FINITE ORTHOGONAL GROUPS AND PERIODICITY OF LINKS

MACIEJ BORODZIK, PRZEMYSŁAW GRABOWSKI, ADAM KRÓL, AND MARIA MARCHWICKA

Abstract. For a prime number $q \neq 2$ and $r > 0$ we study, whether there exists an isometry of order $q^r$ acting on a free $\mathbb{Z}_p^k$-module equipped with a scalar product. We investigate, whether there exists such an isometry with no non-zero fixed points. Both questions are completely answered in this paper if $p \neq 2$, $q$. As an application we refine Naik’s criterion for periodicity of links in $S^3$. The periodicity criterion we obtain is effectively computable and gives concrete restrictions for periodicity of low-crossing knots.

1. Introduction

Let $L \subset S^3$ be a link. We say that $L$ is $m$-periodic if there exists an orientation-preserving diffeomorphism $\phi: S^3 \to S^3$ such that $\phi^m = id$, $\phi^j \neq id$ for $j < m$, $\phi(L) = L$ and $L$ is disjoint from the rotation axis of $\phi$. One asks which links are periodic and how is the periodicity reflected in the symmetry of link invariants.

Classical obstructions to knot periodicity include [5,6,10–12,14,16,17]. Several new criteria appeared recently, based mostly on homological invariants, like [1,7,13], but also on the study of fundamental groups [3].

Among known periodicity criteria, the criterion of Naik [12] is very effective in obstructing periodicity. It relies on an elementary observation that if $L$ is $m$-periodic, then the $\mathbb{Z}_m$-symmetry of the link induces a $\mathbb{Z}_m$ action on the homology of a branched cover, and this action preserves the linking form. A non-trivial result relates the fixed point set of the action to the homology of the quotient. Naik’s criterion relies on understanding, which finite abelian groups (or which linking forms) admit an action with no non-zero fixed points; see Section 2 for more details. The goal of this article is to strengthen Naik’s criterion.

Before we state our main result, let us introduce some terminology.

Definition 1.1. Let $p$ be a prime number and $m$ an odd number coprime with $p$. We denote by $[m|p]$ the minimal positive exponent $s$ such that either $m|(p^s - 1)$ or $m|(p^s + 1)$. We define $\eta(m) = 1$ if $m|(p^{|[m|p]} - 1)$ and $\eta(m) = -1$ if $m|(p^{|[m|p]} + 1)$.

Remark 1.2. We note that $\eta(m) = -1$ if and only if $p$ is a root of $-1$ in $\mathbb{Z}_m$, that is, if some power of $p$ is equal to $-1$ in $\mathbb{Z}_m$. Moreover, for any $n > 0$, $m$ divides $p^{n|p|} - \eta(m)^n$.

We recall also that if $p \neq 2$ and $k > 0$, a free $\mathbb{Z}_{p^k}$-module of rank $n$ can be equipped with two non-equivalent symmetric bilinear forms with values in $\mathbb{Z}_{p^k}$, these are distinguished by a sign $\epsilon$, which we introduce rigorously in Definition 3.5.

Our new criterion is based on a result that gives even more understanding of cyclic group actions on linking (or bilinear) forms. We believe that it is of independent interest.

Date: October 10, 2018.

2010 Mathematics Subject Classification. primary: 57M25.

Key words and phrases. periodic links, linking forms, orthogonal groups.
Theorem 1.3. Let $p \neq q$ be odd prime numbers. Let $B$ be a free $\mathbb{Z}_p^k$-module of rank $n > 0$, for some $k > 0$. Let $\beta : B \times B \to \mathbb{Z}_p^k$ be a non-degenerate symmetric bilinear form. Let $s$ be the maximal integer such that $q^s | \frac{p^n}{(p^2 - 1)}$. Fix an integer $r > 0$ and set $\tilde{r} = \max(r - s, 0)$.

(a) There exists an isometry of $(B, \beta)$ of order $q^r$ if and only if $n \geq 2[q|p]|q^{\tilde{r}} + 1$, or $n = 2[q|p]|q^{\tilde{r}}$ and $\epsilon(B, \beta) = \eta(q)$.

(b) There exists an isometry of $(B, \beta)$ of order $q^r$ with no non-zero fixed points if and only if $n = 2[q|p]d$ for $d \geq q^{\tilde{r}}$ and $\epsilon(B, \beta) = \eta(q)^d$.

The proof of Theorem 1.3 stretches for Sections 3–8. Sections 3–6 deal with part (a), while Sections 7 and 8 take care with part (b).

In more detail, in Section 3 we recall the Wall’s result on classification of symmetric bilinear forms on free $\mathbb{Z}_p^k$-modules. We recall the definition of the index $\epsilon(B, \beta)$, which is crucial in our applications. In Section 4 we recall a classical result on the rank of the group of isometries of a symmetric bilinear form on a $\mathbb{Z}_p$-module. We introduce an important concept of a (mod $p$)-reduction, which allows us to translate various results on forms on $\mathbb{Z}_p$-modules to forms on $\mathbb{Z}_p^k$-modules for $k > 1$. One of such results is the calculation of the Sylow $q$-group of isometries by Weir [20], stated in Section 5, which is shown to hold for isometries of forms on $\mathbb{Z}_p^k$-modules by Theorem 5.2.

The description of the Sylow $q$-groups in Theorem 5.5 is given in terms of the wreath product, see Definition 5.3. In Section 6 we use an elementary properties of the wreath product to find the maximal $r$ such that the Sylow $q$-group of the group of isometries contains an element of order $q^r$. Section 6 is concluded with Theorem 6.2 which contains the (a) part of Theorem 1.3.

Part (b) of Theorem 1.3 is proved in Sections 7 and 8. It is essentially done on a case by case analysis. We begin with showing that if the conditions $n = 2[q|p]d$, $d \geq q^\tilde{r}$ and $\epsilon(B, \beta) = \eta(q)^d$ are not satisfied, then any isometry of order $q^\tilde{r}$ must have a non-zero fixed point. This is the statement of Theorem 7.1 in Section 7. Section 8 is devoted to a construction of an isometry with non-zero fixed points. We perform the construction separately in the case $\tilde{r} = r - s$ and in the case $\tilde{r} = 0$ (i.e. $r \leq s$). The key results are Lemmas 8.3 and 8.7 which show that if $n = 2[q|p]|q^{s-r}$ and $\epsilon(B, \beta) = \eta(q)^{q^{-s}}$, then every isometry of order $q^{s-r}$ has only zero as its fixed point. Lemma 8.3 deals with the case of $\mathbb{Z}_p$-forms and Lemma 8.7 takes care of general $\mathbb{Z}_p^k$-forms via the (mod $p$)-reduction. Lemma 8.8 deals with the case $\tilde{r} = 0$, but the key argument is essentially the same as in Lemma 8.3. The three lemmas are used to give a proof of Theorem 8.1. This theorem concludes the proof of Theorem 1.3.

The main application of Theorem 1.3 in our paper is the following refinement of Naik’s theorem [12, Theorem 5].

Theorem 1.4. Let $L$ be a $q^r$-periodic link with $r \geq 1$ and $q$ an odd prime. Let $T_p$ be the $p$-torsion subgroup of $H_1(\Sigma_k(L); \mathbb{Z})$, where $\Sigma_k(L)$ is a $k$-fold branched cyclic cover for $k > 1$ and $p \neq q$ an odd prime.

(a) If $T_p$ is non-trivial, then $T_p$ splits as an sum $T_{p,1} \oplus T_{p,2} \oplus \ldots$ of pairwise orthogonal summands. A summand $T_{p,i}$ is a free $\mathbb{Z}_p^r$-module with linking form $\lambda_{p,i}$. The $\mathbb{Z}_p^r$-symmetry of $L$ yields an action of $\mathbb{Z}_p^r$ on $T_p$ preserving the orthogonal splitting.

(b) Suppose the first homology of the $k$-fold cover of the quotient link $\Sigma_k(L/\mathbb{Z}_q^r)$ has no $p$-torsion. If $T_{p,i}$ is non-trivial, then there exists an integer $d_i \geq q^{s-r}$ such that $\text{rank} \ T_{p,i} = 2[q|p]|d_i$ and $\epsilon(T_{p,i}) = \eta(q)^{d_i}$. 


**Proof.** Part (a) is proved as Proposition 2.3. To prove part (b) we use Proposition 2.2 to conclude that \( \mathbb{Z}_q^r \) acts on \( T_p \) with no non-zero fixed points. Then by part (a) we know that \( \mathbb{Z}_q^r \) acts on each of the \( T_{p,i} \) preserving the linking form and with no non-zero fixed points.

Now \( T_{p,i} \) is a free \( \mathbb{Z}_q^r \)-module and by the results of Section 3 a linking form \( T_{p,i} \times T_{p,i} \rightarrow \mathbb{Q}/\mathbb{Z} \) induces a symmetric bilinear form on \( T_{p,i} \) with values in \( \mathbb{Z}_q^r \). Isometries of the linking form are isometries of the symmetric bilinear forms, see Lemma 3.1. Thus we obtain an action of \( \mathbb{Z}_q^r \) on \( T_{p,i} \) equipped with a symmetric bilinear form, the action is by isometries and with no non-zero fixed points. We conclude by Theorem 1.3. \( \square \)

Our result extends [12, Theorem 5] in the following two ways.

- While Naik’s result deals with links admitting a \( \mathbb{Z}_q \)-action with \( q \) prime, we extend it to links that admit an action of \( \mathbb{Z}_q^r \) for \( r > 1 \).
- Our new condition \( \epsilon(T_{p,i}) = \eta(q)^d \) rules out approximately half of linking forms that can appear as linking forms of a periodic link such that the quotient has no \( p \)-torison.

This is a substantial strengthening of Naik’s criterion, as shown in Section 11.

