Combinatorics, Probability and Computing (2007) 16, 503–514. © 2007 Cambridge University Press
doi:10.1017/S0963548306007875 First published online 21 February 2007 Printed in the United Kingdom

Reconstructing Odd Necklaces

LUKE PEBODY

Trinity College, Cambridge CB2 1TQ, UK
(e-mail: ltp1000@cam.ac.uk)

Received 11 March 2005; revised 23 July 2005

Improving upon work in [2], the precise value of the set reconstruction number is given for all cyclic groups of odd order.

1. Introduction and problem definition

Throughout, C is a fixed cyclic group. Theorems and lemmas only require that $|C|$ be odd if they state so explicitly.

Definition 1. A *necklace* N is a subset of C. Two necklaces N_1 and N_2 are *isomorphic* if there is some element $i \in C$ with $i + N_1 = N_2$.

Informally, necklaces can be thought of as a circle of $|C|$ pearls, coloured black (contained in N) and white (not contained in N), where beads can be moved around the circle. However, the necklace is on somebody's neck, so you cannot reverse the order of the pearls.

The necklace problem deals with whether you can identify the black/white make-up of a necklace (knowing $|C|$), given a specific peculiar sight deficiency. Namely, for a given integer k, you will be able to see the relative positions of only k black beads at a time. Such a person is said to be *k-blind*.

Definition 2. Given necklaces N_1, N_2, N_1 is a *subnecklace* of N_2 if N_1 is a subset of N_2. The *k-deck* $N^{(k)}$ of a necklace N is the multiset of isomorphism-classes of its subnecklaces of size at most k.

Therefore someone is k-blind if all they can tell about a necklace is its k-deck. The question in general asks for a fixed $|C|$ and k, whether k-blind people can recognize all necklaces of $|C|$ beads.

Definition 3. Given necklaces N_1, N_2, N_1 and N_2 are *k-isomorphic* if they have identical k-decks. The *isomorphism level of N_1 and N_2* $r(N_1, N_2)$ is the lowest k such that N_1 and N_2 are not k-isomorphic. If there is no such k, $r(N_1, N_2) = \infty$.

Here is a trivial bound on finite isomorphism levels.

Lemma 1.1. *If $r(N_1, N_2) > |C|$, then $r(N_1, N_2) = \infty$ and N_1 is isomorphic to N_2.*

Proof. Since $r(N_1, N_2) > |C| \geqslant |N_1|$, N_2 and N_1 are $|N_1|$-isomorphic. The $|N_1|$-deck of N_1 consists solely of 1 set in the isomorphism class of N_1.

Therefore N_2 has precisely 1 subset of size $|N_1|$ and this subset is isomorphic to N_1. Therefore N_2 is isomorphic to N_1. □

Usually the bound of $|C|$ in Lemma 1.1 is not strict, leading to the following definition.

Definition 4. Given necklace N_1, define the *reconstruction number* of N_1, $r(N_1)$, to be the lowest integer k such that if N_1 is k-isomorphic to any necklace N_2, N_1 must be isomorphic to N_2.

Define the *reconstruction number* of C, $r(C)$, to be the largest $r(N_1)$ for any necklace N_1 of C. Equivalently, $r(C)$ is the lowest integer k such that if any two necklaces are k-isomorphic, they must be isomorphic.

Then Lemma 1.1 states the following.

Corollary 1.2. $r(C) \leqslant |C|$.

In [1], Alon, Caro, Krasikov and Roditty prove that $r(C) \leqslant 1 + \log |C|$. In [3], Radcliffe and Scott prove that $r(C) \leqslant 9.\#(\text{prime factors of } |C|)$ in general and that if $|C|$ is prime and $|C| \geqslant 5$, then $r(C) = 3$.

In [2], the author reduced these bounds to $r(C) \leqslant 6$ in general, and $r(C) \leqslant 4$ for $|C|$ odd. In this paper the exact value of $r(C)$ is given for all cyclic groups with $|C|$ odd. Define $f(n)$ to be the number of not necessarily distinct prime factors n has. For example, $f(p^a q^b) = a + b$.

Theorem 1.3. *Let C be a cyclic group of odd order. Then*

$$r(C) = \begin{cases} 1, & \text{if } |C| = 1, 3, \\ 2, & \text{if } |C| = 5, \\ 3, & \text{if } f(|C|) < 4 \text{ or } |C| \text{ is a prime power,} \\ 4, & \text{otherwise.} \end{cases}$$

Therefore, if a lady (or indeed a gentleman) were to wear any necklace with an odd number of pearls, this necklace could be recognizable by 4-blind people, but there are some odd-length necklaces which are not recognizable by 3-blind people.

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

This paper first views things from the perspective of a jeweller, attempting to make ornate necklaces. After this, it helps activists for the partially sighted, ensuring that necklaces will never get too ornate.

