Reconstructing subsets of $\mathbb{Z}_n$

A.J. Radcliffe [1]
Department of Mathematics and Statistics
University of Nebraska-Lincoln
Lincoln, NE 68588-0323

A.D. Scott
Department of Mathematics, University College
Gower Street, London WC1E 6BT
and
Trinity College, Cambridge CB2 1TQ, England

[1]Partially supported by NSF Grant DMS-9401351

Abstract

In this paper we consider the problem of reconstructing a subset $A \subset \mathbb{Z}_n$, up to translation, from the collection of its subsets of size k, given up to translation (its k-*deck*). Results of Alon, Caro, Krasikov, and Roditty [1] show that this is possible provided $k > \log_2 n$. Mnukhin [10] showed that every subset of $\mathbb{Z}_n$ of size k is reconstructible from its $(k-1)$-deck, provided $k \geq 4$. We show that when n is prime every subset of $\mathbb{Z}_n$ is reconstructible from its 3-deck; that for arbitrary n almost all subsets of $\mathbb{Z}_n$ are reconstructible from their 3-decks; and that for any n every subset of $\mathbb{Z}_n$ is reconstructible from its $9\alpha(n)$-deck, where $\alpha(n)$ is the number of distinct prime factors of n. We also comment on analogous questions for arbitrary groups, in particular the cube $\mathbb{Z}_2^n$.

Our approach is to generalize the problem to that of reconstructing arbitrary rational functions on $\mathbb{Z}_n$. We prove — by analysing the interaction between the ideal structure of the group ring $\mathbb{Q}\,\mathbb{Z}_n$ and the operation of pointwise multiplication of functions — that with a suitable definition of deck every rational-valued function on $\mathbb{Z}_n$ is reconstructible from its $9\alpha(n)$-deck.

1 Introduction.

The reconstruction problem has a long history, started by the Reconstruction Conjecture (in 1941) and the Edge Reconstruction Conjecture (in 1960). The very general problem is to reconstruct a combinatorial object (up to isomorphism) from the collection of isomorphism classes of its subobjects (see Bondy [2] and Bondy and Hemminger [3] for discussion of the two classical problems). Of course it is the word "isomorphism" in the last sentence which makes the problem interesting.

In this paper we consider the problem of reconstructing subsets of the cyclic group $\mathbb{Z}_n$ from their subsets. The information provided about a subset of $\mathbb{Z}_n$ is the multiset of isomorphism classes of its subsets of fixed size k, where two subsets are isomorphic if one subset is a translate of the other in $\mathbb{Z}_n$. We call this collection the *k-deck* of a set in $\mathbb{Z}_n$. We say that a set $A \subset \mathbb{Z}_n$ with $|A| \geq k$ is *reconstructible from its k-deck* if any set $B \subset \mathbb{Z}_n$ having the same k-deck is a translate of A.

Maybe the first thing to notice is that for $|A| \geq k$ one can reconstruct the l-deck of A from the k-deck for any $l \leq k$. This is analogous to Kelly's lemma (see [2]). On the other hand if $|A| < k$ then the k-deck of A is empty, and therefore A cannot be distinguished from any other subset of size strictly less than k. It makes the statement of our theorems slightly easier if we use a definition of deck for which this issue does not arise. The definition we adopt below regards the deck as a function on multisets of size k from $\mathbb{Z}_n$. It is straightforward to check that this form of the k-deck can be determined from the deck as defined above, provided $|A| \geq k$.

Definition 1 Let n be a positive integer and let $X \subset \mathbb{Z}_n$. The *k-deck* of X is the function defined on multisets Y from $\mathbb{Z}_n$ of size k by

$$d_{X,k}(Y) = |\{i \in \mathbb{Z}_n : \operatorname{supp}(Y + i) \subset X\}|,$$

where $\operatorname{supp}(Y)$ is the set of elements of Y, considered without multiplicity. We say that X is *reconstructible from its k-deck* if we can deduce X up to translation from its k-deck; in other words, we have

$$d_{W,k} \equiv d_{X,k} \Rightarrow W = X + i, \text{for some } i \in \mathbb{Z}_n.$$

More generally we say that a function of X is *reconstructible from the k-deck of X* if its value is a function of $d_{X,k}$. ■

Thus in $\mathbb{Z}_{12}$ the sets $\{1, 2, 4, 8\}$ and $\{1, 2, 5, 7\}$ are not distinguishable from their 2-decks, but are reconstructible from their 3-decks. In fact, any two cyclic difference sets in $\mathbb{Z}_n$ will have the same 2-deck (viz., each possible pair with multiplicity 1). Since there are non-equivalent cyclic difference sets for arbitrarily large n (see [5]), there are subsets of $\mathbb{Z}_n$ for infinitely many n which are not reconstructible from their 2-decks. There are more elementary examples: A cannot be distinguished from $-A$ by examining their 2-decks; $A + B$ and $A - B$ have the same 2-deck for any subsets $A, B \subset \mathbb{Z}_n$. This last example also shows that for sufficiently large n we cannot hope to reconstruct even up to reflection by looking solely at the 2-deck.

It is straightforward to check that the l-deck of $X \subset \mathbb{Z}_n$ is reconstructible from the k-deck for $l \leq k$.

Alon, Caro, Krasikov and Roditty [1] consider the closely related problem of reconstructing subsets of $\mathbb{Z}_n$ under the natural action of D_n. Two sets $X, Y \subset \mathbb{Z}_n$ are *D_n-isomorphic* or *isomorphic up to reflection* if $X = Y + i$ or $X = -Y + i$ for some $i \in \mathbb{Z}_n$. The *k-deck of $X \subset \mathbb{Z}_n$ given up to reflection* is the function $D_{X,k}$ on multisets Y of size k from $\mathbb{Z}_n$, where $D_{X,k}(Y) = d_{X,k}(Y)$ if Y and $-Y$ are isomorphic up to translation and $D_{X,k}(Y) = d_{X,k}(Y) + d_{X,k}(-Y)$ otherwise. We say that X is *reconstructible up to reflection* if $D_{X,k} \equiv D_{W,k}$ implies that W and X are isomorphic up to reflection.

For $n \geq 1$, we define $f(n)$ to be the smallest k such that every $X \subset \mathbb{Z}_n$ is reconstructible from its k-deck. We define $F(n)$ to be the smallest K such that every $X \subset \mathbb{Z}_n$ is reconstructible up to reflection from its k-deck; it is easily checked that $F(n) \geq f(n)$. Alon, Caro, Krasikov and Roditty [1] proved that

$$F(n) \leq \log_2 n + 1,$$

which implies that

$$f(n) \leq \log_2 n + 1.$$

The example given above shows that, for sufficiently large n,

$$f(n) \geq 3.$$

The main result of this paper (Theorem 18) is that

$$f(n) \leq 9\alpha(n),$$

where $\alpha(n)$ is the number of distinct prime factors of n, while for p prime we prove (Theorem 3) that

$$f(p) \leq 3,$$

which is best possible for p sufficiently large. Thus $f(n)$ does *not* tend to infinity with n. This suggests that either $f(n) \leq C$ for some absolute constant C or else that $f(n)$ is sensitive to the precise multiplicative structure of n. We conjecture that it is the latter.

