Information transmission, holographic defect detection and signal permutation in active flow networks

Francis G. Woodhouse, Joanna B. Fawcett, and Jörn Dunkel

Department of Applied Mathematics and Theoretical Physics, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, U.K.

Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, U.K.

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge MA 02139-4307, U.S.A.

(Dated: May 2, 2017)

Active networks driven by local energy conversion are ubiquitous in nature, yet little is known about how information propagates through these far-from-equilibrium systems. Through a mathematical analogy with spin-ice vertex models, we investigate here the input-output characteristics of generic incompressible active flow networks (AFNs). Our analysis shows that information transport through an AFN is inherently different from conventional pressure or voltage driven networks. Active flows on hexagonal arrays preserve input information over longer distances than their passive counterparts and are highly sensitive to bulk topological defects, which can be inferred holographically from marginal input-output distributions. This sensitivity further allows controlled permutations on parallel inputs, revealing an unexpected link between active matter and group theory that can guide new microfluidic mixing strategies facilitated by active matter and aid the design of generic autonomous information transport networks.

INTRODUCTION

Group theory forms the mathematical foundation of ancient cryptography. Systematic permutations of the symbols in a given alphabet define the most basic algorithms for encoding information. The efficiency and robustness of such encryption schemes is tightly linked to the structural properties of the underlying permutation groups. This profound connection was first realized by the Polish mathematician Marian Rejewski in 1932 and, a few years later, used by Alan Turing to decipher codes produced by the Enigma machine, a mechanical encoding device employed by the German Army during WWII. Nowadays, information transfer and encryption assume ever-increasing importance in the development of new technologies, from the internet and smart phones to quantum communication. Yet, information transport is also a salient feature of many, if not all, biological systems. This raises interesting conceptual and practical questions as to whether one can use biological or engineered active matter components to transport and encrypt information, and how efficiently such active information transportation devices can operate relative to conventional passive information flow networks.

Here, we explore these questions theoretically by focusing on quasi-incompressible active flow networks (AFNs) that can be realized with dense suspensions of bacteria or other types of natural or engineered microswimmers. In contrast to voltage-driven electric or pressure-driven microfluidic circuits, material and information transport in AFNs is facilitated by the conversion of chemical energy into kinetic energy at the level of the microscopic constituents, such as bacteria or Janus particles, which can carry information individually or collectively. Building on a mathematical correspondence with discrete spin-ice vertex models, we will investigate the similarities and differences between the propagation of input signals through internally driven active and externally driven passive flow networks for different lattice geometries. This analysis shows that topological constraints intrinsic to incompressible AFNs enable more robust information flow than in comparable passive networks. In the second part, we will demonstrate how bulk topological defects in AFN lattices can be detected holographically from input–output correlations and can be utilized to realize specific permutation groups. In doing so, we will establish a fundamental connection between active matter flows in complex topologies and the Cayley graph structure of permutation groups. We conclude by showing how these ideas can be extended to general random graphs to achieve more efficient signal coding. These results will lay the conceptual foundation for the implementation of encryption and mixing strategies using active matter-based devices.

RESULTS AND DISCUSSION

Active matter vertex models

To model an AFN—that is, a network of narrow channels filled with incompressible active matter—we adopt a coarse-grained approach, employing a pseudo-
equilibrium approach. Define the energy of a configuration through geometric channel patterning \[29\]. This is then augmented with input–output capability through boundary vertices whose mass flux is either controlled, for inputs, or free, for outputs, in contrast to the mass-conserving internal vertices at which the self-organized flows of active matter interact \[15\]. This is formalized as follows.

Let \( \Gamma \) be a graph with edge set \( E \) and vertex set \( V \cup \partial \Gamma \), where \( V \) is the set of interior vertices and \( \partial \Gamma \) are degree-1 boundary vertices used as inputs and outputs. Every edge \( e \in E \) is assigned an arbitrary orientation, from which we define the \(|V| \times |E|\) incidence matrix \( D = [D_{ve}] \) where \( D_{ve} = -1 \) if edge \( e \) is oriented outwards from vertex \( v \), \( +1 \) if \( e \) points into \( v \), and \( 0 \) if \( v \) and \( e \) are not incident. A flow configuration \( \Phi = (\phi_e) \) on \( \Gamma \) is then a vector of signed flows \( \phi_e \in \{-1, 0, +1\} \) along each \( e \in E \), where \( \phi_e = +1 \) represents flow with the orientation of \( e \) and \( \phi_e = -1 \) is flow against the orientation of \( e \), so that the flux into vertex \( v \) along edge \( e \) is \( f_{ve} = D_{ve} \phi_e \).

The space of permissible flows \( \Phi \) is constrained by flux conservation, through which we implement inputs and outputs. Every internal vertex \( v \in V \) must have as many in-flows as out-flows, corresponding to the flux incompressibility condition
\[
\sum_e f_{ve} = (D \cdot \Phi)_v = 0.
\]

Inputs and outputs are set and read through the flux at the boundary vertices \( \partial \Gamma = \partial \Gamma_{\text{in}} \cup \partial \Gamma_{\text{out}} \). For a given digital input vector \( I = (I_v) \in \{0, 1\}^{\partial \Gamma_{\text{in}}} \) we impose that the vertex \( v \in \partial \Gamma_{\text{in}} \) corresponding to input \( I_v \) have net flux
\[
\sum_e f_{ve} = (D \cdot \Phi)_v = -I_v,
\]
so that an activated input injects matter into the network. Output vertices, on the other hand, are left unconstrained to allow matter to flow out of them or not as network interactions dictate; the output vector \( O = (O_v) \in \{0, 1\}^{\partial \Gamma_{\text{out}}} \) for flow state \( \Phi \) is then read off as the flow
\[
O_v \equiv \sum_e f_{ve} = (D \cdot \Phi)_v,
\]
through each \( v \in \partial \Gamma_{\text{out}} \). Finally, to prevent spurious matter inflow through the outputs, we impose that each edge \( e \) incident to an output vertex (of which there is one per output, as outputs have degree 1) only permit flow toward the output, \( \phi_e \in \{0,+1\} \). In microfluidic realizations, such an active matter diode can be realized through geometric channel patterning \[29\].

To model the spontaneous self-organized flow typical of active matter \[18 19 23 30\], we adopt a pseudo-equilibrium approach. Define the energy of a configuration \( \Phi \) to be
\[
H(\Phi) = -\frac{1}{12} \lambda \sum_{e \in E} |\phi_e|,
\]
with polarization strength constant \( \lambda \) (where the factor of \( 1/12 \) is for consistency with previous continuum models \[28\]). For a fixed input vector \( I \) we then assume a pseudo-equilibrium model selecting states according to the Boltzmann distribution \( p(\Phi|I) \propto e^{-\beta H(\Phi)} \) subject to the incompressibility and input–output constraints. This favors configurations with more flowing edges, as we might expect from active matter systems in confinement \[19 22 30 31\]. The result is a form of vertex model on general graphs in the same family as ice-type or loop models \[32 35\], endowed with input–output capability, which qualitatively replicates the full continuous lattice field model of Ref. \[28\] (SM Text).

States comprise flowing edges with \( |\phi_e| = 1 \) and non-flowing edges with \( \phi_e = 0 \), with flows balanced at every internal vertex and flow out of each activated input. If we now restrict \( \Gamma \) to have vertices of degree at most 3, then incompressibility implies that flows become mutually excluding: each internal vertex must have either zero flowing edges or two flowing edges, one in and one out, so stable states comprise non-intersecting flow paths from each activated input to an output with the remaining edges filled by non-intersecting closed cycles of flow (Fig. 1A,B). Since this is where topology design has the greatest potential impact on active flow, we restrict attention to this case here. We also confine ourselves to the low-noise regime \((\beta \lambda)^{-1} \ll 1\) where appropriate, relevant for strongly confined active matter in a well-controlled environment \[19 23 30\].

