An Application of the Combinatorial Nullstellensatz to a Graph Labelling Problem

Bachelor Thesis

Annina Saluz

Department of Mathematics
ETH Zürich

Advisor: Dr. Dan Hefetz
Professor: Prof. Dr. Angelika Steger

May 28, 2008
Abstract

A graph $G = (V, E)$ is called antimagic if there exists a bijection from the set of edges to the integers $1, \ldots, |E|$ such that all $|V|$ vertex sums are pairwise distinct, where a vertex sum is the sum of labels of all edges incident with that vertex. According to Ringel’s Conjecture in [4], every simple connected graph, other than $K_2$, is antimagic. In [5], Hefetz proved that every graph on $n = 3^k$ vertices for some positive integer $k$, that admits a $K_3$-factor, is antimagic. The main tool used in his proof is the Combinatorial Nullstellensatz. We extend some parts of his proof to graphs on $n = p^k$ vertices that admit a $C_p$-factor for arbitrary odd primes $p$. We are not able to generalize all parts of the proof for all odd primes $p$, but we prove the case $p = 5$ completely.
1 Introduction

Combinatorial problems and in particular graph labelling problems can sometimes be solved by the use of algebraic techniques. In this thesis we apply the Combinatorial Nullstellensatz (CNSS) to a graph labelling problem. We first introduce some concepts that we are going to use.

As usual, let $G = (V, E)$ denote a graph on the vertex set $V$ and on the edge set $E$. The following definition was introduced in [4].

**Definition 1.1** (Antimagic) An antimagic labelling of a graph $G = (V, E)$ with $n$ vertices and $m$ edges is a bijection from the set of edges to the 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.

As is shown in Figure 1, the triangle $K_3$ is an antimagic graph, whereas a single edge $K_2$ is not.

![Figure 1](image-url)

The following generalization was introduced in [5].

**Definition 1.2** ($\omega$-antimagic) An $\omega$-antimagic labelling of a graph $G = (V, E)$, where $\omega : V \rightarrow \mathbb{N}$ is a weight function on the set of vertices, is a bijection from the set of edges to the integers $1, 2, \ldots, |E|$ such that all $|V|$ 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.

Note that antimagic is the same as $0$-antimagic, where the $0$ is the zero function $\omega \equiv 0$.

When dealing with regular graphs, adding a fixed constant to every edge “preserves antimagicness” (maps antimagic labellings to antimagic labellings and labelings which are not antimagic to labelings which are not antimagic). Hence, we can use the labels $0, 1, \ldots, m - 1$ instead of $1, 2, \ldots, m$ and do this whenever it is convenient.

To denote a labelling of a graph with $m$ edges we use permutations $\pi \in S_m$. We use two different notations for a permutation $\pi$. Whenever we use a permutation we choose the notation that is more convenient. If $\pi$ is of the form $\pi = (\pi(0), \pi(1), \ldots, \pi(m-1))$, then we interpret this permutation as a mapping such that $i \mapsto \pi(i)$ for every $0 \leq i \leq m-1$. If we use a notation without commas $\pi = (\pi(0)\pi(1)\ldots\pi(m-1))$, then we interpret this permutation as a mapping such that $\pi(i) \mapsto \pi(i+1)$ for every $0 \leq i \leq m-2$ and $\pi(m-1) \mapsto \pi(0)$.

Ringel conjectured in [4] that every simple connected graph, other than $K_2$, is...
antimagic. In [5], Hefetz proved that if $G$ is a graph on $n = 3^k$ vertices for some positive integer $k$ and if $G$ admits a $K_3$-factor, then $G$ is antimagic. In this paper we consider graphs that admit a $C_p$-factor for an odd prime $p$ and extend some parts of Hefetz’s proof. We are not able to extend all parts of his proof to arbitrary primes $p$ but we prove the statement for the case $p = 5$ completely. The main idea of the proof is the application of the Combinatorial Nullstellensatz (CNSS) that we discuss in Section 2.
2 Combinatorial Nullstellensatz

In this section we introduce the algebraic concepts that we are going to use. These results can be found in [1]. The first theorem we present here is a strengthening of a special case of Hilbert’s Nullstellensatz (HNSS) which asserts the following:

Theorem 2.1 (HNSS) If \( \mathbb{F} \) is an algebraically closed field, and \( f, g_1, \ldots, g_m \) are polynomials in the ring of polynomials \( \mathbb{F}[x_1, \ldots, x_n] \), where \( f \) vanishes over all common zeros of \( g_1, \ldots, g_m \), then there is an integer \( k \) and polynomials \( h_1, \ldots, h_m \) in \( \mathbb{F}[x_1, \ldots, x_n] \) so that

\[
f^k = \sum_{i=1}^{n} h_ig_i.
\]

In the special case \( m = n \), where each \( g_i \) is a univariate polynomial of the form \( \prod_{s \in S_i}(x_i - s) \), a stronger conclusion holds, as shown in Theorem 2.2.

Theorem 2.2 Let \( \mathbb{F} \) be an arbitrary field, and let \( f = f(x_1, \ldots, x_n) \) be a polynomial in \( \mathbb{F}[x_1, \ldots, x_n] \). Let \( S_1, \ldots, S_n \) be nonempty subsets of \( \mathbb{F} \) and define 
\[ g_i(x_i) = \prod_{s \in S_i}(x_i - s). \]

If \( f \) vanishes over all the common zeros of \( g_1, \ldots, g_n \) (that is; if \( f(s_1, \ldots, s_n) = 0 \) for all \( (s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n \)), then there are polynomials \( h_1, \ldots, h_n \in \mathbb{F}[x_1, \ldots, x_n] \) satisfying \( \deg(h_i) \leq \deg(f) - \deg(g_i) \) so that

\[
f = \sum_{i=1}^{n} h_ig_i.
\]

Moreover, if \( f, g_1, \ldots, g_n \) lie in \( R[x_1, \ldots, x_n] \) for some subring \( R \) of \( \mathbb{F} \) then there are polynomials \( h_i \in R[x_1, \ldots, x_n] \) as above.

To prove Theorem 2.2 we use the following lemma.

Lemma 2.1 Let \( P = P(x_1, \ldots, x_n) \) be a polynomial in \( n \) variables over an arbitrary field \( \mathbb{F} \). Suppose that the degree of \( P \) as a polynomial in \( x_i \) is at most \( t_i \) for \( 1 \leq i \leq n \), and let \( S_i \subset \mathbb{F} \) be a set of at least \( t_i + 1 \) distinct members of \( \mathbb{F} \). If \( P(x_1, \ldots, x_n) = 0 \) for all \( n \)-tuples \( (x_1, \ldots, x_n) \in S_1 \times S_2 \times \cdots \times S_n \), then \( P = 0 \).

Proof of Lemma 2.1. We prove the lemma by induction on \( n \). For \( n = 1 \), the assertion of the lemma holds because a nonzero polynomial of degree \( t_1 \) in one variable can have at most \( t_1 \) distinct zeros. We assume that the assertion of the lemma holds for \( n - 1 \), and prove it for \( n \) \((n \geq 2)\). Given a polynomial \( P = P(x_1, \ldots, x_n) \) and sets \( S_i \) satisfying the hypotheses of the lemma, let us write \( P \) as a polynomial in \( x_n \); that is,

\[
P = \sum_{i=1}^{t_n} P_i(x_1, \ldots, x_{n-1})x_n^{d_i},
\]

where each \( P_i \) is a polynomial with \( x_j \)-degree bounded by \( t_j \) for \( 1 \leq j \leq n - 1 \). For each fixed \((n - 1)\)-tuple

\[
(x_1, \ldots, x_{n-1}) \in S_1 \times S_2 \times \cdots \times S_{n-1},
\]

...
the polynomial in $x_n$ obtained from $P$ by substituting the values of $x_1, \ldots, x_{n-1}$ vanishes for all $x_n \in S_n$, and is therefore identically 0 by the assertion of the lemma in case $n = 1$. Thus $P_i(x_1, \ldots, x_{n-1}) = 0$ for all $(x_1, \ldots, x_{n-1})$ in $S_1 \times \cdots \times S_{n-1}$. Hence, by the induction hypothesis, $P_i \equiv 0$ for all $i$, implying that $P \equiv 0$. This completes the induction and the proof of Lemma 2.1.

□

**Proof of Theorem 2.2.** Define $t_i = |S_i| - 1$ for all $i$. By assumption,

$$f(x_1, \ldots, x_n) = 0$$

for every $n$-tuple $(x_1, \ldots, x_n) \in S_1 \times S_2 \times \cdots \times S_n$. (1)

For each $i$, $1 \leq i \leq n$, let

$$g_i(x_i) = \prod_{s \in S_i} (x_i - s) = x_i^{t_i+1} - \sum_{j=0}^{t_i} g_{ij}x_i^j.$$  

Observe that,

if $x_i \in S_i$ then $g_i(x_i) = 0$; that is, $x_i^{t_i+1} = \sum_{j=0}^{t_i} g_{ij}x_i^j$. (2)

Let $\bar{f}$ be the polynomial obtained by writing $f$ as a linear combination of monomials and replacing, repeatedly, each occurrence of $x_i^{t_i}$ ($1 \leq i \leq n$), where $f_i > t_i$, by a linear combination of smaller powers of $x_i$, using the relations (2). The resulting polynomial $\bar{f}$ is clearly of degree at most $t_i$ in $x_i$, for each $1 \leq i \leq n$. Replacing $x_i^{t_i+1}h_i$, for a polynomial $h_i$ satisfying $\deg(h_i) \leq \deg(f) - (t_i + 1)$, can be written as

$$x_i^{t_i+1}h_i - \left(x_i^{t_i+1} - \sum_{j=0}^{t_i} g_{ij}x_i^j\right) h_i = x_i^{t_i+1}h_i - g_i h_i,$$

Therefore we obtain $\bar{f}$ from $f$ by subtracting from it products of the form $h_ig_i$, where the degree of each polynomial $h_i \in \mathbb{F}[x_1, \ldots, x_n]$ does not exceed $\deg(f) - \deg(g_i)$ and where the coefficients of each $h_i$ are in the smallest ring containing all coefficients of $f$ and $g_1, \ldots, g_n$. That is, $\bar{f} = f - \sum_{i=1}^{n} g_i h_i$.

Moreover, $\bar{f}(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$, for all $(x_1, \ldots, x_n) \in S_1 \times \cdots \times S_n$, since the relations in (2) hold for these values of $x_1, \ldots, x_n$. Therefore, by (1), $\bar{f}(x_1, \ldots, x_n) = 0$ for every $n$-tuple $(x_1, \ldots, x_n) \in S_1 \times \cdots \times S_n$ and hence $\bar{f} \equiv 0$ by Lemma 2.1. This implies that $f = \sum_{i=1}^{n} h_i g_i$, and completes the proof.

□

As a consequence of Theorem 2.2 one can prove the following Theorem 2.3. Theorem 2.2 and Theorem 2.3 may be called **Combinatorial Nullstellensatz**. We use Theorem 2.3 if we refer to the CNSS.
Theorem 2.3 (CNSS) Let $F$ be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Suppose the degree $\deg(f)$ of $f$ is $\sum_{i=1}^{n} t_i$, where each $t_i$ is a nonnegative 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 $F$ with $|S_i| > t_i$, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ so that $f(s_1, \ldots, s_n) \neq 0$.

