An application of the Combinatorial Nullstellensatz to a graph labelling problem

Dan Hefetz ∗ Annina Saluz † Huong T. T. Tran ‡

September 21, 2009

Abstract

An antimagic labelling of a graph $G$ with $m$ edges and $n$ vertices, is a bijection from the set of edges of $G$ to the set of integers $\{1, \ldots, m\}$, such that all $n$ vertex sums are pairwise distinct, where a vertex sum is the sum of labels of all edges incident with that vertex. A graph is called antimagic if it admits an antimagic labelling. In [7], Ringel has conjectured that every simple connected graph, other than $K_2$, is antimagic. In this paper, we prove a special case of this conjecture. Namely, we prove that if $G$ is a graph on $n = p^k$ vertices, where $p$ is an odd prime and $k$ is a positive integer, that admits a $C_p$-factor, then it is antimagic. The case $p = 3$ was proved in [8]. Our main tool is the Combinatorial Nullstellensatz (c.f. [1]).

1 Introduction

An antimagic labelling of a graph $G$ with $m$ edges and $n$ vertices, is a bijection from the set of edges of $G$ to the set of integers $\{1, 2, \ldots, m\}$, such that all $n$ vertex sums are pairwise distinct, where a vertex sum is the sum of labels of all edges incident with that vertex. A graph is called antimagic if it admits an antimagic labelling.

Note that labelling the edges of a graph $G = (V, E)$ with the labels $1, 2, \ldots, |E|$ is analogous to permuting the edges of $G$. It is therefore not surprising that properties of permutations play an important role in proving that certain graphs are antimagic.

In [7], Ringel has conjectured that every simple connected graph, other than $K_2$, is antimagic. Despite some effort in recent years, this conjecture is still open. However, some special cases of it are known to be true. Alon et al [2] proved that large dense graphs are antimagic; that is, there exists a universal constant $c > 0$ such that any graph with $n$ vertices and minimum degree at least $c \log n$ is antimagic. Hefetz [8] proved that any graph on $n = 3^k$ vertices that admits a triangle factor is antimagic. Cranston [4] proved that any regular bipartite graph, with minimum degree at least 2, is antimagic. Kaplan et al [9] proved that the members of a rich, though not very large, family of trees are antimagic. For more related results, the reader is referred to the survey [5].

In this paper, we generalize the aforementioned result of [8] as follows.

∗Institute of Theoretical Computer Science, ETH Zurich, CH-8092 Switzerland. Email: dan.hefetz@inf.ethz.ch
†Department of Mathematics, ETH Zurich, CH-8092 Switzerland. Email: asaluz@student.ethz.ch
‡Institute of Mathematics, 18 Hoang Quoc Viet, 10307 Hanoi, Vietnam. Email: ttthuong@math.ac.vn. This work was carried out while this author was undertaking an internship at ETH Zurich. The work of this author was partially sponsored by the Vietnamese National Foundation for Science and Technology Development.
Theorem 1.1 Let $G$ be a graph on $n = p^k$ vertices, where $p$ is an odd prime and $k$ is a positive integer. If $G$ admits a $C_p$-factor, then it is antimagic.

Note that we do not require $G$ to be connected. Moreover, it will follow from our proof that the same assertion holds, even if the range $\{1, 2, \ldots, m\}$ in the definition of an antimagic labelling is replaced with any set $S \subseteq \mathbb{R}$ of size $m$.

The proof of Theorem 1.1 uses similar ideas to the ones developed in [8], but is much more involved and contains new ideas (mostly in Section 4). The main reason for additional complications for the case $p > 3$ stems from the fact that the automorphism group of $C_3$ is “simpler” than the automorphism group of $C_p$, $p > 3$. Indeed, even the case $p = 5$ that was analyzed in [10] required some new ideas. We will elaborate on this matter later in the paper.

The main tool used in this paper is the following theorem of Alon [1].

**Theorem 1.2 (Combinatorial Nullstellensatz)** Let $\mathbb{F}$ be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. Suppose the degree $\deg(f)$ of $f$ is $\sum_{i=1}^n t_i$, where each $t_i$ is a non-negative integer, and suppose the coefficient of $\prod_{i=1}^n x_i^{t_i}$ in $f$ is nonzero. Then, if $S_1, \ldots, S_n$ are subsets of $\mathbb{F}$ with $|S_i| > t_i$, then there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ so that $f(s_1, \ldots, s_n) \neq 0$.

The rest of the paper is organized as follows. In Section 2 we introduce some terminology that will be used in the proof of Theorem 1.1. In Section 3 we prove Theorem 1.1. Many of the more technical details of the proof will be postponed to Section 4. Finally, we present some conclusions and open problems in Section 5.

## 2 Preliminaries

In this section, we introduce some notation and terminology that will be used throughout the paper.

An $\omega$-antimagic labelling of a graph $G = (V, E)$, where $\omega : V \rightarrow \mathbb{R}$ is a weight function on the set of vertices of $G$, is a bijection from the set of edges of $G$ to the set of integers $\{1, 2, \ldots, m\}$, such that all $n$ vertex sums are pairwise distinct, where a vertex sum is the sum of labels of all edges incident with that vertex and its initial weight under $\omega$. A graph is called $\omega$-antimagic, if it admits an $\omega$-antimagic labelling (thus antimagic is the same as 0-antimagic, where 0 stands for the zero function).

For a set $A \subseteq \mathbb{Z}$ and a positive integer $n$, let $A \mod n$ denote the set $\{a \mod n : a \in A\}$. Similarly, for a vector $(a_1, a_2, \ldots, a_t) \in \mathbb{Z}^t$ and a positive integer $n$, let $(a_1 \mod n, a_2 \mod n, \ldots, a_t \mod n)$ denote the vector $(a_1 \mod n, a_2 \mod n, \ldots, a_t \mod n)$. For a finite set $A \subseteq \mathbb{Z}$ and a positive integer $q$, we say that the elements of $A$ are distributed uniformly modulo $q$, if $|\{a \in A : a \equiv i \mod q\}| = |\{a \in A : a \equiv j \mod q\}|$, for every $0 \leq i < j \leq q - 1$.

