

# Reconstructing random jigsaws

Paul Balister, Béla Bollobás, and Bhargav Narayanan

ABSTRACT. A colouring of the edges of an  $n \times n$  grid is said to be *reconstructible* if the colouring is uniquely determined by the multiset of its  $n^2$  *tiles*, where the tile corresponding to a vertex of the grid specifies the colours of the edges incident to that vertex in some fixed order. In 2015, Mossel and Ross asked the following question: if the edges of an  $n \times n$  grid are coloured independently and uniformly at random using  $q = q(n)$  different colours, then is the resulting colouring reconstructible with high probability? From below, Mossel and Ross showed that such a colouring is not reconstructible when  $q = o(n^{2/3})$  and from above, Bordenave, Feige and Mossel and Nenadov, Pfister and Steger independently showed, for any fixed  $\varepsilon > 0$ , that such a colouring is reconstructible when  $q \geq n^{1+\varepsilon}$ . Here, we improve on these results and prove the following: there exist absolute constants  $C, c > 0$  such that, as  $n \rightarrow \infty$ , the probability that a random colouring as above is reconstructible tends to 1 if  $q \geq Cn$  and to 0 if  $q \leq cn$ .

## 1. INTRODUCTION

The reconstruction problem for a family of discrete structures asks the following: is it possible to uniquely reconstruct a structure in this family from the ‘deck’ of all its substructures of some fixed size? Combinatorial reconstruction problems have a very rich history. The oldest such problem is perhaps the graph reconstruction conjecture of Kelly and Ulam [7, 15, 6], and analogous questions for various other families of discrete structures have since been studied; see, for instance, the results of Alon, Caro, Krasikov and Roditty [1] on reconstructing finite sets satisfying symmetry conditions, Pebody’s [11, 12] results on reconstructing finite abelian groups, and the results of Pebody, Radcliffe and Scott [13] on reconstructing finite subsets of the plane.

Another natural line of enquiry, and the one we pursue here, is to ask how the answer to the reconstruction problem changes when we are required to reconstruct a *typical* (as opposed to an arbitrary) structure in a family of discrete structures. These probabilistic questions typically have substantially different answers as compared to their extremal counterparts, as evidenced by the results of Bollobás [2] and Radcliffe and Scott [14], for example.

---

*Date:* 30 May 2017.

*2010 Mathematics Subject Classification.* Primary 60C05; Secondary 60K35, 68R15.

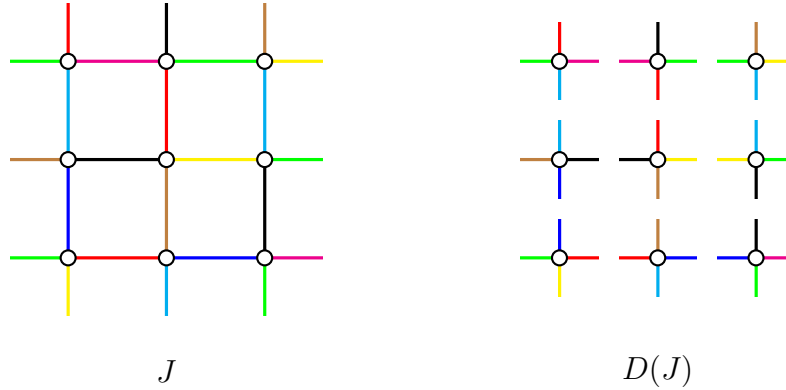


FIGURE 1. A  $(3, 8)$ -jigsaw and its deck.

Here, we shall study a reconstruction problem proposed by Mossel and Ross in connection with the problem of shotgun-sequencing DNA sequences. To state this problem, we need a few definitions.

For  $n \in \mathbb{N}$ , we write  $[n]$  for the set  $\{1, 2, \dots, n\}$ , and by the *extended*  $n \times n$  grid, we mean the grid  $[n]^2 \subset \mathbb{Z}^2$  together with the edges of  $\mathbb{Z}^2$  incident to the boundary vertices. For  $n, q \in \mathbb{N}$ , an  $(n, q)$ -jigsaw is a  $q$ -coloured extended  $n \times n$  grid, i.e., an extended  $n \times n$  grid whose  $2n(n+1)$  edges are coloured using a set of  $q$  different colours which we take to be  $[q]$  for concreteness. The *tile* of an  $(n, q)$ -jigsaw corresponding to a vertex  $v \in [n]^2$  is given by the colouring of the four edges incident to  $v$ ; more precisely, writing  $e_1 = (0, 1)$ ,  $e_2 = (1, 0)$ ,  $e_3 = -e_1$  and  $e_4 = -e_2$ , if the edge between  $v$  and  $v + e_i$  gets colour  $c_i \in [q]$  for  $1 \leq i \leq 4$ , then the tile corresponding to  $v$  is the tuple  $(c_i)_{i=1}^4 \in [q]^4$ . Finally, the *deck* of an  $(n, q)$ -jigsaw is the multiset of the tiles of the jigsaw, one for each vertex of  $[n]^2$ .

We now define what it means for a jigsaw to be reconstructible from its deck. Writing  $\mathcal{J}(n, q)$  for the set of all  $(n, q)$ -jigsaws and  $\mathcal{D}(n, q)$  for the family of all multisets of size  $n^2$  whose elements are chosen from  $[q]^4$ , let  $D: \mathcal{J}(n, q) \rightarrow \mathcal{D}(n, q)$  be the map sending a jigsaw  $J$  to its deck  $D(J)$ . We say that a jigsaw  $J \in \mathcal{J}(n, q)$  is *reconstructible* if  $D^{-1}(D(J)) = \{J\}$ ; equivalently, a jigsaw  $J$  is reconstructible if  $D(J) = D(J')$  implies  $J = J'$ .

We view  $\mathcal{J}(n, q)$  as a probability space by endowing it with the uniform distribution, and write  $J(n, q)$  for a random  $(n, q)$ -jigsaw drawn from this distribution; equivalently,  $J(n, q)$  is a random  $(n, q)$ -jigsaw generated by independently colouring each edge of the extended  $n \times n$  grid with a randomly chosen element of  $[q]$ . Our primary concern is the following problem about the reconstructibility of a random  $(n, q)$ -jigsaw raised by

Mossel and Ross [9]; of course, there exists only one  $(n, 1)$ -jigsaw for each  $n \in \mathbb{N}$  (and this jigsaw is trivially reconstructible), so in what follows, we assume implicitly that  $q \geq 2$ .

**Problem 1.1.** *For what  $q = q(n)$  is  $J(n, q)$  reconstructible with high probability?*

From below, Mossel and Ross [9] showed that  $\mathbb{P}(J(n, q) \text{ is reconstructible}) \rightarrow 0$  when  $q = o(n^{2/3})$  due to the presence of local obstacles to reconstruction: in this regime, a random  $(n, q)$ -jigsaw contains, with high probability, two configurations each consisting of two neighbouring vertices which may be ‘exchanged’ in the jigsaw, and this is easily seen to obstruct unique reconstruction; however, this argument does not extend to configurations involving single exchangeable vertices (and to a corresponding bound when  $q = o(n)$ ) since the presence of two identical tiles in the deck does not necessarily prevent unique reconstruction. From above, Bordenave, Feige and Mossel [4] and Nenadov, Pfister and Steger [10] independently showed, for any fixed  $\varepsilon > 0$ , that  $\mathbb{P}(J(n, q) \text{ is reconstructible}) \rightarrow 1$  when  $q \geq n^{1+\varepsilon}$ . Here, we improve on both of these bounds and prove the following nearly optimal result.

**Theorem 1.2.** *There exist absolute constants  $C, c > 0$  such that, as  $n \rightarrow \infty$ , we have*

$$\mathbb{P}(J(n, q) \text{ is reconstructible}) \rightarrow \begin{cases} 1 & \text{if } q \geq Cn, \text{ and} \\ 0 & \text{if } 2 \leq q \leq cn. \end{cases}$$

The two results contained in the statement of Theorem 1.2 are proved by very different methods: the ‘0-statement’ follows from a double counting argument, while the proof of the ‘1-statement’ is based on an isoperimetric argument which draws from (but is somewhat more involved than) the strategy used by Bordenave, Feige and Mossel [4] where one attempts to reconstruct a suitably large neighbourhood of a tile in order to identify its neighbours in the jigsaw.

We shall prove Theorem 1.2 with  $C = 10^{40}$  and  $c = 1/\sqrt{e}$ . With some more effort, it should be possible to refine our proof of Theorem 1.2 to show that the result holds for any  $C > 1$  (at which point our argument breaks down); however, we choose not to present the details of this stronger claim because we believe the critical number of colours for an  $n \times n$  grid to be  $n/\sqrt{e}$ , and conjecture that the 0-statement in Theorem 1.2 is sharp.

**Conjecture 1.3.** *For any  $\varepsilon > 0$ , as  $n \rightarrow \infty$ , we have*

$$\mathbb{P}(J(n, q) \text{ is reconstructible}) \rightarrow 1$$

*for all  $q \geq (1/\sqrt{e} + \varepsilon)n$ .*

This paper is organised as follows. We begin with some notation and preliminary discussion in Section 2. We give the short proof of the 0-statement in Theorem 1.2

in Section 3. We prove the key estimate required for the proof of the 1-statement in Theorem 1.2 in Section 4, and complete the proof of our main result in Section 5. We conclude with some discussion in Section 6.

