This example implies a new graph labelling, called a mixed odd-elegant labelling (see g_1 shown in Fig.3 and h_1 shown in Fig.4).

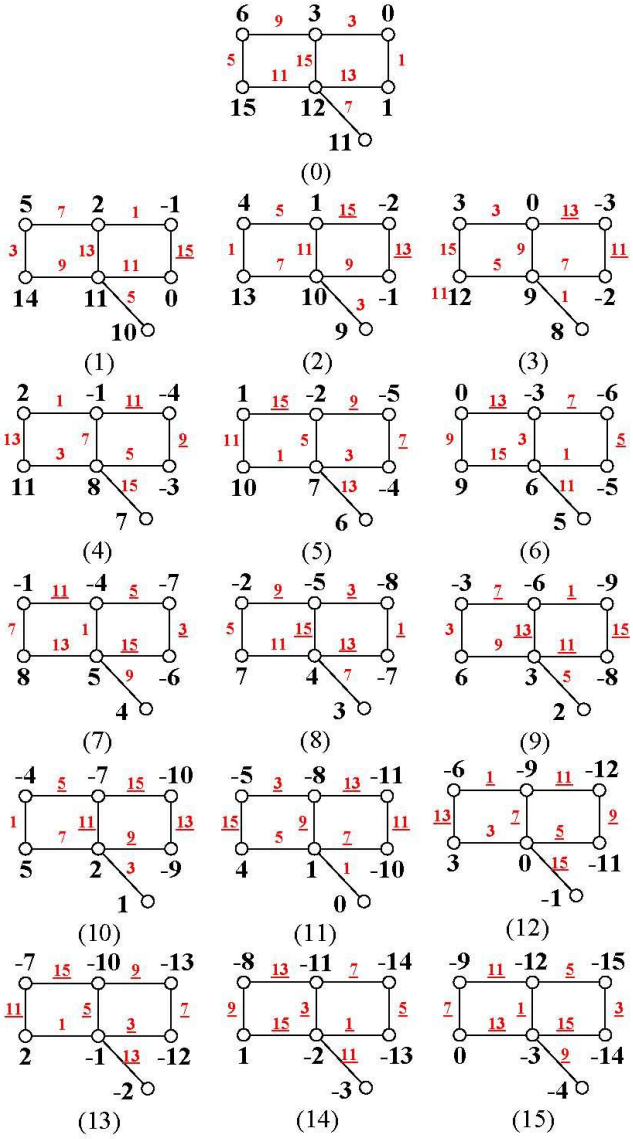

Fig. 4. A negative-labelling graphical group opposite with the group shown in Fig. 3.

Theorem 3. *The set $MO_{dde}(H)$ based on a (p,q)-graph H_1 forms an Abelian group, we call $MO_{dde}(H)$ a labelling graphical group (labelling graphical Abelian group) based on the graph G hereafter.*

Proof: A labelling graphical group H_{roup} is formed by two collections A and B. Define a 2-element operation on H_{roup} defined by

(i) $[g_i(x)+g_j(x)-g_k(x)]_{(\mathrm{mod}\ 2q)}$,

(ii) $[h_i(x)+h_j(x)-h_k(x)]_{(\mathrm{mod}\ 2q)}$,

(iii) $[g_i(x)+g_j(x)-h_k(x)]_{(\mathrm{mod}\ 2q)}$,

(iv) $[h_i(x)+h_j(x)-g_k(x)]_{(\mathrm{mod}\ 2q)}$,

(v) $[h_i(x)+g_j(x)-h_k(x)]_{(\mathrm{mod}\ 2q)}$

(vi) $[g_i(x)+h_j(x)-g_k(x)]_{(\mathrm{mod}\ 2q)}$.

It is not hard to verify $g_i(x) = h_{2q-i}(x)$ (mod $2q$) for $i \in [1,2q-1]$, and $g_0(x) = h_0(x)$. So, this theorem holds true according to Theorem 1.

4 Conclusion

Based on the new definition of graph coloring / labeling operations, we found the graph coloring / label constitute a algebraic group. In Theorem 1, we found that set $O_{dde}(H)$ and 2-element operation $F(H_i) \oplus_k F(H_j)$ constitute a algebraic group for which we are in the same class label, converted from one label to another label provides a feasible method. Our results show that there are groups in which any element can be defined as the zero element by the 2-element operation $\oplus_{k_0}$ in [14].