For a positive integer $n$, let $S_n$ denote the group of all permutations $\sigma : \{0, 1, \ldots, n-1\} \rightarrow \{0, 1, \ldots, n-1\}$. The identity element of $S_n$ will be denoted by $id_n$. Often we will use vectors to denote permutations, that is, if $\sigma \in S_n$ is such that $\sigma(i) = a_i$ for every $0 \leq i \leq n - 1$, then we write $\sigma = (a_0, a_1, \ldots, a_{n-1})$. For $\pi = (\pi(0), \pi(1), \ldots, \pi(n-1)) \in S_n$ and for $i \in \mathbb{Z}$, let $\pi + i$ denote the permutation $\pi(0) + i, \pi(1) + i, \ldots, \pi(n-1) + i \mod n \in S_n$. Let $p$ and $r$ be positive integers, and let $n = pr$; for any vector $x \in \mathbb{Z}^n$, and for every $0 \leq i \leq r - 1$, the vector $(x[ip), x[ip+1), \ldots, x[ip+(p-1))]$ is called the $i$th $p$-cycle of $x$. 

2
For integers $p \geq 3$ and $r \geq 1$, let $C_p^r$ denote the graph on the vertex set \{0, 1, \ldots, n-1\}, where $n = pr$, that consists of $r$ pairwise disjoint $p$-cycles; we abbreviate $C_p^1$ to $C_p$. Note that $C_p^r$ is isomorphic to its line graph. Let $C_p^0, C_p^1, \ldots, C_p^{r-1}$ denote the cycles that constitute $C_p^r$. We will assume that, for every $0 \leq i \leq r-1$, the edges of $C_i$ are ordered according to the $i$th $p$-cycle of $id_n$. A labelling $\pi : E(C_p^i) \to \{0, 1, \ldots, n-1\}$, where $E(C_p^i)$ denotes the set of edges of $C_p^i$, will be viewed as an element of $S_n$. For a graph $G$, let $Aut(G)$ denote the automorphism group of $G$. Moreover, let $H_n = S_n/\text{Aut}(C_p^r)$. Let $[\pi]H_n$ denote an element (coset) of $H_n$; whenever there is no risk of confusion, we abbreviate $[\pi]H_n$ to $[\pi]$. For a permutation $\tau \in S_p$, let $\tau^r \in S_n$ denote the permutation $(\tau(0)r, \ldots, \tau(p-1)r, \tau(0)r+1, \ldots, \tau(0)r+(r-1), \ldots, \tau(p-1)r+(r-1))$; that is, $\tau^r \in S_n$ is the permutation whose $i$th $p$-cycle is $\tau(0)r+i, \tau(1)r+i, \ldots, \tau(p-1)r+i$ for every $0 \leq i \leq r-1$.

The following definition is central to this paper.

**Definition 2.1** Let $n$ be a positive integer and let $\sigma \in S_n$. The period of $\sigma$, denoted by $k_\sigma$, is the smallest positive integer such that $\sigma$ and $\sigma+k_\sigma$ are in the same coset of $H_n$.

Note that it follows immediately from the definition of $k_\pi$, that if $\sigma, \tau \in S_n$ are such that $[\sigma] = [\tau]$, then $k_\pi = k_\tau$.

### 3 Proof of Theorem 1.1

The proof of Theorem 1.1 is fairly long and involves many technical details regarding permutations. For the sake of readability and clarity of presentation we only sketch the proof in this section, thereby presenting most of the main ideas involved. All the gaps will be closed in the next section.

In the proof of Theorem 1.1, we will make use of the following lemma from [11]:

**Lemma 3.1** If $P(x_1, x_2, \ldots, x_n) \in \mathbb{R}[x_1, x_2, \ldots, x_n]$ is of degree $\leq s_1 + s_2 + \ldots + s_n$, where $n$ is a positive integer and $s_1, s_2, \ldots, s_n$ are non-negative integers, then

$$
\left( \frac{\partial}{\partial x_1} \right)^{s_1} \left( \frac{\partial}{\partial x_2} \right)^{s_2} \cdots \left( \frac{\partial}{\partial x_n} \right)^{s_n} P(x_1, x_2, \ldots, x_n) = \sum_{x_1=0}^{s_1} \cdots \sum_{x_n=0}^{s_n} (-1)^{x_1} \frac{s_1}{x_1} \cdots (-1)^{x_n} \frac{s_n}{x_n} P(x_1, x_2, \ldots, x_n).
$$

Let $G = (V, E')$, where $V = \{0, 1, \ldots, n-1\}$, $n = p^k$, be a graph that admits a $C_p$-factor $f = (V, E)$, and let $r = n/p$ denote the number of $p$-cycles in $f$; that is, $f \cong C_p^r$. Label the edges of $E' \setminus E$ arbitrarily using labels from the set $\{n+1, \ldots, |E'|\}$. For every vertex $v \in V$, denote its current vertex sum by $\omega(v)$. It suffices to prove that $f$ is $\omega$-antimagic. We will prove this to be true for any weight function $\omega$. Let $P_{\omega}(x_0, x_n-1) = \prod_{n-1 \geq i \geq j \geq 0}(x_i + x_j + \omega(i) - x_j - x_j - \omega(j))$, where $x_i, x_j$ represent the edges of $f$ that are incident with $i$ and $x_j, x_j$ represent the edges of $f$ that are incident with $j$. Let $Q_{\omega}(x_0, x_n-1) = \prod_{n-1 \geq i \geq j \geq 0}(x_i - x_j) P_{\omega}(x_0, x_n-1)$. Clearly $f$ is $\omega$-antimagic if and only if there exists a vector $(a_0, \ldots, a_{n-1}) \in \{1, \ldots, n\}^n$ such that $Q_{\omega}(a_0, \ldots, a_{n-1}) \neq 0$. By Theorem 1.2, in order to prove the existence of such a vector, it suffices to prove that there exists a monomial $c\prod_{i=0}^{n-1} x_i^{n-1}$, where $c \neq 0$, in the expansion
of $Q_\omega(x_0,\ldots,x_{n-1})$. The coefficient $c$ is equal to the coefficient of the same monomial in the expansion of $Q_0(x_0,\ldots,x_{n-1}) = \prod_{n-1 \geq j > 0} (x_i - x_j)P_0(x_0,\ldots,x_{n-1})$, where $P_0(x_0,\ldots,x_{n-1}) = \prod_{n-1 \geq j > 0} (x_{i1} + x_{i2} - x_{j1} - x_{j2})$. Using Lemma 3.1 we get