## 2. PRELIMINARIES

For a pair of integers  $a \leq b$ , we write  $[a, b]$  for the set  $\{a, a+1, \dots, b\}$ , and for a natural number  $n \in \mathbb{N}$ , we abbreviate the set  $[1, n]$  by  $[n]$ .

We define the vectors  $e_1 = (0, 1)$ ,  $e_2 = (1, 0)$ ,  $e_3 = -e_1$  and  $e_4 = -e_2$ , and we endow the square lattice  $\mathbb{Z}^2$  with the graph structure of the infinite grid where two vertices  $u, v \in \mathbb{Z}^2$  are adjacent if  $u - v = e_i$  for some  $1 \leq i \leq 4$ ; also, we write  $\Lambda$  for the set of edges of the infinite grid on  $\mathbb{Z}^2$ .

Let  $X \subset \mathbb{Z}^2$  be a finite subset of the square lattice. We write  $\Lambda(X) \subset \Lambda$  for the set of edges of the grid induced by  $X$  and  $\partial X \subset \Lambda$  for the *boundary* of  $X$ , i.e., the set of edges between  $X$  and  $\mathbb{Z}^2 \setminus X$ ; also, we write  $\bar{\Lambda}(X) = \Lambda(X) \cup \partial X$  for the set of edges of the grid with at least one endpoint in  $X$ . Since  $X$  is finite, note that  $\mathbb{Z}^2 \setminus X$  contains a unique infinite connected component; the *external boundary* of  $X$ , written  $\partial_e X$ , is the set of edges between  $X$  and this infinite component, and the *internal boundary* of  $X$ , written  $\partial_i X$ , is defined to be  $\partial X \setminus \partial_e X$ . Finally, the *vertex boundary* of  $X$  is defined to be the set of vertices of  $X$  incident to some edge of  $\partial_e X$ .

Observe that if the points of a finite set  $X \subset \mathbb{Z}^2$  have  $a$  different  $x$ -coordinates and  $b$  different  $y$ -coordinates in total, then  $|X| \leq ab$  and the external boundary of  $X$  has size at least  $2a + 2b$ ; this observation implies the following well-known isoperimetric statement.

**Proposition 2.1.** *For any finite set  $X \subset \mathbb{Z}^2$ , we have  $|\partial X| \geq |\partial_e X| \geq 4|X|^{1/2}$ .*  $\square$

We say that a finite set  $X \subset \mathbb{Z}^2$  is *connected* if it is connected when viewed as a subset of the vertex set of the infinite grid, and in what follows, the distance between two points  $u, v \in \mathbb{Z}^2$  will always mean the graph-distance between  $u$  and  $v$  in the infinite grid. Also, we say that a finite set of edges  $A \subset \Lambda$  is *dual-connected* if the corresponding set of edges in the planar dual of the infinite grid is connected. Finally, for  $X \subset \mathbb{Z}^2$  and  $A \subset \Lambda$ , we write  $D(X, A)$  for the graph on  $X$  whose edge set is  $\Lambda(X) \setminus A$ ; in other words,  $D(X, A)$  is the graph induced by  $X$  in the grid after we delete the edges in  $A$ .

It will be convenient to have some notation to deal with maps from  $\mathbb{Z}^2$  to  $\mathbb{Z}^2$ . Let  $f$  be an injective map from a finite set  $X \subset \mathbb{Z}^2$  to  $\mathbb{Z}^2$ . We say that a set  $Y \subset X$  is  *$f$ -rigid* if  $f(x) - f(y) = x - y$  for all  $x, y \in Y$ . A *block* of  $f$  is a maximal connected rigid subset of  $X$ ; it is easy to check that each vertex of  $X$  belongs to a unique block, so the blocks of  $f$  partition  $X$ . An edge  $z \in \Lambda(X)$  is said to be  *$f$ -split* if the endpoints of  $z$  belong to different blocks of  $f$ . We write  $\Lambda_f \subset \Lambda$  for the union of  $\partial X$  and the set of  $f$ -split edges; loosely speaking,  $\Lambda_f$  is the set of those edges across which we cannot

‘control’  $f$ . Note that  $\Lambda_f$  may be decomposed into dual-connected components; the following geometric fact about such components will prove useful.

**Proposition 2.2.** *Let  $f$  be an injective map from a finite set  $X \subset \mathbb{Z}^2$  to  $\mathbb{Z}^2$  and let  $A$  be a dual-connected component of  $\Lambda_f$ . If  $Y \subset X$  is a connected component of  $D(X, A)$ , then the vertices of  $Y$  incident to some edge of  $A$  are all contained in a single block of  $f$ .*  $\square$

We will also need the following property of finite grids.

**Proposition 2.3.** *For  $n \in \mathbb{N}$ , if  $X \subset [n]^2$  is such that the distance between any pair of distinct vertices in  $X$  is at least three, then  $[n]^2 \setminus X$  is connected.*  $\square$

Finally, let us quickly restate the problem at hand formally. Note that the edges of the extended  $n \times n$  grid are precisely the elements of the set  $\bar{\Lambda}([n]^2)$ , so an  $(n, q)$ -jigsaw  $J$  is a map  $J: \bar{\Lambda}([n]^2) \rightarrow [q]$ . Given an  $(n, q)$ -jigsaw  $J$ , the tile  $J_v$  corresponding to a vertex  $v \in [n]^2$  is the sequence  $(J(v, v + e_i))_{i=1}^4 \in [q]^4$ , and the deck  $D(J)$  of  $J$  is the multiset  $\{J_v : v \in [n]^2\}$ . As defined previously, a jigsaw  $J$  is reconstructible from its deck if  $D(J') = D(J)$  implies that  $J' = J$ . We write  $J(n, q)$  to denote a random  $(n, q)$ -jigsaw generated by independently colouring each edge of  $\bar{\Lambda}([n]^2)$  with a randomly chosen element of  $[q]$ . In this language, our primary concern is the following question: for what  $q = q(n)$  is  $J(n, q)$  reconstructible with high probability?

We shall make use of standard asymptotic notation; in what follows, the variable tending to infinity will always be  $n$  unless we explicitly specify otherwise. We use the term *with high probability* to mean with probability tending to 1 as  $n \rightarrow \infty$ . For the sake of clarity of presentation, we systematically omit floor and ceiling signs whenever they are not crucial.

### 3. PROOF OF THE 0-STATEMENT

In this short section, we prove the 0-statement in Theorem 1.2 by an elementary counting argument.

*Proof of the 0-statement in Theorem 1.2.* Recall that  $\mathcal{J}(n, q)$  is the set of all  $(n, q)$ -jigsaws,  $\mathcal{D}(n, q)$  is the family of all multisets of size  $n^2$  whose elements are chosen from  $[q]^4$ , and  $D: \mathcal{J}(n, q) \rightarrow \mathcal{D}(n, q)$  is the map sending a jigsaw  $J$  to its deck  $D(J)$ .

Let  $\mathcal{J}_R(n, q) \subset \mathcal{J}(n, q)$  denote the set of all reconstructible jigsaws, i.e., jigsaws  $J$  such that  $D^{-1}(D(J)) = \{J\}$ . Since  $D: \mathcal{J}_R(n, q) \rightarrow \mathcal{D}(n, q)$  is an injection,  $|\mathcal{J}_R(n, q)| \leq |\mathcal{D}(n, q)|$ . Consequently, we have

$$\mathbb{P}(J(n, q) \text{ is reconstructible}) = |\mathcal{J}_R(n, q)|/|\mathcal{J}(n, q)| \leq |\mathcal{D}(n, q)|/|\mathcal{J}(n, q)|.$$

Now, it is easy to see that

$$|\mathcal{D}(n, q)| = \binom{n^2 + q^4 - 1}{n^2} \quad \text{and} \quad |\mathcal{J}(n, q)| = q^{2n(n+1)},$$

so it follows that

$$\mathbb{P}(J(n, q) \text{ is reconstructible}) \leq \binom{n^2 + q^4 - 1}{n^2 - 1} q^{-2n^2 - 2n} \leq \binom{n^2 + q^4}{n^2} q^{-2n^2 - 2n}.$$

If  $2 \leq q \leq \sqrt{n}$ , then we have

$$\binom{n^2 + q^4}{n^2} q^{-2n^2 - 2n} \leq \binom{2n^2}{n^2} 2^{-2n^2 - 2n} \leq 2^{-2n}.$$

If  $\sqrt{n} < q \leq n/\sqrt{e}$  on the other hand, then we deduce using Stirling's approximation that

$$\begin{aligned} \binom{n^2 + q^4}{n^2} q^{-2n^2 - 2n} &= \frac{q^{2n^2 - 2n}}{(n^2)!} \prod_{i=1}^{n^2} \left(1 + \frac{i}{q^4}\right) \leq \frac{q^{2n^2 - 2n}}{(n^2)!} \left(1 + \frac{n^2}{q^4}\right)^{n^2} \\ &= O\left(\frac{q^{-2n}}{n} \exp\left(n^2 \log\left(\frac{q^2}{n^2}\right) + \frac{n^4}{q^4} + n^2\right)\right) = O(q^{-2n}). \end{aligned}$$