Conjecture 1 $f(n)$ is unbounded as n tends to infinity.

Note that the bound in terms of $\alpha(n)$ implies

$$f(n) \leq (9 + o(1)) \ln n / \ln \ln n,$$

(see §22.12 of Hardy and Wright [7]; note that we use $\alpha(n)$ for their $\omega(n)$) which is smaller than $\ln n$ for all sufficiently large n. Furthermore, for almost every n, we have

$$f(n) \leq (9 + o(1)) \ln \ln n$$

(this follows immediately from Theorem 436 of Hardy and Wright [7]). For most sets, however, we can do much better: we prove below (Theorem 4) that as $n \to \infty$, almost every $X \subset \mathbb{Z}_n$ is reconstructible from its 3-deck.

These results also yield improvements on the result of Alon, Caro, Krasikov and Roditty [1]. It is proved in [12] that

$$F(n) \leq 2f(n).$$

Thus the results above imply that for any n

$$F(n) \leq 18\alpha(n),$$

while for p prime

$$F(n) \leq 6.$$

Furthermore, as $n \to \infty$, almost every $X \subset \mathbb{Z}_n$ is reconstructible up to reflection from its 6-deck given up to reflection.

The way in which we prove our main result is somewhat unexpected. We generalize the objects being reconstructed and the notion of k-deck. To be precise we consider reconstructing arbitrary rational-valued functions on $\mathbb{Z}_n$, and base our results on a careful analysis of the ideal structure of the group ring $\mathbb{Q}\,\mathbb{Z}_n$, and its interaction with the operation of pointwise multiplication.

We begin in Section 2, however, with a simpler proof which implies that subsets of $\mathbb{Z}_p$ for p prime are reconstructible from their 3-decks, and gives as a corollary that, as n tends to infinity, almost all subsets of $\mathbb{Z}_n$ are reconstructible from their 3-decks. In Section 3 we describe the basic setup for the general proof and give some definitions that we shall need. In Section 4 we prove the results we need concerning the $\star$-product operation, defined in Section 3. In Section 5 we prove the algebraic facts that we require, and the proof of our main theorem is completed in Section 6. In Section 7 we consider the action of $\mathbb{Z}_2^n$ on itself and make some remarks on the situation for arbitrary groups.

We use χ_A throughout to refer to the characteristic function of a set A. We will frequently use the arithmetic of $\mathbb{Z}_n$ without further comment, for instance in subscripts.

2 The case of prime n.

In this section we present a rather quick and straightforward proof that if p is a prime then $f(p) \leq 3$. Though couched in slightly different language than our later general proof, it should make the later work more transparent.

We start with two simple lemmas; the first of which allows us to identify a sequence which is a translate of $(1, 0, 0, \ldots, 0)$, and the second of which shows that the identification can be made based only on the 3-deck.

Lemma 1 *If $(c_i)_{i=0}^{n-1}$ is a sequence of real numbers satisfying the two conditions $\sum_{i=0}^{n-1} c_i^2 = 1$, and $\sum_{i=0}^{n-1} c_i^3 = 1$ then all the c_i are zero, except for one which is 1.*

Proof. Since $\sum c_i^2 = 1$ we have that $|c_i| \leq 1$ for $i = 0, 1, \ldots, n-1$. Hence we have $1 = \sum c_i^3 \leq \sum |c_i|^3 \leq \sum c_i^2 = 1$. We must have therefore that $|c_i|^3 = c_i^2$ for $i = 0, 1, \ldots, n-1$, and hence that each c_i belongs to $\{-1, 0, 1\}$. The condition on $\sum c_i^2$ establishes that there is one non-zero coefficient, and the condition on $\sum c_i^3$ shows that that coefficient is 1. ∎

Lemma 2 *For any $k \leq n$, any set $A \subset Z_n$, and any multiset $\{i_1, i_2, \ldots, i_k\}$ from $\mathbb{Z}_n$ we can reconstruct the size of $(A - i_1) \cap (A - i_2) \cap \cdots \cap (A - i_k)$ from the k-deck of A.*

Proof. This size is simply $d_{A,k}(\{i_1, i_2, \ldots, i_k\})$. ∎

These preliminaries out of the way, we turn to the main result of this section: that for p prime we can reconstruct all subsets of $\mathbb{Z}_p$ from their 3-decks.

Theorem 3 *If p is prime then any subset of $\mathbb{Z}_p$ can be reconstructed from its 3-deck.*

Proof. Consider a subset $A \subset \mathbb{Z}_p$ and another, B say, with the same 3-deck as A. We associate with A the circulant matrix $M_A = [m_{ij}]$ defined by $m_{ij} = \chi_A(j-i)$, $i, j = 0, 1, \ldots, n-1$. If we write Z for the fundamental circulant matrix $Z = [z_{ij}]$, $z_{ij} = \delta_{(i+1)j}$, then $M_A = \sum_{j \in A} Z^j$. Since the eigenvalues of Z are exactly the p^{th} roots of unity ζ_p^i, $i = 0, 1, \ldots, p-1$, (where $\zeta_p = \mathrm{e}^{2\pi i/p}$) it follows that M_A has eigenvalues $\sum_{j \in A} \zeta_p^{ij}$, $i = 0, 1, \ldots, p-1$. We distinguish two cases, according to whether M_A is invertible or not.

Case 1. M_A is invertible

M_A has (circulant) inverse Λ, with first row λ_i, $i = 0, 1, \ldots, p-1$. Now consider the (circulant) matrix $C = \Lambda M_B$, with first row c_i, $i = 0, 1, \ldots, p-1$. We claim that $(c_i)_{i=0}^{n-1}$ satisfies the conditions of Lemma 1 above. To show this, we will prove that $\sum_{j=0}^{p-1} c_j^r$, $r = 2, 3$, considered as functions of B, are reconstructible from the 3-deck of B. Knowing this, we conclude that these expressions must take on the same value as they do for $\Lambda M_A = I$. Well,

$$\begin{aligned}
\sum_{i=0}^{p-1} c_i^2 &= \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \lambda_j \chi_B(j-i) \right)^2 \\
&= \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \lambda_j \lambda_k \sum_{i=0}^{p-1} \chi_B(j-i)\chi_B(k-i) \\
&= \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \lambda_j \lambda_k |(B-j) \cap (B-k)|.
\end{aligned}$$

By Lemma 2 the factor $|(B-j) \cap (B-k)|$ occuring in the innermost sum on the last line can be determined from the 2-deck of B. Hence the entire sum can be computed from the 2-deck of B (and hence from the 3-deck of B). The sum of the c_i^3 can be determined the same way:

$$\begin{aligned}
\sum_{i=0}^{p-1} c_i^3 &= \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \lambda_j \chi_B(j-i) \right)^3 \\
&= \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \sum_{l=0}^{p-1} \lambda_j \lambda_k \lambda_l \sum_{i=0}^{p-1} \chi_B(j-i)\chi_B(k-i)\chi_B(l-i) \\
&= \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \sum_{l=0}^{p-1} \lambda_j \lambda_k \lambda_l |(B-j) \cap (B-k) \cap (B-l)|.
\end{aligned}$$

The last expression is, by Lemma 2, reconstructible from the 3-deck of B.

