Polynomial method for perfect 2-colourings of circulant graphs

Svyatoslav Novikov

Abstract

In this paper we prove that if an infinite circulant graph with $k$ distances has a perfect 2-colouring with parameters $(b, c)$, then $b + c \leq 2k + \frac{b+c}{q^t}$ for all positive integers $t$ and primes $q$ satisfying $\frac{b+c}{\gcd(b,c)}q^t$. In addition, we show that if $b + c = q^t$, then this necessary condition becomes sufficient for the existence of perfect 2-colourings in circulant graphs.

1 Introduction

A perfect 2-colouring of a regular graph $G$ with parameters $(b, c)$ is a colouring of its vertices in 2 colours (black and white), in which each black vertex has exactly $b$ white neighbours and each white vertex has $c$ black neighbours.

Perfect colourings are often referred to as equitable partitions; this term was introduced by Delsarte in the book [14].

An infinite circulant graph with $k$ distances $l_1, ..., l_k$ is a graph (possibly, with loops and multiple edges), whose vertices are integer numbers; numbers, which differ by $l_i$ for some $i$, are connected with an edge. Denote such a graph by $C_\infty(l_1, ..., l_k)$. Remark that $C_\infty(l_1, ..., l_k)$ is a regular graph of degree $2k$.

Perfect 2-colourings of circulant graphs and their parameters are being subject of active research (see, e.g., [1], [2], [3], [4], [5]). However, the above works consider only the cases when the distances $l_1, ..., l_k$ have some special form.

On the contrary, in this work we prove some inequalities between permissible values of $b, c, k$, which apply to arbitrary values of $l_1, ..., l_k$. In particular,
we prove the hypothesis (stated in [1]) that the parameters \((5, 3)\) are not permissible for 3 distances.

For this purpose we introduce the notion of *multitiling* of an abelian group, which is a natural generalization of the notion of tiling. Next, for the group \(\mathbb{Z}/P\mathbb{Z}\) we describe multitilings in terms of polynomials with integer coefficients, which satisfy some divisibility condition, and, in terms of cyclotomic polynomials, we obtain a necessary and sufficient condition for the existence of a multitiling of fixed multiplicity with some fixed "tile". One can show that the question of permissibility of the parameters \(b, c, k\) for perfect 2-colourings of graphs \(C_\infty(l_1, ..., l_k)\) can be reduced to the same question for graphs \(G_P = C_P(l_1, ..., l_k)\) on the residues modulo \(P\) for \(P\). Finally, perfect 2-colourings of graphs \(C_P(l_1, ..., l_k)\) are represented as particular instances of multitilings of multiplicity \(c\) of the group \(\mathbb{Z}/P\mathbb{Z}\) with some tile \(u_{l_1, ..., l_k; b, c, P}\), which allows to deduce an inequality on \(b, c, k\), which is the main result of the work. Moreover, we show that if \(b + c\) is a prime power then the same condition is also a sufficient condition for the permissibility of the parameters \(b, c\) for \(k\) distances.

Remark that in some other works (see, e.g., [8], [9], [10], [11], [12], [13]) similar reformulations of tilings in terms of polynomials are introduced, and, moreover, similarly to this work, cyclotomic polynomials are applied. However, in such works the condition \((T1)\), first introduced in [8], is considered and used only for tilings of multiplicity 1. In this work we generalize \((T1)\) (point 1 of lemma [1]) to multitilings and apply it to perfect 2-colourings.

## 2 Preliminaries and main results

Polynomials \(\Phi_n(x) = \prod_{1 \leq k \leq n; \gcd(k,n)=1} (x - e^{2\pi ik/n})\), \(n \geq 1\), \(n \in \mathbb{Z}\), are called cyclotomic polynomials. Below some of their properties are given:

**Proposition 1.**

1) \(\Phi_n(x)\) are irreducible in \(\mathbb{Q}[x]\) and have integer coefficients.

2) \(\Phi_n(1) = 1\), if \(n > 1\), and \(n\) is not a prime power.

3) \(\Phi_{p^k}(1) = p\), if \(k \geq 1\) and \(p\) is a prime.

4) \(x^n - 1 = \prod_{d|n} \Phi_d(x)\).

5) \(\Phi_{p^k}(x) = \frac{x^{p^k-1} - 1}{x^{p-1} - 1} = \sum_{l=0}^{p-1} x^{pk-l}\)
For an abelian group $H$ we will call a tile on $H$ an arbitrary function $u : H \rightarrow \mathbb{Z}$.

We call an $m$-multitiling of a group $H$ with a tile $u$ a function $v : H \rightarrow \mathbb{Z}$ such that
\[
\sum_{h \in H} u(g-h)v(h) = m
\]
for each $g \in H$. Assume that $m \in \mathbb{Z}$, $m \neq 0$.

