TYPICAL AUTOMORPHISM GROUPS OF FINITE NONRIGID STRUCTURES

VERA KOPONEN

Abstract. We work with a finite relational vocabulary with at least one relation symbol with arity at least 2. Fix any integer $m > 1$. For almost all finite structures (labelled or unlabelled) such that at least m elements are moved by some automorphisms, the automorphism group is $(\mathbb{Z}_2)^i$ for some $i \leq (m+1)/2$; and if some relation symbol has arity at least 3, then the automorphism group is almost always $\mathbb{Z}_2$.
Keywords: finite model theory, limit law, random structure, automorphism group.

1. Introduction

This article complements the work in [1] with quite explicit information about the automorphism group of "almost all" finite structures such that at least m elements are moved by some automorphisms, for any fixed integer m. It turns out that the automorphism group is almost always a power of $\mathbb{Z}_2$, where the maximal power is bounded by $(m+1)/2$. As part of proving this we prove that almost all finite structures such that at least m elements are moved by some automorphisms have the property that exactly m' elements are moved by some automorphism, where $m' = m$ if m is even and $m' = m + 1$ otherwise. Perhaps surprisingly, we get different results depending on the maximal arity of the relation symbols (of the finite relational language). If the maximal arity is at least 3, then the typical automorphism group is always $\mathbb{Z}_2$, no matter what m is. If the maximal arity is 2, then for each $i = 1, \ldots, m'/2$, $(\mathbb{Z}_2)^i$ appears as an automorphism group with positive probability (given by the uniform probability measure on the set of n-element structures). The situation is slightly different if we restrict attention to finite structures such that *exactly* m elements are moved by some automorphisms. Then $\mathbb{Z}_3$ or the symmetric group on three elements appear as a subgroup of the typical automorphism group if m is odd. These results hold for both labelled and unlabelled structures (See Remark 1.3).

We now introduce some notation and terminology which will be used throughout the article and then state the two main results. We work with a finite relational vocabulary (also called signature) $V = \{R_1, \ldots, R_\rho\}$, where each relation symbol R_i has arity r_i. The number $\mathbf{ari}(V) = \max\{r_1, \ldots, r_\rho\}$ is called the *maximal arity* and the we assume that it is at least 2. Let $N_{\max}(V)$ is the number of relation symbols of arity $\mathbf{ari}(V)$ and $N_{\max-1}(V)$ the number of relation symbols of arity $\mathbf{ari}(V)-1$. The set of all structures for this vocabulary with universe $[n] = \{1, \ldots, n\}$ is denoted $\mathbf{S}_n$ and we let $\mathbf{S} = \bigcup_{n=1}^{\infty} \mathbf{S}_n$. For any set A, $|A|$ is its cardinality and $Sym(A)$ the group of all permutations of A. Suppose that $f_1, \ldots f_k \in Sym(A)$. Then $\langle f_1, \ldots, f_k \rangle$ denotes the subgroup of $Sym(A)$ generated by $f_1, \ldots f_k$ and we define

$$\mathrm{Spt}(f_1, \ldots, f_k) \;=\; \{a \in A : g(a) \neq a \text{ for some } g \in \langle f_1, \ldots, f_k \rangle\}$$

and let $\mathrm{spt}(f_1, \ldots, f_k) = |\mathrm{Spt}(f_1, \ldots, f_k)|$. We call $\mathrm{Spt}(f_1, \ldots, f_k)$ the *support* of $f_1, \ldots, f_k$. For any finite structure $\mathcal{M}$ we let $\mathrm{Aut}(\mathcal{M})$ denote its group of automorphisms,

$$\begin{aligned}\mathrm{spt}(\mathcal{M}) &= \max\{\mathrm{spt}(f) : f \in \mathrm{Aut}(\mathcal{M})\},\\ \mathrm{Spt}^*(\mathcal{M}) &= \{a \in M : a \in \mathrm{Spt}(f) \text{ for some } f \in \mathrm{Aut}(\mathcal{M})\}, \quad \text{and}\\ \mathrm{spt}^*(\mathcal{M}) &= \big|\mathrm{Spt}^*(\mathcal{M})\big|.\end{aligned}$$

We call $\mathrm{Spt}^*(\mathcal{M})$ the *support* of $\mathcal{M}$. For every $m \in \mathbb{N}$ define

$$\begin{aligned}\mathbf{S}_n(\mathrm{spt} \geq m) &= \{\mathcal{M} \in \mathbf{S}_n : \mathrm{spt}(\mathcal{M}) \geq m\} \quad \text{and}\\ \mathbf{S}_n(\mathrm{spt}^* \geq m) &= \{\mathcal{M} \in \mathbf{S}_n : \mathrm{spt}^*(\mathcal{M}) \geq m\}.\end{aligned}$$

Whenever $\mathbf{S}'_n \subseteq \mathbf{S}_n$ is defined for all $n \in \mathbb{N}^+$ we let $\mathbf{S}' = \bigcup_{n=1}^{\infty} \mathbf{S}'_n$. With the expression *almost all* $\mathcal{M} \in \mathbf{S}'$ *has the property* P we mean that

$$\lim_{n\to\infty} \frac{\big|\{\mathcal{M} \in \mathbf{S}'_n : \ \mathcal{M} \text{ has } P\}\big|}{\big|\mathbf{S}'_n\big|} = 1.$$

Theorem 1.1. *Suppose that* $\mathbf{ari}(V) = 2$. *Let* $m \geq 2$ *be an integer and let* $m' = m$ *if* m *is even and* $m' = m + 1$ *otherwise.*
(i) For almost all $\mathcal{M} \in \mathbf{S}(\mathrm{spt} \geq m)$, $\mathrm{spt}^*(\mathcal{M}) = m'$ *and* $\mathrm{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^i$ *for some* $i \in \{1, \ldots, m'/2\}$.
(ii) For every $i \in \{1, \ldots, m'/2\}$ *there is a rational number* $0 < a_i \leq 1$ *(where* $a_i < 1$ *if* $m > 2$*) such that the proportion of* $\mathcal{M} \in \mathbf{S}_n(\mathrm{spt} \geq m)$ *such that* $\mathrm{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^i$ *converges to* a_i *as* $n \to \infty$.
(iii) Parts (i) and (ii) hold if '$\mathrm{spt} \geq m$*' is replaced with '*$\mathrm{spt}^* \geq m$*'.*

Theorem 1.2. *Suppose that* $\mathbf{ari}(V) \geq 3$ *and let* $m \geq 2$ *be an integer. Let* $m' = m$ *if* m *is even and* $m' = m+1$ *otherwise. Then, for almost all* $\mathcal{M} \in \mathbf{S}(\mathrm{spt} \geq m)$, $\mathrm{spt}^*(\mathcal{M}) = m'$ *and* $\mathrm{Aut}(\mathcal{M}) \cong \mathbb{Z}_2$. *The same is true if '*$\mathrm{spt} \geq m$*' is replaced with '*$\mathrm{spt}^* \geq m$*'.*

Intuitively, one may interpret the theorems as saying that finite structures tend to be as "rigid" as we allow them to be; their automorphisms typically move as few elements as possible (given the restriction that some minimum number of elements are moved) and the automorphism group typically acts in the simplest possible way on the elements which are moved. This is a generalisation of the well known result, proved via a sequence of articles [4, 5, 6, 7, 8], that almost all $\mathcal{M} \in \mathbf{S}$ are *rigid*, that is, $\mathrm{Aut}(\mathcal{M})$ is trivial (i.e. contains only one element).

Remark 1.3. (i) Theorems 1.1 and 1.2 also hold if we consider *unlabelled* structures, that is, if we count structures only up to isomorphism. This follows from the proof of Theorem 7.7 in [1].
(ii) Theorems 1.1 and 1.2 also hold if we require that all relations are *irreflexive* or that all relations are *irreflexive and symmetric*, in the sense explained in Remark 1.5 in [1]. Only minor modifications of the proofs (and some technical results) in [1] and this article are necessary.

