VC-Dimension of Sets of Permutations

Ran Raz
Weizmann Institute *

Abstract

We define the *VC-dimension* of a set of permutations $A \subset S_n$ to be the maximal k such that there exist distinct $i_1, ..., i_k \in \{1, ..., n\}$ that appear in A in all possible linear orders, that is, every linear order of $\{i_1, ..., i_k\}$ is equivalent to the standard order of $\{\pi(i_1), ..., \pi(i_k)\}$ for at least one permutation $\pi \in A$.

In other words, the VC-dimension of A is the maximal k such that for some $i_1, ..., i_k$ the restriction of A to $\{i_1, ..., i_k\}$ contains all possible linear orders. This is analogous to the VC-dimension of a set of strings.

Our main result is that there exists a universal constant C such that any set of permutations $A \subset S_n$ with VC-dimension 2 is of size $< C^n$. This is analogous to Sauer's lemma for the case of VC-dimension 2.

One corollary of our main result is that any acyclic set of linear orders of $\{1, ..., n\}$ is of size $< C^n$, (a set A of linear orders on $\{1, ..., n\}$ is called *acyclic* if no 3 elements $i, j, k \in \{1, ..., n\}$ appear in A in all 3 orders (i, j, k), (k, i, j) and (j, k, i)). The size of the largest acyclic set of linear orders has interested researchers for many years because it is the largest number of linear orders of n alternatives such that the following is always satisfied: if each one of a set of voters chooses one of these orders as his preference then the majority relation between each two alternatives is transitive.

1 Introduction

The *VC-dimension* of a set $A \subset \{0, 1\}^n$ is the maximal k such that for some distinct $i_1, ..., i_k \in \{1, ..., n\}$ the restriction of A to $\{i_1, ..., i_k\}$ contains all 2^k possible assignments. This definition, first given by Vapnik and Chervonenkis in 1971 [VC], has become a central definition in combinatorics and in certain areas of theoretical computer science. The following lemma, known as Sauer's lemma, was proven independently by Sauer [Sau], Perles and Shelah, and in a slightly weaker form by Vapnik and Chervonenkis.

*ranraz@wisdom.weizmann.ac.il, Department of Applied Mathematics, Weizmann Institute, Rehovot 76100, ISRAEL

Lemma 1.1 *For every n and every $A \subset \{0,1\}^n$ with VC-dimension k*

$$|A| \leq \sum_{i=0}^{k} \binom{n}{i}.$$

Lemma 1.1 gives a tight bound for the size of any set with VC-dimension k. The lemma has numerous of applications in combinatorics and in theoretical computer science. In this paper we extend the definition of VC-dimension to sets of permutations and we prove that every set of permutations with VC-dimension 2 is of size $< C^n$ (for some universal constant C). This bound is tight (up to determining the exact constant), and is analogous to Lemma 1.1 for $k = 2$.

Denote by S_n the set of all permutations on $\{1, ..., n\}$. A permutation $\pi \in S_n$ corresponds to a linear order of the n elements $1, ..., n$ in the following way: for every i, j we say that $i <_\pi j$ iff $\pi(i) < \pi(j)$. That is, the order given by π is

$$\pi^{-1}(1) <_\pi \pi^{-1}(2) <_\pi ... <_\pi \pi^{-1}(n).$$

In particular, for every 3 elements i, j, k, the permutation π defines a linear order of $\{i, j, k\}$, given by the standard order of $\{\pi(i), \pi(j), \pi(k)\}$. That order is referred to below as the restriction of π to $\{i, j, k\}$. More generally, the restriction of π to $\{i_1, ..., i_k\}$ is the linear order of $\{i_1, ..., i_k\}$ given by the standard order of $\{\pi(i_1), ..., \pi(i_k)\}$.

