arXiv:2301.11019v1 [math.CO] 26 Jan 2023

从两两距离的随机子集中重构点集

António Girão† Freddie Illingworth† Lukas Michel†Emil Powierski† 亚历克斯·斯科特†

摘要

设V是实数轴上的n个点组成的集合。假设每一对点的两两距离都以p的概率独立地已知。点集V有多少部分可以在等距变换意义下重构?

我们证明，$p = (\log n)/n$是重构整个V的尖锐阈值，这改进了 Benjamini 和 Tzalik 的一项结果。该结论源于一个关于随机过程的命中时刻结果：在这一过程中，两两距离按均匀随机的顺序逐一揭示。我们还证明，$1/n$是重构V中线性比例部分的弱阈值。

1 引言

设 V $\subset \mathbb{R}^1$ 是实数轴上的一个有限点集，并假设我们所知道的仅是其中某些点对 $\mathcal{P} \subset \binom{V}{2}$ 之间的距离。更确切地说，将这些点标记为 $v_1, \ldots, v_n$，若点对 $v_i v_j \in \mathcal{P}$，则 v_i 与 v_j 之间的距离为 [1]。我们能重构 V 的多少部分？能否重构整个 V？重构集合 U $\subseteq$ V，意味着在等距变换意义下推断 U 中带标记点的位置；等价地说，就是推断 U 中所有点的两两距离。本文考虑这样一种情形：每一对点的距离都以概率 p 独立地为已知，即 (V, $\mathcal{P}$) 服从 Erd˝os–Rényi 二项随机图$\mathcal{G}$(n, p) 的分布。

Benjamini 和 Tzalik [BT22] 最近证明了以下结果。

定理 1.1 (Benjamini 和 Tzalik [BT22])。 设 V 是实数轴上的 n 个点组成的集合。存在一个充分大的常数 C，使得若已知两两距离构成的图 $G(V, \mathcal{P})$ 服从分布 $\mathcal{G}(n,p)$，其中 $p = C\log(n)/n$，则以高概率（ whp ）可以重构整个 V。

2020 年数学学科分类：05C80（随机图）

†英国牛津大学数学研究所（{girao,illingworth,michel,powierski,scott}@maths.ox.ac.uk）。AG、FI 和 AS 的研究由英国工程与自然科学研究委员会资助，项目编号 EP/V007327/1。[1] 关于点未标识、仅给出两两距离多重集的问题也已有研究，参见 [ACKR89、PRS03]。通常，仅凭这些信息不足以重构点集，因为$A + B$和$A - B$无法区分。不过，维度至多为二的点集可以从大小为常数的子集中重构。

我们强化了这一结果。我们的首个结果确定了随着 p 增大，最大可重构集合演变过程中的两个重要转折点。我们通过证明重构整个 V的尖锐阈值结果，改进了定理 1.1 ；此外，我们还确定了重构 V的正比例所对应的阈值。

定理 1.2. 设 V 是实数轴上的 n 个点构成的集合。假设已知两两距离的图 $G(V, \mathcal{P})$服从 $\mathcal{G}(n, p)$。那么以下结论以高概率成立。

a. 若 $p \geqslant 42/n$，则存在一个大小为$\Omega(n)$的可重构集合。*b.* 若 $pn \to \infty$，则存在一个大小为$(1-o(1))n$ 的可重构集合。*c.* 若 $p \leqslant \log n+\log\log n-\omega(1)$ n，则无法~~重构 V 的全部点~~。*d.* 若 $p \geqslant \log n+\log\log n+\omega(1)$ n，则可以重构 V 的全部点。

除 a 部分的常数因子外，这些结果都是最佳的a[2]。事实上，当$p = c/n$且常数$c < 1$时，G 中最大连通分量的大小为 $\mathcal{O}(\log n)$。当$p = c/n$ 且常数$c > 1$时，以高概率，G 的最大连通分量是一个巨型分量，其大小至多为某个常数dn 。

定理 1.2 的最后两部分可由一个更强的击中时刻结果推出。假设两两距离按随机顺序逐一揭示：换言之，已知两两距离图遵循随机图过程（G_t: $0 \leqslant t \leqslant \binom{n}{2}$）。我们将证明，当 G_t 的最小度至少为二时，V 以高概率可重构。不过，V 也可能在此之前不久就已可重构。如果某个点 u 恰好关联一个已揭示距离，那么相对于它的邻点，u 有两个可能的位置；但这两个可能位置之一可能已经被占据，因此实际上 u 可以被重构。为此，若不同点的有序对 (u, v) 满足 $w = 2v - u$（即 u 关于 v 的反射）也属于 V，我们就称该有序对是安全的。

定理 1.3。 设 V 是实数轴上的 n 个点构成的集合。假设 V 中各点对之间的距离按均匀随机顺序逐一揭示。那么，V 以高概率恰好在以下两个条件首次同时满足时可重构。

- 每个点都至少关联一条已揭示距离。
- 若点 u 恰好关联一条已揭示距离，且该距离连接到点 v，则(u, v) 是安全的。

由此可知，如果每个点都至少关联两条已揭示距离，那么以高概率，整个V 都是可重构的。事实上，当且仅当$o(n^2)$ 安全点对位于V中时，这一时刻以高概率就是完全可重构性的命中时刻。这是因为，关联到最后一个仅有一条已揭示距离的点的那条唯一距离，在$\binom{V}{2}$中均匀随机分布。一个含有$\Omega(n^2)$ 个安全点对的集合示例是$V = \{1, 2, \ldots, n\}$。反过来，我们将证明（定理 3.4），如果有 $\omega(1)$ 个点仅关联一条已揭示距离，那么以高概率，整个V 都不可重构。

还可以得到一个算法命中时间结果，无需了解底层点集V ，即可确定V 整体何时可重构。

定理1.4。 存在一种关于 n 的多项式期望运行时间的在线算法

[2]我们在部分a中并未对值 42 进行优化：简短的计算表明，我们的方法最多只能得到 9，而我们认为正确的阈值是 $1+\varepsilon$（参见第 4 节以了解更多讨论）。

