文章编号:1671-4229(2022)01-0027-07

关于任意零元阿贝尔有限模可加图群及其在信息安全中的应用

赵梅梅[1],姚 兵[2]
(1. 甘肃农业大学 理学院,甘肃 兰州 730070;2. 西北师范大学 数学与统计学院,甘肃 兰州 730070)

摘 要: 文章定义了$(q+1)$-模(负)优美标号和混合优美标号,基于这些新标号建立了任意零元阿贝尔有限模可加图群。给出了$(q+1)$-模混合优美图可以生成的图群和图子群及它们的阶。提出了每个$(q+1)$-模优美图可以生成顶点模图,每个顶点模图又可以生成边模图,这些顶点模图和边模图构成了任意零元阿贝尔有限模可加图群。对于$(q+1)$-模负优美图和$(q+1)$-模混合优美图也得到了类似的结果。此外,给出了任意零元阿贝尔有限模可加图群对网络整体加密的例子。

关键词: 图形密码;任意零元阿贝尔有限模可加图群;优美标号;边模图;顶点模图
中图分类号: O 157.5 **文献标志码:** A

On every-zero Abelian finite-modular additive graphic groups and its application in information security

ZHAO Mei-mei[1], *YAO Bing*[2]
(1. College of Science, Gansu Agricultural University, Lanzhou 730070, China;
2. College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China)

Abstract: The $(q+1)$-modular (negative) graceful labelling and mixed graceful labelling are defined. Based on these new labellings, the every-zero Abelian finite-modular additive graphic groups are established. The graphic groups and subgroups that can be generated and their orders are given when the graph is a $(q+1)$-modular mixed graceful graph. It is proposed that each $(q+1)$-modular graceful graph can generate vertex-modular graphs, each vertex-modular graph can generate edge-modular graphs, and these vertex-modular graphs and edge-modular graphs can form every-zero Abelian finite-modular additive graphic groups. Similar results are obtained for $(q+1)$-modular negative graceful graph and $(q+1)$-modular mixed graceful graph. Moreover, an example is given for the application of the every-zero Abelian finite-modular additive graphic groups to integral network encryption.

Key words: graphical password; every-zero Abelian finite-modular additive graphic group; graceful labelling; edge-modular graph; vertex-modular graph

---

基金项目: 国家自然科学基金资助项目(61363060, 61662066)
作者简介: 赵梅梅(1986—),女,讲师,硕士. E-mail:zhaomeimei125@163.com
引文格式:赵梅梅,姚兵. 关于任意零元阿贝尔有限模可加图群及其在信息安全中的应用[J]. 广州大学学报(自然科学版),2022,21(1):27-33.

1 研究简介

众所周知,密码保护系统的安全性取决于多个因素,公钥和私钥在密码学中发挥着重要作用。密码问题的经典研究可以追溯到40多年前,一些学者对现有的图形密码做了深入的研究[1-3]。图形密码是不同于文本密码的一种新型密码,图形密码易于用户记忆,而且很难被攻击者破解。现有的图形密码缺点是图片频繁更改会占用计算机庞大的空间,用户需要学习更多的相关知识并具有良好的记忆,不支持更多的个性化创意和个性化的图形密码。为了解决图形密码的缺点,王宏宇等[4-6]提出了拓扑图形密码,其思想是"拓扑结构+数论"。拓扑图形密码是由图论中的拓扑结构和着色(标号)组成的。由于拓扑图形密码通过代数矩阵保存在计算机中[7],这就使得拓扑图形密码比现有的图形密码占用计算机的空间小,关于数矩阵的算法是多形式的,因此,可以快速实现拓扑图形密码。更为重要的是,拓扑图形密码可以用来对网络进行整体加密,加之大量的NP-问题和猜想存在于拓扑图形密码中,使得拓扑图形密码具有抗量子计算的能力[8]。

云计算引入"同态加密"技术提供了一种对加密数据进行处理的功能[9],提高了数据的安全隐私保护,实现"数据不可见"性。同态加密技术可以应用在很多领域,例如,在案件调查过程中,警察可以搜索嫌犯的行程、财务记录,以及调查通讯和邮件记录,且不会暴露嫌犯的数据。医学研究人员可以根据数百万患者的记录,来识别基于人口结构和地理位置的疾病趋势。政府和商业机构能够很好地对财务数据进行分析和处理。值得注意的是,同态加密技术也可以在原有基础上使用区块链技术,且不会对区块链属性造成任何重大的改变。图群整体加密技术在公有区块链上进行加密,随时加密公用区块链上的数据。