2. Trivial lower bounds

In this section, the easier lower bounds in Theorem 1.3 are proved. First note that the 1-blind do not have much hope of recognizing necklaces.

Theorem 2.1. *Let* $|C| > 3$. *Then* $r(C) \geqslant 2$.

Proof. Let N_1 be the necklace $\{0,1\}$. (Here and throughout, the integers are seen as elements of all cyclic groups.) Let N_2 be the necklace $\{0,2\}$. It is clear that N_1 and N_2 are 1-isomorphic.

However, N_1 and N_2 are not isomorphic: if they are, there exists an integer i such that $i + \{0,1\} = \{0,2\} (\mathrm{mod}\ n)$. Then either $i \equiv 0$ and $i+1 \equiv 2$, in which case $n|1$, or $i \equiv 2$ and $i+1 \equiv 0$, in which case $n|3$. Since $n = |C| > 3$, this cannot happen. □

The 2-blind are not much better off. This is because 2-blind people cannot tell if a necklace is on the right way, or back-to-front.

Theorem 2.2. *Let* $|C| > 5$. *Then* $r(C) \geqslant 3$.

Proof. Let N_1 be the necklace $\{0,1,3\}$ and let N_2 be the necklace $\{0,2,3\}$. Then the 2-deck of N_1 has 1 subnecklace isomorphic to $\{\}$, 3 subnecklaces isomorphic to $\{0\}$, and 1 subnecklace isomorphic to each of $\{0,1\}$, $\{0,2\}$ and $\{0,3\}$. (Note that $\{0,1\},\{0,2\}$ and $\{0,3\}$ are pairwise non-isomorphic as $|C| > 5$.) Since this is also the 2-deck of N_2, N_1 and N_2 are 2-isomorphic.

However, suppose N_1 and N_2 are isomorphic. Then there must exist an i such that $i + \{0,1,3\} = \{0,2,3\} (\mathrm{mod}\ n)$. Then i must be an element of N_2 such that $i+1 \in N_2$. Therefore i must be 2. Then $i = 2$ and $i+1 = 3$, so $i+3$ must equal 0. However, $|C| > 5$ so $i+3 \neq 0$. □

Informally, the 2-deck tells you the pairwise distances of beads in N. If you reverse N, you do not change the 2-deck, but (for $|C| > 5$), you may change the necklace. The remaining lower bound requires a little more groundwork.

3. Construction

Suppose that C is a cyclic group of odd order with $f(|C|) \geqslant 4$ and that $|C|$ is not a prime power. Then $|C|$ can be expressed as the product $pqrs$ with $\gcd(r,s) = 1$, $p,q,r,s > 2$. Fix such an expression. It is useful to describe two properties that necklaces can have.

Definition 5. Given factor m of $|C|$, define a necklace S of C to be *m-periodic* if, for all $x \in C$, $x \in S$ if and only if $x + m \in S$.

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

Define a necklace to be *m-balanced* if the number of elements of S equivalent to i mod m is independent of i.

The following operation on necklaces will be of use in this section.

Definition 6. Given necklaces $S_0, S_1, \dots, S_{p-1}$ of $\mathbb{Z}_k$, define the *splice* of $S_0, S_1, \dots, S_{p-1}$, which we denote by $\mathrm{Splice}(S_0, S_1, \dots, S_{p-1})$, to be the necklace of $\mathbb{Z}_{pk}$ consisting of $px + i$ where $x \in S_i$ and $0 \leqslant i < p$.

These definitions are enough to construct ornate necklaces that are 3-isomorphic but not isomorphic. Recall that we have an expression $|C| = pqrs$ with $\gcd(r,s) = 1$, $p, q, r, s > 2$.

Theorem 3.1. *Suppose S_1 and S_2 are necklaces of $\mathbb{Z}_{qrs}$ which are q-balanced, with S_1 qr-periodic and S_2 qs-periodic. Let*

$$T_0 = \mathrm{Splice}(S_1, S_2, \emptyset, \dots, \emptyset) \quad \textit{and} \quad T_1 = \mathrm{Splice}(S_1 + 1, S_2, \emptyset, \dots, \emptyset).$$

Then T_0 and T_1 are 3-isomorphic.

Proof. Let $S \subset C$ with $|S| \leqslant 3$. It is required to prove that the number of $i \in C$ with $S + i \subseteq T_a$ does not depend on a.

Case I: S contains integers in 3 distinct residue classes (mod p).
Then so does $S + i$ for all i. However, T_a does not for either value of a. Therefore the number of such i is zero, regardless of a.