该算法逐一获取已揭示距离，并以高概率识别出 V 首次可重构的时刻，并将其重构。

可重构性与图刚性密切相关；图刚性研究图在 $\mathbb{R}^d$中的一般嵌入。顶点集V 在 $\mathbb{R}^d$ 中的嵌入称为一般嵌入，如果其顶点的$d|V|$ 坐标集合在有理数域上代数独立。若一个图在中全局刚性 $\mathbb{R}^d$，则它在 $\mathbb{R}^d$ 中存在某种一般嵌入，且可根据其边长重构。事实上，一个图全局刚性，当且仅当它的所有一般嵌入都能根据其边长重构 [Con05，GHT10]。

随机图在 $\mathbb{R}^d$ 中的（全局）刚性已得到广泛研究，相关工作既考察整个图何时具有（全局）刚性 [JSS07, KT13, JT22]，也研究其何时拥有线性规模的刚性分量 [KMT11, BLM18]。Lew、Nevo、Peled 和 Raz [LNPR22] 最近给出了一个击中时刻结果：$\mathbb{R}^d$ 中的随机图过程恰好在最小度达到 $d+1$时变为全局刚性。由于一般嵌入中不存在安全点对，这意味着定理 1.3 对一般嵌入成立。然而，全局刚性的定义局限于一般嵌入，这一限制大大削弱了该概念。例如，众所周知（见 [JW17, 定理 63.2.7]），图在 $\mathbb{R}$ 中全局刚性，当且仅当它是二连通的；但对于任意点集的重构，情况则大不相同。事实上，我们证明，存在连通度任意高的图，它们可以嵌入 $\mathbb{R}$，使得其顶点集无法根据其边长重构。这推翻了 Benjamini 和 Tzalik 的一个猜想 [BT22]。

定理1.5。 设 k 为正整数。存在顶点数任意多的 k-连通图，它们可以嵌入实数轴，使得顶点的最大可重构子集大小为 k。

证明。固定正整数 k，并令 $n = \ell k$ 为 k 的任意倍数。设 $C_1, \dots, C_\ell$ beℓ 为互不相交的 k-团。记 $C_i = \{a_1^{(i)}, \dots, a^{(i)}k\}$。令 G 为由 $C_1, \dots, C_\ell$ 的并通过添加匹配 $\{a_1^{(i)} a_1^{(i+1)}, a_2^{(i)} a_2^{(i+1)}, \dots, a^{(i)}k\, a^{(i+1)}k\}$ 而得到的图，其中对于每个 $i = 1, \dots, \ell - 1$，这些匹配连接 C_i 和 C_{i+1}。注意，G 是 K_k 和 P_ℓ 的笛卡尔积，因此显然是 k-连通的。

嵌入 C_i，使得 $a_1^{(i)}, \dots, a^{(i)}k$ 按此顺序构成 k个连续整数，也就是说，$|a_s^{(i)} - a^{(i)}t| = |s - t|$。我们规定每条边 $a_s^{(i)}a_s^{(i+1)}$的长度为 k^i。显然，可以将每个 $a_s^{(i)}$放置在 $k^{i-1} + k^{i-2} + \cdots + k + $处，从而实现这样的嵌入。此外，将 $C_1, \dots, C_i$ 放置在这些点之后，$C_{i+1}, \dots, C_\ell$的位置有多种选择：可以放在 C_i 的右侧，也可以放在 C_1的左侧。特别地，任何大小至少为 $k+1$ 的顶点子集都包含来自至少两个不同 C_i 的顶点，因此不可重构。

□

本文其余部分安排如下。我们将在a 和b 两部分中定理 1.2的第2节中证明。我们将在定理1.2的其余部分以及定理1.3和1.4 中证明，见第3节。最后，我们将在第 4 节讨论一些开放问题。

全文中，我们使用标准的渐近记号，并假设n 足够大。

2 重构线性比例的点 s

本节中，我们证明定理 1.2的a和b两部分。取V 为实数轴上n 个点组成的集合。我们通过短环来重构V 的一段线性部分。首先，我们证明，对于大多数短环C ，若其顶点属于V，且C 的边对应的距离均已揭示，那么C 的顶点便可在等距变换意义下重构。这是因为，若一个短环在实数轴上存在多种可能的嵌入，就会导致环上相邻点之间的两两距离出现一个较小的“线性相关”关系。我们将在第 2.1 节证明，这种线性相关只会出现在少数短环中。

接下来，在第 2.2 节中，我们假设每个两两距离都以概率$p = 42/n$独立地已知。注意，随机图$G \sim \mathcal{G}(n, 42/n)$ 通常会有$\Omega(n^2)$ 对顶点包含在短环中。由于大多数短环都可以重构，我们可以重构$\Omega(n^2)$ 对点之间的距离。这使我们能够应用 Benjamini 和 Tzalik 的以下极值结果 [BT22] ，重构所有点的线性比例，从而证明第a部分。

定理 2.1 (Benjamini 和 Tzalik [BT22])。设 V 是实数轴上由 n 个点组成的集合。假设已知两两距离的集合 $\mathcal{P}$ 的大小大于$40n^{3/2}$。那么存在一个由$\Omega(|\mathcal{P}|/n)$ 个点组成的集合，这些点可以被重构。

最后，为了得到b部分，我们从已经重构的所有点的这一线性比例开始。然后，通过增大p 并加入一些额外的边，我们会发现，对于大多数点，我们至少知道它们到已重构集合的两个距离，因此也能重构这些点。