Proof of Theorem 2.3. We may assume that $|S_i| = t_i + 1$ for all $i$, because $|S_i| > t_i$ by assumption and if the assertion of Lemma 2.1 holds for $|S_i| = t_i + 1$ it will also hold if we have more options to choose $s_i \in S_i$, that is if $|S_i| > t_i + 1$. Assume for the sake of contradiction that $f(s_1, \ldots, s_n) = 0$ for all $n$-tuples $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$, and define $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$. By Theorem 2.2 there are polynomials $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ satisfying

$$\deg(h_j) \leq \deg(f) - \deg(g_j) = \sum_{i=1}^{n} t_i - \deg(g_j) \quad (3)$$

so that

$$f = \sum_{i=1}^{n} h_i g_i.$$

By assumption, the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ on the left hand side is nonzero, and hence so is the coefficient of this monomial on the right hand side. However, the degree of $h_i g_i = h_i \prod_{s \in S_i} (x_i - s)$ is at most $\deg(f)$ by (3). Moreover, by the definition of $g_i$, if there are any monomials of degree $\deg(f)$ in this product they are divisible by $x_i^{t_i+1}$. That is because a monomial of maximum degree in $h_i g_i$ is of the form $h_i \cdot x_i^{t_i+1}$, where $h_i$ is a monomial in $h_i$ of maximum degree in $x_i$. Since $\prod_{i=1}^{n} x_i^{t_i}$ is not divisible by $x_i^{t_i+1}$, it follows that its coefficient on the right hand side is zero, and this contradiction completes the proof of Theorem 2.3.

$\square$
3 A class of antimagic graphs

The theorem we present in this section characterises a class of antimagic graphs. As mentioned in the introduction, this result is proved in [5] for the case \( p = 3 \).

**Theorem 3.1** Let \( G \) be a graph on \( n = p^k \) vertices, where \( p \in \{3, 5\} \) and \( k \in \mathbb{N} \). If \( G \) admits a \( C_p \)-factor then it is antimagic.

Some parts of the proof of Theorem 3.1 will be more general and will apply to any odd prime \( p \). As we are not able to generalize all parts of Hefetz’s proof for arbitrary odd primes, some parts of the proof of Theorem 3.1 will be restricted to \( p = 3 \) or to \( p = 5 \).

**Proof of Theorem 3.1.** In order to prove Theorem 3.1 we need the following lemma from [6]:

**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 at most \( s_1 + s_2 + \cdots + s_n \), where \( n \) is a positive integer and \( s_1, s_2, \ldots, s_n \) are nonnegative integers, then

\[
\left( \frac{\partial}{\partial x_1} \right)^{s_1} \left( \frac{\partial}{\partial x_2} \right)^{s_2} \cdots \left( \frac{\partial}{\partial x_n} \right)^{s_n} P(x_1, x_2, \ldots, x_n) = \\
\sum_{x_1=0}^{s_1} \cdots \sum_{x_n=0}^{s_n} (-1)^{s_1+x_1} \binom{s_1}{x_1} \cdots (-1)^{s_n+x_n} \binom{s_n}{x_n} P(x_1, x_2, \ldots, x_n). \tag{4}
\]

**Proof of Lemma 3.1.** This is an extension of the following identity

\[
\sum_{x=0}^{s} (-1)^{x+s} \binom{s}{x} x^r = \begin{cases} 
0, & \text{if } 0 \leq r < s, \\
r!, & \text{if } r = s \geq 0,
\end{cases} \tag{5}
\]

which can be deduced by counting the surjective functions from a set \( A \) to a set \( B \), where \(|A| = r\) and \( B = \{y_1, y_2, \ldots, y_s\} \). Indeed, if \( 0 \leq r < s \) then there are no surjective functions from \( A \) to \( B \) and if \( r = s \) then there are \( r! \) surjective functions from \( A \) to \( B \). Let \( F \) be the set of all functions from \( A \) to \( B \) and for every \( 1 \leq i \leq s \), let \( A_i \) be the set of all functions \( f : A \to B \) in which \( y_i \) has no source. By the inclusion-exclusion principle it follows that the number of surjective functions from \( A \) to \( B \) is given by

\[
|A_1^c \cap A_2^c \cap \ldots \cap A_s^c| = |F| - |A_1 \cup A_2 \cup \ldots \cup A_s|
\]

\[
= s^r - \sum_{s-x=1}^{s} (-1)^{s-x+1} \sum_{|I|=s-x, i \in I} \prod_{i \in I} |A_i|
\]

\[
= s^r + \sum_{s-x=1}^{s} (-1)^{s-x} \binom{s}{s-x} x^r
\]

\[
= \sum_{x=0}^{s} (-1)^{s+x} \binom{s}{x} x^r.
\]

This completes the proof of identity (5).
Let us return to the proof of equation (4). It suffices to consider polynomials of the form $P(x_1, x_2, \ldots, x_n) = x_1^{r_1} \cdot x_2^{r_2} \cdots x_n^{r_n}$, where $\sum_{i=1}^{n} r_i \leq \sum_{i=1}^{n} s_i$. In the general case $P$ is the sum of monomials of the above form, where each monomial is multiplied by some scalar and the reduction to the aforementioned special case follows by the linearity of the differentiation operator. If $r_i < s_i$ for some $i$, then the left hand side of equation (4) is zero. If we split the sum on the right hand side into products of sums as follows

$$
\sum_{x_1=0}^{s_1} \cdots \sum_{x_n=0}^{s_n} (-1)^{s_1+x_1} \left( \begin{array}{c} s_1 \\ x_1 \end{array} \right) \cdots (-1)^{s_n+x_n} \left( \begin{array}{c} s_n \\ x_n \end{array} \right) x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n} = \\
\sum_{x_1=0}^{s_1} (-1)^{s_1+x_1} \left( \begin{array}{c} s_1 \\ x_1 \end{array} \right) x_1^{r_1} \cdots \sum_{x_n=0}^{s_n} (-1)^{s_n+x_n} \left( \begin{array}{c} s_n \\ x_n \end{array} \right) x_n^{r_n},
$$

we can deduce from equation (5) that the right hand side is zero, too. If $s_i = r_i$, for every $1 \leq i \leq n$, then we have

$$
\left( \frac{\partial}{\partial x_1} \right)^{r_1} \left( \frac{\partial}{\partial x_2} \right)^{r_2} \cdots \left( \frac{\partial}{\partial x_n} \right)^{r_n} (x_1^{r_1} \cdot x_2^{r_2} \cdots x_n^{r_n}) = r_1! \cdot r_2! \cdots r_n!
$$

for the left hand side of equation (4). We get the same result for the right hand side by splitting the sum into products as above and using identity (5), which completes the proof of Lemma 3.1.

Let now $G = (V, E')$, where $V = \{v_1, v_2, \ldots, v_n\}$, $n = p^k$, be a graph that admits a $C_p$-factor $f = (V, E)$, and let $r$ denote the number of $p$-cycles in $f$, that is $r = \frac{n}{p}$. Label the edges of $E' \setminus E$ arbitrarily using labels from the set $\{n+1, n+2, \ldots, |E'|\}$. For every vertex $v \in V$ denote its current vertex sum by $\omega(v)$. In Figure 2 we show an example of a graph on $n = 3^2$ vertices that admits a $C_3$-factor. The $C_3$-factor is black and the current vertex sums are colored in red.

![Figure 2: An example of a graph that admits a $C_3$-factor](image)

We will prove that $f$ is $\omega$-antimagic for any weight function $\omega$. As a consequence it will follow that $G$ is antimagic. Note that $f$ is 2-regular. Therefore, as mentioned in the introduction, we can use the labels 0, 1, $\ldots$, $n - 1$ instead of 1, 2, $\ldots$, $n$ for the edges of $f$.

For $f$ and $\omega$ we define the polynomials

$$
P_\omega(x_1, x_2, \ldots, x_n) := \prod_{n \geq i > j \geq 1} (x_{i_1} + x_{i_2} + \omega(v_i) - x_{j_1} - x_{j_2} - \omega(v_j)),
$$
where \( x_{i1}, x_{i2} \) represent the edges of \( f \) incident with \( v_i \) for every \( 1 \leq i \leq n \) and
\[
Q_\omega(x_1, x_2, \ldots, x_n) := \prod_{n \geq i > j \geq 1} (x_i - x_j) P_\omega(x_1, x_2, \ldots, x_n).
\]

If we look at the \( x_i \)'s as the labels of the edges in \( f \), then the factors in \( P_\omega \) represent the differences of the vertex sums in \( f \). The meaning of the \( x_{ij} \) is illustrated in the example of a \( C_3 \) in Figure 3, where we have \( x_{11} = x_1, x_{12} = x_2, x_{21} = x_1, x_{22} = x_3, x_{31} = x_2 \) and \( x_{32} = x_3 \).

![Figure 3](image)

If \( Q_\omega(x_1, \ldots, x_n) \) is not zero, then all the labels \( x_i \), \( 1 \leq i \leq n \), must be different because of the product \( \prod_{n \geq i > j \geq 1} (x_i - x_j) \). We also see that the polynomial \( P_\omega(x_1, \ldots, x_n) \) must not be zero in that case, which asserts that all the vertex sums are different. Therefore \( f \) is \( \omega \)-antimagic if and only if there exists \( a_1, a_2, \ldots, a_n \in \{1, 2, \ldots, n\} \) such that \( Q_\omega(a_1, a_2, \ldots, a_n) \neq 0 \). By the Combinatorial Nullstellensatz (Theorem 2.3) it suffices to prove that in the expansion of \( Q_\omega(x_1, x_2, \ldots, x_n) \) there exists a leading monomial \( c \prod_{i=1}^{n} x_i^{n-1} \) such that \( c \neq 0 \). Since \( c \) is a coefficient of a monomial of maximum degree it is equal to the coefficient of the same monomial in the expansion of \( Q_0(x_1, x_2, \ldots, x_n) \), where the 0 is the zero function \( \omega \equiv 0 \). Using Lemma 3.1 we find that
\[
c[(n-1)!]^n = \left( \frac{\partial}{\partial x_1} \right)^{n-1} \left( \frac{\partial}{\partial x_2} \right)^{n-1} \cdots \left( \frac{\partial}{\partial x_n} \right)^{n-1} Q_0(x_1, x_2, \ldots, x_n)
\]
\[
= \sum_{x_1=0}^{n-1} \cdots \sum_{x_n=0}^{n-1} (-1)^{x_1+x_2+\cdots+x_n} \binom{n-1}{x_1} \cdots \binom{n-1}{x_n} Q_0(x_1, x_2, \ldots, x_n)
\]
\[
= \sum_{\sigma \in S_n} \left( (-1)^{\sigma(0)+\sigma(1)+\cdots+\sigma(n-1)} \prod_{i=1}^{n-1} \binom{n-1}{\sigma(i)} \right.
\]
\[
\times Q_0(\sigma(0), \sigma(1), \ldots, \sigma(n-1))
\]
\[
= (-1)^{\binom{n}{2}} \left( \frac{n-1}{0} \right) \cdots \left( \frac{n-1}{n-1} \right) \prod_{n \geq i > j \geq 1} (i-j)
\]
\[
\times \sum_{\sigma \in S_n} \text{sign}(\sigma) P_0(\sigma(0), \sigma(1), \ldots, \sigma(n-1)).
\]

In order to prove that \( G \) is antimagic it is therefore sufficient to prove that
\[
\sum_{\sigma \in S_n} \text{sign}(\sigma) P_0(\sigma(0), \sigma(1), \ldots, \sigma(n-1)) \neq 0.
\]

(6)
Let $H = S_n / \text{Aut}(f)$, where $\text{Aut}(f)$ denotes the automorphism group of the line graph of $f$. Since the line graph of a cycle is isomorphic to the cycle itself it follows that $f$ is isomorphic to its line graph. Therefore the automorphism group of $f$ is isomorphic to $\text{Aut}(f)$, too. If $\pi \in \text{Aut}(f)$, then permuting the labels assigned to the edges of $E$ according to $\pi$ yields a permutation of the vertex sums of $V$, which we will denote by $\pi_v$. Let $\sigma, \tau \in S_n$ be in the same coset of $H$, that is $\sigma = g\tau$ for some $g \in \text{Aut}(f)$. Since $g$ is in $\text{Aut}(f)$, $g_v$ does not change the vertex sums of $f$ and therefore $\sigma$ and $\tau$ yield the same vertex sums.