Case II: S contains integers in non-consecutive residue classes (mod p).
Then so does $S + i$ for all i. However, T_a does not for either a. Therefore the number of such i is zero, regardless of a. (Note that for $p > 3$, Case I is a subcase of Case II)

Case III: All the elements of S are in the same residue class (mod p).
Then, by translating S it can be assumed that all elements of S are multiples of p, so there exists a qrs-necklace S' such that $S = \mathrm{Splice}(S', \emptyset, \dots, \emptyset)$. Then the number of S-translates in T_a is equal to the total number of S'-translates in $S_1 + a$ and S_2 combined. As such, it clearly does not depend on a.

Case IV: The elements of S lie in two consecutive residue classes (mod p).
Then, by translating S it can be assumed that all elements of S are equivalent to $0, 1 (\mathrm{mod}\ p)$, so there exists S', S'' such that $S = \mathrm{Splice}(S', S'', \emptyset, \dots, \emptyset)$. Then $i + S \subset T_a$ if and only if $i = px$ where $x + S' \subset S_1 + a$ and $x + S'' \subset S_2$.

Now, as S_1 is qr-periodic, the validity of $x + S' \subset S_1 + a$ depends only on the qr-residue of x. Similarly, the validity of $x + S'' \subset S_2$ depends only on the qs-residue of x.

Now, $\gcd(r,s) = 1$. Therefore, given the q-residue of x, the qr-residue and qs-residue are independent. This means that the number of solutions to $i + S \subset T_a$ can be evaluated by summing over the q-residue classes of x the product of the number of solutions of $x + S' \subset S_1 + a$ and the number of solutions of $x + S'' \subset S_2$.

However, $3 \geqslant |S| = |S'| + |S''|$. Therefore, either $|S'| = 1$ or $|S''| = 1$.

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

If $|S'| = 1$, then since S_1 is q-balanced, the number of solutions of $x + S' \subset S_1 + a$ in each residue-class is constant, say c. Therefore the number of solutions to $i + S \subset T_a$ is c times the number of solutions of $x + S'' \subset S_2$ and does not depend on a.

If $|S''| = 1$, then since S_2 is q-balanced, the number of solutions of $x + S' \subset S_2$ in each residue-class is constant, say c. Therefore the number of solutions to $i + S \subset T_a$ is c times the number of solutions of $x + S'' \subset S_2$ and does not depend on a. □

This proof depends on the fact that when a three-element set is split up into at least two parts, one part has at most one element. However, this does not hold for four element sets, leading to the following theorem.

Theorem 3.2. *There exist necklaces S_1 and S_2 of $\mathbb{Z}_{qrs}$ which are q-balanced, with S_1 qr-periodic and S_2 qs-periodic, and such that if $T_0 = \text{Splice}(S_1, S_2, \emptyset, \ldots, \emptyset)$ and $T_1 = \text{Splice}(S_1 + 1, S_2, \emptyset, \ldots, \emptyset)$ then T_0 and T_1 are not isomorphic.*

Proof. Let S_1 be the set of elements of $\mathbb{Z}_{qrs}$ such that their residue (mod qr) is at most q, and let S_2 be the set of elements of $\mathbb{Z}_{qrs}$ such that their residue (mod qs) is at most q.

Then consider the number of elements $x \in C$ such that $x, x+1, x+p, x+p+1$ are all in T_0. Such x are of the form py where $y, y+1$ are both in S_1 and S_2. If y is of residue $i(\text{mod } q)$, then in order to be in S_1, it must be of residue $i(\text{mod } qr)$, and in order to be in S_2, it must be of residue $i(\text{mod } qs)$. Therefore it has to be equal to $i(\text{mod } qrs)$. Furthermore, if $i = q-1$ then $y+1$ will not be in S_1 or S_2. Therefore there are $q-1$ such x.

Then $x, x+1, x+p, x+p+1$ are all in T_1 if x is of the form py, where $y, y+1$ are in S_2 and $y, y-1$ are in S_1. The same argument as before says y has to be $i(\text{mod } qrs)$ with $0 \leqslant i < q$. Also, as before, if $i = q-1$, $y+1$ is not in S_2. Furthermore, if $i = 0$, $y-1$ is not in S_1. Therefore there are $q-2$ such x. This shows that in this case of S_1 and S_2, T_0 and T_1 have different 4-decks, showing that they are not isomorphic. □

This gives the final required lower bound.

Corollary 3.3. *If C is a cyclic group of odd order with $p(|C|) \geqslant 4$ and $|C|$ is not a prime power, $r(C) \geqslant 4$.*

Proof. Express $|C|$ in the manner $|C| = pqrs$ where $p, q, r, s > 2$ and $\gcd(r, s) = 1$ and then construct T_0 and T_1 as in the proof of Theorem 3.2. Theorem 3.1 shows that T_0 and T_1 have the same 3-decks, whilst Theorem 3.2 shows that T_0 and T_1 are not isomorphic. Therefore $r(\mathbb{Z}_n) \geqslant 4$. □

The construction section of the paper is over, and now the strengths of the partially blind must be highlighted. Since various of the main results of [2] will be used, these will be stated in the next section. This will leave only two types of odd $|C|$ for which $r(C)$ is unknown, which will be dealt with by a technical lemma about the cyclotomic roots of 0,1-polynomials.