**Example 1.5.** As explained in detail in Section 11, the knots 13n3659, 14n908, 14n913, 14n2451, 14n2458, 14n6565, 14n9035, 14n11989, 14n14577, 14n23051 and 14n24618 pass Naik’s periodicity criterion for period 3, but are shown not to be 3-periodic by Theorem 1.3. Section 9 shows an explicit way of applying Theorem 1.4 to obstruct periodicity. An elaborated example of a knot that actually passes the criterion is given in Section 10.

**Acknowledgments.** The authors would like to thank Jan Okniński for helpful discussions and for pointing us the article of Weir. They are also grateful to Wojciech Polarczyk for fruitful conversations and to Chuck Livingston for his comments on the early draft of the paper. MB, PG, AK and MM are supported by the National Science Center grant 2016/22/E/ST1/00040.

## 2. Review of Naik’s criterion

Let \( L \) be an \( m \)-periodic link and let \( L/\mathbb{Z}_m \) be the quotient link. For \( k > 1 \) consider the branched covers \( \Sigma_k(L) \) and \( \Sigma_k(L/\mathbb{Z}_m) \). We write \( \Sigma(L), \Sigma(L/\mathbb{Z}_m) \) instead of \( \Sigma_2(L) \) and \( \Sigma_2(L/\mathbb{Z}_m) \).

For simplicity we will always assume that \( k \) is such that \( \Sigma_k(L) \) is a rational homology sphere. In particular, there is a non-degenerate linking form \( H_1(\Sigma_k(L); \mathbb{Z}) \times H_1(\Sigma_k(L); \mathbb{Z}) \rightarrow \mathbb{Q}/\mathbb{Z} \).

We have the following observation, see [11, Section 2].

**Lemma 2.1.** An action of \( \mathbb{Z}_m \) on \( S^3 \) that preserves \( L \) and whose fixed points are disjoint from \( L \), lifts to an action of \( \mathbb{Z}_m \) on \( \Sigma_k(L) \). The quotient \( \Sigma_k(L)/\mathbb{Z}_m \) is diffeomorphic to the branched cover \( \Sigma_k(L/\mathbb{Z}_m) \) of the quotient link.

The following result relates Lemma 2.1 with the group action on homology.

**Proposition 2.2** (see [11, Proposition 2.5]). If \( p \) is a prime number, \( p \nmid m \) and \( \phi: \Sigma_k(L) \rightarrow \Sigma_k(L) \) is a generator of the action of \( \mathbb{Z}_m \) on \( \Sigma_k(L) \), then \( \phi^* \) is an isometry of \( H_1(\Sigma_k(L)) \) (with respect to the linking form) and the fixed point set

\[
\text{Fix } \phi^* : H_1(\Sigma_k(L))_p \rightarrow H_1(\Sigma_k(L))_p
\]

is equal to \( H_1(\Sigma_k(L/\mathbb{Z}_m))_p \). Here the subscript \( p \) denotes the \( p \)-primary part.
Proposition 2.2 is non-trivial and the condition $p \nmid m$, in general cannot be relaxed. For example, if $K = T(2, 5)$, then $K$ is clearly 5-periodic. We have $H_1(\Sigma_2(K)) = \mathbb{Z}_5$. The only action of $\mathbb{Z}_5$ on $\mathbb{Z}_5$ by isometries is trivial (because any isometry of $\mathbb{Z}_5$ has order 1 or 2), hence $\mathbb{Z}_5$ is a fixed subspace of this action. However the quotient knot $K/\mathbb{Z}_5$ is trivial, $H_1(\Sigma_2(K/\mathbb{Z}_5); \mathbb{Z}) = 0$.

In order to apply Proposition 2.2 we use the following result.

**Proposition 2.3.** For an odd prime number $p$, that is coprime with $m$, the group $T = H_1(\Sigma_k(L))_p$ decomposes as a sum $T_{p,1} \oplus T_{p,2} \oplus \ldots$, where each of the $T_{p,i}$ is a free $\mathbb{Z}_p$-module. The decomposition is orthogonal with respect to the linking form. Moreover, if $\mathbb{Z}_m$ acts on $T$ by isometries, then the decomposition can be made invariant with respect to this action.

**Proof.** The result is rather standard, we present a quick proof for the reader’s convenience. Write $T = H_1(\Sigma_k(L))_p$ and consider the linking form $\lambda: T \times T \to \mathbb{Q}/\mathbb{Z}$.

For an element $x \in T$ let $r(x)$ be the minimal positive integer such that $p^{r(x)}x = 0 \in T$. Take $x \in T$ for which $r(x)$ is maximal possible. As $\lambda$ is non-degenerate, there exists $y \in T$ such that $p^{r(x)-1}\lambda(x, y) \neq 0 \in \mathbb{Q}/\mathbb{Z}$, in fact, if for all $y \in T$ we have $p^{r(x)-1}\lambda(x, y) = 0$, then $p^{r(x)-1}x = 0$ pairs trivially with all $y \in T$, contradicting non-degeneracy of $\lambda$. Note also that we have $r(y) = r(x)$.

Consider now $p^{r(x)-1}\lambda(x, x)$, $p^{r(x)-1}\lambda(y, y)$ and $p^{r(x)-1}\lambda(x+y, x+y)$. If all three expressions are zero in $\mathbb{Q}/\mathbb{Z}$, we conclude that $p^{r(x)-1}\lambda(x, y) = 0$ contradicting the assumptions (here we use the assumption that 2 is invertible modulo $p$). Thus there is an element $z \in T$ such that $r(z)$ is maximal possible and $p^{r(z)-1}\lambda(z, z) \neq 0$.

Let $T_z$ be the $\mathbb{Z}$-submodule of $T$ generated by $z, \phi(z), \ldots, \phi^{m-1}(z)$. The number of generators of $T_z$ is equal to $n_z$, where $n_z$ is the minimal $n$ such that $\phi^n(z)$ belongs to the subgroup generated by $z, \phi(z), \ldots, \phi^{m-1}(z)$. We have an isomorphism of $\mathbb{Z}$-modules $T_z \cong \mathbb{Z}_p^{m_z}$, in particular $T_z$ is a free $\mathbb{Z}_p^{r(z)}$-module.

Let $T'$ be the orthogonal complement of $T_z$ in $T$. As the linking form is invariant under $\phi$, and $T_z$ is invariant, $T'$ is also invariant.

Now $T'$ has smaller number of generators than $T$ and we repeat the procedure to split off another orthogonal component from $T'$. As a result of a recursive application of the procedure, we present $T$ as an orthogonal sum of modules $T_{z_1} \oplus \cdots \oplus T_{z_m}$. We set

$$T_{p,i} = \bigoplus_{j: r(z_j) = i} T_{z_j}. \quad \square$$

Next result gives a number theoretical contribution to Proposition 2.2. It is due to Davis [4], see also [12].

**Theorem 2.4.** If $q$ is a prime number different than 2 and $p$, and $\mathbb{Z}_q$ acts on $T_{p,i}$ with no non-zero fixed points by isometries, then the rank of $T_{p,i}$ as a $\mathbb{Z}_p$-module is a multiple of $2[q/p]$.

Theorem 1.3 of the present paper is a generalisation of Theorem 2.4.

The condition described in Theorem 2.4 requires some knowledge of fixed point set of the action of $\mathbb{Z}_q$. By Proposition 2.2 this fixed point set is the homology of the cover of the quotient link. As explained in [11][12] it is often possible to check whether $H_1(\Sigma_k(L/\mathbb{Z}_q); \mathbb{Z})_p = 0$ using Murasugi’s criterion, which we now recall.
Theorem 2.5 (Murasugi’s criterion for knots, see [10]). Suppose $K \subset S^3$ is a $q^r$-periodic knot with $q$ prime and $r > 0$. Let $\Delta$ be the Alexander polynomial of $K$ and $\Delta'$ be the Alexander polynomial of the quotient knot $K' = K/\mathbb{Z}_q$. Let $\ell$ be the absolute value of linking number of $K$ with the symmetry axis. Then $\Delta' q^{r} \Delta$ and up to multiplication by a power of $t$ we have
\begin{equation}
\Delta = \Delta' q^{r} (1 + t + \ldots + t^{\ell-1})^{q-r-1} \mod q.
\end{equation}

There are various versions of Murasugi’s criterion for links, see [15], [18, Theorem 1.10.1], the precise statements depend on the action of the symmetry group on the set of components of the symmetric link.

Naik’s homological criterion relies on combining Proposition 2.2, Theorem 2.4, and Murasugi’s criterion (Theorem 2.5). We will show two such combinations, both due to Naik [12]. As Propositions 2.7 and 2.8 are instructive and indicate how Theorem 1.3 can be applied, we include short proofs, not claiming any originality.

Proposition 2.7. Let now $L$ be a $q$-periodic link with $q$ prime. Let $\Delta$ be the Alexander polynomial of $L$. Suppose $\Delta'$ is the Alexander polynomial of the quotient. For any prime number $p \neq 2, q$, if $s = s(p)$ is a maximal positive integer such that $p^s$ divides $\Delta(1)/\Delta'(-1)$, then $s$ is a multiple of $2[q,p]$.

Proof. Let $T$ be the $p$-torsion part of $H_1(\Sigma(L); \mathbb{Z})$. The rank of $T$ is equal to $p^{s_0}$, where $s_0$ is the maximal positive integer such that $p^{s_0}$ divides $|H_1(\Sigma(L); \mathbb{Z})| = |\det(L)| = |\Delta(1)|$.

By Proposition 2.2, the fixed point set of the $\mathbb{Z}_q$ action has rank equal to $|H_1(\Sigma(L)/\mathbb{Z}_q); \mathbb{Z})| = |\Delta'(-1)|$. Therefore the action of $\mathbb{Z}_q$ on $H_1(\Sigma(L); \mathbb{Z})_p$ induces an action on the quotient $H_1(\Sigma(L); \mathbb{Z})/H_1(\Sigma(L)/\mathbb{Z}_q); \mathbb{Z})_p$ with only trivial fixed points, which has rank $p^s$. We conclude by Theorem 2.4. \hfill $\square$

Proposition 2.8. Let $L$ be a $q$-periodic link and suppose $\Delta'$ is the Alexander polynomial of the quotient. If $p \neq 2, q$ is a prime number such that $p$ does not divide $\Delta'(-1)$, then the $p$-torsion part $H_1(\Sigma(L); \mathbb{Z})_p$ decomposes as an orthogonal sum of modules $T_{p,1}, \ldots$, where each of the $T_{p,i}$ is a free $\mathbb{Z}_{p^i}$-module, whose rank is divisible by $2[q,p]$.