**Topologically protected information transport**

Active flow networks display markedly different characteristics compared to passive pressure-driven flows or simple random walks. This is best explored in a lattice topology. Let \( \Gamma \) be an \( M \times N \) hexagonal lattice with \( N \) inputs and \( N \) outputs labelled \( i = 1, \ldots, N \), as in Fig. 1A. We refer to the number \( M \) of lattice layers between the inputs and the outputs as the depth of \( \Gamma \). When one input is activated, the AFN picks out a distinct path from the input to an output, with any remaining space filled with vertex-disjoint closed cycles (Fig. 1A). The particular output chosen is probabilistic \[12\], and taking an ensemble average (or time average, if dynamics are specified) yields a probability distribution \( p(j|i) = P(O_j = 1|I_i = 1) \) for the output from a given input (Fig. 1A). This can then be compared to the steady output flux in an equivalent microfluidic network having fixed inflow \( I \) on \( \partial \Gamma_{\text{in}} \), zero pressure on \( \partial \Gamma_{\text{out}} \),
and equal resistance on every edge, or, equivalently, the steady-state probability distribution of a symmetric random walk starting at input $i$ with sinks at the outputs $R$. These have the same matter or probability flux as the active flow network, and we henceforth combine them under the umbrella of ‘passive flow.’ While passive flow from a single input disperses among all output nodes, the equivalent ensemble-averaged output distribution from the AFN instead still retains a distinct signature of its input for larger lattices where passive output is near-uniform (Fig. 1C). Thus, the globally exploratory nature of active network flow allows for output from a non-trivial active network to be traceable to the original input, whereas passive flow is virtually untraceable on all lattices.

When multiple inputs are activated, the vertex-disjoint input–output paths mutually exclude one another in AFNs. This alters the output distribution in a fashion dependent on the graph topology, offering additional control over signal propagation compared with passive networks. Furthermore, the discrete nature of active flow means that each input can be traced to its output without visualizing the intervening network by distinctly marking the input flows. For a planar network such as that in Fig. 1, the order of the outputs must match the order of the inputs: if input 1 is activated and connects to output 3, say, then input 2 can only connect to output 4 onwards (Fig. 1B), in stark contrast to the linearity of passive network flow. This suggests that active flows may be particularly adept at retaining input configuration memory when more than one input is activated.

The extent to which inputs can be inferred from outputs is captured by the mutual information $I(X;Y)$. Suppose we uniformly at random choose one input $X$ to activate. This connects to one output $Y$ according to a topology-dependent probability distribution $p(y|x)$ (Fig. 1C). If we
can only measure the output and do not know which input was activated, then how well the activated input can be inferred from an observed output is described by the 1-input relative mutual information (SM Text)

\[ U_1(X|Y) = \frac{1}{N \log N} \sum_{x,y} p(y|x) \log \left( \frac{p(y|x)}{p(y)} \right). \]

This measures the information gained relative to the maximum possible \( \log_2 N \) bits, so that \( U_1 = 1 \) means exact input–output matching and \( U_1 = 0 \) means input and output are independent. The equivalent notion of output observation in the case of passive flow is that of seeing a single random walker arrive at an output for random walks, or observing the destination of a single input tracer particle in pressure-driven microfluidic flow. Numerically evaluating \( U_1 \) over a range of hexagonal lattice sizes shows that AFNs preserve input information over notably larger graphs than passive flow (Fig. 1D), allowing the activated input to be inferred with high confidence using comparatively few system samples.

With two labelled inputs activated, mutual information \([38]\) captures a fundamental difference between AFNs and classical flow. The randomly chosen activated inputs \( X_1 \) and \( X_2 \) are now represented by an ordered pair \( X = (X_1, X_2) \) with \( X_1 \neq X_2 \), where \( X_1 \) is labelled red and \( X_2 \) is labelled blue, say. This yields an output pair \( Y = (Y_1, Y_2) \), where \( Y_1 \) is the output observed red and \( Y_2 \) the output observed blue, again sampled from a distribution \( p(y|x) \). The two-input relative mutual information is then (SM Text)

\[ U_2(X|Y) = \frac{1}{N(N-1) \log N(N-1)} \sum_{x,y} p(y|x) \log \left( \frac{p(y|x)}{p(y)} \right), \]

where the modified prefactor reflects the \( N(N-1) \) possible labelled input pairs. Evaluating \( U_2 \) for AFNs and classical flow (Fig. 1E) now yields a qualitative distinction: not only do AFNs preserve information better on larger graphs, as with one input, but \( U_2 \) asymptotes to a non-zero constant \( 1/\log_2 N(N-1) \). This is because mutual exclusion of input–output streams in planar networks means that these AFNs preserve the ordering of their inputs, implying a guaranteed bit of information for even the largest planar lattices.

With regard to applications, the partial topological protection of input–output correlations in planar AFNs suggests interesting possibilities for tuning and enhancing information propagation through the inclusion of auxiliary control currents. Moreover, as we shall show next, it also allows holographic detection of non-planar lattice defects from input and output distributions alone.

**FIG. 2.** Holographic detection of lattice defects. (A) Example active flow on a 5 × 5 lattice with 3 activated inputs. (B) Joint distribution \( p(x,y,z) \) of activated outputs \( 2 \rightarrow X, 3 \rightarrow Y, 4 \rightarrow Z \) for the three activated inputs 2, 3, 4 in (A) at low noise \((2\lambda)^{-1} = 0.02\), shown by the three marginal densities derived from summing over one each of \( X, Y \) and \( Z \) as determined by exhaustive evaluation (SM Text). Grey cells indicate topologically prohibited output orderings violating \( X < Y < Z \). (C) As in (A) but for a lattice with a planarity defect, allowing input–output streams to cross. (D) Output densities as in (B) but now for the defective lattice in (C), demonstrating non-zero probabilities in regions of the distribution previously prohibited by topology.

**Holographic defect detection**

If \( \Gamma \) is not planar then input streams can cross, yielding qualitative changes in the joint distribution of output probabilities compared to that of a similar planar graph. Suppose, for instance, that inputs 2, 3 and 4 are activated on the 5 × 5 hexagonal lattice of Fig. 2A. Denoting the activated inputs’ respective random outputs by \( X, Y \) and \( Z \), planarity of the lattice means that we must always have \( X < Y < Z \) (under our labeling of inputs and outputs as in Fig. 2A). This implies that the joint distribution \( p(x,y,z) = P(2 \rightarrow x, 3 \rightarrow y, 4 \rightarrow z) \) is only non-zero in the small subspace \( x < y < z \) (Fig. 2B). Now, introduce a small planarity defect into the lattice by exchanging endpoints between two horizontal edges of one hexagon (Fig. 2C), akin to the rewiring construction of Watts–Strogatz networks [39]. Two input–output streams can now cross once, allowing output ordering to change and thereby introducing non-zero probabilities within previously prohibited regions of \( p(x,y,z) \) (Fig. 2D). This holographic reflection of bulk lattice

![Fig. 2](https://via.placeholder.com/150)
structure in the surface marginals presents a planarity rejection test if the intervening graph is unknown or difficult to embed.

