Reconstructing subsets of reals

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

A.D. Scott
Department of Mathematics
University College
Gower Street
London WC1E 6BT
A.Scott@ucl.ac.uk

Submitted: November 24, 1998; Accepted: March 15, 1999

[1]Partially supported by NSF Grant DMS-9401351

Abstract

We consider the problem of reconstructing a set of real numbers up to translation from the multiset of its subsets of fixed size, given up to translation. This is impossible in general: for instance almost all subsets of $\mathbb{Z}$ contain infinitely many translates of every finite subset of $\mathbb{Z}$. We therefore restrict our attention to subsets of $\mathbb{R}$ which are *locally finite*; those which contain only finitely many translates of any given finite set of size at least 2.

We prove that every locally finite subset of $\mathbb{R}$ is reconstructible from the multiset of its 3-subsets, given up to translation.

Primary: 05E99; Secondary: 05C60

1 Introduction.

Reconstructing combinatorial objects from information about their subobjects is a long-standing problem. The Reconstruction Conjecture and the Edge Reconstruction Conjecture both deal with the problem of reconstructing a graph from a multiset of subgraphs; in one case the collection of all induced subgraphs with one fewer vertex, in the other the collection of all subgraphs with one fewer edge (see Bondy [2] and Bondy and Hemminger [3]).

The very general problem is that of reconstructing a combinatorial object (up to isomorphism) from the collection of isomorphism classes of its subobjects. Isomorphism plays a crucial rôle. Thus it seems that the natural ingredients for a reconstruction problem are a group action (to provide a notion of isomorphism) and an idea of what constitutes a subobject. Reconstruction problems have been considered from this perspective by, for instance, Alon, Caro, Krasikov and Roditty [1], Radcliffe and Scott [11], [10], Cameron [4], [5], and Mnukhin [7], [8], [9].

In this paper we consider the problem of reconstructing subsets of the groups $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ from the multiset of isomorphism classes of their subsets of fixed size, where two subsets are isomorphic if one subset is a translate of the other. Where the subsets have size k we call this collection the *k-deck*.

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 a straightforward translation of 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. 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 A be a subset of $\mathbb{F}$, where $\mathbb{F}$ is one of $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$. The *k-deck* of A is the function defined on multisets Y of size k from $\mathbb{F}$ by

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

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

$$d_{B,k} \equiv d_{A,k} \Rightarrow B = A + i, \text{for some } i \in \mathbb{F}.$$

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

Certain subtleties arise since the groups involved are infinite. It may be that the k-deck of $A \subset \mathbb{F}$ takes the value ∞ on some finite (multi)sets. In fact, for any fixed finite subset $F \subset \mathbb{Z}$, almost all subsets of $\mathbb{Z}$ (with respect to the obvious symmetric probability measure on $\mathcal{P}(\mathbb{Z})$) contain infinitely many translates of F. Thus it is trivial to find, for all $k \geq 1$, two subsets of $\mathbb{Z}$ with the same k-deck which are not translates of one another.

For this reason we restrict our attention to subsets $A \subset \mathbb{F}$ for which the 2-deck (and *a fortiori* the k-deck for all $k \geq 2$) takes only finite values, or equivalently, every distance occurs at most fintely many times. We shall call such sets *locally finite*.

It is easily seen that every finite subset $A \subset \mathbb{R}$ can be reconstructed from its 3-deck, $d_{A,3}$: indeed, let $n = \operatorname{diam} A := \max A - \min A$; then

$$A \simeq \{0, n\} \cup \{r : d_{A,3}(\{0, r, n\}) > 0\}.$$

The 2-deck is not, however, in general enough. For instance, if A and B are finite sets of reals then $A + B$ and $A - B$ have the same 2-deck.

Our aim in this note is to prove a reconstruction result for locally finite sets of reals. We begin by proving a result for $\mathbb{Z}$ and work in stages towards $\mathbb{R}$. We shall write $A \simeq B$ if A is a translation of B.

Theorem 1 *Let $A \subset \mathbb{Z}$ be locally finite. Then A is reconstructible from its 3-deck. In other words, if $A, B \subset \mathbb{Z}$ have the same 3-deck then $A \simeq B$.*

We shall first prove a lemma. For subsets $A, B \subset \mathbb{Z}$, we define $A + B$ to be the multiset of all $a + b$ with $a \in A$ and $b \in B$. (This multiset might of course take infinte values). Thus, for finite A and B, if we identify A with $a(x) = \sum_{i \in A} x^i$ and B with $b(x) = \sum_{i \in B} x^i$, then $A + B$ can be identified with $a(x)b(x)$, where the coefficient of x^i in $a(x)b(x)$ is the multiplicity of i in the sum $A + B$.