Proof. The assumptions of the proposition imply via Proposition 2.2 that $\mathbb{Z}_q$ acts on $H_1(\Sigma(L); \mathbb{Z})_p$ with no non-zero fixed points. We conclude by Theorem 2.4. \hfill $\square$

While Propositions 2.7 and 2.8 do not exhaust potential applications of Naik’s criterion, they give a very good balance between applicability and generality. We show the result of implementing Proposition 2.7 and Proposition 2.8 in Section 1.1.

3. Linking forms and symmetric forms

Let $L$ be an $m$-periodic link and suppose $k > 1$ is such that $\Sigma_k(L)$ is a rational homology sphere. We let $T$ denote the group $H_1(\Sigma_k(L); \mathbb{Z})$. Finally, let $\lambda : T \times T \rightarrow \mathbb{Q}/\mathbb{Z}$ be the linking form.

For a prime number $p$ we write $T_p$ for the $p$-torsion part of $T$, so that $T = \bigoplus T_p$, where the sum is over all prime numbers $p$. The summands are pairwise orthogonal with respect to the linking form. In order to study the linking form on $T_p$ in more detail, we split $T_p$ into forms $T_{p,k}$ according to Proposition 2.3. Each of the $T_{p,k}$ is a free $\mathbb{Z}_{p^k}$-module and the linking form restricts over $T_{p,k}$ to a form
\[\lambda : \mathbb{Z}_{p^k}^n \times \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z},\]
where \( n \) is the rank of \( T_{p,k} \).

Let \( \lambda: \mathbb{Z}_{p,k}^n \times \mathbb{Z}_{p,k}^n \to \mathbb{Q}/\mathbb{Z} \) be a non-degenerate linking form. As for any \( x, y \in \mathbb{Z}_{p,k}^n \) we have \( p^k x = 0 \), we infer that \( p^k \lambda(x, y) = 0 \in \mathbb{Q}/\mathbb{Z} \). It follows that

\[
\lambda(x, y) = \frac{\beta(x, y)}{p^k}
\]

for some \( \beta(x, y) \in \mathbb{Z} \) well-defined modulo \( p^k \). The following fact does not require a proof.

**Lemma 3.1.** The form \( \beta(x, y): \mathbb{Z}_{p,k}^n \times \mathbb{Z}_{p,k}^n \to \mathbb{Z}_{p,k} \) is a symmetric, non-degenerate bilinear form. Moreover any automorphism \( \psi \) preserving the linking form is an isometry of the bilinear form \( \beta \). Conversely, any isometry of the bilinear form \( b \) gives an automorphism of the linking form.

Lemma 3.1 gives a translation from linking forms to symmetric bilinear forms. The reverse passage is also possible, a form \( \beta(x, y) \) induces a linking form \( \lambda(x, y) = \beta(x, y)/p^k \). In particular the classification and the symmetries of linking forms correspond to the classification and the symmetries of bilinear forms.

**Definition 3.2.** A \( p^k \)-form or, if the context is clear, simply a form, is a pair \( (B, \beta) \), where \( B \) is a free and finitely generated \( \mathbb{Z}_{p,k} \)-module and \( \beta: B \times B \to \mathbb{Z}_{p,k} \) is a symmetric non-degenerate bilinear form. The rank of the form is the rank of \( B \) as a \( \mathbb{Z}_{p,k} \)-module.

The classification of \( p^k \)-forms is well-known, we recall a classical result of Wall [19], see also [8].

**Theorem 3.3.** Let \( p > 2 \) be a prime, \( k, n > 0 \). Any \( p^k \)-form of rank \( n \) is isometric to one of the two following diagonal forms:

- the standard form, having \( +1 \) on the diagonal, i.e. \( \beta(x, y) = \sum x_i y_i \), where \( x = (x_1, \ldots, x_n) \), \( y = (y_1, \ldots, y_n) \);
- the non-standard form, \( \beta(x, y) = \tau x_1 y_1 + \sum_{i > 1} x_i y_i \), where \( \tau \) is not a square modulo \( p^k \).

**Remark 3.4.** It is an immediate consequence of Theorem 3.3 that for every \( p^k \)-form \( (B, \beta) \) of rank \( n \) there exists a basis \( x_1, \ldots, x_n \) of \( B \), such that \( \beta(x_i, x_j) = c_i c_j \) and \( c_i = 1 \) for \( i = 2, \ldots, n \), while \( c_1 = 1 \) if the form is standard, and \( c_1 \) is not a square modulo \( p^k \) if the form is not standard.

We will now introduce a notion of an index of a \( p^k \)-form, which distinguishes the standard form from the non-standard one. For reasons that will become clear later, the index of a standard form is not always equal to \( +1 \), a correction term (denoted by \( \epsilon_2 \) below) depending on the rank and the prime number \( p \) is needed.

**Definition 3.5.** If \( (B, \beta) \) is a \( p^k \)-form of rank \( n \), the index \( \epsilon(B, \beta) \) (written also \( \epsilon(B) \) if no risk of confusion arises) is defined as \( \epsilon_1 \epsilon_2 \), where \( \epsilon_1 = 1 \) if the form is standard (using the terminology of Theorem 3.3) and \( \epsilon_1 = -1 \) otherwise. We set \( \epsilon_2 = -1 \) if \( p \equiv 3 \mod 4 \) and \( n = 2 \mod 4 \), otherwise \( \epsilon_2 = 1 \).

If \( M \) is a free \( \mathbb{Z}_{p,k} \)-module and \( \lambda: M \times M \to \mathbb{Q}/\mathbb{Z} \) is a linking form, then the index \( \epsilon(M) \) is the index of the \( p^k \)-form associated with \( (M, \lambda) \) via Lemma 3.1.

**Remark 3.6.** In the present paper we use the index of a form to distinguish isomorphism classes of its group of isometries. By Theorem 4.2 below, the groups of isometries of forms
of odd rank do not depend on the index. Our interest will be mainly the index of a form of even rank, the index of a form of an odd rank is defined for completeness.

**Lemma 3.7.** Suppose that \((B, \beta) = (B', \beta') \oplus (B'', \beta'')\) and \(B', B''\) have even rank. Then \(\epsilon(B, \beta) = \epsilon(B', \beta') \epsilon(B'', \beta'').\)

**Proof.** Clearly \(\epsilon_1(B, \beta) = \epsilon_1(B', \beta') \epsilon_1(B'', \beta'')\). So we have to check that the same holds for \(\epsilon_2\). This is obvious if \(p \equiv 1 \mod 4\), because then \(\epsilon_2 = 1\). If \(p \equiv 3 \mod 4\), then we check \(\epsilon_2(B, \beta) = \epsilon_2(B', \beta') \epsilon_2(B'', \beta'')\) on a (trivial) case by case basis. \(\Box\)

### 4. Ranks of groups of isometries

**Definition 4.1.** For a form \((B, \beta)\) we write \(O(B)\) to be the group of isometries of \(B\). More specifically, the group \(O(p^k, n, \epsilon)\) is the group of isometries of the \(p^k\)-form of rank \(n\) with index \(\epsilon\).

We have the following result, for which we refer to the book of Wilson [21].

**Theorem 4.2.** The rank of \(O(p, n, \epsilon)\) is equal to

- \(2p^m(p^2 - 1)(p^4 - 1)\ldots(p^{2m} - 1)\) if \(n = 2m + 1\);
- \(2p^m(p^{2m - 1} - 1)(p^4 - 1)\ldots(p^{2m - 2} - 1)(p^n - \epsilon)\) if \(n = 2m\).

Moreover, if \(n\) is odd, the groups \(O(p, n, +1)\) and \(O(p, n, -1)\) are isomorphic.

We will extend Theorem 4.2 to compute the order of \(O(p^k, n, \epsilon)\) for \(k > 1\). First we need the following construction.

**Definition 4.3.** Let \((B, \beta)\) be a \(p^k\)-form. A \((\mod p)\)-reduction (or just: a reduction) of \((B, \beta)\) is a symmetric bilinear form \((B_{red}, \beta_{red})\) where \(B_{red} = B/p^{k - 1}B\) is a free \(\mathbb{Z}_p\)-module and for \(x, y \in B_{red}\) we set

\[
\beta_{red}(x, y) = \left[\beta(\tilde{x}, \tilde{y})\right] \in B/p^{k - 1}B,
\]

where \(\tilde{x}, \tilde{y} \in B\) are lifts of \(x, y\) to \(B\) and \([\cdot]\) denotes the class in the quotient.

Informally, one may think of \(B_{red}\) as \(\{B \mod p\}\) and of \(\beta_{red}\) as \(\{\beta \mod p\}\). We have an obvious observation.

**Lemma 4.4.** The form \((B_{red}, \beta_{red})\) is non-degenerate. In particular a reduction of a \(p^k\)-form is a \(p\)-form.

Let \((B, \beta)\) be a \(p^k\)-form and \((B_{red}, \beta_{red})\) be a \((\mod p)\)-reduction. Suppose \(\phi \in O(B)\). We define the isometry \(\pi(\phi) \in O(B_{red})\) by the formula

\[
(4.5) \quad \pi(\phi)(x) = [\phi(\tilde{x})],
\]

where \(x \in B_{red}\) and \(\tilde{x}\) is any lift of \(x\) to \(B\). Formula (4.5) defines a group homomorphism

\[\pi: O(B) \to O(B_{red}),\]

which is also referred to as the \((\mod p)\)-reduction of an isometry.