**Realizing permutation groups with active flows**

Activating all inputs of a hexagonal lattice with crossover defects results in a stochastic permutation device. In this case, since there are as many outputs as inputs, each permissible flow configuration defines a bijection \(f: \{1, \ldots, N\} \rightarrow \{1, \ldots, N\}\) (that is, a permutation of the integers 1 to \(N\)) where input \(i\) connects to output \(f(i)\). If the stream at input \(i\) is then given label \(v_i\), this arrives at output \(f(i)\). Denoting the vector of all input labels by \(v = (v_i)\) and the vector of output labels by \(w = (w_j)\), where \(w_j\) is the label read at output \(j\), any such permutation can be compactly written as \(w = \sigma v\) for some unique invertible permutation matrix \(\sigma\) \[^{1,2}\]. Now, without any crossover defects, planarity implies that the only possible \(\sigma\) is the identity map, since flows cannot swap due to the complete topological protection in this case. However, introducing crossover defects makes non-trivial \(\sigma\) possible. In general, an output configuration of such an AFN consists of a permutation \(\sigma \in \Sigma\) randomly chosen from the set \(\Sigma\) of all possible permutations, where \(\Sigma\), and each permutation’s selection probability, is defined by the placement of interior defects. Furthermore, when all inputs are activated, the lattice topology implies that permissible flow configurations \(\Phi\) all have the same number of flowing edges and hence the same energy \(H(\Phi)\). The Boltzmann distribution \(\propto e^{-\beta H(\Phi)}\) is therefore uniform, rendering the flow states and permutation selection probabilities independent of the noise strength \((\beta \lambda)^{-1}\) for these lattices.

As an example, consider the 1-defect lattice in Fig. 2A. When all inputs are activated, this can realize three different permutations \(f\), mapping \((1,2,3,4,5)\) to one of \((1,2,3,4,5)\), \((1,3,2,4,5)\) or \((2,1,3,4,5)\). These are, respectively, the identity and the transpositions \((23)\) and \((12)\) in group-theoretic cycle notation \[^2\]. Thus, this lattice has a set \(\Sigma = \{\sigma_1, \sigma_2, \sigma_3\}\) of three possible matrices representing these permutations acting on the input vector \(v\). The first is the 5 \(\times\) 5 identity matrix \(I_5\), while the second and third read

\[
\sigma_2 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}, \quad \sigma_3 = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}. \quad \text{(1)}
\]

These have respective selection probabilities \(p_1 = 1/3\), \(p_2 = 1/2\) and \(p_3 = 1/6\), as computed by exhaustive evaluation (SM Text).

In many technological applications, including material mixing and signal encoding, one is interested not in generating a few particular permutations but instead in realizing an entire permutation group. For instance, perhaps we wish to employ a microfluidic AFN to combine all five components. If we want this to occur in any random order at all, the full symmetric group \(S_5\) is called for; alternatively, we may have certain restrictions on ordering—objects 1 to 3 must precede objects 4 and 5, say—necessitating subgroups of \(S_5\) acting on those five objects. This can be compactly achieved by concatenation of an AFN with copies of itself. Repeatedly chaining together a small hexagonal lattice containing one or more crossover defects (Fig. 3A) causes the input flows to repeatedly permute, akin to a braid \[^{10,11}\]\[^2\], realizing different permutation groups according to the lattice defect structure. Formally, because label permutation \(\sigma v\) obeys (matrix) composition \((\tau \circ \sigma)v = \tau(\sigma v)\), passing the outputs of an AFN \(\Gamma\) straight into the inputs of a copy of \(\Gamma\) gives a new AFN with permutation set \(\Sigma^2 = \{\sigma \tau : \sigma, \tau \in \Sigma\}\) built from all pairwise products of elements in \(\Sigma\). Concatenating a further copy of \(\Gamma\) yields an AFN with set \(\Sigma^3 = \{\rho \sigma \tau : \rho, \sigma, \tau \in \Sigma\}\), and

![FIG. 3. Realizing permutation groups through AFN concatenation. (A) Example flow through a 3-fold concatenation of a 3 \(\times\) 5 hexagonal lattice with 3 planarity defects, realizing the permutation (12)(45) as the composition (23)(45) \(\circ\) (2345) \(\circ\) (12)(45). (B) Groups converged on by repeated concatenation of a 3 \(\times\) 5 lattice with between 1 to 5 defects. Group frequencies are shown as their likelihood of occurrence from random defect placements, determined over all possible configurations with each number of defects. The permutation set for each graph was found by exhaustive evaluation from which the group convergence was then evaluated (SM Text). ‘∅’ denotes non-convergence in repeated concatenation.]
so on. This process either converges, in that there exists an $s$ such that $\Sigma^n = \Sigma^s$ for all $n \geq s$, or eventually results in a repeating periodic sequence of permutation sets. In general, concatenation converges when $\Sigma^k \subseteq \Sigma^{k+1}$ for some $k$, in which case it must converge on a group (SM Text). Alternatively, Markov chain theory yields a geometric condition: concatenation converges precisely when the Cayley graph generated by $\Sigma$ contains a set of cycles whose lengths have a greatest common divisor of 1. The underlying proofs, whose details are given in the SM Text, establish a remarkable mathematically rigorous connection between topologically protected active matter flows and the Cayley graph structure of permutation groups, with direct practical implications for material mixing and information encryption.

Continuing the example above, if the network in Fig. 2C is concatenated with one copy of itself, the permutations $\Sigma = \{\sigma_1, \sigma_2, \sigma_3\}$ in Eq. (1) yield a larger set $\Sigma' = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ of five permutations, where the two new elements read

$$
\sigma_4 = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix},
\quad
\sigma_5 = \begin{pmatrix}
0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1
\end{pmatrix}.
$$

These arise as $\sigma_4 = \sigma_2 \sigma_3$ and $\sigma_5 = \sigma_3 \sigma_2$, representing the permutations (132) and (123) in cycle notation \(2\). Concatenating a second copy of the network results in the 6-element set $\Sigma^2 = \Sigma \cup \{\sigma_6\}$, where $\sigma_6$ represents the transposition (13). Any further concatenation creates no new permutations—that is, $\Sigma^n = \Sigma^3$ for $n \geq 3$—so the concatenation converges, in this case to the symmetric group $S_3$ acting on the first three inputs. Observe that convergence was guaranteed by finding $\Sigma \subseteq \Sigma^2$, itself a consequence of $\Sigma$ containing the identity (SM Text).

Through concatenation, a variety of groups can be constructed. Figure 2B illustrates the relative abundance of the groups generated by repeated concatenation of $3 \times 5$ lattices with up to 5 local crossover defects, determined by evaluating all possible networks with each number of defects. The largest possible group on five inputs, the symmetric group $S_5$, is present, along with six of its 14 non-trivial non-isomorphic proper subgroups. In fact, $S_5$ can be generated even with only two defects, but this comes at the expense of many concatenations; as the number of defects increases, the probability of generating $S_5$ rises [42] and the requisite number of concatenations falls (Fig. S1). The swapping performed by the local crossover defects is reflected in the subgroups generated: all but $A_5$ are precisely those that can be generated by a set of transpositions [43]. Notable among the absences are the familiar dihedral groups $D_8$ and $D_{10}$, the symmetry groups of the square and pentagon, respectively. Though $S_3 \times C_2$ is generated frequently and is technically isomorphic to the hexagonal symmetry group $D_{12}$, it only appears here through the natural action of $S_3 \times C_2$ on 5 points rather than as hexagonal symmetries of 6 points.