We conclude from the above estimates that

$$\mathbb{P}(J(n, q) \text{ is reconstructible}) = o(1)$$

for all  $2 \leq q \leq n/\sqrt{e}$ . □

#### 4. RECONSTRUCTING LARGE NEIGHBOURHOODS

The starting point of our approach to proving the 1-statement in Theorem 1.2 is the strategy adopted by Bordenave, Feige and Mossel [4] to show that  $J = J(n, q)$  is reconstructible with high probability when  $q \geq n^{1+\varepsilon}$  for some fixed  $\varepsilon > 0$ . Given the deck  $D(J)$  of  $J$ , Bordenave, Feige and Mossel use the following procedure to identify the neighbours of a given tile  $J_v$  with  $v \in [n]^2$ . For some large integer  $k \approx 1/\varepsilon$ , they consider all subsets of  $D(J)$  of size  $(2k+1)^2$  that include the tile  $J_v$  and for each such set, they check if the tiles in that set can be ‘legally assembled’ on a  $(2k+1) \times (2k+1)$  grid with  $J_v$  at the centre of this grid. While there might exist many such legal assemblies with  $J_v$  at the centre, they show that with high probability, the four neighbours of  $J_v$  in any such legal assembly are identical to the four tiles neighbouring  $J_v$  in the original jigsaw. This allows them to identify the neighbours of all tiles corresponding to vertices at distance at least  $k$  from the boundary of the grid; once this has been accomplished, it is reasonably straightforward to reconstruct  $J$ .

We adopt a similar strategy to the one described above, although in order to show that  $J(n, q)$  is reconstructible when  $q \approx n$  (as opposed to when  $q \geq n^{1+\varepsilon}$ ), we require

more delicate arguments; for example, we need to take  $k \approx \log n$  (as opposed to  $k \approx 1/\varepsilon$ ) and this in turn necessitates more careful estimates.

We now fix positive integers  $n, q \in \mathbb{N}$  and set  $k = k(n) = \lceil \log n \rceil$ ; all inequalities in the sequel will hold provided  $n$  and  $k$  are sufficiently large.

**4.1. Constraint graphs.** Let  $J: \bar{\Lambda}([n]^2) \rightarrow [q]$  be an  $(n, q)$ -jigsaw, and let  $f$  be an injection from a finite set  $X \subset \mathbb{Z}^2$  to  $[n]^2$ . We say that  $f$  is *feasible for  $J$*  if for any pair of adjacent vertices  $x, y \in X$ , we have  $J(x', x' + y - x) = J(y', y' + x - y)$ , where  $x' = f(x)$  and  $y' = f(y)$ . Clearly, any injective function  $f$  as above describes an arrangement of a subset of the tiles of  $J$  on the grid at the vertices of  $X$  (where the tile placed at a position  $x \in X$  is precisely  $J_{f(x)}$ ); our definition of feasibility makes precise the notion of when  $f$  describes a legal arrangement of tiles. Constraint graphs provide us with an alternate description of legal arrangements and we define these objects below.

The *constraint graph* of an injective map  $f$  from a finite set  $X \subset \mathbb{Z}^2$  to  $\mathbb{Z}^2$ , denoted by  $\mathcal{G}_f$ , is a graph whose vertex set is a subset of  $\Lambda$  and whose edge set contains one edge, called a *constraint*, for each  $f$ -split edge, where if  $\{x, y\}$  is an  $f$ -split edge with  $y = x + e_i$  for some  $1 \leq i \leq 4$ , then the constraint corresponding to this edge is an edge joining  $\{f(x), f(x) + e_i\}$  and  $\{f(y), f(y) - e_i\}$  in the constraint graph; the vertex set of  $\mathcal{G}_f$  is the subset of  $\Lambda$  spanned by the edges of  $\mathcal{G}_f$ . In the language of constraint graphs, it is clear that if  $J: \bar{\Lambda}([n]^2) \rightarrow [q]$  is an  $(n, q)$ -jigsaw and  $f$  is an injection from a finite subset of  $\mathbb{Z}^2$  to  $[n]^2$ , then  $f$  is feasible for  $J$  if and only if  $J$  is constant on each connected component of  $\mathcal{G}_f$ . We define  $\gamma(f)$  to be the difference between the size of the vertex set of  $\mathcal{G}_f$  and the number of connected components of  $\mathcal{G}_f$ . We require the following observation due to Bordenave, Feige and Mossel [4]; we include the short proof for completeness.

**Proposition 4.1.** *For any injective map  $f$  from a finite subset of  $\mathbb{Z}^2$  to  $[n]^2$ , we have*

$$\mathbb{P}(f \text{ is feasible for } J(n, q)) = q^{-\gamma(f)}.$$

*Proof.* First, choose a representative from each connected component of  $\mathcal{G}_f$ . It is clear that  $f$  is feasible for  $J = J(n, q)$  if and only if the following holds: for each vertex of  $\mathcal{G}_f$ , the colour assigned by  $J$  to this vertex is equal to the colour assigned by  $J$  to the representative vertex from the corresponding connected component of  $\mathcal{G}_f$ . Thus, the event that  $f$  is feasible for  $J$  is an intersection of  $\gamma(f)$  independent events, and each of these events has probability  $1/q$ ; the claim follows.  $\square$

It is easy to see that the maximum degree of a constraint graph is at most two, so every constraint graph is a union of paths and cycles; this observation implies the following.



**Proposition 4.2.** *If  $f$  is an injection from a finite subset of  $\mathbb{Z}^2$  to  $\mathbb{Z}^2$ , then  $\gamma(f) \geq |V(\mathcal{G}_f)|/2 \geq |E(\mathcal{G}_f)|/2$ .  $\square$*

**4.2. Windows.** To make precise the idea of recovering the four tiles neighbouring a given tile by attempting to reconstruct a large neighbourhood the tile in question, we need the notion of a ‘window’.

For  $v \in [n]^2$  and an  $(n, q)$ -jigsaw  $J$ , a  $v$ -window with respect to  $J$  is an injective map  $f: [-k, k]^2 \rightarrow [n]^2$  such that  $f(0, 0) = v$  and  $f$  is feasible for  $J$ ; we remind the reader that  $k = \lceil \log n \rceil$  here, and in what follows.

If  $v \in [n]^2$  is at distance at least  $k$  from the vertex boundary of the  $n \times n$  grid, then the map defined by  $f(x) = v + x$  for all  $x \in [-k, k]^2$  is a  $v$ -window; more generally, if there exists some  $v' \in [n]^2$  at distance at least  $k$  from the vertex boundary of the  $n \times n$  grid such that  $J_{v'} = J_v$ , then the map defined by  $f(0, 0) = v$  and  $f(x) = v' + x$  for all  $x \in [-k, k]^2 \setminus \{(0, 0)\}$  is a  $v$ -window. A  $v$ -window  $f$  is said to be *trivial* if  $(J_{f(e_i)})_{i=1}^4 = (J_{v'+e_i})_{i=1}^4$  for some  $v' \in [n]^2$  such that  $J_{v'} = J_v$ ; in other words, a  $v$ -window is trivial if the four tiles neighbouring  $J_v$  in the  $v$ -window are identical to the four tiles neighbouring some tile  $J_{v'}$  in the jigsaw, with  $J_{v'}$  itself identical to  $J_v$ . This definition of triviality is motivated by the fact that when  $q \approx n$ , the deck of  $J(n, q)$  may contain some tiles of multiplicity greater than one (though, as we shall see, this will not present an obstacle to reconstruction). We shall show, provided  $q$  is suitably large, that all windows with respect to  $J(n, q)$  are trivial with high probability; the aim of this section is to establish the following lemma.

**Lemma 4.3.** *If  $q \geq 10^{40}n$ , then  $J(n, q)$  has the following property with high probability: for each  $v \in [n]^2$ , every  $v$ -window with respect to  $J(n, q)$  is trivial.*

**4.3. Templates.** To prove Lemma 4.3, it is natural to first attempt to use a union bound over all candidate injective maps from  $[-k, k]^2$  to  $[n]^2$ ; however, this turns out to be too crude for our purposes. The reason for this is roughly as follows: the number of candidate windows is artificially inflated by maps  $f: [-k, k]^2 \rightarrow [n]^2$  with a large number of ‘holes’; more precisely, there exist too many candidate windows  $f: [-k, k]^2 \rightarrow [n]^2$  with the property that one of the blocks of  $f$  is contained entirely in the interior of another block of  $f$ . One could hope to address this issue by locally modifying a candidate window so as to remove such pairs of ‘nested blocks’, but attempting to do so results in a situation where some tiles of the jigsaw end up getting used multiple times.

To circumvent the difficulties outlined above, we introduce the notion of a ‘template’. To introduce this notion, it will be helpful to first have some notation.

