

# 一类代数图的Cayley性

杨富元, 章超\*

贵州大学数学与统计学院, 贵州 贵阳

收稿日期: 2021年10月2日; 录用日期: 2021年10月23日; 发布日期: 2021年11月4日

---

## 摘要

设 $R$ 是一个有限环。本文基于代数图论的基本事实, 研究一类重要的图族的Cayley性质, 构造了代数图 $B\Gamma_n(R; f_2, \dots, f_n)$ 的一个无限子族, 其中每个图都是Cayley图, 在此基础上进一步考虑这类代数图的最大圈。

## 关键词

Cayley图, Hamilton图, 广义二面体群

---

# Cayley Properties of a Class of Algebraic Graphs

Fuyuan Yang, Chao Zhang\*

School of Mathematics and Statistics, Guizhou University, Guiyang Guizhou

Received: Oct. 2<sup>nd</sup>, 2021; accepted: Oct. 23<sup>rd</sup>, 2021; published: Nov. 4<sup>th</sup>, 2021

---

## Abstract

Let  $R$  be a finite ring. Based on the basic facts of algebraic graph theory, this paper studies the Cayley properties of an important family of graphs, and constructs an

---

\* 通讯作者 Email: zhangc@amss.ac.cn

infinite subfamily of algebraic graphs  $B\Gamma_n(R; f_2, \dots, f_n)$ , in which each graph is Cayley graph. On this basis, the maximal cycle of this kind of algebraic graph is further considered.

## Keywords

Cayley Graph, Hamiltonian Graph, Generalized Dihedral Group

Copyright © 2021 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## 1. 引言

本文中, 所有的图都是简单的无loop无向图。方程组定义的图最早是由Lazebnik提出的一类图, 最初用来解决极值图论中的问题 [1], Lazebnik和Woldar建立了这类图的一些重要的性质 [2], 包括正则性和双正则性。2002年, 文章 [3]讨论了一系列半对称的方程组定义的图并判定了它们是否连通, 这一系列图不是Cayley图并且函数不全是对称的。此外, 图 $B\Gamma_n(R; f_2, \dots, f_n)$ 的更多性质和问题可以在Lazebnik的文章 [4]中找到。在应用方面, Ustimenko和他的合作者将方程组定义的图应用于编码理论和密码学 [5]。

Cayley图 $\text{Cay}(G, S)$ 是以群 $G$ 中元素为顶点, 以子集 $S$ 定义边的一类图, 它与Hamilton图被广泛研究 [6]。Lazebnik 在文章 [2]的5.2节中给出了图的一些公开问题, 本文主要研究其中一个重要的公开问题, 即方程组定义图的哪些函数确定图 $B\Gamma_n(R; f_2, \dots, f_n)$ 是Cayley图或者是Hamilton图, 这是一个有趣的且有意义的问题, 本文构造了一系列方程组定义的Cayley图, 并且得到图 $B\Gamma_2(\mathbb{F}_q; p_1 l_1)$ 的最大圈。

## 2. 预备知识

设 $\Gamma$ 是一个图, 我们总是用 $V(\Gamma)$ 表示顶点集, 用 $E(\Gamma)$ 表示边集,  $x \sim y$ 表示顶点 $x$ 和 $y$ 相邻。

定义 1 [2] 设 $R$ 是有限环, 函数 $f_i : R^{2i-2} \rightarrow R$ 是任意给定的函数。我们定义二分图 $B\Gamma_n = B\Gamma_n(R; f_2, \dots, f_n)$ 。它的两个部集是分别等于 $R^n$ 的 $P_n$ 和 $L_n$ ,  $P_n$ 和 $L_n$ 中的元素分别称为点 $(p) = (p_1, \dots, p_n)$ 和线 $[l] = [l_1, \dots, l_n]$ 。我们定义顶点 $(p)$ 和 $[l]$ 邻接当且仅当下面 $n - 1$ 个条件成立:

$$\begin{aligned} p_2 + l_2 &= f_2(p_1, l_1), \\ p_3 + l_3 &= f_3(p_1, l_1, p_2, l_2), \\ &\dots \dots \\ p_n + l_n &= f_n(p_1, l_1, p_2, l_2, \dots, p_{n-1}, l_{n-1}). \end{aligned}$$

显然, 如果 $R$ 的阶是 $r$ , 那么图 $B\Gamma_n(R; f_2, \dots, f_n)$ 的顶点数是 $2r^n$ 且是 $r$ -正则的, 因为对于任何顶点 $a \in V(B\Gamma_n)$ 和 $x \in R$ , 存在唯一的顶点 $b \in V(B\Gamma_n)$ , 使得 $b$ 与 $a$ 相邻, 并且 $b$ 的第一个坐标是 $x$ .