$$c[(n-1)!]^n = \left( \frac{\partial}{\partial x_0} \right)^{n-1} \left( \frac{\partial}{\partial x_1} \right)^{n-1} \cdots \left( \frac{\partial}{\partial x_{n-1}} \right)^{n-1} Q_0(x_0,x_1,\ldots,x_{n-1})$$

$$= \sum_{x_0=0}^{n-1} \cdots \sum_{x_{n-1}=0}^{n-1} (-1)^{x_0 + x_1 + \cdots + x_{n-1}} \prod_{i=0}^{n-1} \left( \frac{n-1}{x_i} \right) Q_0(x_0,x_1,\ldots,x_{n-1})$$

$$= \sum_{\sigma \in S_n} (-1)^{\sigma(0)+\sigma(1)+\cdots+\sigma(n-1)} \prod_{i=0}^{n-1} \left( \frac{n-1}{\sigma(i)} \right) Q_0(\sigma(0),\ldots,\sigma(n-1))$$

$$= (-1)^{(n)} \prod_{i=0}^{n-1} \left( \frac{n-1}{i} \right) \prod_{n-1 \geq j \geq 0} (i-j) \sum_{\sigma \in S_n} \text{sign}(\sigma)P_0(\sigma(0),\ldots,\sigma(n-1)).$$

It is therefore sufficient to prove that $\sum_{\sigma \in S_n} \text{sign}(\sigma)P_0(\sigma(0),\ldots,\sigma(n-1)) \neq 0$.

It follows by part (i) of Lemma 4.4 (see the definition of $a(\pi)$, preceding the statement of Lemma 4.3), that

$$\sum_{\sigma \in S_n} \text{sign}(\sigma)P_0(\sigma(0),\ldots,\sigma(n-1)) = (2p)^r \sum_{[\tau] \in H_n} \text{sign}(\tau)P_0(\tau(0),\ldots,\tau(n-1)),$$

where $\tau$ is any representative of its coset.

For any $\pi \in S_n$ let

$$S(\pi) := \frac{P_0(\pi(0),\ldots,\pi(n-1))}{\prod_{n-1 \geq j \geq 0} (i-j)} \text{ mod } p.$$ 

Note that $S(\pi)$ is well defined by part (i) of Lemma 4.3.

Hence, it suffices to prove that $\sum_{[\tau] \in H_n} \text{sign}(\tau)S(\tau) \neq 0 \text{ mod } p$.

**Remark:** Up to this point, the proof of Theorem 1.1 is essentially the same as the proof of Theorem 1.1 from [8]. However, proving that $\sum_{[\tau] \in H_n} \text{sign}(\tau)S(\tau) \neq 0 \text{ mod } p$ turns out to be significantly harder for general $p$ than for $p = 3$. We will elaborate on the differences between the two proofs in the next section.

Let $B_1 = \{[\pi] \in H_n : p \nmid k_\pi\}$, and let $B_2 = \{[\pi] \in H_n : k_\pi = 1\}$. Recall that if $[\pi] = [\sigma]$, then $k_\pi = k_\sigma$. It follows that $B_1$ and $B_2$ are well defined. Moreover, it follows by part (iv) of Lemma 4.1, that $B_2 = \{[\tau^r] \in H_n : \tau \in S_p, k_\tau = 1\}$. By part (iii) of Lemma 4.1, we conclude that $H_n = B_1 \cup B_2$, entailing

$$\sum_{[\tau] \in H_n} \text{sign}(\tau)S(\tau) = \sum_{[\tau] \in B_1} \text{sign}(\tau)S(\tau) + \sum_{[\tau] \in B_2} \text{sign}(\tau)S(\tau).$$

We will prove that $\sum_{[\tau] \in B_1} \text{sign}(\tau)S(\tau) = 0 \text{ mod } p$, but $\sum_{[\tau] \in B_2} \text{sign}(\tau)S(\tau) \neq 0 \text{ mod } p$.

Let $\pi \in S_n$ be such that $[\pi] \in B_1$. It follows from part (ii) of Lemma 4.1 that $[\pi + i] \in B_1$ for every $0 \leq i \leq k_\pi - 1$. Moreover, it follows from the definition of $k_\pi$ that $A_\pi := \{[\pi + i] : 0 \leq i \leq k_\pi - 1\} \subset B_1$.
is of size \( k \pi \). Furthermore \( \text{sign}(\sigma)S(\sigma) = \text{sign}(\tau)S(\tau) \) for every \( \sigma, \tau \in S_n \) such that \([\sigma], [\tau] \in A_\pi\), by part (ii) of Lemma 4.2, part (iv) of Lemma 4.3, and part (i) of Lemma 4.4. Hence,

\[
\sum_{[\tau] \in A_\pi} \text{sign}(\tau)S(\tau) = k_\pi \text{sign}(\pi)S(\pi) = 0 \mod p.
\]

Continuing this way with some permutation \( \sigma \in S_n \) such that \([\sigma] \in B_1 \setminus A_\pi\), we conclude that

\[
\sum_{[\tau] \in B_1} \text{sign}(\tau)S(\tau) = 0 \mod p.
\]

Similarly, it follows from part (v) of Lemma 4.1, part (v) of Lemma 4.3, and parts (i) and (ii) of Lemma 4.4, that

\[
\sum_{[\tau] \in B_2} \text{sign}(\tau)S(\tau) = \frac{p-1}{2} \cdot \text{sign}(id_p^r)S(id_p^r) \neq 0 \mod p.
\]

\[\square\]

4 Closing the gaps in the proof of Theorem 1.1

The first lemma we need describes some useful properties of the period of a permutation.