Let $A \subset S_n$ be a set of permutations. The projection of A on the 3 elements i, j, k is defined to be the set of all linear orders of $\{i, j, k\}$ that are restrictions of π to $\{i, j, k\}$ for some $\pi \in A$. We say that the projection of A on 3 distinct elements i, j, k is complete if it contains all 6 linear orders of $\{i, j, k\}$. More generally, the projection of A on $\{i_1, ..., i_k\}$ is defined to be the set of all linear orders of $\{i_1, ..., i_k\}$ that are restrictions of π to $\{i_1, ..., i_k\}$ for some $\pi \in A$, and we say that the projection of A on k distinct elements $i_1, ..., i_k$ is complete if it contains all $k!$ linear orders of $\{i_1, ..., i_k\}$.

Definition 1.1 *The* **VC-dimension** *of a set $A \subset S_n$ is the maximal k such that for some distinct $i_1, ..., i_k$ the projection of A on $\{i_1, ..., i_k\}$ is complete.*

In this paper we are interested in sets A with VC-dimension 2. By the definition, if A is a set with VC-dimension 2 then the projection of A on any 3 distinct elements i, j, k is not complete. That is, at least one linear order is missing from each such projection. We will prove that in that case $|A| < C^n$ for some (large enough) constant C.

Theorem 1.1 *There exists a universal constant C such that for every n and every $A \subset S_n$ with VC-dimension 2*

$$|A| < C^n.$$

Theorem1.1 gives an upper bound for the size of sets $A \subset S_n$ with VC-dimension 2. Since it is not hard to give examples for such sets A of size larger than c^n for some other constant c, the upper bound is tight (up to determining the exact constant). This paper does not attempt to find the smallest constant C.

1.1 Acyclic Linear Orders and the Voting Paradox

The initial motivation for our work came from the problem known as the acyclic linear orders problem which is related to the so called voting paradox.

Let V be a finite set, and for every $v \in V$ let π_v be a linear order of the n elements $\{1, ..., n\}$. We think of V as a set of voters, and of π_v as the preferences of each voter between n alternatives. The voting paradox, first recognized by the Marquis de Condorcet [Con], is that the majority relation between each two alternatives is not necessarily transitive. That is, it may be the case that most voters rank i higher than j, most voters rank j higher than k and still most voters rank k higher than i. (For an historical account see [Bla, Rik].)

One way to prevent the voting paradox is to restrict the domain of possible individual preferences. That is, we specify a subset A of linear orders, and for every $v \in V$ we require π_v to belong to the set A. A set A of linear orders of $\{1, ..., n\}$ is called *consistent* if for any set V and preferences $\pi_v \in A$ the majority relation between each two alternatives is transitive.

Can such a set A be characterized ? A set A of linear orders on $\{1, ..., n\}$ is called *acyclic* if no 3 elements $i, j, k \in \{1, ..., n\}$ appear in A in all 3 orders (i, j, k), (k, i, j) and (j, k, i). It is not hard to prove that a set A is acyclic if and only if it is consistent ! For that reason, acyclic sets of linear orders have interested social choice theorists for many years.

How large can an acyclic set be ? Let $f(n)$ be the maximum size of an acyclic set of linear orders on $\{1, ..., n\}$. Determining $f(n)$ has been the subject of an extensive work in the last 25 years. For $n \leq 5$, the values of $f(n)$ have been determined exactly. For arbitrary large n, the best construction for an acyclic set was given by Fishburn [Fis], showing that $f(n) \geq (2.1708)^n$. However, no good upper bounds for $f(n)$ were known (upper bounds in some special cases were proved by Abello [Abe]).

Let A be an acyclic set. Then, viewing A as a set of permutations, A is a set with VC-dimension 2. Hence, as an immediate corollary of Theorem 1.1 we obtain the upper bound $f(n) < C^n$. This bound was conjectured in [Fis].

For more about the acyclic linear orders problem see [Abe, Fis] and the numerous of references there.

1.2 Discussion

We prove that any set of permutations of VC-dimension 2 is of size $< C^n$ (for some universal constant C). Two immediate open problems come to mind:

First, can the same be proved for every constant VC-dimension ? That is, is it the case that for every k there exists a universal constant C_k such that any set of permutations of VC-dimension k is of size $< (C_k)^n$? It seems that generalizations of our methods may give a bound of $\Omega(\log n)^n$. It is very interesting to know whether a bound of $(C_k)^n$ can be achieved.