For $g$ in $\text{Aut}(f)$ we have $\text{sign}(g) = \text{sign}(g_v)$. To see this, we first show that this equality holds for $g$ in the automorphism group of an odd cycle $C_{2n-1}$ for some integer $n \geq 2$. The automorphism group of $C_{2n-1}$ consists of $2n-1$ rotations and $2n-1$ reflections. If $g$ is a rotation, then $g_v$ represents the same rotation of the vertex sums and therefore we have $\text{sign}(g) = \text{sign}(g_v)$. If $g$ is a reflection, then it is the product of $n-1$ transpositions because every axis of a reflection goes through one edge and through one vertex. Therefore $2n-2$ vertex sums are reflected and one remains at its place and hence the permutation of the vertex sums also consists of $n-1$ transpositions. It follows that $\text{sign}(g) = \text{sign}(g_v)$ for every reflection $g$ in $\text{Aut}(C_{2n-1})$, too. By construction, $f$ is a disjoint union of cycles of odd length $p$. An element in the automorphism group of $f$ can consist of permutations inside the $p$-cycles and of switches of all labels of two $p$-cycles. If $g$ is a permutation that switches the labels of the edges of two $C_p$'s, then $g_v$ switches the vertex sums in the same way and we also have $\text{sign}(g) = \text{sign}(g_v)$. It follows that $\text{sign}(g) = \text{sign}(g_v)$ holds for every $g \in \text{Aut}(f)$. Hence, it follows that

$$
\text{sign}(\sigma)P_0(\sigma(0), \sigma(1), \ldots, \sigma(n-1))
= \text{sign}(g)\text{sign}(\sigma)\text{sign}(g_v)P_0(\sigma(0), \sigma(1), \ldots, \sigma(n-1))
= \text{sign}(\tau)P_0(\tau(0), \tau(1), \ldots, \tau(n-1)).
$$

Moreover, $|\text{Aut}(f)| = (2p)^r! r!$ because there are $p$ reflections and $p$ transpositions in each cycle such that we remain in the same coset and we have $r$ cycles, which we can also switch. Hence, we find that

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

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

Note that in this part it was essential that we work with cycles of odd length. In general, the equality $\text{sign}(g) = \text{sign}(g_v)$ does not hold for even cycles: Consider for example a labelled cycle of length 4 with the labelling given by the permutation $\sigma = (0, 2, 3, 1)$. We have 4 rotations and 4 reflections in the automorphism group of this graph $C_4$. For the rotations we again have $\text{sign}(g) = \text{sign}(g_v)$ because the vertex sums are permutated in the same way as the labels of the
edges. An example of a rotation $\pi_1$ in $\text{Aut}(C_4)$ is shown in Figure 4. For this permutation $\pi_1 = (0132)$ we find that $\pi_1 = (0132) = (01)(13)(32)$ and therefore $\text{sign}(\pi_1) = -1$. For the permutation of the vertex sums we have $(\pi_1)_v = (1452) = (14)(45)(52)$ so we also have $\text{sign}((\pi_1)_v) = -1$.

![Figure 4: $\pi_1 = (0132)$ an example of a rotation in $\text{Aut}(C_4)$](image)

For the other rotations we have $\pi_2 = (0132)^2 = (03)(12)$ and so we find that $\text{sign}(\pi_2) = 1 = \text{sign}((\pi_2)_v)$ and $\pi_3 = (0132)^3 = (0132)^{-1} = (0231)$ and therefore $\text{sign}(\pi_3) = -1 = \text{sign}((\pi_3)_v)$ and $\pi_4 = (0132)^4 = \text{id}$ which yields $\text{sign}(\pi_4) = 1 = \text{sign}((\pi_4)_v)$.

In contrast, we obtain different signs for $\pi$ and $\pi_v$ if $\pi$ is a reflection.

![Figure 5: $\pi_5 = (12)$ a reflection in $\text{Aut}(C_4)$](image)

For the reflection $\pi_5 = (12)$, the corresponding permutation of the vertex sums is $(\pi_5)_v = (12)(45)$ and therefore $\text{sign}(\pi_5) = -1 \neq 1 = \text{sign}((\pi_5)_v)$.

Another reflection in the automorphism group of $C_4$ is given by $\pi_6 = (03)$

![Figure 6: $\pi_6 = (03)$ a reflection in $\text{Aut}(C_4)$](image)

for which $(\pi_6)_v = (14)(25)$ and therefore $\text{sign}(\pi_6) = -1 \neq 1 = \text{sign}((\pi_6)_v)$.

For $\pi_7 = (01)(23)$ in $\text{Aut}(C_4)$ we have

![Figure 7: $\pi_7 = (01)(23)$ a reflection in $\text{Aut}(C_4)$](image)

so $(\pi_7)_v = (24)$ and thus $\text{sign}(\pi_7) = 1 \neq -1 = \text{sign}((\pi_7)_v)$.

And for the last reflection in the automorphism group of $C_4$ we have
Figure 8: $\pi_8 = (02)(13)$ a reflection in $Aut(C_4)$

$\pi_8 = (02)(13)$, which results in the following permutation of the vertex sums $(\pi_8)_v = (15)$. Hence, $sign(\pi_8) = 1 \neq -1 = sign((\pi_8)_v)$. Combining these results there are four permutations in the automorphism group of $C_4$ for which $sign(\pi) = sign(\pi_v)$ and four permutations for which $sign(\pi) \neq sign(\pi_v)$.

Hence,

$$
\sum_{\sigma \in S_4} sign(\sigma)P_0(\sigma(0),\ldots,\sigma(n-1))
= \sum_{[\sigma] \in \pi^{\#}_{Aut(C_4)}} \sum_{\tau \in [\sigma]} sign(\tau)P_0(\tau(0),\ldots,\tau(n-1))
= \sum_{[\sigma] \in \pi^{\#}_{Aut(C_4)}} \sum_{g \in Aut(C_4)} sign(g)sign(\sigma)\sum_{[\sigma] \in \pi^{\#}_{Aut(C_4)}} sign(g_v)P_0(\sigma(0),\ldots,\sigma(n-1))
= \sum_{[\sigma] \in \pi^{\#}_{Aut(C_4)}} (4-4)sign(\sigma)P_0(\sigma(0),\ldots,\sigma(n-1))
= 0.
$$

This result is general in the sense that the sum in (6) is always zero if $f$ is a factor of cycles of even length. This demonstrates that this proof does not work for cycles of even length because it is based on showing that exactly this sum is not zero.

Let $S(\pi) = P_0(\pi(0),\ldots,\pi(n-1)) \mod p$. By definition, $P_0(\pi(0),\ldots,\pi(n-1))$ is a product of differences of $n$ integers. Hence, $S(\pi)$ is well defined by the following lemma:

**Lemma 3.2** Let $n$ be a positive integer and let $P(a_1,a_2,\ldots,a_n)$ denote the product $\prod_{n \geq i > j \geq 1} (a_i - a_j)$. Then

$$
\prod_{n \geq i > j \geq 1} (i-j) \mid P(a_1,a_2,\ldots,a_n), \quad (8)
$$

for every $a_1,a_2,\ldots,a_n \in \mathbb{Z}$.

We give two different proofs of Lemma 3.2. In the first proof, which can be found in [3], one uses some properties of the distribution of different sets of integers amongst the residue classes modulo $p^l$, where $l$ is a positive integer. This is a useful idea, which we will use in other proofs as well.

**Proof of Lemma 3.2.** Let $\prod_{n \geq i > j \geq 1}(i-j) = p_1^{l_1}p_2^{l_2} \cdots p_m^{l_m}$ be the factorization...
in prime factors. We want to show that each prime or power of a prime in the factorization divides \( P(a_1, a_2, \ldots, a_n) \). To do this we consider arbitrary primes \( p \) and show that the number of times that \( p \) divides \( \prod_{i \geq j \geq 1} (i - j) \) is at most as large as the number of times that \( p \) divides \( P(a_1, a_2, \ldots, a_n) \).

If \( a_i = a_j \) for some \( i \neq j \) in \( \{1, 2, \ldots, n\} \), then \( P(a_1, a_2, \ldots, a_n) \) is zero and therefore divisible by \( \prod_{i \geq j \geq 1} (i - j) \). Thus, we assume that the \( a_i \)'s are \( n \) pairwise distinct integers.

Let us fix a prime \( p \). We want to compare the number of times that \( p \) divides \( \prod_{n \geq i > j \geq 1} (i - j) \) with the number of times that \( p \) divides \( P(a_1, a_2, \ldots, a_n) \). First calculate the remainders \( i \mod p, i \mod p^2, \ldots, i \mod p^k \), for every \( 1 \leq i \leq n \) and \( k \geq 1 \). If \( p \) divides a difference \( (i - j) \) for some \( 1 \leq j < i \leq n \), then \( i \) and \( j \) are in the same residue class modulo \( p \). Similarly, if \( p^l \), for some positive integer \( l \), divides a difference \( (i - j) \), then \( i \) and \( j \) are in the same residue class modulo \( p^l \). In addition, we know that there are \( \lfloor n/p^l \rfloor \) or \( \lceil n/p^l \rceil \) elements in each residue class if we calculate the remainders \( i \mod p^l, 1 \leq i \leq n \), that means that the numbers are distributed uniformly amongst the residue classes.

For every \( 0 \leq i \leq p^l - 1 \) and \( l \geq 1 \) let \( x_i^l \) denote the number of elements of \( \{1, 2, \ldots, n\} \) in the residue class with remainder \( i \mod p^l \). Since \( p^l \) divides a difference \( (i - j) \) if and only if \( i \) and \( j \) are in the same residue class modulo \( p^l \), it follows that the number of differences in the product \( \prod_{n \geq i > j \geq 1} (i - j) \) that are divisible by \( p^l \) is given by

\[
\left( \frac{x_i^l}{2} \right) + \left( \frac{x_i^l}{2} \right) + \cdots + \left( \frac{x_i^{p^l-1}}{2} \right).
\]

To count the number of times that \( p \) divides \( \prod_{n \geq i > j \geq 1} (i - j) \) we have to count exactly \( l \) times a difference \( (i - j) \) that is divisible by \( p^l \) but not by \( p^{l+1} \). It follows that the number of times that \( p \) divides the product \( \prod_{n \geq i > j \geq 1} (i - j) \) (assume that \( \left( \frac{x}{2} \right) = 0 \) if \( x < 2 \)) is

\[
q_1 := \sum_{k=1}^{\infty} \sum_{i=0}^{p^k-1} \left( \frac{x_i}{2} \right).
\]  

(9)

In the same way, we calculate the number of times that \( p \) divides \( P(a_1, \ldots, a_n) \). It is sufficient to show that this number is at least \( q_1 \). For every \( 0 \leq i \leq p^l - 1 \) and \( l \geq 1 \) we define \( y_i^l \) to be the number of elements of \( \{a_1, a_2, \ldots, a_n\} \) that are in the residue class with remainder \( i \mod p^l \). As above, it follows that the number of times that \( p \) divides \( P(a_1, \ldots, a_n) \) is

\[
q_2 := \sum_{k=1}^{\infty} \sum_{i=0}^{p^k-1} \left( \frac{y_i}{2} \right).
\]

It remains to show that \( q_1 \leq q_2 \), which is an immediate corollary of the following claim:

**Claim:** Let \( r, x_1, x_2, \ldots, x_r \) be nonnegative integers, then \( \left( \frac{x_1}{2} \right) + \left( \frac{x_2}{2} \right) + \cdots + \left( \frac{x_r}{2} \right) \), where \( x_1 + x_2 + \cdots + x_r = n \), attains its minimum when the \( x_i \)'s are almost
equal, that is \( x_i \in \{\lfloor n/r \rfloor, \lceil n/r \rceil \} \).

