

Scrambling Permutations and Entropy of Hypergraphs

Zoltán Füredi

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61801-2975 and Mathematical Institute of the Hungarian Academy of Sciences, Budapest 1364, Hungary

ABSTRACT

The following result is proved by using entropy of hypergraphs. If π_1, \dots, π_d are permutations of the n element set P such that for every triple $x, y, z \in P$, one can find a π_i such that $\pi_i(x)$ is between $\pi_i(y)$ and $\pi_i(z)$, then $n < \exp(d/2)$. We also study k -scrambling permutations. Several problems remained open. © 1996 John Wiley & Sons, Inc.

1. MIXING PERMUTATIONS AND A CONTAINMENT PROBLEM OF ORTHANTS

The permutations π_1, \dots, π_d of the n -element set P are called *3-mixing* if for any 3-element set $\{i, j, k\} \subset P$, one of the permutations places i between j and k , another one puts j between the other two, and the same holds for k , too. Let $g(d)$ denote the maximum n with the above property.

Theorem 1.1. *For all $d \geq 2$ we have $g(d) < e^{d/2} < 1.65^d$.*

This problem is easily seen to be equivalent to the following. What is the largest number n such that one can find an n -point set $X \subset \mathbb{R}^d$ with the property that each orthant $\text{orth}(x, \epsilon)$ whose origin x belongs to X and whose faces are parallel to the axis contains at most one additional point of X . Here $\epsilon = (\epsilon_1, \epsilon_2, \dots, \epsilon_d) \in \{1, -1\}^d$ and $\text{orth}(x, \epsilon)$ is defined as the set of all vectors of the

form $x_i + \epsilon_i t_i$ with $t_i \geq 0$ for all coordinates $1 \leq i \leq d$. The pigeon hole principle gives $g(d) := \max n \leq 1 + 2^d$. Enomoto (unpublished) proved $g(d) = o(2^d)$ and this improved by Ishigami [7, 8] to

$$7^{\lfloor d/5 \rfloor} \leq g(d) \leq 4 \binom{d}{\lfloor d/4 \rfloor} \quad (1.1)$$

These bounds asymptotically are $(1.475 \dots)^d$ and $(4/3^{3/4})^d \sim (1.754 \dots)^d$.

For small values we have $g(2) = 2$, $g(3) = 3$, $g(4) = 4$, and $g(5) \geq 7$ by the following example from [8]: $\mathcal{P} = \{1234567, 5273461, 4217365, 3251764, 7245163\}$. Actually, it is easy to see that $g(5) = 7$ as was shown by one of the referees as follows. Suppose that there exists an example with five permutations on eight elements. Consider the elements in the positions 1, 2, 7, and 8 of these permutations. There are 20 such places. It is easy to see that no element can occur four times here. So there are at least four elements occurring exactly three times. However, if an element appears three times then all the three must be in positions 2 and 7. However, this is impossible since there are only 10 such places.

Let $l(n, d)$ be the largest number such that for every n -element set $P \subset \mathbb{R}^d$ there exist an $x \in P$ and an $\epsilon \in \{1, -1\}^d$ satisfying $|\text{orth}(x, \epsilon) \cap P| \geq 1 + l(n, d)$. It is easy to verify that $l(2, d) = 1$ and $l(n, 2) = \lceil n/2 \rceil$ (see [8]). Ishigami [8] showed that

$$\frac{n}{4 \binom{d}{\lfloor d/4 \rfloor}} \leq l(n, d) \leq \left\lceil \frac{n}{g(d)} \right\rceil \leq \left\lceil \frac{n}{7^{\lfloor d/5 \rfloor}} \right\rceil$$

Theorem 1.1 is implied by the following stronger result.

Theorem 1.2. *For $n, d \geq 3$ we have $l(n, d) > n \exp(-d/2)$.*

The proof is given in the next two sections. In Section 4 we show that $\lim_{d \rightarrow \infty} g(d)^{1/d}$ exists. Section 5 contains further extremal results, and in Section 6 we propose a series of open problems.