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

4. Main results of [2]

An earlier paper of the author [2] deals with the necklace problem by looking at multinecklaces: necklaces where more than 1 pearl is allowed to be at the same place. For ease of argument, it actually made sense to allow negative or rational numbers of pearls at any place. Formally a *multinecklace* is a function $f : C \to \mathbb{Q}$. Multinecklaces f_1, f_2 are *isomorphic* if $f_1(x) = f_2(x+i)$ for some $i \in C$.

The k-*deck* of multinecklace f is the function $f^{(k)} : C^k \to \mathbb{Q}$ defined by

$$f^{(k)}(x_1, x_2, \ldots, x_k) = \sum_{i=0}^{n-1} f(x_1+i)f(x_2+i)\cdots f(x_k+i).$$

Then f_1,f_2 are k-*isomorphic* if $f_1^{(k)} = f_1^{(k)}$. The *multiset reconstruction number* of C, $r_m(C)$, is the smallest k such that if f_1, f_2 are k-isomorphic they are isomorphic. It is trivial that $r(C) \leqslant r_m(C)$.

Fix a primitive $|C|$th root of unity ω. Then, given a multinecklace $f : C \to \mathbb{Q}$, define $\widetilde{f} : C \to \mathbb{C}$ to be the finite Fourier transform of f:

$$\widetilde{f}(k) = \sum_{j \in C} f(j)\omega^j.$$

The first result of [2] describes k-isomorphism of multinecklaces in terms of their Fourier transform.

Theorem 4.1. *Let f, g be multinecklaces of C. Then f and g are k-isomorphic if and only if, for all $x_1, x_2, \ldots, x_k \in C$ with $\sum_{i=1}^{i=k} x_i = 0$,*

$$\prod_{i=1}^{i=k} \widetilde{f}(x_i) = \prod_{i=1}^{i=k} \widetilde{g}(x_i).$$

This has the following corollary.

Corollary 4.2. *2-isomorphic multinecklaces have zeroes at the same places in their Fourier transforms.*

Proof. Let f, g be 2-isomorphic. Then for all i, if $\widetilde{f}(i) = 0$ and $\widetilde{g}(i) \neq 0$, $\widetilde{g}(i)\widetilde{g}(-i) = \widetilde{f}(i)\widetilde{f}(-i) = 0$. Therefore $\widetilde{g}(-i) = 0$. However, if i, j are of the same order (for example $j = -i$), then $\widetilde{g}(i)$ and $\widetilde{g}(j)$ are algebraic conjugates. Therefore $\widetilde{g}(i)$ is a root of $x = 0$ and is hence 0. □

Then, given 2-isomorphic multinecklaces g_1, g_2, the double Fourier function $f_{g_1,g_2}(x)$ is defined to be 0 if $\widetilde{g_1}(x) = 0$ and $\frac{\widetilde{g_2}(x)}{\widetilde{g_1}(x)}$ otherwise.

Corollary 4.3. *Let g_1, g_2 be 2-isomorphic multinecklaces of C. Then g_1 and g_2 are k-isomorphic if and only if, for all $x_1, x_2, \ldots, x_k$ with $\sum x_i = 0$, $\prod_{i=1}^{i=k} f_{g_1,g_2}(x) \in \{0, 1\}$.*

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

Proof. $\prod_{i=1}^{i=k} f_{g_1,g_2}(x) = 0$ is equivalent to

$$\prod_{i=1}^{i=k} \widetilde{g_1}(x) = \prod_{i=1}^{i=k} \widetilde{g_2}(x) = 0.$$

Furthermore, $\prod_{i=1}^{i=k} f_{g_1,g_2}(x) = 1$ is equivalent to

$$\prod_{i=1}^{i=k} \widetilde{g_1}(x) = \prod_{i=1}^{i=k} \widetilde{g_2}(x) \neq 0.$$ □

Define a function $f : C \to \mathbb{C}$ to be *strong* if, whenever i, j are integers with $f(i) \neq 0$ and $f(ji) \neq 0$, $f(ji) = f(i)^j$. The following corollary from [2] will be useful.

Corollary 4.4. *Let g_1, g_2 be 3-isomorphic multinecklaces of C with $|C|$ odd. Then f_{g_1,g_2} is strong.*

Furthermore, an easy way to detect if g_1 and g_2 are isomorphic is given. Define a function $f : C \to \mathbb{C}$ to be *trivial* if there is an nth root ω of unity such that, for every i, $f(i) \in \{\omega^i, 0\}$.