2.1 嵌入中的可重构元组

在本节中，我们将证明，如果短环的边是已揭示距离，那么大多数短环都可以重构。为此，我们给出以下定义。

定义 2.2。若给定两两距离 $|v_2 - v_1|, \ldots, |v_k - v_{k-1}|$和 $|v_1 - v_k|$，就能在等距变换意义下重构 $\{v_1, \ldots, v_k\}$ ，则 V 中由不同点组成的元组 $T = (v_1, v_2, \ldots, v_k)$ 称为可由循环重构。

考虑某个k元组$T = (v_1, v_2, \ldots, v_k)$ ，并令$d_1 = |v_2 - v_1|, \ldots, d_{k-1} = |v_k - v_{k-1}|$和$d_k = |v_1 - v_k|$。显然，存在一些 $\varepsilon_1, \ldots, \varepsilon_{k-1} \in \{-1, 1\}$ ，使得

$$\sum_{i=1}^{k-1} \varepsilon_i d_i = d_k. \tag{1}$$

如果 T 不能由循环重构，那么至少存在两个 $(\varepsilon_1, \ldots, \varepsilon_{k-1}) \in \{-1, 1\}^{k-1}$满足（1）。将这两个表达式相减并把结果除以二，可得某个非零向量 $(\gamma_1, \ldots, \gamma_{k-1}) \in \{-1, 0, 1\}^{k-1}$ 满足

$$\sum_{i=1}^{k-1} \gamma_i d_i = 0. \tag{2}$$

这使我们能够对不可由循环重构的k元组的数量给出上界。

引理 2.3。 设 $k \leqslant 0.9\log n$。所有 k 元组中，至多有 $n^{-0.01}$ 的比例不可由循环重构。

证明。均匀随机地从 V 中选取一个由不同点组成的 k 元组 T $=(v_1,v_2,\ldots,v_k)$。令 $d_1 = |v_2 - v_1|,\ldots,$ $d_{k-1} = |v_k - v_{k-1}|$。若存在某个非零向量 $(\gamma_1,\ldots,\gamma_{s-1}) \in \{-1,0,1\}^{s-1}$ 满足 $\sum_{i<s}\gamma_i d_i = d_s$，则称 v $_{s+1}$ 失败（对于 $1 \leqslant s \leqslant k-1$）。根据前面的讨论，如果 T 不可由循环重构，那么某个 v_{s+1} 会失败。

给定 $v_1,\ldots,v_s$，对于至多 3^{s-1} 个 $d_s = |v_{s+1} - v_s|$ 取值，存在一个向量 $(\gamma_1,\ldots,\gamma_{s-1})$ $\in \{-1,0,1\}^{s-1}$ 满足 $d_s = \sum_{i<s}\gamma_i d_i$。每个这样的 d_s 对应 v_{s+1} 的两个可能取值（即 v $_s \pm d_s$）。特别地，由于 $n-s$ 是 v_{s+1}的可能选择数，

$$\mathbb{P}(v_{s+1} \text{ fails}) \leqslant \frac{2\cdot 3^{s-1}}{n-s} \leqslant \frac{3^s}{n},$$

因此，应用并合界，

$$\mathbb{P}(T \text{ not cycle-reconstructible}) \leqslant \sum_{s\leqslant 0.9\log n}\frac{3^s}{n} \leqslant \frac{3^{0.9\log n+1}}{2n} = \frac{3}{2}n^{0.9\log 3-1} \leqslant n^{-0.01}. \quad \square$$

我们称点对 u,v 是 k-坏的，如果包含 $u^{-0.005}$ 和 v 的 k 元组中，有超过的部分不可由循环重构。根据前一个引理可知，点中这样的 k-坏点对只有很少几个。

引理 2.4. 令 $k \leqslant 0.9\log n$。所有点对中，至多有 $n^{-0.005}$ 的部分是 k-坏的。

证明。注意，每个点对都包含在相同数量的 k 元组中——将这个共同值记为 A。令 u、v 为 V 中均匀随机选取的点对，并令 X 表示同时包含 u 和 v 的不可由循环重构的 k 元组数量。我们将对满足以下条件的 (T, {u, v}) 的数量进行双重计数：T 是一个不可由循环重构的 k 元组，且点对 u、v 包含在 T 中。根据引理 2.3，这个数量至多为

$$n^{-0.01}\cdot \text{number of } k\text{-tuples}\cdot\binom{k}{2} = n^{-0.01}\cdot A\binom{n}{2}.$$

另一方面，该数量恰好等于 $\mathbb{E}(X)\cdot\binom{n}{2}$。因此 $\mathbb{E}(X) \leqslant$ 一个$^{-0.01}$。于是，根据马尔可夫不等式，

$$\mathbb{P}(u,v \text{ is } k\text{-bad}) = \mathbb{P}(X > An^{-0.005}) \leqslant \frac{\mathbb{E}(X)}{An^{-0.005}} \leqslant n^{-0.005}. \quad \square$$

如果点对 u、v 对任意 $k \leqslant 0.9\log n$ 都不是 k-坏点对，那么随机短环中包含 u 和 v 的部分，很可能使我们能够重构 u和v之间的距离，其中该随机短环取自$\mathcal{G}(n,p)$。这启发了以下定义。

定义 2.5。 点对 u、v 是 无用的，如果存在某个 $k \leqslant 0.9\log n$，使得点对 u、v 是 k-坏点对。否则 u、v 是 有用的。

Usi结合前面的结果，我们可以给无用点对的数量设定上界。

推论 2.6。 无用点对至多有 $n^{2-0.004}$ 个。

证明。 根据 引理 2.4，无用点对的数量至多为

$$\sum_{k\leqslant 0.9\log n}\text{number of } k\text{-bad pairs} \leqslant (0.9\log n)n^{2-0.005} \leqslant n^{2-0.004}. \quad \square$$

2.2 从 $\mathcal{G}(n,p)$ 中的短环重构

鉴于上一节的结果，证明 $\mathcal{G}(n、p)$ 中的大多数点对都包含在一个短环中将很有帮助。我们将使用以下关于随机图的直接结果。

引理 2.7。 随机图 $G \sim \mathcal{G}(n,42/n)$ 以高概率包含$\Omega(n^2)$ 个点对，这些点对位于长度至多为$0.9\log n$ 的环上。