Proof of claim. For \( 1 \leq i \leq r \) let \( x_i \) be almost equal and let \( y_i \) be some arbitrary integers such that \( \sum_{i=1}^{r} x_i = \sum_{i=1}^{r} y_i = n \). We have to show that

\[
\left( \frac{x_1}{2} \right) + \left( \frac{x_2}{2} \right) + \cdots + \left( \frac{x_r}{2} \right) \leq \left( \frac{y_1}{2} \right) + \left( \frac{y_2}{2} \right) + \cdots + \left( \frac{y_r}{2} \right).
\]

Note that

\[
\sum_{i=1}^{r} \left( \frac{x_i}{2} \right) = \frac{1}{2} \sum_{i=1}^{r} (x_i^2 - x_i) = \frac{1}{2} \sum_{i=1}^{r} x_i^2 - \frac{1}{2} \sum_{i=1}^{r} x_i = \frac{1}{2} \sum_{i=1}^{r} x_i^2 - \frac{1}{2} n,
\]

and similarly

\[
\sum_{i=1}^{r} \left( \frac{y_i}{2} \right) = \frac{1}{2} \sum_{i=1}^{r} y_i^2 - \frac{1}{2} n.
\]

Hence, it suffices to prove that

\[
\sum_{i=1}^{r} x_i^2 \leq \sum_{i=1}^{r} y_i^2,
\]

that is that the sum of squares of the \( x_i \) is minimal under the condition that \( \sum_{i=1}^{r} x_i = n \). For \( 1 \leq i \leq r \) let \( z_i \) be such that \( \sum_{i=1}^{r} z_i = n \) and such that the sum of squares of the \( z_i \)'s is minimal. Assume for the sake of contradiction that the \( z_i \)'s are not almost equal. Then there exists an index \( 1 \leq i \leq r \) such that either \( z_i < \lfloor n/r \rfloor \) or \( z_i > \lceil n/r \rceil \). Assume without loss of generality that \( z_i < \lfloor n/r \rfloor \) (an analogous argument applies to the case \( z_i > \lceil n/r \rceil \)). Because the sum of the \( z_i \)'s is equal to \( n \), there must exist an index \( 1 \leq j \neq i \leq r \) such that \( z_j \geq \lceil n/r \rceil + 1 \). Let \( \tilde{z}_i = z_i + 1 \), \( \tilde{z}_j = z_j - 1 \) and \( \tilde{z}_k = z_k \) for every \( k \in \{1, \ldots, r\} \). Clearly, \( \sum_{i=1}^{r} \tilde{z}_i = n \) and we have

\[
\sum_{k=1}^{r} (z_k^2 - \tilde{z}_k^2) = z_i^2 - (z_i + 1)^2 + z_j^2 - (z_j - 1)^2
\]

\[
= 2(z_j - z_i - 1)
\]

\[
> 2(\lceil n/r \rceil + 1 - \lfloor n/r \rfloor - 1)
\]

\[
= 0.
\]

Hence, the sum of the squares of the \( z_i \) is not minimal, which is a contradiction to our assumption. This concludes the proof of the claim.

In (9) we now find that for every \( k \) the sum \( \sum_{i=0}^{k-1} \left( \frac{x_i^2}{2} \right) \) is minimal under the appropriate restrictions and therefore \( q_1 \leq q_2 \).

Recall that \( \prod_{n \geq 1 \geq j \geq 1}(i-j) = p_1^{r_1} \cdot p_2^{r_2} \cdots p_l^{r_l} \) is the factorization of the product

\[15]
in primes. We deduce that $p_i^{r_i} \mid P(a_1, a_2, \ldots, a_n)$ for every $1 \leq i \leq l$. Since the $p_i$’s are prime for every $1 \leq i \leq l$, we conclude that

$$
\prod_{n \geq 1, j \geq 1} (i - j) = \prod_{i \geq 1} p_i^{r_i} \mid P(a_1, a_2, \ldots, a_n).
$$

\[\square\]

We give an alternative proof of Lemma 3.2 from [2], using some properties of the Vandermonde determinant

$$
V(a_1, a_2, \ldots, a_n) := \begin{vmatrix}
1 & 1 & 1 & \cdots & 1 \\
a_1 & a_2 & a_3 & \cdots & a_n \\
a_1^2 & a_2^2 & a_3^2 & \cdots & a_n^2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \cdots & a_n^{n-1}
\end{vmatrix}.
$$

We prove by induction on $n$ that the value of the Vandermonde determinant $V(a_1, a_2, \ldots, a_n)$ is equal to $P(a_1, a_2, \ldots, a_n)$. For $n = 2$ the Vandermonde determinant is

$$
V(a_1, a_2) = \begin{vmatrix}
1 & 1 \\
a_1 & a_2
\end{vmatrix} = a_2 - a_1 = P(a_1, a_2),
$$

which proves the claim for $n = 2$. For $n > 2$ we apply elementary row and column operations. First, subtract the first column from all other columns to obtain

$$
V(a_1, a_2, \ldots, a_n) = \begin{vmatrix}
1 & 0 & \cdots & 0 \\
a_1 & a_2 - a_1 & \cdots & a_n - a_1 \\
\vdots & \vdots & \ddots & \vdots \\
a_1^{n-1} & a_2^{n-1} - a_1^{n-1} & \cdots & a_n^{n-1} - a_1^{n-1}
\end{vmatrix}.
$$

Expanding this determinant along the first row yields

$$
V(a_1, a_2, \ldots, a_n) = \begin{vmatrix}
a_2 - a_1 & \cdots & a_n - a_1 \\
a_2^2 - a_1^2 & \cdots & a_n^2 - a_1^2 \\
\vdots & \ddots & \vdots \\
a_2^{n-1} - a_1^{n-1} & \cdots & a_n^{n-1} - a_1^{n-1}
\end{vmatrix}.
$$

By the multilinearity of the determinant with regard to columns we can take the factor $a_k - a_1$ out of the $(k - 1)$-th column for every $2 \leq k \leq n$. Since $(a_k^1 - a_1^1) = (a_k - a_1) \sum_{i=0}^{l-1} a_k^{l-1-i} a_1^i$ it follows that

\[
V(a_1, a_2, \ldots, a_n) = \prod_{k=2}^{n} (a_k - a_1) \begin{vmatrix}
1 & 1 & \cdots & 1 \\
a_2 + a_1 & a_3 + a_1 & \cdots & a_n + a_1 \\
a_2^2 + a_1^2 + a_1 a_2 & a_3^2 + a_1 a_3 + a_1^2 & \cdots & a_n^2 + a_1 a_n + a_1^2 \\
\vdots & \vdots & \ddots & \vdots \\
\sum_{i=0}^{n-2} a_2^{n-2-i} a_1^i & \sum_{i=0}^{n-2} a_3^{n-2-i} a_1^i & \cdots & \sum_{i=0}^{n-2} a_n^{n-2-i} a_1^i
\end{vmatrix}.
\]

16
Subtracting from the $k$-th row $a_1$-times the $(k - 1)$-th row, for each $2 \leq k \leq n$, shows that

$$V(a_1, a_2, \ldots, a_n) = \prod_{k=2}^{n} (a_k - a_1) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_2 & a_3 & \cdots & a_n \\ a_2^2 & a_3^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_2^{n-2} & a_3^{n-2} & \cdots & a_n^{n-2} \end{vmatrix}.$$ 

By the induction hypothesis it follows that

$$V(a_1, a_2, \ldots, a_n) = \prod_{k=2}^{n} (a_k - a_1) \prod_{n \geq i > j \geq 1} (a_i - a_j) = \prod_{n \geq i > j \geq 1} (a_i - a_j) = P(a_1, a_2, \ldots, a_n),$$

which proves that $P(a_1, a_2, \ldots, a_n)$ is indeed the value of the Vandermonde determinant.

If $f_i$ are any monic polynomials of degree $i$ in one variable for every $1 \leq i \leq n - 1$, then

$$\begin{vmatrix} 1 & f_1(a_1) & f_1(a_2) & \cdots & f_1(a_n) \\ f_1(a_1) & 1 & f_1(a_2) & \cdots & f_1(a_n) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ f_{n-1}(a_1) & f_{n-1}(a_2) & \cdots & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ a_1 + \lambda_0 & a_2 + \lambda_0 & \cdots & a_n + \lambda_0 \\ a_1^2 + \lambda_1 a_1 + \lambda_0 & a_2^2 + \lambda_1 a_2 + \lambda_0 & \cdots & a_n^2 + \lambda_1 a_n + \lambda_0 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} + \sum_{i=0}^{n-2} \lambda_{i+1} a_1^i & a_2^{n-1} + \sum_{i=0}^{n-2} \lambda_{i+1} a_2^i & \cdots & a_n^{n-1} + \sum_{i=0}^{n-2} \lambda_{i+1} a_n^i \end{vmatrix},$$

for some coefficients $\lambda_i$ and $0 \leq i \leq n - 2$, $1 \leq j \leq n - 1$. Applying elementary row operations to this determinant (subtract from the $i$-th row $\lambda_{i-2}$-times the $(i - 1)$-th row and then $(\lambda_{i-3} - \lambda_{i-2} - 1)\lambda_{i-3}$-times the $(i - 2)$-th row and so on) shows that its value is equal to $V(a_1, a_2, \ldots, a_n)$ and therefore also equal to $P(a_1, a_2, \ldots, a_n)$. For every $1 \leq i \leq n - 1$ consider

$$f_i(a) = a(a - 1)(a - 2) \cdots (a - i + 1).$$

If $a \geq i$ we can write $f_i(a) = \frac{a^i}{(a-i)!} = \binom{a}{i} i!$. Since

$$P(a_1, a_2, \ldots, a_n) = P(a_1 + 1, a_2 + 1, \ldots, a_n + 1)$$

we can assume that each $a_i \geq n - 1$ and therefore $\binom{a_i}{i}$ is an integer for each $1 \leq j \leq n$ and $1 \leq i \leq n - 1$. Hence, each entry in the $i$-th row of this
determinant is divisible by \((i - 1)!\). By the multilinearity of the determinant with regard to rows it follows that

\[
P(a_1, a_2, \ldots, a_n) = \left(\prod_{i=1}^{n} (i - 1)!\right) \begin{vmatrix}
1 & 1 & \cdots & 1 \\
\binom{a_1}{1} & \binom{a_2}{1} & \cdots & \binom{a_n}{1} \\
\vdots & \vdots & \ddots & \vdots \\
\binom{a_1}{n-1} & \binom{a_2}{n-1} & \cdots & \binom{a_n}{n-1}
\end{vmatrix}
\]

and therefore \(P(a_1, a_2, \ldots, a_n)\) is divisible by \(\prod_{i=1}^{n} (i - 1)!\). Since

\[
\prod_{n \geq i > j \geq 1} (i - j) = \prod_{i=1}^{n} (i - 1)!
\]

we deduce that \(\prod_{n \geq i > j \geq 1} (i - j)\) divides \(P(a_1, a_2, \ldots, a_n)\).

With Lemma 3.2 it follows by (7) and by the definition of \(S(\tau)\) that in order to prove that \(\sum_{\sigma \in S_n} \text{sign}(\sigma) P_0(\sigma(0), \sigma(1), \ldots, \sigma(n-1)) \neq 0\), it suffices to show that

\[
\sum_{[\tau] \in H} \text{sign}(\tau) S(\tau) \mod p \neq 0.
\] (12)

For every \(\sigma \in S_n\), let \(k_\sigma\) be the smallest positive integer such that \(\sigma\) and \(\sigma + k_\sigma\), where \((\sigma + k_\sigma)(i) = (\sigma(i) + k_\sigma) \mod n\) for every \(0 \leq i \leq n - 1\), are in the same coset of \(H\). Note that \(\sigma\) and \(\sigma + n\) are the same entailing that \(1 \leq k_\sigma \leq n\) for every permutation \(\sigma \in S_n\).

Figure 9 and Figure 10 illustrate how \(k_\pi\) depends on the labelling of the edges. In the first example we consider a labelling given by \(\pi = (0, 3, 6, 1, 4, 7, 2, 5, 8)\). If we add 1 to every label of the edges, then we remain in the same coset and therefore \(k_\pi = 1\).

![Figure 9: An example of a labelling \(\pi\) such that \(k_\pi = 1\)](image)

In the second example we look at the labelling given by \(\sigma = (0, 1, 2, 3, 4, 5, 6, 7, 8)\) in which \(k_\sigma = 3\).