Theorem 4.5. *Let g_1, g_2 be 2-isomorphic multinecklaces of $\mathbb{Z}_n$. Then g_1 and g_2 are isomorphic if and only if f_{g_1,g_2} is trivial.*

An equivalent definition of triviality is given by the following theorem.

Theorem 4.6. *Given $f : C \to \mathbb{C}$, f is trivial if and only if f is strong, and for all integers x, y, z with xy and xz both factors of $|C|$, $\gcd(y, z) = 1$ and $y, z > 1$, $f(xy)^z = f(xz)^y$ or $f(xy)f(xz) = 0$.*

This led to an evaluation $r_m(C)$ for all finite cyclic C, and indeed $r_m(G)$ for all finite abelian G.

Theorem 4.7. *Let n be an integer. Then*

$$r_m(\mathbb{Z}_n) = \begin{cases} 1 & \textit{for} \quad n = 1, \\ 2 & \textit{for} \quad n = 2, \\ 3 & \textit{for} \quad n \textit{ is an odd prime power or } n = pq \textit{ for odd primes } p,q, \\ 4 & \textit{for} \quad n \textit{ is any other odd number}, \\ 4 & \textit{for} \quad n = 2^k, k > 1, \\ 4 & \textit{for} \quad n = 2p^k, k \geqslant 1 \textit{ and some odd prime } p, \\ 5 & \textit{for} \quad n = 2^l p^k, l > 1, k \geqslant 1 \textit{ and some odd prime } p, \\ 6 & \textit{for} \quad n \textit{ is any other even number}. \end{cases}$$

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

There are only a few cyclic groups C of odd order for which the claimed value of $r(C)$ in Theorem 1.3 differs from the value of $r_m(C)$ in Theorem 4.7. These are those where Theorem 1.3 claims that $r(C) = 3$, and yet Theorem 4.7 claims that $r_m(C) = 4$. These are those of the form p^2q for distinct p, q and pqr for distinct p, q, r, and will be dealt with in the next three sections. Firstly the cases $n = 3, 5$ must be dealt with.

Theorem 4.8. $r(\mathbb{Z}_3) = 1$ *and* $r(\mathbb{Z}_5) = 2$.

Proof. There are 4 isomorphism classes of $\mathbb{Z}_3$ necklaces, each determined by the size (and hence 1-deck) of the set.

If a $\mathbb{Z}_5$ necklace is of size $0, 1, 4, 5$, then it is determined by its size, and hence by its 1-deck. If it is of size 2, it is either isomorphic to $\{0, 1\}$ or $\{0, 2\}$, which have the same 1-deck but differing 2-decks. If it is of size 3, it is either isomorphic to $\{0, 1, 2\}$ or $\{0, 1, 3\}$, which have the same 1-deck but differing 2-decks. □

5. Cyclotomic roots of 0,1 polynomials

Given a subset S of C, let the associated polynomial P_S be $\sum_{i\in S} x^i$, where the sum is over integers in the range 0 to $|C| - 1$ whose residues mod $|C|$ are in S. Write $r(S)$ for the set of integers $i > 1$ such that i is a factor of $|C|$ and all primitive ith roots of unity are roots of P_S.

This has a connection with the concepts of the previous section: $\widehat{S}(i)$ is P_S applied to ω_n^i, which is a primitive $\frac{n}{\gcd(n,i)}$th root of unity. Therefore $\widehat{S}(i) = 0$ if and only if $\frac{|C|}{\gcd(|C|,i)} \in r(S)$. Note that the properties of S being balanced and periodic can be detected from $r(S)$.

Theorem 5.1. *Let k be a factor of $|C|$. Then S is k-balanced if and only if $i \in r(S)$ for all factors i of k with $1 < i$. S is k-periodic if and only if $i \in r(S)$ for all factors of $|C|$ which are not factors of k.*

Proof. The product of the ith cyclotomic polynomials, where i ranges over the factors i of k with $1 < i$, is $\frac{x^k-1}{x-1}$. Performing the division $P_S = Q(x^k - 1) + R$ where $\deg R < k$, then the x^i coefficient of R is the sum of x^{i+kt} coefficients of P_S, which is the number of elements of S whose k residue is i. Therefore S is k-balanced if and only if R is a multiple of $\frac{x^k-1}{x-1}$, which is true if and only if P_S is.

The product of the ith cyclotomic polynomials, where i ranges over all factors of $|C|$ that are not factors of k, is $p = \frac{x^{|C|}-1}{x^k-1} = 1 + x^k + x^{2k} + \cdots + x^{|C|-k}$. Writing $P_S = Qp + R$ with $\deg R < |C| - k$, then clearly $\deg Q = \deg P_S - (|C| - k) < k$.