令 $\mathrm{diam}(G)$ 表示 G 的同一连通分量中两个顶点之间的最大距离。我们将使用 Riordan 和 Wormald 的一项（远为一般的）结果的以下推论 [RW10，定理 1。1]。证明与引理 2.7 类似结论的其他初等方法也存在，但为简洁起见，我们采用这一结果。

引理 2.8。 随机图 $G \sim \mathcal{G}(n,21/n)$ 以高概率满足$\mathrm{diam}(G) \leqslant 0.44\log n$。

引理 2.7 的证明。令 $V = V_1 \cup V_2$，其中 $|V_1| = |V_2| = n/2$。首先揭示 V_1 和 V_2，内部的边，并令 C_1 和 C_2 分别为 $G[V_1]$ 和 $G[V_2]$ 中的最大连通分量。$G[V_1]$ 和 $G[V_2]$ 独立分布为 $\mathcal{G}(n/2, 21/(n/2))$。

关于随机图的标准事实（例如，参见 [Bol01，第 6]章）表明，C_1 和C_2的大小均为$\Omega(n)$，以高概率成立。此外，引理 2.8 意味着，以高概率，C_1 和C_2 的直径至多为 $0.44\log n$。

接下来，我们揭示 V_1 与 V_2 之间的边。固定一个顶点 $v \in C_1$，记 X_v 为示性随机变量，表示事件“v 在 C_2 中有一个邻点”。我们有$\mathbb{P}(X_v = 0) = (1 - 42/n)^{|C_2|} \leqslant e^{-42|C_2|/n}$，其至多为某个常数 $a < 1$。由于对于 $v \in C_1$，变量 X_v 相互独立，根据 Chernoff 不等式，以高概率有 $\sum_v X_v \geqslant (1 - a)|C_1|/2$，因此，集合 A（由 C_1 中在 C_2 中有邻点的顶点组成）的大小至少为 $\Omega(n)$。现在，对于 $A \in$ 中任意一对顶点 u、v，将它们在 C_1，中的最短路径，与它们各自通往顶点 w_u、$w_v \in C_2$，的边，以及 w_u 和 w_v 在 C_2 中的最短路径拼接起来，就得到一个包含 u 和 v 的环，其长度至多为 $0.44 \log n + 0 0.44 \log n + 2 \leqslant 0 0.9 \log n$。

□

回忆一下，$\mathcal{P}$ 是已知距离的集合。如果点 u、v 在 $(V, \mathcal{P})$ 的一个长度至多为 $0.9 \log n$ 的环上，我们就称这对点 u、v 为接近。如果 $|u - v|$ 可以由 $\mathcal{P}$唯一确定，我们就称点对 u、v 是可推导的。注意，如果 $\mathcal{P}$ 中存在一个包含 u 和 v 的可重构环，那么点对 u、v 就是可推导的。有鉴于此，我们对处于短环中、有用但其距离无法确定的点对数量进行界定。

引理 2.9. 如果$(V, \mathcal{P})$服从 $\mathcal{G}(n,p)$ 分布，那么以高概率，接近且有用但不可推导的点对至多有 $n^{2-0.002}$ 对。

证明。 固定一对点$u、v \in V$，并令$k \leqslant 0.9 \log n$。在$(V、\mathcal{P})$ 包含一个含有u 和v的k-环这一事件的条件下，任何特定的、包含u 和v 的k-元组在$(V、\mathcal{P})$ 中作为环出现的概率均匀。如果u、v 是有用的，那么这些k-元组中至多有$n^{-0.005}$ 的比例是不可重构的，因此

$$\mathbb{P}(u, v \text{ not deducible} \mid u, v \text{ in a } k\text{-cycle and useful}) \leqslant n^{-0.005}.$$

这对所有$k \leqslant 0.9 \log n$均成立，因此$\mathbb{P}(u、v$不可推导$\mid u、v$相近且有用$) \leqslant n^{-0.005}$。因此，

$$\mathbb{P}(u, v \text{ close and useful but not deducible}) \leqslant n^{-0.005}.$$

令X表示既接近又有用、但不可推导的点对数量。则$\mathbb{E}(X) \leqslant n^{-0.005} \cdot \binom{n}{2}$。由马尔可夫不等式，

$$\mathbb{P}(X > n^{2-0.002}) \leqslant \frac{\mathbb{E}(X)}{n^{2-0.002}} \leqslant n^{-0.003}. \qquad \square$$

现在我们可以证明定理 1.2的a和b部分。

定理 *1.2a* 的证明。 由引理 2.7，以高概率，$(V, \mathcal{P})$中有 $\Omega(n^2)$ 个相近的点对。在这些相近的点对中，根据推论 2.6 ，至多有$n^{2-0.004}$ 个点对无用；根据引理 2.9，以高概率至多有$n^{2-0.002}$ 个点对有用但不可推导。特别地，以高概率，$(V, \mathcal{P})$ 中至少有 $\Omega(n^2)$个顶点点对可推导。

最后，定理 2.1 意味着，以高概率存在一个包含 $\Omega(n)$ 个顶点的集合，该集合可在等距变换意义下重构。 $\square$

注意，如果我们已经重构了一个点集 S ，并且知道另一个点 v 到 S中某些点的至少两个距离，那么就能唯一确定 v相对于 S的位置，因此我们可以重构 $S \cup \{v\}$。这使我们能够证明 b 部分。

定理 定理 *1.2b* 的证明。 由定理 1.2a，存在常数 $c > 0$ ，使得当$p = 42/n$时，以高概率存在一个至少包含cn 个点的集合R ，这些点可以被重构。令常数$d > c$ ，取$q = d/(cn)$ ，并考虑$G \sim \mathcal{G}(n, q)$。每个顶点$v \notin R$ 都满足

$$\mathbb{P}(|N_G(v) \cap R| < 2) = (1-q)^{|R|} + |R|q(1-q)^{|R|-1} \leqslant 2nq(1-q)^{cn} \leqslant (2d/c)e^{-d}.$$