2. THE ENTROPY LEMMA

Let \mathcal{F} be a multihypergraph with (the finite) underlying set (or vertex set) V , i.e., it is a collection of subsets of V , $\mathcal{F} = \{F_1, F_2, \dots, F_m\}$, where repetition of the members is allowed. The multiplicity of the set $S \subset V$ is denoted by $\mu(S)$ [or $\mu(S, \mathcal{F})$ to be precise], and set $\mu = \mu(\mathcal{F})$ the maximum multiplicity, $\mu = \max_{S \subset V} \mu(S)$. Here $\mu(S)$ is a nonnegative integer with $\sum_{S \subset V} \mu(S) = m$. Define the entropy function $H(y) = y \log_2(1/y) + (1-y) \log_2(1/(1-y))$ for all $0 < y < 1$, $H(0) = H(1) = 0$. Then H is a concave real function. The binary entropy of the hypergraph \mathcal{F} is defined as

$$H(\mathcal{F}) = \sum_{S \subset V} \frac{\mu(S)}{m} \log_2 \frac{m}{\mu(S)}.$$

We are going to use the following lemma which was first proved (for $\mu = 1$) by Kleitman, Shearer, and Sturtevant [11]. The proof for multihypergraphs is

identical to the original one, we omit it. It is a consequence of the basic entropy inequality $H(\xi) \leq \sum_i H(\xi_i)$, where ξ and ξ_1, \dots, ξ_k are random variables such that the values of the ξ_i 's completely determine ξ . The interested reader can find a thorough discussion and additional applications in the survey of Alon [1].

Lemma 2.1. *Let \mathcal{F} be a multihypergraph of m sets with maximum multiplicity μ and underlying set V . Let $p(x)$ denote the fraction of sets in \mathcal{F} that contain the element $x \in V$. Then*

$$\log_2(m/\mu) \leq \sum_{x \in V} H(p(x)).$$

Let us remark that, as far as the author knows, the entropy function for extremal combinatorial problems was first used by Katona [10] in 1966, and later the method was renewed in [11] and [3].

3. PROOF OF THEOREM 1.2

From now on we consider only the permutation version of the problem. Let P be an n -element set, it is usually identified with $[n] := \{1, 2, \dots, n\}$. The matrix $M = [M_{i,j}]$ is called a $d \times n$ permutation matrix if each of its d rows contains each element of P exactly once. The rank of an element v in the i th row is denoted by $\pi_i(v)$, i.e., $\pi_i(v) = j$ for $M_{i,j} = v$. For $\epsilon \in \{1, -1\}^d$ let $L(v, \epsilon)$ denote the set of $w \in P \setminus \{v\}$, with the property that $\pi_i(w) < \pi_i(v)$ if and only if $\epsilon_i = -1$. That is, the element $w \in L(v, \epsilon)$ precedes v in the i th permutation if and only if $\epsilon_i = -1$. Define $l(M) = \max\{|L(v, \epsilon)| : v \in P, \epsilon \in \{1, -1\}^d\}$. [If \mathcal{P} is a system of permutations, then $l(\mathcal{P})$ is defined as $l(M)$, where M is a matrix with rows corresponding to the members of \mathcal{P} .] Finally, let $l(n, d) = \min\{l(M) : M \text{ is a } d \times n \text{ permutation matrix}\}$, $g(d) = \max\{n : l(n, d) \leq 1\}$.

For any two elements $x, y \in P$ define the set $F(y, x) \subset [d]$ as the set of indices i with $\pi_i(y) < \pi_i(x)$. Define the multihypergraph $\mathcal{F}(x) = \{F(y, x) : x \neq y \in P\}$. It has $n-1$ members with maximum multiplicity at most $l = l(M)$. The element i appears in the members of $\mathcal{F}(x)$ exactly $\pi_i(x) - 1$ times. The entropy lemma implies that

$$\log_2 \frac{n-1}{l} \leq \sum_{1 \leq i \leq d} H\left(\frac{\pi_i(x) - 1}{n-1}\right).$$

Add up the above inequalities for all $x \in P$:

$$\begin{aligned} n \log_2 \frac{n-1}{l} &\leq \sum_{x \in P} \sum_{1 \leq i \leq d} H\left(\frac{\pi_i(x) - 1}{n-1}\right) \\ &= \sum_{1 \leq i \leq d} \sum_{x \in P} H\left(\frac{\pi_i(x) - 1}{n-1}\right) = d \sum_{0 \leq j \leq n-1} H\left(\frac{j}{n-1}\right). \end{aligned}$$