2. Preliminaries

Terminology and notation 2.1. Recall the terminology and notation introduced before Theorem 1.1. So in particular we have fixed a finite relational vocabulary with maximal arity at least 2. Structures (for this vocabulary) are denoted $\mathcal{A}, \mathcal{B}, \ldots, \mathcal{M}, \mathcal{N}$ and their universes $A, B, \ldots, M, N$. For any set A, $|A|$ denotes its cardinality. Since we mainly deal with structures $\mathcal{M} \in \mathbf{S}$, the universe will usually be $[n] = \{1, \ldots, n\}$ for some integer $n > 0$. For structures $\mathcal{M}$ and $\mathcal{N}$, $\mathcal{M} \cong \mathcal{N}$ means that they are isomorphic. If A is a subset of the universe of $\mathcal{M}$, then $\mathcal{M}{\restriction}A$ denotes the substructure of $\mathcal{M}$ with universe A, which is well defined since the vocabulary has only relation symbols. (See for example [3, 9] for basic model theory.) For groups G and H, $G \cong H$ means that they are isomorphic as abstract groups.

Suppose that f is a permutation of a set Ω and that H is a group of permutations of Ω. Then $a \in \Omega$ is called a *fixed point of* f if $f(a) = a$. If a is a fixed point of every $h \in H$, then we say that a is a *fixed point of* H. For a structure $\mathcal{A}$ and $a \in A$, we call a a *fixed point of* $\mathcal{A}$ if a is a fixed point of $\mathrm{Aut}(\mathcal{A})$, where we recall that $\mathrm{Aut}(\mathcal{A})$ is the automorphism group of $\mathcal{A}$. $Sym(\Omega)$ denotes the group of all permutations of Ω, i.e. the symmetric group of Ω, and we let $Sym_n = Sym([n])$. Still assuming that H is a group of permutations of Ω, we let $\mathbf{fld}(H) = |\Omega|$ (for "field size" of H), we let $\mathbf{orb}_1(H)$ be the number of orbits of H on Ω, and $\mathbf{orb}_2(H)$ the number of orbits of H on $\Omega \times \Omega$ by the action of H on $\Omega \times \Omega$ given by $h(a, b) = (h(a), h(b))$ for $h \in H$ and $(a, b) \in \Omega \times \Omega$.

For a function $f : A \to B$ and $X \subseteq A$, $f \restriction X$ is the restriction of f to X. If H is a permutation group on Ω and $X \subseteq \Omega$ is a union of orbits of H on Ω, then $H \restriction X = \{h \restriction X : h \in H\}$ and note that $H \restriction X$ is a permutation group on X. (For basic permutation group theory see [2] for example.)

It will be convenient to extend the notation used in the main results as follows:

$$\begin{aligned}
\mathbf{S}_n(\mathrm{spt}^* = m) &= \{\mathcal{M} \in \mathbf{S}_n : \mathrm{spt}^*(\mathcal{M}) = m\}, \\
\mathbf{S}_n(\mathrm{spt}^* \leq m) &= \{\mathcal{M} \in \mathbf{S}_n : \mathrm{spt}^*(\mathcal{M}) \leq m\}, \\
\mathbf{S}_n(m \leq \mathrm{spt}^* \leq m') &= \{\mathcal{M} \in \mathbf{S}_n : m \leq \mathrm{spt}(\mathcal{M}) \leq m'\}.
\end{aligned}$$

We will use a some notions and results from [1] which we now state. The first gives an upper bound for $\mathrm{spt}^*(\mathcal{M})$ for almost all $\mathcal{M} \in \mathbf{S}(\mathrm{spt} \geq m)$ and almost all $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* \geq m)$.

Proposition 2.2. [1, Corollary 3.7] *For every $m \in \mathbb{N}$ there is $m' \in \mathbb{N}$ such that*

$$\begin{aligned}
&\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt} \geq m) \ \cap \ \mathbf{S}_n(\mathrm{spt}^* \leq m')\big|}{\big|\mathbf{S}_n(\mathrm{spt} \geq m)\big|} \ = \\
&\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* \geq m) \ \cap \ \mathbf{S}_n(\mathrm{spt}^* \leq m')\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* \geq m)\big|} \ = \ 1.
\end{aligned}$$

Note that for every structure $\mathcal{M}$, $\mathrm{Spt}^*(\mathcal{M})$ is the union of all nonsingleton orbits of $\mathrm{Aut}(\mathcal{M})$ on M, so it makes sense to speak about $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M})$ and we always have $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M}) \cong \mathrm{Aut}(\mathcal{M})$.

Definition 2.3. Let $\mathcal{A} \in \mathbf{S}$ be such that $\mathrm{Aut}(\mathcal{A})$ has no fixed point. Suppose that H is a subgroup of $\mathrm{Aut}(\mathcal{A})$ such that H has no fixed point. For each integer $n > 0$, $\mathbf{S}_n(\mathcal{A}, H)$ is the set of $\mathcal{M} \in \mathbf{S}_n$ such that there is an embedding $f : \mathcal{A} \to \mathcal{M}$ such that $\mathrm{Spt}^*(\mathcal{M})$ is the image of f and $H_f = \{f \sigma f^{-1} : \sigma \in H\}$ is a subgroup of $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M})$.[1]

Lemma 2.4. [1, Lemma 4.2] *Let $m \geq 2$ be an integer. There are $\mathcal{A}_1, \ldots, \mathcal{A}_l \in \mathbf{S}_m$ without any fixed point and, for each $i = 1, \ldots, l$, subgroups $H_{i,1}, \ldots, H_{i,l_i} \subseteq \mathrm{Aut}(\mathcal{A}_i)$ without any fixed point such that*

$$\mathbf{S}(\mathrm{spt}^* = m) \ = \ \bigcup_{i=1}^{l} \bigcup_{j=1}^{l_i} \mathbf{S}(\mathcal{A}_i, H_{i,j}).$$

Recall the notation $\mathbf{ari}(V)$, $N_{\max}$ and $N_{\max-1}$ from the introduction.

Definition 2.5. With $r = \mathbf{ari}(V)$, $k = N_{\max}$ and $l = N_{\max-1}$, let

$$\beta(x, y, z) \ = \ k\binom{r}{2}x^2 \ - \ kr(r-1)xy \ - \ l(r-1)x \ + \ l(r-1)y \ + \ k\binom{r}{2}z.$$

[1] Instead of saying "embedding $f : \mathcal{A} \to \mathcal{M}$ such that $\mathrm{Spt}^*(\mathcal{M})$ is the image of f" we could (equivalently) say "isomorphism $f : \mathcal{A} \to \mathcal{M} \restriction \mathrm{Spt}^*(\mathcal{M})$".

Proposition 2.6. [1, Proposition 5.1] *Suppose that $\mathcal{A}, \mathcal{A}' \in \mathbf{S}$ are such that neither* $\mathrm{Aut}(\mathcal{A})$ *nor* $\mathrm{Aut}(\mathcal{A}')$ *has a fixed point. Moreover, suppose that H is a subgroup of* $\mathrm{Aut}(\mathcal{A})$ *without fixed any point and that H' is a subgroup of* $\mathrm{Aut}(\mathcal{A}')$ *without any fixed point. Let $p = \mathbf{fld}(H)$, $q = \mathbf{orb}_1(H)$, $s = \mathbf{orb}_2(H)$, $p' = \mathbf{fld}(H')$, $q' = \mathbf{orb}_1(H')$ and $s' = \mathbf{orb}_2(H')$.*
(i) The following limit exists in $\mathbb{Q} \cup \{\infty\}$:

$$\lim_{n\to\infty} \frac{\left|\mathbf{S}_n(\mathcal{A}', H')\right|}{\left|\mathbf{S}_n(\mathcal{A}, H)\right|}.$$

(ii) Suppose that $\mathbf{ari}(V) = 2$.