Indeed, since $P_S = \sum_{i=0}^{|C|-1} a_i x^i$ with $a_i = 0$ if $i \notin S$ and $a_i = 1$ if $i \in S$, then it can be easily seen that $Q = a_{|C|-1}x^{k-1} + a_{|C|-2}x^{|C|-2} + \cdots + a_{|C|-k}$, and hence

$$R = \sum_{i=0}^{\frac{n}{k}-1} \sum_{j=0}^{k-1} (a_{ki+j} - a_{(n-k)+j})x^{ki+j},$$

and so $R = 0$ if and only if S is k-periodic. □

Here is a simple property of root sets.

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

Theorem 5.2. *Let p, q be distinct primes and let S be some subset of $\mathbb{Z}_{pq}$. If $pq \in r(S)$, then either $p \in r(S)$ or $q \in r(S)$, and hence S is p-periodic or q-periodic.*

Proof. Since $pq \in r(S)$, $C_{pq}|P_S$. Now x is a primitive pqth root of unity if and only if it is a factor of both $\frac{x^{pq}-1}{x^p-1}$ and $\frac{x^{pq}-1}{x^q-1}$. Therefore C_{pq} is the greatest common divisor of $\frac{x^{pq}-1}{x^p-1}$ and $\frac{x^{pq}-1}{x^q-1}$.

If C_{pq} is a factor of P_S, as $\mathbb{Z}[X]$ is a Euclidean domain, there must therefore exist polynomials P_1 and P_2 such that $P_S = P_1\frac{x^{pq}-1}{x^p-1} - P_2\frac{x^{pq}-1}{x^q-1}$. Now, there exists Q_1, R_1 with $P_1 = Q_1\frac{x^p-1}{x-1} + R_1$ and $\deg R_2 < p-1$, and Q_2, R_2 with $P_2 = Q_2\frac{x^q-1}{x-1} + R_2$ and $\deg R_2 < q-1$. Then $P_S = R_1\frac{x^{pq}-1}{x^p-1} - R_2\frac{x^{pq}-1}{x^q-1}$.

Suppose that a_ix^i is a term in R_1 and b_jx^j is a term in R_2. Then, by the Chinese Remainder Theorem, there exists a k with $0 \leqslant k < pq$ such that $k = i + pt$ for some $0 \leqslant t < q$ and $k = j + qu$ for some $0 \leqslant u < q$. Then the x^k coefficient of the right-hand side is $a_i - b_j$. Of the left-hand side it is 0 or 1. Therefore $a_i \in \{b_j, b_j + 1\}$ for all i, j.

Now since $b_{q-1} = 0$, this means that $a_i \in \{0, 1\}$ for all i. Since $a_{p-1} = 0$, this means that $b_j \in \{0, -1\}$ for all j. Also, it is not possible that some $a_i = 1$ and some $b_j = -1$. Therefore either $a_i \equiv 0$ for all i, in which case P_S is a multiple of $\frac{x^{pq}-1}{x^q-1}$ and $p \in r(S)$, or $b_j \equiv 0$ for all j, in which case P_S is a multiple of $\frac{x^{pq}-1}{x^q-1}$ and $q \in r(S)$. If $p \in r(S)$, then all factors of pq which are not factors of q are in $r(S)$, and so S is q-periodic. Similarly, if $q \in r(s)$, then S is p-periodic. □

This can be generalized to a bigger setting.

Corollary 5.3. *Let p, q be distinct primes, and let S be some subset of $\mathbb{Z}_{pqn}$. Suppose that $r(S)$ contains all factors of n (other than 1) and all factors of pqn which are not themselves factors of pn or qn. Then $r(S)$ must contain pn or qn.*

Proof. Define subsets $S_0, S_1, \ldots, S_{n-1}$ of $\mathbb{Z}_{pq}$ by $i \in S_j \Leftrightarrow (ni + j) \in S$. Then

$$P_S(z) = \sum_{i=0}^{n-1} x^i P_{S_i}(x^n).$$

Note that all factors of n are in $r(S)$, and hence (by Theorem 5.1) S is n-balanced, so each S_i has the same number of elements. If $|S_i| \equiv 0$ or $|S_i| \equiv pq$, then $S = \emptyset$ or $\mathbb{Z}_{pqn}$ respectively. Either way $r(S)$ contains all factors of pqn (except possibly 1), and the theorem is proved. Therefore assume that $0 < |S_i| < pq$.

Further, every integer j which is a factor of pqn, but not of pn or qn, is of the form pqi with i a factor of n. Therefore $i \in r(S)$. Thus every common root of $\frac{x^{pqn}-1}{x^{pn}-1}$ and $\frac{x^{pqn}-1}{x^{qn}-1}$ is a root of P_S.