**Lemma 4.1** Let \( n = p^k \), where \( p \) is an odd prime and \( k \) is a positive integer, and let \( r = n/p \). For every \( \pi \in S_n \) it holds that

(i) \([\pi + i] = [\pi + k_\pi + i] \) for every \( i \in \mathbb{Z} \);

(ii) \( k_{\pi+i} = k_\pi \) for every \( i \in \mathbb{Z} \);

(iii) \( k_\pi | n \);

(iv) If \( k_\pi = 1 \), then \( \pi \) is in the same coset of \( H_n \) as \( \tau^r \) for some \( \tau \in S_p \), such that \( k_\tau = 1 \);

(v) If \( \tau \in S_p \) is of period 1, then \( \tau \) is in the same coset of \( H_p \) as \((0, t, 2t, \ldots, (p-1)t) \mod p \) for some \( 1 \leq t \leq \frac{p-1}{2} \). Moreover \([\!(0, t, 2t, \ldots, (p-1)t) \mod p\!] \neq [(0, s, 2s, \ldots, (p-1)s) \mod p]\) for every \( 1 \leq t < s \leq \frac{p-1}{2} \).

**Proof of Lemma 4.1:**

(i) Let \( i \in \mathbb{Z} \). Let \( \tau \) be an arbitrary permutation of \([\pi + i]\). It follows that \( \tau - i \in [\pi] = [\pi + k_\pi] \).

Hence, \( \tau \in [\pi + k_\pi + i] \), entailing \([\pi + i] \subseteq [\pi + k_\pi + i] \). The proof of the opposite inclusion is analogous.

(ii) Let \( i \in \mathbb{Z} \). Since \([\pi + i] = [(\pi + i) + k_\pi] \), by part (i) of this lemma, it follows from the definition of \( k_{\pi+i} \), that \( k_{\pi+i} \leq k_\pi \). Similarly, \([\pi] = [(\pi + i) - i] = [(\pi + i - i) + k_{\pi+i}] = [\pi + k_{\pi+i}] \) by part (i) of this lemma, entailing \( k_\pi \leq k_{\pi+i} \).
(iii) Let \( a \in \mathbb{N} \) and \( 0 \leq b < k_\pi \), be such that \( n = ak_\pi + b \). Then, by part (i) of this lemma, it follows that
\[
[\pi] = [\pi + n] = [\pi + ak_\pi + b] = [\pi + b]..
\]
By the minimality of \( k_\pi \) we conclude that \( b = 0 \); that is, \( k_\pi \mid n \) as claimed.

(iv) There exists some \( 0 \leq i \leq r - 1 \), such that the elements of the \( i \)th \( p \)-cycle of \( \pi \) are \( 0, a_1, a_2, \ldots, a_{p-1} \), where \( 0 < a_1, \ldots, a_{p-1} < n \). By the definition of \( k_\pi \), we have that \( \pi \) and \( \pi + k_\pi \) are in the same coset of \( H_n \). Therefore, \( \{dk_\pi, a_1 + dk_\pi, \ldots, a_{p-1} + dk_\pi\} \mod n \) is the set of elements of some \( p \)-cycle of \( \pi \) for every \( d \in \mathbb{N} \). Let \( q \) be the smallest positive integer such that
\[
\{0, a_1, \ldots, a_{p-1}\} = \{qk_\pi, a_1 + qk_\pi, \ldots, a_{p-1} + qk_\pi\} \mod n,
\]
that is, \( q \) is the smallest positive integer for which the elements of the \( i \)th \( p \)-cycle of \( \pi \) are the same as the elements of the \( i \)th \( p \)-cycle of \( \pi + qk_\pi \) (possibly in a different order). It follows from the definition of \( q \) that \( q \leq n \), and thus, in particular, \( q \) is finite. By definition, adding \( k_\pi \) to the elements of a \( p \)-cycle of \( \pi \) yields the labels of a \( p \)-cycle of \( \pi \). Since \( \pi \) consists of \( r \) \( p \)-cycles, we conclude that \( q \leq r \).

If \( qk_\pi \mod n = 0 \), then \( k_\pi \mod p = 0 \), as \( n = p^k \) and \( q \leq r < n \), which contradicts our assumption. Hence, \( qk_\pi \mod n = a_i \) for some \( 1 \leq i \leq p - 1 \); without loss of generality we can assume that \( i = 1 \). It follows that
\[
\{0, a_1, \ldots, a_{p-1}\} = \{a_1, 2a_1, a_2 + a_1, \ldots, a_{p-1} + a_1\} \mod n.
\]
Since \( 0 < a_1 < n \), it follows that \( 2a_1 \mod n \neq 0 \); hence, \( 2a_1 \mod n = a_i \) for some \( 2 \leq i \leq p - 1 \). Without loss of generality we can assume that \( i = 2 \). It follows that \( a_2 + a_1 \mod n = 3a_1 \mod n \). Continuing in this way, we conclude that
\[
\{0, a_1, a_2, \ldots, a_{p-1}\} = \{a_1, 2a_1, 3a_1, \ldots, pa_1\} \mod n.
\]
Since \( 0 < a_1 < n \), it follows that \( ia_1 \mod n \neq 0 \) for every \( 1 \leq i \leq p - 1 \); hence, \( pa_1 \mod n = 0 \) entailing \( a_1 = s \cdot r \), for some \( 1 \leq s \leq p - 1 \). We conclude that the \( i \)th \( p \)-cycle of \( \pi \) is \( (\tau(0)r, \tau(1)r, \ldots, \tau(p-1)r) \), for some \( \tau \in S_p \). Now, for every \( 1 \leq j \leq r - 1 \), add \( j = jk_\pi \) to the \( i \)th \( p \)-cycle of \( \pi \) to obtain some \( p \)-cycle of \( \pi \). It follows that \[ [\pi] = [\tau^r] \] as claimed. Finally, it is easy to see that \( \pi + r = g\pi \) for some \( g \in Aut(C_p^v) \), and that \( g \) maps the \( 0 \)th \( p \)-cycle of \( \pi \) to itself. It is clear that the restriction of \( g \) to the \( 0 \)th \( p \)-cycle of \( \pi \) induces a permutation \( g' \in S_p \) acting on \( \tau \); moreover \( g' \in Aut(C_p) \) since \( g \in Aut(C_p^v) \). Since \( g \) maps \( (\tau(0)r, \ldots, \tau(p-1)r) \) to \( (\tau(0)r + r, \ldots, \tau(p-1)r + r) \mod n = ((\tau(0) + 1 \mod p)r, \ldots, (\tau(p-1) + 1 \mod p)r) = ((\tau + 1)(0)r, \ldots, (\tau + 1)(p-1)r) \), it follows that \( g' \) maps \( \tau \) to \( \tau + 1 \). We conclude that \( k_\tau = 1 \) as claimed.