(a) *If $p - q < p' - q'$ or if both $p - q = p' - q'$ and $p > p'$, then*

$$\lim_{n\to\infty} \frac{\left|\mathbf{S}_n(\mathcal{A}', H')\right|}{\left|\mathbf{S}_n(\mathcal{A}, H)\right|} \ = \ 0.$$

(b) *If $p - q = p - q'$ and $p = p'$ then there is a rational number $a > 0$, depending only on $\mathcal{A}$, $\mathcal{A}'$, H, H' and the vocabulary, such that*

$$\lim_{n\to\infty} \frac{\left|\mathbf{S}_n(\mathcal{A}', H')\right|}{\left|\mathbf{S}_n(\mathcal{A}, H)\right|} \ = \ a.$$

(iii) Suppose that $\mathbf{ari}(V) > 2$ and let $\beta(x, y, z)$ be as in Definition 2.5. If any one of the two conditions

$p - q < p' - q'$, *or*
$p - q = p' - q'$ *and* $\beta(p, q, s) > \beta(p', q', s')$

hold, then

$$\lim_{n\to\infty} \frac{\left|\mathbf{S}_n(\mathcal{A}', H')\right|}{\left|\mathbf{S}_n(\mathcal{A}, H)\right|} \ = \ 0.$$

Proposition 2.7. [1, Proposition 5.9] *Let $\mathcal{A}_1, \ldots, \mathcal{A}_m, \mathcal{A}'_1, \ldots, \mathcal{A}'_{m'} \in \mathbf{S}$ be such that none of them has any fixed point. Suppose that for every $i = 1, \ldots, m$ and $j = 1, \ldots, l_i$, $H_{i,j}$ is a subgroup of* $\mathrm{Aut}(\mathcal{A}_i)$ *without any fixed point and that for every $i = 1, \ldots, m'$ and $j = 1, \ldots, l'_i$ $H'_{i,j}$ is a subgroup of* $\mathrm{Aut}(\mathcal{A}'_i)$ *without any fixed point. Then the following limit exists in $\mathbb{Q} \cup \{\infty\}$:*

$$\lim_{n\to\infty} \frac{\left|\bigcup_{i=1}^{m'} \bigcup_{j=1}^{l'_i} \mathbf{S}_n(\mathcal{A}'_i, H'_{i,j})\right|}{\left|\bigcup_{i=1}^{m} \bigcup_{j=1}^{l_i} \mathbf{S}_n(\mathcal{A}_i, H_{i,j})\right|}. \tag{2.1}$$

Definition 2.8. Suppose that $\mathcal{A} \in \mathbf{S}$ has no fixed point and that H is a subgroup of $\mathrm{Aut}(\mathcal{A})$ without any fixed point. For $\mathcal{M} \in \mathbf{S}_n(\mathcal{A}, H)$ we say that H is the *full automorphism group of $\mathcal{M}$* if for every isomorphism $f : \mathcal{A} \to \mathcal{M}{\restriction}\mathrm{Spt}^*(\mathcal{M})$ such that $H_f = \{f\sigma f^{-1} : \sigma \in H\}$ is a subgroup of $\mathrm{Aut}(\mathcal{M}){\restriction}\mathrm{Spt}^*(\mathcal{M})$ we have $H_f = \mathrm{Aut}(\mathcal{M}){\restriction} \mathrm{Spt}^*(\mathcal{M})$.

Lemma 2.9. [1, Lemmas 5.11 and 5.13] *Suppose that $\mathcal{A} \in \mathbf{S}$ has no fixed point and that H is a subgroup of* $\mathrm{Aut}(\mathcal{A})$ *without any fixed point.*
(i) For almost every $\mathcal{M} \in \mathbf{S}(\mathcal{A}, H)$, $\mathrm{Aut}(\mathcal{M}){\restriction}\mathrm{Spt}^*(\mathcal{M})$ has the same number of orbits as H.
(ii) Let $G \leq H$. The proportion of $\mathcal{M} \in \mathbf{S}_n(\mathcal{A}, H)$ such that $G \cong \mathrm{Aut}(\mathcal{M})$ converges to either 0 or 1 as $n \to \infty$.

Lemma 2.10. *Let i be a positive integer.*
(i) For almost all $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 2i)$, $\mathrm{Aut}(\mathcal{M}){\restriction}\mathrm{Spt}^*(\mathcal{M})$ has exactly i orbits on $\mathrm{Spt}^*(\mathcal{M})$, so every such orbit has cardinality 2.

(ii) For almost all $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 2i+1)$, $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M})$ has exactly i orbits, so $i-1$ orbits have cardinality 2 and the remaining orbit has cardinality 3.

Proof. We will use parts (ii) and (iii) of Proposition 2.6.

(i) By Lemma 2.4, there are $\mathcal{A}_1, \ldots, \mathcal{A}_m \in \mathbf{S}_{2i}$ without fixed points and for each $i = 1, \ldots, m$ a number l_i and subgroups $H_{i,1}, \ldots, H_{i,l_i}$ of $\mathrm{Aut}(\mathcal{A}_i)$ without fixed points such that $\mathbf{S}_n(\mathrm{spt}^* = 2i) = \bigcup_{i=1}^m \bigcup_{j=1}^{l_i} \mathbf{S}_n(\mathcal{A}_i, H_{i,j})$ for each large enough n. Moreover, by Lemma 2.9, for almost every $\mathcal{M} \in \mathbf{S}(\mathcal{A}_i, H_{i,j})$ the number of orbits of $H_{i,j}$ on $A_{i,j}$ is $\mathbf{orb}_1(H_{i,j})$. Therefore it suffices to prove that there are $\mathcal{A} \in \mathbf{S}_{2i}$ without fixed point and a subgroup $H \subseteq \mathrm{Aut}(\mathcal{A})$ with exactly i orbits of cardinality 2 (then H has no fixed points) and that if $\mathcal{A}' \in \mathbf{S}_{2i}$ has no fixed point and H' is a subgroup of $\mathrm{Aut}(\mathcal{A}')$ without fixed points such that H' does *not* have exactly i orbits of cardinality 2, then

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathcal{A}', H')\big|}{\big|\mathbf{S}_n(\mathcal{A}, H)\big|} = 0. \tag{2.2}$$

First suppose that $\mathcal{A} \in \mathbf{S}_{2i}$ and that $H \subseteq \mathrm{Aut}(\mathcal{A})$ has exactly i orbits of cardinality 2. Also suppose that $\mathcal{A}' \in \mathbf{S}_{2i}$ and $H' \subseteq \mathrm{Aut}(\mathcal{A}')$ are as described above. Then $\mathbf{fld}(H) = 2i$ and $\mathbf{fld}(H') = 2i$. By parts (ii) and (iii) of Proposition 2.6, we have (2.2) if $\mathbf{fld}(H) - \mathbf{orb}_1(H) < \mathbf{fld}(H') - \mathbf{orb}_1(H')$. By assumption we have $\mathbf{fld}(H) - \mathbf{orb}_1(H) = 2i - i = i$. By assumption, H' has no fixed points, so H' has at most i orbits. As we also assume that H' does not have i orbits, it follows that H' has i' orbits for some $i' < i$ and we get $\mathbf{fld}(H') - \mathbf{orb}_1(H') = 2i - i' > i = \mathbf{fld}(H) - \mathbf{orb}_1(H)$, so (2.2) follows from Proposition 2.6.

We must now prove that there are $\mathcal{A} \in \mathbf{S}_{2i}$ without fixed point and a subgroup $H \subseteq \mathrm{Aut}(\mathcal{A})$ without fixed point such that H has exactly i orbits. But this holds if we let the interpretation of every relation symbol be empty (so $\mathrm{Aut}(\mathcal{A}) = Sym_{2i}$) and let H the permutation group on $[2i]$ with only one nontrivial permutation and this one takes α to 2α for every $\alpha \in [i]$.