Using the symmetry and concavity of the function H , one gets that

$$\sum_{0 \leq j \leq n-1} \frac{1}{n-1} H\left(\frac{j}{n-1}\right) < \int_0^1 H(x) dx.$$

On the other hand, it is a simple calculus problem to determine this integral.

$$\int_0^1 -x \log_2 x - (1-x) \log_2(1-x) dx = (-2) \left[\frac{x^2}{2} \log_2 x - \frac{1}{4 \ln 2} x^2 \right]_{x=0}^1 = \frac{\log_2 e}{2}.$$

Summarizing, we get

$$n \log_2 \frac{n-1}{l} < d(n-1) \frac{\log_2 e}{2}.$$

This is equivalent to $l > (n-1) \exp(-\frac{d}{2} \frac{n-1}{n})$, which is larger than $n \exp(-d/2)$ (for $n, d \geq 3$). \square

4. THE EXISTENCE OF LIMIT

Call a system of permutations \mathcal{P} *2-scrambling* if it reverses each pair, i.e., for every $x, y \in P$ one can find $\pi, \pi' \in \mathcal{P}$ with $\pi(x) < \pi(y)$ and $\pi'(y) < \pi'(x)$. Let $l^*(n, d) = \min\{l(\mathcal{P}) : \mathcal{P} \text{ is a 2-scrambling } d \times n \text{ system of permutations}\}$. Finally, define $g^*(d) = \max\{n : l^*(n, d) \leq 1\}$. Obviously,

$$l^*(n, d) \geq l(n, d) \quad \text{and} \quad g^*(d) \leq g(d). \quad (4.1)$$

Any permutation and its reverse form a 2-scrambling system, so, taking a set of permutations and joining one of the reverses to it, one can make the system 2-scrambling. Hence

$$l^*(n, d) \leq l(n, d-1) \quad \text{and} \quad g^*(d) \geq g(d-1). \quad (4.2)$$

Proposition 4.1. $\lim_{d \rightarrow \infty} (g(d))^{1/d} = \lim_{d \rightarrow \infty} (g^*(d))^{1/d}$.

Proof. First, we show that

$$l^*(n_1 n_2, d_1 + d_2) \leq l^*(n_1, d_1) l^*(n_2, d_2). \quad (4.3)$$

Indeed, consider the 2-scrambling systems, \mathcal{P} and \mathcal{Q} of sizes $d_1 \times n_1$ and $d_2 \times n_2$ and with underlying sets $P = \{p_1, p_2, \dots, p_{n_1}\}$ and $Q = \{q_1, \dots, q_{n_2}\}$, respectively. Consider the product of their underlying sets, $P \times Q$. We define $d_1 + d_2$ permutations of $P \times Q$ in the following rather natural way. Take a permutation $\pi \in \mathcal{P}$, and form the ordered blocks $R_p = \{(p, q_1), (p, q_2), \dots, (p, q_{n_2})\}$. Then order these blocks using π . Similarly, a permutation $\pi' \in \mathcal{Q}$ naturally extends by using the blocks $C_i = \{(p_1, q_i), (p_2, q_i), \dots, (p_{n_1}, q_i)\}$. We claim that we obtain a 2-scrambling system; if $(p, q_i), (p', q_j) \in P \times Q$ with $i < j$, then their order is reversed in the extension of a permutation $\pi' \in \mathcal{Q}$ reversing q_i and q_j .