Let  $A \subset \bar{\Lambda}([-k, k]^2)$  be a set of edges of the grid. Recall that  $D([-k, k]^2, A)$  is the graph on  $[-k, k]^2$  whose edge set is  $\Lambda([-k, k]^2) \setminus A$ . For any connected component  $X \subset [-k, k]^2$  of  $D([-k, k]^2, A)$ , we define the *quasiblock*  $\hat{X}$  associated with  $X$  to be the set of vertices of  $X$  incident to some edge in  $A$ ; in the sequel, when we refer to a



quasiblock  $\hat{X}$  of  $A$ , we implicitly assume that the corresponding connected component of  $D([-k, k]^2, A)$  is denoted by  $X$ . Finally, we write  $A^*$  for the set  $A \cap \Lambda([-k, k]^2)$ .

For  $v \in [n]^2$ , a  $v$ -template is a pair  $(A, h)$ , where  $A \subset \bar{\Lambda}([-k, k]^2)$  and  $h$  is an injective map from the union of the quasiblocks of  $A$  to  $[n]^2$ , such that

- (1)  $A$  contains at least one edge incident to  $(0, 0)$ ,
- (2)  $A$  does not consist of precisely the four edges incident either to  $(0, 0)$  or one of its four neighbours,
- (3)  $A$  is dual-connected,
- (4)  $h(0, 0) = v$ ,
- (5) either  $\partial[-k, k]^2 \subset A$  or  $\partial[-k, k]^2 \cap A = \emptyset$ ,
- (6) each quasiblock of  $A$  is  $h$ -rigid, and
- (7) each edge of  $A^*$  is  $h$ -split.

Given an  $(n, q)$ -jigsaw  $J$ , we abuse notation slightly and say that a  $v$ -template  $(A, h)$  is feasible for  $J$  if  $h$  is feasible for  $J$ . The definition of a template is motivated by the following fact.

**Proposition 4.4.** *Let  $J$  be an  $(n, q)$ -jigsaw and let  $v \in [n]^2$ . If there exists a nontrivial  $v$ -window  $f$  with respect to  $J$ , then there exists a  $v$ -template  $(A, h)$  that is feasible for  $J$ .*

*Proof.* Since any tile is uniquely determined by its four neighbours in any valid arrangement of tiles, it is easy to check using the fact that  $f$  is a nontrivial  $v$ -window that there exists an  $f$ -split edge  $z$  incident to  $(0, 0)$  with the property that the dual-connected component of  $z$  in  $\Lambda_f$  does not consist of precisely the four edges incident either to  $(0, 0)$  or one of its four neighbours. We now take  $A$  to be the dual-connected component of  $z$  in  $\Lambda_f$  and  $h$  to be the restriction of  $f$  to the endpoints of  $A$  in  $[-k, k]^2$ .

Clearly,  $A$  contains at least one edge incident to  $(0, 0)$ , does not consist of precisely the four edges incident either to  $(0, 0)$  or one of its four neighbours, and is dual-connected. As  $f$  is a  $v$ -window that extends  $h$ , we have  $h(0, 0) = v$ . Next, since  $A$  is a dual-connected component of  $\Lambda_f$  and  $\partial[-k, k]^2$  is a dual-connected subset of  $\Lambda_f$ , either  $\partial[-k, k]^2 \subset A$  or  $\partial[-k, k]^2 \cap A = \emptyset$ . Furthermore, it follows from Proposition 2.2 that every quasiblock of  $A$  is a subset of a single block of  $f$ ; since  $f$  extends  $h$ , it follows that every quasiblock of  $A$  is  $h$ -rigid. Finally, since each edge of  $A^*$  is  $f$ -split, each edge of  $A^*$  must also be  $h$ -split.  $\square$

We shall prove Lemma 4.3 using a union bound over templates as opposed to windows; in particular, we shall show, provided  $q$  is suitably large, that with sufficiently high probability, no  $v$ -template  $(A, h)$  is feasible for  $J(n, q)$ .

We say that a template  $(A, h)$  is *large* if  $\partial[-k, k]^2 \subset A$ , and *small* if  $A \cap \partial[-k, k]^2 = \emptyset$ . Of course, every template is either large or small. We shall require slightly different arguments to deal with large and small templates. The following fact will prove useful

when estimating the number of templates of both types; see Problem 45 in [3], for instance.

**Proposition 4.5.** *In a graph of maximal degree  $\Delta$ , the number of connected induced subgraphs with  $l + 1$  vertices, one of which is a given vertex, is at most  $(e(\Delta - 1))^l$ .  $\square$*

**4.4. Large templates.** We will need an estimate for the number of large templates, as well as an estimate for the probability that such a template is feasible for  $J(n, q)$ .

In order to simplify our bookkeeping, it will be helpful to introduce the notion of a ‘cluster’. Let  $(A, h)$  be a large  $v$ -template. For a quasiblock  $\hat{X} \subset [-k, k]^2$  of  $A$ , let  $h(\hat{X}) \subset [n]^2$  denote the (rigid) image of  $\hat{X}$  under  $h$ . Let us define the *cluster graph* of  $(A, h)$  to be the graph on the quasiblocks of  $A$  where two quasiblocks  $\hat{X}$  and  $\hat{Y}$  are adjacent if there exists an edge of the lattice between  $h(x)$  and  $h(y)$  for some  $x \in \hat{X}$  and  $y \in \hat{Y}$  and furthermore, this edge belongs to the external boundary of both  $h(\hat{X})$  and  $h(\hat{Y})$ . A *cluster* of  $(A, h)$  is then a subset of  $[n]^2$  consisting of the images of all the quasiblocks in a connected component of the cluster graph.

For non-negative integers  $\delta$ ,  $r_1$  and  $r_2$ , we say that a large  $v$ -template  $(A, h)$  is of type  $(\delta, r_1, r_2)$  if  $|A| = \delta$ , the number of quasiblocks of  $A$  is  $r_1 + r_2$ , and the number of clusters of  $(A, h)$  is  $r_1$ . Writing  $N_l(\delta, r_1, r_2)$  for the number of large  $v$ -templates of type  $(\delta, r_1, r_2)$ , we have the following estimate.

**Proposition 4.6.** *For non-negative integers  $\delta$ ,  $r_1$  and  $r_2$ , we have*

$$N_l(\delta, r_1, r_2) = \begin{cases} 0 & \text{if } \delta < 8k + 4 \text{ or } \delta < r_1 + r_2, \text{ and} \\ O(30^\delta n^{2r_1} k^{6r_2} / n^2) & \text{otherwise.} \end{cases}$$

*Proof.* We estimate the number of large  $v$ -templates  $(A, h)$  of type  $(\delta, r_1, r_2)$  by first estimating the number of ways in which we may choose  $A$ , and then estimating the number of ways in which we may choose  $h$  once we are given  $A$ .

First, we may assume that  $\delta \geq 8k + 4$  since if  $(A, h)$  is a large  $v$ -template, then  $\partial[-k, k]^2 \subset A$  by definition. Second, we may also suppose that  $\delta \geq r_1 + r_2$ ; indeed, by considering a northern most vertex of each quasiblock of  $A$  for example, we observe that the number of quasiblocks of  $A$  is at most the size of  $A$ , so the claimed bound holds trivially in the case where  $\delta < r_1 + r_2$ .

We now estimate the number of ways to choose  $A$ . Since  $A$  must contain an edge incident to  $(0, 0)$  and must additionally be dual-connected, it follows from Proposition 4.5 that the number of choices for  $A$  (even ignoring the restriction that  $A$  has precisely  $r_1 + r_2$  quasiblocks) is at most  $4(5e)^{\delta-1} \leq 15^\delta$  as each edge of the square lattice is adjacent to six other edges of the square lattice in the planar dual of the lattice.

Next, we estimate the number of ways to choose  $h$  for a given  $A$ . Once we fix an  $A$  with  $r_1 + r_2$  quasiblocks, it suffices to specify the image of one vertex from each

quasiblock of  $A$  under  $h$  to completely specify  $h$  since each quasiblock of  $A$  is  $h$ -rigid. We count the number of ways to choose  $h$  as follows. We first choose  $r_1$  *representative* quasiblocks in such a way that these quasiblocks all belong to different clusters, while ensuring that the quasiblock containing  $(0, 0)$  is one of these representatives; the number of ways to choose these representatives is at most

$$\binom{r_1 + r_2 - 1}{r_1 - 1} \leq 2^{r_1 + r_2} \leq 2^\delta.$$

Of course, since  $h(0, 0) = v$ , this specifies the image of the quasiblock containing  $(0, 0)$ . We then specify the image of a vertex (say the northernmost) from each of the remaining  $r_1 - 1$  representative quasiblocks; this may be done in  $n^{2(r_1 - 1)}$  ways. Finally, we note that there are  $O(k^6)$  choices for the image of one of the  $r_2$  leftover quasiblocks. To see this, note that each leftover quasiblock belongs to the same cluster as one of the representative quasiblocks, so the image of such a leftover quasiblock must be at distance at most  $(2k + 1)^2$  from the image of one of the representative quasiblocks; the claimed bound follows since there are at most  $(2k + 1)^2$  points contained in the representative quasiblocks, and there are at most  $(2d + 1)^2$  points at distance at most  $d$  from any fixed point of the grid. Combining these estimates, we see that the number of choices for  $h$  once we have specified  $A$  is  $O(2^\delta n^{2(r_1 - 1)} k^{6r_2})$ .