本文介绍的任意零元阿贝尔有限模可加图群可以应用于"同态图群",这将产生"同态图群加密"技术,在云计算、抗量子计算中具有可应用性。下面给出一个网络整体加密的例子,采用了图1中的任意零元(7)-模混合优美图群,它是一个任意零元阿贝尔有限模可加图群。图2为给网络 T 进行整体加密。

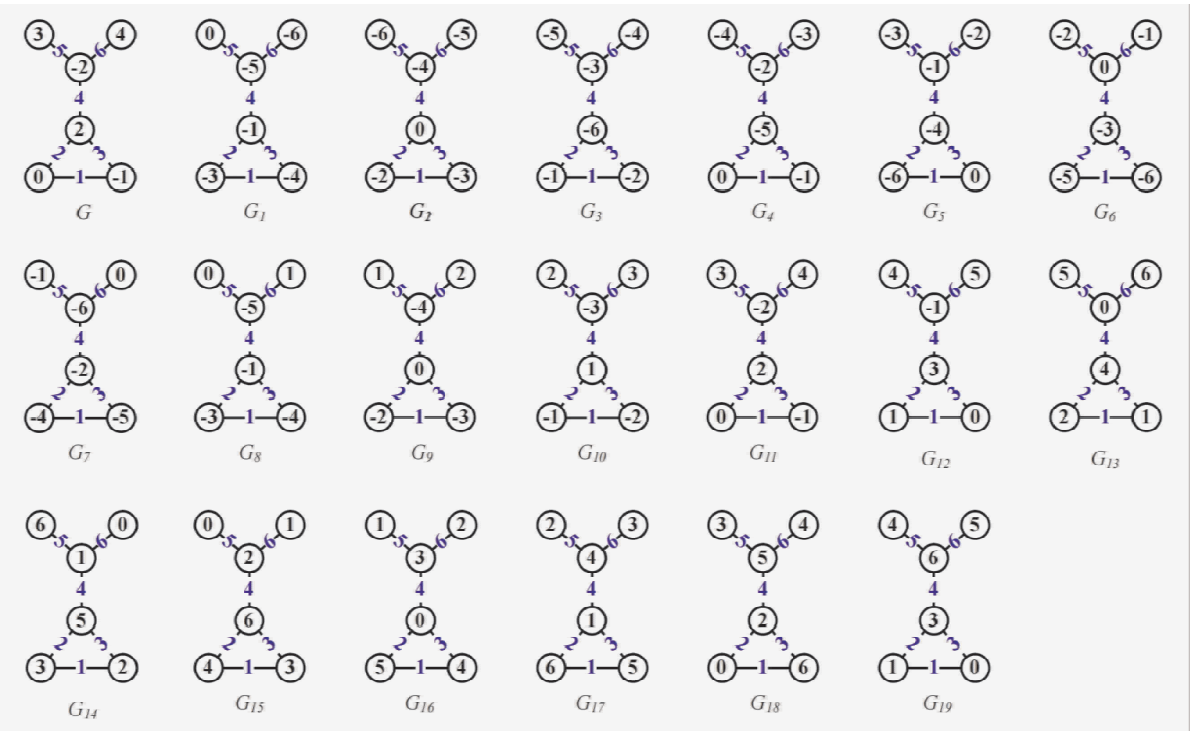

图1 一个(7)-模混合优美图 G 能生成19个(7)-模图

Fig. 1 A(7)-modular mixed graceful graph can generate 19 (7)-modular graphs

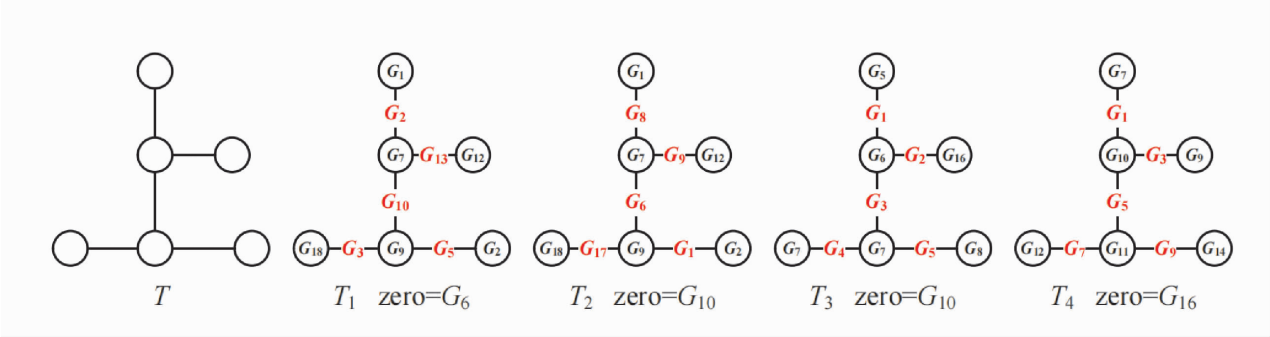

图 2　给网络 T 进行整体加密

Fig. 2　Encrypting integrally a network T

图 2 给出网络 T 的 4 个整体加密，其中，T_1 和 T_2 的节点着色相同，但是边着色不同，这是用于网络整体加密的零元不同，T_1 的零元是(7)-模混合优美图群中的 G_6，T_2 的零元是(7)-模混合优美图群中的 G_{10}。T_3 和 T_4 的边着色有着规律，T_3 的边着色为 G_1,G_2,G_3,G_4,G_5，不难看到，T_4 的边着色为 G_1,G_3,G_5,G_7,G_9。每个 $G_k(k\in[1,19])$ 可以产生数字串，例如，G_1 导出数字串

$$S_{1,i}=314\ 123\ 134\ 145\ 055\ 566 \qquad (1)$$

它由 18 个数字组成。图 2 中的 T_1 的节点 G_1 和节点 G_7 被标有 G_2 的边连接在一起，节点 G_1 导出的数字串 $S_{1,i}$ 与节点 G_7 导出的数字串 $S_{7,i}$ 通过标有 G_2 的边导出的数字串 $S_{2,i}$ 进行连接认证，使得节点 G_1 和节点 G_7 之间有通讯联通，认证是由 54 个数字组成。当网络整体的零元发生变化后，连接 2 个节点边着色也发生变化，边着色导出的数字串也发生变化，使得 2 个节点的通讯认证必须采用新的数字认证。