We call an $m$-tiling of a group $H$ with a tile $u$ an $m$-multitiling of the group $H$ with some tile $u$ such that $v(h) \in \{0, 1\}$ for each $h \in H$.

Consider the case $H = \mathbb{Z}/P\mathbb{Z}$. Introduce the polynomials
\[
Q_u(x) = \sum_{a=0}^{P-1} u(a)x^a
\]
\[
Q_v(x) = \sum_{a=0}^{P-1} v(a)x^a
\]
(In the works [9], [10], [13] polynomials similar to $Q_u(x)$, $Q_v(x)$ are referred to as mask polynomials; in [11] as characteristic polynomials; they also appear in [8], [12])

Let $M = \max(l_1, \ldots, l_k)$; $l_1, \ldots, l_k$ are nonnegative integers; let $b > 0, c > 0$ also be integers.

For $g \in \mathbb{Z}/P\mathbb{Z}$ denote by $\delta_g(h)$ a function on $\mathbb{Z}/P\mathbb{Z}$, which is equal to 1 at $h = g$, 0 otherwise. Also introduce on $\mathbb{Z}/P\mathbb{Z}$ the following function:
\[
u_{l_1, \ldots, l_k; b,c}(h) = (b + c - 2k)\delta_M(h) + \sum_{i=1}^{k}(\delta_{M+l_i}(h) + \delta_{M-l_i}(h)).
\]

Denote
\[
A(x) = x^M(b + c - 2k + \sum_{i=1}^{k}(x^{l_i} + x^{-l_i})).
\]
\[
S_P(x) = \prod_{n: n|P, \Phi_n(x)|A(x)} \Phi_n(x).
\]
\[
\tilde{S}_P(x) = \prod_{n: n|P, \Phi_n(x)|A(x), n \text{ is a prime power}} \Phi_n(x).
\]
Denote by $G_P = C_P(l_1, \ldots, l_k)$ a graph on $P$ vertices, obtained from the graph $C_\infty(l_1, \ldots, l_k)$ by factorization of vertices modulo $P$.

We can construct a 1-1 correspondence between 2-colourings of the graph $G_P$ with parameters $(b, c)$ and $c$-tilings $v$ of the group $\mathbb{Z}/P\mathbb{Z}$ with the tile $u_{l_1, \ldots, l_k; b, c; P}$: consider a graph $\tilde{G}_P$, which is obtained by adding $b+c-2k$ loops in each vertex. A black-and-white colouring of $G_P$ is perfect with parameters $(b, c)$ if and only if in the same colouring, considered as a colouring of the graph $\tilde{G}_P$, each vertex has exactly $c$ black neighbours (white vertices still have $c$ black neighbours, black vertices had $2k-b$ black neighbours, now they have $(b+c-2k)+(2k-b) = c$ black neighbours). Such black-and-white colourings of the graph $\tilde{G}_P$ (we call them "good") are in a 1-1 correspondence with $c$-tilings $v$ of the group $\mathbb{Z}/P\mathbb{Z}$ with the tile $u_{l_1, \ldots, l_k; b, c; P}$: if we color as black exactly the elements $g$ of the group $\mathbb{Z}/P\mathbb{Z}$, for which $v(g) = 1$, we obtain a "good" colouring of the graph $\tilde{G}_P$; if, in turn, we let $v(g) = 1$ for all black vertices $g$ and $v(g) = 0$ for white vertices of some "good" colouring of the graph $\tilde{G}_P$ with parameters $(b, c)$, we obtain a $c$-tiling of the group $\mathbb{Z}/P\mathbb{Z}$ with the tile $u_{l_1, \ldots, l_k; b, c; P}$.

Below the main results of the work are given:

**Theorem 1.**
1) If the graph $G_P = C_P(l_1, \ldots, l_k)$ has a perfect 2-colouring with parameters $(b, c)$, then $\tilde{S}_P(1) = \frac{b+c}{\gcd(b, c)}$.

2) If $P = q^t$ for some prime number $q$ and integer $t > 0$, then the graph $G_P = C_P(l_1, \ldots, l_k)$ has a perfect 2-colouring with parameters $(b, c)$ if and only if $\tilde{S}_P(1) = \frac{b+c}{\gcd(b, c)}$.

**Theorem 2.** If there exists a circulant graph with $k$ distances, which has a perfect 2-colouring with parameters $(b, c)$, then for each prime $q$ and positive integer $t$ such that $\frac{b+c}{\gcd(b, c)}q^t$, it holds that $b+c \leq 2k + \frac{b+c}{q^t}$.