Let $\epsilon \in \{1, -1\}^{d_1 + d_2}$ and write it in the form $\epsilon = (\epsilon^1, \epsilon^2)$, where $\epsilon^1 \in \{1, -1\}^{d_1}$. It is obvious that $L((p, 1), \epsilon)$ contains $L(p, \epsilon^1) \times L(q, \epsilon^2)$, and it is contained in

$$(L(p, \epsilon^1) \cup \{p\}) \times (L(q, \epsilon^2) \cup \{q\}) \setminus (p, q).$$

We claim that if there is any $(p, q') \in L((p, q), \epsilon)$, then $L((p, q), \epsilon) = \{p\} \times L(q, \epsilon^2)$. Indeed, let $q = q_i$ and $q' = q_j$ and suppose that $i < j$. [The other case, and also the case $(p', q) \in L((p, q), \epsilon)$ are similar.] Then (p, q_i) precedes (p, q_j)

in the block R_p and so they are not reversed in each of the permutations obtained from a $\pi \in \mathcal{P}$. We get $\epsilon^1 = \{1, 1, \dots, 1\}$. However, the permutations obtained from \mathcal{P} form a 2-scrambling system, so if $p'' \neq p$, then there exists a permutation π'' placing the block $R_{p''}$ before R_p , implying $(p'', q'') \notin L((p, q), \epsilon)$.

Summarizing, we get that $L((p, q), \epsilon)$ is either equal to $L(p, \epsilon^1) \times L(q, \epsilon^2)$ or to $\{p\} \times L(q, \epsilon^2)$ or to $L(p, \epsilon^1) \times \{q\}$. In all of these cases its size is at most $l(\mathcal{P})l(\mathcal{Q})$.

Using (4.3), we get $g^*(d_1 + d_2) \geq g^*(d_1)g^*(d_2)$. The sequence $(1/d) \log g^*(d)$ is bounded above, so classical calculus (Fekete's theorem) can be applied to get that $\lim_{d \rightarrow \infty} (1/d) \log g^*(d)$ exists and equals to its supremum. Finally, (4.1) and (4.2) imply that $(1/d) \log g(d)$ also must have the same limit. \square

Note that, the 5×7 example in section 1 is not 2-scrambling (the pair $\{2, 6\}$ is not reversed) so we do not have $g^*(5) = 7$. It is very likely that $g^*(5)$ is only 6. However, $\{2, 6\}$ is the only unreversed pair so with a slightly modified definition of the product $\mathcal{P} \times \mathcal{Q}$ one can get Ishigami's lower bound (1.1), too. We omit the details.

5. COMPLETELY SCRAMBLING PERMUTATIONS

Call a family of permutations π_1, \dots, π_t of the n -element underlying set P *completely k -scrambling* if for every ordered k -set (p_1, \dots, p_k) of k distinct elements of P there is some i with $\pi_i(p_1) < \pi_i(p_2) < \dots < \pi_i(p_k)$. That is, the π_i 's give all the $k!$ permutations of every k -set. The cardinality of the minimal completely k -scrambling family is denoted by $N^*(n, k)$. Spencer [15] proved that

$$\log_2 n \leq N^*(n, k) \leq \frac{k}{\log_2(k!/(k! - 1))} \log_2 n \quad (5.1)$$

as $k \geq 3$, fixed, and $n \rightarrow \infty$. Obviously, for a completely 3-scrambling system \mathcal{P} one has $l(\mathcal{P}) = 1$. On the other hand, starting with a 3-mixing system, $\{\pi_1, \dots, \pi_d\}$, and reversing each of them, one gets a completely 3-scrambling system of permutations. So Theorem 1.1 and Ishigami's example give

$$2 \ln 2 \log_2 n < N^*(n, 3) < (10/\log_2 7) \log_2 n + O(1).$$

The coefficients here are 1.386... and 3.562... [in (5.1) for $k = 3$ we get 1 and 11.405...].

For $k > 3$ Ishigami [9] have recently improved the lower bound in (5.1) to $(k-2)!/(\log_2 k) \log_2 n$ for n large compared to k . One of the referees noted that a very simple argument gives $N^*(n, k) \geq (k-2)! \log_2(n-k+2)$ for all $n \leq k \leq 3$.

Theorem 5.1. *For all $n \geq k \geq 3$ we have $N^*(n, k) > \frac{1}{2}(k-1)! \log_2 n$.*

For the proof we have to recall an old problem of Rényi [14]. Given an arbitrary underlying set V , and consider two of its partitions P, P' . These are called *crossing* (or *qualitatively independent*) if every class of P has a nonempty intersection with every class of P' . A partition into t parts is called a t -partition.