(v) Let \( \tau = (0, a_1, a_2, \ldots, a_{p-1}) \in S_p \). Since \( k_\tau = 1 \), adding \( a_1 \neq 0 \) to every element of \( \tau \), yields a permutation \( \sigma = \tau + a_1 \), such that \[ [\tau] = [\sigma] \]; let \( \sigma = g\tau \), where \( g \in Aut(C_p) \). Since \( a_1 \neq 0 \mod p \), \( g \) has no fixed point and is thus not a reflection. Hence, \( g \) must be a rotation, entailing \( a_i = ia_1 \mod p \), for every \( 2 \leq i \leq p - 1 \). It follows that \[ [\tau] = [(0, t, \ldots, (p-1)t) \mod p] \] for some \( 1 \leq t \leq p - 1 \). However, the reflection with a fixed point at \( 0 \), shows that \[ [(0, t, \ldots, (p-1)t) \mod p] = [(0, (p-t), \ldots, (p-1)(p-t)) \mod p] \]; hence, \[ [\tau] = [(0, t, \ldots, (p-1)t) \mod p] \] for some \( 1 \leq t \leq \frac{p-1}{2} \). Finally, if \( [(0, s, \ldots, (p-1)s) \mod p] = [(0, t, \ldots, (p-1)t) \mod p] \) for some \( 1 \leq t \leq \frac{p-1}{2} \) and \( 1 \leq s \leq p - 1 \), then either \( s \equiv t \mod p \) or \( s \equiv -t \mod p \).
Remark: It is instructive to compare Lemma 4.1 and its proof to Lemma 2.2 from [8]. The latter asserts that $k_\pi \equiv 0 \pmod{3}$ unless $\pi$ is in a unique special coset. Its proof is a part of the proof of part (iv) of the proof of Lemma 4.1. Unfortunately, when $p > 3$ there is more than one special coset. In parts (iv) and (v) of Lemma 4.1 we characterize all of these cosets; it turns out that there are exactly $\frac{p-1}{2}$ of them. A crucial step towards this characterization is part (iii) which asserts that if $k_\pi \neq 0 \pmod{p}$, then $k_\pi = 1$.

The following lemma determines some relations between the signs of certain permutations.

Lemma 4.2 Let $p$ and $r$ be positive odd integers, and let $n = pr$. Let $\pi \in S_n$, and let $\tau \in S_p$.

(i) $\text{sign}(\tau^r) = \text{sign}(\tau)\text{sign}(\text{id}_p^r)$;

(ii) $\text{sign}(\pi + i) = \text{sign}(\pi)$ for every $i \in \mathbb{Z}$.

Proof of Lemma 4.2:

(i) It is clear that $\text{sign}(\tau^r) = (\text{sign}(\tau))^r \cdot \text{sign}(\text{id}_p^r)$. The claim now follows since $r$ is odd.

(ii) Clearly it is sufficient to prove the assertion of the lemma for $i = 1$. Let $\pi = (\pi(0), \pi(1), \ldots, \pi(n-1))$; then $\pi + 1 = (\pi(0) + 1, \pi(1) + 1, \ldots, \pi(n-1) + 1) \pmod{n}$. Let $\{\sigma_l\}_{l=1}^l$ be a series of transpositions that transform $\pi$ into the identity permutation $\text{id}_n = (0, 1, \ldots, n-1)$. Applying the same series of transpositions to $\pi + 1$, yields the permutation $\tau = (1, 2, \ldots, n-1, 0)$. Transforming $\tau$ into the identity permutation requires $n-1$ transpositions. Hence,

$$\text{sign}(\pi + 1) = (-1)^{l+n-1} = (-1)^l = \text{sign}(\pi),$$

where the second equality follows since $n$ is odd.

Let $p$ and $r$ be positive odd integers, and let $n = pr$. Let $\pi$ be a bijection from the set of edges of $C_p^n$ to $\{0, 1, \ldots, n-1\}$. Let $v_\pi = (v_\pi(0), \ldots, v_\pi(n-1))$, where $v_\pi(i)$ denotes the vertex sum of $i$ under $\pi$, for every $0 \leq i \leq n-1$. Let

$$a(\pi) = \prod_{n-1 \geq i > j \geq 0} (v_\pi(i) - v_\pi(j)).$$

(1)

Splitting the product in (1) into differences of vertex sums from the same $p$-cycle of $\pi$, and differences of vertex sums from two distinct $p$-cycles of $\pi$, we write $a(\pi) = b(\pi)c(\pi)$, where

$$b(\pi) = \prod_{l=0}^{r-1} \prod_{p-1 \geq i > j \geq 0} (v_\pi(lp + i) - v_\pi(lp + j)),$$

(2)

and

$$c(\pi) = \prod_{r-1 \geq i > j \geq 0} \prod_{p-1 \geq a, b \geq 0} (v_\pi(ip + a) - v_\pi(jp + b)).$$

(3)
Note that, if \( r = 1 \), then \( b(\pi) = a(\pi) \) and \( c(\pi) = 1 \) (by definition).