If L is a multiset of $\mathbb{Z}$ we write $m_L(i)$ for the multiplicity of i in L.

Lemma 2 *Let $A, B, C \subset \mathbb{Z}$ be finite and suppose that $A + C = B + C$. Then $A = B$.*

Proof. Straightforward by induction on $|A|$, noting that $\min(A + C) = \min A + \min C$. ■

Lemma 3 *If $A, B \subset \mathbb{Z}$ are locally finite, infinite sets with $A \triangle B$ finite, and C is a finite set with $A + C = B + C$ then $A = B$.*

Proof. Let $A_0 = A \setminus B$, let $B_0 = B \setminus A$, and set $R = A \cap B$. Now for all i we have

$$\begin{aligned} m_{A_0+C}(i) &= m_{A+C}(i) - m_{R+C}(i) \\ &= m_{B+C}(i) - m_{R+C}(i) \\ &= m_{B_0+C}(i). \end{aligned}$$

Thus $A_0 + C = B_0 + C$ and it follows from Lemma 2 that $A_0 = B_0$ and so $A = B$. ■

Lemma 4 *If $A, B \subset \mathbb{Z}$ are locally finite, infinite sets, and C is a finite set with $A + C = B + C$ then $A = B$.*

Proof. We may suppose, without loss of generality, that $0 \in C$. Now let $S = \{i : C + i \subset A + C\}$ and $c = \operatorname{diam}(C)$. We aim to show that, except for a finite amount of confusion, we have $S = A$. To this end, let N be sufficiently large such that for all distinct $a, a' \in A$ with $|a| > N$ we have $|a' - a| > 4c$ and for all distinct $b, b' \in B$ with $|b| > N$ we have $|b' - b| > 4c$. (Such an N exists since A and B are locally finite.) Suppose now that k, with $|k| > N + 4c$, belongs to two sets from $\{C + i : i \in S\}$, say $k \in (C + i) \cap (C + j)$. Define $D = (C + i) \cup (C + j)$. Since $\operatorname{diam}(D) > c$, while $D \subset A + C$, there must be distinct elements $a_1, a_2 \in A$ such that D meets both $C + a_1$ and $C + a_2$. But this is impossible, for then $|a_1 - a_2| \leq 4c$, while $|a_1| > N$. Thus every $k \in A + C$ with $|k| > N + 4c$ belongs to exactly one set $C + i$. It follows that $i \in A$, and by the same reasoning $i \in B$.

Now set $R = \{i \in S : |i| > N + 4c\}$. We have just established that $R \subset A$ and $R \subset B$, and obviously $R \supset \{a \in A : |a| > N + 4c\}$ and $R \supset \{b \in B : |b| > N + 4c\}$. Thus $A \Delta B$ is finite, and by Lemma 3 the result is established. ■

Lemma 5 *Let $A, B \subset \mathbb{Z}$ be locally finite infinite sets and let $C, D \subset \mathbb{Z}$ be finite. If $A + C = B + D$ then $A \simeq B$ and $C \simeq D$.*

Proof. We may clearly assume that $\min C = \min D = 0$. Under this hypothesis we will prove that $A = B$ and $C = D$.

We will show that C (and equally D) is the largest set such that infinitely many translates of C are contained in $A + C = B + D$. Suppose then that $A + C$ contains infinitely many translates of some set E and that no translate of E is a subset of C. Let $E_1, E_2, \ldots$ be translates of E, where $E_i \subset A + C$ and $|\min E_i| \to \infty$ as $i \to \infty$. Since E is contained in no translate of C, every E_i must meet at least two translates of C, say C_{a_i} and C_{b_i}, where a_i and b_i are distinct elements of A. Thus there are distinct $a_i, b_i \in A$ with

$$|a_i - b_i| \leq 2\,\mathrm{diam}(C) + \mathrm{diam}(E)$$

and $|a_i| \to \infty$; since there are only finitely many possibilities for $a_i - b_i$ and infinitely many a_i, some distance must occur infinitely many times, which contradicts the assumption that A is locally finite.

We conclude that C is the largest set (uniquely defined up to translation) that has infinitely many translates as subsets of $A+C$. Hence we have $C \simeq D$ and so $C \equiv D$, since $\min C = \min D$. Thus $A + C = B + D = B + C$, and by Lemma 4, $A = B$. ■

Proof. [of Theorem 1] If A is finite then it is easily reconstructed from its 3-deck, as noted above. Thus we may assume that A is infinite.