**Lemma 4.6.** The kernel of \(\pi\) has cardinality \(p^{(k - 1)(n)}\). The map \(\pi\) is a surjection.

**Proof.** We focus on the case where \(B\) is standard, the other case is analogous. Choose a basis \(\{\epsilon_i\}_{i=1}^n\) such that \(\beta\) is the identity matrix in this base. By \(\overline{r}_i\) we will denote the basis of \(B_{red}\) obtained by reducing the basis \(e_1, \ldots, e_n\). Take \(\phi_1 \in O(B_{red})\). Using the basis \(\overline{e}_1, \ldots, \overline{e}_n\) we represent \(\phi_1\) as a matrix \(\Phi_p\) with coefficients in \(\mathbb{Z}_p\). Choose a lift of the matrix \(\Phi_p\) to a
matrix $\Phi$ over $\mathbb{Z}$, that is, lift all the coefficients to $\mathbb{Z}$. The matrix $\Phi$ defines also a linear map $\phi: B \rightarrow B$. Obviously, $\phi$ depends on the choice of a lift of $\Phi_p$ to $\Phi$.

We want to find vectors $v_1, \ldots, v_n$ in $\mathbb{Z}_p^k$ such that $\tilde{\phi}$ defined by $\tilde{\phi}(e_i) = \phi(e_i) + pv_i$ is an isometry. Note that regardless of the choice of $v_i$ we have $\pi(\tilde{\phi}) = \pi(\phi)$. Moreover, if the vectors $v_1, \ldots, v_n$ are replaced by $v'_1, \ldots, v'_n$ such that $v_i - v'_i$ is a multiple of $p^{k-1}$, then $\tilde{\phi}$ does not change.

The map $\tilde{\phi}$ is an isometry if and only if the vectors $v_i$ satisfy the following condition for all $1 \leq i \leq j \leq n$

$$
(4.7) \quad (\phi(e_i) + pv_i)^T(\phi(e_j) + pv_j) = \delta_{ij},
$$

where $\delta_{ij}$ is the Kronecker’s delta. Here and afterwards in the proof, we write $x^Ty$ for the scalar product of $x$ and $y$, that is, for $\beta(x, y)$.

As $\phi$ is an isometry, we infer that $\phi(e_i)^T\phi(e_j) = \delta_{ij} + p\epsilon_{ij}$ for some $\epsilon_{ij}$, hence (4.7) becomes

$$
(4.8) \quad p(\epsilon_{ij} + v_i^T\phi(e_j) + \phi(e_i)^Tv_j) = 0.
$$

The equation (4.8) taken for all $i \leq j$ gives a system of $\frac{n(n+1)}{2}$ linear independent equations with $n^2$ variables: the variables are coefficients of the vectors $v_i$, which should be considered as elements of the space over $\mathbb{Z}_{p^{k-1}}$, because, as it was mentioned above, changing coordinates of $v_i$ by a multiple of $p^{k-1}$ does not change $\tilde{\phi}$.

The independence of the system (4.8) follows easily from the independence of vectors $\phi(e_j)$. The space of solutions has dimension $n^2 - \frac{n(n+1)}{2} = \binom{n}{2}$. Therefore the number of solutions is equal to $p^{(k-1)\binom{n}{2}}$ as desired. \hfill $\Box$

As a corollary we obtain the following fact.

**Corollary 4.9.** Let $B$ be a $p^k$-form of rank $n$ and $B_{\text{red}}$ its (mod $p$)-reduction. Then

$$
|O(B)| = p^{(k-1)\binom{n}{2}}|O(B_{\text{red}})|.
$$

5. SYLOW GROUPS OF THE ORTHOGONAL GROUP $O(B)$

In this section we let $q$ be a fixed odd prime number different than $p$.

**Definition 5.1.** For a group $G$, we denote by $\text{Syl}_q G$ a Sylow $q$-subgroup of $G$.

We have the following relation between Sylow groups of the orthogonal group of a form and Sylow groups of the orthogonal group of the (mod $p$)-reduction.

**Theorem 5.2.** The (mod $p$)-reduction $\pi: O(B) \rightarrow O(B_{\text{red}})$ takes a Sylow group $\text{Syl}_q O(B)$ isomorphically to a Sylow group of $O(B_{\text{red}})$.

**Proof.** To begin with $\text{Syl}_q O(B)$ has rank equal to $q^s$, where $s$ is the maximum integer such that $q^s$ divides $|O(B)|$. Likewise the rank of $\text{Syl}_q O(B_{\text{red}})$ is equal to $q^{s_1}$ for $s_1$ being the maximal positive integer such that $q^{s_1}$ divides $|O(B_{\text{red}})|$. By Corollary 4.9 we obtain $|\text{Syl}_q O(B)| = |\text{Syl}_q O(B_{\text{red}})|$.

Let now $G = \pi(\text{Syl}_q O(B))$, where $\pi: O(B) \rightarrow O(B_{\text{red}})$. Then $G$ is clearly a $q$-subgroup of $O(B_{\text{red}})$. The map $\pi|_{\text{Syl}_q O(B)}: \text{Syl}_q O(B) \rightarrow G$ is a homomorphism of groups. The kernel of $\pi|_{\text{Syl}_q O(B)}$ is a subgroup of $\text{Syl}_q O(B)$ and also a subgroup of $\ker \pi$. But $\ker \pi$ is a $p$-group.
by Lemma 4.6 and so its intersection with \( \text{Syl}_q O(B) \) is trivial. In particular \( \pi|_{\text{Syl}_q O(B)} \) is an isomorphism onto its image.

By Sylow’s theorem there exists a Sylow \( q \)-group \( H \) of \( O(B_{\text{red}}) \), such that \( G \subset H \). But \( |G| = |\text{Syl}_q O(B)| \) and \( |H| = |\text{Syl}_q O(B_{\text{red}})| = |\text{Syl}_q O(B)| \). So \( |G| = |H| \) and hence \( G = H \).

To understand the structure of \( \text{Syl}_q O(B) \) we will use Weir’s theorem [20]. We need to recall the definition of a regular wreath product.

**Definition 5.3.** Let \( H \) and \( G \) be finite groups. Let \( K = \Pi_{g \in G} H \). Let \( \psi \) be action of \( G \) on \( K \) by left multiplication of indices. We call a semidirect product of \( K \) and \( G \) a regular wreath product of \( H \) and \( G \). We denote it by \( H \ltimes G = K \rtimes \psi \).

**Remark 5.4.** The subscript \( r \) in the symbol \( \iota_r \) is not a parameter. It is a shorthand for ‘regular’.

The following result is due to Weir [20]. Note that the original statement is for \( p \)-forms. By Theorem 5.2 the result carries through to \( p^k \)-forms for general \( k \geq 1 \).

**Theorem 5.5 (see [20]).** Let \( d \) be a natural number with \( q \)-adic expansion given by \( d = a_0 + a_1 q + a_2 q^2 + \ldots \). Let \( (B, \beta) \) be a \( p \)-form of rank \( 2[q]p \) such that \( \epsilon(B) = \eta(q)^d \). Any Sylow \( q \)-subgroup of \( O(B) \) is isomorphic to:

\[
Z_{q^a_0} \times (Z_{q^a_1} \cdot \iota_1 Z_{q^a_1}) \times \cdots \times (Z_{q^a_k} \cdot \iota_k Z_{q^a_k}) \times \eta(q)^d \times \iota_{\eta(q)} Z_{\eta(q)},
\]

where \( s \) is such that \( q^s | p^{2[q]p} - 1 \) and \( q^{s+1} \not| p^{2[q]p} - 1 \).

The general case of \( (B, \beta) \) not satisfying the assumptions \( \text{rk} B = 2[q]p \), \( \epsilon(B) = \eta(q)^d \) will be reduced to Theorem 5.5. The approach is implicit in [20], but it will be used in several places in the present paper, so we sketch in briefly below.

Let \( B \) be a form of rank \( 2[q]p \) with \( 0 \leq R < 2[q]p \). We want to find a decomposition of \( B \) into an orthogonal sum of forms \( B' \) and \( B'' \) in such a way that the inclusion induced map \( O(B') \to O(B) \) (extending an isometry of \( B' \) by an identity on \( B'' \)) induces an isomorphism of Sylow \( q \)-groups and for \( B' \) the hypotheses of Theorem 5.5 are satisfied. To this end, we let \( 1_+ \) denote the one-dimensional \( p \)-form with \( \epsilon = 1 \) and \( 1_- \) denote the one-dimensional form with \( \epsilon = -1 \). We have the following possibilities:

- **Case 1:** \( R = 0 \) and \( \epsilon(B) = \eta(q)^d \). Then \( B \) already satisfies the assumptions of Theorem 5.5. We set \( B' = B \) and \( B'' = 1_+ \) (zero-dimensional).
- **Case 2:** we have \( R > 0 \). We define \( B' \) to be the unique form of rank \( 2[q]p \) for which \( \epsilon(B') = \eta(q)^d \). We let \( B'' \) to be a form of rank \( R \) that is a direct sum of \( 1_+ \) and \( 1_- \). arranged in such a way that \( \epsilon(B' \oplus B'' \oplus B''') = \epsilon(B) \). Then \( B \) and \( B' \oplus B'' \) have the same rank and the same \( \epsilon \), so they are isomorphic.
- **Case 3:** we have \( R = 0 \) but \( \epsilon(B) \neq \eta(q)^d \). We define \( B' \) to be the unique form of rank \( 2[q]p \) such that \( \epsilon(B') = \eta(q)^{d-1} \). As in the previous case we choose \( B' \) to be a direct sum of \( 2[q]p \) forms \( 1_+ \) and \( 1_- \) in such a way that \( \epsilon(B' \oplus B'' \oplus B''') = \epsilon(B) \).

**Remark 5.7.** In the above construction we do not use the fact that \( \epsilon(B' \oplus B'' \oplus B''') = \epsilon(B') \epsilon(B'') \), notice that multiplicativity of \( \epsilon \) was proved only if the summands have even rank, this is not necessarily true in Case 2 above.