Finally, note that

\[
S(\pi) = \frac{a(\pi)}{\prod_{n-1 \geq i > j \geq 0} (i - j)} \mod p.
\] (4)

The following lemma describes some useful properties of \( S(\pi) \).

**Lemma 4.3** Let \( n = p^k \), where \( p \) is an odd prime and \( k \) is a positive integer, and let \( r = n/p \). Let \( i \in \mathbb{Z} \), let \( \pi \in S_n \), and let \( \tau, \sigma \in S_p \).

(i) \( S(\pi) \) is well defined;

(ii) \( S(\pi) \neq 0 \) if and only if the elements of \( v_\pi \) are distributed uniformly modulo \( p^i \) for every \( 1 \leq t \leq k \);

(iii) Let \( \gamma(\tau) \) be the largest integer such that \( p^{\gamma(\tau)} \mid c(\tau^r) \), and let \( \hat{c}(\tau^r) = \frac{c(\tau^r)}{p^{\gamma(\tau)}} \); define \( \gamma(\sigma) \) and \( \hat{c}(\sigma^r) \) analogously. Then, \( \gamma(\pi) = \gamma(\sigma) \) and \( \hat{c}(\pi^r) \mod p = \hat{c}(\sigma^r) \mod p \);

(iv) \( S(\pi + i) = S(\pi) \);

(v) \( S(\sigma^r_i) \neq 0 \), where \( 1 \leq t \leq \frac{p-1}{2} \) and \( \sigma_t = (0, t, \ldots, (p-1)t) \mod p \).

**Proof of Lemma 4.3:**

(i) It is known that \( \prod_{n-1 \geq i > j \geq 0} (i - j) \mid \prod_{n-1 \geq i > j \geq 0} (a_i - a_j) \) for every \( (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}^n \) (see e.g. [6] and [3]). It follows that \( \frac{\prod_{n-1 \geq i > j \geq 0} (v_\pi(i) - v_\pi(j))}{\prod_{n-1 \geq i > j \geq 0} (i - j)} \) is an integer and thus \( S(\pi) \) is well defined.

(ii) This is implicit in the proof of (i) given in [6]. The main idea of this proof is to count the number of times \( p \) divides \( a(\pi) \) and to note that this is minimized if and only if the elements of \( v_\pi \) are distributed uniformly modulo \( p^i \) for every \( 1 \leq t \leq k \). The interested reader can also consult [10].

(iii) For \( r = 1 \) this follows trivially from the definition of \( c(\pi) \); assume that \( r \geq 2 \). For \( \tau \in S_p \) we have

\[
c(\tau^r) = \prod_{r-1 \geq i > j \geq 0, p-1 \geq a, b \geq 0} (v_{\tau r}(ip + a) - v_{\tau r}(jp + b))
= \prod_{r-1 \geq i > j \geq 0, p-1 \geq a, b \geq 0} (r (\tau(a) + \tau(a + 1 \mod p) - \tau(b) - \tau(b + 1 \mod p)) + 2(i - j))
\]

An analogous statement holds for \( \sigma \in S_p \).

Since \( r \) does not divide \( 2(i - j) \) for any \( r-1 \geq i > j \geq 0 \), it follows that for every integer \( x \), if \( p^l \mid (rx + 2(i - j)) \), then \( t \leq k - 2 \). Hence

\[
p^l \mid (r (\tau(a) + \tau(a + 1 \mod p) - \tau(b) - \tau(b + 1 \mod p)) + 2(i - j))
\]

if and only if

\[
p^l \mid (r (\sigma(a) + \sigma(a + 1 \mod p) - \sigma(b) - \sigma(b + 1 \mod p)) + 2(i - j))
\]

8
for every positive integer $t$, and for every $p - 1 \geq a, b \geq 0$. In particular $\gamma(\tau) = \gamma(\sigma)$.

Moreover, if

$$p^t \mid (r(\tau(a) + \tau(a + 1 \mod p) - \tau(b) - \tau(b + 1 \mod p)) + 2(i - j)),$$

then

$$(r(\sigma(a) + \sigma(a + 1 \mod p) - \sigma(b) - \sigma(b + 1 \mod p)) + 2(i - j)) / p^t \mod p = 2(i - j) / p^t \mod p.$$

It follows that $\tilde{c}(\sigma^\tau) \mod p = \tilde{c}(\sigma^\tau) \mod p$ as claimed.

(iv) Clearly, it suffices to prove this claim for $i = 1$. The permutation $\pi + 1$ is obtained by adding 1 to every element of $\pi$ and then subtracting $n$ from one of them, as the addition is modulo $n$. Since the elements of $\pi$ correspond to labels of edges of $C_\ell$, and since $C_\ell$ is 2-regular, $v_{\pi + 1}$ is obtained by adding 2 to every element of $v_\pi$, and then subtracting $n$ from two of them. Since $n \equiv 0 \mod p^t$ for every $1 \leq t \leq k$, it follows that, for every $1 \leq t \leq k$, the elements of $v_{\pi + 1}$ are distributed uniformly modulo $p^t$ if and only if the elements of $v_\pi$ are distributed uniformly modulo $p^t$. Hence, by part (ii) of this lemma, $S(\pi + 1) = 0$ if and only if $S(\pi) = 0$.

Assume then, that $S(\pi) \neq 0$ (and thus also $S(\pi + 1) \neq 0$). We claim that $n$ does not divide $v_\pi(i) - v_\pi(j)$ for any $n - 1 \geq i > j \geq 0$. Indeed, if $n \mid (v_\pi(i) - v_\pi(j))$ for some $n - 1 \geq i > j \geq 0$, then $v_\pi(i) \equiv v_\pi(j) \mod n$. However, this is impossible by part (ii) of this lemma, and by our assumption that $S(\pi) \neq 0$.