定义 2 [7] 设 $G$ 是群,  $S$ 是 $G$ 的子集. 有向图 $\Gamma = \text{Cay}(G, S)$ 是Cayley图, 如果 $\text{Cay}(G, S)$ 的顶点集为 $G$ 且两个顶点 $x, y \in G$ 相邻, 当且仅当 $yx^{-1} \in S$ . 如果 $S^{-1} = S$ , 则该邻接关系是对称的, 此时Cayley图 $\text{Cay}(G, S)$ 等价一个无向图.

定义 3 设 $\Gamma$ 是一个图,  $H$ 是全自同构群 $\text{Aut}(\Gamma)$ 的一个子群. 如果 $H$ 在 $V(\Gamma)$ 是传递的且对于任意 $v \in V(\Gamma)$ 和 $\sigma \in H$ , 使得 $\sigma(v) = v$ , 那么 $\sigma$ 是恒等自同构, 则称 $H$ 在 $V(\Gamma)$ 上是正则的.

引理 1 [7] 图 $\Gamma$ 是群 $G$ 的Cayley图当且仅当 $\text{Aut}(\Gamma)$ 包含与 $G$ 同构的子群在 $V(\Gamma)$ 上是正则的.

定义 4 群 $G$ 是广义二面体群, 如果它有一个指数为2的交换子群 $A$ 和一个阶为2的元素 $\pi \in G \setminus A$ , 对任意 $g \in A$ , 使得 $\pi g \pi = g^{-1}$ . 在这种情况下, 我们记作 $G = \langle \pi, A \rangle$ .

定义 5 [8] 包含图 $\Gamma$ 的每个顶点的路径称为 $\Gamma$ 的Hamilton路径; 类似地,  $\Gamma$ 的Hamilton圈是包含 $\Gamma$ 的每个顶点的圈. 若图 $\Gamma$ 包含Hamilton圈, 则称图 $\Gamma$ 是Hamilton图或者是hamiltonian.

引理 2 [6] 设 $G$ 是有限群,  $S$ 是 $G$ 的子集. 此外满足,

- (1)  $S$ 是 $G$ 的生成集,
- (2)  $A$ 是 $G$ 的正规 $p$ -子群对某些素数 $p$ , 且
- (3)  $st^{-1} \in A$ 对所有的 $s, t \in S$ ,

那么 $\text{Cay}(G, S)$ 有一个Hamilton圈.

### 3. 主要结果

下面构造了一系列方程组定义的图 $B\Gamma_n(R; f_2, \dots, f_n)$ 都是Cayley图.

定理 1 若 $\{f_i \mid i = 2, \dots, n\}$ 满足以下情况, 则图 $B\Gamma_n(R; f_2, \dots, f_n)$ 是Cayley图.

- (1)  $f_i = \sum_{s=1}^{i-1} a_s(p_s + l_s)^{b_s} + c$ , 其中 $a_s, c \in R$ 是常数且 $b_s$ 是整数;
- (2)  $n = 2$ 且 $f_2 = cp_1l_1$ 对常数 $c \in R$ , 其中 $R$ 是交换环且 $2^{-1} \in R$ ;
- (3)  $f_n = \sum_{s=1}^{n-1} b_s(p_sl_s) + \sum_{s=1}^{n-1} c_s(p_s + l_s)^{d_s} + \sum_{s=1}^{n-1} e_s(p_sl_s)^{mp} + c$ 和 $f_i = \sum_{s=1}^{i-1} a_{i,s}(p_s + l_s)^{b_{i,s}} + d_i$ 对 $i = 2, \dots, n-1$ , 其中 $R$ 是特征 $p$ 且 $2^{-1} \in R$ 的交换环,  $mp$ 是奇数,  $a_{i,s}, b_s, c_s, e_s, c, d_i \in R$ ,  $b_{i,s}, d_s$ 是整数;
- (4)  $f_m = p_{m-1}l_{m-1}$ ,  $f_i = p_1 + l_1$ 对 $2 \leq i < m$ 和 $f_i = p_{m-1} + l_{m-1}$ 对 $m < i \leq n$ , 其中 $R$ 是交换环且 $2^{-1} \in R$ .