一般情形下，一个任意零元阿贝尔有限模可加图群中的图 G_k 导出 m_k 个数字构成的数字串，k 为整数。任意 2 个节点 G_i,G_j，通过 G_k 通讯认证需由 $m_i+m_j+m_k$ 个数字构成。因为涉及到图的同构，加之已经有数百种着色运用于实际[10,11]，所以由式(1)中的数字串 $S_{1,i}$ 找到图 1 中的着色图 G_1 是及其困难的。这说明用任意零元阿贝尔有限模可加图群进行网络整体加密的优势。

2　基本术语、定义

文中所考虑的图均为有限、无向、简单图。文中没有定义的术语和符号参考文献[12]。为叙述简便起见，用记号$[m,n]$表示集合$\{m,m+1,m+2,\cdots,n\}$，其中，m 和 n 均为整数，且满足 $m<n$；用记号$[s,t]^0$ 表示集合$\{s,s+2,s+4,\cdots,t\}$，其中，s 和 t 均为奇数。一个 (p,q) - 图 G 是指 $V(G)=p$ 和 $E(G)=q$。图 G 的一个从顶点集 $V(G)$(或边集 $E(G)$，或全集 $V(G)\cup E(G)$)到一个数集的单射 f 是指任何 2 个不同顶点 u，v(或 2 条边，或 2 个元素)的像不同，即 $f(u)\neq f(v)$，称 f 为 G 的一个标号(labelling)。以下顶点标号集合$\{f(u):u\in V(G)\}$简记为 $f(V(G))$，边标号集合$\{f(uv):uv\in E(G)\}$简记为 $f(E(G))$。

对于$(q+1)$-模混合优美图，其最小的顶点标号是负数，最大的顶点标号是正数。设图 G 有 $(q+1)$-模混合优美标号 $f:V(G)\to[-q,q]$，使得 $f(E(G))=\{f(uv)=|f(u)-f(v)|:uv(E(G)\}$