Thus all three expressions are determined by the 3-deck of B. Since this is by hypothesis the same as the 3-deck of A, it must be that these expression take the same value for ΛM_B as for $\Lambda M_A = I$, i.e., each takes the value 1. Thus by Lemma 1 $(c_i)_{i=0}^{n-1}$ is a standard unit vector, and so $\Lambda M_B = Z^k$ for some k in $\{0, 1, \ldots, p-1\}$. Thus $M_B = Z^k M_A$ and $B = A + k$. Thus A can be reconstructed from its 3-deck.

Case 2. M_A is not invertible

First note that $\emptyset \subset \mathbb{Z}_n$ is the only subset whose 1-deck is identically zero, so we may suppose $A \neq \emptyset$. Since the eigenvalues of A are the p values $\alpha_i = \sum_{j \in A} \zeta_p^{ij}$, for $i = 0, 1, \ldots, p-1$, in order for A to be singular there must exist $i \in \{0, 1, 2, \ldots, p-1\}$ with $\alpha_i = 0$. Now $\alpha_0 = |A| \neq 0$ so we must have $0 < i \leq p-1$. The minimal polynomial of ζ_p^i is $m_p(x) = \sum_{j=0}^{p-1} x^j$ while $\sum_{j \in A} (\zeta_p^i)^j = 0$. Thus we must have $m_p(x) \mid \sum_{j \in A} x^j$. This implies that $A = \{0, 1, \ldots, p-1\}$, which is certainly reconstructible from its 3-deck. ∎

Using a similar method we can show that almost all subsets of $\mathbb{Z}_n$ are reconstructible from their 3-decks.

Theorem 4 *The proportion of subsets of $\mathbb{Z}_n$ which are* not *reconstructible from their 3-decks tends to 0 as n tends to infinity.*

Proof. The proof of Theorem 3 applies equally here, provided that the matrix M_A is invertible. This requires that $\sum_{j \in A} \zeta_n^{ij} \neq 0$, $i = 0, 1, \ldots, n-1$. If we write p_A for the polynomial $\sum_{j \in A} x^j$ then we aim to show that the fraction of subsets $A \subset \mathbb{Z}_n$ for which there exists $i \in \{0, 1, \ldots, n-1\}$ with $p_A(\zeta_n^i) = 0$ tends to zero as n tends to infinity.

Kleitman's extension [9] of Erdős's theorem [6] concerning the Littlewood-Offord problem states that if $(x_i)_{i=1}^n$ is collection of vectors from some normed space with $\|x_i\| \geq 1$, $i = 1, 2, \ldots, n$, then at most $\binom{n}{\lfloor n/2 \rfloor}$ of the subset sums $\left\{\sum_{i \in B} x_i \,:\, B \subset \{1, 2, \ldots, n\}\right\}$ can belong to any fixed set of diameter 1. In particular if we consider, for fixed i, the collection of complex numbers $\{\zeta_n^{ij} \,:\, j = 0, 1, \ldots, n-1\}$, at most $\binom{n}{\lfloor n/2 \rfloor}$ sets $A \subset \mathbb{Z}_n$ can have $p_A(\zeta_n^i) = \sum_{j \in A} \zeta_n^{ij} = 0$. Thus for any fixed i at most $\binom{n}{\lfloor n/2 \rfloor}$ subsets of $\mathbb{Z}_n$ have ζ_n^i as a root of p_A.

To complete the proof note that the minimal polynomial of ζ_n^i is the cyclotomic polynomial $\Phi_{n/(n,i)}$ and if $p(x)$ is any polynomial we have $p(\zeta_n^i) = 0$ iff $\Phi_{n/(n,i)} \mid p$. Thus $p_A(\zeta_n^i) = 0$ for some i iff $p_A(\zeta_n^d) = 0$ for some *divisor* d of n. Thus the fraction of subsets $A \subset \mathbb{Z}_n$ with $p_A(\zeta_n^i) = 0$ for some i is at most $d(n)\binom{n}{\lfloor n/2 \rfloor}/2^n$

where $d(n)$ is the number of divisors of n. Since $\binom{n}{\lfloor n/2 \rfloor}/2^n = O(n^{-1/2})$ and $d(n) = o(n^\epsilon)$ for every $\epsilon > 0$ (see Theorem 315 of Hardy and Wright [7]) this proportion tends to zero as n tends to infinity. ∎

It seems to us an exceptionally natural question to ask whether the result of Theorem 4 holds for the 2-deck as well, to the extent that is possible.

Conjecture 2 Almost every subset of $\mathbb{Z}_n$ is reconstructible up to reflection from its 2-deck.

3 The approach for general n.

In this section we outline our approach to the problem of reconstructing subsets of $\mathbb{Z}_n$ when n is not prime.

Alon, Caro, Krasikov and Roditty [1] deduce their result, that $F(n) \leq \log_2 n + 1$, from a general result about reconstructing sets under the action of permutation groups. Several other authors, including Cameron [4], Mnukhin [10], and Pouzet [11] have looked at such reconstruction problems. Indeed, from one point of view *every* reconstruction problem concerns the action of a group on the collection of combinatorial objects being reconstructed, and on their subobjects.

Definition 2 Let Γ be a permutation group acting on a set Ω. We say two sets $X, Y \subset \Omega$ are *isomorphic* if $gX = Y$ for some $g \in \Gamma$. For $X \subset \Omega$, the *k-deck* of X is the function defined on multisets from Ω of size k by

$$d_{X,k}(Y) = |\{g \in \Gamma : \mathrm{supp}(gY) \subset X\}|.$$

We say that Γ *is reconstructible from its k-deck* if

$$d_{X,k} \equiv d_{Y,k} \Rightarrow X = gY \text{ for some } g \in \Gamma.$$

∎

Thus the Edge Reconstruction conjecture claims that every subset E of $X^{(2)}$ of size 4 or more is reconstructible from its $(|E|-1)$-deck under the induced action of the symmetric group Σ_X on $X^{(2)}$. Mnukhin [10] deals with the action of $\mathbb{Z}_n$ on itself, and proves that all k-subsets of $\mathbb{Z}_n$ are reconstuctible from their $(k-1)$-decks, provided $k \geq 4$.