It now follows that

$$N(\delta, r_1, r_2) = O(15^\delta 2^\delta n^{2(r_1 - 1)} k^{6r_2}) = O(30^\delta n^{2r_1} k^{6r_2} / n^2). \quad \square$$

To estimate the probability that a large  $v$ -template  $(A, h)$  is feasible for  $J(n, q)$ , we shall appeal to Proposition 4.1 which gives us a bound for this probability in terms of  $\gamma(h)$ ; recall that  $\gamma(h)$  is the difference between the size of the vertex set of  $\mathcal{G}_h$  and the number of connected components of  $\mathcal{G}_h$ , where  $\mathcal{G}_h$  is the constraint graph of  $h$ .

**Proposition 4.7.** *If  $(A, h)$  is a large  $v$ -template of type  $(\delta, r_1, r_2)$ , then we have  $\gamma(h) \geq \delta/20$  and  $\gamma(h) \geq 2r_1 + r_2/2 - 2r_1/(2k + 1)$ .*

*Proof.* We shall use Proposition 4.2 to bound  $\gamma(h)$  from below. We will estimate the size of both the vertex set and the edge set of  $\mathcal{G}_h$ .

Since  $\mathcal{G}_h$  contains one edge for each  $h$ -split edge, it is easy to see that the edge set of  $\mathcal{G}_h$  has size at least  $A^*$ , so  $|E(\mathcal{G}_h)| \geq |A^*| = |A| - (8k + 4)$  as  $|\partial[-k, k]^2| = 8k + 4$ . Now, since  $A$  contains an edge incident to  $(0, 0)$ , is dual-connected and also contains  $\partial[-k, k]^2$ , we have  $|A^*| \geq k$  and consequently,  $|A| \geq 9k + 4$ ; it follows, provided  $k$  is sufficiently large, that  $|E(\mathcal{G}_h)| \geq |A| - (8k + 4) \geq |A|/10 = \delta/10$ . We now conclude from Proposition 4.2 that  $\gamma(h) \geq |E(\mathcal{G}_h)|/2 \geq \delta/20$ .

To estimate the size of the vertex set of  $\mathcal{G}_h$ , we begin with the following observation. First, if  $\hat{X}$  is a quasiblock of  $A$ , then since  $\hat{X}$  is  $h$ -rigid, there is a one-to-one correspondence between  $\partial_e \hat{X}$  and  $\partial_e h(\hat{X})$ . Next, note that each edge of  $\partial_e \hat{X}$  is either an element

of  $A^*$  (and consequently  $h$ -split) or an element of  $\partial[-k, k]^2$ . It now follows that each edge of  $\partial_e h(\hat{X})$  that corresponds to an edge of  $\partial_e \hat{X}$  contained in  $A^*$  must belong to the vertex set of  $\mathcal{G}_h$ .

For a cluster  $K$  of the template  $(A, h)$  composed of the images of the quasiblocks  $\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m$ , we write  $S(K)$  for the set of edges between  $\hat{X}_i$  and  $\hat{X}_j$  for some  $1 \leq i < j \leq m$  and  $T(K)$  for the set  $S(K) \cup \partial_e K$ . First, it is clear that  $S(K)$  and  $\partial_e K$  are disjoint for each cluster  $K$ . Furthermore, it is also easy to see that if  $K_1$  and  $K_2$  are distinct clusters, then the sets  $T(K_1)$  and  $T(K_2)$  are disjoint. Let  $T \subset \bar{\Lambda}([n]^2)$  denote the union of the sets  $T(K)$ , where  $K$  runs over the  $r_1$  clusters of  $(A, h)$ . From our earlier discussion, it follows that an edge of  $T$  is a vertex of  $\mathcal{G}_h$  unless it corresponds to an edge in  $\partial[-k, k]^2$ . Consequently, we have  $|V(\mathcal{G}_h)| \geq |T| - (8k + 4)$ .

We now use an isoperimetric argument to bound  $|T|$  from below; we begin with following observation.

**Claim 4.8.** *For a cluster  $K$  of  $(A, h)$  composed of the images of the quasiblocks  $\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m$ , we have*

$$|T(K)| \geq 4\sqrt{|X_1| + |X_2| + \dots + |X_m|} + m - 1.$$

*Proof.* It immediately follows from the fact that  $K$  corresponds to a connected component of size  $m$  in the cluster graph of  $(A, h)$  that  $|S(K)| \geq m - 1$ . Next, while Proposition 2.1 immediately tells us that

$$|\partial_e K| \geq 4\sqrt{|\hat{X}_1| + |\hat{X}_2| + \dots + |\hat{X}_m|},$$

we may get a better estimate as follows. Note that since  $\partial[-k, k]^2 \subset A$ , the quasiblock  $\hat{X}$  of  $A$  associated with a connected component  $X$  of  $D([-k, k]^2, A)$  is in fact the vertex boundary of  $X$ . Therefore, it follows from the Jordan curve theorem that each quasiblock of  $A$  must divide the plane into an exterior and an interior region. From the definition of a cluster, it follows that  $h(\hat{X}_i)$  lies in the exterior of  $h(\hat{X}_j)$  for all  $i \neq j$ . Consequently, it follows that  $\partial_e K$  is in fact the external boundary of a set of size  $|X_1| + |X_2| + \dots + |X_m|$ ; therefore, we have

$$|\partial_e K| \geq 4\sqrt{|X_1| + |X_2| + \dots + |X_m|}.$$

The claim follows since  $S(K)$  and  $\partial_e K$  are disjoint.  $\square$

By summing the bound from Proposition 4.8 over the  $r_1$  clusters of  $(A, h)$ , we obtain a bound of the form

$$|T| \geq 4\sqrt{a_1} + 4\sqrt{a_2} + \dots + 4\sqrt{a_{r_1}} + r_2$$

for some collection of positive integers  $a_1, a_2, \dots, a_{r_1}$  satisfying  $a_1 + a_2 + \dots + a_{r_1} = (2k+1)^2$ ; this is immediate once we note that each connected component of  $D([-k, k]^2, A)$

contributes precisely once to the bound in Proposition 4.8 as we run over the clusters of  $(A, h)$ . We conclude, using convexity, that

$$|T| \geq 4(r_1 - 1) + 4\sqrt{(2k + 1)^2 - (r_1 - 1)} + r_2 \geq 4r_1 + r_2 + 8k + 4 - \frac{4r_1}{(2k + 1)}.$$

We know from Proposition 4.2 that  $\gamma(h) \geq |V(\mathcal{G}_h)|/2 \geq |T|/2 - (4k + 2)$ ; it now follows that  $\gamma(h) \geq 2r_1 + r_2 - 2r_1/(2k + 1)$ .  $\square$

**4.5. Small templates.** We shall handle small templates using arguments similar to those used to deal with large templates; however, some small subtleties necessitate a slightly different approach to bookkeeping. If  $(A, h)$  is small  $v$ -template, then it may well be the case that  $|A|$  is small, so our estimates need to be capable of handling this; this cannot happen when  $(A, h)$  is large since  $\partial[-k, k]^2 \subset A$  in this case. On the other hand, if  $(A, h)$  is small, then since  $\partial[-k, k]^2 \cap A = \emptyset$ , we do not need to worry about overcounting contributions from  $\partial[-k, k]^2$  when estimating  $\gamma(h)$ . We will modify the arguments we used to deal with large templates slightly in order to balance these considerations.

Let  $(A, h)$  be a small  $v$ -template. Since  $A \cap \partial[-k, k]^2 = \emptyset$ , it is easy to verify that the vertex boundary of  $[-k, k]^2$  is contained in a single connected component of  $D([-k, k]^2, A)$ ; we call the quasiblock corresponding to this connected component the *boundary quasiblock* of  $A$ , and refer to the other quasiblocks of  $A$  as *non-boundary quasiblocks*.

We will need a slight modification of the notion of a ‘cluster’ that distinguishes between the boundary quasiblock and non-boundary quasiblocks. Let  $(A, h)$  be a small  $v$ -template and as before, for a quasiblock  $\hat{X} \subset [-k, k]^2$  of  $A$ , let  $h(\hat{X}) \subset [n]^2$  denote the (rigid) image of  $\hat{X}$  under  $h$ . Let us define the *cluster graph* of  $(A, h)$  to be the graph on the quasiblocks of  $A$  where

- (1) two non-boundary quasiblocks  $\hat{X}$  and  $\hat{Y}$  are adjacent if there exists an edge of the square lattice between  $h(x)$  and  $h(y)$  for some  $x \in \hat{X}$  and  $y \in \hat{Y}$  and furthermore, this edge belongs to the external boundary of both  $h(\hat{X})$  and  $h(\hat{Y})$ , and
- (2) the boundary quasiblock  $\hat{X}$  and a non-boundary quasiblock  $\hat{Y}$  are adjacent if there exists an edge of the square lattice between  $h(x)$  and  $h(y)$  for some  $x \in \hat{X}$  and  $y \in \hat{Y}$  and furthermore, this edge belongs to the internal boundary of  $h(\hat{X})$  and the external boundary of  $h(\hat{Y})$ .

A *cluster* of  $(A, h)$  is then a subset  $[n]^2$  consisting of the images of all the quasiblocks in a connected component of the cluster graph; again, we call the cluster containing the image of the boundary quasiblock the *boundary cluster* and refer to the other clusters as *non-boundary clusters*.