(ii) Suppose that $\mathcal{A} \in \mathbf{S}_{2i+1}$ has no fixed point and that H is a subgroup of $\mathrm{Aut}(\mathcal{A})$ without fixed points. Then $\mathbf{fld}(H) = 2i + 1$. For the same reasons as in part (i) we only need to show that (subject to the constraint $\mathbf{fld}(H) = 2i + 1$) $\mathbf{fld}(H) - \mathbf{orb}_1(H)$ is minimal if and only if H has exactly i orbits. As H has no fixed point it has at most i orbits. Hence $\mathbf{fld}(H) - \mathbf{orb}_1(H) \geq 2i+1-i = i+1$ and $\mathbf{fld}(H) - \mathbf{orb}_1(H) = i+1$ if and only if H has exactly i orbits. It now suffices to prove that there are $\mathcal{A} \in \mathbf{S}_{2i+1}$ without fixed point and a subgroup $H \subseteq \mathrm{Aut}(\mathcal{A})$ without fixed point such that H has exactly i orbits. If $i = 1$ and we let the interpretation of every relation symbol be empty, then this clearly holds. So suppose that $i > 1$. Let $B = [2i - 2]$ and $C = \{2i - 1, 2i, 2i + 1\}$. Let the interpretation of every relation symbol be empty and let $H \subseteq \mathrm{Aut}(\mathcal{A})$ be the group $H_1 \times H_2$, where H_1 has only one nontrivial permutation and this one sends α to 2α for every $\alpha \in [i-1]$ and fixes every $\alpha \in C$, every $\alpha \in B$ is a fixed point of H_2 and $H_2 \restriction C$ is the symmetric group of C. Then $\mathrm{Aut}(\mathcal{A}) \cong \mathbb{Z}_2 \times Sym_3$ and $\mathcal{A}$ has exactly i orbits. □

3. Proof of Theorem 1.1

In this section we prove Theorem 1.1. Lemmas 3.1 and 3.2 may be of some interest in themselves. Throughout this section we assume that $\mathbf{ari}(V) = 2$ although this assumption is restated in the results.

Lemma 3.1. *Suppose that $i \geq 1$ and $\mathbf{ari}(V) = 2$. For almost every $\mathcal{M} \in \mathbf{S}_n(\mathrm{spt}^* = 2i)$, $\mathrm{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^t$ for some $t \in \{1, \ldots, i\}$. Moreover, for every $t \in \{1, \ldots, i\}$ there is a rational number $0 < a_t \leq 1$ such that*

$$\lim_{n\to\infty} \frac{\big|\{\mathcal{M} \in \mathbf{S}_n(\mathrm{spt}^* = 2i) : \mathrm{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^t\}\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i)\big|} = a_t,$$

and if $i > 1$ *then* $a_t < 1$.

Proof. By Lemma 2.10, for almost every $\mathcal{M} \in \mathbf{S}_n(\text{spt}^* = 2i)$, $\text{Aut}(\mathcal{M}) \restriction \text{Spt}^*(\mathcal{M})$ has i orbits, each one of cardinality 2. For every $\mathcal{M} \in \mathbf{S}_n(\text{spt}^* = 2i)$ such that $\text{Aut}(\mathcal{M}) \restriction \text{Spt}^*(\mathcal{M})$ has i orbits and every $f \in \text{Aut}(\mathcal{M})$, f^2 is the identity. Hence, for almost every $\mathcal{M} \in \mathbf{S}_n(\text{spt}^* = 2i)$ there is $t \in \{1, \ldots, i\}$ such that $\text{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^t$.

By Lemma 2.4, there are $\mathcal{A}_1, \ldots, \mathcal{A}_m \in \mathbf{S}_{2i}$ without fixed points and for each $i = 1, \ldots, m$ a number l_i and subgroups $H_{i,1}, \ldots, H_{i,l_i}$ of $\text{Aut}(\mathcal{A}_i)$ without fixed points such that

$$\mathbf{S}_n(\text{spt}^* = 2i) \ = \ \bigcup_{i=1}^{m} \bigcup_{j=1}^{l_i} \mathbf{S}_n(\mathcal{A}_i, H_{i,j})$$

for each sufficiently large n. Recall Lemma 2.9. Fix $1 \leq t \leq i$. Let $\mathcal{A}'_i$, $i = 1, \ldots, m$ and $H'_{i,j}$, $j = 1, \ldots, l'_i$, enumerate all pairs $(\mathcal{A}_i, H_{i,j})$ such that $H_{i,j} \cong (\mathbb{Z}_2)^t$ and the proportion of $\mathcal{M} \in \mathbf{S}_n(\mathcal{A}_i, H_{i,j})$ such that $\text{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^t$ converges to 1. Now it suffices to prove that

$$\frac{\left| \bigcup_{i=1}^{m'} \bigcup_{j=1}^{l'_i} \mathbf{S}_n(\mathcal{A}'_i, H'_{i,j}) \right|}{\left| \bigcup_{i=1}^{m} \bigcup_{j=1}^{l_i} \mathbf{S}_n(\mathcal{A}_i, H_{i,j}) \right|}$$

converges to a rational number as $n \to \infty$. But this follows from Proposition 2.7. Part (ii)(b) of Proposition 2.6 guarantees that the limit is larger than 0 if $i > 1$. $\square$

Lemma 3.2. *Suppose that* $i \geq 1$ *and* $\mathbf{ari}(V) = 2$. *(i) For almost every* $\mathcal{M} \in \mathbf{S}_n(\text{spt}^* = 3)$, $\text{Aut}(\mathcal{M}) \cong \mathbb{Z}_3$ *or* $\text{Aut}(\mathcal{M}) \cong Sym_3$. *Moreover, for each one of these groups, call it* G, *there is a rational number* $0 < a_G < 1$ *such that*

$$\lim_{n\to\infty} \frac{\left|\{\mathcal{M} \in \mathbf{S}_n(\text{spt}^* = 2i+1) : \text{Aut}(\mathcal{M}) \cong G\}\right|}{\left|\mathbf{S}_n(\text{spt}^* = 2i+1)\right|} \ = \ a_G.$$

(ii) Suppose that $i > 1$. *For almost every* $\mathcal{M} \in \mathbf{S}_n(\text{spt}^* = 2i+1)$, $\text{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^t \times \mathbb{Z}_3$ *or* $\text{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^t \times Sym_3$ *for some* $t \in \{1, \ldots, i-1\}$. *Moreover, for each one of these groups, call it* G, *there is a rational number* $0 < a_G < 1$ *such that*

$$\lim_{n\to\infty} \frac{\left|\{\mathcal{M} \in \mathbf{S}_n(\text{spt}^* = 2i+1) : \text{Aut}(\mathcal{M}) \cong G\}\right|}{\left|\mathbf{S}_n(\text{spt}^* = 2i+1)\right|} \ = \ a_G.$$

Proof. The first claim of part (i) is immediate because a permutation group without fixed points on a set of cardinality 3 must be isomorphic to either $\mathbb{Z}_3$ (if no nonidentity permutation has a fixed point) or Sym_3. The second claim of part (i) is proved in the same way as the second claim of Lemma 3.1, with the help of Propositions 2.7 and 2.6 and Lemma 2.9.

Now we prove part (ii), so suppose that $i > 1$. By Lemma 2.10, for almost every $\mathcal{M} \in \mathbf{S}(\text{spt}^* = 2i+1)$, $\text{Aut}(\mathcal{M}) \restriction \text{Spt}^*(\mathcal{M})$ has $i-1$ orbits, say $O_1, \ldots, O_{i-1}$, of cardinality 2 and one orbit O_i of cardinality 3. Hence, for the first statement of (ii), it suffices to prove that for each $\mathcal{M} \in \mathbf{S}_n(\text{spt}^* = 2i+1)$ with $i-1$ orbits $O_1, \ldots, O_{i-1}$, of cardinality 2 and one orbit O_i of cardinality 3, $\text{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^t \times \mathbb{Z}_3$ or $\text{Aut}(\mathcal{M}) \cong (\mathbb{Z}_2)^t \times Sym_3$ for some $t \in \{1, \ldots, i-1\}$. The second statement of part (ii) is proved in the same way as the second statement of part (i) (and the second statement of Lemma 3.1).

With the given assumptions we have

$$\text{Aut}(\mathcal{M}) \restriction (O_1 \cup \ldots \cup O_{i-1}) \ \cong \ (\mathbb{Z}_2)^t$$

for some $t \geq 1$, because for every $f \in \text{Aut}(\mathcal{M}) \restriction (O_1 \cup \ldots \cup O_{i-1})$, f^2 is the identity. The next step is to show that $\text{Aut}(\mathcal{M}) \restriction \text{Spt}^*(\mathcal{M})$ is the direct product of $\text{Aut}(\mathcal{M}) \restriction (O_1 \cup \ldots \cup O_{i-1})$ and $\text{Aut}(\mathcal{M}) \restriction O_i$, since it follows from the case $i = 1$ that $\text{Aut}(\mathcal{M}) \restriction O_i \cong \mathbb{Z}_3$ or $\text{Aut} \restriction O_i \cong Sym_3$.