Let $I_t(v)$ denote the largest cardinality of a family of t -partitions of a v -element set under the restriction that any two partitions in the family are crossing. Recently, Gargano, Körner, and Vaccaro [6] have proved that

$$\limsup_{v \rightarrow \infty} \frac{1}{v} \log_2 I_t(v) = \frac{2}{t}$$

holds for every t . We only use the following upper bound, which is an easy corollary of a theorem of Bollobás [2], as was pointed out by Poljak and Tuza [13]:

$$|I_t(v)| \leq \binom{\lfloor 2v/t \rfloor}{\lfloor v/t \rfloor}. \quad (5.2)$$

Proof of Theorem 5.1. Let π_1, \dots, π_d be a completely k -scrambling system of permutations of the set $[n]$. Consider the subpermutations $(\pi_i(1), \dots, \pi_i(k-2))$ for all $i \in [d]$. There is a permutation of $[k-2]$, say it is (p_1, \dots, p_{k-2}) , which occurs at most $d/(k-2)!$ times. Let $V := \{i : \pi_i(p_1) < \pi_i(p_2) < \dots < \pi_i(p_{k-2})\}$. For every element $x \in [n] \setminus [k-2]$ we define a $(k-1)$ -partition of V , $P(x) := (P_1(x), P_2(x), \dots, P_{k-1}(x))$ as follows: $P_1(x) := \{i \in V : \pi_i(x) < \pi_i(p_1)\}$, $P_\alpha(x) := \{i \in V : \pi_i(p_{\alpha-1}) < \pi_i(x) < \pi_i(p_\alpha)\}$ for $2 \leq \alpha \leq k-2$ and $P_{k-1}(x) := \{i \in V : \pi_i(p_{k-2}) < \pi_i(x)\}$. Any two partitions $P(x)$ and $P(y)$ are crossing because there are permutations which places x and y in all possible $(k-1)^2$ ways between, before and after the elements p_1, \dots, p_{k-2} . So (5.2) implies $n - (k-2) \leq \binom{2|V|/(k-1)}{|V|/(k-1)}$. Using $|V| \leq d/(k-2)!$, an easy calculation gives the desired lower bound for d . \square

6. FURTHER PROBLEMS, CONJECTURES

One can propose the more general problem of looking for the minimal number of permutations of n elements that scramble all k -element subsets up in various ways. More precisely, let \mathcal{S} be a family of families of k -permutations and call a system \mathcal{P} of n -permutations \mathcal{S} -mixing if for all k -element subsets $K \subset [n]$ the system $\{\pi(K) : \pi \in \mathcal{P}\} \in \mathcal{S}$. What is the minimum size, $f(n, \mathcal{S})$, of a family of \mathcal{S} -mixing permutations? In other words, we are looking for the minimum number of permutations of $[n]$ with prescribed k -subpermutations.

An important example is the following. Call the set of permutations \mathcal{P} k -scrambling if for every (now unordered) k -set $\{p_1, \dots, p_k\} \subset P$ and for every distinguished element of the set, say p_j , there is a permutation $\pi \in \mathcal{P}$ such that $\pi(p_j)$ precedes all the other $(k-1)$ p_i 's. The cardinality of the smallest k -scrambling family is denoted by $N(n, k)$. This notion goes back to Dushnik [4] who found a formula for $N(n, k)$ when $2\sqrt{n} \leq k \leq n$. For k is fixed and $n \rightarrow \infty$ an argument due to Hajnal and Spencer [15] gives that

$$\log_2 \log_2 n \leq N(n, k) \leq \frac{k-1}{\log_2(2^{k-1}/(2^{k-1}-1))} \log_2 \log_2 n.$$

In [5] the asymptotic $N(n, 3) = \log_2 \log_2 n + (\frac{1}{2} + o(1)) \log_2 \log_2 \log_2 n$ was proved. The determination of $N(n, k)$ is equivalent to the question of the

dimension of the partially ordered set formed by the $(k-1)$ - and 1-element subsets of $[n]$ and ordered by inclusion. More about poset dimensions and their connections with permutations can be found in [16].

It would be interesting to decide if the order of $f(n, \mathcal{P})$ is always $O(1)$, $\Theta(\log \log n)$ or $\Theta(\log n)$, for *monotone* systems. Monotonicity means that $\mathcal{A} \in \mathcal{P}$, $\mathcal{A} \subset \mathcal{B}$ implies $\mathcal{B} \in \mathcal{P}$. (All the above results dealt with monotone properties.)