As before, for non-negative integers  $\delta$ ,  $r_1$  and  $r_2$ , we say that a small  $v$ -template  $(A, h)$  is of type  $(\delta, r_1, r_2)$  if  $|A| = \delta$ , the number of quasiblocks of  $A$  is  $r_1 + r_2$ , and the number of clusters of  $(A, h)$  is  $r_1$ . Writing  $N_s(\delta, r_1, r_2)$  for the number of small  $v$ -templates of type  $(\delta, r_1, r_2)$ , we have the following estimate, the proof of which is identical to that of Proposition 4.6.

**Proposition 4.9.** *For non-negative integers  $\delta$ ,  $r_1$  and  $r_2$ , we have*

$$N_s(\delta, r_1, r_2) = O(30^\delta n^{2r_1} k^{6r_2} / n^2). \quad \square$$

To estimate the probability that a small  $v$ -template  $(A, h)$  is feasible for  $J(n, q)$ , we will use the following.

**Proposition 4.10.** *If  $(A, h)$  is a small  $v$ -template of type  $(\delta, r_1, r_2)$ , then we have  $\gamma(h) \geq \delta/2$  and  $\gamma(h) \geq 2r_1 + r_2/2 + 1/2$ .*

*Proof.* As before, we will estimate the size of both the vertex set and the edge set of the constraint graph  $\mathcal{G}_h$ .

Since  $\mathcal{G}_h$  contains one edge for each  $h$ -split edge, it is easy to see that edge set of  $\mathcal{G}_h$  has size at least  $A^*$ . Since  $\partial[-k, k]^2 \cap A = \emptyset$ , we have  $A^* = A$ , so  $|E(\mathcal{G}_h)| \geq |A| = \delta$ . We now conclude from Proposition 4.2 that  $\gamma(h) \geq |E(\mathcal{G}_h)|/2 \geq \delta/2$ .

To estimate the size of the vertex set of  $\mathcal{G}_h$ , we begin with the following observations. First, if  $\hat{X}$  is a non-boundary quasiblock of  $A$ , then since  $\hat{X}$  is  $h$ -rigid, there is a one-to-one correspondence between  $\partial_e \hat{X}$  and  $\partial_e h(\hat{X})$ ; since each edge of  $\partial_e \hat{X}$  is an element of  $A$  (and consequently  $h$ -split, as  $A = A^*$ ), it follows that each edge of  $\partial_e h(\hat{X})$  must belong to the vertex set of  $\mathcal{G}_h$ . Next, if  $\hat{X}$  is the boundary quasiblock of  $A$ , then since each edge of  $\partial_i \hat{X}$  is an element of  $A$ , it follows that each edge of  $\partial_i h(\hat{X})$  must belong to the vertex set of  $\mathcal{G}_h$ .

For a non-boundary cluster  $K$  of  $(A, h)$  composed of the images of the non-boundary quasiblocks  $\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m$ , we write  $S(K)$  for the set of edges between  $\hat{X}_i$  and  $\hat{X}_j$  for some  $1 \leq i < j \leq m$  and  $T(K)$  for the set  $S(K) \cup \partial_e K$ ; it is clear that  $S(K)$  and  $\partial_e K$  are disjoint, so  $T(K)$  is in fact the disjoint union of these sets. For the boundary cluster  $K$  composed of the images of the boundary quasiblock  $X$  and non-boundary quasiblocks  $\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m$ , we write  $S(K)$  for the set of edges between  $\hat{X}_i$  and  $\hat{X}_j$  for some  $1 \leq i < j \leq m$  and  $T(K)$  for the set  $S(K) \cup \partial_i h(\hat{X})$ ; again, it is clear that  $S(K)$  and  $\partial_i h(\hat{X})$  are disjoint and that  $T(K)$  is the disjoint union of these sets. Finally, it is also easy to see that if  $K_1$  and  $K_2$  are distinct clusters, then the sets  $T(K_1)$  and  $T(K_2)$  are disjoint. As before, let  $T \subset \bar{\Lambda}([n]^2)$  denote the union of the sets  $T(K)$ , where  $K$  runs over the  $r_1$  clusters of  $(A, h)$ . From our earlier observations, it follows that each edge of  $T$  is a vertex of  $\mathcal{G}_h$ ; consequently, we have  $|V(\mathcal{G}_h)| \geq |T|$ .

To bound  $|T|$  from below, we first deal with non-boundary clusters.

**Claim 4.11.** *For a non-boundary cluster  $K$  of  $(A, h)$  composed of the images of the non-boundary quasiblocks  $\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m$ , we have  $|T(K)| \geq 4 + (m - 1)$ .*

*Proof.* It immediately follows from the fact that  $K$  corresponds to a connected component of size  $m$  in the cluster graph of  $(A, h)$  that  $|S(K)| \geq m - 1$ . Since the external boundary of a non-empty subset of the square lattice contains at least four edges, it follows that  $|\partial_e K| \geq 4$ . The claim follows since  $S(K)$  and  $\partial_e K$  are disjoint.  $\square$

Next, we have the following estimate for the boundary cluster.

**Claim 4.12.** *If the boundary cluster  $K$  of  $(A, h)$  is composed of the images the boundary quasiblock  $\hat{X}$  and non-boundary quasiblocks  $\hat{X}_1, \hat{X}_2, \dots, \hat{X}_m$ , then  $|T(K)| \geq 6 + (m - 1)$ .*

*Proof.* As before, it is clear that  $|S(K)| \geq m - 1$ . We claim that  $|\partial_i h(\hat{X})| \geq 6$ . To see this, consider the connected component  $X$  of  $D([-k, k]^2, A)$  containing the vertex boundary of  $[-k, k]^2$ . Writing  $X' = [-k, k]^2 \setminus X$ , note we must have  $|X'| \geq 2$ , for if not, then  $A$  must consist of precisely the four edges incident either to  $(0, 0)$  or one of its four neighbours. Note also that  $\partial_e X' \subset \partial_i X$ . Now since  $X'$  contains at least two vertices, it is easily verified that  $\partial_e X'$  contains at least six edges; consequently  $|\partial_i h(\hat{X})| = |\partial_i \hat{X}| = |\partial_i X| \geq 6$ . The claim follows since  $S(K)$  and  $\partial_i h(\hat{X})$  are disjoint.  $\square$

By summing the bound from Claim 4.11 over the  $r_1 - 1$  non-boundary clusters of  $(A, h)$  and then adding the bound from Claim 4.12, we obtain

$$|T| \geq 4(r_1 - 1) + 6 + (r_2 - 1) = 4r_1 + r_2 + 1.$$

We know from Proposition 4.2 that  $\gamma(h) \geq |V(\mathcal{G}_h)|/2 \geq |T|/2$ , so it follows from the above bound that  $\gamma(h) \geq 2r_1 + r_2/2 + 1/2$ .  $\square$

**4.6. Proof of the main lemma.** We are now in a position to prove Lemma 4.3.

*Proof of Lemma 4.3.* We shall show for any  $v \in [n]^2$ , using a union bound over all  $v$ -templates, that the probability that there exists a  $v$ -template that is feasible for  $J = J(n, q)$  is  $o(n^{-2})$  when  $q \geq 10^{40}n$ ; the lemma then follows from a union bound over the elements of  $[n]^2$ .

Fix a vertex  $v \in [n]^2$ . Let  $E_l$  denote the event that there exists a large  $v$ -template that is feasible for  $J$ , and let  $E_s$  denote the event that there exists a small  $v$ -template that is feasible for  $J$ .

First, we bound  $\mathbb{P}(E_l)$  as follows. Consider the event  $E_l(\delta, r_1, r_2)$  that there exists a large  $v$ -template of type  $(\delta, r_1, r_2)$  that is feasible for  $J$ . Of course, Proposition 4.6 implies that  $\mathbb{P}(E_l(\delta, r_1, r_2)) = 0$  either if  $\delta < 8k + 4$  or if  $\delta < r_1 + r_2$ . Otherwise, from



Propositions 4.6 and 4.7 and the fact that  $k = \lceil \log n \rceil$ , we see that

$$\begin{aligned}\mathbb{P}(E_l(\delta, r_1, r_2)) &= O\left(\frac{30^\delta n^{2r_1} k^{6r_2}}{n^2 100^\delta n^{2r_1+r_2/2-2r_1/(2k+1)}}\right) = O\left(\frac{30^\delta n^{2r_1/(2k+1)}}{n^2 100^\delta}\right) \\ &= O\left(\frac{e^{r_1}}{n^2 3^\delta}\right) = O\left(\frac{e^\delta}{n^2 3^\delta}\right) = O\left(\frac{(e/3)^{\log n}}{n^2}\right) = O(n^{-1-\log 3}).\end{aligned}$$

Now, since  $1 + \log 3 > 2$  and  $k = \lceil \log n \rceil$ , we deduce from the above estimate that

$$\mathbb{P}(E_l) = \sum_{\delta=1}^{4(2k+1)^2} \sum_{r_1=1}^{(2k+1)^2} \sum_{r_2=1}^{(2k+1)^2} \mathbb{P}(E_l(\delta, r_1, r_2)) = O(4(2k+1)^6 n^{-1-\log 3}) = o(n^{-2}).$$