$(\{q+1-|f(u)-f(v)|:uv(E(G)\}=[1,q]$。

如果 G 中最小的顶点标号为 s，最大的顶点标号为 t，记 G 的标号 $f=f_m$，其中，$m=t+q+1$，$G=G_m$，那么对于 G 的每个拷贝 G_k，定义其$(q+1)$-模混合优美标号为：$f_k(x)=f_m(x)-(m-k)\ (mod q+1)$，其中 $x\in V(G)$，$k\in[1,3q+1]$。

定义 1[10,12]　对于给定的 (p,q)-图 G，如果存在一个单射 $f:V(G)\to[0,q]$，使得边标号集合 $f(E(G))=\{f(uv)=|f(u)-f(v)|:uv\in E(G)\}=[1,q]$，则称 f 是 G 的一个优美标号(graceful labelling)，也称 G 为优美图(graceful graph)。此外，若图 G 是具有顶点二部划分(X,Y)的二部图，且 f 满足 $\max\{f(x)|x\in X\}<\min\{f(y)|y\in Y\}$(简记为 $f(X)<f(Y)$)，则称 f 是 G 的一个集有序优美标号(set-ordered graceful labelling)。

定义 2　对于给定的 (p,q)-图 G，如果存在

一个单射$f:V(G)\to[-q,q]$，使得G的任何不同的2个顶点u，v满足$f(u)\neq f(v)$，且边标号集合$f(E(G))=\{f(uv)=|f(u)-f(v)|:uv(E(G)\}$

($\{q+1-|f(u)-f(v)|:uv(E(G)\}=[1,q]$，则称$f$是图$G$的一个$(q+1)$-模混合优美标号($(q+1)$-modular mixed graceful labelling)，也称G为$(q+1)$-模混合优美图($(q+1)$-modular mixed graceful graph)。特别地，若$f:V(G)\to[0,q]$，则称f是图G的一个$(q+1)$-模优美标号($(q+1)$-modular graceful labelling)；若$f:V(G)\to[-q,0]$，则称f是图G的一个$(q+1)$-模负优美标号($(q+1)$-modular negative graceful labelling)。

3 主要结果及证明

假设F是群，F'是它的非空子集且对于F中的加法运算封闭，如果F'本身对于F中这个加法运算是群，则称F'是F的子群，并且表示成$F'<F$[13]。此外，如果F是有限集合，则称F是有限群。F中所含的元素个数称为F的阶，记作$|F|$[13]。

已知，一个$(q+1)$-模混合优美图G拷贝可以得到$3q+1$个图。事实上，$(q+1)$-模混合优美图的顶点标号是在$[-q,q]$中取得，$(q+1)$-模优美图的顶点标号是在$[0,q]$中取得，$(q+1)$-模负优美图的顶点标号在$[-q,0]$中的取得。这些图做成一个集合，称此集合是由$(q+1)$-模混合优美图G生成的，记作$M_{ixg}(G)$。

任取一个固定的元$G_k\in M_{ixg}(G)$，对任意的2个元$G_i,G_j\in M_{ixg}(G)=\{G_k:k\in[1,3q+1]\}$，定义加法运算“$G_i\oplus_k G_j$”如下：

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

其中，$\lambda=i+j-k(\mathrm{mod}q+1)$，$x\in V(G)=V(G_i)=V(G_j)=V(G_k)$。

(1)若$[f_i(x)+f_j(x)-f_k(x)]<-q$，则$[f_i(x)+f_j(x)-f_k(x)]_{(\mathrm{mod}q+1)}=q+1+f_i(x)+f_j(x)-f_k(x)$；

(2)若$[f_i(x)+f_j(x)-f_k(x)]>q$，则$[f_i(x)+f_j(x)-f_k(x)]_{(\mathrm{mod}q+1)}=f_i(x)+f_j(x)-f_k(x)-(q+1)$；

(3)若不是上面(1)和(2)的情形，$[f_i(x)+f_j(x)-f_k(x)]_{(\mathrm{mod}q+1)}=f_i(x)+f_j(x)-f_k(x)$。