In another related series of problems one considers partitions instead of permutations. For example, Körner [12] proved the following. Let $f(d)$ be the maximum n such that one can find d partitions $A_i \cup B_i = [n]$, $A_i \cap B_i = \emptyset$, $1 \leq i \leq d$ such that for every triple $T \subset [n]$, and element $x \in T$ one can find an i with either $A_i \cap T = \{x\}$ or $B_i \cap T = \{x\}$. Then $(2/\sqrt{3} - o(1))^d < f(d) < (\sqrt{2} + o(1))^d$.

ACKNOWLEDGMENTS

The author is indebted to E. Szegedi and N. Danielsson (Stockholm) for fruitful conversations. The research was supported in part by the Hungarian National Science Foundation under Grants OTKA 4269, and OTKA 016389, and by a National Security Agency Grant No. MDA904-95-H-1045. The author is greatly indebted to the referees for helpful comments.

REFERENCES

- [1] N. Alon, Probabilistic methods in extremal finite set theory, in *Extremal Problems for Finite Sets*, Proc. Colloq., Visegrád, Hungary, 1991, P. Frankl et al., Eds., *Bolyai Soc. Math. Stud.*, **3**, 39–57 (1994).
- [2] B. Bollobás, On generalized graphs, *Acta Math. Acad. Sci. Hung.*, **16**, 441–452 (1965).
- [3] F. R. K. Chung, P. Frankl, R. L. Graham, and J. B. Shearer, Some intersection theorems for ordered sets and graphs, *J. Combinat. Theor. Ser. A*, **43**, 23–37 (1986).
- [4] B. Dushnik, Concerning a certain set of arrangements, *Proc. Am. Math. Soc.* **1**, 788–796 (1950).
- [5] Z. Füredi, P. Hajnal, V. Rödl, and W. T. Trotter, Interval orders and shift graphs, in *Sets, Graphs and Numbers*, A. Hajnal and V. T. Sós, Eds., *Proc. Colloq. Math. Soc. János Bolyai*, **60**, Budapest, Hungary, 1991, North-Holland, Amsterdam, 1992, pp. 297–313.
- [6] L. Gargano, J. Körner, and U. Vaccaro, Sperner capacities, *Graphs Combinat.* **9**, 31–46 (1993).
- [7] Y. Ishigami, An extremal problem of orthants containing at most one point besides the origin, *Discrete Math.*, **132**, 383–386 (1994).
- [8] Y. Ishigami, Containment problems in high-dimensional spaces, *Graphs Combinat.*, to appear.
- [9] Y. Ishigami, An extremal problem of d permutations containing every permutation of every t elements, *Discrete Math.*, to appear.
- [10] G. O. H. Katona, On separating systems of a finite set, *J. Combinat. Theor.*, **1**, 174–194 (1966).

- [11] D. J. Kleitman, J. B. Shearer, and D. Sturtevant, Intersection of k -element sets, *Combinatorica*, **1**, 381–384 (1981).
- [12] J. Körner, On the extremal combinatorics of the Hamming space, *J. Combinat. Theor. Ser. A*, **71**, 112–126 (1995).
- [13] S. Poljak and Z. Tuza, On the maximum number of qualitatively independent partitions, *J. Combinat. Theor. Ser. A*, **51**, 111–116 (1989).
- [14] A. Rényi, *Foundations of Probability*, Wiley, New York, 1971.
- [15] J. Spencer, Minimal scrambling sets of simple orders, *Acta. Math. Hung.*, **22**, 349–353 (1972).
- [16] W. T. Trotter, *Combinatorics and Partially Ordered Sets: Dimension Theory*, The Johns Hopkins University Press, Baltimore, MD, 1991. Also see: Progress and new directions in dimension theory for finite partially ordered sets, in *Extremal Problems for Finite Sets*, Proc. Colloq., Visegrád, Hungary, 1991, P. Frankl et al., Eds., *Bolyai Soc. Math. Stud.*, **3** (1994), pp. 457–477.

Received January 19, 1995

Accepted August 25, 1995