**Corollary 1.**
1) No infinite circulant graph with 2 distances has a perfect 2-colouring with parameters $(4, 3)$.

2) No infinite circulant graph with 3 distances has a perfect 2-colouring with parameters $(5, 3), (5, 4), (6, 4) \text{ or } (6, 5)$.

3) No infinite circulant graph with 4 distances has a perfect 2-colouring with parameters $(6, 5), (7, 4), (8, 3), (7, 5), (7, 6), (8, 5), (8, 6) \text{ or } (8, 7)$.

Thus, the hypothesis of inadmissibility of parameters $(5, 3)$ for 3 distances, stated in [1], is proven.
When \(b + c\) is a prime power, one can obtain a necessary and sufficient condition for the existence of a circulant graph with \(k\) distances, which has a perfect 2-colouring with parameters \((b, c)\):

**Theorem 3.** Let \(b + c = q^s\) for some integer \(s > 0\) and prime \(q\). Then there exists a circulant graph with \(k\) distances and its perfect 2-colouring with parameters \((b, c)\), if and only if \(b + c \leq 2k + \gcd(b, c)\).

### 3 Polynomial method for multitilings

**Proposition 2.** The condition \(\text{(1)}\) is equivalent to

\[
Q_u(x)Q_v(x) - m \frac{x^P - 1}{x - 1}; (x^P - 1). \tag{2}
\]

**Proof.** Remark that

\[
Q_u(x)Q_v(x) = \sum_{c=0}^{P-1} \left( \sum_{0 \leq a, b \leq P-1; \ a + b \equiv c \ (mod \ p)} u(a)v(b) \right) x^{a+b}
\]

\[
\equiv \sum_{c=0}^{P-1} \left( \sum_{0 \leq a, b \leq P-1; \ a + b \equiv c \ (mod \ p)} u(a)v(b) \right) x^{c} \ (mod \ x^P - 1)
\]

On the other hand,

\[
m \frac{x^P - 1}{x - 1} = \sum_{c=0}^{P-1} mx^c
\]

Hence, the condition \(\text{(2)}\) is equivalent to

\[
\left( \sum_{0 \leq a, b \leq P-1; \ a + b \equiv c \ (mod \ p)} u(a)v(b) \right) = m
\]

for all \(c\), that is, \(\text{(1)}\). \qed

A divisibility condition similar to \(\text{(2)}\) is also used in \([8], [11], [12], [13]\).
Introduce analogs of the polynomials $S_A$ from [9], which also appear in [8], [10], [11], [12], [13]:

\[ d_u(x) = \prod_{n \mid P, \Phi_n(x) \mid Q_u(x)} \Phi_n(x). \]

\[ \tilde{d}_u(x) = \prod_{n \mid P, \Phi_n(x) \mid Q_u(x)} \Phi_n(x), \quad n \text{ is a prime power} \]

**Lemma 1.**

1) Let $m \in \mathbb{Z}$, $m \neq 0$. Then an $m$-multitiling $v$ of the group $\mathbb{Z}/P\mathbb{Z}$ with a tile $u : \mathbb{Z}/P\mathbb{Z} \to \mathbb{Z}$ exists if and only if $m \cdot \tilde{d}_u(1) : Q_u(1)$.

2) If $m \cdot \tilde{d}_u(1) : Q_u(1)$, $P = q^t$ for some prime $q$ and positive integer $t$ and, in addition, $0 < m \leq Q_u(1)$, then there exists an $m$-tiling $v$ of the group $\mathbb{Z}/P\mathbb{Z}$ with the tile $u : \mathbb{Z}/P\mathbb{Z} \to \mathbb{Z}$.

*Proof.* As $x^P - 1 = \prod_{n \mid P} \Phi_n(x)$, where $\Phi_n(x)$ are irreducible over $\mathbb{Q}[x]$ (in particular, they are pairwise coprime), we obtain $\gcd(Q_u(x), x^P - 1) = \prod_{\Phi_n(x) \mid (x^P - 1), \Phi_n(x) \mid Q_u(x)} \Phi_n(x) = d_u(x)$. If $Q_u(1) = 0$, then the condition (2) does not hold; but if $Q_u(1) \neq 0$, then $(x - 1) \nmid d_u(x)$, hence, (2) is equivalent to

\[ \frac{Q_u(x)}{d_u(x)} Q_v(x) - m \frac{x^P - 1}{(x - 1)d_u(x)} : \frac{x^P - 1}{d_u(x)}. \quad (3) \]

From the definition of $d_u$ the polynomials $\frac{Q_u(x)}{d_u(x)}$ and $\frac{x^P - 1}{(x - 1)d_u(x)}$ are coprime, hence, due to (3), $Q_u(x) : \frac{x^P - 1}{(x - 1)d_u(x)}$, that is, $Q_u(x)$ is representable as $\frac{x^P - 1}{(x - 1)d_u(x)} R_v(x)$, where $R_v(x)$ is a polynomial with integer coefficients such that $\deg(R_v) + \deg \left( \frac{x^P - 1}{(x - 1)d_u(x)} \right) \leq P - 1$. Then (3) is equivalent to

\[ \frac{Q_u(1)}{d_u(1)} R_v(1) = m. \]