集合$M_{ixg}(G)$和加法运算构成一个任意零元阿贝尔有限模可加图群(见定理1的证明)，特记作$\{M_{ixg}(G),f;\oplus\}$。

定理1 设(p,q)-图G有$(q+1)$-模混合优美标号f。以下结论成立：

(1)G生成了$3q+1$个图，构成一个任意零元阿贝尔有限模可加图群$\{M_{ixg}(G),f;\oplus\}$。

(2)任意连续的$q+1+i$个图构成一个任意零元阿贝尔有限模可加图子群，且阶为$3q+1-i$的子群有$i+1$个，其中，$i\in[0,2q]$。

(3)G可以生成2个特殊的任意零元阿贝尔有限模可加图子群，其中，一个子群中的图都是$(q+1)$-模优美的，另一个子群中的图都是$(q+1)$-模负优美的。

证明 任取一个图$G_{k_0}\in M_{ixg}(G)$作为零元，对任意2个元$G_i,G_j\in M_{ixg}(G)$，定义加法运算$G_i\oplus_{k_0}G_j=G_\lambda$ ($\lambda=i+j-k_0(\mathrm{mod}q+1)\in[1,3q+1]$)如下：

$$[f_i(x)+f_j(x)-f_{k_0}(x)]_{(\mathrm{mod}q+1)}=f_m(x)-[m-(i+j-k_0)](\mathrm{mod}q+1)=f_\lambda(x)\quad(3)$$

其中，$\lambda=i+j-k_0(\mathrm{mod}q+1)$，$x\in V(G)=V(G_i)=V(G_j)=V(G_{k_0})$。

(1)首先证明$M_{ixg}(G)$是任意零元阿贝尔有限模可加图群。$G_i\oplus_{k_0}G_j\in M_{ixg}(G)$，假设$G_i\oplus_{k_0}G_j=G_\lambda$，$G_i\oplus_{k_0}G_j=G_\mu$，则有$\lambda=i+j-k_0(\mathrm{mod}q+1)=\mu$。

1)零元 因为$G_i\oplus_{k_0}G_{k_0}=G_i$，所以$G_{k_0}$是$M_{ixg}(G)$的零元。

2)逆元 因为$G_i\oplus_{k_0}G_{2k_0-i}=G_{k_0}$，所以$G_i\in M_{ixg}(G)$的逆元是$G_{2k_0-i}\in M_{ixg}(G)$。

3)结合律 因为$[G_i\oplus_{k_0}G_j]\oplus_{k_0}G_l=G_{i+j-k_0}\oplus_{k_0}G_l=G_{i+j+l-2k_0}$以及$G_i\oplus_{k_0}[G_j\oplus_{k_0}G_l]=G_i\oplus_{k_0}G_{j+l-k_0}=G_{i+j+l-2k_0}$，所以$[G_i\oplus_{k_0}G_j]\oplus_{k_0}G_l=G_i\oplus_{k_0}[G_j\oplus_{k_0}G_l]$。

综上，$M_{ixg}(G)$是一个任意零元阿贝尔有限模可加图群$\{M_{ixg}(G),f;\oplus\}$。而$G_i\oplus_{k_0}G_j=G_j\oplus_{k_0}G_i$，可知它又是交换群。

(2)$M_{ixg}(G)$中任取连续的$q+1+i$个图，构成集合H，可得H是$M_{ixg}(G)$的一个任意零元阿

贝尔有限模可加图子群，且阶为 $3q+1-i$ 的子群有 i+1 个，其中，$i\in[0,2q]$。

(3)显然，$M_{ixg}(G)$ 中的前 $q+1$ 个图都是($q+1$)-模负优美的，后 $q+1$ 个图都是($q+1$)-模优美的。它们构成的图群都是 $M_{ixg}(G)$ 的任意零元阿贝尔有限模可加图子群。

事实上，图 1 中的 19 个图就是按照图 3 中 G_k 的生成方式由 G 生成的，其中，前 7 个图是(7)-模负优美的，后 7 个图是(7)-模优美的，中间的图都是(7)-模混合优美的。

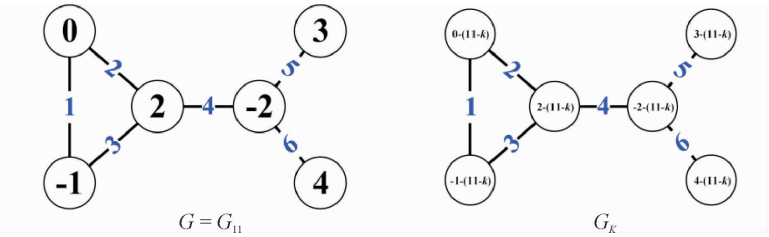

图 3　图 G 是(7)-模混合优美图，G 能生成 19 个(7)-模图 G_k，其中 $k\in[1,19]$

Fig. 3　Graph G is a (7)-modular mixed graceful graph, G can generate (7)-modular graphs with $k\in[1,19]$