Also, what is the maximal size of a set of permutations of VC-dimension 2 ? We have proved an upper bound. Can one prove tighter upper bounds ? [1]

2 Proof of the Main Theorem

In this section we state our main lemma and show how the main theorem follows easily from the main lemma. It will be much harder to prove the main lemma.

Fix n, and let A be a subset of S_n. For every $1 \leq i \leq n$, denote

$$A(i) = \{\pi(i) \mid \pi \in A\},$$

and denote

$$v(A) = \sum_{i=1}^{n} |A(i)|/n.$$

For every real number x, denote

$$\rho(x) = 1 - 2^{15} \cdot \ln(x)/x^{3/2}.$$

We will only use $\rho(x)$ for very large values of x, and hence $\rho(x)$ should be thought of as a value between 0 and 1.

Theorem 1.1 will be an easy corollary of the following Lemma 2.1. It will be much harder to prove Lemma 2.1.

Lemma 2.1 *There exists an integer C_0 such that for every n and every $A \subset S_n$ with VC-dimension 2*

$$|A| \leq (C_0)^n \cdot \left(\prod_{r=C_0 \cdot n+1}^{v(A) \cdot n} \rho(r/n) \right)^{-1}.$$

Proof of Theorem 1.1:
Let C_0 be the constant from Lemma 2.1. We assume that C_0 is large enough (i.e., the argument below is correct for large enough C_0). Since every A satisfies $v(A) \leq n$, we have by Lemma 2.1

$$|A| \leq (C_0)^n \cdot \left(\prod_{r=C_0 \cdot n+1}^{v(A) \cdot n} \rho(r/n) \right)^{-1} \leq (C_0)^n \cdot \left(\prod_{r=C_0 \cdot n+1}^{n^2} \rho(r/n) \right)^{-1}$$

$$\leq (C_0)^n \cdot \left(\prod_{d=C_0}^{n} \rho(d) \right)^{-n} \leq (C_0)^n \cdot \left(\prod_{d=C_0}^{\infty} \rho(d) \right)^{-n}.$$

However, for large enough C_0 the infinite product

$$\prod_{d=C_0}^{\infty} \rho(d)$$

[1] It was suggested by the referee of this paper that maybe the exact number is the Catalan number $\frac{1}{n+1}\binom{2n}{n}$. Can one prove such a bound ?

converges to a positive constant C_1 (this follows from the fact that $\sum_{d=1}^{\infty} \ln(d)/d^{3/2}$ converges). Hence, for large enough constant C,

$$|A| \leq (C_0/C_1)^n < C^n.$$

$\square$

3 Proof of the Main Lemma

In this section we give the proof of Lemma 2.1. For simplicity, let us assume that C_0 is a large constant (without defining its exact value). The proof of Lemma 2.1 will be by induction on $v(A)$. The base case will be $v(A) \leq C_0$. We will then prove the inductive step by separating to three cases.

The base case:
The base case of the induction is given by the following claim:

Claim 3.1 *If $v(A) \leq C_0$ then*

$$|A| \leq (C_0)^n.$$

Proof:
Obviously for any set A,

$$|A| \leq \prod_{i=1}^{n} |A(i)| \leq \left(\sum_{i=1}^{n} |A(i)|/n \right)^n = v(A)^n.$$

Hence, if $v(A) \leq C_0$ then

$$|A| \leq (C_0)^n.$$

$\square$

We will now assume that $v(A) > C_0$ and that the lemma is correct for every A' with $v(A') < v(A)$. We need to prove an upper bound for the size of A. We will do that by finding a large subset $A' \subset A$ with $v(A') < v(A)$. The upper bound for $|A|$ will then follow by bounding $|A|/|A'|$ and by the inductive hypothesis for A'. Formally, it will be enough to find $A' \subset A$ such that if $d \stackrel{\text{def}}{=} v(A) \cdot n - v(A') \cdot n$, and $p \stackrel{\text{def}}{=} |A|/|A'|$, then

$$d \cdot [1 - \rho(v(A))] \geq \ln(p).$$

The following claim shows that if there exists such a subset A' then Lemma 2.1 follows by the inductive hypothesis for A'.