**Lemma 5.8.** The inclusion \( O(B') \to O(B) \) induces an isomorphism \( \text{Syl}_q O(B') \cong \text{Syl}_q O(B) \).
Proof. Let $G$ be a Sylow $q$-group of $O(B')$. Write $i : O(B') \rightarrow O(B)$ for the inclusion induced map. Then $i(G)$ is a subgroup of $O(B)$ and as such, it is contained in some Sylow group $H$ of $O(B)$. Now $|H|/|G|$ is equal to the maximal exponent $s$ such that $q^s$ divides $|O(B)|/|O(B')|$. However, by Theorem 1.2 and Corollary 4.9, $q$ does not divide $|O(B)|/|O(B')|$. Therefore $|H|/|G| = 1$ and $i(G) \subset H$, so $i(G) = H$. 

Definition 5.9. The form $B'$ is called the maximal $q$-regular subform of $B$. The form $B''$ is called the complementary form.

6. Elements of maximal order in Sylow groups

Let $G$ be a finite group. For a prime $q$ we define $\mu_q(G)$ to be the maximal order of those elements of $G$, whose order is a power of $q$. We have the following result, which is well-known to the experts in group theory. For the reader’s convenience we present a proof.

Lemma 6.1. Let $H$ be a finite $q$-group and $\mu_q(H) = q^t$ for some $t > 0$, then $\mu_q(Ht_r \mathbb{Z}_q) = q^{t+1}$.

Proof. Let $h$ be an element of $H$ such that $\text{ord}(h) = \mu_q(H)$ and let $e$ be the identity of $H$. Then $h^* = ((h, e, e, \ldots, e), 1) \in Ht_r \mathbb{Z}_q$ has order equal to $q^{t+1}$. Therefore $\mu_q(Ht_r \mathbb{Z}_q) \geq q^{t+1}$.

To obtain the opposite inequality we first observe that if $G = K \rtimes \psi H$, then $\mu_q(G) \leq \mu_q(K)\mu_q(H)$. Indeed, consider $x = (k, h) \in K \rtimes \psi \mathbb{Z}_q$, then

$$x^u = (k\psi_h(k) \ldots \psi_{h^{u-1}}(k), h^u).$$

Suppose $u$ is the minimal power such that $h^u = e \in H$ and set $y = k\psi_h(k) \ldots \psi_{h^{u-1}}(k)$. Then we have $x^u = (y, e)$ for some $y$ and thus $x^{ru} = (y^r, e)$. From this it easily follows that $\mu_q(G) \leq \mu_q(K)\mu_q(H)$.

Given the last inequality, by Definition 5.3 we write $Ht_r \mathbb{Z}_q$ as $K \rtimes \psi \mathbb{Z}_q$, where $K = \Pi_{p \in \mathbb{Z}_q} H$. We have $\mu_q(K) = \mu_q(H)$, hence $\mu(Ht_r \mathbb{Z}_q) \leq \mu_q(H)\mu_q(\mathbb{Z}_q)$ as desired.

Lemma 6.1 combined with Weir’s theorem (Theorem 5.3) allows us to describe all spaces such that their orthogonal groups have elements of given order $q^t$. The following result proves part (a) of Theorem 1.3 from the introduction.

Theorem 6.2. Let $s$ be a natural number such that $q^s | p^{2[q|p]} - 1$ and $q^{s+1} \not| p^{2[q|p]} - 1$. Let $B$ be a $p^k$-form.

For $r \geq s$ the group $O(B)$ contains an element of order $q^t$ if and only if $B$ has rank $2[q|p]q^{r-s}$ and $\epsilon(B) = \eta(q)^{q^{r-s}}$, or $B$ has rank strictly greater than $2[q|p]q^{r-s}$.

If $r < s$, the group $O(B)$ contains an element of order $q^t$ if and only if $B$ has rank $2[q|p]$ with $\epsilon(B) = \eta(q)$, or rank $B$ is greater than $2[q|p]$.

Proof. Let $B'$ be a maximal $q$-regular subform of $B$ as in Definition 5.9. By Lemma 5.8 we have an isomorphism of Sylow $q$-groups of $B$ and $B'$. Therefore in the proof of Theorem 6.2 it is enough to restrict to the case, where $B$ has rank $2[q|p]d$ and $\epsilon(B) = \eta(q)^d$. We clearly have $\mu_q(G \times H) = \max_i \mu_q(((Z_q^* t_r \mathbb{Z}_q) t_r \mathbb{Z}_q) \ldots) t_r \mathbb{Z}_q)$, hence by (6.1) we have

$$\mu_q(O(B)) = \max_i a_i \mu_q(((Z_q^* t_r \mathbb{Z}_q) t_r \mathbb{Z}_q) \ldots) t_r \mathbb{Z}_q),$$

where $a_i$ form the $q$-adic presentation of $d$, that is, $d = a_0 + a_1 q + a_2 q^2 + \ldots$. 


By Lemma 6.1 we obtain that \( \mu_q((Z_{q^d})^\epsilon \cup \cdots / \cup Z_q) = q^{s+i} \) if the wreath product is taken \( i \) times. In particular

\[
(6.3) \quad \mu_q(O(B)) = \max_{i; d \neq 0} q^{s+i}.
\]

It follows that if \( r \geq s \), we have \( \mu_q(O(B)) = q^r \) if and only if some of the \( a_i > 0 \) for \( t \geq r - s \). This amounts to saying that \( d \geq q^{r-s} \), if \( r \geq s \), or \( d \geq 1 \) if \( r < s \).

7. Fixed points of isometries of order \( q^r \)

Let \( B \) be a \( p^k \)-form and let \( \phi: B \to B \) be an isometry. We study the fixed point set

\[
\operatorname{Fix} \phi = \{ x \in B : \phi(x) = x \}.
\]

The following result gives a one way implication in Theorem 1.3(b).

**Theorem 7.1.** Let \( B \) be a \( p^k \)-form of rank \( n = 2[q|p]d + R \) with \( 0 \leq R < 2[q|p] \). Let \( \phi \in \mathrm{Syl}_q O(B) \) has order \( q^r \). Write also \( s \) for the maximal integer such that \( q^r[p^2q|p] - 1 \).

1. If \( R > 0 \), then \( \phi \) has a fixed subspace of rank at least \( R \), more precisely there is an orthogonal decomposition of \( B \) into submodules \( B_1 \) and \( B_2 \), such that \( B_1 \) has rank divisible by \( 2[q|p] \) and \( \phi|_{B_2} \) is the identity.
2. If \( R = 0 \) and \( \eta(q)^i \neq \epsilon(B) \), then \( \phi \) has a fixed subspace of rank at least \( 2[q|p] \).

**Proof.** Write \( B = B' \oplus B'' \), where \( B' \) and \( B'' \) are as in Definition 5.9. Note that \( B'' \) is non-trivial. Let \( i: O(B') \to O(B) \) be the inclusion induced map. Recall that \( i \) takes an element \( \psi \in O(B') \) and extends it by the identity on \( B'' \). This implies, in particular, that \( B'' \) is contained in the fixed point set of any element of \( O(B) \) that is in the image of \( i \).

Let \( G \) be a Sylow group of \( O(B') \). By Lemma 5.8 we have that \( i(G) \) is a Sylow group of \( O(B) \).

Take \( \phi \in O(B) \) of rank \( q^r \) and let \( H \subset O(B) \) be a Sylow group containing \( \phi \). As all Sylow groups are conjugate, we have that \( i(G) = gHg^{-1} \) for some \( g \in O(B) \). In particular \( \phi = g\phi'g^{-1} \) for some \( \phi' \in i(G) \). Define \( B_1 = gB' \) and \( B_2 = gB'' \). Then \( B_1 \) has rank divisible by \( 2[q|p] \) and \( B_2 \) contained in the fixed point set of \( \phi \). \( \square \)

8. Isometries with no non-zero fixed points

The goal of this section is to provide the reverse (as opposed to Theorem 7.1) implication of Theorem 1.3.

**Theorem 8.1.** Suppose we have a \( p^k \)-form \( (B, \beta) \) of rank \( n = 2[q|p]d \) and \( \eta(q)^d = \epsilon(B) \). Suppose also that \( \mathrm{Syl}_q O(B) \) contains an element of order \( q^r \). There exists \( \psi \in O(B) \) of order \( q^r \) such that \( \psi \) has no non-zero fixed points.

The remaining part of Section 8 is devoted to the proof of Theorem 8.1. We first prove some auxiliary results, then give the proof of Theorem 8.1.

The first step in the proof of Theorem 8.1 is a result, which is of independent interest.

**Proposition 8.2.** Let \( (B, \beta) \) be a \( p \)-form and let \( \phi \in O(B) \) be of order \( q^r \) for some \( r > 0 \). Then there exists an orthogonal decomposition of \( B \) into free \( \mathbb{Z}_p \)-modules \( B_{\text{fix}} \) and \( B_{\text{oth}} \), such that \( \phi \) is the identity of \( B_{\text{fix}} \) and \( \phi \) acts with no non-zero fixed points on \( B_{\text{oth}} \).
Proof. Let $\zeta$ be a primitive root of unity of order $q^r$ and consider the ring $\Lambda = \mathbb{Z}_p[\zeta]$. By Maschke’s theorem, $\Lambda$ is semisimple. On the other hand $B$ has a structure of a $\Lambda$-module, where multiplication by $\zeta$ corresponds the action of $\phi$. Hence, $B$ can be written as a direct sum of cyclic $\Lambda$-modules. Let $B_{fix}$ be the sum of those cyclic modules on which $\zeta$ acts trivially and $B_{oth}$ be the sum of all the others. The decomposition is orthogonal, indeed consider the map $B_{fix} \rightarrow B_{oth}$ given by the inclusion of $B_{fix}$ to $B$ followed by the orthogonal projection to $B_{oth}$. This map has to be trivial by Schur’s lemma, and therefore $B_{fix}$ is orthogonal to $B_{oth}$. By the construction $B_{fix}$ is the fixed point set of $\phi$ and $\phi$ acts on $B_{oth}$ with no non-zero fixed points. \hfill $\Box$

Proposition $8.2$ allows us to prove the following lemma, which is the key argument in the proof of Theorem $8.1$.