定理 2　设 H 是 $M_{ixg}(G)$ 的一个非空子集，则 H 是 $M_{ixg}(G)$ 的任意零元阿贝尔有限模可加图子群的充分必要条件是对于任意 $H_i,H_j\in H$，给定 H_{k_0}，有 $H_i\oplus_{k_0}H_{2k_0-j}\in H$。

证明　充分性。由于 $H_i\in H$，给定 H_{k_0}，则有 $H_{k_0}=H_i\oplus_{k_0}H_{2k_0-i}\in H$，因此，对于任意的 $H_j\in H$，$H_{2k_0-j}=H_{k_0}\oplus_{k_0}H_{2k_0-j}\in H$。如果 $H_i,H_j\in H$，那么 $H_{2k_0-j}\in H$，所以 $H_i\oplus_{k_0}H_j=H_i\oplus_{k_0}H_{2k_0-(2k_0-j)}\in H$。因为 $M_{ixg}(G)$ 是任意零元阿贝尔有限模可加图群，从而 H 中的加法运算满足结合律，所以 H 是 $M_{ixg}(G)$ 的任意零元阿贝尔有限模可加图子群。

必要性。显然。

设连通图 G 有 ($q+1$)-模优美标号 $f:V(G)\to[0,q]$，使得

$$f(E(G))=\{f(uv)=|f(u)-f(v)|:uv(E(G)\}(\{q+1-|f(u)-f(v)|:uv(E(G)\}=[1,q]。$$

记图 G 的($q+1$)－模优美标号 $f=f_1,G=G_1$。则对于 G 的每个拷贝 G_k 定义($q+1$)－模优美标号 f_k 如下：

$$f_k(x)=f_1(x)+(k-1)(\mathrm{mod}q+1),$$

其中，$x\in V(G),k\in[1,q+1]$。

如果 G 有 ($q+1$)-模负优美标号号 $f:V(G)\to[-q,0]$，使得

$$f(E(G))=\{f(uv)=|f(u)-f(v)|:uv(E(G)\}(\{q+1-|f(u)-f(v)|:uv(E(G)\}=[1,q]。$$

记图 G 的($q+1$)-模负优美标号 $f=f_1,G=G_1$。则对于 G 的每个拷贝 G_k 定义($q+1$)-模负优美标号 f_k 如下：

$$f_k(x)=f_1(x)-(k-1)(\mathrm{mod}q+1),$$

其中，$x\in V(G),k\in[1,q+1]$。可得以下结论：

推论 1　设图 G 有($q+1$)-模(负)优美标号 f，则 G 能生成 $q+1$ 个($q+1$)-模(负)优美图，这些图构成一个阶为 $q+1$ 的任意零元阿贝尔有限模可加图群。

定义 ($q+1$)-模混合优美标号 f_k 的对偶标号为 $\bar{f}_k(x)=q+1-f_k(x)$，$x\in V(G)$。记 $\overline{M}_{ixg}(G)$ 是其相应的对偶图构成的集合，则有

推论 2　集合 $\overline{M}_{ixg}(G)$ 是任意零元阿贝尔有限模可加图群，且 $\overline{M}_{ixg}(G)$ 中的图都是 ($q+1$)-模混合优美的。

推论 3　($q+1$)-模(负)优美图的对偶图能生成 $q+1$ 个 ($q+1$)-模(负)优美图，这些图构成一个阶为 $q+1$ 的任意零元阿贝尔有限模可加图群。

设(p,q)－图 G 有 ($q+1$)-模优美标号 $f:V(G)\to[0,q]$，如果 G 按照 $f_l(uv)=f_1(uv)+(l-1)(\mathrm{mod}q+1)$ 能生成 $q+1$ 个图，其中，$uv\in E(G)=E(G_l)$，$G_1=G$，$G_{k+q+1}=G_k(\mathrm{mod}q+1)$，那么，边标号 $f:E(G_l)\to[0,q]$，称这 $q+1$ 个图是边模图，它们有着相同的顶点标号。这些图组成的集合记作 $G_g(G)=\{G_l:l\in[1,q+1]\}$。下面在 G_g