Let $O_i = \{a, b, c\}$. There is $f \in \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ such that $f(a) = b$ and $g \in \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ such that $g(b) = c$. If $f(c) = c$ and $g(a) = a$ then fg has no fixed point in O_i. Otherwise either f or g has no fixed point in O_i. So under all circumstances there exists $f \in \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ which has no fixed point in O_i. Since $|O_j| = 2$ for every $j \in \{1, \ldots, i-1\}$ it follows that every $d \in O_1 \cup \ldots \cup O_{i-1}$ is a fixed point of f^2. Take any $j \in \{1, \ldots, i-1\}$ and let $O_j = \{d, e\}$, so both d and e are fixed points of f^2. Since there is $h \in \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ such that $h(d) = e$ (and $h(e) = d$) it follows, using f and h, that $O_j \times O_i$ is an orbit of $\mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ on $\mathrm{Spt}^*(\mathcal{M}) \times \mathrm{Spt}^*(\mathcal{M})$. This holds for every $j \in \{1, \ldots, i-1\}$, and therefore

$$\mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M}) \;\cong\; \mathrm{Aut}(\mathcal{M})\restriction(O_1 \cup \ldots \cup O_{i-1}) \times \mathrm{Aut}(\mathcal{M})\restriction O_i.$$

Hence, for either $\mathcal{G} = \mathbb{Z}_3$ or $\mathcal{G} = Sym_3$, and some $t \in \{1, \ldots, i-1\}$, $\mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M}) \cong (\mathbb{Z}_2)^t \times \mathcal{G}$, and clearly the same holds with $\mathrm{Aut}(\mathcal{M})$ in place of $\mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$. □

The next corollary is an immediate consequence of Lemmas 3.1 and 3.2.

Corollary 3.3. *Let $m \geq 2$. Almost every $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = m)$ has an automorphism whose support has cardinality m.*

Lemma 3.4. *Suppose that $i \geq 1$ and $\mathbf{ari}(V) = 2$. Then*

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i+1)\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i)\big|} \;=\; 0.$$

Proof. By Lemma 2.10, for almost every $\mathcal{M} \in \mathbf{S}_n(\mathrm{spt}^* = 2i)$, $H = \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ has exactly i orbits, and for almost every $\mathcal{M}' \in \mathbf{S}_n(\mathrm{spt}^* = 2i+1)$, $H' = \mathrm{Aut}(\mathcal{M}')\restriction \mathrm{Spt}^*(\mathcal{M}')$ has exactly i orbits. For such H and H' we have

$$\mathbf{fld}(H) - \mathbf{orb}_1(H) \;=\; i \;<\; i+1 = \mathbf{fld}(H') - \mathbf{orb}_1(H'),$$

so if $\mathcal{A} = \mathcal{M}\restriction\mathrm{Spt}^*(\mathcal{M})$ and $\mathcal{A}' = \mathcal{M}'\restriction\mathrm{Spt}^*(\mathcal{M}')$ (and $\mathcal{M}$ and $\mathcal{M}'$ are as above), then Proposition 2.6 (ii) implies that $\big|S_n(\mathcal{A}', H')\big| / \big|S_n(\mathcal{A}, H)\big| \to 0$ as $n \to \infty$. The lemma follows from this because, by Lemma 2.4, each one of $\mathbf{S}(\mathrm{spt}^* = 2i)$ and $\mathbf{S}(\mathrm{spt}^* = 2i+1)$ is a union of finitely many sets of the form $\mathbf{S}(\mathcal{A}, H)$. □

Lemma 3.5. *Suppose that $i \geq 1$ and $\mathbf{ari}(V) = 2$. Then*

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i+1)\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i+2)\big|} \;=\; 0.$$

Proof. By Lemma 2.10, for almost every $\mathcal{M} \in \mathbf{S}_n(\mathrm{spt}^* = 2i+2)$, $H = \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ has exactly $i+1$ orbits, and for almost every $\mathcal{M}' \in \mathbf{S}_n(\mathrm{spt}^* = 2i+1)$, $H' = \mathrm{Aut}(\mathcal{M}')\restriction \mathrm{Spt}^*(\mathcal{M}')$ has exactly i orbits. It follows that

$$\mathbf{fld}(H) - \mathbf{orb}_1(H) \;= 2i+2-(i+1) \;=\; i+1 \;=\; 2i+1-i \;=\; \mathbf{fld}(H') - \mathbf{orb}_1(H')$$

and

$$\mathbf{fld}(H) \;=\; 2i+2 \;>\; 2i+1 \;=\; \mathbf{fld}(H').$$

So if $\mathcal{M}$ and $\mathcal{M}'$ are as above, $\mathcal{A} = \mathcal{M}\restriction\mathrm{Spt}^*(\mathcal{M})$ and $\mathcal{A}' = \mathcal{M}'\restriction\mathrm{Spt}^*(\mathcal{M}')$, then Proposition 2.6 (ii) implies that $\big|S_n(\mathcal{A}', H')\big| / \big|S_n(\mathcal{A}, H)\big| \to 0$ as $n \to \infty$. The lemma follows because each one of $\mathbf{S}(\mathrm{spt}^* = 2i+1)$ and $\mathbf{S}(\mathrm{spt}^* = 2i+2)$ is a union of finitely many sets of the form $\mathbf{S}(\mathcal{A}, H)$. □

Lemma 3.6. *Suppose that $\mathbf{ari}(V) = 2$ and either $m = 0$ or $m \geq 2$. Then*

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = m+2)\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* = m)\big|} \;=\; 0.$$

Proof. The case $m = 0$ follows from the fact that almost all $\mathcal{M} \in \mathbf{S}$ are rigid [5]. Now suppose that $m \geq 2$. By Lemma 2.10, for almost every $\mathcal{M} \in \mathbf{S}_n(\mathrm{spt}^* = m)$, $H = \mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M})$ has exactly $\lfloor \frac{m}{2} \rfloor$ orbits, and for almost every $\mathcal{M}' \in \mathbf{S}_n(\mathrm{spt}^* = m+2)$, $H' = \mathrm{Aut}(\mathcal{M}') \restriction \mathrm{Spt}^*(\mathcal{M}')$ has exactly $\lfloor \frac{m+2}{2} \rfloor = \lfloor \frac{m}{2} \rfloor + 1$ orbits. Since

$$\mathbf{fld}(H) - \mathbf{orb}_1(H) \ = m - \left\lfloor \frac{m}{2} \right\rfloor \ < \ m - \left\lfloor \frac{m}{2} \right\rfloor + 1 \ = \ \mathbf{fld}(H') - \mathbf{orb}_1(H'),$$

it follows that if $\mathcal{M}$ and $\mathcal{M}'$ are as above, $\mathcal{A} = \mathcal{M} \restriction \mathrm{Spt}^*(\mathcal{M})$ and $\mathcal{A}' = \mathcal{M}' \restriction \mathrm{Spt}^*(\mathcal{M}')$, then Proposition 2.6 (ii) implies that $\big|S_n(\mathcal{A}', H')\big| / \big|S_n(\mathcal{A}, H)\big| \to 0$ as $n \to \infty$, which in turn implies the lemma (just as in the proofs of the preceeding two lemmas). □

Lemma 3.7. *Suppose that* $\mathbf{ari}(V) = 2$*. Also assume that* $m = 0$ *or* $m \geq 2$ *and that* $T > m$ *and* $T \geq 2$*. Let* $m' = m$ *if* m *is even and* $m' = m + 1$ *otherwise. Then*

$$\lim_{n \to \infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = m')\big|}{\big|\mathbf{S}_n(m \leq \mathrm{spt}^* \leq T)\big|} \ = \ 1.$$

Proof. The case when $m = 0$ follows from [5], so suppose that $m \geq 2$. If $T = m+1$ then the result follows from Lemmas 3.4 and 3.5. Now suppose that $m \geq 2$ and $T \geq m + 2$. For each $i \in \{m + 2, \ldots, T\}$ we have, by Lemma 3.6,

$$\frac{\big|\mathbf{S}_n(\mathrm{spt}^* = i)\big|}{\big|\mathbf{S}_n(m \leq \mathrm{spt}^* \leq T)\big|} \ \leq \ \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = i)\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* = i - 2)\big|} \ \to \ 0$$

as $n \to \infty$. From this it follows that

$$\lim_{n \to \infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = m) \cup \mathbf{S}_n(\mathrm{spt}^* = m + 1)\big|}{\big|\mathbf{S}_n(m \leq \mathrm{spt}^* \leq T)\big|} \ = \ 1.$$