Our approach is to consider not just subsets of G but the larger class of rational-valued functions on the group, where we associate $S \subset G$ with its characteristic function $\chi_S : G \to \{0,1\}$. Clearly there is an action of G on this set of functions given by

$$g.f(x) = f(g^{-1}x)$$

for $g \in G$ and $f : G \to \mathbb{Q}$. Note that the set of rational-valued functions on G under the action of G can be identified with the elements of the group ring $\mathbb{Q}G$. Consideration of this larger class requires us to refine our notion of deck. Since we can think of elements of $\mathbb{Q}\mathbb{Z}_n$ as generalizations of multisets from $\mathbb{Z}_n$, it is natural that the deck of $\alpha \in \mathbb{Q}\mathbb{Z}_n$ should be a function defined on the set of all multisets from $\mathbb{Z}_n$ of size k, agreeing with our earlier convention about the k-deck for subsets.

Definition 3 If $f \in \mathbb{Q}G$ and $k \geq 1$ the *k-deck* of f is the function defined on multisets of G of size k by

$$d_{f,k}(Y) = \sum_{g \in G} \prod_{x \in gY} f(x).$$

We say that f is *reconstructible from its k-deck* if

$$d_{f,k} \equiv d_{f',k} \Rightarrow f' = g.f \text{ for some } g \in G.$$

We define $r_{\mathbb{Q}}(G)$ to be the smallest k such that every function $f : G \to \mathbb{Q}$ is reconstructible from its k-deck. Again we loosely talk of an expression involving f being reconstructible from the k-deck if any two elements of $\mathbb{Q}G$ with the same k-deck have the same value for that expression. ■

Definition 4 If $f \in \mathbb{Q}G$ and f' is another element of the group ring with the property that $d_{f,k} \equiv d_{f',k}$ and yet there is no $g \in G$ with $f' = g.f$ then we say that f' is a *k-imposter* for f. ■

Remark 1 There is another plausible notion of k-deck for elements of $\mathbb{Q}G$. One could consider the collection of all partial functions obtained by restricting f to subsets of G of size k. The deck defined above is reconstructible from such a deck, thus the results we prove apply just as well to this notion of deck.

Remark 2 Note that, for $S \subset G$, we have $d_{\chi_S,k} \equiv d_{S,k}$.

Remark 3 In the case $G = \mathbb{Z}_n$ we have, for $I = \{i_1, i_2, \ldots, i_k\}$ a multiset of size k,

$$d_{f,k}(I) = \sum_{j=0}^{n-1} f(j+i_1)f(j+i_2)\ldots f(j+i_k).$$

We will eventually show that every element of the group ring $\mathbb{Q}\,\mathbb{Z}_n$ can be reconstructed from its $9\alpha(n)$-deck; in the rest of this section we discuss $\mathbb{Q}\,\mathbb{Z}_n$ and its ideals.

The first thing to notice is that the group ring $\mathbb{Q}\,\mathbb{Z}_n$ is isomorphic to the ring $Q_n = \mathbb{Q}\,[x]/(x^n - 1)$. The action of $\mathbb{Z}_n$ on $\mathbb{Q}\,\mathbb{Z}_n$ is isomorphic to the action of $\mathbb{Z}_n$ on Q_n given by $i.\alpha = x^i\alpha$. We write (abusing notation slightly) $\alpha = \sum_{j=0}^{n-1} a_j x^j$ for a typical element of Q_n, where properly we should indicate that we are dealing with equivalence classes of polynomials.

Q_n is of course a vector space over $\mathbb{Q}$ in a natural way; is a subring of $C_n = \mathbb{C}[x]/(x^n - 1)$; and comes equipped with the inner product $\langle \alpha, \beta \rangle = \sum_{j=0}^{n-1} a_j b_j$, with respect to which the collection $\{x^j : j = 0, 1, \ldots, n-1\}$ forms an orthonormal basis. When we discuss Q_n we will think of the indices as elements of $\mathbb{Z}_n$; in particular we will perform all arithmetic on subscripts in $\mathbb{Z}_n$.

One way we will investigate Q_n is through the Fourier transform, which we will consider in Section 5. This requires us to widen our viewpoint somewhat, since the natural domain for the Fourier transform is C_n (which is of course the same thing as $\mathbb{C}\mathbb{Z}_n$). The Fourier transform is an isomorphism between C_n and the ring $\mathbb{C}^n$, equipped with pointwise multiplication.

The *support* of an element $\alpha = \sum_{j=0}^{n-1} a_j x^j \in Q_n$ is the set $\operatorname{supp}(\alpha) = \{j : a_j \neq 0\} \subset \mathbb{Z}_n$. Similarly, the *support* of a sequence is the set of places where it takes a non-zero value, and the support of a multiset is the set of its elements considered without multiplicity.

We will want to consider the following operation (of pointwise multiplication of coefficients) on the ring Q_n.

Definition 5 Given two elements of Q_n define their *star product* to be

$$\left(\sum_{j=0}^{n-1} a_j x^j\right) \star \left(\sum_{j=0}^{n-1} b_j x^j\right) = \left(\sum_{j=0}^{n-1} a_j b_j x^j\right).$$

In particular we will consider expressions of the following form. Given a multiset $I = \{i_1, i_2, \ldots, i_l\}$ from $\{0, 1, \ldots, n-1\}$ define

$$\alpha^I = (x^{i_1}\alpha) \star (x^{i_2}\alpha) \star \cdots \star (x^{i_l}\alpha).$$

A linear combination of such expressions, e.g., $p(\alpha) = \sum_{I\in\mathcal{I}} \lambda_I \alpha^I$, we call a $\star$-*polynomial*. The *degree* of p is defined to be $\max\{|I| : I \in \mathcal{I}\}$. We are also interested in the linear map $S : Q_n \to \mathbb{Q}$ defined by

$$S\left(\sum_{j=0}^{n-1} a_j x^j\right) = \sum_{j=0}^{n-1} a_j$$

and the compositions $S \circ p$ for $\star$-polynomials p. Therefore define the $\star$-*term* corresponding to the multiset $I = \{i_1, i_2, \ldots, i_l\}$ from $\{0, \ldots, n-1\}$ to be the function $S_I : Q_n \to \mathbb{Q}$ given by $S_I(\alpha) = S(\alpha^I)$. Thus

$$S_{\{i_1,i_2,\ldots,i_k\}} = \sum_{j=0}^{n-1} a_{j-i_1} a_{j-i_2} \ldots a_{j-i_k}.$$

Similarly define a $\star$-*expression* to be the composition of S and a $\star$-polynomial. The *degree* of a $\star$-expression is defined to be $\max\{|I| : I \in \mathcal{I}\}$. ■