(G) 上定义加法运算“$G_i \oplus_k G_j$”，任意给定 $G_k \in G_g(G)$，则

$$[f_i(uv)+f_j(uv)-f_k(uv)]_{(\mathrm{mod}q+1)}=f_\lambda(uv),$$

其中，$\lambda=i+j-k(\mathrm{mod}q+1)$，$uv\in E(G)=E(G_i)=E(G_j)=E(G_k)$，

(1)若$[f_i(uv)+f_j(uv)-f_k(uv)]<-q$，则 $[f_i(uv)+f_j(uv)-f_k(uv)]_{(\mathrm{mod}q+1)}=q+1+f_i(uv)+f_j(uv)-f_k(uv)$；

(2)若$[f_i(uv)+f_j(uv)-f_k(uv)]>q$，则 $[f_i(uv)+f_j(uv)-f_k(uv)]_{(\mathrm{mod}q+1)}=f_i(uv)+f_j(uv)-f_k(uv)-(q+1)$；

(3)其他情况时，$[f_i(uv)+f_j(uv)-f_k(uv)]_{(\mathrm{mod}q+1)}=f_i(uv)+f_j(uv)-f_k(uv)$。

那么 $G_g(G)$ 是任意零元阿贝尔有限模可加图群，记作$\{G_g(G),f;\oplus\}$。

设(p,q)－图 G 有$(q+1)$-模优美标号 f，根据运算 $f_k(x)=f_1(x)+(k-1)(\mathrm{mod}q+1)$ 能生成 $q+1$ 个图，其中，$x\in V(G)=V(G_k)$，$G_1=G$，$k\in[1,q+1]$，这些图称为顶点模图。每个图 G_k 保持顶点不变，根据运算 $f_{k,l}(uv)=f_{k,1}(uv)+(l-1)(\mathrm{mod}q+1)$ 又可以生成 $q+1$ 个边模图，其中，$uv\in E(G_{k,l})(G_{k,l}\cong G_k)$，$l\in[1,q+1]$，$k\in[1,q+1]$。$G_{k,l}$的标号$f_{k,l}$定义如下：

$$f_{k,1}(x)=f_{1,1}(x)+(k-1)(\mathrm{mod}q+1),$$

$$f_{k,l}(uv)=f_{k,1}(uv)+(l-1)(\mathrm{mod}q+1),$$

其中，$x\in V(G)=V(G_{k,l})$，$uv\in E(G)=E(G_{k,l})$，$G_{1,1}=G$，$f_{1,1}=f$，$l,k\in[1,q+1]$。

事实上，边模图 $G_{k,1},G_{k,2},\cdots,G_{k,q+1}$构成了一个任意零元阿贝尔有限模可加图群，又 $k\in[1,q+1]$，因此，有 $q+1$ 个由边模图构成的任意零元阿贝尔有限模可加图群。顶点模图 $G_{1,l},G_{2,l},\cdots,G_{q+1,l}$构成了一个任意零元阿贝尔有限模可加图群，又 $l\in[1,q+1]$，因此，有 $q+1$ 个由顶点模图构成的任意零元阿贝尔有限模可加图群。故每个 $(q+1)$-模优美图 G 可以生成 $(q+1)^2$ 个图，记作 $G_{k,l}(k,l\in[1,q+1])$，这些图构成了 $2(q+1)$ 个任意零元阿贝尔有限模可加图群。

类似可得，每个$(q+1)$-模负优美图可以生成 $q+1$ 个顶点模图，每个顶点模图又可以生成 $q+1$ 个边模图，这些图构成了 $2(q+1)$ 个任意零元阿贝尔有限模可加图群(图4)。每个$(q+1)$-模混合优美图可以生成 $3q+1$ 个顶点模图，每个顶点模图又可以生成 $q+1$ 个边模图，从而得到 $4q+2$ 个任意零元阿贝尔有限模可加图群。