**Lemma 8.3.** Suppose $(B, \beta)$ is a $p$-form. Set as usual $s$ to be the maximal integer such that $q^s | (p^2 | q^s | p^2) - 1$. Assume $r \geq s$ and the rank of $B$ is $2[q|p]q^{r-s}$. If $\epsilon(B) = \eta(q)^{r-s}$ then an isometry $\psi \in O(B)$ of order $q^r$ has no fixed non-zero fixed points on $B$.

Proof. Suppose contrary, that is, take $\psi \in O(B)$ of order $q^r$ and assume it has a fixed subspace. Then by Proposition $8.2$ we infer that $B$ splits as a direct sum of $B_{fix}$ and $B_{oth}$. The map $\psi$ preserves the splitting and write $\psi'$ for the restriction of $\psi$ to $B_{oth}$. Then $\psi' \in O(B_{oth})$ has order $q^r$. But the rank of $B_{oth}$ is smaller than $2[q|p]q^{r-s}$, so by Theorem $6.2$ $O(B_{oth})$ cannot contain an element of order $q^r$. This contradiction shows that $\psi$ itself cannot have a non-zero fixed point. \hfill $\Box$

Proposition $8.2$ was stated and proved only for $p$-forms, and not for general $p^k$-forms. In fact, it does not hold for $p^k$-forms in general. As an example one can take the module $\mathbb{Z}_{p^3}^2$ with the standard linking form and a morphism $\phi$ given by the matrix

\[
(8.4) \quad A = \begin{pmatrix} 1 - 2p^2 & -2p \\ 2p & 1 - 2p^2 \end{pmatrix},
\]

Over $\mathbb{Z}_{p^3}$ we have $A^T A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, hence $\phi$ is an isometry. The point $(p^2, p^2)$ is a non-zero fixed point of $A$, however there is no free $\mathbb{Z}_{p^3}$-submodule on which $\phi$ acts trivially.

To deal with $p^k$-forms we apply again the (mod $p$)-reduction.

**Lemma 8.5.** Suppose $(B, \beta)$ is a $p^k$-form, $\psi$ is an isometry and $z \in B$ is a non-zero fixed point of $\psi$. Let $(B_{red}, \beta_{red})$ be the (mod $p$)-reduction and let $\psi_{red}$ be the reduction of $\psi$. Then $\psi_{red}$ has a non-trivial fixed point.

Proof. If the reduction $\pi(z)$ is non-trivial, then clearly $\pi(z)$ is a fixed point of $\psi_{red}$. Otherwise, if $\pi(z)$ is trivial, then $z$ can be written as $z = p^\ell y$ for some $\ell > 0$ and $y$ such that $\pi(y) \neq 0$. As $\psi(z) - z = 0$ and $\psi$ is linear, we infer that $\psi(y) - y = p^{k-\ell}u$ for some $u \in B$. But this means that $\psi_{red}(\pi(y)) - \pi(y) = 0$. Hence $\pi(y)$ is a non-trivial fixed point of $\psi_{red}$. \hfill $\Box$

**Example 8.6.** If $A$ is a matrix as in $(8.4)$ defining a morphism $\phi$ of $\mathbb{Z}_{p^3}^2$, then the (mod $p$)-reduction $\pi(\phi)$ is the identity matrix.

Given Lemma $8.5$ we quickly generalize Lemma $8.3$ to $p^k$-forms.

**Lemma 8.7.** Let $s$ be as in Lemma $8.3$ and $r \geq s$. Let $(B, \beta)$ be a $p^k$-form of rank $2[q|p]q^{r-s}$ and $\epsilon(B) = \eta(q)^{r-s}$. Any element $\psi \in O(B)$ of order $q^r$ has no non-zero fixed points.
Proof. If such an isometry $\psi$ has a non-trivial fixed point, then $\pi(\psi)$ has a non-trivial fixed point (and hence a fixed subspace) by Lemma 8.5. The isometry $\pi(\psi)$ has the same order $q^r$ because by Theorem 5.2 the reduction operation yields an isomorphism on Sylow $q$-groups. But this contradicts Lemma 8.3. □

The method of the proof of Lemma 8.7 gives the following simple result, which is needed to complete the proof of Theorem 8.1.

**Lemma 8.8.** Suppose $B$ has rank $2[q/p]$ and $\epsilon(B) = \eta(q)$. Then for any $\ell$ such that $1 \leq \ell \leq s$, there exists an isometry of $B$ of order $q^\ell$ with no non-zero fixed points.

**Proof.** We act as in the proof of Lemma 8.3. Suppose $\mathfrak{A}$ is a Seifert matrix. Write $\mathfrak{A}$ as a direct sum of isometries on $B_{\text{fix}}$ and $B_{\text{oth}}$, but $B_{\text{oth}}$ has rank less than $2[q/p]$ and hence it does not admit any isometry of order $q^\ell$ for $\ell > 0$.

For $p^k$-forms we use the same argument as in Lemma 8.7. □

Now we can give a proof of Theorem 8.1.

**Proof of Theorem 8.1.** First assume that $r \geq s$. We must have $d \geq q^{r-s}$, for otherwise there is no element in $O(B)$ of order $q^r$ by Theorem 6.2. Let $B_0$ be the unique form of rank $2[q/p]q^{r-s}$ and $\epsilon(B_0) = \eta(q)q^{r-s}$. Take also forms $B_1, \ldots, B_{d-q^{r-s}}$ that have rank $2[q/p]$ and index $\eta(q)$. The form $\hat{B} = B_0 \oplus B_1 \oplus \ldots B_{d-q^{r-s}}$ has the same rank as $B$ and, by Lemma 8.7, we have that $\epsilon(B) = \epsilon(\hat{B}) = \eta(q)d$. Hence $B$ and $\hat{B}$ are isometric.

We construct now an isometry on $\hat{B}$ of order $q^r$ which does not have non-zero fixed points. It is a block sum of isometries on $B_0$ and $B_1, \ldots, B_{d-q^{r-s}}$. On $B_0$ we use an isometry $\psi_0 : B_0 \to B_0$ with no non-zero fixed points, which is provided by Lemma 8.7. For $j = 1, \ldots, d-q^{r-s}$ we take an isometry $\psi_j : B_j \to B_j$ which is of order $q$ and which is provided by Lemma 8.8. The block sum of such isometries gives an isometry of $B$ with no non-zero fixed points and of order $q^r$.

If $r < s$, the proof is analogous. Namely, as $(B, \beta)$ has rank $2[q/p]d$ we can present it as a direct sum of $d$ copies of a form $(B_0, \beta_0)$ such that $\epsilon(B_0, \beta_0) = \eta(q)$. The form $(B_0, \beta_0)$ admits an isometry $\phi_0$ of order $q^r$ with no non-zero fixed points by Lemma 8.8. The isometry on $B$ is a direct sum of $d$ copies of $\phi_0$. □

9. Computing $\epsilon(B)$ for forms on the double branched cover

In order to apply effectively Theorem 1.4 we need a way to compute the indices $\epsilon(B)$ of forms associated with linking forms on branched covers of links. We present now such an algorithm. A detailed example is given in Section 10.

Suppose $L$ is a link and $S$ a Seifert matrix. Write $A = S + S^T$. If $\det(A) \neq 0$, then the double branched cover $\Sigma(L)$ is a rational homology sphere. For the rest of this section we shall assume that this is the case. Let $n$ denote the size of matrix $A$. Then

$$H_1(\Sigma(L); \mathbb{Z}) \cong \mathbb{Z}^n/A\mathbb{Z}^n.$$ 

Under this identification, the linking form is given by

$$\lambda_A : \mathbb{Z}^n/A\mathbb{Z}^n \times \mathbb{Z}^n/A\mathbb{Z}^n \to \mathbb{Q}/\mathbb{Z}$$

$$\lambda_A(x, y) = x^T A^{-1} y.$$
Put $A$ into the Smith Normal Form, that is, write
\[ A = CDE, \]
where $C$ and $E$ are invertible over $\mathbb{Z}$ and $D$ is diagonal with integer entries $(d_1, \ldots, d_n)$ on the diagonal such that $d_i | d_{i+1}$ for $i = 1, \ldots, n - 1$.

The following simple result gives an effective way of computing the linking form on $\Sigma(L)$.

**Lemma 9.2.** The pairing (9.1) is isometric to the pairing
\[ \lambda_D : \mathbb{Z}^n / DZ^n \times \mathbb{Z}^n / DZ^n \to \mathbb{Q} / \mathbb{Z} \]
\[ (x, y) \mapsto x^T C^T E^{-1} D^{-1} y. \]

**Proof.** The map $\mathbb{Z}^n \xrightarrow{C} \mathbb{Z}^n$ descends to an isomorphism of abelian groups from $\mathbb{Z}^n / DZ^n$ to $\mathbb{Z}^n / AZ^n$. Now if $x, y \in \mathbb{Z}^n / DZ^n$, then $Cx, Cy \in \mathbb{Z}^n / AZ^n$ and we have $\lambda_A(Cx, Cy) = (Cx)^T (CDE)^{-1} Cy = \lambda_D(x, y)$. \( \square \)

Let $p$ be an odd prime. Let $0 = \alpha_0 \leq \alpha_1 \leq \ldots$ be the integers such that if $\alpha_k \leq i < \alpha_{k+1}$, then $p^i | d_i$ but $p^{i+1} \not| d_i$. Let $h_i$ to be the vectors having 0 at all places except for the $i$-th coordinate, which is equal to $d_i/p^k$. Define $T_{p,k}$ for the submodule of $\mathbb{Z}^n / DZ^n$ generated by $h_{\alpha_k}, \ldots, h_{\alpha_{k+1}-1}$. Then $T_{p,k}$ is a free $\mathbb{Z}_p$-module. The sum $T_{p,1} \oplus T_{p,2} \oplus \ldots$ generates the $p$-torsion part of the module $\mathbb{Z}^n / DZ^n$. The notation $T_{p,k}$ reminds of Proposition 2.3 we remark that in the present case the summands do not have to be pairwise orthogonal.