To generate these particular group actions necessitates more complex fundamental permutations than the local swap defects we consider here. In fact, these can be generated by more general AFN topologies, as we will soon describe.

Repeated concatenation continues to have a quantitative effect beyond the point where the qualitative effect ends. As more copies are added on, even if the permutation set $\Sigma^n$ is constant as $n$ increases, the underlying probability of generating each element of $\Sigma^n$ changes with each additional copy. Provided $\Sigma^n$ converges to a group, Markov chain theory implies that these probabilities approach the uniform distribution in the limit $n \to \infty$ (SM Text), allowing fine-grained control over output frequencies. To exemplify this, consider once more the network in Fig. 2C and let $G = \Sigma^3$ be the group it generates by concatenation. If we let $P_{ij}$ be the probability that a single copy of the AFN permutes state $g_i \in G$ to state $g_j \in G$, then the probability that our initial unpermuted (identity) state $g_1$ is sent to $g_i \in G$ after $n$ concatenations is $P^n_{1i}$. Using the permutation probabilities found above, this transition matrix reads (SM Text)

$$
[P_{ij}] = \begin{pmatrix}
1/3 & 1/2 & 1/6 & 0 & 0 & 0 \\
1/2 & 1/3 & 0 & 0 & 1/6 & 0 \\
1/6 & 0 & 1/3 & 1/2 & 0 & 0 \\
0 & 0 & 1/2 & 1/3 & 0 & 1/6 \\
0 & 1/6 & 0 & 0 & 1/3 & 1/2 \\
0 & 0 & 0 & 1/6 & 1/2 & 1/3
\end{pmatrix},
$$

with row and column indexes corresponding to the permutations as before. Then at $n = 3$ we have non-uniform probabilities—$P_{12} \approx 0.32$ versus $P_{16} \approx 0.06$, for example—but by $n = 20$ these have converged to 1/6 at two decimal places.

**General random graphs**

Finally, we turn to permutations realized by general graphs. As the internal structure linking inputs to outputs becomes topologically more complex, many more permutations can often be realized with the same number of internal vertices than in a defect-riddled hexagonal lattice, trading complexity for functionality. General graphs are also typically not independent of $\beta$, commonly realizing far more permutations when $T = \beta^{-1} > 0$ beyond the ground-state permutations seen when $T = 0$. To illustrate this, we computed the exact number of permutations $|\Sigma|$ output by samples of input–output-augmented random cubic graphs at fixed (necessarily even) numbers $V$ of bulk vertices for $V$ between 22 and 56 (SM...
As shown in Fig. 4, $|\Sigma|$ clearly tends to increase with $V$ in both the $T = 0$ and $T > 0$ regimes. Indeed, the majority of 56-vertex graphs attain all possible $5! = 120$ permutations when $T > 0$, thus directly outputting $S_5$ with fewer vertices than any of the $S_5$-generating concatenations in Fig. 3.

When repeatedly concatenated, zero-noise random AFNs generate a large zoo of $S_5$ subgroups. Upon analyzing the random sample in Fig. 3B, we found $T = 0$ AFNs generating almost all subgroups of $S_5$, including the familiar $D_4$ and $D_{10}$ missing from the hexagonal lattices of Fig. 2B. This suggests that general AFNs at $T = 0$ can realize almost any desired group action on repeated concatenation. A less exotic list of groups is generated when $T > 0$, identical to those in Fig. 2B. However, the elements of rarer groups can likely still be realized with high probability provided $T$ is low and the number of concatenations is as few as possible.

CONCLUSION

To conclude, recent technological advances in the fabrication of soft and fluid-based active materials demand novel theoretical and algorithmic ideas to guide the functional design of autonomous logical units, pattern recognition systems, and information transport devices operating far from thermal equilibrium. Vertex models that account for the relevant physical conservation laws and locally driven matter fluxes offer a flexible testbed for exploring generic properties and limitations of signal transduction in active systems. Building on this framework, our analysis shows how topological constraints inherent to quasi-incompressible AFNs can be utilized to realize the actions of fundamental symmetry groups underlying discrete mixing processes and standard signal encryption protocols. The planar and non-planar network designs proposed and investigated here could be implemented and tested in microfluidic chips, exploiting recent progress in 3D printing and in the geometric control of collective transport in dense suspensions of microorganisms and ATP-powered microtubule bundles.

More broadly, however, the above results establish a direct link between active matter and ostensibly unrelated mathematical concepts in information and group theory, thus promising novel symmetry-based approaches to autonomous network design.

This work was supported by Trinity College, Cambridge (F.G.W.), the London Mathematical Society (J.B.F.), an Alfred P. Sloan Research Fellowship (J.D.), an Edmund F. Kelly Research Award (J.D.), NSF Award CBET-1510768 (J.D.) and a Complex Systems Scholar Award of the James S. McDonnell Foundation (J.D.).

* f.g.woodhouse@damtp.cam.ac.uk

[1] M. Artin, Algebra (Prentice Hall, Boston, 2011), second edn.
[2] J. Rotman, An Introduction to the Theory of Groups (Springer-Verlag, New York, 1995).
[3] D. Kahn, The Codebreakers: A Comprehensive History of Secret Communication from Ancient Times to the Internet, Revised and Updated. (Scribner, New York, 1996).
[4] J. Katz, Y. Lindell, Introduction to Modern Cryptography (Chapman & Hall/CRC, Boca Raton, 2014), second edn.
[5] M. Rejewski, How Polish mathematicians deciphered the Enigma. Ann. Hist. Comput. 3, 213–234 (1981).
[6] A. Hodges, Alan Turing: The Enigma (Princeton University Press, Princeton, 2012).
[50] D. J. Earl, M. W. Deem, Parallel tempering: Theory, applications, and new perspectives. *Phys. Chem. Chem. Phys.* 7, 3910–3916 (2005).

[51] E. Bittner, A. Nußbaumer, W. Janke, Make life simple: Unleash the full power of the parallel tempering algorithm. *Phys. Rev. Lett.* 101, 130603 (2008).

[52] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.3* (2016). [http://www.gap-system.org](http://www.gap-system.org).

[53] J. R. Norris, *Markov Chains* (Cambridge University Press, New York, 1997).
Incompressible sample space

To reduce dimensionality when evaluating $H(\Phi)$, we sample from a special incompressible space for $\Phi$, as we now describe.

In a network without inputs or outputs, the space of integer-valued incompressible flows (that is, more general flows with $\phi_e \in \mathbb{Z}$) is spanned by a cycle basis $B_1 = \{ C_a \}$, $1 \leq a \leq |E| - |V| + 1$. This is a set of linearly independent cycles, each defined by its flow vector $C_a = (c_{ae})$ on the edges of $\Gamma$. Lattices, and planar graphs in general, possess an intuitive form of such a basis comprising one cycle around each face except the external infinite face: Euler’s formula $|E| - |V| + |F| = 2$ for finite connected planar graphs with $|F|$ faces then guarantees $B_1$ has the correct dimension.

Now, suppose $\Gamma$ has $N$ inputs and $N$ outputs. To allow for input–output flows, two further components are needed. The first is a set $I = \{ D_i \}$, $1 \leq i \leq N$, where $D_i = (d_{ie})$ is a flow from input $i$ to output $i$. These are not basis elements as such, but instead will be added to the flow according to which inputs are activated. On its own, however, $I$ does not allow an input to connect to an arbitrary output. The second component needed is a set $B_2 = \{ E_j \}$, $1 \leq j \leq N - 1$, where $E_j = (e_{je})$ is a flow from output $j$ to output $j + 1$. The $E_j$ are not valid flows in themselves as each disobeys the diode constraint of an output-adjacent edge. Rather, they work in tandem with $I$ to allow flow from an input to exit from an arbitrary output. For example, $D_1 + E_{12}$ represents a valid flow from input 1 to output 2 if the vectors do not intersect other than at the edge to output 1; if they do, it can be made valid by adding cycles or subtracting cycles from $B_1$ as necessary.