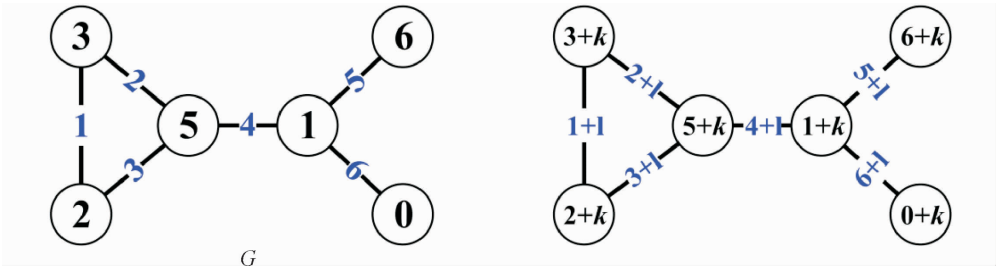

图4 (6,6)-图 G 是(7)-模优美图，G 可生成顶点模图和边模图，其中 $k,l\in[0,6]$

Fig. 4 The (6,6)-graph G is a (7)-modular graceful graph, G can generate vertex-modular graphs and edge-modular graphs, $k,l\in[0,6]$

4 结 语

给出了$(q+1)$-模混合优美标号，子群，有限群，边模图和顶点模图等概念。定理1给出了(p,q)－图 G 是$(q+1)$-模混合优美图时可以生成的任意零元阿贝尔有限模可加图群和图子群及它们的阶。定理2证明了 H 是 $M_{ixg}(G)$ 的一个非空子集，则 H 是 $M_{ixg}(G)$ 的任意零元阿贝尔有限模可加图子群的充分必要条件是对于任意 $H_i,H_j\in H$，给定 H_{k_0}，有 $H_i\oplus_{k_0}H_{2k_0-j}\in H$。最后提出了每个 $(q+1)$-模优美图 G 可以生成 $q+1$ 个顶点模图，每个顶点模图又可以生成 $q+1$ 个边模图，这些图构成了 $2(q+1)$ 个任意零元阿贝尔有限模可加图群。对于$(q+1)$-模负优美图和$(q+1)$-模混合优美图也可以得到类似的结果。在同态图群加密技

术中，若图的顶点或者边数较多，并结合已有的数百种着色就可以大大提高信息的安全性。这里讨论的都是有限图，对于无限群是否会有类似的结论？这是今后需要继续研究的课题。

参考文献:

[1] Suo X Y, Zhu Y, Owen G S. Graphical password: A survey[C]//Proceedings of Annual Computer Security Applications Conference. Tucson: IEEE, 2005: 463-472.

[2] Biddle R, Chiasson S, Van Oorschot P C. Graphical passwords: Learning from the first twelve years[J]. Acm Computing Surveys, 2012, 44(4): 1-41.

[3] Gao H C, Jia W, Ye F, et al. A survey on the use of graphical passwords in security[J]. Journal of Software, 2013, 8(7): 1678-1698.

[4] Wang H Y, Xu J, Yao B. Exploring new cryptographical construction of complex network data[C]//Proceedings of IEEE First International Conference on Data Science in Cyberspace. Piscataway: IEEE Computer Society, 2016: 155-160.

[5] Wang H Y, Xu J, Yao B. The key-models and their lockmodels for designing new labellings of networks[C]//Proceedings of 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference. Piscataway: IEEE, 2016: 565-568.

[6] Wang H Y, Yao B, Yao M. Generalized edge-magic total labellings of models from researching networks[J]. Information Sciences, 2014, 279:460-467.

[7] Yao B, Zhao M M, Zhang X H, et al. Topological coding and topological matrices toward network overall security[EB/OL](2019-09-15)[2021-09-30]. arXiv:1909.01587v2 [cs.IT] 15 Sep 2019.

[8] Bernstein D J, Buchmann J, Dahmen E. Post-quantum cryptography[M]. Berlin: Springer-Verlag, 2009.

[9] Yao B, Sun H, Zhao M M, et al. On coloring/labelling graphical groups for creating new graphical passwords[C]// Technology, Networking, Electronic & Automation Control Conference. Piscataway: IEEE, 2018.

[10] Zhou X Q, Yao B, Chen X E, et al. A proof to the odd-gracefulness of all lobsters[J]. Ars Combinatoria, 2012, 103: 13-18.

[11] Yao B, Liu X, Yao M. Connections between labellings of trees[J]. Bulletin of the Iranian Mathematical Society, 2017, 43(2):275-283.

[12] Bondy J A, Murty U S R. Graph Theory[M]. New York: Springer, 2008.

[13] 聂灵沼, 丁石孙. 代数学引论[M]. 北京: 高等教育出版社, 2000.

【责任编辑: 陈　钢】