Let k be a difference that occurs in A (i.e. there are $a_1, a_2 \in A$ with $a_1 - a_2 = k$). We shall show that A can be reconstructed from its 3-deck; moreover, it can be reconstructed from its 3-deck restricted to multisets of the form $\{0, k, \alpha\}$. Indeed, let B be another set with the same 3-deck. Define

$$X_A = \{a \in A \,:\, a + k \in A\}$$

and

$$X_B = \{b \in B \,:\, b + k \in B\}.$$

Then, translating if necessary, we may assume that $\min X_A = \min X_B$. We claim now that $A = B$.

In order to prove our result it is enough to show that $-A+X_A = -B+X_B$, for then the result follows immediately from Lemma 5: since $-A = -B$ we also have $A = B$.

Now for $i \in \mathbb{Z}$, the multiplicity of i in $-A + X_A$ is

$$\begin{aligned} |\{j \,:\, j \in X_A, i - j \in -A\}| &= |\{j \,:\, j \in X_A, j - i \in A\}| \\ &= |\{j \,:\, j, j + k, j - i \in A\}|. \end{aligned}$$

If $i \neq 0, -k$, then this is the multiplicity of $\{0, i, i+k\}$ in the 3-deck of A; if $i = 0$ or $i = -k$ then this is $|X_A|$, the multiplicity of $\{0, k\}$ in the 2-deck of A. Clearly, similar calculations hold for B, so $-A + X_A = -B + X_B$. ∎

Theorem 6 *Lemmas 2, 3, 4, and 5 hold in $\mathbb{Z}^n$ for all positive integers n. Moreover if $A, B \subset \mathbb{Z}^n$ have the same 3-deck then $A \simeq B$.*

Proof. The proofs are almost identical to those for the corresponding results about $\mathbb{Z}$. We use the norm $|a| = \|a\|_2$, and order $\mathbb{Z}^n$ lexicographically, so $a \leq b$ if the first nonzero coordinate of $b - a$ is positive. The assumptions $\min C = \min D$ in the proof of Lemma 2 and $\min X_A = \min X_B$ in the proof of Theorem 1 then make sense. Moreover, the claim in the proof of Lemma 4 that $\mathrm{diam}(D) > \mathrm{diam}(C)$ is easily seen to hold in $\mathbb{Z}^n$ also: suppose $D = (C+i) \cup (C+j)$ and $x, y \in C$ satisfy $|x-y| = \mathrm{diam}(C)$. Let $v = i - j \neq 0$. Now $|(x+i) - (y+j)| = |(x-y) + v|$ and $|(x+j) - (y+i)| = |(x-y) - v|$ and one of these two norms is strictly greater than $|x-y| = \mathrm{diam}(C)$ (by the strict convexity of the norm we have chosen). ∎

Theorem 7 *Let $A, B \subset \mathbb{Q}$ be locally finite and have the same 3-deck, then $A \simeq B$.*

Proof. Suppose A and B are locally finite subsets of $\mathbb{Q}$ with the same 3-deck. Let k be some distance that occurs in A, and again define $X_A = \{a \in A : a + k \in A\}$ and $X_B = \{b \in B : b + k \in B\}$ as in the proof of Theorem 1. We may assume $\min X_A = \min X_B = 0$. Now suppose n is an integer such that $1/n$ divides k and all differences in X_A and X_B. That is, $nk \in \mathbb{Z}$ and for all $q, r \in X_A \cup X_B$ we have $n(q - r) \in \mathbb{Z}$. In particular $nq \in \mathbb{Z}$ for all $q \in X_A \cup X_B$. We will show that for all i we have

$$A \cap \frac{1}{in}\mathbb{Z} = B \cap \frac{1}{in}\mathbb{Z}$$

Since $\mathbb{Q} = \bigcup_{i \geq 1} \frac{1}{in}\mathbb{Z}$ the result will then be proved.