![Figure 10: An example of a labelling \(\sigma\) such that \(k_\sigma = 3\)](image)
Lemma 3.3 If \( k_π \mod p \neq 0 \) then \( π \) is in the same coset of \( H \) as one of the permutations 
\[
τ_0 \ldots τ_r = (τ_0(0)r, τ_0(1)(r), \ldots, τ_0(p-1)(r), τ_1(0)r + 1, \ldots, τ_1(p-1)r + 1, \ldots, τ_{r-1}(0)r + r - 1, \ldots, τ_{r-1}(p-1)r + r - 1, \ldots, τ_r(0)r),
\]
where \( τ_i ∈ S_{Aut(C_p)} \) for every \( 0 ≤ i ≤ r - 1 \). That is, the labels of a \( C_p \) are in 
\[
\{i, r+i, \ldots, (p-1)r+i\}
\]
for some \( 0 ≤ i ≤ r - 1 \).

Proof of Lemma 3.3. Let \( π ∈ S_n \). The edges of some \( p \)-cycle \( C \) are labelled
\( 0, a_1, a_2, \ldots, a_{p-1} \), where \( 0 < a_1, \ldots, a_{p-1} < n \). By the definition of \( k_π \), if we add \( k_π \mod n \) to every label of the edges of this \( p \)-cycle, then we remain in the same coset of \( H \). Therefore, \( \{mk_π, (a_1 + mk_π), \ldots, (a_{p-1} + mk_π)\} \mod n \) is the set of the labels of some \( p \)-cycle in \( f \) for every \( m ∈ N \). Let \( q \) be the smallest positive integer such that
\[
\{0, a_1, \ldots, a_{p-1}\} = \{qk_π, (a_1 + qk_π), \ldots, (a_{p-1} + qk_π)\} \mod n,
\]
that is, \( π \) and \( π + qk_π \) assign the same labels to \( C \) (possibly in a different order).
Since \( q \) is finite (clearly \( q ≤ n \)) and since we always get a \( C_p \) in \( f \) if we add \( k_π \)
and \( f \) consists of \( r \) cycles \( C_p \), it follows that \( q ≤ r \).
If \( qk_π \mod n = 0 \) then \( k_π \mod n = 0 \) because \( n = p^k \) and \( q ≤ r < n \). Otherwise
\( qk_π \mod n = a_i \) for some \( 1 ≤ i ≤ p - 1 \). Without loss of generality we can assume that
\( qk_π \mod n = a_1 \). We obtain 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 \( a_1 < n \) it follows that \( 2a_1 \mod n ≠ 0 \). Therefore \( 2a_1 \mod n = a_i \) for some
\( 2 ≤ i ≤ p - 1 \). Without loss of generality we can assume that \( i = 2 \). It follows that
\( a_2 + a_1 \mod n = 3a_1 \mod n \). Inductively, it follows that
\[
\{0, a_1, a_2, \ldots, a_{p-1}\} = \{a_1, 2a_1, 3a_1, \ldots, pa_1\} \mod n.
\]
Since \( a_1 < n \) it follows that \( i a_1 \mod n ≠ 0 \) for every \( 1 ≤ i ≤ p - 1 \) and
hence \( pa_1 \mod n = 0 \) and \( a_1 = r \). We conclude that the labels of this \( p \)-cycle
are \( \{0, r, 2r, \ldots, (p-1)r\} \). Now we add \( k_π \) to every label, by definition we get
another cycle. Since \( k_π \mod n ≠ 0 \) it follows that there exists an \( x ∈ N \) such that
\( xk_π \mod n = 1 \). Hence we get all cycles by adding \( k_π \mod n \) several times
to the labels. Therefore the labels of a cycle are \( \{l, r + l, \ldots, (p-1)r + l\} \) for
some \( 0 ≤ l ≤ r - 1 \).

Lemma 3.4 Let \( σ \) denote the permutation \( (0, r, 2r, \ldots, (p-1)r, 1, r + 1, 2r + 1, \ldots, (p-1)r + 1, \ldots, r - 1, 2r - 1, 3r - 1, \ldots, pr - 1) \), then \( S(σ) ≠ 0 \).

Proof of Lemma 3.4. It is sufficient to prove that for every \( 1 ≤ t ≤ k \) and
\( 0 ≤ i, j ≤ p^l - 1 \) the number of vertex sums from \( σ_v \) with remainder \( i \mod p^l \) is
equal to the number of those with remainder \( j \mod p^l \). This is because, as in
the proof of Lemma 3.2, we can reduce this problem to a problem of counting
the numbers of elements of \( \{1, 2, \ldots, n\} \) and of \( σ_v \) in the residue classes
to modulo \( p^l \), where \( p \) is a prime and \( l \) is a positive integer. Recall that the integers
\{1, 2, \ldots, n\} are distributed uniformly amongst the residue classes. If the vertex sums from \(\sigma_v\) were also distributed uniformly amongst the residue classes modulo \(p^l\) for every \(1 \leq l \leq k\), it would follow that \(p^l | P_{0}(\sigma(0), \sigma(1), \ldots, \sigma(n-1))\) if and only if \(p^l | \prod_{n \geq i > j \geq 1}(i - j)\) for all \(l \in \mathbb{N}\). This is because in that case we get the same number by counting the number of times that \(p\) divides \(P_{0}(\sigma(0), \sigma(1), \ldots, \sigma(n-1))\) and by counting the number of times that \(p\) divides \(\prod_{n \geq i > j \geq 1}(i - j)\). Therefore we would find that \(S(\sigma) \neq 0\). In order to prove that the vertex sums from \(\sigma_v\) are distributed uniformly amongst the residue classes mod \(p^l\), for every \(1 \leq t \leq k\), we proceed by induction on \(k\).

If \(k = 1\), then \(\sigma_v = (1, 3, 5, \ldots, p-2, p, p+2, \ldots, 2p-3, p-1)\) and so for every remainder \(j \in \{0, 1, 2, \ldots, p-1\}\) there is exactly one number \(i\) in \(\sigma_v\) such that \(i \mod p = j\). Let \(n = p^{k+1}\) and for every \(0 \leq i \leq p-1\) let \(R_i\) denote the set of vertex sums of \(\sigma_v\) with remainder \(i \mod p\). Then \(|R_0| = |R_1| = \cdots = |R_{p-1}|\).

To see this we group the elements of \(\sigma_v\) in such a way that we always have the \(p\) vertex sums of a \(p\)-cycle in a set. The set of the vertex sums of the \(i\)-th cycle is given by \((r+2(i-1), 3r+2(i-1), \ldots, (2p-3)r+2(i-1), (p-1)r+2(i-1))\). As \(r = p^k\) and \(k \geq 1\), all the elements in a \(p\)-cycle yield the same residue modulo \(p\). Thus, to prove that the vertex sums are distributed uniformly amongst the residue classes modulo \(p\), it suffices to look at the smallest vertex sum in each of the \(r\) cycles and show that all these vertex sums are distributed uniformly amongst the residue classes modulo \(p\). The smallest vertex sums are the following \(r = p^k\) numbers \(r, r+2, r+4, \ldots, r+(r-1), r+(r+1), \ldots, r+(r-2)\), which are distributed amongst the residue classes modulo \(p\) in the same way as the numbers \(0, 2, 4, \ldots, (r-1), 1, 3, 5, \ldots, r-2\) and therefore uniformly.

Next, we would like to use the induction hypothesis. To do this we have to transform the vertex sums of \(\sigma_v\) to the vertex sums one obtains for \(n = p^k\). Observe that one obtains the labels of the edges of the \((i+1)\)-st \(p\)-cycle by adding \(i\) to the labels of the edges of the first \(p\)-cycle. Therefore one adds \(2i\) to every vertex sum. To obtain the set of vertex sums if \(n = p^k\) we therefore have to subtract an even number from the current vertex sums and then divide by \(p\). For \(0 \leq i \leq p-1\) let \(A_i = \{\frac{m-i}{p} | m \in R_i\}\) if \(i\) is even and \(A_i = \{\frac{m-(p+i)}{p} | m \in R_i\}\) if \(i\) is odd. Then \(A_0 = A_1 = \cdots = A_{p-1}\) is the set of vertex sums obtained from \(\sigma\) if \(n = p^k\).

In Figure 11 we illustrate this for \(p = 5\) and \(r = 5\). The sets \(R_i\) are given by \(R_0 = \{5, 15, 20, 25, 35\}, R_1 = \{11, 21, 26, 31, 41\}, R_2 = \{7, 17, 22, 27, 37\}, R_3 = \{13, 23, 28, 33, 43\}\) and \(R_4 = \{9, 19, 24, 29, 39\}\). We obtain that \(A_0 = A_1 = \cdots = A_4 = \{1, 3, 4, 5, 7\}\), which is the set of vertex sums obtained from the labelling \((0, 1, 2, 3, 4)\) for 1-cycle.

![Figure 11](image)

By the induction hypothesis we know that for every integer \(2 \leq t \leq k + 1\) the number of elements of \(A_0\) with remainder \(i \mod p^{t-1}\) is equal to the number of
those with remainder \( j \mod p^{l-1} \) for all \( 0 \leq i, j \leq p^{l-1} - 1 \).

It remains to prove that the elements of

\[
pA_0 + x := \{ a_i + 2x \mid a_i \in A_0, x \in \{0,1,\ldots,p-1\}\}
\]

are distributed uniformly amongst the residue classes modulo \( p^l \). To prove this it is sufficient to show the following claim for two elements \( a_0, a_1 \) of \( A_0 \):

Claim: If \( a_1 \) and \( a_2 \) are in the same residue class modulo \( p^{l-1} \) then \( p a_1 + 2x \) and \( p a_2 + 2x \) are also in the same residue class modulo \( p^l \) for every \( x \leq p - 1 \). In contrast, \( p a_1 + 2x \) and \( p a_2 + 2y \) are in different residue classes if \( x \neq y \). If \( a_1 \mod p^{l-1} \neq a_2 \mod p^{l-1} \), then \( p a_1 + 2x \mod p^l \neq p a_2 + 2y \mod p^l \) for every \( x, y \leq p - 1 \).

This claim is sufficient because if we calculate the remainders modulo \( p^{l-1} \) of the \( p^k \) elements in \( A_0 \), then there are \( p^{l-1} \) residue classes each containing \( p^{k-l+1} \) elements, by the induction hypothesis. By calculating the set \( pA_0 + x \) every residue class contributes \( p \cdot p^{k-l+1} = p^{k-l+2} \) elements. Therefore there are \( p^{l-1} \cdot p^{k-l+2} = p^{k+1} \) elements in \( pA_0 + x \). If we show the above mentioned claim, it follows that two elements \( p a_1 + x, p a_2 + y \) of \( pA_0 + x \) are in the same residue class modulo \( p^l \) if and only if \( x = y \) and \( a_1 \) and \( a_2 \) are in the same residue class modulo \( p^{l-1} \). Thus, we have \( p^{k+1-l} \) elements in each residue class if we calculate the remainders of \( pA_0 + x \mod p^l \) and hence the \( p^{k+1} \) elements are distributed uniformly amongst the residue classes modulo \( p^l \).

Proof of claim: Let us first assume that \( a_1 \) and \( a_2 \) are in the same residue class modulo \( p^{l-1} \). Then we have \( a_1 = k_1 p^{l-1} + c \) and \( a_2 = k_2 p^{l-1} + c \) for some positive integers \( k_1, k_2 \) and \( 0 \leq c < p^{l-1} \). For every \( x \leq p - 1 \) it follows that

\[
(a_1 p + 2x) - (a_2 p + 2x) = (k_1 - k_2)p^l
\]

and therefore \( a_1 p + 2x \) and \( a_2 p + 2x \) are in the same residue class modulo \( p^l \). In contrast, we have

\[
(a_1 p + 2x) - (a_2 p + 2y) \mod p^l = (k_1 - k_2)p^l + 2(x - y) \mod p^l
\]

\[
= 2(x - y) \mod p^l
\]

\[
\neq 0
\]

for \( x \neq y \) since \( 0 \neq 2(x - y) < 2p < p^l \). Therefore \( a_1 p + 2x \) and \( a_2 p + 2y \) are not in the same residue class modulo \( p^l \).