We already know that there is a label f of graph G, then it must have the corresponding dual label $\overline{f}$. That is to say, the original label and its dual label always appear in pairs 2. According to Definition 2 we can define a negative- labelling, and a mixed-labelling for a graph G. In theorem 3, We find a way to extend the two groups into a new group.

The mixed odd-elegant labelling, mentioned the above, can leads to some mathematical conjectures , such as: *There is a mixed odd-elegant labelling of every tree*. Furthermore, we can transplant this new labelling to other graph labellings, for instance, felicitous labelling in [8], (generalized) edge-magic total labelling in [9], [10] and [12], strongly graceful labelling in [11], even other labellings in [13] and so on, which means that exploring new graphical passwords will bring more new mathematical subjects and problems. Moreover, the mixed odd-graceful labeling has been studied in [14]. Exploring the topological structure of some kind of graphs, finding its more intrinsic properties, and providing theoretical help for new graphical cryptography are indispensable. [15] and [16] explore the equivalent definitions of cactus graphs and euler graphs respectively. [17] and [18] explore odd-graceful labeling and odd-elegant labeling on ring computer networks. Finally, we will explore other new 2-element

operations and design new graphical passwords for determining graphical quasi-groups/groups in practice.

Acknowledgements.

The work has been supported by the National Natural Science Foundation of China under grants No. 61163054, No. 61363060, and No. 616620660.

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* **6**, pp 156-163, (1967).
5. Bela Bollobás, The Modern Graph Theory, *Springer-Verlag*, New Tork, Inc. (1998)
6. Joseph A. Gallian, A Dynamic Survey of Graph Labelling. *The Electronic Journal of Combinatorics*, **14** (2013), #DS6.
7. Douglas B. West. Introduction to Graph Theory (Second Edition). *Mechanical Industry Press*, Bei Jing (2006).
8. Zhang J, Yao B, Wang Z, et al. Felicitous Labellings of Some Network Models. *Journal of Software Engineering and Applications* (2013) **6** (3):29-32.
9. Hongyu Wang, Bing Yao, Chao Yang, Sihua Yang, Xiang-en Chen, Ming Yao, Zhenxue Zhao. Edge-Magic Total Labellings Of Some Network Models. *Proceeding of ISCCCA13*, *Applied Mechanics and Materials* Vols. 347-350 (2013) pp 2752-2757.
10. Hongyu Wang, Bing Yao, Chao Yang, Sihua Yang, Xiang'En Chen. Labelling Properties Of Models Related with Complex Networks Based On Constructible Structures. *Advanced Materials Research* Vols.765-767 (2013) pp 1118-1123. DOI:10.4028/www.scientific.net/AMR.765-767.1118
11. Bing Yao, Hui Cheng, Ming Yao and Meimei Zhao, A Note on Strongly Graceful Trees. *Ars Combinatoria* **92** (2009), 155-169.
12. Hongyu Wang, Bing Yao, Ming Yao. Generalized Edge-Magic Total Labellings Of Models from researching Networks. *Information Sciences* **279** (2014) 460-467. DOI:10.1016/j.ins.2014.03.132
13. Bing Yao, Xia. Liu and Ming Yao. Connections Between Labellings Of Trees. *Bulletin of the Iranian Mathematical Society*, Vol. **43** (2017), No. 2, pp. 275-283.
14. Bing Yao, Hui Sun, Meimei Zhao, Jingwen Li and Guanghui Yan. On Coloring/Labelling Graphical Groups For Creating New Graphical Passwords. 2017 submitted. in Press.
15. Hui Sun, Bing Yao. On Equivalent Definitions Of Cactus Graphs. 2017 submitted.
16. Hui Sun, Bing Yao. Exploring equivalent definitions of Euler graphs. 2017 submitted.
17. Hui Sun, Bing Yao. Exploring the Odd Gracefulness of Cyclic-Dragon Graphs. 2017 submitted.
18. Hui Sun, Bing Yao. On the odd-elegant quality of cyclic-dragon graphs. 2017 submitted.