Given the vector of inputs $I$, we express candidate flows as $\Phi = \Psi + \sum_i I_i D_i$, where $\Psi$ is an integer-coefficient linear combination of vectors in $B = B_1 \cup B_2$. This is still a super set of the exact configuration space of $\Phi$, and flows need to be rejected if they have invalid components $\phi_e \notin \{-1, 0, +1\}$ for any $e$. Nevertheless, the vertex flux constraints are now always fulfilled and the sample space is in a form that is much more amenable to exhaustive and Monte Carlo sampling.

Flow space construction

In practice, the sets $B_1, B_2, I$ were constructed using Mathematica. We used different algorithmic approaches depending on the type of graph considered.

Random graphs. For the general graphs in Fig. 3 of the main text, the cycle basis $B_1$ was constructed by a basic implementation of Horton’s minimal weight basis algorithm [49]: all cycles of length 3 are found and each progressively appended to $B_1$ if the added cycle is linearly independent of those already in $B_1$, followed by cycles of length 4, and so on until $B_1$ has the correct size. (Though Mathematica includes a native command to compute a cycle basis, these often contain many large elements sharing the same edge. A minimal weight basis, consisting of the shortest possible cycles, has few overlaps between elements and so is preferable here to reduce rejected state changes in Monte Carlo sampling.) The input–output pairs $I$ were simply constructed by taking (one of) the shortest path(s) between each input–output pair. Finally, in this case the basis $B_2$ was not necessary as these graphs were always considered with all inputs and outputs activated, leaving no free outputs for flows to switch between; if it were needed, shortest paths between output pairs would again be a simple scheme.

Planar hexagonal networks. The cycle basis $B_1$ was taken to be the set of equally-oriented flows around each hexagonal face of the lattice. Base input–output paths $I$ were constructed to take the same form of route between each input–output pair so as to be pairwise disjoint, and output–output switching flows $B_2$ were taken as the shortest paths (length 4) between adjacent outputs.

Hexagonal networks with crossover defects. We started from the sets $B_1, B_2, I$ for the equivalent planar hexagonal lattice. Cycle basis elements corresponding to rewired hexagonal faces were removed from $B_1$ and replacement basis elements then generated by applying Horton’s algorithm, as above, starting from the existing set of good cycles. New input–output paths $I$ were found as shortest paths between input–output pairs. Finally, output–output connections $B_2$ remained intact from the planar hexagonal network.

Exhaustive sampling

For sufficiently small graphs, including all those in Figs. 3 and 4 in the main text, we used exhaustive brute force sampling to evaluate all states. To improve efficiency, rather than naively sampling all $3^{|E|}$ candidate flows $\Phi \in \{-1, 0, +1\}^{|E|}$, we employed an approach exploiting the cycle basis to first construct undirected flows which are then counted with the appropriate orientational multiplicity.

For a set of binary coefficients $b_j \in \{0, 1\}$ ($1 \leq j \leq |B|$)
of the base flows \( X_j \in \mathcal{B} \), the binary vector
\[
\hat{\Phi} = \left( \sum_j b_j X_j + \sum_i I_i D_i \right) \mod 2
\]
defines an undirected flow on an unoriented form of \( \Gamma \). Unless \( \hat{\Phi} \) connects a pair of outputs, this is an unoriented form of a permissible flow. In the full AFN, this flow has energy \( H(\hat{\Phi}) \) and orientational multiplicity \( 2^m \), where \( m \) is the number of closed cycles in \( \hat{\Phi} \) as can be determined by a depth-first search. Each flow is guaranteed to be unique up to orientation because \( \mathcal{B}_1 \) is a basis for cycles on the closed graph, so we need only sample the \( 2^{|\mathcal{B}_1|} \) sets of coefficients \( \{b_i\} \) to cover the entire space.

**Monte Carlo sampling**

For AFNs that could not be reasonably sampled by brute force, we employed a replica exchange (parallel tempering) algorithm. In essence, this algorithm runs multiple Markov chain Monte Carlo simulations of the AFN in parallel, each at a different temperature, randomly switching states between the replicas to better mix and explore different regions of configuration space. The pairwise switching is performed with an energy-dependent probability guaranteed to preserve a Boltzmann distribution of states for each replica. The details of such algorithms are well documented elsewhere [50], so we only discuss model specifics here.

At each iteration, the state of each replica is a coefficient vector \( b_i \in \mathbb{Z} \) over \( X_i \in \mathcal{B} \) representing a valid flow \( \Phi = \sum_i b_i X_i + \sum_i I_i D_i \). We use a Gibbs algorithm to step forward: a new value for each basis element \( b_i \) is picked, one at a time, according to the conditional distribution \( p(b_i \mid \{b_j : j \neq i\}) \), with zero probability for any value of \( b_i \) resulting in an invalid flow \( \Phi \). In practice we only need to check candidate values for \( b_i \) between \( b_i - 2 \) and \( b_i + 2 \) inclusive, since these are the largest changes that could occur without guaranteeing an edge going beyond flow ±1. Sweeping over all elements \( b_i \) comprises one iteration.

We experimentally found an aggressive replica switching scheme to be effective, attempting to swap a random pair of adjacent replicas after every iteration, and we typically used six replicas as a good balance between computation time and speed of configuration space exploration. The replica temperatures within a run were roughly tuned to give a 30–50% swap acceptance rate, which we found reasonable for our purposes [51].

Termination was conditional on the running standard errors \( \varepsilon \) in the simulated observables \( \langle x \rangle \), determined by a subsampling procedure as follows. Every \( n_s \) iterations, a checkpoint \( i \) is reached and we compute the mean \( m^i \) of \( x \) only from iterations between this checkpoint and the last. From all past means \( \{m^i\} \) the running standard error \( \varepsilon^i \) is computed, which is used to approximate the standard error of the numerically computed mean \( \langle x \rangle \) from all iterations. The simulation was then terminated when both \( \max_j \varepsilon_j^i < \varepsilon_{\text{max}} \) and \( \langle \varepsilon_j^i \rangle_j < \varepsilon_{\text{avg}} \) was satisfied for all replicas, for maximum and average absolute error thresholds set to \( \varepsilon_{\text{max}} = 0.005 \) and \( \varepsilon_{\text{avg}} = 0.0025 \). For this to be statistically valid, a sufficiently large number of inter-checkpoint iterations \( n_s \) must be used such that the \( \{m^i\} \) are independent; in practice we found \( n_s = 10000 \) sufficed, verified by evaluating the autocorrelation of the inter-checkpoint means.

**Numerical determination of permutation groups**

The converged groups in Fig. 3 of the main text were determined as follows. For a given defect-riddled 3 \( \times \) 5 hexagonal lattice, exhaustive sampling was first performed to determine the base set of permutations \( \Sigma \). This was then imported into GAP [52], with which the convergence or periodicity of \( \Sigma \) was established by taking powers of \( \Sigma \). (See later for proof that a convergent or periodic sequence is guaranteed.) Finally, if the concatenation converged, the generated group \( G = \langle \Sigma \rangle \) was characterized using the StructureDescription and MovedPoints functions of GAP.

Note that composition of permutations is performed left-to-right in GAP, as opposed to right-to-left as we use here.