Next, let us assume that \( a_1 \) and \( a_2 \) are in different residue classes modulo \( p^{l-1} \), that is \( a_1 = k_1 p^{l-1} + r \) and \( a_2 = k_2 p^{l-1} + s \) for some positive integers \( k_1, k_2 \) and without loss of generality we can assume that \( 0 \leq s < r \leq p^{l-1} - 1 \). It follows that

\[
(a_1 p + 2x) - (a_2 p + 2y) \mod p^l = (k_1 - k_2)p^l + (r - s)p + 2(x - y) \mod p^l
\]

\[
= (r - s)p + 2(x - y).
\]

If \( r - s \leq p^{l-1} - 2 \) then

\[
0 \neq (r - s)p + 2(x - y) \leq p^l - 2p + 2(p - 1) < p^l
\]

21
and therefore \( a_1p + 2x \) and \( a_2p + 2y \) are not in the same residue class modulo \( p^t \) for all possible \( x \) and \( y \). If \( r - s = p^{t-1} - 1 \) then

\[
(r - s)p + 2(x - y) \mod p^t = p^t - p + 2(x - y) \mod p^t \neq 0
\]
since \( p \) is odd. Thus \( a_1p + 2x \) and \( a_2p + 2y \) are not in the same residue class modulo \( p^t \). This finishes the proof of the claim.

As explained above, it follows that the number of elements in \( R_0 \cup \ldots \cup R_{p-1} = pA_0 + x \) with remainder \( i \mod p^t \) is equal to the number of elements with remainder \( j \mod p^t \) for every \( 1 \leq t \leq k + 1 \) and for all \( 0 \leq i, j \leq p^t - 1 \), which completes the proof of Lemma 3.4.

\[ \square \]

With the following lemma we can finish the proof of Theorem 3.1 for the case \( p = 3 \).

**Lemma 3.5** For every \( \pi \in S_n \) and for every \( l \in \mathbb{Z} \) we have \( S(\pi + l) = S(\pi) \) and \( \text{sign}(\pi + l) = \text{sign}(\pi) \).

**Proof of Lemma 3.5.** Clearly, it is sufficient to prove the statement for \( l = 1 \). For technical reasons we consider \( S(\pi + 1) \) and \( S(\pi - 1) \). Observe that \( \pi + 1 \) is obtained from \( \pi \) by adding 1 to every element of \( \pi \) and then subtracting \( n \) from one of them because the addition is modulo \( n \). Since the elements of \( \pi \) correspond to labels of edges, and because \( f \) is a 2-regular graph, \( (\pi + 1)_e \) is obtained from \( \pi_e \) by adding 2 to every element and then subtracting \( n \) from two of them. Similarly, \( \pi - 1 \) is obtained from \( \pi \) by subtracting 1 from every element of \( \pi \) and adding \( n \) to one of them. It follows that \( (\pi - 1)_e \) is obtained from \( \pi_e \) by subtracting 2 from every element of \( \pi_e \) and then adding \( n \) to two of them. Since \( n \mod p^t = 0 \) for every \( 1 \leq t \leq k \), this does not change the number of elements of \( \pi_e \) in the residue classes modulo \( p^t \) for every \( 1 \leq t \leq k \). Therefore, in every residue class modulo \( p^t \), for every \( 1 \leq t \leq k \), the number of elements from \( \pi_e \) is equal to the number of elements from \( (\pi + 1)_e \). It follows that the number of times that \( p \) divides \( P_0(\pi(0), \ldots, \pi(n - 1)) \) is equal to the number of times that \( p \) divides \( P_0((\pi \pm 1)(0), \ldots, (\pi \pm 1)(n - 1)) \). Let us first consider the case in which \( S(\pi) = 0 \). Then the number of times that \( p \) divides \( \prod_{n \geq i > j \geq 1} (i - j) \) is smaller than the number of times that \( p \) divides \( P_0(\pi(0), \ldots, \pi(n - 1)) \). Hence, the number of times that \( p \) divides \( \prod_{n \geq i > j \geq 1} (i - j) \) is smaller than the number of times that \( p \) divides \( P_0((\pi \pm 1)(0), \ldots, (\pi \pm 1)(n - 1)) \). It follows that \( S(\pi \pm 1) = 0 \), too. Using the same argument it follows that if \( S(\pi \pm 1) = 0 \), then \( S(\pi) = 0 \) and \( S(\pi \mp 1) = 0 \). Hence, we can assume that \( S(\pi) \neq 0 \) and \( S(\pi \pm 1) \neq 0 \). Clearly, adding 2 to every vertex sum does not affect \( S(\pi) \) since \( \prod (a_i - a_j) = \prod (a_i + 2 - (a_j + 2)) \). Therefore it is sufficient to show that \( S(\pi) \) does not change if we subtract \( n \) from one vertex sum in \( \pi_e \). If

\[
S(\pi) = \frac{\prod_{n \geq i > j \geq 1} (a_i - a_j)}{\prod_{n \geq i > j \geq 1} (i - j)} \mod p
\]
let $b_1 = a_1 - n$ and $b_i = a_i$ for $2 \leq i \leq n$ (for convenience we choose $b_1 = a_1 - n$, a similar argument applies if we choose $b_1 = a_i - n$ for some $i > 1$). If we write

$$\frac{\prod_{n \geq i > j \geq 1} (b_i - b_j)}{\prod_{n \geq i > j \geq 1} (i - j)} \mod p$$

$$= \frac{\prod_{n \geq i > j \geq 2} (a_i - a_j) \prod_{n \geq i \geq 2} (a_i - a_1 + n)}{\prod_{n \geq i > j \geq 1} (i - j)} \mod p$$

$$= \sum_{i=0}^{n-1} T_i(a_1, \ldots, a_n) \cdot n^i \mod p$$

$$= S(\pi) + p \sum_{i=1}^{n-1} p^{ki-1} T_i(a_1, \ldots, a_n) \mod p,$$

where

$$T_0(a_1, \ldots, a_n) = \prod_{n \geq i > j \geq 1} (a_i - a_j),$$

entailing that $T_0(a_1, \ldots, a_n) \mod p = S(\pi)$ and where

$$T_i(a_1, \ldots, a_n) = \prod_{n \geq i > j \geq 1} (a_i - a_j) \sum_{I \subseteq \{2, \ldots, n\}, \#I = i} \frac{1}{\prod_{l \in I} (a_i - a_1)},$$

if $i \geq 1$. From Lemma 3.2 we know that $\prod_{n \geq i > j \geq 1} (a_i - a_j)$ is an integer. We do the calculation of the term $p \sum_{i=1}^{n-1} p^{ki-1} T_i(a_1, \ldots, a_n)$ in (13) in $\mathbb{Z}_p$ where we can use the fact that $a \equiv b \mod p$ if $b \mod p \neq 0$. It remains to prove that $n = p^k$ does not divide $(a_i - a_1)$ for all $2 \leq l \leq n$ because in that case the product $\prod_{I \subseteq \{1, \ldots, n\}} (a_i - a_1)$ in the denominator is divisible by $p$ at most $(k - 1)i \leq ki - 1$ times and therefore there remains at least one factor $p$ in the term $p \sum_{i=1}^{n-1} p^{ki-1} T_i(a_1, \ldots, a_n)$. Hence, this term is zero modulo $p$ and

$$\frac{\prod_{n \geq i > j \geq 1} (b_i - b_j)}{\prod_{n \geq i > j \geq 1} (i - j)} \mod p = S(\pi),$$

which implies that $S(\pi) = S(\pi + 1)$. In order to prove that $p^k$ does not divide $(a_i - a_1)$ for all $2 \leq l \leq n$, note that $0 \leq a_i \leq 2n - 3$ for every $1 \leq l \leq n$, as $a_i$ is the sum of two distinct integers from the set $\{0, 1, \ldots, n - 1\}$. It follows that $|a_i - a_j| < 2n - 2p^k$ for every $2 \leq l \leq n$. Therefore, if $p^k$ divides $(a_i - a_1)$ for some $2 \leq l \leq n$, then $(a_i - a_1) = 0 \mod p$. But if $(a_i - a_1) = 0$ then $S(\pi) = 0$, if $(a_i - a_1) = n$ then $S(\pi - 1) = 0$ and if $(a_i - a_1) = -n$ then $S(\pi + 1) = 0$ and therefore these cases give a contradiction to our assumptions.
that $S(\pi) \neq 0$ and $S(\pi \pm 1) \neq 0$. It follows that $S(\pi) = S(\pi + 1) = S(\pi - 1)$ as claimed.

It remains to prove that $\text{sign}(\pi + 1) = \text{sign}(\pi)$ for every $\pi \in S_n$. Let us first consider the case when $\pi = \text{id}$. We have $\pi = (0, 1, \ldots, n - 2, n - 1)$ and $\pi + 1 = (1, 2, \ldots, n - 1, 0)$. To obtain $\pi$ from $\pi + 1$ we have to move the 0 on the last position back to the first position. This requires $n - 1$ transpositions. Since $n$ is odd we have $\text{sign}(\text{id} + 1) = (-1)^{n-1} = 1 = \text{sign}(\text{id})$. Next, let $\pi$ denote an arbitrary permutation in $S_n$ given by $\pi = (\pi(0), \pi(1), \ldots, \pi(n - 1))$. It follows that $\pi + 1$ is given by $(\pi(0) + 1, \pi(1) + 1, \ldots, \pi(n - 1) + 1) \mod n$. To get the identity from the permutation $\pi$ we have to use a certain number $x$ of transpositions. If we apply the same transpositions to the permutation $\pi + 1$ we will obtain the permutation $(1, 2, \ldots, n - 1, 0)$. From the case $\pi = \text{id}$, we know that we need $n - 1$ transpositions to obtain the identity from this permutation. Hence, we can use $x + n - 1$ transpositions to obtain the identity from the permutation $\pi + 1$. Since $n - 1$ is an even number it follows that $\text{sign}(\pi + 1) = (-1)^{x+n-1} = (-1)^x = \text{sign}(\pi)$.

\[ \square \]

As noted above we can now finish the proof of Theorem 3.1 in the case $p = 3$. Note that the internal ordering of the labels in a triangle is not important as if $\pi$ and $\sigma$ are such that $\pi$ is obtained from $\sigma$ by permuting the labels of some triangle, then $\pi$ and $\sigma$ are in the same coset of $H$. In Lemma 3.3 we find the more powerful conclusion that $k_\pi \neq 0 \mod 3$ if and only if $\pi$ is in the same coset of $H$ as $\sigma := \sigma^{\pi_0, \ldots, \pi_r}$ (recall that the permutation $\sigma^{\pi_0, \ldots, \pi_r}$ was defined in Lemma 3.3). This is because the permutations $\sigma^{\pi_0, \ldots, \pi_r}$ are all in the same coset of $H$ as $\sigma$ since these permutations only differ in the internal ordering of the labels in the triangles, which is not relevant in case $p = 3$, as explained above. For $\sigma$ one can easily check that $k_\sigma = 1$. Hence, $3|k_\sigma$ for every $\pi$ which is not in the same coset of $H$ as $\sigma = (0, r, 2r, 1, r + 1, 2r + 1, \ldots, r - 1, 2r - 1, 3r - 1)$. From Lemma 3.5 it follows that for each permutation $\pi$ there are $k_\pi$ cosets $[\pi]$ with the same value $\text{sign}(\pi)S(\pi)$. Let $K$ denote a maximal (with respect to inclusion) set of cosets $[\pi] \in H \setminus [\sigma]$ such that for each coset $[\tau] \in K$ there is no other coset $[\pi] \in K$ with $\pi = \tau + i$ for any $1 \leq i \leq k_\pi - 1$. It follows that

$$\sum_{[\pi] \in H} \text{sign}(\pi)S(\pi) \mod 3 = \text{sign}(\sigma)S(\sigma) + \sum_{[\pi] \in H \setminus [\sigma]} \text{sign}(\pi)S(\pi) \mod 3$$

$$= \text{sign}(\sigma)S(\sigma) + \sum_{[\pi] \in K} k_\pi \text{sign}(\pi)S(\pi) \mod 3$$

$$= \text{sign}(\sigma)S(\sigma)$$

$$\neq 0,$$

where the last inequality follows by Lemma 3.4. By (24) this concludes the proof for the case $p = 3$.