Claim 3.2 *If there exists $A' \subset A$ such that $v(A') < v(A)$, and such that*

$$[v(A) \cdot n - v(A') \cdot n] \cdot [2^{15} \cdot \ln(v(A))/v(A)^{3/2}] \geq \ln(|A|/|A'|)$$

then

$$|A| \leq (C_0)^n \cdot \left(\prod_{r=C_0 \cdot n+1}^{v(A) \cdot n} \rho(r/n) \right)^{-1}.$$

Proof:
Denote

$$d = v(A) \cdot n - v(A') \cdot n,$$

and

$$p = |A|/|A'|,$$

and denote

$$\delta = 2^{15} \cdot \ln(v(A))/v(A)^{3/2}.$$

Then we have

$$d \cdot \delta \geq \ln(p).$$

Since $v(A') < v(A)$, we can use the inductive hypothesis for A' to get

$$|A'| \leq (C_0)^n \cdot \left(\prod_{r=C_0 \cdot n+1}^{v(A') \cdot n} \rho(r/n) \right)^{-1},$$

and hence

$$|A| \leq (C_0)^n \cdot \left(\prod_{r=C_0 \cdot n+1}^{v(A') \cdot n} \rho(r/n) \right)^{-1} \cdot p.$$

Therefore, to prove Claim 3.2 we just have to verify that

$$p \leq \left(\prod_{r=v(A') \cdot n+1}^{v(A) \cdot n} \rho(r/n) \right)^{-1}.$$

This is true because,

$$\left(\prod_{r=v(A') \cdot n+1}^{v(A) \cdot n} \rho(r/n) \right)^{-1} = \left(\prod_{r=v(A) \cdot n-(d-1)}^{v(A) \cdot n} \rho(r/n) \right)^{-1} \geq$$

$$\rho(v(A))^{-d} = (1-\delta)^{-d} \geq e^{d \cdot \delta} \geq e^{\ln(p)} = p,$$

(where e is the base for the natural logarithm.) $\square$

Thus all we need in order to prove Lemma 2.1 is to find $A' \subset A$ that satisfies the requirements of Claim 3.2. The set A' will be defined differently in each one of three cases.

In all that comes below we denote by π a random permutation uniformly distributed over the set A. This is referred to explicitly by writing $\pi \in_R A$. We are now ready to do the first case, which is the easiest one.

The first case:

Claim 3.3 *If there exist $i \in \{1, ..., n\}$ and $j \in A(i)$ such that*

$$PROB_{\pi \in_R A}[\pi(i) = j] < v(A)^{-2}$$

then

$$|A| \leq (C_0)^n \cdot \left(\prod_{r=C_0 \cdot n+1}^{v(A) \cdot n} \rho(r/n) \right)^{-1}.$$

Proof:
The proof doesn't use the condition that the VC-dimension of A is 2. We define A' by

$$A' = \{\pi \in A \mid \pi(i) \neq j\},$$

that is, we restrict $\pi(i)$ to be different than j. We will show that A' satisfies the requirements of Claim 3.2.

Obviously, $|A'(i)| = |A(i)| - 1$. Also, since $A' \subset A$, for every $l \in \{1, ..., n\}$ we have $|A'(l)| \leq |A(l)|$. Hence,

$$\sum_{l=1}^{n} |A'(l)| \leq \sum_{l=1}^{n} |A(l)| - 1,$$

that is

$$d \stackrel{\text{def}}{=} v(A) \cdot n - v(A') \cdot n \geq 1.$$

Since we assumed that $\mathrm{PROB}_{\pi \in_R A}[\pi(i) = j] < v(A)^{-2}$, we have

$$|A'| > |A| \cdot (1 - v(A)^{-2}),$$

that is,

$$p \stackrel{\text{def}}{=} |A|/|A'| < (1 - v(A)^{-2})^{-1},$$

and since by $v(A) \geq C_0$ we can assume that $v(A)$ is not too small we have

$$\ln(p) < \ln((1 - v(A)^{-2})^{-1}) < \ln(1 + 2 \cdot v(A)^{-2}) < 2 \cdot v(A)^{-2} < 1 - \rho(v(A)).$$