由于这些事件彼此独立，切尔诺夫界意味着，以高概率，至多有(4d/c)e^{-d}n个点v $\notin$ R在R中至多有一个邻居。由于每个在R中有两个邻居的点也可以相对于R重构，因此，以高概率，在 $\mathcal{G}$(n, p) $\cup \mathcal{G}$(n, q)中可以重构至少(1 −(4d/c)e^{-d})n个点，进而在 $\mathcal{G}$(n, p + q) $\sim$ $\mathcal{G}$(n, ω/n)中也可以重构，其中 $\omega = 42 +$d/c。由于(4d/c)$e^{-d} \to 0$当d $\to \infty$时，这就证明了该结论。 $\square$

3 完全重建的命中时间

本节中，我们证明定理 1.3。为此，我们使用以下随机图的标准耦合。设 $(U_e)_{e \in E(K_n)}$ 是一组相互独立且均匀分布于 $[0,1]$ 的随机变量。对于 p $\in [0,1]$，令 G^p 为 K_n 的子图，其边恰好是满足 $U_e \leqslant$ p 的边 e。注意，G^p 的分布为 $\mathcal{G}$(n, p)；当 p 从 0 连续增至 1 时，G^p 按随机图过程演变，边以均匀随机顺序逐条加入（注意，所有 U_e 互不相同的概率为 1）。我们利用这一过程来模拟以均匀随机顺序逐个揭示 V 中点对之间距离的过程。本节中我们将直接使用以下关于 $\mathcal{G}$(n, p) 的事实（例如参见 [Bol01，第 7] 章）。对于任意正

整数 k：若 p $\leqslant$(log n $+$(k $-$1) log log n $-\omega(1)$)/n，则以高概率 $\mathcal{G}$(n, p) 的最小度至多为 k $-$1；若 p $\geqslant$(log n $+$(k $-$1) log log n $+\omega(1)$)/n，则以高概率 $\mathcal{G}$(n, p) 的最小度至少为 k。

在我们的分析中，以下三个特定的 p 值将起到重要作用。 定理 1.2b 意味着存在某个足够大的常数 ω，使得以高概率存在一个大小至少为 $0.9n$ 的集合 $R \subseteq V$，它可以在 $G_{\omega/n}$中重构。令 $p_1 = \omega/n$。令 $p_2 = p_1 + (0.9 \log n)/n$，且$p_3 = (2 \log n)/n$。注意，以高概率$G_{p_2}$仍包含孤立顶点，因此整个$V$ 尚不可重构。我们将证明整个V 可以在G_{p_3}中重构，因此我们的分析将聚焦于范围 $[p_2,p_3]$。

引理 3.1。 以高概率，对于 G_{p_3} 中的每条边 uv，若 $u,v \not\in R$，则 u,v 中至少有一个顶点在 G_{p_2}中有至少两个邻点属于 R。

证明。首先，揭示 G_{p_1}中的所有边。这确定了 R，而切尔诺夫界意味着以高概率 G_{p_1} 至多有 $2p_1\binom{n}{2} \leqslant \omega n$ 条边。现在，揭示 G_{p_3} 中补集 R 内的边。这以至多 p_3 的概率将每条边独立地加入图 G_{p_1}。因此，切尔诺夫界意味着以高概率，这会向补集 R 中至多添加 $2p_3\binom{n}{2} \leqslant 2n \log n$ 条边，所以 G_{p_3} 在补集 R 中总共至多有 $\omega n + 2n \log n \leqslant 3n \log n =: m$ 条边。

最后，揭示G_{p_2} 中R 与R的补集之间的边。每条这样的边要么已存在于G_{p_1} 中，要么以至少$p := p_2 - p_1 = (0.9 \log n)/n$ 的概率独立地加入图G_{p_1}中。因此，每个点$v \not\in R$ 都满足

$$\begin{aligned}\mathbb{P}(|N_{G_{p_2}}(v) \cap R| < 2) &\leqslant (1-p)^{|R|} + |R|p(1-p)^{|R|-1} \leqslant 2np(1-p)^{|R|} \\ &\leqslant 2np(1-p)^{0.9n} \leqslant (2np)e^{-0.9pn} \leqslant (2\log n)n^{-0.81} \leqslant n^{-0.8}.\end{aligned}$$

由于这些事件在不同点$u,v \not\in R$之间相互独立，因此可得

$$\mathbb{P}(\max(|N_{G_{p_2}}(u) \cap R|, |N_{G_{p_2}}(v) \cap R|) < 2) \leqslant (n^{-0.8})^2 = n^{-1.6}.$$

令X 表示G_{p_3} 中满足以下条件的边uv 的数量：$u,v \not\in R$，且u 和v 在G_{p_2}中各自在R 内至多有一个邻点。由于G_{p_3} 在R的补集中至多有m 条边，因此可得 $\mathbb{E}(X) \leqslant m \cdot n^{-1.6} \leqslant 3n^{-0.6} \log n \leqslant n^{-0.5}$，于是$\mathbb{P}(X \geqslant 1) \leqslant n$。

□

如果一个顶点 v 在一个可重构集合中有两个邻居，那么相对于该集合，v的位置可以被重构。基于此，我们对每个$p \in [0,1]$，定义 R'_p 和 R''_p 如下。

$$\begin{aligned}R'_p &= R \cup \{v \in V : |N_{G_p}(v) \cap R| \geqslant 2\}, \\ R''_p &= R'_p \cup \{v \in V : |N_{G_p}(v) \cap R'_p| \geqslant 2\}.\end{aligned}$$