In particular,

\[ m \cdot d_u(1) : Q_u(1). \quad (4) \]

If $n > 1$ and $n$ is not a prime power then $\Phi_n(1) = 1$, hence, $d_u(1) = \tilde{d}_u(1)$. Consequently, point 1) is proved in one direction.
Conversely, remark that if \([4] \) is satisfied, then one can take \( R_v(x) = \frac{md_u(1)}{Q_u(1)} \), \( Q_v(x) = \frac{md_u(1)}{Q_u(1)} \frac{x^P - 1}{(x-1)d_u(x)} \), which provides an \( m \)-multitiling of the group \( \mathbb{Z}/P\mathbb{Z} \) with the tile \( u \).

In order to prove the point 2) it is enough to contrust a polynomial \( Q_v(x) \), which satisfies \([2] \), whose coefficients are equal to either 0 or 1. As \( Q_v(x) \) can be represented as \( \frac{x^P - 1}{(x-1)d_u(x)} R_v(x) \), it is enough to construct \( R_v(x) \) with integer coefficients of degree not larger than \( P - 1 - \deg \left( \frac{x^P - 1}{(x-1)d_u(x)} \right) = \deg (d_u(x)) \) such that \( R_v(1) = \frac{md_u(1)}{Q_u(1)} \), and each coefficient of \( \frac{x^P - 1}{(x-1)d_u(x)} R_v(x) \) equals either 0 or 1. As \( d_u(x) | \frac{x^q - 1}{x-1} = \prod_{l=1}^{t} \Phi_q(x) \), there exists \( X \subset \{1, \ldots, t\} \) such that

\[
\tilde{d}_u(x) = d_u(x) = \prod_{r \in X} \Phi_q(x) = \prod_{r \in X} \sum_{i=0}^{q-1} x^q \cdot \frac{x^q - 1}{x-1}.
\]

Hence, all coefficients of \( d_u(x) \) are equal to either 0 or 1. As due to the conditions of the lemma \( 0 < \frac{md_u(1)}{Q_u(1)} \leq d_u(1) \), one can take as \( R_v(x) \) a sum of arbitrary \( \frac{md_u(1)}{Q_u(1)} \) monomials whose coefficients are equal to 1 in \( d_u(x) \). Then \( \deg (R_v(x)) \leq \deg (d_u(x)) \). Moreover,

\[
\frac{x^P - 1}{(x-1)d_u(x)} = \left( \prod_{r \in \{1, \ldots, t\}} \sum_{i=0}^{q-1} x^q \cdot \frac{x^q - 1}{x-1} \right) / \left( \prod_{r \in X} \sum_{i=0}^{q-1} x^q \cdot \frac{x^q - 1}{x-1} \right) = \prod_{r \in \{1, \ldots, t\} \setminus X} \sum_{i=0}^{q-1} x^q \cdot \frac{x^q - 1}{x-1},
\]

from which the coefficients of \( \frac{x^P - 1}{(x-1)d_u(x)} \) are nonnegative, hence, for each integer \( a \geq 0, a < P \), the coefficient of the polynomial \( Q_v(x) = R_v(x) \frac{x^P - 1}{(x-1)d_u(x)} \) at \( x^a \) is a nonnegative integer which does not exceed the coefficient at \( x^a \) of the polynomial \( d_u(x) \frac{x^P - 1}{(x-1)d_u(x)} = \frac{x^P - 1}{x-1} \), which, in turn, equals 1. Consequently, each coefficient of \( Q_v(x) \) equals either 0 or 1, then for the tile \( v \) it holds that \( \text{range}(v) \subset \{0, 1\} \).

Remark that the condition \( m \cdot \tilde{d}_u(1); Q_u(1) \) is a generalization of \((T1)\) from \([5]\) to multitilings.

7
4 Proofs of main results

It is a known fact ([1]), that if a perfect 2-colouring of the graph $C_\infty(l_1, ..., l_k)$ exists, then it has some period $P$. In other words, for this $P$ there exists a perfect 2-colouring $S$ with parameters $(b, c)$ of the graph $G_P = C_{P}(l_1, ..., l_k)$.

Hence, due to the correspondence between perfect colourings of the graph $G_P$ and tilings of the group $\mathbb{Z}/P\mathbb{Z}$, described in Section 2, theorem 2 is a corollary of the following lemma:

Lemma 2. The following conditions are equivalent:

1) There exist nonnegative integers $l_1, ..., l_k$, an integer $P > 1$ and a c-multitiling of the group $\mathbb{Z}/P\mathbb{Z}$ with the tile $u_{l_1, ..., l_k; b,c; P}$.