Next, we bound  $\mathbb{P}(E_s)$  as follows. Consider the event  $E_s(\delta, r_1, r_2)$  that there exists a small  $v$ -template of type  $(\delta, r_1, r_2)$  that is feasible for  $J$ . From Propositions 4.9 and 4.10 and the fact that  $k = \lceil \log n \rceil$ , we see that

$$\mathbb{P}(E_s(\delta, r_1, r_2)) = O\left(\frac{30^\delta n^{2r_1} k^{6r_2}}{n^2 10^{20\delta} n^{2r_1+r_2/2+1/2}}\right) = O\left(\frac{30^\delta}{n^{2+1/2} 100^\delta}\right) = O(n^{-2-1/2}).$$

As before, since  $k = \lceil \log n \rceil$ , we deduce from the above estimate that

$$\mathbb{P}(E_s) = \sum_{\delta=1}^{4(2k+1)^2} \sum_{r_1=1}^{(2k+1)^2} \sum_{r_2=1}^{(2k+1)^2} \mathbb{P}(E_s(\delta, r_1, r_2)) = O(4(2k+1)^6 n^{-2-1/2}) = o(n^{-2}).$$

It follows that the probability that there exists  $v$ -template that is feasible for  $J$  is  $o(n^{-2})$ ; the lemma follows from a union bound over the vertices of the grid.  $\square$

## 5. PROOF OF THE 1-STATEMENT

In this section, we prove the 1-statement in Theorem 1.2. We proceed roughly as in [4] by first assembling the ‘central bulk’ of a random jigsaw using Lemma 4.3, and then extending this assembly to the ‘periphery’ in a fairly straightforward fashion; our arguments will however require a bit more work than the one in [4] since we have fewer colours to work with.

*Proof of the 1-statement in Theorem 1.2.* Suppose that  $q \geq 10^{40}n$ , let  $J = J(n, q)$  and, as in Section 4, let  $k = \lceil \log n \rceil$ . To prove the 1-statement, we shall describe an algorithm that reconstructs  $J$  from its deck  $D(J)$  with high probability.

We begin by addressing the possibility of tiles occurring with multiplicity greater than one in  $D(J)$ . Let  $X_1$  denote the number of pairs  $(u, v) \in ([n]^2)^2$  with  $J_u = J_v$ , and let  $X_2$  denote the number of pairs  $(u, v) \in ([n]^2)^2$  with  $J_u = J_v$  such that  $u$  and  $v$  are additionally at distance at most two from each other. We then observe the following.

**Claim 5.1.**  $\mathbb{E}[X_1] \leq 1$  and  $\mathbb{E}[X_2] = o(1)$ .

*Proof.* The claim follows immediately from noting that  $\mathbb{E}[X_1] = n^4 q^{-4}$  and that  $\mathbb{E}[X_2] = O(n^2 q^{-4})$ .  $\square$

Let us now record some properties that are possessed by  $J$  with high probability.

- (A) There exist no non-trivial  $v$ -windows with respect to  $J$  for any  $v \in [n]^2$ ; this follows from Lemma 4.3.
- (B) The number of vertices  $v \in [n]^2$  such that the tile  $J_v$  has multiplicity greater than one in  $D(J)$  is at most  $\log n$ ; this follows from Claim 5.1 and Markov's inequality.
- (C) If  $J_u = J_v$  for some  $u, v \in [n]^2$ , then the distance between  $u$  and  $v$  is at least three; this again follows from Claim 5.1 and Markov's inequality.

We first show how one may reconstruct a large subgrid of  $J$  from  $D(J)$  with high probability; we do this by showing how one may perform this reconstruction assuming that  $J$  satisfies ((A)), ((B)) and ((C)). To this end, we proceed by building a labelled, directed graph  $H$  on  $D(J)$  to encode the relative positions of the tiles in the jigsaw. In what follows, a component of the directed graph  $H$  will mean a connected component of the underlying undirected graph.

First, we consider every tile  $t \in D(J)$  which occurs in the deck with multiplicity one. For such a tile  $t$ , we consider all possible subsets of  $(2k+1)^2$  tiles that include  $t$ , and for each such set, we consider all possible arrangements of this set of tiles on the grid  $[-k, k]^2$  with  $t$  being placed at  $(0, 0)$ . Finally, for each such arrangement that is feasible, we record the tuple  $(t, t_1, t_2, t_3, t_4)$ , where  $t_i$  is the tile placed at  $e_i$  in this arrangement for  $1 \leq i \leq 4$ . Now, for each recorded tuple  $(t, t_1, t_2, t_3, t_4)$ , we add an edge directed from  $t$  to  $t_i$  labelled  $e_i$  in  $H$  if the tile  $t_i$  also occurs with multiplicity one in the deck.

It follows from ((A)) that if there exists a directed edge from a tile  $t$  to a tile  $t'$  labelled  $e_i$  in  $H$ , then it must be the case that  $t = J_v$  and  $t' = J_{v'}$ , where  $v, v' \in [n]^2$  are vertices such that  $v' = v + e_i$ . Consequently, each component of  $H$  describes the relative positions of the tiles in that component in  $J$ ; in other words, for any two tiles  $t = J_v$  and  $t' = J_{v'}$  that belong to the same component in  $H$ , we may determine  $v - v'$  using  $H$ .

From ((C)) and Proposition 2.3, we deduce that the tiles of  $J$  coming from the central  $(n - 2k) \times (n - 2k)$  subgrid of  $[n]^2$  which furthermore appear with multiplicity one in  $D(J)$  all belong to the same component of  $H$ ; it follows from ((B)) that this component contains at least  $(n - 2k)^2 - \log n > n^2/2$  tiles, and is consequently the unique largest component of  $H$ .

Next, we fill in the 'holes' in the largest component of  $H$  as follows. We know that we may determine, up to translation, the positions on the square lattice of all the tiles in a given component of  $H$ ; we fix an arrangement of the tiles in the largest component by placing one of these tiles at the origin and the other tiles at their appropriate positions

relative to the origin. Suppose that there is no tile at some position  $x \in \mathbb{Z}^2$  in this arrangement, but that there is a tile at each of the four positions neighbouring  $x$ . Now, the tiles in the positions neighbouring  $x$  uniquely determine the missing tile at  $x$ , and since all pairs of adjacent tiles in  $H$  come from adjacent positions in  $[n]^2$ , it follows that such a missing tile must be an isolated vertex of  $H$ . Once we add each such missing tile to the largest component of  $H$  (by adding in the appropriately labelled directed edges), it follows from ((C)) that the largest component of  $H$  contains each tile of  $J$  coming from the central  $(n - 2k - 2) \times (n - 2k - 2)$  subgrid of  $[n]^2$ . Let  $S_H$  denote the largest square subgrid contained in the largest connected component of  $H$  at this juncture; we know from the above discussion that with high probability,  $S_H$  is a fully-assembled  $s \times s$  subgrid of  $J$  with  $s \geq n - 2k - 2$ .

We now finish the proof by showing that  $J$  has the following property with high probability: given any fully-assembled  $m \times m$  subgrid  $M$  of  $J$  with  $m \geq n - 2k - 2$ , there is a unique way to assemble the tiles not in  $M$  around  $M$  to produce a feasible assembly of tiles on an  $n \times n$  grid; of course, this final assembly of tiles must then coincide with  $J$ .

Let us now describe an extension procedure that, with high probability, extends a given large fully-assembled subgrid  $M$  uniquely to  $J$  using the tiles not in  $M$ . This extension procedure will proceed by repeatedly extending  $M$ , first upwards, then downwards, then to the left and finally to the right, adding an entire row or column of tiles at each step (thus ensuring that  $M$  remains a subgrid at each stage). Suppose first that we wish to add a row of tiles to the top of  $M$ . Let  $M'$  denote the set of tiles  $t$  in the top row of  $M$  not located at one of the two corners, and let  $M''$  denote the set of two tiles at the top corners of  $M$ . For each  $t \in M'$ , we record all triples  $(t', t'_l, t'_r)$  of tiles from the deck (not already in  $M$ ) such that we may feasibly place  $t'$  above  $t$ ,  $t'_l$  to the immediate left of  $t'$ , and  $t'_r$  to the immediate right of  $t'$ . We then proceed as follows.

- (1) If no such feasible triple of tiles  $(t', t'_l, t'_r)$  exists for some tile  $t \in M'$ , then we stop attempting to extend  $M$  upwards and change directions.
- (2) If there exist two distinct choices for the tile  $t'$  over all recorded feasible triples  $(t', t'_l, t'_r)$  for some tile  $t \in M'$ , then we abort.
- (3) If there exists a single choice for  $t'$  (though potentially more than one choice for  $t'_l$  and  $t'_r$ ) over all recorded feasible triples for each tile  $t \in M'$ , then we add a new row of tiles to the top of  $M$  by first placing  $t'$  above  $t$  for each tile  $t \in M'$ . We then check if there exists a unique way to place two tiles (that are not already in  $M$ ) feasibly above the two tiles in  $M''$ , and if so, we finish adding a new row to the top of  $M$  by placing these two tiles in place; if we either cannot find such a pair of tiles, or if multiple choices exist for this pair, then we again abort.