Definition 6 Given ideals M, $N \subset Q_n$ we define their $\star$-*product* $M \star N$ to be the ideal generated by M and N together with the set of all $\star$-products of one element from M and one from N. Note that $M \star N$ contains the ideal generated by $\{m \star n : m \in M, n \in N\}$, but that the two ideals need not be equal. The k^{th} $\star$-*power* of M is the ideal $M^{\star k} = M^{\star(k-1)} \star M = M \star M \star \cdots \star M$, where k factors of M appear. Note that if $M = (\alpha)$ then $M^{\star k} = \{p(\alpha) : p \text{ is a } \star\text{-polynomial with } \deg(p) \le k\}$. These definitions have natural generalizations to C_n, which we adopt without further comment. ■

In our proof of the main theorem, Theorem 18, we will show that given $\alpha \in Q_n$ we can find a $\star$-polynomial p such that $p(\alpha) = 1 \in Q_n$, and that moreover it can be done in such a way that p has reasonably low degree; at most l say. Then we will show that the values of $\star$-expressions of degree at most k are reconstructible from the k-deck. This will enable us to prove, with a little work, that if $\beta \in \mathbb{Q}_n$ has $d_{\beta,3l} \equiv d_{\alpha,3l}$ then we must have $p(\beta) = x^i$ for some $i \in \{0, \ldots, n-1\}$, and then that $\beta = x^i\alpha$.

4 $\star$-expressions.

The main result we require concerning $\star$-expressions is simply the fact that if α and β are elements of C_n with $d_{\alpha,k} \equiv d_{\beta,k}$ then all $\star$-expressions of degree at most k take the same value at α as at β.

Lemma 5 *Suppose k is an integer with $k \geq 1$ and $\alpha, \beta \in C_n$ have*

$$d_{\alpha,k} \equiv d_{\beta,k}.$$

If

$$f = \sum_{I \in \mathcal{I}} \lambda_I S_I$$

is a $\star$-expression of degree at most k then $f(\alpha) = f(\beta)$.

Proof. It is clearly sufficient to prove the result when f is a $\star$-term; $f = S_I$ with $I = \{i_1, i_2, \ldots, i_l\}$, $l \leq k$. Then we simply have

$$\begin{aligned} f(\alpha) &= \sum_{j=0}^{n-1} a_{j-i_1} a_{j-i_2} \ldots a_{j-i_l} \\ &= d_{\alpha,l}(\{-i_1, -i_2, \ldots, -i_l\}) \\ &= d_{\beta,l}(\{-i_1, -i_2, \ldots, -i_l\}) \\ &= f(\beta) \end{aligned}$$

■

The next result allows us to identify, by means of $\star$-expressions, the elements x^i, $i \in \{0, \ldots, n-1\}$, of Q_n.

Lemma 6 *Suppose $\alpha \in Q_n$ satisfies*

$$S_{\{0,0\}}(\alpha) = S_{\{0,0,0\}}(\alpha) = 1.$$

Then for some $i \in \{0, \ldots, n-1\}$ we have $\alpha = x^i$.

Proof. This is identical with Lemma 1. ■

Lemma 7 *Let p, q be $\star$-polynomials and f be a $\star$-expression. Then $p \circ q$ is a $\star$-polynomial of degree at most $\deg(p)\deg(q)$ and $f \circ p$ is a $\star$-expression of degree at most $\deg(f)\deg(p)$.*

Proof. Straightforward calculation. ■

The next two results are the key to our approach; they give, respectively, a simple combinatorial condition and a simple algebraic condition on $\alpha \in Q_n$ which guarantee its reconstructibility,

Proposition 8 *Suppose that $\alpha = \sum_{j=0}^{n-1} a_j x^j$ is an element of Q_n and that there exists a $\star$-polynomial p such that $p(\alpha) = 1$. If $\deg(p) \leq k$ and $\beta \in Q_n$ has $d_{\beta,3k} \equiv d_{\alpha,3k}$ then $\beta = x^i \alpha$ for some $i \in \{0, \dots, n-1\}$.*

Proof. Let $\iota = p(\beta)$. Applying the $\star$-term $S_{\{0,0,0\}}$ to p we get (by Lemma 7) a $\star$-expression $f = S_{\{0,0,0\}} \circ p$ of degree at most $3k$. By Lemma 5, we have $S_{\{0,0,0\}}(\iota) = f(\beta) = f(\alpha) = S_{\{0,0,0\}}(1) = 1$. Similarly we have $S_{\{0,0\}}(\iota) = 1$. By Lemma 6 it must be the case that $\iota = x^i$ for some $i \in \{0, \dots, n-1\}$. Now, for $j = 0, \dots, n-1$, consider the function on Q_n given by $\beta \mapsto \langle x^j \iota, \beta \rangle$. This function is some $\star$-expression g_j of degree at most $3k$ (of course, in fact at most $k+1$). Hence, writing $(b_j)_{j=0}^{n-1}$ for the coefficients of β,

$$\begin{aligned} b_{i+j} &= \langle x^j x^i, \beta \rangle \\ &= \langle x^j \iota, \beta \rangle \\ &= g_j(\beta) \\ &= g_j(\alpha) \\ &= \langle x^j 1, \alpha \rangle \\ &= a_j. \end{aligned}$$

In other words, $\beta = x^i \alpha$. ∎

Theorem 9 *If $\alpha \in Q_n$ generates the ideal $J = (\alpha)$ and $J^{\star k} = Q_n$ then there are no $(3k)$-imposters for α.*

Proof. Since $1 \in Q_n = J^{\star k}$ there exists some $\star$-polynomial p of degree k such that $p(\alpha) = 1$. By Proposition 8 any $\beta \in C_n$ with $d_{\beta,3k} \equiv d_{\alpha,3k}$ must be of the form $\beta = x^i \alpha$ for some $i \in \{0, \dots, n-1\}$. ∎

In the next section we will work on determining the minimal k for which the conditions of Theorem 9 hold, and we will deduce the main result in section 6.

5 Algebraic Background

Recall that we are chiefly interested in the ring $Q_n = \mathbb{Q}[x]/(x^n - 1)$ and that in order to understand its ideals better we will also consider the ring $\mathbb{C}^n$ with pointwise multiplication. We have seen in Theorem 9 that any element $\alpha \in Q_n$ which has the property that $(\alpha)^{\star k} = Q_n$ is reconstructible from its $3k$-deck; the faster the $\star$-powers of (α) grow, the easier it is to reconstruct α. In this section we analyse the behaviour of $\star$-powers of arbitrary ideals of Q_n, using the Fourier transform as our chief tool.

First note that if $\xi \in \mathbb{C}$ is an n^{th} root of unity then the evaluation map $\alpha \mapsto \alpha(\xi)$ is well defined for $\alpha \in C_n$. Analogously we may talk about $p \in \mathbb{C}[x]$ dividing $\alpha \in C_n$ provided $p \mid x^n - 1$. We write ζ_n for $\mathrm{e}^{2\pi i/n}$.