When $p > 3$, this becomes more complicated because in that case we find for each
coset of a $p$-cycle different permutations $\sigma^{\tau_0 \cdots \tau_{r-1}}$ as described in Lemma 3.3. Since in case $p > 3$ a $p$-cycle can be labelled in different ways using the same numbers, we have more than one coset for one $p$-cycle. Therefore, we probably also have more than one permutation $\sigma$ in Lemma 3.4 such that $S(\sigma) \neq 0$. For example, if $p = 5$ and $f$ consists of exactly one cycle (that is, $k = 1$), then $|S_{G_{\text{Aut}(C_5)}}/\text{Aut}(C_5)| = 12$. One representative of each coset is shown in Figure 12. For a labelling that is not antimagic the vertex sums that coincide with other vertex sums are colored in green.

![Figure 12: Cosets of a $C_5$](image)

In the following we will prove Theorem 3.1 for the case $p = 5$. In this part of the proof we use some properties of the antimagic labellings for 5-cycles that we deduce from the explicit representation of these labellings. Therefore this part does not extend to $p > 5$. We first consider the special case $p = 5$ and $k = 1$. In Figure 12, one can see that only the three permutations in the upper row given by $\sigma_1 = (0, 1, 2, 3, 4)$, $\sigma_2 = (0, 2, 4, 1, 3)$ and $\sigma_3 = (0, 1, 3, 4, 2)$ yield an antimagic labelling. The other permutations are not relevant because if $\tau$ is a permutation that yields a labelling that is not antimagic, then it follows that $P_0(\tau(0), \ldots, \tau(n-1)) = 0$ entailing $S(\tau) = 0$; therefore this permutation does not affect the sum $\sum_{[\pi] \in H} \text{sign}(\pi)S(\pi)$. For the permutation $\sigma_3 = (0, 1, 3, 4, 2)$ we have $k_{\sigma_3} \mod 5 = 0$. On the other hand $k_{\sigma_1} = k_{\sigma_2} = 1$. Therefore there remain only two permutations $\sigma$ such that $k_\sigma \text{sign}(\sigma)S(\sigma) \mod 5 \neq 0$. In these two cases we calculate $\text{sign}(\sigma)S(\sigma)$ explicitly. To do this we fix an ordering $v_1, v_2, \ldots, v_5$ of the vertices as shown in Figure 13.
The permutation $\sigma_1 = (0, 1, 2, 3, 4) = \text{id}$ is positive and for

$$S(\sigma_1) = \frac{P_0(\sigma_1(0), \ldots, \sigma_1(4))}{\prod_{5 \geq i > j \geq 1} (i - j)} \mod 5 = \frac{P_0(0, 1, 2, 3, 4)}{\prod_{5 \geq i > j \geq 1} (i - j)} \mod 5$$

we calculate

$$\prod_{5 \geq i > j \geq 1} (i - j) = 4!3!2! \cdot 288,$$

and

$$P_0(0, 1, 2, 3, 4) = (2 + 4 - 2 - 0)(4 + 1 - 2 - 0)(1 + 3 - 2 - 0)(3 + 0 - 2 - 0)$$

$$\times (4 + 1 - 4 - 2)(1 + 3 - 4 - 2)(3 + 0 - 4 - 2)$$

$$\times (1 + 3 - 1 - 4)(3 + 0 - 1 - 4)(3 + 0 - 3 - 1)$$

$$= 4 \cdot 3 \cdot 2 \cdot 1 \cdot (-1)(-2)(-3)(-1)(-2)(-1)$$

$$= 6912,$$

and therefore $S(\sigma_1) = \frac{6912}{288} \mod 5 = 4$.

For $\sigma_2 = (0, 2, 4, 1, 3) = (1243)$ we have a negative sign and

$$S(\sigma_2) = \frac{P_0(\sigma_2(0), \ldots, \sigma_2(4))}{\prod_{5 \geq i > j \geq 1} (i - j)} \mod 5 = \frac{P_0(0, 2, 4, 1, 3)}{288} \mod 5.$$

We have

$$P_0(0, 2, 4, 1, 3) = (2 + 4 - 2 - 0)(4 + 1 - 2 - 0)(1 + 3 - 2 - 0)(3 + 0 - 2 - 0)$$

$$\times (4 + 1 - 4 - 2)(1 + 3 - 4 - 2)(3 + 0 - 4 - 2)$$

$$\times (1 + 3 - 1 - 4)(3 + 0 - 1 - 4)(3 + 0 - 3 - 1)$$

$$= 4 \cdot 3 \cdot 2 \cdot 1 \cdot (-1)(-2)(-3)(-1)(-2)(-1)$$

$$= 288,$$

and therefore $S(\sigma_2) = \frac{288}{288} \mod 5 = 1$. If we calculate the sum in (12) we find

$$\sum_{[\pi] \in H} \text{sign}(\pi)S(\pi) \mod 5$$

$$= \text{sign}(\sigma_1)S(\sigma_1) + \text{sign}(\sigma_2)S(\sigma_2) + \sum_{[\tau] \in K} k_{\tau}\text{sign}(\tau)S(\tau) \mod 5$$

$$= \text{sign}(\sigma_1)S(\sigma_1) + \text{sign}(\sigma_2)S(\sigma_2) \mod 5$$

$$= 4 - 1$$

$$\neq 0.$$
which completes the proof of Theorem 3.1 for the case \( p = 5 \) and \( k = 1 \).

Recall that there are two permutations \( \sigma_1 = (0, 1, 2, 3, 4) \) and \( \sigma_2 = (0, 2, 4, 1, 3) \) that yield an antimagic labelling for one 5-cycle and such that \( k_{\sigma_i} \neq 0 \) for \( i = 1, 2 \). In Lemma 3.4 we proved that \( S(\sigma_1) \neq 0 \) if \( \sigma_1 \) is the permutation obtained by labelling \( r \) 5-cycles with an internal ordering according to \( \sigma_1 \) and where the labels of a cycle are in \( \{ i, r+i, 2r+i, 3r+i, 4r+i \} \) for some \( 0 \leq i \leq r-1 \). In the following lemma we prove that \( S(\sigma_2) \neq 0 \), too, if \( \sigma_2 \) is the permutation obtained by labelling \( r \) 5-cycles with an internal ordering according to \( \sigma_2 \) and where the labels of a cycle are in \( \{ i, r+i, 2r+i, 3r+i, 4r+i \} \) for some \( 0 \leq i \leq r-1 \).

**Lemma 3.6** Let \( p = 5 \) and let \( \sigma_2 \) denote the permutation \((0, 3r, r, 4r, 2r, 1, 3r+1, r+1, 4r+1, 2r+1, \ldots, r-1, 4r-1, 2r-1, 5r-1, 3r-1)\), then \( S(\sigma_2) \neq 0 \).

In order to prove Lemma 3.6 we use the same ideas as in the proof of Lemma 3.4. Recall that it is sufficient to prove that the vertex sums from \( (\sigma_2)_v \) are distributed uniformly amongst the residue classes modulo 5. Let \( n = 5^{k+1} \) and, for every \( 0 \leq i \leq 4 \), let \( R_i \) denote the set of vertex sums from \( (\sigma_2)_v \) with remainder \( i \) mod 5. Then \( |R_0| = |R_1| = \ldots = |R_4| \). As in Lemma 3.4 this can be seen if one considers the vertex sums of each 5-cycle. The vertex sums of the \( i \)-th cycle are given by

\[
(3r + 2(i - 1), 4r + 2(i - 1), 5r + 2(i - 1), 6r + 2(i - 1), 2r + 2(i - 1)).
\]

As \( k \geq 1 \) it follows that 5 divides \( r = 5^k \) and therefore all the vertex sums in a 5-cycle yield the same residue modulo 5. Hence, to prove that the vertex sums are distributed uniformly amongst the residue classes modulo 5, it is sufficient to choose one vertex sum in each 5-cycle and show that the distribution of these vertex sums is uniform amongst the residue classes modulo 5. Let us choose the following \( 5^k \) vertex sums \( 3r, 3r+2, 3r+4, \ldots, 3r+2(r-1) \). The distribution of these integers amongst the residue classes modulo 5 is the same as the distribution of the integers 0, 2, 4, \ldots, \( r-1, 1, 3, 5, \ldots, r-2 \) and is therefore uniform.

As in Lemma 3.4, let \( A_i = \{ \frac{m-i}{5} | m \in R_i \} \) if \( i \) is even and \( A_i = \{ \frac{m-(i+5)}{5} | m \in R_i \} \) if \( i \) is odd. Then \( A_0 = \ldots = A_4 \) is the set of vertex sums obtained from \( \sigma_2 \) if \( n = 5^k \). From the induction hypothesis it follows that for every integer \( 2 \leq t \leq k+1 \) the number of elements of \( A_0 \) with remainder \( i \) mod \( 5^{t-1} \) is equal to the number of those with remainder \( j \) mod \( 5^{t-1} \) for all \( 0 \leq i, j \leq 5^{t-1} - 1 \). Let \( 5A_0 + x = \{ 5a_i + 2x | a_i \in A_0, x \in \{ 0, 1, \ldots, 4 \} \} \). As in Lemma 3.4, it follows that the number of elements in \( R_0 \cup \ldots \cup R_4 = 5A_0 + x \) with remainder \( i \) mod \( 5^t \) is equal to the number of elements with remainder \( j \) mod \( 5^t \) for all \( 1 \leq t \leq k+1 \) and for all \( 0 \leq i, j \leq 5^{t-1} - 1 \).

\[ \square \]

As we have seen in Lemma 3.3, if \( k_\pi \) mod \( p \neq 0 \), then the labels of a \( p \)-cycle are in \( \{ i, r+i, \ldots, (p-1)r+i \} \) for some \( 0 \leq i \leq r-1 \). In the following Lemma
we prove that the ordering of the labels must be the same in all cycles if \( p = 5 \) and \( S(\pi) \neq 0 \).

**Lemma 3.7** If \( k_\pi \mod 5 \neq 0 \) and \( S(\pi) \neq 0 \), then \( \pi \) is in the same coset of \( H \) as one of the permutations

\[
\sigma^{\tau_{\pi}} = (\tau(0)r, \tau(1)r, \ldots, \tau(4)r, \ldots, \tau(0)r + r - 1, \ldots, \tau(4)r + r - 1),
\]

where \( \tau \in S_5/\text{Aut}(C_5) \). That is, the labels of the \((i + 1)\)-st 5-cycle are in the set \{\(i, r + i, \ldots, 4r + i\}\) for \(0 \leq i \leq r - 1\) and the internal ordering of the labels is the same in all 5-cycles.

**Proof of Lemma 3.7.** From Lemma 3.3 we know that the labels of the cycles are in the set \{\(i, r + i, \ldots, 4r + i\)\} for some \(0 \leq i \leq r - 1\). It remains to prove that the ordering of the labels is the same for all 5-cycles. Note that \( S(\pi) = 0 \) if \( \pi \) denotes a labelling that is not antimagic. Therefore we only have to consider the antimagic labellings. For one 5-cycle there are the following three antimagic labellings \( \sigma_1 = (0, 1, 2, 3, 4) \), \( \sigma_2 = (0, 2, 4, 1, 3) \) and \( \sigma_3 = (0, 1, 3, 4, 2) \), as shown in Figure 12. The corresponding vertex sums are \((\sigma_1)_v = (1, 3, 5, 7, 4)\), \((\sigma_2)_v = (2, 6, 5, 4, 3)\) and \((\sigma_3)_v = (1, 4, 7, 6, 2)\). Clearly, the vertex sums from \((\sigma_3)_v\) are not distributed uniformly amongst the residue classes modulo 5. On the other hand the vertex sums from \((\sigma_1)_v\) and \((\sigma_2)_v\) are distributed uniformly amongst the residue classes modulo 5. From the proof of Lemma 3.2 it follows that \( S(\sigma_3) = 0 \) since the number of times 5 divides \( \prod_{0 \leq i \leq j \leq 1}(i - j) \) is smaller than the number of times 5 divides \( P_0(\sigma_3(0), \ldots, \sigma_3(4)) \). On the other hand \( S(\sigma_1) \neq 0 \) by Lemma 3.4 and \( S(\sigma_2) \neq 0 \) by Lemma 3.6.