现在我们汇总一些关于R'_p 和R''_p的重要事实。

引理 3.2。 以下各项均以高概率成立。

a. 对所有 $p \geqslant p_1$, R'_p 和 R''_p 在 G_p 中都是可重构的。*b.* 对所有 $p \in [p_2,p_3]$, , G_p 中的每条边都与 R'_p 中的一个顶点关联。*c.* 对所有 $p \in [p_2,p_3]$, , R''_p 包含 G_p 中所有度至少为二的顶点。

证明。注意到R 在G^{p_1}中是可重构的。对于任意$p \geqslant p_1$, G^p 包含G^{p_1}，因此R 在G^p中是可重构的。R'_p 由R 以及所有在R中至少有两个邻点的顶点组成，因此在G^p中也是可重构的。同理可得R''_p。这就证明了a。

由引理 3.1可知，以高概率，G^{p_3} 中的每条边都至少有一个端点在R'_{p_2}中。现在令$p \in [p_2,p_3]$，并令uv 为G^p的一条边。则uv 是G^{p_3}的一条边。因此，u、v 中至少有一个在$R'_{p_2} \subseteq R'_p$中。这证明了b。

令u 为G^p中一个度至少为二的顶点。由b可知，u 要么在R'_p 中，要么u 的每个邻点都在R'_p中。无论哪种情况，u 都在R''_p 中，这证明了c。 □

现在，以高概率，$\mathcal{G}(n,p_3)$ 的最小度至少为二，因此当耦合中的随机图过程达到最小度为二时，引理 3.2 告诉我们，以高概率，整个V 都可以被重构。定理 1.2d立即成立。

我们称有序点对 (u,v) 在不确定于 G^p ，如果 uv 是与u 关联的唯一一条边，并且点 $w = 2v - u$ 是V 中的一个点，且在 G^p中的度为一。如果对某个$v \in V$，(u,v) 在G^p 中不确定，则称u在G^p中不确定。

引理 3.3。 以高概率，对于所有满足 $p \in [p_2,p_3]$, G^p 的 p，都不存在不确定点。

证明。 设(u,v) 是一个有序点对，使得$w = 2v - u$ 是V中的一个点。若(u,v) 在G^p 中不确定，且满足某个$p \in [p_2,p_3]$,，则存在一个点x，使得边uv 和wx 出现在$G_p \subseteq G^{p_3}$中，但与u 和w 关联的其他所有边都不可能出现在$G_p \supseteq G^{p_2}$中。特别地，我们得到

$$\begin{aligned}\mathbb{P}((u,v) \text{ is uncertain in some } G_p) &\leqslant np_3^2(1-p_2)^{2n-5} \leqslant 2np_3^2(1-p_2)^{2n} \\ &\leqslant (2np_3^2)e^{-2np_2} \leqslant 8(\log n)^2 n^{-1} n^{-1.8} \leqslant n^{-2.5}.\end{aligned}$$

令 X 表示在某个G^p中不确定的点的有序对(u,v) 的数量。由于点的有序对至多有n^2 个，这意味着 $\mathbb{E}(X) \leqslant n^2 \cdot n^{-2.5} = n^{-0.5}$，因此 $\mathbb{P}(X \geqslant 1) \leqslant n^{-0.5}$。

□

我们称点 u 在 G^p 中是不可判定的，如果它在 G^p 中的度为 1，且(u, v) 不安全，其中 v 是 u 的唯一邻点。注意，定理 1.3 指出，以高概率 G^p 可重构，当且仅当它没有孤立点和不可判定点。

定理 1.3 的证明。利用引理 3.2 和引理 3.3，我们知道，对于所有 $p \in [p_2,p_3]$，以下结论均以高概率成立。首先，R''_p 可以在 G^p中重构。其次，G^p 中的每条边都与 R''_p中的一个顶点关联。第三，G^p 中不含不确定点。第四，R''_p 包含 G^p中所有度至少为 2 的顶点。最后，G^{p_2} 含有孤立点，而 G^{p_3} 的最小度至少为 2。

现在，考虑使图G^p 既没有孤立点，也没有不可判定点的最小p。根据最后一个性质，我们知道$p_2 < p \leqslant p_3$。特别地，根据第一个性质，R''_p 可以在G^p 中重构。令u 为R''_p补集中的一个点。由于u 不是孤立点，u 必定有一个唯一邻点v，根据第二个性质，该邻点必定属于R''_p。因此v 已被重构，所以我们知道u 只能位于u 或$w = 2v - u$的位置。

鉴于u 不是不可判定点，(u,v) 必定是安全的，这意味着w 是V中的一个点。由于w 不能是孤立点，且根据第三个性质u 不具有不确定性，因此w 的度至少为二。于是，根据第四个性质，$w \in R''_p$，因此w 已被重构。由此可知，位置w 已被u以外的一个点占据，因此u 相对于其余点只能处于一个可能的位置。这样，我们也可以重构u。由于u 是R''_p补集中的任意点，因此G^p 中的所有点都可以在等距变换意义下重构。

最后请注意，随机图过程里先于G^p 出现的图含有一个孤立点或不可判定点$v \in V$。相对于V 中的其余点，这样的点至少有两个可能位置，因此无法在等距变换意义下确定。因此，G^p 是随机图过程中第一个能够在等距变换意义下重构的图。 □