Proposition 10 *The map $\mathcal{F} : C_n \to \mathbb{C}^n$ defined by*

$$\mathcal{F}(\alpha) = \left(\alpha(\zeta_n^j)\right)_{j=0}^{n-1}$$

is a ring isomorphism with inverse

$$\mathcal{F}^{-1}\left((z_j)_{j=0}^{n-1}\right) = \sum_{j=0}^{n-1}\left(\frac{1}{n}\sum_{r\in\{0,\ldots,n-1\}} z_r\zeta_n^{-rj}\right)x^j. \tag{1}$$

■

In order to make progress we will need to understand the ideals of C_n and $\mathbb{C}^n$. The basic facts are recorded in the following definition and proposition.

Definition 7 Let

$$\begin{aligned} Z_S &= \left\{(f_i)_{i=0}^{n-1} \in \mathbb{C}^n \ : \ f_i = 0 \ \forall i \in S\right\} \\ NZ_S = Z_{\mathbb{Z}_n\setminus S} &= \left\{(f_i)_{i=0}^{n-1} \in \mathbb{C}^n \ : \ f_i = 0 \ \forall i \notin S\right\}. \end{aligned}$$

■

Proposition 11 *C_n (and hence $\mathbb{C}^n$) is a principal ideal domain. C_n has 2^n ideals, indexed by subsets of the set $\{\zeta_n^i \ : \ i = 0,\ldots,n-1\}$ of n^{th} roots of unity. The subset T corresponds to the ideal $M_T = \left(\prod_{\zeta_n^j\in T}(x-\zeta_n^j)\right)$. The ideals of $\mathbb{C}^n$ are indexed by subsets of $\{0,\ldots,n-1\}$. A subset $S \subset \{0,\ldots,n-1\}$ corresponds to the ideal Z_S of those vectors whose j^{th} coordinate is 0 for each $j \in S$. The Fourier transform maps the ideal M_T to the ideal $Z_{\{j\,:\,\zeta_n^j\in T\}}$.*

Proof. The ideals of $C_n = \mathbb{C}[x]/(x^n-1)$ are in 1-1 correspondence with the ideals J of $\mathbb{C}[x]$ with $(x^n-1) \subset J \subset \mathbb{C}[x]$. Since $\mathbb{C}[x]$ is a principal ideal domain these correspond to factors of x^n-1. Since $\mathbb{C}[x]$ is a unique factorization domain these are exactly all possible products of irreducible factors of x^n-1, viz., the polynomials $x-\zeta_n^i$ for $i \in \{0,\ldots,n-1\}$. The description of the ideals of $\mathbb{C}^n$ and the correspondence between M_T and $Z_{\{j\,:\,\zeta_n^j \in T\}}$ follows from noting that $\mathcal{F}(p(x))(j) = 0$ iff $(x - \zeta_n^j) \mid p(x)$. ■

The reason that reconstructing elements of Q_n is easier than reconstructing arbitrary elements of C_n is that the ideal structure of Q_n is more interesting than that of C_n; Proposition 12 records the facts we require. We also need a little bit of notation.

Definition 8 Let $F = \mathbb{Q}[\zeta_n]$ be the splitting field of $x^n - 1$ over $\mathbb{Q}$. Define

$$\Phi_n(x) = \prod_{\zeta'} (x - \zeta')$$

where the product is over the set of all primitive n^{th} roots of unity in F. We write Φ_D, where D is a subset of the divisors of n, for the product $\prod_{d \in D} \Phi_d$. ■

Definition 9 If D is a subset of $\{d \,:\, d \mid n\}$ we set

$$S(D) = \{j \in \mathbb{Z}_n \,:\, (n, j) = n/d \text{ for some } d \in D\}$$

and

$$S^c(D) = \mathbb{Z}_n \setminus S(D) = \{j \in \mathbb{Z}_n \,:\, n/(n, j) \notin D\}.$$

■

Proposition 12

• *For all $n \geq 1$ the polynomial Φ_n has integer coefficients. Φ_n is irreducible in $\mathbb{Q}[x]$ and has degree $\phi(n)$, the Euler totient function counting the number of residues mod n that are coprime to n.*

• *The automorphisms of F over $\mathbb{Q}$ are the maps $\zeta_n \mapsto \zeta_n^j$ for $j \in \{0, \ldots, n-1\}$ with $(j, n) = 1$. The polynomial $x^n - 1$ factorizes in $\mathbb{Q}[x]$ as*

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

• *The zeros of Φ_d, for d a divisor of n are given by $\Phi_d(\zeta_n^j) = 0$ iff $(n, j) = n/d$.*

• *For any $D \subset \{d \,:\, d \mid n\}$ the characteristic function of $S(D)$ is in $\mathcal{F}(Q_n)$. The Fourier transform of the ideal $(\Phi_D) \subset Q_n$ is $\mathcal{F}(Q_n) \cap Z_{S(D)}$.*

Proof. Most parts are standard facts; see e.g. Hungerford [8]. The last section maybe requires some remark. Note that the expressions appearing in the calculation of $\mathcal{F}^{-1}(\chi_{S(D)})$ are clearly invariant under the automorphism group of F over $\mathbb{Q}$, and hence, since F is a Galois extension of $\mathbb{Q}$, are in $\mathbb{Q}$. For the second part, notice that we clearly have $\mathcal{F}((\Phi_D)) \subset \mathcal{F}(Q_n) \cap Z_{S(D)}$. To show the reverse inclusion consider $f \in \mathcal{F}(Q_n) \cap Z_{S(D)}$ and let $\alpha = \mathcal{F}^{-1}(f)$. Clearly $\alpha \in Q_n$. Since $f \in Z_{S(D)}$, for each $d \in D$ we have $\alpha(\zeta_n^{n/d}) = \alpha(\zeta_d) = 0$; but the minimal polynomial of ζ_d is Φ_d, hence $\Phi_d \mid \alpha$. Thus $\Phi_D \mid \alpha$ and $\alpha \in (\Phi_D)$. ■

To have our project succeed we must be able to bound the k for which $I^{\star k} = Q_n$, where I is an ideal of Q_n. (At least when such a k exists; we will see later that possible periodicity in I may restrict all the $\star$-powers of I to less than all of Q_n.) We will then be able to use Theorem 9 to obtain our main result. The next result describes the effect of the $\star$-product on the Fourier transforms of ideals.