**Random graph generation**

In the main text, we consider permutations generated by samples of general random graphs at fixed numbers of bulk vertices \( V \) and inputs and outputs \( N \). These were generated in Mathematica, as follows.

First, generate a random connected 3-regular base graph \( \Gamma_0 \) with \( V - 2N \) internal vertices; if \( \Gamma_0 \) is isomorphic to any previous base graphs, discard and repeat as necessary. Next, pick \( 2N \) random edges. For each edge, split it in two by inserting a new vertex, and onto that new vertex add a new edge with a single degree-1 vertex at its other end. The first \( N \) new degree-1 vertices are then designated inputs and the other \( N \) are designated outputs; if both the input and output split-edge sets were chosen before for this \( \Gamma_0 \), repeat until distinct edges are picked. This process is then repeated multiple times with \( \Gamma_0 \) to create a set of random input–output augmentations (in our case 10 times), and this process is then repeated over multiple base graphs \( \Gamma_0 \) (in our case, 50 samples) at each number of internal vertices \( V \). Finally, graphs not permitting any valid flow state with all inputs activated are discarded.
CONTINUUM MODEL

In the following, we present a definition of active flow networks for fully continuous flows $\phi_e \in \mathbb{R}$ employing local edge flux potentials and soft constraints, as considered in previous work \[15, 28\]. The discretization employed in the main text is a simplification of this model allowing for much easier state space exploration and comprehension while still retaining the same qualitative features.

As in the main text, let $\Gamma$ be a graph with edge set $E$ and vertex set $V \cup \partial \Gamma$, where $V$ is the set of interior vertices and $\partial \Gamma$ are degree-1 boundary vertices used as inputs and outputs, and assign every edge $e \in E$ an arbitrary orientation. These orientations define the $|V| \times |E|$ incidence matrix $D = [D_{ve}]$ where $D_{ve}$ is $-1$ if edge $e$ is oriented outwards from vertex $v$, $+1$ if $e$ points into $v$, and $0$ if $v$ and $e$ are not incident. A continuous flow configuration $\Phi = (\phi_e)_{e \in \Gamma}$ is a vector of signed flows $\phi_e \in \mathbb{R}$ along each $e \in E$, where $\phi_e > 0$ represents flow with the orientation of $e$ and $\phi_e < 0$ is flow against the orientation of $e$. The pseudo-equilibrium model governing the system behaviour is then defined by an energy $H = H_0 + H_D$ comprising a bulk energy $H_0$ and a boundary energy $H_{\partial \Gamma}$. We will discuss each of these in turn.

The bulk energy $H_0$ encodes spontaneous self-organized flow as well as incompressibility at internal vertices. This takes the form

$$H_0(\Phi) = \lambda \sum_{e \in E} U(\phi_e) + \frac{1}{2} \mu \sum_{v \in V} [(D \cdot \Phi)_v]^2.$$  \hfill (2)

The first term, with coupling constant $\lambda$, uses a double-welled potential $U(\phi_e) = -\frac{1}{4} \phi_e^4 + \frac{1}{6} \phi_e^6$ with minima at $\phi_e = \pm 1$ to model the propensity for spontaneous active flows $\phi_e \approx \pm 1$ along each edge $e \in E$. The second term, with coupling constant $\mu \gg \lambda$, imposes the soft incompressibility constraint $(D \cdot \Phi)_v \approx 0$ at every bulk vertex $v \in V$. This results in states where every edge $e \in E$ is either flowing, with $\phi_e \approx \pm 1$, or in a non-flowing state, $\phi_e \approx 0$, with inflow and outflow balanced at every internal vertex $v \in V$. Configurations with greater numbers of flowing edges have lower $H_0$ and are therefore energetically preferred. Note that the higher-order term of $U(\phi_e)$ than a typical quartic potential in a Landau-like theory is to avoid a hidden symmetry when the incompressibility constraint is added, which leads to unrealistic continuously-valued flow configurations rather than semi-discretized flows $\phi_e \approx \{-1, 0, +1\}$; any double-welled potential of form other than simple quartic suffices. When the AFN is closed, so that $\partial \Gamma = \emptyset$, we have $H = H_0$ and Langevin dynamics then yield topology-dependent stochastic cycle switching phenomena \[28\].

Inputs and outputs are set and read through the boundary vertices $\partial \Gamma = \partial \Gamma_{in} + \partial \Gamma_{out}$. For a given digital input vector $I = (I_v)_{v \in \{0,1\}^{\partial \Gamma_{in}}}$ we constrain the vertex $v \in \partial \Gamma_{in}$ corresponding to input $I_v$ to have net flux $(D \cdot \Phi)_v \approx -I_v$, so that an activated input $I_v = 1$ injects matter into the network through $v$. Output vertices, on the other hand, are left unconstrained to allow matter to flow out of them or not as network interactions dictate; the output $O_v$ of $v \in \partial \Gamma_{out}$ is read off as the (integer-rounded) flow $(D \cdot \Phi)_v$ through $v$, forming the output vector $O = (O_v)_{v \in \{0,1\}^{\partial \Gamma_{out}}}$. Finally, to prevent spurious matter inflow through the outputs, we impose that the unique edge incident to each output vertex only permits flow toward the output, like a diode, as could be realized microfluidically through geometric channel patterning \[29\]. The input flux constraints and diode edges are implemented through the boundary energy

$$H_{\partial \Gamma} = \frac{1}{2} \mu \sum_{v \in \partial \Gamma_{in}} [(D \cdot \Phi)_v + I_v]^2 + H_+,$$ \hfill (3)

where the diode energy $H_+$ is infinite if any output-adjacent edge has flow into the network and zero otherwise.

Provided the coupling constants $\lambda$ and $\mu$ are sufficiently large with respect to the intrinsic noise strength (pseudo-temperature) $T = \beta^{-1}$, stable states of $H$ that is, local minima—comprise flowing edges with $|\phi_e| = 1$ and non-flowing edges with $\phi_e = 0$, with flows balanced at every internal vertex and flow out of each activated input. The energy $H$ is then proportional to the number of flowing edges, favoring states with more flow.

In this work, to tractably explore the entire state space on general networks, we employ a discrete form of this model by restricting exclusively to flows $\Phi \in \{-1,0,+1\}^{|E|}$. Furthermore, taking the incompressible limit $\mu \rightarrow \infty$ with $\lambda$ fixed restricts to the space of flows that exactly obey the inputs $I$ and are perfectly incompressible at all internal vertices. In this subspace, the energy reads $H(\Phi) = -\frac{1}{2} \lambda \sum_e |\phi_e|$ proportional to the number of flowing edges $\phi_e = \pm 1$. As discussed in the main text, this results in a system that at least qualitatively replicates the full continuous lattice field model of Eqs. \[2\] and \[3\].

PASSIVE FLOW

In the main text, we compare AFNs to passive flow networks, which we now give a brief overview of. We frame the mathematics in terms of microfluidics here, but the same formulae apply for all of Newtonian microfluidics, linear resistor networks and symmetric random walks \[37\]. In this section, repeated indices imply summation.