For every $0 \leq j < i \leq n - 1$, let $x_{ij}$ be the largest integer such that $p^{x_{ij}} \mid (i - j)$, let $y_{ij}$ be the largest integer such that $p^{y_{ij}} \mid (v_\pi(i) - v_\pi(j))$, and let $z_{ij}$ be the largest integer such that $p^{z_{ij}} \mid (v_{\pi + 1}(i) - v_{\pi + 1}(j))$. Moreover, let $a_{ij} = (i - j) / p^{x_{ij}}$, let $b_{ij} = (v_\pi(i) - v_\pi(j)) / p^{y_{ij}}$, and let $c_{ij} = (v_{\pi + 1}(i) - v_{\pi + 1}(j)) / p^{z_{ij}}$. Note that by definition we have $a_{ij} \neq 0 \mod p$, $b_{ij} \neq 0 \mod p$, and $c_{ij} \neq 0 \mod p$.

Since $n$ does not divide $v_\pi(i) - v_\pi(j)$ for any $n - 1 \geq i > j \geq 0$, it follows that $c_{ij} \equiv b_{ij} \mod p$ for every $n - 1 \geq i > j \geq 0$. Moreover, by part (ii) of this lemma, and by our assumption that $S(\pi) \neq 0$ and $S(\pi + 1) \neq 0$, it follows that

$$S(\pi + 1) = \prod_{n - 1 \geq i > j \geq 0} c_{ij} \mod p = \prod_{n - 1 \geq i > j \geq 0} (c_{ij} \mod p) \prod_{n - 1 \geq i > j \geq 0} (a_{ij} \mod p)^{-1} = \prod_{n - 1 \geq i > j \geq 0} (b_{ij} \mod p) \prod_{n - 1 \geq i > j \geq 0} (a_{ij} \mod p)^{-1} = \prod_{n - 1 \geq i > j \geq 0} b_{ij} \mod p \prod_{n - 1 \geq i > j \geq 0} a_{ij} = S(\pi).$$

Note that $(a_{ij} \mod p)^{-1}$ stands for the inverse of $a_{ij} \mod p$ in $\mathbb{GF}(p)$ (the field with $p$ elements).

(v) Let $1 \leq t \leq \frac{p - 1}{2}$. By part (ii) of this lemma, it suffices to prove that the elements of $v_{\sigma_i^t}$ are distributed uniformly modulo $p^t$ for every $1 \leq s \leq k$. We will prove this by induction on $k$. Clearly, this holds for $k = 1$ as $p$ and $t$ are coprime.
Let \( n' = p^{k+1} \) and, for every \( 0 \leq i \leq p - 1 \), let \( R_i = \{ 0 \leq j \leq n' - 1 : v_{\sigma^p_i}(j) \equiv i \mod p \} \). It is easy to see that \(|R_0| = |R_1| = \cdots = |R_{p-1}|\). Indeed, since \( k \geq 1 \), for every \( 0 \leq j \leq n - 1 \), the elements of the \( j \)th \( p \)-cycle of \( v_{\sigma^p_i} \) are all the same modulo \( p \). It is therefore sufficient to choose one element from each \( p \)-cycle and show that these elements are distributed uniformly modulo \( p \). We choose the elements of \( \{ i + (tn + i) : 0 \leq i \leq n - 1 \} = \{ nt + 2i : 0 \leq i \leq n - 1 \} \), which are distributed uniformly modulo \( p \), since \( p \) is odd.

For every \( 0 \leq i \leq p - 1 \), let

\[
A_i = \begin{cases} 
\{ \frac{m - i}{p} : m \in R_i \} & \text{if } i \text{ is even} \\
\{ \frac{m - (p+i)}{p} : m \in R_i \} & \text{if } i \text{ is odd}
\end{cases}
\]

Then \( A_0 = A_1 = \cdots = A_{p-1} \) is the set of vertex sums obtained from \( \sigma^p_i \).

By the induction hypothesis, we know that the elements of \( A_0 \) are distributed uniformly modulo \( p^{s-1} \), for every \( 2 \leq s \leq k + 1 \). Hence, it suffices to prove that, for every \( 2 \leq s \leq k + 1 \), the elements of \( R_0 \cup R_1 \cup \cdots \cup R_{p-1} = pA_0 + 2x := \{ a, p + 2x : a_i \in A_0, x \in \{ 0, 1, \ldots, p - 1 \} \} \) are distributed uniformly modulo \( p^s \). However, it is straightforward to verify that, for every \( a, b \in A_0, 0 \leq x, y \leq p - 1 \) and \( 2 \leq s \leq k + 1 \), it holds that \( ap + 2y \equiv bp + 2x \mod p^s \) if and only if \( x = y \) and \( a \equiv b \mod p^{s-1} \) (the interested reader can consult [10]). The assertion readily follows.

\[ \square \]

**Remark:** It is instructive to compare Lemma 4.3 and its proof to Lemma 2.3 as well as some other parts of the proof of Theorem 1.1 from [8]. Parts (iv) and (v) of the former are technically involved generalizations of the latter. Note that part (v) of Lemma 4.3 asserts that \( S(\sigma^p_t) \neq 0 \). For \( p = 3 \) this immediately entails that \( \sum_{\tau \in B_2} \text{sign}(\tau)S(\tau) \neq 0 \mod p \), as in this case \( B_2 = \{ [\sigma^3_t] \} \).

This is clearly not the case for general \( p \). Part (iii) of Lemma 4.3 is a first step towards proving this stronger claim.

Finally, we state and prove a lemma that combines some properties of \( \text{sign}(\pi) \) and \( S(\pi) \).

**Lemma 4.4** Let \( n = p^k \), where \( p \) is an odd prime and \( k \) is a positive integer, and let \( r = n/p \). Let \( \tau, \pi \in S_n \), and let \( 1 \leq t \leq \frac{p-1}{2} \).