Lemma 13 *Let $I,\ J \subset Q_n$ be ideals with $I = (\Phi_D)$ and $J = (\Phi_E)$. Then the Fourier transform of the $\star$-product of I and J is given by*

$$\mathcal{F}(I \star J) = \mathcal{F}(Q_n) \cap NZ_{S^c(D) \cup S^c(E) \cup (S^c(D)+S^c(E))}.$$

Proof. First notice that $\mathcal{F}^{-1}$ maps the pointwise product of elements of $\mathbb{C}^n$ to the polynomial product of their images. Now $\mathcal{F}$ is essentially the same as $\mathcal{F}^{-1}$ – it simply uses evaluation at ζ_n^{-i} rather than ζ_n^i. Thus let us define $\star : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^n$ by

$$(z_i)_{i=0}^{n-1} \star (w_i)_{i=0}^{n-1} = \left(n \sum_{j+k=i} z_j w_k \right)_{i=0}^{n-1}.$$

A straightforward calculation shows that if $\alpha, \beta \in C_n$ with $\mathcal{F}(\alpha) = a$ and $\mathcal{F}(\beta) = b$ then $\mathcal{F}(\alpha \star \beta) = a \star b$.

Now consider ideals I, J, as in the statement of the Lemma. Let $S = S^c(D) \cup S^c(E) \cup (S^c(D) + S^c(E))$. By Proposition 12 we have $\chi_{S^c(D)} \in \mathcal{F}(I)$ and $\chi_{S^c(E)} \in \mathcal{F}(J)$ and thus $\chi_{S^c(D)} \star \chi_{S^c(E)} \in \mathcal{F}(I \star J)$. Now $\mathrm{supp}(\chi_{S^c(D)} + \chi_{S^c(E)} + \chi_{S^c(D} \star \chi_{S^c(E)}) = S$ so, since we have exhibited an element of $\mathcal{F}(I \star J)$ which is non-zero on all of S we have $\mathcal{F}(I \star J) \supset \mathcal{F}(Q_n) \cap NZ_S$.

To prove the reverse inclusion note that whenever $i \notin S$ and $a \in \mathcal{F}(I)$, $b \in \mathcal{F}(J)$ every term of the sum $\sum_{j+k=i} a_j b_k$ is zero, and thus $(a \star b)_i = 0$. Moreover $a_i = b_i = 0$, so the i^{th} coordinate is zero for every element of $\mathcal{F}(I \star J)$. Thus $\mathcal{F}(I \star J) \subset \mathcal{F}(Q_n) \cap NZ_S$. ■

Since $S^c(D) = \left\{r\frac{n}{d} : r \in \mathbb{Z}_n^*, d \in \mathbb{Z}_n \setminus S\right\}$, we can get a handle on the sets appearing in the statement of Lemma 13 provided we can understand the sets $\mathbb{Z}_n^*$, $\mathbb{Z}_n^* + \mathbb{Z}_n^*$, $\mathbb{Z}_n^* + \mathbb{Z}_n^* + \mathbb{Z}_n^*, \dots$. The next lemma establishes the essential facts.

Lemma 14 *If n is odd then $\mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*) = \mathbb{Z}_n$. If n is even then $\mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*) \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^* + \mathbb{Z}_n^*) = \mathbb{Z}_n$.*

Proof. By the Chinese remainder theorem we know that if $n = p_1^{k_1} \dots p_r^{k_r}$ is the prime factorization of n then $\mathbb{Z}_n \cong \bigoplus_{i=1}^r \mathbb{Z}_{p_i^{k_i}}$. In this representation $\mathbb{Z}_n^*$ is the subset of elements for which the i^{th} coordinate belongs to $\mathbb{Z}_{p^i}^*$ for every i. To prove the lemma for odd values if n it suffices to note that $\mathbb{Z}_{p^i}^* + \mathbb{Z}_{p^i}^* = \mathbb{Z}_{p^i}$ for all odd prime powers p^i. This is straightforward. For even values of n we are limited by the fact that $\mathbb{Z}_{2^k}^* + \mathbb{Z}_{2^k}^* = 2\mathbb{Z}_{2^k}$. Thus if $i \equiv p \pmod{2p}$, where p is an odd prime dividing n, then $i \notin \mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*)$. However it is easy to check that these are the only missing values. Since these are all odd residues we have that $i \notin \mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*)$ implies $i - 1 \in \mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*)$. Hence, since $1 \in \mathbb{Z}_n^*$, we have $\mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*) \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^* + \mathbb{Z}_n^*) = \mathbb{Z}_n$. ∎

One issue we have not touched on so far is that of periodicity. It clearly affects our approach since if α is a periodic element of Q_n then all $\star$-powers of (α) are also periodic; in particular no $\star$-power of (α) contains 1. To make our discussion easier let us give names to the fundamental periodic elements of Q_n: let $\pi_{n,d} = (1 + x^d + x^{2d} + \dots + x^{n-d})$ where d is a divisor of n. Clearly $\alpha = x^d\alpha$ iff $\pi_{n,d} \mid \alpha$. Note that since $x^n - 1 = (x^d - 1)\pi_{n,d}$ we have $\pi_{n,d} = \Phi_{\{e : e|n \text{ and } e \nmid d\}}$.

Definition 10 We say that $\alpha \in Q_n$ is *periodic* if $\alpha = x^d\alpha$ for some divisor d of n with $d \neq n$. We say that an ideal $I \subset Q_n$ is *periodic* if there exists some $d \neq n$, $d \mid n$ such that $\alpha = x^d\alpha$ for all $\alpha \in I$. ∎

Lemma 15 *The ideal $I = (\alpha)$ is periodic iff α is periodic. Φ_D (and hence (Φ_D)) is periodic iff D contains some top face of the lattice of divisors of n. In other words Φ_D is periodic iff there exists some prime p dividing n such that $\{p^m e : e \mid n/p^m\} \subset D$ where p^m is the highest power of p dividing n.*

Proof. For the first part note that I being periodic implies that every element of I is periodic, in particular α is periodic. Conversely, if $\alpha = x^d\alpha$ then $\pi_{n,d} \mid \alpha$ and hence $\pi_{n,d} \mid \beta$ for all $\beta \in I$.

Suppose now that Φ_D is periodic with period d; then it is also periodic with period e for any $d \mid e \mid n$. In particular it is periodic with period n/p for some prime p dividing n. So $\pi_{n,n/p} \mid \Phi_D$, hence $\{d \mid n : d \nmid n/p\} \subset D$. This set is the top face of the divisor lattice of n in the p direction. ■

Theorem 16 *If $\alpha \in Q_n$ and n has m distinct prime factors then either α is periodic or $(\alpha)^{\star 3m} = Q_n$.*