The lemma now follows from Lemmas 3.4 and 3.5. □

Lemma 3.8. *Suppose that* $\mathbf{ari}(V) = 2$ *and* $m \geq 2$*. Let* $m' = m$ *if* m *is even and* $m' = m + 1$ *otherwise. Then*

$$\lim_{n \to \infty} \frac{\big|\mathbf{S}_n(\mathrm{spt} \geq m) \cap \mathbf{S}_n(\mathrm{spt}^* = m')\big|}{\big|\mathbf{S}_n(\mathrm{spt} \geq m)\big|} \ = \ \lim_{n \to \infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = m')\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* \geq m)\big|} \ = \ 1.$$

Proof. Let $m \geq 2$. Proposition 2.2 says that there is $T > m$ such that

$$\lim_{n \to \infty} \frac{\big|\mathbf{S}_n(m \leq \mathrm{spt}^* \leq T)\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* \geq m)\big|} \ = \ \lim_{n \to \infty} \frac{\big|\mathbf{S}_n(\mathrm{spt} \geq m) \ \cap \ \mathbf{S}_n(\mathrm{spt}^* \leq T)\big|}{\big|\mathbf{S}_n(\mathrm{spt} \geq m)\big|} \ = \ 1.$$

By Corollary 3.3 it suffices to prove that

$$\lim_{n \to \infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = m')\big|}{\big|\mathbf{S}_n(m \leq \mathrm{spt}^* \leq T)\big|} \ = \ 1,$$

but this follows from Lemma 3.7. □

We get Theorem 1.1 by combining Lemmas 3.1 and 3.8.

4. Proof of Theorem 1.2

Theorem 1.2 is proved in this section, but Lemmas 4.1 and 4.4 may be of interest in themselves. In this section we assume that $\mathbf{ari}(V) \geq 3$.

Lemma 4.1. *Suppose that* $\mathbf{ari}(V) \geq 3$ *and* $i \geq 1$*. For almost all* $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 2i)$, $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M})$ *has exactly* $2i^2$ *orbits on* $\mathrm{Spt}^*(\mathcal{M}) \times \mathrm{Spt}^*(\mathcal{M})$*, so every orbit on* $\mathrm{Spt}^*(\mathcal{M}) \times \mathrm{Spt}^*(\mathcal{M})$ *has cardinality 2.*

Proof. First note that if H is the permutation group on $\Omega = \{v_1, \ldots, v_i, w_1, \ldots, w_i\}$ whose only nontrivial permutation sends v_j to w_j for every j, then H has i orbits on Ω and $2i^2$ orbits on $\Omega \times \Omega$, because every orbit on $\Omega \times \Omega$ has cardinality 2. Hence $\mathbf{orb}_2(H) = 2i^2$. Moreover, for every permutation group on Ω without fixed points, the number of orbits on $\Omega \times \Omega$ cannot exceed $(2i)^2/2 = 2i^2$. So if H is as described then $\mathbf{orb}_2(H)$ is maximal among permutation groups on a set of cardinality $2i$. We also have $\mathbf{fld}(H) - \mathbf{orb}_1(H) = i$ which is minimal among permutation groups without any fixed point on a set of cardinality $2i$.

Let $\mathcal{A}$ be any structure without fixed point with universe $A = \Omega$ and H a subgroup of $\mathrm{Aut}(\mathcal{A})$ without any fixed point. For example, let the interpretation of every relation symbol be empty. Suppose that $\mathcal{A}'$ is a structure with universe of cardinality $2i$ and without any fixed point and suppose, moreover, that H' is a subgroup of $\mathrm{Aut}(\mathcal{A}')$ such that H' has no fixed point and either $\mathbf{orb}_1(H') < i$ or $\mathbf{orb}_2(H') < 2i^2$. If $\mathbf{orb}_1(H') < i$ then, as $\mathbf{fld}(H') = \mathbf{fld}(H) = 2i$, we get $\mathbf{fld}(H') - \mathbf{orb}_1(H') > i = \mathbf{fld}(H) - \mathbf{orb}_1(H)$. Otherwise $\mathbf{orb}_1(H') \geq i$ so $\mathbf{fld}(H') - \mathbf{orb}_1(H') \leq i$ and (as explained above) we have $i = \mathbf{fld}(H) - \mathbf{orb}_1(H) \leq \mathbf{fld}(H') - \mathbf{orb}_1(H')$, so $\mathbf{fld}(H) - \mathbf{orb}_1(H) = \mathbf{fld}(H') - \mathbf{orb}_1(H')$ and hence $\mathbf{fld}(H) = \mathbf{fld}(H')$ and $\mathbf{orb}_1(H) = \mathbf{orb}_1(H')$. Hence, in any case (using that $\mathbf{orb}_2(H) = 2i^2$ and that $\mathbf{orb}_2(H') < 2i^2$ if $\mathbf{orb}_1(H') \geq i$), Proposition 2.6 (iii) implies that $\left|\mathbf{S}_n(\mathcal{A}', H')\right| \Big/ \left|\mathbf{S}_n(\mathcal{A}, H)\right| \to 0$ as $n \to \infty$. (The assumption that $\mathbf{ari}(V) > 2$ is used in the application of Proposition 2.6 (iii).) By Lemma 2.9, almost all $\mathcal{M} \in \mathbf{S}(\mathcal{A}, H)$ have the property that the number of orbits of $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M})$ on $\mathrm{Spt}^*(\mathcal{M})$ is $\mathbf{orb}_1(H) = i$ and the number of orbits of $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M})$ on $\mathrm{Spt}^*(\mathcal{M}) \times \mathrm{Spt}^*(\mathcal{M})$ is $\mathbf{orb}_2(H) = 2i^2$. Now the lemma follows, because $\mathbf{S}(\mathrm{spt}^* = 2i)$ is a union of finitely many sets of the form $\mathbf{S}(\mathcal{A}, H)$ where the universe of $\mathcal{A}$ has cardinality $2i$, $\mathcal{A}$ has no fixed point and H is subgroup of $\mathrm{Aut}(\mathcal{A})$ without fixed point. □

Lemma 4.2. *Suppose that* $\mathbf{ari}(V) \geq 3$ *and* $i \geq 1$. *For almost all* $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 2i)$, $\mathrm{Aut}(\mathcal{M}) \cong \mathbb{Z}_2$.

Proof. Since $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M}) \cong \mathrm{Aut}(\mathcal{M})$ it suffices to prove that for almost all $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 2i)$, $\mathrm{Aut}(\mathcal{M}) \restriction \mathrm{Spt}^*(\mathcal{M}) \cong \mathbb{Z}_2$. By Lemmas 2.10 and 4.1 it suffices to prove that if H is a permutation group on $[2i]$ such that every orbit of H on $[2i]$ has cardinality 2 and every orbit of H on $[2i] \times [2i]$ has cardinality 2, then $H \cong \mathbb{Z}_2$. This is obvious if $i = 1$, so for the rest of the proof we assume that $i \geq 2$.

So suppose that H is a permutation group on $[2i]$ such that every orbit of H on $[2i]$ has cardinality 2 and every orbit of H on $[2i] \times [2i]$ has cardinality 2. We first prove an auxilliary claim.

Claim. If a and b belong to different orbits of H on $[2i]$ and $f \in H$ is not the identity, then $\{f(a), f(b)\} \cap \{a, b\} = \emptyset$.