2) For each prime $q$ and positive integer $t$ such that $b + c + \gcd(b,c) \cdot q^t$, it holds that $b + c + \frac{b + c}{\gcd(b,c)}$.

Moreover, if 2) is satisfied, then in 1) one can take $P = \frac{b + c}{\gcd(b,c)}$, if $b + c + \frac{b + c}{\gcd(b,c)}$ is odd and $P = 2\frac{b + c}{\gcd(b,c)}$, if $b + c + \frac{b + c}{\gcd(b,c)}$ is even.

Since for each nonnegative integer $g$ it holds that $Q_{\delta_g}(x) \equiv x^g \pmod{x^P - 1}$, where $\delta_g : \mathbb{Z}/P\mathbb{Z} \to \mathbb{Z}$, $\delta_g(h) = 1$, if $g \mod P = h$, $\delta_g(h) = 0$ otherwise, then for $u = u_{l_1, ..., l_k; b,c; P}$ we have $A(x) - Q_u(x);(x^P - 1)$, hence, $d_u(x) = S_P(x)$, $\tilde{d}_u(x) = \tilde{S}_P(x)$.

Theorem 1, in turn, due to the correspondence between c-tilings and perfect colourings with parameters $(b, c)$, described in Section 2, is a corollary of the following lemma:

Lemma 3. 1) There exists a c-multitiling of the group $\mathbb{Z}/P\mathbb{Z}$ with the tile $u_{l_1, ..., l_k; b,c; P}$ if and only if $\tilde{S}_P(1) = \frac{b + c}{\gcd(b,c)}$.

2) If $P = q^t$ for some prime $q$ and positive integer $t$, then there exists a c-tiling of the group $\mathbb{Z}/P\mathbb{Z}$ with the tile $u_{l_1, ..., l_k; b,c; P}$.

Proof. Substitute $m = c$, $u = u_{l_1, ..., l_k; b,c; P}$ in lemma 1 the condition $m \cdot \tilde{d}_u(1);Q_u(1)$ can be rewritten as $c \cdot \tilde{S}_P(1);(b + c)$, since $Q_u(1) = b + c$. This, in turn, is equivalent to $\tilde{S}_P(1) = \frac{b + c}{\gcd(b,c)}$. The condition $0 < m \leq Q_u(1)$ from point 2) of lemma 1 is also satisfied. □

Proof of lemma 2: "⇒" Since $\Phi_{p^k}(1) = p$ for each prime $p$ and integer $k > 0,$
then
\[ \tilde{S}_P(1) = \prod_{(p,k): p \text{ простое}, k>0, p^k | P, \Phi_{p^k}(x) | A(x)} p. \] 

From the conditions of lemma 2 combined with lemma 3 it follows that \( \tilde{S}_P(1); q^t \). Hence, for at least \( t \) pairs \((p,k)\) from the product (5) it holds that \( p = q \), which implies that there exist \( 0 < s_1 < ... < s_t \) such that for each \( 1 \leq i \leq t \) it holds that

\[ A(x); \Phi_{q^{s_i}}(x) = \frac{x^{q^{s_i}} - 1}{x^{q^{s_i-1}} - 1} (**) \]

Denote \( h_{j,r} = \sum_{r': q^{s_i-1} | (r'-r)} a_{r'} \), where \( a_{r'} \) is the coefficient of the polynomial \( A(x) \) at \( x^{r'} \). Then it is easy to see that (**) can be rewritten as \( h_{s_i,r} = h_{s_i,r+q^{s_i-1}} \) for each \( i, r \), since

\[ (x^{q^{s_i-1}} - 1)A(x) \equiv \sum_{r=0}^{q^{s_i-1}} h_{s_i,r-q^{s_i-1}} \cdot x^r - \sum_{r=0}^{q^{s_i-1}} h_{s_i,r} \cdot x^r \ (mod \ x^{q^{s_i}} - 1). \]

For convenience we will consider that \( s_0 = 0 \).