Thus A' satisfies the requirements of Claim 3.2. $\square$

Hence, if there exist $i \in \{1, ..., n\}$ and $j \in A(i)$ such that $\mathrm{PROB}_{\pi \in_R A}[\pi(i) = j] < v(A)^{-2}$ the proof of Lemma 2.1 follows from Claim 3.3. We can therefore assume for the rest of the proof that for every $i \in \{1, ..., n\}$ and $j \in A(i)$,

$$\mathrm{PROB}_{\pi \in_R A}[\pi(i) = j] \geq v(A)^{-2}.$$

For the rest of the paper let us denote for simplicity by $[q, r]$ the set of integers $\{q, q + 1, ..., r - 1, r\}$, and by $[n]$ the set $[1, n]$. For the rest of the proof we will need the following technical lemma. Intuitively, the lemma claims that there exist two indices $s, t \in [1, n]$ and a large set of indices $I \subset [1, n]$ such that for every $i \in I$, $A(i)$ has a large intersection with each of the sets: $[1, s]$, $[s, t]$ and $[t, n]$. The lemma will be proved for any set $A \subset S_n$ (we do not use here the condition that the VC-dimension of A is 2). In fact, the lemma is solely about the sets $A(i)$ and doesn't use the fact that A is a set of permutations. We will assume (for simplicity) that $v(A)$ is larger than some fixed constant (say $v(A) > 20$). That's OK because we can assume that $C_0 \geq 20$. The proof of the lemma is deferred to the next section.

Lemma 3.1 *For every n and every $A \subset S_n$, if $v(A) > 20$ then there exist two indices $s \leq t$, a number $m \geq (1/16) \cdot v(A)$ and a set $I \subset [1, n]$ with $|I| = m$ such that for every $i \in I$:*

1. $|A(i)| \geq (1/2) \cdot v(A)$
2. $|A(i) \cap [1, s]| \geq (1/8) \cdot |A(i)|$
3. $|A(i) \cap [t, n]| \geq (1/8) \cdot |A(i)|$
4. $|A(i) \cap [s, t]| \geq (1/68) \cdot v(A)^{3/2} \cdot m^{-1}$

Fix s, t, m, I from Lemma 3.1. For simplicity we assume that m is larger than some fixed constant (say $m > 20$). That's OK because we can assume that C_0 is large enough. Note that so far we have not used the assumption that the VC-dimension of A is 2. This assumption will be used now.

For every $i \neq j$, denote by $R_{i,j}$ the set of all $k \in [n] \setminus \{i, j\}$ such that the projection of A on the 3 elements i, j, k does not contain the linear order (i, k, j), i.e., the set of all $k \in [n] \setminus \{i, j\}$ such that no permutation $\pi \in A$ satisfies $\pi(i) < \pi(k) < \pi(j)$. For $i = j$ we define $R_{i,j}$ to be the empty set. Since the VC-dimension of A is 2, no triple (i, j, k) appears in all 6 possible linear orders, and hence every triple (i, j, k) contributes 1 to at least one of the 6 sets: $R_{i,j}$,$R_{j,i}$,$R_{i,k}$,$R_{k,i}$,$R_{j,k}$,$R_{k,j}$. Therefore,

$$\sum_{i,j} |R_{i,j}| \geq \binom{n}{3}.$$

In the same way, we can restrict ourselves to I. We define $R_{i,j}(I) = R_{i,j} \cap I$ and we get

$$\sum_{(i,j) \in I \times I} |R_{i,j}(I)| \geq \binom{m}{3} > (1/8) \cdot m^3.$$