Let $p_v$ be the hydrodynamic pressure at vertex $v$ and let $u_e$ be the flow along edge $e$ (signed according to the graph orientation, as for the active flows). Mass conservation implies that at a bulk vertex $v \in V$, we have $D_{ve} u_e = 0$. Now, assuming the flow along an edge is
PERMUTATION NETWORKS

When an $N$-input, $N$-output cubic AFN has all $N$ inputs activated and uniquely labelled, mutual exclusivity of input–output paths means that the network permutes the input streams. Copies of the network can then be concatenated together to generate more complex permutations from the initial set. In this section we prove a variety of results on the convergence or non-convergence of this concatenation process. Given a set $\Sigma$ of permutations an AFN is capable of performing, we first establish the fundamental behaviour of the $n$-fold concatenation $\Sigma^n$ as a function of $n$. This foundation then lets us view concatenation as a random walk on the Cayley graph generated by $\Sigma$, from which we can use Markov chain theory to write down a graph-theoretic condition for convergence of concatenation.

Fundamental behaviour of $\Sigma^n$

In the following, Theorem 2 proves concatenation always settles into a repeated finite sequence and Theorem 4 gives equivalent conditions for convergence to a group. We also briefly give a sufficient condition to guarantee convergence and another to guarantee non-convergence.

Let $\Sigma$ and $\Pi$ be non-empty subsets of $S_N$ where $N$ is a positive integer. Define the product $\Sigma\Pi$ to be $\{\sigma\tau : \sigma \in \Sigma, \tau \in \Pi\}$, and for a positive integer $m$, let $\Sigma^m := \{\sigma_1\cdots\sigma_m : \sigma_1,\ldots,\sigma_m \in \Sigma\}$. Note that $\Sigma^{k+\ell} = \Sigma^k\Sigma^\ell$ for all positive integers $k$ and $\ell$. Further, if $\Sigma$ is a group, then $\Sigma^m = \Sigma$ for all $m > 0$.

Lemma 1. Let $\Sigma$ be a non-empty subset of $S_N$.

(i) If the identity $1 \in \Sigma$, then $\Sigma^m = \Sigma^{m+1}$ for some $m > 0$, and $\Sigma^m$ is a group.

(ii) There exists $k > 0$ such that $\Sigma^k$ is a group.

(iii) There exists $\ell > 0$ such that $\Sigma^{\ell}$ is a group.

Proof. (i) Suppose that $1 \in \Sigma$. If $\sigma \in \Sigma^i$, then $\sigma = \sigma \cdot 1 \in \Sigma^i\Sigma = \Sigma^{i+1}$. Thus $\Sigma^i \subseteq \Sigma^{i+1}$ for all $i > 0$. Since $S_N$ is finite, it follows that $\Sigma^m = \Sigma^{m+1}$ for some $m > 0$. Observe that $\Sigma^i = \Sigma^m$ for all $i \geq m$. Let $\sigma, \tau \in \Sigma^m$. Then $\sigma\tau \in \Sigma^m\Sigma^m = \Sigma^m$. Since every element of $S_N$ has finite order (the order of an element $\sigma$ is the minimal $v > 0$ such that $\sigma^v = 1$), it follows that $\Sigma^m$ is a group.

(ii) There exists $\sigma \in \Sigma$, and $\sigma$ has finite order $k$, so $\sigma^k \in \Sigma^k$.

(iii) By (ii), there exists $k > 0$ such that $\sigma^k \in \Sigma^k$. Let $\Pi := \Sigma^k$. By (i), there exists $m > 0$ such that $\Pi^m$ is a group. Take $\ell := km$. \qed

Define the signature of $\Sigma$ to be the smallest positive integer $s$ such that $\Sigma^s$ is a group. Since $\Sigma^{s+s} = \Sigma^s$, we
may define the period of $\Sigma$ to be the smallest positive integer $p$ such that $\Sigma^{s+p} = \Sigma^s$.

**Theorem 2.** Let $\Sigma$ be a non-empty subset of $S_N$ with signature $s$ and period $p$. For all integers $k \geq s$, there exists an integer $i$ such that $0 \leq i < p$ and $\Sigma^k = \Sigma^{s+i}$.

**Proof.** There exists an integer $i$ such that $0 \leq i < p$ and $k - s \equiv i \mod p$. Now $k = s + mp + i$ for some $m \geq 0$, and $\Sigma^{s+mp} = \Sigma^s$, so $\Sigma^k = \Sigma^{s+i}$.

Thus $\Sigma^s$ converges precisely when $p = 1$, and the group it converges to is $\Sigma^s$.

Let $\langle \Sigma \rangle$ denote the subgroup of $S_N$ generated by the elements of $\Sigma$ (that is, the group comprising all finite products of elements in $\Sigma$). Clearly $\Sigma^m \subseteq \langle \Sigma \rangle$ for all $m > 0$. In particular, $\Sigma^s \subseteq \langle \Sigma \rangle$, but in general these need not be equal. For example, if $|\Sigma| = 1$, then $\Sigma^s = \{\iota\}$.

**Proposition 3.** Let $\Sigma$ be a non-empty subset of $S_N$ with signature $s$ and period $p$. If $p$ divides $s$, then $\Sigma^s = \langle \Sigma^p \rangle$.

**Proof.** Since $\iota \in \Sigma^s$ and $\Sigma^s \Sigma^p = \Sigma^s$, it follows that $\Sigma^p \subseteq \Sigma^s$. Thus $\langle \Sigma^p \rangle \subseteq \Sigma^s$. On the other hand, $s = pm$ for some integer $m$, so $\Sigma^s = (\Sigma^p)^m \subseteq \langle \Sigma^p \rangle$.

**Theorem 4.** Let $\Sigma$ be a non-empty subset of $S_N$ with signature $s$ and period $p$. The following are equivalent.

(i) $p = 1$.

(ii) $\Sigma^s = \langle \Sigma \rangle$.

(iii) $\Sigma \subseteq \Sigma^s$.

(iv) $\Sigma^k = \Sigma^s$ for all $k \geq s$.

(v) $\Sigma^\ell \subseteq \Sigma^{\ell+1}$ for some $\ell > 0$.

**Proof.** First, (i) implies (ii) by Proposition 3. Clearly (ii) implies (iii). Note that if $\Pi \subseteq \Sigma^s$, then $\Pi \Sigma^s = \Sigma^s$ since $\Sigma^s$ is a group. Thus (iii) implies (iv). Clearly (iv) implies (v). Lastly, suppose that (v) holds. Now $\Sigma^k \subseteq \Sigma^{k+1}$ for all $k \geq \ell$. By Theorem 2 there exists $k \geq \ell$ such that $\Sigma^k = \Sigma^s$, and it follows that $\Sigma^s \subseteq \Sigma^{s+1} \cdots \subseteq \Sigma^{s+p} = \Sigma^s$. Thus $\Sigma^{s+1} = \Sigma^s$ and (i) holds.

**Proposition 5.** Let $\Sigma$ be a non-empty subset of $S_N$ with period $p$. If $\iota \in \Sigma$, then $p = 1$.

**Proof.** Let $s$ be the signature of $\Sigma$. If $\iota \in \Sigma$, then $\Sigma \subseteq \Sigma^s$, so $p = 1$ by Theorem 4.

The converse of Proposition 5 is not true in general. For example, if $\sigma$ is a transposition and $\tau$ is a 3-cycle that is disjoint from $\sigma$, then $\{\sigma, \tau\}$ has signature 5 and period 1 but does not contain the identity.

Recall that any permutation $\sigma$ in $S_N$ may be written as a product of transpositions; the permutation $\sigma$ is even (resp. odd) if this product has an even (resp. odd) number of transpositions.

**Proposition 6.** Let $\Sigma$ be a non-empty subset of $S_N$ with signature $s$ and period $p$. If $\Sigma$ consists only of odd permutations, then $s$ and $p$ are even.