定理1.4 现在很容易得出，因为我们只需沿用本节和上一节中的证明，即可得到所需的算法。

定理*1.4*的证明。 我们的算法由以下步骤组成。

a. 逐一揭示两两距离，直到已知两两距离图中有 42n 条边。将此图记为 G′。 b. 通过从任意顶点出发并依次选择邻点，枚举 G′中长度不超过 0.9 log n 且不重复边的所有游走。据此找出 G′中长度不超过 0.9 log n 的所有环的列表。 c. 然后检查 G′中长度不超过 0.9 log n 的每个环 $v_1 \dots v_k$。若环上相邻点之间的距离为 $d_1, \dots, d_k$，并且存在唯一的$\varepsilon_1, \dots, \varepsilon_{k-1} \in \{-1, 1\}$ 使得 $\sum^{k-1} i=1 \varepsilon_i d_i = d_k$，那么 v_i与 v^j 之间的距离必定为 $|\sum^{j-1}_{=} l i \varepsilon_l d_l|$。 d. 使用这些新距离，应用定理 2.1 重构一个点集 R（根据 [BT22]中的证明可以得到一个多项式时间算法）。 e. 重构并将每个在 R 中有两个邻点的顶点，以及每个在 R 中有一个邻点且其另一个可能位置已被 R 中某个顶点占据的顶点，加入 R。 f. 继续逐一揭示两两距离。每次添加点 u、v 之间的距离，且 $v \in R$ 而 $u \notin R$ 时，检查 u 在 R 中是否有两个邻点，或者 u 关于 v 的反射是否在 R 中。若出现这两种情况中的任一种，就重构 u 并将其加入 R。

令p 满足G' 在耦合中对应G^p 。根据切尔诺夫界，失败概率随n呈指数级衰减，$42/n < p < 168/n$。当$p < 168/n$时，G^p 中长度至多为 $0.9 \log n$ 且不重复经过边的游走的期望数量至多为

$$\sum_{k \leqslant 0.9 \log n} p^k n^{k+1} < n \sum_{k \leqslant 0.9 \log n} 168^k < n^6,$$

而这类游走的数量最多为 $n^{0.9 \log n}$。因此，G' 中这类游走的期望数量是 n 的多项式，这意味着步骤 b的期望运行时间是n的多项式。还可推出，若X 表示G'中长度至多为 0.9 log$n$ 的环的数量，则 $\mathbb{E}(X)$ 是n的多项式。对于每个长度至多为 0.9 log$n$的环，

最多有 $2^{0.9\log n}$种可能的 $(\varepsilon_1,\dots,\varepsilon_{k-1})$，因此步骤 c 中的每次检查都需要 n的多项式时间，这意味着部分c的运行时间为 X 乘以 n的某个多项式。因此，前三个步骤的期望运行时间是 n的多项式。最后三个步骤可以在多项式时间内完成。

由算法得到的集合 R 必然是可重构的。接下来我们要验证，以高概率 $R = V$ 当且仅当 V 是可重构的。正如定理证明中所示，定理 1.2和 定理 1.3，以高概率，初始集合 R 的大小为$\Omega(n)$，随后我们会将每个度为二，或度为一且不可判定的点都加入 R 。因此，根据 定理 1.3，以高概率，该算法会恰好在能够重构 V 时重构出它。

□

我们已经证明，如果每个点都至少关联两条已知距离，那么以高概率，整个V 都可重构。尽管在某些情况下，整个V 可能在此之前就已可重构，但我们现在将证明，这种情况不会早太多发生。

定理 3.4. 设 $f\colon \mathbb{N}\to\mathbb{R}$是任意一个趋于无穷大的函数。设 V 是实数轴上的一个含有 n 个点的集合。假设 V 中各点对之间的距离按照均匀随机顺序逐一揭示。如果至少有 $f(n)$ 个点仅关联一条已揭示距离，那么以高概率无法重构整个 V。

证明。 我们不妨假设对于所有n，$f(n)\leqslant n/100$。令$G=(V,\mathcal{P})$为已知距离图，并假设G 中至少有$f(n)$ 个度为一的点。只需证明，以高概率存在一个点u ，其唯一的边uv 满足(u,v) 不是安全点对。

我们首先给出安全点对数量的上界。将 V 中的点记为 $v_1<v_2<\cdots<v_n$。固定 $k\leqslant n/2$。对于至多 $k-1$ 个点 $u\in\{v_{k+1},\dots,v_n\}$，$(u,v_k)$ 是安全点对，因为 u 关于 v_k 的反射必须是 $v_1,\dots,v_{k-1}$ 中的某一个点。特别地，对于 $u\in V$，至多有 $2(k-1)$ 个点使得 (u,v_k) 是安全点对，因此第二个顶点位于 V 前半部分的安全点对数量为

$$\sum_{k\leqslant n/2}2(k-1)=2\binom{\lfloor n/2\rfloor}{2}\leqslant n^2/4.$$

因此，安全点对的总数至多为 $n^2/2$。

现在，进行以下随机过程。首先，均匀随机地选取 G 中一个度为一的顶点 u_1，并令 v_1 为 u_1 的唯一邻点。对于 $s=2,\dots,\lfloor f(n)/3\rfloor$，令 u_s 为 $V\setminus\{u_1,v_1,u_2,v_2,\dots,u_{s-1},v_{s-1}\}$ 中均匀随机选取的一个度为一的顶点，并令 v_s 为 u_s 的唯一邻点。给定 $\{u_1,v_1,u_2,v_2,\dots,u_{s-1},v_{s-1}\}$，注意到 (u_s,v_s) 是从

$$\{(x,y)\colon x\neq y,\ x\in V\setminus\{u_1,v_1,\dots,u_{s-1},v_{s-1}\},\ y\in V\setminus\{u_1,u_2\dots,u_{s-1}\}\}.$$

该集合的大小至少为 $3n^2/4$，因此，给定 $\{u_1,v_1,u_2,v_2,\dots,u_{s-1},v_{s-1}\}$ 后，(u_s,v_s) 是安全点对的概率至多为 $(n^2/2)/(3n^2/4)=2/3$。特别地，对于所有 $s\leqslant\lfloor f(n)/3\rfloor$，$(u_s,v_s)$ 均为安全点对的概率至多为 $(2/3)^{\lfloor f(n)/3\rfloor}=o(1)$。 □

现在，如果 $p\leqslant(\log n+\log\log n-\omega(1))/n$，那么以高概率 $\mathcal{G}(n,p)$ 会有任意多个度为一的顶点（例如参见 [Bol01, 第 7]章），因此 定理 1.2c 得证。