Therefore, $P_S = T\frac{x^{pqn}-1}{x^{pn}-1} + U\frac{x^{pqn}-1}{x^{qn}-1}$ for some polynomials T, U. Then splitting T, U up as

$$T = \sum_{i=0}^{n-1} x^i T_i(x^n) \quad \text{and} \quad U = \sum_{i=0}^{n-1} x^i U_i(x_n),$$

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

it follows that $P_{S_i}(z) = T_i\frac{x^{pq}-1}{x^p-1} + U_i\frac{x^{pq-1}}{x^q-1}$. Therefore $pq \in r(S_i)$ and hence by Theorem 5.2, S_i is either p-periodic or q-periodic. Since $0 < |S_i| < pq$, $|S_i|$ is not divisible by both p or q. Therefore the period of S_i can be detected from $|S_i|$, and hence is independent of i.

Therefore either S_i is p-periodic for all i, or S_i is q-periodic for all i. In the first case, S is clearly np-periodic, and hence $r(S)$ contains qn by Theorem 5.1. In the second case, S is clearly nq-periodic, and hence $r(S)$ contains pn by Theorem 5.1. □

This corollary, when viewed in combination with Theorem 4.6, will give the remaining upper bounds.

6. Upper bound for p^2q

Let S_1, S_2 be subsets of $\mathbb{Z}_{p^2q}$ which are not translates but have the same 3-deck. Let f be the double Fourier function.

Theorem 6.1. *It must hold that $f(p)f(q) \neq 0$ and $f(p)^q \neq f(q)^p$. Therefore $f(pq) = 0$ and $f(1) = 0$.*

Proof. By Theorem 4.5, f is not trivial (as S_1, S_2 are not translates). Therefore by Theorem 4.6, there are x, y, z such that $xyz|n$, $f(xy)f(xz) \neq 0$, $f(xy)^z \neq f(xz)^y$, $\gcd(y, z) = 1$, $y \neq 1$, $z \neq 1$. Note that, by Corollary 4.4, $f(k)$ is a $\frac{n}{k}$th root of unity for all $k|n$. Hence xyz cannot be equal to n, as if it were, $f(xy)^z$ would be equal to 1, as would $f(xz)^y$.

Looking for x, y, z with $xyz|p^2q$, $\gcd(y, z) = 1$, $y \neq 1$ and $z \neq 1$ shows that of y, z, one must be a power of p, the other a power of q. That $xyz < p^2q$ implies $x = 1$ and $\{y, z\}$ are $\{q, p\}$. Therefore $f(p)f(q) \neq 0$ and $f(p)^q \neq f(q)^p$.

Now if $f(1) \neq 0$, by Corollary 4.4, $f(p) = f(1)^p$ and $f(q) = f(1)^q$, whence $f(p)^q = f(q)^p = f(1)^{pq}$, causing a contradiction. Similarly, if $f(pq) \neq 0$, $f(pq) = f(p)^q = f(q)^p$. □

It turns out that these conditions on f are enough to contradict Corollary 5.3.

Corollary 6.2. *No such S_1, S_2 can exist. Therefore $r(\mathbb{Z}_{p^2q}) \leqslant 3$.*

Proof. Theorem 6.1 states that $f(1) = 0$, $f(p) \neq 0$, $f(q) \neq 0$ and $f(pq) = 0$. In terms of $r(S_i)$, this translates to $p^2q, p \in r(S_i)$ and $p^2, pq \notin r(S_i)$.

Now apply Corollary 5.3 with $n = p$. The conditions hold: $r(S_i)$ contains all factors of p other than 1, and all factors of p^2q which are not factors of p^2 or pq. The theorem must apply, and hence $r(S_i)$ must contain p^2 or pq, which it does not. □

7. Upper bound for pqr

Let S_1, S_2 be subsets of C which are not translates, but have the same 3-deck, where $|C|$ is the product of three distinct primes, which have yet to be labelled. Let f be the double Fourier function.

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

Theorem 7.1. *There are two prime factors p, q of n such that $f(p)f(q) \neq 0$ and $f(p)^q \neq f(q)^p$. Therefore $f(pq) = 0$ and $f(1) = 0$.*

Proof. As in the proof of Theorem 6.1, there are x, y, z with $xyz||C|$ such that $f(xy)f(xz) \neq 0$, $f(xy)^z \neq f(xz)^y$, $\gcd(y, z) = 1$, $y \neq 1$, $z \neq 1$ and $xyz < |C|$.

Since y has at least 1 prime factor, z has at least 1 prime factor, and xyz has at most 2 prime factors, it follows that $x = 1$ and y and z are prime. Label $p = y$, and $z = q$. Then $f(p)^q \neq f(q)^p$ and $f(p)f(q) \neq 0$.

As in the proof of Theorem 6.1, it follows that $f(pq) = 0$ and $f(1) = 0$. □

Let r be the remaining prime factor of $|C|$.