Proof. Suppose for a contradiction that the claim does not hold. Then there are orbits $\{a, c\}, \{b, d\} \subseteq [2i]$ and a permutation $f \in H$ such that $f(a) = c$ and $f(b) = b$. Then $f(d) = d$ and as $\{b, d\}$ is an orbit there is $g \in H$ such that $g(b) = d$ and $g(d) = b$. If $g(a) = a$ then $\{a, c\} \times \{b, d\}$ is an orbit of H on $[2i] \times [2i]$, contradicting the assumption that all orbits on $[2i] \times [2i]$ have cardinality 2. Hence $g(a) = c$ and $g(c) = a$. Then $gf(a) = a$ and $gf(b) = d$ and again, by the use of f, gf and compositions of them, it follows that $\{a, c\} \times \{b, d\}$ is an orbit, contradicting our assumption. □

Now we prove that if $f \in H$ is not the identity, then f has no fixed point. Suppose, for a contradiction, that $f \in H$ is not the identity and has a fixed point a. As the orbit to which a belongs, say $\{a, c\}$, has cardinality 2 and we assume that $i \geq 2$ it follows that there is $b \in [2i] \setminus \{a, c\}$ such that $f(b) \neq b$. Then we have $a = f(a) \in \{f(a), f(b)\} \cap \{a, b\}$, contradicting the claim.

Next, we prove that H has a unique nonidentity permutation from which it follows that $H \cong \mathbb{Z}_2$. So suppose for a contradiciton that $f, g \in H$ are nonidentity permutations and $f(a) \neq g(a)$ for some a. Then $a, f(a)$ and $g(a)$ belong to the same orbit. Since neither f nor g has any fixed point, as we proved above, some orbit of H on $[2i]$ contains at least three elements, contradicting our assumption. □

The next result deals only with permutation groups and is independent of the ingredients from formal logic such as relation symbols and their interpretations.

Lemma 4.3. *Suppose that $i \geq 2$. Let H be a permutation group without fixed points on $[2i+1]$ such that H has exactly $i-1$ orbits of cardinality 2, exactly one orbit of cardinality 3 and no other orbits. If $\mathbf{orb}_2(H)$ is maximal among all H subject to the given constraints, then $H \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbf{orb}_2(H) = 2i^2 - 2i + 3$.*

Proof. Suppose that H is a permutation group without fixed points on $[2i+1]$ such that H has exactly $i-1$ orbits of cardinality 2, exactly one orbit of cardinality 3 and no other orbits. Let $O_1, \ldots, O_{i-1}$ be the orbits with cardinality 2 and let O_i be the orbit with cardinalty 3. Let $\Omega = O_1 \cup \ldots \cup O_{i-1}$. It is easy to see that there is $f \in H \restriction O_i$ without any fixed point. From this it is straightforward to check that the number of orbits of $H \restriction O_i$ on $O_i \times O_i$ is at most 3; indeed if we take distinct $a, b \in O_i$, then $O_i \times O_i$ is the union of the following orbits (which may coincide): one orbit containing (a, a), one orbit containing (a, b), and one orbit containing (b, a).

We first show that if $H \restriction \Omega \cong \mathbb{Z}_2$, $H \restriction O_i \cong \mathbb{Z}_3$ and $H \cong (H \restriction \Omega) \times (H \restriction O_i)$, then $\mathbf{orb}_2(H) = 2i^2 - 2i + 3$. So suppose that $H \restriction \Omega \cong \mathbb{Z}_2$. Then $H \restriction \Omega$ has exactly $i-1$ orbits on Ω, each one of cardinality 2, and $H \restriction \Omega$ has exactly $2(i-1)^2$ orbits on $\Omega \times \Omega$. Now suppose that $H \restriction O_i \cong \mathbb{Z}_3$. Then it is easy to see that no $f \in H \restriction O_i$ other than the identity has a fixed point in O_i and therefore $H \restriction O_i$ has exactly 3 orbits on $O_i \times O_i$. Suppose, in addition to previous assumptions and conclusions, that $H \cong (H \restriction \Omega) \times (H \restriction O_i)$. Then it easily follows that for every $j = 1, \ldots, i-1$, $O_j \times O_i$ and $O_i \times O_j$ are orbits of H on $[2i+1] \times [2i+1]$. Hence, the number of orbits of H on $[2i+1] \times [2i+1]$ which contain (a, b) such that $a \in \Omega$ and $b \in O_i$, or vice versa, is $2(i-1)$. Altogether, we get

$$\mathbf{orb}_2(H) \; = \; 2(i-1)^2 + 3 + 2(i-1) \; = \; 2i^2 - 2i + 3.$$

We now show that if $\mathbf{orb}_2(H)$ is maximal among all H subject to the given constraints in the lemma, then $H \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. This will conclude the proof.

So suppose that $\mathbf{orb}_2(H)$ is maximal among all permutation groups on $[2i+1]$ without fixed points and with exactly $i-1$ orbits of cardinality 2, exactly one orbit of cardinality 3 and no other orbits. As before, let $O_1, \ldots, O_{i-1}$ be the orbits with cardinality 2, let O_i be the orbit with cardinalty 3 and let $\Omega = O_1 \cup \ldots \cup O_{i-1}$. By the same argument as in the proof of Lemma 3.2 there exists $f \in H$ without any fixed point in O_i, and then, just as in that proof, it follows that for every $j = 1, \ldots, i-1$, $O_j \times O_i$ and $O_i \times O_j$ are orbits of H on $[2i+1] \times [2i+1]$. Hence the number of orbits of H on $[2i+1] \times [2i+1]$ that contain a pair (a, b) such that $a \in \Omega$ and $b \in O_i$, or vice versa, is at most $2(i-1)$. The number of orbits of H on $[2i+1] \times [2i+1]$ that contain a pair (a, b) where $a, b \in \Omega$ is at most $(2(i-1))^2/2 = 2(i-1)^2$, because every orbit has at least two members. As explained in the beginning of the proof, the number of orbits of H on $[2i+1] \times [2i+1]$ that contain a pair (a, b) where $a, b \in O_i$ is at most 3. This means that

$$\mathbf{orb}_2(H) \; \leq \; 2(i-1) + 2(i-1)^2 + 3 \; = \; 2i^2 - 2i + 3.$$

By the assumption that $\mathbf{orb}_2(H)$ is maximal and since the value $2i^2 - 2i + 3$ can be reached, as shown above, we get $\mathbf{orb}_2(H) = 2i^2 - 2i + 3$. From the argument above it follows that $\mathbf{orb}_2(H)$ cannot be maximal unless $H\restriction\Omega$ has a maximal number of orbits on $\Omega \times \Omega$. Hence $H\restriction\Omega$ must have the maximal possible number of orbits on $\Omega \times \Omega$ which is $(2(i-1))^2/2 = 2(i-1)^2$ and consequently every orbit of $H\restriction\Omega$ on $\Omega \times \Omega$ has cardinality 2. By the argument in the proof of Lemma 4.2 it follows that $H\restriction\Omega \cong \mathbb{Z}_2$.

We have seen that $H\restriction O_i$ can have at most 3 orbits on $O_i \times O_i$. Also it is easy to see that $H\restriction O_i$ has 3 orbits on $O_i \times O_i$ if and only if for any distinct $a, b \in O_i$, (a, b) and (b, a) belong to different orbits. Moreover, if for any distinct $a, b \in O_i$, (a, b) and (b, a) belong to different orbits, then no $f \in H\restriction O_i$ has order 2, so $H\restriction O_i \cong \mathbb{Z}_3$.

By the same argument as in the proof of Lemma 3.2, using only the assumptions about the orbits of H on Ω, it follows that $H \cong (H\restriction\Omega) \times (H \restriction O_i) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. □

Lemma 4.4. *Suppose that* $\mathbf{ari}(V) \geq 3$.
(i) For almost all $\mathcal{M} \in \mathbf{S}_n(\mathrm{spt}^* = 3)$, $\mathrm{Aut}(\mathcal{M}) \cong \mathbb{Z}_3$.
(ii) If $i \geq 2$ *then for almost all* $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 2i+1)$, $\mathrm{Aut}(\mathcal{M}) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ *and* $s\big(\mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})\big) = 2i^2 - 2i + 3$.