On $T_{p,k}$ we have the linking form that is a restriction of the linking form $\lambda_D$. Write $\beta_{p,k}$ for the associated bilinear form. In the basis $h_{\alpha_k}, \ldots, h_{\alpha_{k+1}-1}$, the form can be written by a matrix, which we denote $B_k$. Note that the $ij$-entry of $B_k$ is given by $p^k \lambda_D(h_{i+\alpha_k-1}, h_{j+\alpha_k-1})$.

Write $\tilde{T}_{p,k}$ for the (mod $p$)-reduction of $T_{p,k}$ and let $\tilde{B}_k$ be the matrix of the reduced form. Clearly we have
\[ \det \tilde{B}_k \equiv \det B_k \pmod{p}. \]

**Proposition 9.4.** The linking form on the $p^k$-torsion part of $H_1(\Sigma(K); \mathbb{Z})$ has $\epsilon_1 = +1$ (see Definition 3.5) if and only if $\det \tilde{B}_k$ is a square modulo $p$.

**Proof.** We first give the proof under an extra assumption that $T_{p,k}$ is orthogonal to $T_{p,k'}$ with respect to the form $\lambda_D$, for all $k, k'$ such that $k \neq k'$. By Theorem 3.3 there exists a matrix $U$ with coefficients in $\mathbb{Z}_{p^k}$ such that $UB_k U^T$ is a diagonal matrix, whose all the diagonal entries but the first one are equal to 1, and the top-left entry is either 1 (if $\epsilon_1 = 1$) or a non-square modulo $p^k$, if $\epsilon_1 = -1$. Thus, the index $\epsilon_1$ depends on whether $\det UB_k U^T$ is a square modulo $p^k$ or not. But $\det B_k$ and $\det UB_k U^T$ differ by a square. Therefore $\epsilon_1 = 1$ if and only if $\det B_k$ is a square modulo $p^k$. By Hensel’s lemma this is the same as saying that $\det \tilde{B}_k$ is a square modulo $p$.

Now consider the general case, where $T_{p,k}$ are not necessarily orthogonal. Write $T_p = T_{p,1} \oplus T_{p,2} \oplus \ldots$ By Proposition 2.3 $T_p$ splits as a sum $T_{p,1} \oplus T_{p,2} \oplus \ldots$ of pairwise orthogonal summands (with respect to the linking form $\lambda_D$) and such that $T_{p,\ell}$ is a free $\mathbb{Z}_{p^\ell}$-module. We have thus an isometry
\[ \psi : T_{p,1} \oplus T_{p,2} \oplus \ldots \to T'_{p,1} \oplus T'_{p,2} \oplus \ldots. \]

Write $\psi_{ij}$ for the part of $\psi$ mapping from $T_{p,i}$ to $T'_{p,j}$. Choose bases $e_{i1}, \ldots, e_{ik_i}$, respectively $f_{jk_j}, \ldots, f_{jk_j}$ of $T_{p,i}$, respectively $T'_{p,j}$ (for $e_{ij}$ we can take vectors $h_d$ defined before, but here we
Lemma 9.5. There is a congruence $\kappa'_i \equiv q_i^2\kappa_i \pmod{p}$ for some $q_i$ invertible modulo $p$.

Given Lemma 9.5 we quickly finish the proof of Proposition 9.4. Namely,

- The first part of the proof of Proposition 9.4 applied to $T'_{p,i}$ tells that $\epsilon_1 = 1$ if and only if $\kappa'_i$ is a square modulo $p$;
- Lemma 9.5 implies that $\epsilon_1 = 1$ if and only if $\kappa_i$ is a square modulo $p$;
- The bases $\psi_{x_1}, \ldots, \psi_{y_{k_i}}$ and $h_{a_{ij}}, \ldots, h_{a_{i+1,j}}$ differ by an invertible matrix $U_i$. Hence $\kappa_i = \det U_i \det B_i \det U_i^T$, so $\kappa_i = \det B_i (\det U_i)^2$. That is, $\kappa_i$ is a square modulo $p$ if and only if $\det B_i$ is a square modulo $p$.

\[ \square \]

It remains to prove Lemma 9.5.

Proof of Lemma 9.5. Take $x, y \in T_{p,i}$. We have

\[ p^i \lambda_D(x, y) = p^i \lambda_D(\psi x, \psi y) = p^i \lambda_D(\sum_j \psi_{ji} x, \sum_k \psi_{ki} y). \]

The spaces $T'_{p,j}$ are pairwise orthogonal, so we rewrite the last sum as

\[ (9.6) \quad p^i \lambda_D(x, y) = p^i \sum_j \lambda_D(\psi_{ji} x, \psi_{ji} y). \]

Lemma 9.7. If $j \neq i$ we have

\[ (9.8) \quad p^i \lambda_D(\psi_{ji} x, \psi_{ji} y) \equiv 0 \pmod{p}. \]

Proof of Lemma 9.7. Suppose $j < i$. We have $\psi_{ji} x, \psi_{ji} y \in T'_{p,j}$, which is a $p^j$-torsion part. In particular $\lambda_D(\psi_{ji} x, \psi_{ji} y) = q_j p^j$ for some integer $c$. As $i > j$ we obtain (9.8) immediately.

Suppose $j > i$. Both $x, y$ are annihilated by $p^j$. Consequently, $\psi_{ji} x, \psi_{ji} y$ are annihilated by $p^j$. As $T'_{p,j}$ is a free $\mathbb{Z}_{p^j}$-module we infer that $\psi_{ji} x = p^{j-i} x_j$, $\psi_{ji} y = p^{j-i} y_j$ for some elements $x_j, y_j \in T'_{p,j}$. We also have $\lambda_D(x_j, y_j) = c' p^j$ for $c' \in \mathbb{Z}$. Hence

\[ \lambda_D(\psi_{ji} x, \psi_{ji} y) = p^{2j-2i} \lambda_D(x_j, y_j) = c' p^{j-2i}. \]

Therefore $p^j \lambda_D(\psi_{ji} x, \psi_{ji} y) = c' p^{j-2i} \equiv 0 \pmod{p}$, so (9.8) holds also for $j > i$. \hfill \square

Coming back to the proof of Lemma 9.5, from Lemma 9.7 we obtain

\[ (9.9) \quad p^i \lambda_D(x, y) \equiv p^j \lambda_D(\psi_{ii} x, \psi_{ii} y) \pmod{p}. \]

Write $\tilde{T}_{p,i}$, respectively $\tilde{T}'_{p,i}$ for the reductions of the forms on $T_{p,i}$ and $T'_{p,i}$. Equation (9.9) implies that $\psi_{ii}$ induces an isometry between $\tilde{T}_{p,i}$ and $\tilde{T}'_{p,i}$. As the forms $\tilde{T}_{p,i}$ and $\tilde{T}'_{p,i}$ are isometric, their determinants differ by a square modulo $p$. \hfill \square

We conclude this section with the following remark. In the proof of Proposition 9.4 we did not assume that the splitting of $T_p = T_{p,1} \oplus \ldots$ is invariant with respect to the group action. In fact, in the proof of Proposition we showed that the sign of the linking form on the $p^i$-torsion part of $H_1(\Sigma(K); \mathbb{Z})$ does not depend on the particular choice of splitting of $T_p$ into a sum $T_{p,1} \oplus T_{p,2} \oplus \ldots$. 


10. Example. Knot \( 10_{123} \)

Our aim is now to illustrate the algorithm described in Section 9 on a concrete knot. There are many knots that pass Naik’s obstructions but fail to the obstruction provided by Theorem \([1.4]\) see Section \([11]\). However all such knots that are known to us have Seifert matrices of size at least \(14 \times 14\). In order to make the discussion in this section more transparent, we decided to provide an example of a knot that actually is 5-periodic. Its Seifert matrix has size only \(8 \times 8\). We will show, how did we verify that it passes our criterion.

Consider the knot \( K = 10_{123} \). It is well known to be 5-periodic, a 5-periodic diagram can be found in [7, Figure 2] or on the KnotInfo webpage [2]. The Alexander polynomial of \( K \) is equal to

\[
\Delta = t^8 - 6t^7 + 15t^6 - 24t^5 + 29t^4 - 24t^3 + 15t^2 - 6t + 1 = (t^4 - 3t^3 + 3t^2 - 3t + 1)^2.
\]

There are two factors of the Alexander polynomial over \( \mathbb{Z}[t, t^{-1}] \). One is 1, the other one is \( t^4 - 3t^3 + 3t^2 - 3t + 1 \). We check that the latter does not satisfy (2.6) for any \( \ell \). On the other hand, we have a congruence

\[
\Delta \equiv (1 + t + t^2)^4 \mod 5,
\]

so \( \Delta \) (rather unsurprisingly) passes the Murasugi criterion. The polynomial 1 is the only candidate for the Alexander polynomial of the quotient. In particular, by Proposition \([2.2]\) the \( \mathbb{Z}_5 \) symmetry should act on \( H_1(\Sigma(K); \mathbb{Z})_p \) with only 0 as a fixed point for all \( p \neq 5 \).

We study the homology of the double branched cover. The Seifert matrix of \( K \) is

\[
S = \begin{pmatrix}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 1 & -1 & 0 & 0 \\
0 & -1 & 1 & 0 & 0 & 1 & -1 & 0 \\
0 & 0 & -1 & 1 & 0 & 0 & 1 & -1 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

We have

\[
A = S + S^T = CDE,
\]

where \( D \) is diagonal matrix with the diagonal vector \((1, 1, 1, 1, 1, 11, 11, 11)\) and \( C \) and \( E \) are invertible over \( \mathbb{Z} \). We see that the homology of the double branched cover is equal to \( \mathbb{Z}_5^1 \). Now for \( p = 11 \) and \( q = 5 \) we have \( [q/p] = 1 \), because \( 5 | (11 - 1) \). In particular \( 10_{123} \) passes the Naik’s criterion. Note also, for future use, that \( \eta(q) = 1 \).