证明: 对于 $1 \leq k < i \leq n$ 和 $x \in R$ , 我们设下面映射 $\phi, \sigma_{i,x} : R^n \rightarrow R^n$ ,

$$\begin{aligned} \phi & : (p_1, \dots, p_n) \mapsto [p_1, \dots, p_n], \quad [l_1, \dots, l_n] \mapsto (l_1, \dots, l_n). \\ \sigma_{k,x} & : (p) \mapsto (p_1, \dots, p_k + x, p_{k+1} + b_{k+1,k}, \dots, p_i + b_{i,k}, \dots, p_n + b_{n,k}) \\ & [l] \mapsto [l_1, \dots, l_k - x, l_{k+1} + y_{k+1,k}, \dots, l_i + y_{i,k}, \dots, l_n + y_{n,k}]. \end{aligned}$$

对于(1), 定义  $b_{i,k} = 0, y_{i,k} = 0$ 。

对于(2), 令  $b_{2,1} = c(-p_1x - \frac{1}{2}x^2), y_{2,1} = c(l_1x - \frac{1}{2}x^2)$ 。

对于(3), 设  $b_{i,k} = y_{i,k} = 0$  对于  $k < i < n$ , 且

$$b_{n,k} = \sum_{s=1}^{n-1} b_s(-p_sx - \frac{1}{2}x^2) + \sum_{s=1}^{n-1} e_s(-(p_sx)^{mp} - \frac{1}{2}x^{2mp}),$$

$$y_{n,k} = \sum_{s=1}^{n-1} b_s(l_sx - \frac{1}{2}x^2) + \sum_{s=1}^{n-1} e_s((l_sx)^{mp} - \frac{1}{2}x^{2mp}).$$

对于(4), 令  $b_{i,k} = -p_1x - \frac{1}{2}x^2, y_{i,k} = l_1x - \frac{1}{2}x^2$  对  $1 \leq k < m < i \leq n$ ,  $b_{i,k} = y_{i,k} = 0$  对于其他情况。对于任意的  $x, y \in R$  我们不难验证映射  $\phi, \sigma_{i,x}$  是图  $B\Gamma_n$  的自同构且下面交换性成立:

$$\sigma_{k,x}\sigma_{j,y} = \sigma_{j,y}\sigma_{k,x}, \phi\sigma_{k,x}\phi = \sigma_{k,-x} = \sigma_{k,x}^{-1}.$$

设  $A = \langle \sigma_{k,x} \mid k = 1, \dots, n; x \in R \rangle$  和  $G = \langle \phi, A \rangle$ 。不难验证  $A$  是一个交换群。

此外,  $|\phi| = 2$ , 对  $1 \leq k \leq n$ , 集合  $\{\sigma_{k,x} \mid x \in R\}$  有  $r$  个元素。由于  $\sigma_{k,x}\sigma_{k,y} = \sigma_{k,x+y}$ , 则交换群  $A$  有  $r^n$  个自同构, 因此  $G = \langle \phi, A \rangle \leq \text{Aut}(B\Gamma_n)$  是广义二面体群且有  $2r^n$  个元素。我们可以验证  $G$  在  $V(B\Gamma_n)$  上是正则的。由引理1, 可知  $B\Gamma_n$  是广义二面体群上的Cayley图。

现在本文考虑图  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$  和图  $B\Gamma_2(\mathbb{F}_q; p_1+l_1)$  的最大圈, 文章 [3] 中的定理蕴含  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$  是连通的, 下面推论可知  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$  有一个Hamilton圈。