**Proof.** If $\Sigma$ consists only of odd permutations, then for all $i \geq 0$, the set $\Sigma^{2i}$ consists only of even permutations, while $\Sigma^{2i-1}$ consists only of odd permutations. Since $\iota \in \Sigma^s$ and $s$ is even, it follows that $s$ and $p$ are even.

The converse of Proposition 6 is not true in general. For example, if $\sigma$ and $\tau$ disjoint transpositions, then $\langle \sigma, \tau \rangle$ has signature 2 and period 2 but contains the even permutation $\sigma \tau$.

**Concatenation as a Markov Chain**

Our main results in this section are Theorem 8 giving a geometric equivalence to convergence, and Theorem 10 showing that converging concatenations approach uniform random selection of permutations.

Let $G$ be the Cayley graph of the group $G = \langle \Sigma \rangle$ generated by $\Sigma$; that is, the graph with vertex set $G$ and directed edges $v \rightarrow w$ for those $v, w \in G$ for which there exists $\sigma \in \Sigma$ with $\sigma v = w$. (For our purposes we include loops $v \rightarrow v$ in $\mathcal{G}$ if the identity $i \in \Sigma$.) From the above we know $\Sigma^m \subseteq G$, with equality for large $n$ if and only if $p = 1$, so any permutation state of an $n$-fold concatenation is a vertex in $\mathcal{G}$. This lets us view $n$-fold concatenation as an $n$-step random walk on $\mathcal{G}$.

Let $p_\tau$ be the probability that the basic AFN will apply permutation $\sigma \in \Sigma$. Now, starting from the identity map $X_0 = \iota$, let $X_n \in G$ be the random state selected by an $n$-fold concatenation. Then $X_{n+1} = \sigma X_n$ with probability $p_\sigma$, so the transition matrix $P_{gh} = \mathbb{P}(X_{n+1} = h | X_n = g)$ for $X_n$ as a random walk on $G$ reads

$$P_{gh} = \begin{cases} p_\tau & \text{if } \tau = hg^{-1} \in \Sigma, \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

Note that for fixed $g \in G$, $\tau = hg^{-1}$ is distinct for every $h \in G$ and therefore hits every element of $\Sigma$ once, and vice-versa for fixed $h$. This guarantees that $P = [P_{gh}]$ is a doubly-stochastic matrix (that is, a matrix whose rows and columns each sum to 1) and so has a left eigenvector $(1 \cdots 1)$ with eigenvalue 1.

**Lemma 7.** The Markov chain on $G$ with transition matrix given by Eq. (4) is irreducible. Equivalently, the Cayley graph $\mathcal{G}$ is strongly connected.

**Proof.** Suppose $X_n = g$ and we wish to reach state $h$ in a finite number of steps. This is the statement that there exists a finite sequence of generators $\sigma_i, \sigma_j, \ldots, \sigma_k$ such that $\sigma_i \sigma_j \cdots \sigma_k = hg^{-1}$. By closure we have $hg^{-1} \in G$, and by definition of $G$ all elements of $G$ are finite products of $\sigma_i \in \Sigma$. Therefore this sequence exists.
We can now give a geometric condition for convergence of concatenation to a group.

**Theorem 8.** Let \( \Sigma \) be a non-empty subset of \( S_N \) with period \( p \). Then \( p = 1 \) if and only if the Cayley graph \( \mathcal{G} \) generated by \( \Sigma \) is aperiodic; that is, the g.c.d. of the lengths of all directed cycles in \( \mathcal{G} \) is 1.

**Proof.** The set \( \Sigma \) has \( p = 1 \) if and only if \( \Sigma^n = G \) for all sufficiently large \( n \) by Theorem 3. This is equivalent to \( \Pr(X_n = g) > 0 \) for all \( g \in G \) and all sufficiently large \( n \), which is the statement that the Markov chain is aperiodic. Now, the possible return times for a state \( g \in G \) correspond to the lengths of all directed cycles containing \( g \) in \( \mathcal{G} \). Since the chain is irreducible (Lemma 7), all states have the same period \( \|G\| \) given by the g.c.d. of all possible return times for all states. The result follows.

Instead of considering the entire graph \( \mathcal{G} \), we can often simply read off aperiodicity directly from \( \Sigma \), per the following. (Recall that the order of an element \( \sigma \) is the minimal \( v > 0 \) such that \( \sigma^v = \iota \).)

**Proposition 9.** Let \( \Sigma \) be a non-empty subset of \( S_N \) with period \( p \). Let \( v_{\sigma} \) be the order of \( \sigma \in \Sigma \). Then \( \gcd \{ v_{\sigma} : \sigma \in \Sigma \} = 1 \) implies \( p = 1 \).

**Proof.** We will establish that the chain is aperiodic, which implies \( p = 1 \) per Theorem 8. By Lemma 7, we need only establish aperiodicity of one state to imply aperiodicity of the chain \|G\|. Suppose \( X_n = \iota \). Then \( \Pr(X_{n+v_{\sigma}} = \iota) > 0 \) by applying \( \sigma \in \Sigma \) repeatedly \( v_{\sigma} \) times, so each generator \( \sigma \in \Sigma \) implies a possible return time of \( v_{\sigma} \). Thus the g.c.d. of all return times is at most \( \gcd \{ v_{\sigma} : \sigma \in \Sigma \} \), implying \( \iota \) is aperiodic when this equals 1.

Note that the condition of Proposition 9 is sufficient but not necessary for aperiodicity. Consider, for example, \( \Sigma = \{(123),(234)\} \) (in group-theoretic cycle notation). Then both elements of \( \Sigma \) have order 3, but \( \Sigma^* \) converges because \( \mathcal{G} \) contains cycles with the coprime lengths 3 and 4. In this case, \( G = A_4 \).

We conclude by observing that convergent concatenations select permutation elements uniformly at random in the large-\( n \) limit.

**Theorem 10.** Let \( X_n \) be states of the Markov chain on \( G \) with transition matrix given by Eq. (4). If the generating set \( \Sigma \) has period \( p = 1 \), then \( \Pr(X_n = g) \to \frac{1}{|G|} \) as \( n \to \infty \) for all \( g \in G \).

**Proof.** Because the chain is finite, irreducible (Lemma 7) and aperiodic (Theorem 8), it is positive recurrent (as at least one state must be positive recurrent, and all other states are finitely reachable from such a state). Therefore it has a unique limiting distribution \( P^n \to \pi_j \) as \( n \to \infty \) where \( \pi_j = \pi_i P_{ij} \) and \( \sum_j \pi_j = 1 \). We remarked above that \( P \) has a left eigenvector \((1 \cdots 1)^\top\) with eigenvalue 1, which must correspond to \( \pi_j = 1/|G| \) by uniqueness. The result follows.

Generating \( S_5 \) with small lattices

In the main text (Fig. 3), we show that creating permutation devices from the concatenation of small \( 3 \times 5 \) hexagonal lattices with a few local crossover defects can generate the full symmetric group \( S_5 \). For applications it may not be sufficient to know simply if it is possible, but rather how many networks are required and whether there is a trade-off necessary between network topological complexity and repetitions. In fact, as the number of defects increases and the probability of generating \( S_5 \) rises, the number of concatenations required (the signature) tends to fall amongst \( S_5 \)-generating networks.

---

**FIG. S1.** Distributions of the number of concatenations required to generate \( S_5 \) using the relevant lattices in Fig. 3 of the main text, for \( S_5 \)-generating lattices with between 2 and 5 crossover defects. As the number of defects increases, the number of concatenations required (the lattice signature) tends to fall amongst \( S_5 \)-generating networks.