Theorem 7.2. $f(r) = 0$.

Proof. Express r as $pc + qd$. Then $r = p(c + qt) + q(d - pt)$. Now since r is an odd prime and not a factor of q, there exists a t such that r is not a factor of $c + qt$ or $c + q(t + 1)$. Set $a = c + qt$ and $b = d - pt$.

Note that since r is not a factor of pa, it is not a factor of qb. Also, since $pa = r - qb$, q is not a factor of pa, and similarly p is not a factor of qb. Therefore $\gcd(qb, pqr) = q$, and hence $f(-qb)$ is a conjugate of $f(q)$, so $f(-qb) \neq 0$. Therefore by Corollary 4.4 $f(-qb) = f(q)^{-b}$. Similarly, $f(-pa) = f(p)^{-a}$. Therefore, since $f(x)f(y)f(z) \in \{0, 1\}$ for all x, y, z with $x + y + z = 0$, it follows that $f(r)f(p)^{-a}f(q)^{-b} \in \{0, 1\}$. Hence, if $f(r) \neq 0$, $f(r) = f(p)^a f(q)^b$.

Similarly, if $f(r) \neq 0$, $f(r) = f(p)^{a+q}f(q)^{b-p} = f(p)^a f(q)^b \frac{f(p)^q}{f(q)^p} = \frac{f(p)^q}{f(q)^p} f(r)$. However, $\frac{f(p)^q}{f(q)^p} \neq 1$ from Theorem 7.1. Thus $f(r) = 0$. □

The required contradiction is now in place.

Corollary 7.3. *No such S_1, S_2 can exist. Therefore $r(\mathbb{Z}_{pqr}) \leqslant 3$.*

Proof. We know that $f(z) = 0$ for $z \in \{1, r, pq\}$ and $f(z) \neq 0$ for $z \in \{p, q\}$. This means that $\{r, pq, pqr\} \subseteq r(S_i)$ and $\{pr, qr\} \cap r(S_i) = \emptyset$.

Then apply Corollary 5.3 with $n = r$. The conditions hold: $r(S)$ contains all factors of r other than 1, and all factors of pqr which are not factors of pr or qr. Therefore the theorem must apply, and $r(S)$ must contain pr or qr, contradicting what has already been shown. □

All of the bounds have now been proved.

8. Conclusion

Proof of Theorem 1.3. If $|C| = 1, 3$, then the all-white necklace and all-black necklace are distinct, but are 0-isomorphic. Therefore $r(|C|) \geqslant 1$. If $|C| = 1$, by Corollary 1.2, $r(C) \leqslant 1$. If $|C| = 3$, by Theorem 4.8, $r(C) \leqslant 1$. Therefore $r(C) = 1$.

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press

If $|C| = 5$, then by Theorem 2.1, $r(C) \geqslant 2$. By Theorem 4.8, $r(C) \leqslant 2$. Therefore $r(C) = 2$.

Theorem 1.3 claims that $r(C) = 3$ whenever C is a cyclic group of odd order of the form p^k, pq, pqr or p^2q. Suppose $|C|$ is such an integer. Then $r(C) \geqslant 3$ by Theorem 2.2. Now if $|C|$ is of the form p^k or pq, $r(C) \leqslant r_m(C) = 3$ by Theorem 4.7. If $|C|$ is of the form p^2q, $r(C) \leqslant 3$ by Corollary 6.2, and if $|C|$ is of the form C, by Corollary 7.3.

Finally, if $|C| > 5$ and $|C|$ is not of the form p^k, pq, pqr or p^2q, by Corollary 3.3, $r(C) \geqslant 4$. By Theorem 4.7, $r(C) \leqslant r_m(C) = 4$. □

Some progress has been made applying the methods of this paper to cyclic groups C of even order. Having solved many cases, I make the following conjecture.

Conjecture 8.1. $r(C) = 4$ *for all cyclic groups of even order with* $|C| > 10$.

The method which has worked for many even $|C|$ (including all $|C| < 240$) is to find properties that must be true of the root set $r(S)$ for any S which is not 4-reconstructible, and then show that no $r(S)$ can satisfy these properties.

References

[1] Alon, N., Caro, Y., Krasikov, I. and Roditty, Y. (1989) Combinatorial reconstruction problems. *J. Combin. Theory Ser. B* **47** 153–161.

[2] Pebody, L. (2004) The reconstructibility of finite abelian groups. *Combin. Probab. Comput.* **13** 867–892.

[3] Radcliffe, A. J. and Scott, A. D. (1998) Reconstructing subsets of $\mathbb{Z}_n$. *J. Combin. Theory Ser. A* **83** 167–198.

https://doi.org/10.1017/S0963548306007875 Published online by Cambridge University Press