(i) If \( [\tau] = [\pi] \), then \( \text{sign}(\tau)a(\tau) = \text{sign}(\pi)a(\pi) \);

(ii) \( \text{sign}(\sigma^r_t)S(\sigma^r_t) = \text{sign}(id^p_r)S(id^p_r) \), where \( \sigma_t = (0, t, \ldots, (p - 1)t) \mod p \).

**Proof of Lemma 4.4:**

(i) Since \( [\tau] = [\pi] \), there exists a permutation \( g \in \text{Aut}(C^n_p) \) such that \( \tau = g\pi \). We view \( g \) as a bijection from \( E(C^n_p) \) to \( \{ 0, 1, \ldots, n - 1 \} \). Hence, permuting the elements of \( \{ \pi(0), \pi(1), \ldots, \pi(n - 1) \} \) according to \( g \) (yielding \( \tau \)), induces a permutation of the elements of \( \{ v_0, v_1, \ldots, v_{n-1} \} \) (yielding \( v_\tau \)); denote this permutation by \( g_\tau \). Since \( p \) is odd, it follows that \( \text{sign}(g) = \text{sign}(g_\tau) \) (this is clear for a \( p \)-cycle of \( g \) which is a rotation, and holds for a \( p \)-cycle of \( g \) which is a reflection, if \( p \) is odd). Hence

\[
\text{sign}(\tau)a(\tau) = \text{sign}(g\pi)a(g\pi) = \text{sign}(g)\text{sign}(\pi)a(\pi) = \text{sign}(\pi)a(\pi),
\]

as claimed.

10
Lemma 4.4 and parts (ii) following the proof of Lemma 4.3) the case
∪
It follows from Lemma 4.4, parts (ii) and (iii) of Lemma 4.3, we have
c(σᵢ) = \( p^c \), \( c(σᵢ) \neq 0 \mod p \), and
c(idᵢ) = \( p^c(idᵢ) \), \( c(idᵢ) \neq 0 \mod p \), for some non-negative integer γ, and that \( c(σᵢ) \mod p = \hat{c}(idᵢ) \mod p \). One can show by a similar argument that \( b(σᵢ) = p^b(σᵢ) \), \( b(σᵢ) \neq 0 \mod p \), and \( b(idᵢ) = p^b(idᵢ) \), \( b(idᵢ) \neq 0 \mod p \), for some non-negative integer β, and that \( b(σᵢ) \mod p = \left(t^\frac{β}{2}\right) \left(b(idᵢ) \mod p \right) \). Recall also that \( S(σᵢ) \neq 0 \), by part (v) of Lemma 4.3.

For every \( n - 1 \geq i > j \geq 0 \), let \( a_{ij} = (i - j)/p^{x_{ij}} \), where \( x_{ij} \) denotes the largest integer such that \( p^{x_{ij}} \mid (i - j) \) (as in the proof of part (iv) of Lemma 4.3). It follows that

\[
S(σᵢ) = \frac{b(σᵢ)c(σᵢ)}{\prod_{n-1 \geq i > j \geq 0}(i - j) \mod p} = \frac{(b(σᵢ) \mod p)(c(σᵢ) \mod p)}{\prod_{n-1 \geq i > j \geq 0}(a_{ij} \mod p)} = \frac{(t^\frac{β}{2} \mod p)(b(idᵢ) \mod p)(c(idᵢ) \mod p)}{\prod_{n-1 \geq i > j \geq 0}(a_{ij} \mod p)} = \left(t^{\frac{p-1}{2}} \mod p\right) S(idᵢ).
\]

We claim that \( \text{sign}(σᵢ) \cdot \left(t^{\frac{p-1}{2}} \mod p\right) = 1 \). Indeed,

\[
\text{sign}(σᵢ) \left( \prod_{p-1 \geq i > j \geq 0} (i - j) \mod p \right) = \prod_{p-1 \geq i > j \geq 0} (σᵢ(i) - σᵢ(j)) \mod p
\]

\[
= \left(t^\frac{β}{2} \mod p\right) \left( \prod_{p-1 \geq i > j \geq 0} (i - j) \mod p \right),
\]

and thus \( \text{sign}(σᵢ) = t^\frac{β}{2} \mod p \). It follows that \( \text{sign}(σᵢ) \cdot \left(t^{\frac{p-1}{2}} \mod p\right) = t^{p-1} \mod p = 1 \).

Hence

\[
\text{sign}(σᵢ) S(σᵢ) = \text{sign}(σᵢ) \text{sign}(idᵢ) S(σᵢ)
\]

\[
= \text{sign}(idᵢ) S(idᵢ)
\]

where the first equality follows by part (i) of Lemma 4.2.

\[\square\]

Remark: It follows from Lemma 4.4, parts (iv) and (v) of Lemma 4.1, and part (v) of Lemma 4.3 that indeed \( \sum_{\{τ \in B_p\} \text{sign}(τ) S(τ) \neq 0 \mod p \). As was partially indicated previously (see the remark following the proof of Lemma 4.3) the case \( p = 3 \) is simpler in this respect. In fact, part (ii) of Lemma 4.4 and parts (iv) and (v) of Lemma 4.1 are not needed in this special case.
5 Concluding remarks and open problems

We have proved that if $G$ is a graph on $n = p^k$ vertices, where $p$ is an odd prime and $k$ is a positive integer, that admits a $C_p$-factor, then it is antimagic. This is a far reaching generalization of the main result of [8] and its proof is much more involved. A natural next step, would be to generalize our result to every odd integer $p$, or for graphs on $n = pr$ vertices, where $r$ is any odd integer. However, a new idea is needed, as some parts of our proof break down in these cases. For example, it is easy to see that, both part (v) of Lemma 4.3 and part (ii) of Lemma 4.4 do not hold for the graph $C_9$. Moreover, using the computer, we have verified that part (v) of Lemma 4.3 does not hold for $C_5^3$, and part (ii) of Lemma 4.4 does not hold for $C_5^3$.

Acknowledgments

We would like to thank the referees for their comments. They helped improving the presentation of this paper.

References


[10] A. Saluz, An application of the Combinatorial Nullstellensatz to a graph labelling problem, manuscript.