Proof. Suppose α is not periodic. Then, by Lemma 15, we have $(\alpha) = (\Phi_D)$ for some $D \subset \{d : d \mid n\}$ such that for all primes $p \mid n$ there is some divisor f of n with $f \notin D$ and $p \nmid n/f$. Note that $n/f \in S^c(D)$. This implies that we can find a subset S' of $S^c(D)$ which has at most m elements and has greatest common divisor 1 – simply take one "missing" element from each top face. Now, by the gcd condition, we can form any element of $\mathbb{Z}_n$ by taking a linear combination of the elements of S' with coefficients in $\mathbb{Z}_n$. Let $i \in \mathbb{Z}_n$ be written as $i = \sum_{s \in S'} c_s s$, where the c_s lie in $\mathbb{Z}_n$. We can write each c_s in turn as the sum of at most three terms from $\mathbb{Z}_n^*$ (by Lemma 14). Hence, since $\mathbb{Z}_n^* \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^*) \cup (\mathbb{Z}_n^* + \mathbb{Z}_n^* + \mathbb{Z}_n^*) = \mathbb{Z}_n$ we can form any element of Z_n by summing at most $3m$ terms, each of the form rs where $r \in \mathbb{Z}_n^*$ and $s \in S'$. Since $S_c(D)$ is closed under multiplication by elements of $\mathbb{Z}_n^*$ this means that every element of Z_n can be written as a sum of at most $3m$ terms from $S^c(D)$. Hence, by Lemma 13, $(\alpha)^{\star 3m} = Q_n$. ■

6 The main result.

In this section we tie together the strands from Sections 3, 4, and 5 to prove our main results.

Proposition 17 *If $\alpha \in Q_n$ is not periodic and n has m distinct prime factors then there are no $9m$-imposters for α.*

Proof. By Theorem 16 we know that $(\alpha)^{\star 3m} = Q_n$. Then Proposition 8 tells us that there are no $(9m)$-imposters for α. ■

Theorem 18 *No element of Q_n, and hence in particular no two subset of $\mathbb{Z}_n$, has a $9m$-imposter, where m is the number of distinct prime factors of n.*

Proof. Proposition 17 deals effectively with the non-periodic elements of Q_n. We can detect periodicity of $\alpha \in Q_n$ (and indeed the minimal period) from its 2-deck; note that $|S_{\{0,d\}}(\alpha)| \leq S_{\{0,0\}}(\alpha)$, by Cauchy-Schwartz, with equality iff $\alpha = x^d\alpha$. Moreover, if α is periodic with period d we can construct the k-deck of

α considered as an element of Q_d from its k-deck in Q_n. Thus if $\alpha, \beta \in Q_n$ are two periodic elements with the same minimal period d and $d_{\alpha,9m} \equiv d_{\beta,9m}$ then the induced elements $\alpha', \beta' \in Q_d$ have $d_{\alpha',9m} \equiv d_{\beta',9m}$, and moreover α' and β' are non-periodic. Thus, for some $i' \in \{0, 1, \ldots, d-1\}$, $\beta' = x^{i'}\alpha'$. This implies that $\beta = x^i\alpha$ for all $i \equiv i' \pmod{d}$. Thus the theorem is proved. ■

Corollary 19 *For all n we have*

$$r_{\mathbb{Q}}(\mathbb{Z}_n) \leq (9 + o(1)) \ln n / \ln \ln n$$

and for almost all n

$$r_{\mathbb{Q}}(\mathbb{Z}_n) \leq (9 + o(1)) \ln \ln n.$$

Proof. It is known that $\alpha(n) \leq (1 + o(1)) \ln n / \ln \ln n$, and that for almost all n we have $\alpha(n) \leq (1 + o(1)) \ln \ln n$; see for instance Hardy and Wright [7], §22.12 and Theorem 436 respectively. ■

7 Final Remarks

The problems considered to this point have natural analogues for other finite Abelian groups. We make the natural definitions concerning decks and reconstructing. We write $r(G)$ for the *reconstruction number* of G; the smallest k such that every subset of G is reconstructible from its k-deck.

The most natural abelian group to consider after $\mathbb{Z}_n$ is the cube $\mathbb{Z}_2^n$. It is a straightforward consequence of Alon, Caro, Krasikov, and Roditty's [1] Corollary 2.5 that $r(\mathbb{Z}_n^2) \leq \log_2(2^n) = n$. Our techniques, in particular our use of pointwise multiplication and the Fourier transform, do not seem to produce a better result. If we let I be the ideal in $\mathbb{Q}\,\mathbb{Z}_2^n$ consisting of the inverse Fourier transforms of elements of $\mathbb{Q}^{\mathbb{Z}_2^n}$ supported on the singleton sets $\{\{i\} : i = 1, 2, \ldots, n\}$ then I is not a periodic ideal, and yet no earlier $\star$-power of I than the n^{th} is the whole group ring $\mathbb{Q}\,\mathbb{Z}_2^n$.

The above remark lends some support to the following conjecture.

Conjecture 3 $r(\mathbb{Z}_2^n) = r_{\mathbb{Q}}(Z_2^n) = n$.

For other Abelian groups it seems likely that a similar bound holds; we suspect that if $n_1, \ldots, n_k$ are prime powers then

$$r(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}) \leq ck,$$

for some absolute constant c.

When we come to consider non-Abelian groups it seems that our methods must change somewhat. It is possible however, for an arbitrary finite group G, to prove that $r(G) \leq cL(\mathbb{Q}\,G)$, where c is a constant and $L(\mathbb{Q}\,G)$ is the length of the longest increasing chain of ideals in $\mathbb{Q}\,G$ (see [12]).

Finally we make what seems to be an exceptionally natural conjecture.

Conjecture 4 For all finite groups G and H

$$r(G \times H) \leq r(G)r(H).$$

References

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

[2] J.A. Bondy, A graph reconstructor's manual, *in* Surveys in Combinatorics, 1991, ed. A.D. Keedwell, LMS Lecture Note Series 166, 221–252

[3] J.A. Bondy and R.L. Hemminger, Graph reconstruction – a survey, *J. Graph Theory* **1** (1977), 227–268

[4] P.J. Cameron, Stories from the age of reconstruction, Festschrift for C. St. J. A. Nash-Williams, *Congr. Numer.* **113** (1996), 31–41

[5] C.J. Colbourn and J.H. Dinitz (eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, 1996, *xviii* + 753pp.

[6] P. Erdős, On a lemma of Littlewood and Offord, *Bull. AMS* **51** (1945), 898–902

[7] G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Fifth edition, The Clarendon Press, Oxford University Press, New York, 1979, *xvi*+426pp.

[8] T.W. Hungerford, Algebra, Graduate Texts in Mathematics, Springer-Verlag, New York, 1974, *xxiii* + 502 pp.

[9] D.J. Kleitman, On a lemma of Littlewood and Offord on the distribution of certain sums, *Math. Zeitschr.* **90** (1965), 251–259

[10] V. B. Mnukhin, The k-orbit reconstruction and the orbit algebra, *Acta Appl. Math.* **29** (1992), 83–117

[11] M. Pouzet, Application d'une propriété combinatoire des parties d'un ensemble aux groupes et aux relations, *Math. Z.* **150** (1976), 117–134

[12] A.J. Radcliffe and A.D. Scott, Reconstructing subsets of non-Abelian groups, In preparation.