4 开放问题

定理 1.2 表明，$1/n$ 是存在由线性数量顶点构成的可重构集合的弱阈值。确定是否存在尖锐阈值将是很有意思的问题；自然的猜想是该阈值为 $1/n$，因为这与 $\mathcal{G}(n,p)$ 中巨型分量的出现相吻合。

猜想 4.1。设 V 是实数轴上的 n 个点组成的集合。假设已知两两距离图 $(V,\mathcal{P})$ 服从 $\mathcal{G}(n,(1+\varepsilon)/n)$ 分布，其中 $\varepsilon>0$ 是一个常数。那么，以高概率存在一个大小为 $\Omega_\varepsilon(n)$ 的可重构集合。

我们没有尝试优化定理 1.2a 中的常数，但我们的方法无法给出优于 $9/n$ 的界，因为当 p 更小时，足够短的环中点对太少。自举论证或许能将常数降到 9 以下，但无法将其降至 $p=(1+\varepsilon)/n$，因为大多数点对只会出现在长度至少为 $\Omega(\log(n)/\varepsilon)$ 的环中。

此外，刻画巨型可重构分量也很有意思。对于一维的全局图刚性，最大的可重构分量是最大的二连通子图。对于二维的图刚性，巨型可重构分量出现的阈值由 [KMT11] 确定，而该分量的刻画由 [BLM18] 给出。

维度大于一时的可重构性也很有意思。要求重构整个 V 未免太苛刻：考虑一种嵌入，其中 $n-2$ 个点位于一个 $(d-1)$ 维超平面上，而另外两个点 u、v 不在其上。只有当 u 与 v 之间的距离被揭示时，才能完全重构 V（否则 u、v 可能位于超平面的同一侧，也可能位于两侧）。不过，值得探究的是，重构 V 的一个线性大小子集的阈值是多少。$1/n$ 是否也是弱阈值，就像 $d=1$ 时那样？

最后，Benjamini 和 Tzalik [BT22] 还考虑了一种更强的可重构性概念。设 $G=(V,E)$ 是一个图。若对 V 的每一种嵌入，子集 $U\subseteq V$ 都能根据 $|u-v|$（其中 $uv\in E$）的距离重构，我们就称 $U\subseteq V$ 是对抗可重构的。请注意，这与全局刚性的定义类似，只是去掉了一般位置条件。确定 $\mathcal{G}(n,p)$ 在 $\mathbb{R}$ 中对抗可重构的阈值，以及 $\mathcal{G}(n,p)$ 中某个线性大小子集对抗可重构的阈值，将会很有意思。与定理 1.2 相比，最小度至少为二是必要条件，因为可以选择一种嵌入，使得不存在安全点对。Benjamini 和 Tzalik 猜想这也是充分条件：当距离按随机顺序逐一揭示时，图恰好在最小度达到二的时刻变为对抗可重构。

参考文献

[ACKR89] 诺加·阿隆、亚伊尔·卡罗、伊利亚·克拉西科夫和耶胡达·罗迪蒂（1989年）。组合重建问题。《组合理论杂志B辑》47(2)，153–161。 ↑1[BLM18] J. BARRÉ、M. LELARGE 和 D. MITSCHE（2018年）。关于带滑块的随机图的刚性、可定向性和核。《随机结构与算法》52(3)，419–453。 ↑3，12

[Bol01] 贝拉·博洛巴什（2001年）。《随机图》。剑桥高等数学研究丛书，第2版。（剑桥大学出版社）。 ↑6，7，11[BT22] 伊泰·本雅米尼和埃拉德·察利克（2022年）。从两两距离的一个子集中确定直线上的点配置。arXiv:2208.13855。 ↑1，3，4，10，12[Con05] 罗伯特·康纳利（2005年）。一般位置全局刚性。《离散与计算几何：国际数学与计算机科学杂志》33(4)，549–563。↑3[GHT10] 史蒂文·J·戈特勒、亚历山大·D·希利和迪伦·P·瑟斯顿（2010年）。刻画一般位置全局刚性。《美国数学杂志》132(4)，897–939。 ↑3[JSS07] 比尔·杰克逊、布里吉特·塞尔瓦蒂乌斯和赫尔曼·塞尔瓦蒂乌斯（2007年）。某些图族的二维刚性。《图论杂志》54(2)，154–166。 ↑3[JT22] 蒂博尔·约尔丹和谷川伸一（2022年）。随机子图的刚性与刚度矩阵的特征值。《SIAM离散数学杂志》36(3)，2367–2392。 ↑3[JW17] 蒂博尔·约尔丹和沃尔特·怀特利（2017年）。全局刚性。《离散与计算几何手册》（雅各布·E·古德曼、约瑟夫·奥罗克和乔鲍·D·托特编），第3版，第63章。 ↑3[KMT11] 希瓦·普拉萨德·卡西维斯瓦纳坦、克里斯托弗·摩尔和路易斯·特兰（2011年）。随机图中的刚性转变。《第二十二届ACM-SIAM离散算法年会论文集》，1237–1252。arXiv:1010.3605。↑3，12[KT13] 弗兰茨·J·基拉伊和路易斯·特兰（2013年）。压缩感知重建中的相干性与充分采样密度。arXiv:1302.2767。 ↑3[LNPR22] 艾伦·卢、埃兰·内沃、尤瓦尔·佩莱德和奥里特·E·拉兹（2022年）。随机图刚性的尖锐阈值。arXiv:2202.09917。 ↑3[PRS03] 卢克·佩博迪、杰米·拉德克利夫和亚历克斯·斯科特（2003年）。平面的有限子集是18可重构的。《SIAM离散数学杂志》16(2)，262–275。↑1[RW10] 奥利弗·里奥丹和尼古拉斯·沃莫尔德（2010年）。稀疏随机图的直径。《组合学、概率与计算》19(5-6)，835–926。 ↑6