**Claim 1.** For \( 1 \leq i \leq t \) it holds that \( h_{s_{i-1},M} > q \cdot h_{s_i,M} \).

**Proof.** The claim follows from the next relations:

\[ q \cdot h_{s_i,M} = \sum_{b=0}^{q-1} h_{s_i,M+bq^{s_i-1}} = h_{s_{i-1},M} \leq h_{s_{i-1},M} \]

Here the first equality follows from (**) Let us prove the second equality:

\[ h_{s_{i-1},M} = \sum_{r':q^{s_i-1} | (r'-M)} a_{r'} = \sum_{b=0}^{q-1} \sum_{r':q^{s_i-1} | (r'-M-bq^{s_i-1})} a_{r'} = \sum_{b=0}^{q-1} h_{s_i,M+bq^{s_i-1}}. \]

The last inequality follows from the fact that the coefficients of \( A(x) \), except for possibly the coefficient at \( x^M \), are nonnegative. \( \square \)
Applying claim 1 \( t \) times and again using nonnegativity of the coefficients of \( A(x) \), except for possibly the coefficient at \( x^M \), we obtain \( b + c = h(1) = h_{s_0,M} = q^l \cdot h_{s_1,M} \geq q^l \cdot (b + c - 2k) \) as required.

\( ^{n \Leftrightarrow} \) By lemma 3 it is enough to construct \( l_1, \ldots, l_k; P \) such that \( \tilde{S}_P(1): \frac{b+c}{\gcd(b,c)} \). In order to do this we will prove the following proposition:

**Proposition 3.** Let \( \frac{b+c}{\gcd(b,c)} = q_1^{l_1} \cdots q_s^{l_s} \) - be the decomposition of \( \frac{b+c}{\gcd(b,c)} \) into prime multiples. There exist \( l'_{i,1}, \ldots, l'_{i,k} \) such that for each nonnegative integer \( l_1, \ldots, l_k \) and \( P > 1 \) which satisfy the following conditions:

1) \( l_j \equiv l'_{i,j} \mod q_i^{l_i} \) when \( q_i > 2 \),
2) \( l_j \equiv l'_{i,j} \mod 2q_i^{l_i+1} \) when \( q_i = 2 \),
3) \( M = \max(l_1, \ldots, l_k) > q_i^{l_i+1} \).
4) \( P : q_i^{l_i} \) when \( q_i > 2 \),
5) \( P : 2q_i^{l_i+1} \) when \( q_i = 2 \),

it holds that \( \tilde{S}_P(1): q_i^{l_i} \).

First let us make sure that the \( ^{n \Leftrightarrow} \) part of lemma 2 follows from proposition 3. It is enough to apply the Chinese remainder theorem: if \( \frac{b+c}{\gcd(b,c)} \) is odd, one can take \( P = \prod_{i=1}^{k} q_i^{l_i} = \frac{b+c}{\gcd(b,c)} \); if \( \frac{b+c}{\gcd(b,c)} \) is even, one can take \( P = 2 \prod_{i=1}^{k} q_i^{l_i} = 2 \frac{b+c}{\gcd(b,c)} \). Next, one can take arbitrary \( l_1, \ldots, l_k \) such that \( l_j \equiv l'_{i,j} \mod q_i^{l_i} \) when \( q_i > 2 \) and \( l_j \equiv l'_{i,j} \mod 2q_i^{l_i+1} \) when \( q_i = 2 \), then \( \tilde{S}_P(1): \frac{b+c}{\gcd(b,c)} \). Increasing some of \( l_i \) by \( P \) a sufficient number of times, one can satisfy the condition 3).

**Proof of proposition 3.** If \( q_i > 2 \), then \( b + c - 2k \equiv \frac{b+c}{q_i^{l_i}} \mod 2 \) and by the conditions of the lemma 2 \( b + c - 2k \leq \frac{b+c}{q_i^{l_i}} \), therefore, set the values of \( l'_{i,j} \) (in arbitrary order) so that there are \( \frac{b+c}{2q_i^{l_i}} - \frac{b+c-2k}{2} \) zeros among them, and for each integer \( r \geq 1 \), \( r \leq q_i^{l_i-1} \) among \( l'_{i,j} \) there are \( \frac{b+c}{q_i^{l_i}} \) values, equal to \( r \) among them. In total there are exactly

\[
\frac{b + c}{2q_i^{l_i}} - \frac{b + c - 2k}{2} + \frac{q_i^{l_i} - 1}{2} \cdot \frac{b + c}{q_i^{l_i}} = k
\]
values. Then it will hold that (here $M' = M - \frac{q_i^{t_i} - 1}{2}$)

$$A(x) \equiv \frac{b + c}{q_i^{t_i}} (x^{M} \sum_{r=1}^{q_i^{t_i} - 1} (x^r + x^{-r}) + x^{M}) = \frac{b + c}{q_i^{t_i}} x^{M'} \sum_{r=0}^{q_i^{t_i} - 1} x^r$$

$$= \frac{b + c}{q_i^{t_i}} x^{M'} \prod_{j=1}^{t_i} \Phi_{q_i}(x) \pmod{x^{q_i^{t_i}} - 1},$$

since $\prod_{j=1}^{t_i} \Phi_{q_i}(x) = \prod_{j=0}^{q_i^{t_i} - 1} \phi_{q_i}(x)/(x - 1) = \frac{x^{q_i^{t_i} - 1}}{x - 1} = \sum_{r=0}^{q_i^{t_i} - 1} x^r$. Hence,

$$A(x) \mod \prod_{j=1}^{t_i} \Phi_{q_i}(x)$$

and consequently also $\tilde{S}_p(x) \mod \prod_{j=1}^{t_i} \Phi_{q_i}(x)$. Taking into account the fact that $\Phi_{q_i}(1) = q_i$ when $j > 0$, we obtain that when $P: q_i^{t_i}$ it holds that $\tilde{S}_p(1); q_i^{t_i}$ as required.