Assuming that we have not aborted at any stage, we then continue to add rows to the top of  $M$  until we are forced to change directions, and we then similarly extend  $M$  downwards, to the left and finally to the right.

To bound the probability that this extension procedure fails to uniquely reconstruct  $J$  from some large fully-assembled subgrid, we need to define two events. It will be convenient to first have some notation. Let  $B_1 \subset [n]^2$  denote the set of vertices not contained in the central  $(n - 4k - 4) \times (n - 4k - 4)$  subgrid of  $[n]^2$ , and let  $B_2 \subset B_1$  denote the set of vertices in the four  $(2k + 2) \times (2k + 2)$  subgrids at the four corners of  $B_1$ .

We first address the possibility of ‘failing in a corner’ when extending a large subgrid. Let  $E_1$  denote the event that there exists a pair  $(u, v)$  with  $u \in B_2$  and  $v \in B_1$  such that some two edges incident to  $u$  receive the same two colours under  $J$  as some two edges incident to  $v$ . We then have the following estimate.

**Claim 5.2.**  $\mathbb{P}(E_1) = o(1)$ .

*Proof.* Let  $Y_1$  denote the number of pairs  $(u, v)$  which satisfy the conditions of the event  $E_1$ . It is easy to see that

$$\mathbb{E}[Y_1] = O(nk^3q^{-2} + k^2q^{-1}) = o(1);$$

the claim follows from Markov’s inequality.  $\square$

Next, we address the possibility of ‘failing in the bulk of a row or column’ when extending a large subgrid. Let  $E_2$  denote the event that there exists a quadruple  $(u, v, v', v'')$ , where  $u, v, v', v'' \in B_1$  and  $u$  is not one of the four corners of  $[n]^2$ , such that either  $v \neq u + e_1$  and the map  $f: [-1, 1] \times [0, 1] \rightarrow [n]^2$  defined by  $f(-1, 0) = u + e_4$ ,  $f(0, 0) = u$ ,  $f(1, 0) = u + e_2$ ,  $f(-1, 1) = v'$ ,  $f(0, 1) = v$  and  $f(1, 1) = v''$  is feasible for  $J$ , or such that the quadruple satisfies an analogous condition with respect to one of the three other directions. We then have the following estimate.

**Claim 5.3.**  $\mathbb{P}(E_2) = o(1)$ .

*Proof.* Let  $Y_2$  denote the number of quadruples  $(u, v, v', v'')$  which satisfy the conditions of the event  $E_2$ . We may verify (after a somewhat tedious case analysis) that

$$\mathbb{E}[Y_2] = O((nk)^4q^{-5} + (nk)^3q^{-4} + (nk)^2q^{-3}) = o(1);$$

the claim follows from Markov’s inequality.  $\square$

If neither  $E_1$  nor  $E_2$  occurs, then it is easily seen by induction that our extension procedure extends any fully assembled  $m \times m$  subgrid  $M$  with  $m \geq n - 2k - 2$  uniquely to  $J$  using the tiles not already in  $M$ . It follows that we may extend  $S_H$  uniquely to  $J$  with high probability, proving the theorem.  $\square$

## 6. CONCLUSION

We conclude by reminding the reader of Conjecture 1.3 which asserts that the answer to the question of whether  $J(n, q)$  is reconstructible exhibits a sharp transition at  $q \approx n/\sqrt{e}$ . Here, we have established the 0-statement in Conjecture 1.3 using a simple counting argument. We have also proved the 1-statement in this conjecture for all  $q \geq Cn$ , where  $C > 0$  is some absolute constant. As mentioned earlier, it is possible to use our methods to show that we may actually take  $C$  as above to be any constant strictly greater than 1: roughly speaking, our estimates for the number of templates in the ‘small edge boundary’ regime are very crude, and it is possible to do significantly better in this regime using stability results (see [5], for example) for the isoperimetric inequality in  $\mathbb{Z}^2$ . However, showing that we may actually take  $C$  as above to be any constant strictly greater than  $1/\sqrt{e}$  appears to be completely out of the reach of our methods; we expect new ideas will be required to settle this problem.

Of course, one could also ask for the size of the window in the sharp transition predicted by Conjecture 1.3. By repeating the proof of the 0-statement of Theorem 1.3 with more careful estimates, we are led to the following refinement of Conjecture 1.3 whose 0-statement again follows from our counting argument.

**Conjecture 6.1.** *Let  $q = q(n) = n/\sqrt{e} + \log n + \alpha(n)$ . As  $n \rightarrow \infty$ , we have*

$$\mathbb{P}(J(n, q) \text{ is reconstructible}) \rightarrow \begin{cases} 1 & \text{if } \alpha(n) \rightarrow \infty, \text{ and} \\ 0 & \text{if } \alpha(n) \rightarrow -\infty. \end{cases}$$

Finally, it would be of interest to investigate higher-dimensional analogues of the problem considered here. For example, it would be interesting to decide if the analogous  $d$ -dimensional problem of reconstructing a random  $q$ -colouring of (the edges of)  $[n]^d$  from its deck exhibits a sharp threshold at  $q \approx n/e^{1/d}$  for each  $d \geq 3$ .

## ACKNOWLEDGEMENTS

The first and second authors were partially supported by NSF grant DMS-1600742, and the second author also wishes to acknowledge support from EU MULTIPLEX grant 317532. Some of the research in this paper was carried out while the first author was visiting the Isaac Newton Institute for Mathematical Sciences at the University of Cambridge; the first author is grateful for the hospitality of the Institute.

## NOTE ADDED IN PROOF

After we proved the results here (in November 2016), but before we finished writing this paper, Martinsson [8], working independently, also announced (in January 2017) a proof of a result analogous to Theorem 1.2 in a very closely related model (and with

a more reasonable constant in the 1-statement). We briefly point out that while the respective 0-statements are established in essentially the same fashion both here and in [8], the estimates needed to prove the respective 1-statements are established by rather different approaches.

## REFERENCES

1. N. Alon, Y. Caro, I. Krasikov, and Y. Roditty, *Combinatorial reconstruction problems*, J. Combin. Theory Ser. B **47** (1989), 153–161. [1](#)
2. B. Bollobás, *Almost every graph has reconstruction number three*, J. Graph Theory **14** (1990), 1–4. [1](#)
3. ———, *The art of mathematics: Coffee time in memphis*, Cambridge University Press, Cambridge, 2006. [10](#)
4. C. Bordenave, U. Feige, and E. Mossel, *Shotgun assembly of random jigsaw puzzles*, Preprint, arXiv:1605.03086. [3](#), [6](#), [7](#), [16](#)
5. D. Ellis, E. Friedgut, G. Kindler, and A. Yehudayoff, *Geometric stability via information theory*, Discrete Anal. (2016), Paper No. 10, 29. [20](#)
6. F. Harary, *On the reconstruction of a graph from a collection of subgraphs*, Theory of Graphs and its Applications (Proc. Sympos. Smolenice, 1963), Publ. House Czechoslovak Acad. Sci., Prague, 1964, pp. 47–52. [1](#)
7. P. J. Kelly, *A congruence theorem for trees*, Pacific J. Math. **7** (1957), 961–968. [1](#)
8. A. Martinsson, *A linear threshold for uniqueness of solutions to random jigsaw puzzles*, Preprint, arXiv:1701.04813. [20](#), [21](#)
9. E. Mossel and N. Ross, *Shotgun assembly of labeled graphs*, IEEE Trans. Network Sci. Eng., To appear. [3](#)
10. R. Nenadov, P. Pfister, and A. Steger, *Unique reconstruction threshold for random jigsaw puzzles*, Preprint, arXiv:1605.03043. [3](#)
11. L. Pebody, *The reconstructibility of finite abelian groups*, Combin. Probab. Comput. **13** (2004), 867–892. [1](#)
12. ———, *Reconstructing odd necklaces*, Combin. Probab. Comput. **16** (2007), 503–514. [1](#)
13. L. Pebody, A. J. Radcliffe, and A. D. Scott, *Finite subsets of the plane are 18-reconstructible*, SIAM J. Discrete Math. **16** (2003), 262–275. [1](#)
14. A. J. Radcliffe and A. D. Scott, *Reconstructing subsets of  $Z_n$* , J. Combin. Theory Ser. A **83** (1998), 169–187. [1](#)
15. S. M. Ulam, *A collection of mathematical problems*, Interscience Tracts in Pure and Applied Mathematics, Interscience Publishers, New York-London, 1960. [1](#)

DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF MEMPHIS, MEMPHIS TN 38152, USA

*Email address:* pbalistr@memphis.edu

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS, UNIVERSITY OF CAMBRIDGE, WILBERFORCE ROAD, CAMBRIDGE CB3 0WB, UK, *and* DEPARTMENT OF MATHEMATICAL SCIENCES, UNIVERSITY OF MEMPHIS, MEMPHIS TN 38152, USA, *and* LONDON INSTITUTE FOR MATHEMATICAL SCIENCES, 35A SOUTH ST., MAYFAIR, LONDON W1K 2XF, UK

*Email address:* b.bollobas@dpms.cam.ac.uk

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS, UNIVERSITY OF CAMBRIDGE, WILBERFORCE ROAD, CAMBRIDGE CB3 0WB, UK

*Email address:* b.p.narayanan@dpms.cam.ac.uk