As in the proof of Theorem 1, it is enough to show that the 3-decks of $A \cap \frac{1}{in}\mathbb{Z}$ and $B \cap \frac{1}{in}\mathbb{Z}$, restricted to multisets of form $\{0, k, \alpha\}$, are equal. Now if $a + \{0, k, \alpha\} \subset A$ then $a \in X_A$, and so

$$\begin{aligned} a + \{0, k, \alpha\} \subset A \cap \frac{1}{in}\mathbb{Z} \quad &\iff \quad a + \alpha \in \frac{1}{in}\mathbb{Z} \\ &\iff \quad \alpha \in \frac{1}{in}\mathbb{Z}. \end{aligned}$$

Thus the relevant parts of the 3-decks of $A \cap \frac{1}{in}\mathbb{Z}$ and $B \cap \frac{1}{in}\mathbb{Z}$ are equal, and hence $A \cap \frac{1}{in}\mathbb{Z} = B \cap \frac{1}{in}\mathbb{Z}$. ∎

Theorem 8 *Let $A \subset \mathbb{Q}^n$ be locally finite. Then A is reconstructible from its 3-deck.*

Proof. Similar to the proof of Theorem 7, with modifications as indicated in the proof of Theorem 6. ∎

Theorem 9 *Let $A \subset \mathbb{R}$ be locally finite. Then A is reconstructible from its 3-deck.*

Proof. Let $\{q : q \in I\}$ be a Hamel basis for $\mathbb{R}$ over $\mathbb{Q}$, where the set I is well-ordered by $\prec$. This induces a total ordering on $\mathbb{R}$ by defining $x < y$ iff $y - x = \sum_{i=1}^{n} a_i q_i$ with $q_1 \prec q_2 \prec \cdots \prec q_n$ and $a_1 > 0$. Given a subset $S \subset R$ we write $\langle S \rangle$ for the collection of finite $\mathbb{Q}$-linear combinations of elements of S.

Now suppose that $A, B \subset \mathbb{R}$ are locally finite, and that the 3-decks of A and B are the same. Let r be a distance that occurs in A and let $X_A = \{a \in A : a + r \in A\}$, and $X_B = \{b \in B : b + r \in B\}$. We may assume that $\min X_A = \min X_B = 0$. Let $I_0 \subset I$ be a finite subset of I such that $x - y \in \langle I_0 \rangle$ for all $x, y \in X_A \cup X_B$, and also $r \in \langle I_0 \rangle$. Such a subset exists, since $X_A \cup X_B$ is finite and every element of $\mathbb{R}$ can be written as a $\mathbb{Q}$-linear combination of a finite set of elements from I.

We will show that for finite subsets J with $I_0 \subset J \subset I$, the sets $A \cap \langle J \rangle$ and $B \cap \langle J \rangle$ are equal, from which it easily follows that $A = B$. Consider then such a J. If $a + \{0, r, \alpha\} \subset A$ then $a \in X_A$ and

$$\begin{aligned} a + \{0, r, \alpha\} \subset A \cap \langle J \rangle \quad &\iff \quad a + \alpha \in \langle J \rangle \\ &\iff \quad \alpha \in \langle J \rangle . \end{aligned}$$

Since $\langle J \rangle$ is isomorphic to $\mathbb{Q}^N$, for some N, and, by the argument above, the 3-decks of $A \cap \langle J \rangle$ and $B \cap \langle J \rangle$ restricted to multisets of form $\{0, r, \alpha\}$ are the same, it follows from Theorem 8 that $A \cap \langle J \rangle = B \cap \langle J \rangle$. Since $\bigcup_{J \supset I_0} \langle J \rangle = \mathbb{R}$, we have that $A = B$. ∎

It would be interesting to have a measure-theoretic version of this result. Let S be a Lebesgue-measurable set of reals, and for every finite set X, define $S(X) = \lambda(x : X + x \subset S)$. Call S *locally finite* if $S(X)$ is finite whenever $|X| > 1$. We regard sets X, Y as equivalent if $\lambda(X \triangle (Y + t)) = 0$ for some real number t. Can we reconstruct every set of finite measure from its 3-deck? Can we reconstruct every locally finite set from its 3-deck? Or from the k-deck for sufficiently large k?

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] P. J. Cameron, Some open problems on permutation groups, in M. W. Liebeck and J. Saxl, eds, Groups, Combinatorics and Geometry, London Mathematical Society Lecture Notes **165**, CUP, 1992, 340-351

[6] I. Krasikov and Y. Roddity, On a reconstruction problem for sequences, *J. Comb. Theory, Ser. A* **77** (1977), 344-348

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

[8] V. B. Mnukhin, The reconstruction of oriented necklaces, *J. Combinatorics, Information and System Sciences*, **20** (95), 261-272

[9] V. B. Mnukhin, The k-orbit reconstruction for Abelian and Hamiltonian groups, *Acta Applicandae Mathematicae* **52** (98), 149-162

[10] A. J. Radcliffe and A. D. Scott, Reconstruction subsets of $\mathbb{Z}_n$, J. Comb. Theory, Ser. A **83** (98), 169-187

[11] A. J. Radcliffe and A. D. Scott, Reconstructing subsets of non-Abelian groups, manuscript.