Now consider the case when $q_i = 2$, but $\frac{b+c}{2^{t_i}}$ is even. Then $b + c - 2k \equiv \frac{b+c}{2^{t_i}} (mod 2)$, and by the conditions of the lemma $2b + c - 2k \leq \frac{b+c}{2^{t_i}}$, therefore, set $l'_{i,j}$ so that:

I) There are $\frac{b+c}{2^{t_i}} - \frac{b+c - 2k}{2}$ zeros among them.

II) For each integer $r \geq 1$, $r \leq 2^{t_i-1} - 1$ there are $\frac{b+c}{2^{t_i}}$ values equal to $r$ among $l'_{i,j}$.

III) The value $2^{t_i-1}$ appears $\frac{b+c}{2^{t_i}}$ times.

In total we get exactly

$$\frac{b+c}{2^{t_i}} = \frac{b+c - 2k}{2} + (2^{t_i-1} - 1) \cdot \frac{b+c}{2^{t_i}} + \frac{b+c}{2^{t_i+1}} = k$$

values. Next we can proceed absolutely analogously to the above case: it will hold that (here $M' = M - (2^{t_i-1} - 1)$)

$$A(x) \equiv \frac{b + c}{2^{t_i}} (x^{M} \sum_{r=1}^{2^{t_i-1} - 1} (x^r + x^{-r}) + x^{M+2^{t_i-1}} + x^{M}) = \frac{b + c}{2^{t_i}} x^{M'} \sum_{r=0}^{2^{t_i-1} - 1} x^r = \frac{b + c}{2^{t_i}} x^{M'} \prod_{j=1}^{t_i} \Phi_{2j}(x) \pmod{x^{2^{t_i}} - 1},$$

as $\prod_{j=1}^{t_i} \Phi_{2j}(x) = \prod_{j=0}^{t_i} \Phi_{2j}(x)/(x - 1) = \frac{x^{2^{t_i} - 1}}{x - 1} = \sum_{r=0}^{2^{t_i} - 1} x^r$. Hence, $A(x) \mod \prod_{j=1}^{t_i} \Phi_{2j}(x)$.
and consequently also $\tilde{S}_P(x): \prod_{j=1}^{t_i} \Phi_{2j}(x)$. Taking into consideration the fact that $\Phi_{2j}(1) = 2$ when $j > 0$, we obtain that for $P:2t_i$ it holds that $\tilde{S}_P(1):2t_i$ as required.

Finally consider the case when $q_i = 2$ and $\frac{b+c}{2t_i}$ is odd: from the conditions of the lemma combined with the fact that $b+c-2k$ is even, we obtain $b+c-2k \leq \frac{b+c}{2t_i} - 1$. Introduce the polynomial

$$R(x) = \left(\frac{b+c}{2t_i} - 1\right) \sum_{j=0}^{2t_i-1} x^{2j} + \sum_{j=0}^{2t_i-1} x^{2j+1} =$$

$$\left(\frac{b+c}{2t_i} - 1 + x\right) \sum_{j=0}^{2t_i-1} x^{2j} = \left(\frac{b+c}{2t_i} - 1 + x\right) \prod_{j=1}^{t_i} \Phi_{2j+1}(x),$$

as $\prod_{j=1}^{t_i} \Phi_{2j+1}(x) = \prod_{j=0}^{t_i+1} \Phi_{2j}(x)/\prod_{j=0}^{1} \Phi_{2j}(x) = \frac{x^{2^{t_i+1}}-1}{x^{2t_i}-1} = \sum_{j=0}^{2t_i-1} x^{2j}$. Since $\Phi_{2j}(1) = 2$ when $j > 0$, in order for $\tilde{S}_P(1):2t_i$ to be satisfied it is enough to take $P:2t_i+1$ and $l'_{i,1}, ..., l'_{i,k}$ such that

$$A(x) \equiv x^{M}R(x) \mod x^{2t_i+1} - 1).$$

One can achieve this by taking as $l'_{i,j}$:

I) $(\frac{b+c}{2t_i} - 1 - (b+c-2k))/2$ values equal to 0 (it is possible since $\frac{b+c}{2t_i} - 1 - (b+c-2k)$ is even and nonnegative).