推论 1 设  $\mathbb{F}_q$  是一个有限域, 其中  $q = p^k$  且  $p$  是奇素数, 则图  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$  是Hamilton图, 图  $B\Gamma_2(\mathbb{F}_q; p_1+l_1)$  有一个长度为  $2q$  的圈。

证明: 由定理1可知图  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$  和  $B\Gamma_2(\mathbb{F}_q; p_1+l_1)$  是广义二面体群上的Cayley图  $\text{Cay}(G, S)$ 。对于图  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$ , 首先图  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$  是连通的, 由引理1中寻找生成集  $\langle S \rangle$ , 可知  $\phi\sigma_{2, \frac{x^2}{2}}\sigma_{1,x} \in \langle S \rangle$  由于  $(0) \sim [x, 0]$  对任意  $x \in \mathbb{F}_q$ 。令  $x = 0$ , 于是  $\phi \in \langle S \rangle$ ,  $\sigma_{2,x^2}, \sigma_{2,-x^2} \in \langle S \rangle$ , 我们有  $\sigma_{2, -\frac{x^2}{2}} \in \langle S \rangle$  和  $\sigma_{1,x} \in \langle S \rangle$ ,  $x^2 + y^2 = z$  有解  $(x, y)$  对任意的  $z \in \mathbb{F}_q$ , 于是  $\sigma_{2,z} \in \langle S \rangle$ , 可知图  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$  连通。可以验证  $\text{Cay}(G, S)$  满足引理2的条件, 于是图  $B\Gamma_2(\mathbb{F}_q; p_1l_1)$  有一个Hamilton圈。对于图  $B\Gamma_2(\mathbb{F}_q; p_1+l_1)$  同构  $\text{Cay}(G', S')$ , 由于  $(0) \sim [x, x]$ , 其连接集  $S'$  生成的集合  $\langle S' \rangle$  为  $\langle \phi\sigma_{1,x}\sigma_{2,x} \rangle$ , 由定理1中的交换性可知  $\langle \phi\sigma_{1,x}\sigma_{2,x} \rangle = \langle \phi, \sigma_{1,x}\sigma_{2,x} \rangle$  的阶是  $2q$ , 故图  $B\Gamma_2(\mathbb{F}_q; p_1+l_1)$  有一个长度为  $2q$  的圈。

## 基金项目

本文由贵州省科技厅项目(批准号: 黔科合基础[2020]1Y405)资助。

## 参考文献

- [1] Lazebnik, F. and Ustimenko, V.A. (1993) New Examples of Graphs without Small Cycles and of Large Size. *European Journal of Combinatorics*, **14**, 445-460.

<https://doi.org/10.1006/eujc.1993.1048>

- [2] Lazebnik, F. and Woldar, A.J. (2001) General Properties of Some Families of Graphs Defined by Systems of Equations. *Journal of Graph Theory*, **38**, 65-86.  
<https://doi.org/10.1002/jgt.1024>
- [3] Lazebnik, F. and Viglione, R. (2002) An Infinite Series of Regular Edge – But Not Vertex-Transitive Graphs. *Journal of Graph Theory*, **41**, 249-258. <https://doi.org/10.1002/jgt.10064>
- [4] Lazebnik, F., Sun, S. and Wang, Y. (2017) Some Families of Graphs, Hypergraphs and Digraphs Defined by Systems of Equations: A Survey. *Lecture Notes of Seminario Interdisciplinare di Matematica*, **14**, 105-142.
- [5] Klisowski, M. and Ustimenko, V. (2012) On the Comparison of Cryptographical Properties of Two Different Families of Graphs with Large Cycle Indicator. *Mathematics in Computer Science*, **6**, 181-198.
- [6] Morris, D.W. (2012) 2-Generated Cayley Digraphs on Nilpotent Groups Have Hamiltonian Paths. *Contributions to Discrete Mathematics*, **7**, 41-47.  
<https://doi.org/10.11575/cdm.v7i1.62051>
- [7] Biggs, N. (1992) Algebraic Graph Theory. Cambridge University Press, New York.
- [8] Bondy, J.A. and Murty, U.S.R. (1976) Graph Theory with Applications. Macmillan, London.