We calculate the index of the linking form on \( \mathbb{Z}_{11}^8 \). The generators for the module \( \mathbb{Z}^8/\mathbb{Z}^8 \) are \( h_1 = (0, 0, 0, 0, 0, 0, 1, 0) \) and \( h_2 = (0, 0, 0, 0, 0, 0, 1, 1) \). The matrix of the linking form in
this basis is given by the $2 \times 2$ square submatrix of $C^T E^{-1} D^{-1}$ in the bottom left corner:

$$
\begin{pmatrix}
-46 & -20 & -60 & -52 & -62 & -51 & -4 & -5 \\
-20 & -12 & -35 & -34 & -39 & -31 & -3 & -2 \\
-60 & -35 & -98 & -93 & -107 & -85 & -8 & -6 \\
-52 & -34 & -93 & -90 & -103 & -81 & -8 & -5 \\
-62 & -39 & -107 & -103 & -118 & -93 & -9 & -6 \\
-51 & -31 & -85 & -81 & -93 & -74 & -7 & -5 \\
-4 & -3 & -8 & -8 & -9 & -7 & \frac{8}{11} & -\frac{4}{11} \\
-5 & -2 & -6 & -5 & -6 & -5 & \frac{4}{11} & -\frac{6}{11}
\end{pmatrix}.
$$

The associated bilinear form $(B, \beta)$ on $\mathbb{Z}_2^2$ has matrix

$$
\begin{pmatrix}
-8 & -4 \\
-4 & -6
\end{pmatrix}.
$$

The determinant of this matrix is equal to $32 \equiv 10 \pmod{11}$, so it is not a square modulo 11, so the form has $\epsilon_1 = -1$. However, the rank $n = 2$ is congruent to 2 mod 4 and $11 \equiv 3 \pmod{4}$, so according to the definition of the index (Definition 3.5) we have $\epsilon_2 = -1$, so $\epsilon(B) = 1$. Then $\epsilon(B) = \eta(q)$. The knot passes our criterion.

11. Theorem 1.4 for low crossing knots

We applied the following criteria for knots up to 15 crossings and for periods $q = 3, 5, 7, 11, 13$.

- Przytycki’s criterion for HOMFLYPT polynomials [14];
- Murasugi’s criterion as stated in Theorem 2.5;
- Naik’s homological criterion in the way stated in Propositions 2.7 and 2.8;
- Theorem 1.4.

The way we applied these criteria is as follows. For a given knot $K$ and period $q$ we checked the Przytycki’s criterion. Independently, we were looking for all candidates $\Delta'$ for the Alexander polynomial of the quotient, that is, those that satisfy the statement of Theorem 2.5. For each such $\Delta'$ we checked if the criterion of Proposition 2.7 is satisfied for all prime numbers $p$ different than 2 and $q$ that are also factors of $\Delta(-1)$. If $\Delta'$ passed the criterion of Proposition 2.7, we checked if $K$ passes Proposition 2.8 with this $\Delta'$ for all prime numbers $p \neq 2, q$ that divide $\Delta(-1)$ but do not divide $\Delta'(-1)$.

If $\Delta'$ passed also the criterion of Proposition 2.8, we were looking at Theorem 1.4 for all prime numbers $p \neq 2, q$ such that $p|\Delta(-1)$ but $p$ does not divide $\Delta'(-1)$.

If at some moment $\Delta'$ did not pass the criterion, it was discarded from a list of potential Alexander polynomials of the quotient. If the list was empty, we concluded that the knot $K$ is not $q$-periodic. We recorded, if this conclusion is achieved using Proposition 2.7 only, or one needs Proposition 2.8 or even Theorem 1.4 to obstruct $q$-periodicity.

It turns out that for periods greater than 5, Theorem 1.4 did not obstruct any case that was not obstructed by combined Murasugi’s and Naik’s criteria.

For period 5, our criterion obstructed knots 14n26993, 15n80526, 15n83514 and 15n95792, but all of these knots are not 5-periodic by Przytycki’s criterion.
The most interesting situation was for period 3. Here we were able to obstruct knots 12a100 and 12a348, which can also be obstructed using Jabuka and Naik’s \(d\)-invariants criterion, see \cite{JN} Section 2.4 for a detailed discussion of 12a100 knot.

There are also 19 alternating knots with crossing numbers from 13 to 15, whose 3-periodicity is obstructed by Theorem \cite{P}, but not by Naik’s criterion and also not by Przytycki’s criterion. These are:

\[
\begin{align*}
13a4648 & \quad 14a7583 & \quad 14a7948 & \quad 14a8670 & \quad 14a9356 \\
14a14971 & \quad 14a16311 & \quad 14a17173 & \quad 14a17260 & \quad 14a18647 \\
15a6030 & \quad 15a6066 & \quad 15a10622 & \quad 15a15077 & \quad 15a33910 \\
15a36983 & \quad 15a46768 & \quad 15a72333 & \quad 15a82771.
\end{align*}
\]

Among non-alternating knots with 12–15 crossings, there are 57 knots whose 3-periodicity can be obstructed by Theorem \cite{P}, but for which Naik’s criterion and Przytycki’s criterion do not obstruct 3-periodicity. These are 13n3659, 14n908, 14n913, 14n2451, 14n2458, 14n6565, 14n9035, 14n11989, 14n14577, 14n23051 and 14n24618, as well as further 46 knots with 15 crossings.

We note that for these non-alternating examples the Jabuka–Naik criterion \cite{JN} cannot be easily applied, because it requires calculating \(d\)-invariants of double branched covers of non-alternating knots, for which we do not have any algorithm so far. Another criterion involving knot homology, namely Khovanov homology, see \cite{K}, does not work for period 3, so it cannot obstruct periodicity of these 57 knots.

We have also applied Theorem \cite{P} to obstruct \(3^2\)-periodicity of knots, but we could not find any example, where Theorem \cite{P} could obstruct periodicity of any knot that passed the Murasugi’s criterion for period 9. To find interesting examples, one probably needs to consider knots with much more crossings.

References

\begin{enumerate}
\item M. Borodzik and W. Politarczyk, \textit{Khovanov homology and periodic links} (2017). arXiv:1704.07316, to appear in Indiana Univ. J.
\item J. Cha and C. Livingston, \textit{Knotinfo: Table of knot invariants}, http://www.indiana.edu/~knotinfo, 2018.
\item H. Chen, \textit{On the groups of periodic links}, 2018. arXiv:1805.02219.
\item J. Davis, \textit{The homology of irregular dihedral branched covers of} \(S^3\), Math. Ann. \textbf{301} (1995), no. 3, 519–528.
\item J. Davis and C. Livingston, \textit{Alexander polynomials of periodic knots}, Topology \textbf{30} (1991), no. 4, 551–564.
\item J. Hillman, C. Livingston, and S. Naik, \textit{Twisted Alexander polynomials of periodic knots}, Algebr. Geom. Topol. \textbf{6} (2006), 145–169 (electronic).
\item S. Jabuka and S. Naik, \textit{Periodic knots and Heegaard Floer correction terms}, J. Eur. Math. Soc. (JEMS) \textbf{18} (2016), no. 8, 1651–1674.
\item A. Kawauchi and S. Kojima, \textit{Algebraic classification of linking pairings on} \(3\)-\textit{manifolds}, Math. Ann. \textbf{253} (1980), no. 1, 29–42.
\item M. Marchwicka and W. Politarczyk, \textit{A sage script to verify periodicity}, 2018.
\item K. Murasugi, \textit{On periodic knots}, Comment. Math. Helv. \textbf{46} (1971), 162–174.
\item S. Naik, \textit{Periodicity, genera and Alexander polynomials of knots}, Pacific J. Math. \textbf{166} (1994), no. 2, 357–371.
\item \textit{New invariants of periodic knots}, Math. Proc. Cambridge Philos. Soc. \textbf{122} (1997), no. 2, 281–290.
\item W. Politarczyk, \textit{Equivariant Jones polynomials of periodic links}, J. Knot Theory Ramifications \textbf{26} (2017), no. 3, 1741007, 21.
\item J. Przytycki, \textit{On Murasugi’s and Traczyk’s criteria for periodic links}, Math. Ann. \textbf{283} (1989), no. 3, 465–478.
\item M. Sakuma, \textit{On the polynomials of periodic links}, Math. Ann. \textbf{257} (1981), no. 4, 487–494.
\end{enumerate}
[16] P. Traczyk, 10101 has no period 7: a criterion for periodic links, Proc. Amer. Math. Soc. 108 (1990), no. 3, 845–846.
[17]        Periodic knots and the skein polynomial, Invent. Math. 106 (1991), no. 1, 73–84.
[18] V. Turaev, Reidemeister torsion in knot theory, Uspekhi Mat. Nauk 41 (1986), no. 1(247), 97–147, 240.
[19] C. Wall, Quadratic forms on finite groups, and related topics, Topology 2 (1963), 281–298.
[20] A. Weir, Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p, Proc. Amer. Math. Soc. 6 (1955), 529–533.
[21] R. Wilson, The finite simple groups, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009.

Institute of Mathematics, University of Warsaw, ul. Banacha 2, 02-097 Warsaw, Poland
E-mail address: mcboro@mimuw.edu.pl

Institute of Mathematics, University of Warsaw, ul. Banacha 2, 02-097 Warsaw, Poland
E-mail address: pg370922@students.mimuw.edu.pl

Institute of Mathematics, University of Warsaw, ul. Banacha 2, 02-097 Warsaw, Poland
E-mail address: adam.krol@student.uw.edu.pl

Department of Mathematics and Computer Science, Adam Mickiewicz University in Poznań, ul. Umultowska 87, 61-614 Poznań, Poland
E-mail address: maria.marzwicka@amu.edu.pl