II) All the values of the form $2j+1$, where $0 \leq j \leq 2^{t_i-1} - 1$, one time each.

III) All the values of the form $2j$, where $1 \leq j \leq 2^{t_i-1} - 1$, $\frac{b+c}{2t_i} - 1$ times each.

IV) The value $2^t_i \cdot (\frac{b+c}{2t_i} - 1)/2$ times.

Indeed, in total there are

$$(\frac{b+c}{2t_i} - 1 - (b+c-2k))/2 + 2t_i-1 + (\frac{b+c}{2t_i} - 1)(2^{t_i-1} - 1) + (\frac{b+c}{2t_i} - 1)/2 = k.$$
values. Next, we obtain

\[ x^M R(x) \equiv x^M \left( \frac{b + c}{2^t_i} - 1 \right) + x \left( 1 + x^2 + x^4 + \ldots + x^{2^i+1} - 2 \right) \equiv \]

\[ x^M \left( \frac{b + c}{2^t_i} - 1 \right) + \sum_{j=0}^{2^i+1-1} (x^{2j+1} + x^{-2j-1}) + \left( \frac{b + c}{2^t_i} - 1 \right) \sum_{j=1}^{2^i+1-1} (x^{2j} + x^{-2j}) + \]

\[ (x^{2^i} + x^{-2^i}) \left( \frac{b + c}{2^t_i} - 1 \right) / 2 \equiv A(x) \pmod{x^{2^i+1}} \]

Thus, lemma 2 and consequently (as shown in Section 2) theorem 2 is proven.

Proof of theorem 3. "⇒": follows from theorem 2.
"⇐": apply lemma 2 construct the corresponding \( P; l_1, \ldots, l_k \). One can assume that \( P = q^{s'} \) for some \( s' > 0 \). Then by lemma 3 it holds that \( \tilde{S}_P(1); \frac{b+c}{\gcd(b,c)} \), and then by point 2) of theorem 1 the circulant graph with distances \( l_1, \ldots, l_k \) has a \( P \)-periodic perfect 2-colouring with parameters \( (b, c) \).

References

[1] D.B. Khoroshilova, On two-color perfect colorings of circular graphs [Russian], Diskretn. Anal. Issled. Oper., 16:1 (2009), 80-92.

[2] D.B. Khoroshilova, On the parameters of perfect 2-colorings of circulant graphs [Russian], Diskretn. Anal. Issled. Oper., 18:6 (2011), 82–89.

[3] O.G. Parshina, Perfect 2-colorings of infinite circulant graphs with a continuous set of distances, J. Appl. Industr. Math., 8:3 (2014), 357–361.

[4] M.A. Lisitsyna and O.G. Parshina, Perfect colorings of the infinite circulant graph with distances 1 and 2, J. Appl. Industr. Math., 11:3 (2017), 381–388.
[5] O. G. Parshina, M. A. Lisitsyna, *The perfect 2-colorings of infinite circulant graphs with a continuous set of odd distances*, Sib. Elektron. Mat. Izv., 17 (2020), 590–603

[6] S.V. Avgustinovich, M.A. Lisitsyna, *Perfect 2-colorings of transitive cubic graphs*, J. Appl. Industr. Math., 5:4 (2011), 519–528.

[7] M.A. Lisitsyna, S.V. Avgustinovich, *Perfect colorings of the prism graph* [Russian], Siberian Electronic Mathematical Reports 13 (2016), 1116–1128.

[8] E. Coven, A. Meyerowitz, *Tiling the integers with translates of one finite set*, Journal of Algebra, 212:1 (1999), 161-174

[9] R. D. Malikiosis, M.N. Kolountzakis, *Fuglede’s conjecture on cyclic groups of order $p^n q$*, Discrete Analysis, 2017:12, 16 pp.

[10] G. Kiss, R. D. Malikiosis, G. Somlai, M. Vizer, *On the discrete Fuglede and Pompeiu problems*, 13:3 (2020), 765-788

[11] A. Granville, I. Laba, Y. Wang, *On finite sets which tile the integers* (2001), https://www.math.ust.hk/ yangwang/Preprints/t2.pdf

[12] E. Amiot, *Rhythmic canons and Galois theory*, Grazer Math. Ber. 347 (2005), 1-25

[13] R. D. Malikiosis, *On the structure of spectral and tiling subsets of cyclic groups*, 2020, Arxiv preprint, https://arxiv.org/pdf/2005.05800.pdf

[14] P. Delsarte, An Algebraic Approach to the Association Schemes of Coding Theory, Philips Research Reports Supplements, vol. 10, N.V. Philips’ Gloeilampenfabrieken, Eindhoven, 1973