If a labelling \( \pi \) of \( r \) cycles contains at least one cycle labelled according to \( \sigma_3 \) then \( S(\pi) = 0 \). This is because in \((\sigma_3)_v\) the vertex sums 1 and 6 are in the same residue class modulo 5. If the \((i + 1)\)-st cycle in \( \pi \) is labelled according to \( \sigma_3 \) it follows that its labelling is \( (i, r + i, 3r + i, 4r + i, 2r + i) \) and the permutation of its vertex sums is \( (r + 2i, 4r + 2i, 7r + 2i, 6r + 2i, 2r + 2i) \). Hence, \( r + 2i \) and \( 6r + 2i \) yield the same residue modulo 5 and therefore the \( 5^k \) vertex sums in \( \pi \) cannot be distributed uniformly amongst the residue classes modulo \( 5^k \) and thus \( S(\pi) = 0 \).

If \( \pi \) contains a cycle that is labelled according to \( \sigma_1 \) or \( \sigma_2 \), we can add arbitrary integers modulo \( n \) to all labels of this cycle and we remain in the same coset. This is because \( k_{\sigma_1} = k_{\sigma_2} = 1 \) entailing that the ordering of the labels is preserved if we add 1 and calculate then the remainders of the labels modulo 5.

If a cycle with a labelling according to \( \sigma_1 \) or \( \sigma_2 \) should not construct all cycles by adding \( k_\pi \neq 0 \mod 5 \) to its labels, then the cycles with this labelling should have the same distance \( k_\pi \) (number of 5-cycles in between) from a next cycle in this coset. Therefore the number of cycles in this coset divides \( r \). Hence the distance, that is \( k_\pi \), between two labellings in this coset is either 1 or divisible by 5. But if the distance is one, it follows that all the labellings are in the same coset.

\( \square \)

Note that we even proved the stronger result that \( \tau \in \{\sigma_1, \sigma_2\} \).

28
As in the calculation for one 5-cycle it remains to prove that
\[ \sum_{\pi \in H} \text{sign}(\pi)S(\pi) \mod 5 \]
\[ = \text{sign}(\sigma_1)S(\sigma_1) + \text{sign}(\sigma_2)S(\sigma_2) + \sum_{\tau \in K} k_\tau \text{sign}(\tau)S(\tau) \mod 5 \]
\[ = \text{sign}(\sigma_1)S(\sigma_1) + \text{sign}(\sigma_2)S(\sigma_2) \mod 5 \]
\[ \neq 0, \]
which we prove in the following lemma.

**Lemma 3.8** Let \( \sigma_1 \) and \( \sigma_2 \) denote the permutations \( \sigma_1 = (0, r, 2r, 3r, 4r, 1, r + 1, 2r + 1, 3r + 1, 4r + 1, \ldots, r - 1, 2r - 1, 3r - 1, 4r - 1, 5r - 1) \) and \( \sigma_2 = (0, 2r, 4r, r, 3r, 1, 2r + 1, 4r + 1, r + 1, 3r + 1, \ldots, r - 1, 3r - 1, 5r - 1, 2r - 1, 4r - 1) \). Then \( \text{sign}(\sigma_1)S(\sigma_1) + \text{sign}(\sigma_2)S(\sigma_2) \mod 5 \neq 0 \).

**Proof of Lemma 3.8.** We first prove that \( \text{sign}(\sigma_1) \neq \text{sign}(\sigma_2) \). If there is only one cycle, then \( \sigma_1 = (0, 1, 2, 3, 4) \) and \( \sigma_2 = (0, 2, 4, 1, 3) \). The permutation \( \sigma_1 \) is obtained from \( \sigma_2 \) using 3 transpositions:
\[ \sigma_2 = (0, 2, 4, 1, 3) \xrightarrow{(14)} (0, 2, 1, 4, 3) \xrightarrow{(12)} (0, 1, 2, 4, 3) \xrightarrow{(34)} (0, 1, 2, 3, 4) = \sigma_1. \]
If there are \( 5^k \) cycles, for some integer \( k \geq 0 \), then \( \sigma_1 \) is obtained from \( \sigma_2 \) using \( 3 \cdot 5^k \) transpositions, which is an odd number. Thus \( \text{sign}(\sigma_1) \neq \text{sign}(\sigma_2) \) and therefore it is sufficient to show that \( (S(\sigma_1) - S(\sigma_2)) \mod 5 \neq 0 \).

In the following we call \( P_0(\sigma(0), \ldots, \sigma(n - 1)) \) the numerator of \( S(\sigma) \) and we call \( \prod_{0 < i < j < n} (i - j) \) the denominator of \( S(\sigma) \), where \( \sigma \) is a permutation in \( S_n \). Recall that \( S(\sigma_1) \neq 0 \) by Lemma 3.4 and \( S(\sigma_2) \neq 0 \) by Lemma 3.6 respectively. Moreover, we calculated in the proof of Theorem 3.1 for the special case of one 5-cycle that \( S(\sigma_1) = 4 \neq 1 = S(\sigma_2) \). We will prove the fact that \( S(\sigma_1) \neq S(\sigma_2) \) for one cycle, implies that \( S(\sigma_1) \neq S(\sigma_2) \) for \( r = 5^k \) cycles, where \( k \) is a positive integer. Let \( \sigma \in \{\sigma_1, \sigma_2\} \). Assume that the vertices of \( f \) are ordered as in Figure 14:

![Figure 14: Ordering of the labels in the C_5-factor f](image)

The factors in the product \( P_0(\sigma(0), \ldots, \sigma(n - 1)) \) in the numerator of \( S(\sigma) \) consist of differences of two vertex sums from the same 5-cycle and of differences of two vertex sums from different 5-cycles. From Lemma 3.4 we know that the number of times that 5 divides the numerator of \( S(\sigma_1) \) is equal to the number of times that 5 divides the denominator of \( S(\sigma_1) \) and the same result holds for \( S(\sigma_2) \) by Lemma 3.6. Therefore, all factors 5 in the prime factorization of the numerators of \( S(\sigma_1) \) and of \( S(\sigma_2) \) will be cancelled.
Note that in every cycle \( C_i \) the vertex sums from \((\sigma_1)_v\) and from \((\sigma_2)_v\) are the same modulo \( 5r \). Let us look at the differences of vertex sums from two different cycles \( C_i \) and \( C_j \). Calculate the remainders modulo 5 considering that all factors 5 cancel and that the vertex sums from \((\sigma_1)_v\) and from \((\sigma_2)_v\) are the same modulo a power of 5. Thus, after cancelling all factors 5, it follows that all factors of differences of vertex sums from two different 5-cycles are the same in \( S(\sigma_1) \) and in \( S(\sigma_2) \) modulo 5.

Hence, to see if \( S(\sigma_1) \) and \( S(\sigma_2) \) are different, it is enough to consider the differences of vertex sums from the same 5-cycle. Clearly, these differences are the same in all 5-cycles. Thus, it suffices to consider the differences from all vertex sums of the first 5-cycle.

For \( i = 1, 2 \), let \( L_i \) denote the product of all differences of vertex sums from \( \sigma_i \) we calculated in the proof for one 5-cycle. For \( \sigma_1 \) the product of the differences of the vertex sums in the first cycle is

\[
(v_5 - v_4)(v_5 - v_3)(v_5 - v_2)(v_5 - v_1)(v_4 - v_3) \\
\times (v_4 - v_2)(v_4 - v_1)(v_3 - v_2)(v_3 - v_1)(v_2 - v_1) \\
= r^{10} \cdot L_1 \\
= r^{10} \cdot 6912, \tag{14}
\]

and for \( \sigma_2 \) the product of these differences is

\[
(v_5 - v_4)(v_5 - v_3)(v_5 - v_2)(v_5 - v_1)(v_4 - v_3) \\
\times (v_4 - v_2)(v_4 - v_1)(v_3 - v_2)(v_3 - v_1)(v_2 - v_1) \\
= r^{10} \cdot L_2 \\
= r^{10} \cdot 288. \tag{15}
\]

For \( i = 1, 2 \) let \( c_i \) denote the product of all differences of vertex sums of \((\sigma_i)_v\) from different 5-cycles after cancelling all factors 5. Let \( b_i \) denote the product \( \prod_{n \geq i > j \geq 1} (i - j) \) in the denominator of \( S(\sigma_i) \) that remains after cancelling all factors 5 (\( b_i \) is not zero modulo 5 for \( i = 1, 2 \) since the number of times that 5 divides the numerator \( P_0(\sigma_i(0), \ldots, \sigma_i(n - 1)) \) is equal to the number of times
that 5 divides the denominator $\prod_{n \geq i > j \geq 1} (i - j)$ as we have seen in Lemma 3.4 and Lemma 3.6. Clearly, $b_1 = b_2$ since the denominator is the same for $S(\sigma_1)$ and $S(\sigma_2)$. We proved that $c_1 b_1^{-1} \mod 5 = c_2 b_2^{-1} \mod 5$. Moreover, let $a_i$ for $i = 1, 2$ denote the product of all differences of two vertex sums from $(\sigma_i)_v$ that are in the same cycle after cancelling all the factors 5. Since we have now $r$ cycles it follows from (14) that $a_1 = 6912^r$ and from (15) that $a_2 = 288^r$. Thus, we can write

$$S(\sigma_1) = a_1 c_1 b_1^{-1} \mod 5 = (6912^r \mod 5)(c_1 b_1^{-1}) \mod 5,$$

and

$$S(\sigma_2) = a_2 c_2 b_2^{-1} \mod 5 = (288^r \mod 5)(c_1 b_1^{-1}) \mod 5.$$

Since $2^l \mod 5 = 3^l \mod 5$ if and only if $l$ is even it follows that $S(\sigma_1) \neq S(\sigma_2)$ for $5^k$ cycles. This finishes the proof of Lemma 3.8.

Let us go back to the proof of Theorem 3.1. From Lemma 3.8 it follows that

$$\sum_{|\pi| \in H} \text{sign}(\pi)S(\pi) \mod 5 = \text{sign}(\sigma_1)S(\sigma_1) + \text{sign}(\sigma_2)S(\sigma_2) \mod 5 \neq 0,$$

which concludes the proof of Theorem 3.1 for the case $p = 5$. 

\[\square\]
4 Concluding remarks and open problems

We proved that every graph on \( n = p^k \) vertices that admits a \( C_p \)-factor is antimagic, for \( p \in \{3, 5\} \) by extending all parts of Hefetz’s proof for the case \( p = 5 \). We were not able to extend all parts of the proof to arbitrary odd primes \( p \). In Lemma 3.6, Lemma 3.7 and in Lemma 3.8 we used the permutations of the antimagic labellings explicitly. To prove these results for arbitrary odd primes \( p \) one has to find another approach. For \( p > 5 \) there are many antimagic labellings of a \( C_p \). With a computer program we calculated that there are 46 cosets that correspond to an antimagic labelling for one 7-cycle and for one 9-cycle we calculated 924 cosets that correspond to an antimagic labelling. We do not know if Theorem 3.1 extends to arbitrary odd primes \( p \). It would be interesting to prove a more general result.
Acknowledgements

The author would like to thank Dr. Dan Hefetz for his great support.

References