Now define

$$J = \{(i, j) \in I \times I \mid |R_{i,j}(I)| \geq (1/16) \cdot m\},$$

that is, J is the set of all pairs $(i, j) \in I \times I$ such that $|R_{i,j}(I)|$ is not too small. Since for every i, j we have $|R_{i,j}(I)| < m$, we can conclude

$$(1/8) \cdot m^3 < \sum_{(i,j) \in I \times I} |R_{i,j}(I)| = \sum_{(I \times I) \setminus J} |R_{i,j}(I)| + \sum_{J} |R_{i,j}(I)| \leq m^2 \cdot (1/16) \cdot m + |J| \cdot m,$$

that is,

$$|J| > (1/16) \cdot m^2.$$

We are now ready to do the second case of the induction.

The second case:

Claim 3.4 *If there exists $(i, j) \in J$ such that*

$$PROB_{\pi \in_R A}[(\pi(i) \in [1, s]) \wedge (\pi(j) \in [t, n])] \geq 2^{-10} v(A)^{-2}$$

then

$$|A| \leq (C_0)^n \cdot \left(\prod_{r=C_0 \cdot n+1}^{v(A) \cdot n} \rho(r/n) \right)^{-1}.$$

Proof:

In this case, we define A' by

$$A' = \{\pi \in A \mid (\pi(i) \in [1, s]) \wedge (\pi(j) \in [t, n])\},$$

that is, we restrict $\pi(i)$ to be in $[1, s]$ and $\pi(j)$ to be in $[t, n]$. We will show that A' satisfies the requirements of Claim 3.2.

For every $k \in R_{i,j}(I)$, the projection of A on the 3 elements i, j, k does not contain the linear order (i, k, j). Therefore after we restrict $\pi(i)$ to be in $[1, s]$ and $\pi(j)$ to be in $[t, n]$, we cannot have $\pi(k) \in [s, t]$. Hence, for every $k \in R_{i,j}(I)$,

$$|A'(k)| \leq |A(k)| - |A(k) \cap [s, t]| \leq |A(k)| - (1/68) \cdot v(A)^{3/2} \cdot m^{-1}.$$

Since $(i, j) \in J$,

$$|R_{i,j}(I)| \geq (1/16) \cdot m.$$

Hence,

$$\sum_{k=1}^{n} |A'(k)| \leq \sum_{k=1}^{n} |A(k)| - (1/16) \cdot m \cdot (1/68) \cdot v(A)^{3/2} \cdot m^{-1}.$$

That is,

$$d \stackrel{\text{def}}{=} v(A) \cdot n - v(A') \cdot n \geq (1/1088) \cdot v(A)^{3/2}.$$

Since we assumed that $\mathrm{PROB}_{\pi \in_R A}[(\pi(i) \in [1, s]) \wedge (\pi(j) \in [t, n])] \geq 2^{-10} v(A)^{-2}$, we have

$$|A'| \geq |A| \cdot 2^{-10} v(A)^{-2},$$

that is,

$$p \stackrel{\text{def}}{=} |A|/|A'| \leq 2^{10} v(A)^2.$$

and since by $v(A) \geq C_0$ we can assume that $v(A)$ is large enough (say $v(A) \geq 2^{10}$) we have

$$\ln(p) \leq \ln(v(A)^3) = 3 \cdot \ln(v(A)).$$

Thus A' satisfies the requirements of Claim 3.2. □

We will now assume that the requirements of Claim 3.3 and Claim 3.4 are not satisfied. This will be the third case of the induction.

The third case:

Claim 3.5 *If for every $i \in \{1, ..., n\}$ and $k \in A(i)$,*

$$PROB_{\pi \in_R A}[\pi(i) = k] \geq v(A)^{-2},$$

and for every $(i, j) \in J$,

$$PROB_{\pi \in_R A}[(\pi(i) \in [1, s]) \wedge (\pi(j) \in [t, n])] < 2^{-10} v(A)^{-2}$$

then

$$|A| \leq (C_0)^n \cdot \left(\prod_{r = C_0 \cdot n + 1}^{v(A) \cdot n} \rho(r/n) \right)^{-1}.$$

Proof:
For every $i \in I$ define

$$J_i = \{j \in I \mid (i, j) \in J\}.$$

Since $|J| > (1/16) \cdot m^2$, there exists i_0 such that

$$|J_{i_0}| > (1/16) \cdot m \geq (1/256) \cdot v(A).$$

W.l.o.g assume that

$$|J_{i_0}| = \lceil (1/256) \cdot v(A) \rceil,$$

(otherwise discard arbitrarily some elements from J_{i_0}).