Proof. We start with part (ii), so suppose that $i \geq 2$. Suppose that $\mathcal{A} \in \mathbf{S}_{2i+1}$ has no fixed point and suppose that H is a subgroup of $\mathrm{Aut}(\mathcal{A})$ without fixed point. Note that $\mathbf{fld}(H) = 2i+1$. We have seen, in the proof of Lemma 2.10 (ii), that $\mathbf{fld}(H) - \mathbf{orb}_1(H)$ is minimal when $\mathbf{orb}_1(H) = i$ (under the assumption that H acts on a set of cardinality $2i+1$ and has no fixed points), which implies that H has $i-1$ orbits of cardinality 2 and one orbit of cardinality 3. Also, recall Definition 2.5 of $\beta(x, y, z)$ and the notation from the introduction and preliminaries. Observe that if we let

$$r = \mathbf{ari}(V), \quad k = N_{\max}, \quad l = N_{\max-1},$$
$$p = \mathbf{fld}(H) = 2i+1, \quad q = \mathbf{orb}_1(H) = i \quad \text{and} \quad s = \mathbf{orb}_2(H), \quad \text{then}$$

$$\beta(p,q,s) \;=\; k\binom{r}{2}(2i+1)^2 \;-\; kr(r-1)(2i+1)i \;-\; l(r-1)(2i+1) \;+\; l(r-1)i \;+\; k\binom{r}{2}s,$$

where r, k, l and i are fixed parameters. So under the assumptions that $\mathbf{fld}(H) = 2i+1$ and $\mathbf{orb}_1(H) = i$, $\beta(p, q, s)$ is maximised when $s = \mathbf{orb}_2(H)$ is maximised. From Proposition 2.6 (iii) and the fact that $\mathbf{S}(\mathrm{spt}^* = 2i+1)$ is a union of finitely many sets of the form $\mathbf{S}(\mathcal{A}, H)$, where $\mathcal{A} \in \mathbf{S}_{2i+1}$, $\mathcal{A}$ has no fixed point and H is a subgroup of $\mathrm{Aut}(\mathcal{A})$ without any fixed point, it follows that almost every $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 2i+1)$ has the following properties: $H = \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ has exactly i orbits ($i-1$ of cardinality 2 and one of cardinality 3) and $\mathbf{orb}_2(H)$ is maximal among all permutation groups on $[2i+1]$ with i orbits and without a fixed point. From Lemma 4.3 it now follows that for almost every $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 2i+1)$, $\mathrm{Aut}(\mathcal{M}) \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ and $s\big(\mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})\big) = 2i^2 - 2i + 3$.

Now we consider part (i). If $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = 3)$ and $H = \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ then $\mathbf{fld}(H) = 3$ and $\mathbf{orb}_1(H) = 1$. So the question is what $H = \mathrm{Aut}(\mathcal{M})\restriction\mathrm{Spt}^*(\mathcal{M})$ looks like when $\mathbf{orb}_2(H)$, the number of orbits on $\mathrm{Spt}^*(\mathcal{M}) \times \mathrm{Spt}^*(\mathcal{M})$, is maximised. It is easy to see that $\mathbf{orb}_2(H) \leq 3$, and $\mathbf{orb}_2(H) = 3$ if and only if $H \cong \mathbb{Z}_3$. (We argued similarly in Lemma 4.3.) □

From Lemmas 4.2 and 4.4 we get the following:

Corollary 4.5. *Suppose that* $\mathbf{ari}(V) \geq 3$ *and* $m \geq 2$. *Almost every* $\mathcal{M} \in \mathbf{S}(\mathrm{spt}^* = m)$ *has an automorphism whose support has cardinality* m.

Lemma 4.6. *Suppose that* $i \geq 1$ *and* $\mathbf{ari}(V) \geq 3$. *Then*

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i+1)\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i)\big|} \;=\; 0.$$

Proof. Exactly as the proof of Lemma 3.4. □

Lemma 4.7. *If $\beta(x,y,z)$ is defined as in Definition 2.5, then*

$$\beta(2i+2,\ i+1,\ 2(i+1)^2) \ - \ \beta(2i+1,\ i,\ 2i^2-2i+3) \ = \ 2k\binom{r}{2}(2i-1).$$

Proof. Straightforward, but long, calculation. □

Lemma 4.8. *If $\mathbf{ari}(V) \geq 3$ and $i \geq 1$ then*

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i+1)\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* = 2i+2)\big|} \ = \ 0.$$

Proof. By Lemmas 2.10 and 4.1, for almost all $\mathcal{M} \in \mathbf{S}_n(\mathrm{spt}^* = 2i+2)$, if $H = \mathrm{Aut}(\mathcal{M})\restriction \mathrm{Spt}^*(\mathcal{M})$ then $p := \mathbf{fld}(H) = 2i+2$, $q := \mathbf{orb}_1(H) = i+1$ and $s := \mathbf{orb}_2(H) = 2(i+1)^2$. By Lemmas 2.10 and 4.4, for almost all $\mathcal{M}' \in \mathbf{S}_n(\mathrm{spt}^* = 2i+1)$, if $H' = \mathrm{Aut}(\mathcal{M}')\restriction \mathrm{Spt}^*(\mathcal{M})$ then $p' := \mathbf{fld}(H') = 2i+1$, $q' := \mathbf{orb}_1(H') = i$ and $s' := \mathbf{orb}_2(H') = 2i^2 - 2i + 3$. For such H and H' we have

$$p - q \ = \ i+1 \ = \ p' - q'$$

and by Lemma 4.7 we also have

$$\beta(p,q,s) \ > \ \beta(p',q',s'),$$

so Lemma 4.8 follows from Proposition 2.6 (iii). □

Lemma 4.9. *Suppose that $\mathbf{ari}(V) \geq 3$ and either $m = 0$ or $m \geq 2$. Then*

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = m+2)\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* = m)\big|} \ = \ 0.$$

Proof. Exactly as the proof of Lemma 3.6. □

Lemma 4.10. *Suppose that $\mathbf{ari}(V) \geq 3$ and suppose that $m = 0$ or $m \geq 2$. Let $m' = m$ if m is even and $m' = m+1$ otherwise. Then For every integer T such that $T > m$ and $T \geq 2$,*

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = m')\big|}{\big|\mathbf{S}_n(m \leq \mathrm{spt}^* \leq T)\big|} \ = \ 1.$$

Proof. As the proof of Lemma 3.7, but now using Lemmas 4.6, 4.8 and 4.9. □

Lemma 4.11. *Suppose that $\mathbf{ari}(V) \geq 3$ and $m \geq 2$. Let $m' = m$ if m is even and $m' = m+1$ otherwise. Then*

$$\lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt} \geq m) \cap \mathbf{S}_n(\mathrm{spt}^* = m')\big|}{\big|\mathbf{S}_n(\mathrm{spt} \geq m)\big|} \ = \ \lim_{n\to\infty} \frac{\big|\mathbf{S}_n(\mathrm{spt}^* = m')\big|}{\big|\mathbf{S}_n(\mathrm{spt}^* \geq m)\big|} \ = \ 1.$$

Proof. Like the proof of Lemma 3.8, but now using Corollary 4.5 and Lemma 4.10. □

By combining Lemmas 4.2 and 4.11 we get Theorem 1.2.

References

[1] O. Ahlman, V. Koponen, Limit laws and automorphism groups of random nonrigid structures, accepted for publication in *Journal of Logic and Analysis*. Preprint online: `http://arxiv.org/abs/1305.3097`

[2] J. D. Dixon, B. Mortimer, *Permutation Groups*, Springer-Verlag (1996).

[3] H-D Ebbinghaus, J. Flum, *Finite Model Theory*, Second Edition, Springer-Verlag (1999).

[4] P. Erdős, A. Rényi, Asymmetric graphs, *Acta Math. Acad. Sci. Hungar.*, Vol. 14 (1963) 295-315.

[5] R. Fagin, The number of finite relational structures, *Discrete Mathematics*, Vol. 19 (1977) 17–21.

[6] G. W. Ford, G. E. Uhlenbeck, Combinatorial problems in the theory of graphs. IV, *Proceedings of the National Academy of Sciences*, Vol. 43 (1957) 163–167.
[7] F. Harary, Note on Carnap's relational asymptotic relative frequencies, *The Journal of Symbolic Logic*, Vol. 23 (1958) 257-260.
[8] W. Oberschelp, Strukturzahlen in endlichen Relationssystemen, in: H. A. Schmidt et. al. eds. *Contributions to Mathematical Logic*, Proceedings of 1966 Logic Colloquium, North-Holland (1968) 199–213.
[9] Ph. Rothmaler, *Introduction to Model Theory*, Taylor & Francis (2000).

Vera Koponen, Department of Mathematics, Uppsala University, Box 480, 75106 Uppsala, Sweden.
E-mail address: vera@math.uu.se