Here we define A' by

$$A' = \{\pi \in A \mid (\pi(i_0) \in [1, s]) \wedge (\text{for every } j \in J_{i_0}, \pi(j) \notin [t, n])\},$$

We will show that A' satisfies the requirements of Claim 3.2.

Since $|J_{i_0}| \geq (1/256) \cdot v(A)$, and since for every $j \in J_{i_0}$,

$$|A(j)| - |A'(j)| \geq |A(j) \cap [t, n]| \geq (1/8) \cdot |A(j)| \geq (1/16) \cdot v(A),$$

we have

$$\sum_{j=1}^{n} |A'(j)| \leq \sum_{j=1}^{n} |A(j)| - (1/256) \cdot v(A) \cdot (1/16) \cdot v(A).$$

That is,

$$d \stackrel{\text{def}}{=} v(A) \cdot n - v(A') \cdot n \geq (2^{-12}) \cdot v(A)^2.$$

Let us now turn to bounding $|A|/|A'|$. Since

$$|A(i_0) \cap [1, s]| \geq (1/8) \cdot |A(i_0)| \geq (1/16) \cdot v(A),$$

and since for every $k \in A(i_0)$,

$$\text{PROB}_{\pi \in_R A}[\pi(i_0) = k] \geq v(A)^{-2},$$

we have

$$\mathrm{PROB}_{\pi \in_R A}[\pi(i_0) \in [1, s]] \geq (1/16) \cdot v(A) \cdot v(A)^{-2} = (1/16) \cdot v(A)^{-1}.$$

Also, since for every $(i, j) \in J$

$$\mathrm{PROB}_{\pi \in_R A}[(\pi(i) \in [1, s]) \wedge (\pi(j) \in [t, n])] < 2^{-10} v(A)^{-2},$$

we have for every $j \in J_{i_0}$,

$$\mathrm{PROB}_{\pi \in_R A}[(\pi(j) \in [t, n]) \ \mid \ (\pi(i_0) \in [1, s])] =$$

$$\mathrm{PROB}_{\pi \in_R A}[(\pi(j) \in [t, n]) \wedge (\pi(i_0) \in [1, s])] \ / \ \mathrm{PROB}_{\pi \in_R A}[\pi(i_0) \in [1, s]]$$
$$< 2^{-10} v(A)^{-2} \ / \ [(1/16) \cdot v(A)^{-1}] = 2^{-6} v(A)^{-1}.$$

Therefore

$$\mathrm{PROB}_{\pi \in_R A}[(\exists j \in J_{i_0} \text{ s.t., } \pi(j) \in [t, n]) \ \mid \ (\pi(i_0) \in [1, s])] \ <$$
$$|J_{i_0}| \cdot 2^{-6} v(A)^{-1} = \lceil (1/256) \cdot v(A) \rceil \cdot 2^{-6} v(A)^{-1} < 2^{-13},$$

(where we assume again that $v(A)$ is large enough).

We can conclude that

$$|A'| = |A| \cdot \mathrm{PROB}_{\pi \in_R A}[\pi(i_0) \in [1, s]] \cdot \mathrm{PROB}_{\pi \in_R A}[(\forall j \in J_{i_0}, \ \ \pi(j) \notin [t, n]) \ \mid \ (\pi(i_0) \in [1, s])]$$
$$\geq |A| \cdot (1/16) \cdot v(A)^{-1} \cdot (1 - 2^{-13}) > |A| \cdot (1/32) \cdot v(A)^{-1},$$

That is

$$p \stackrel{\text{def}}{=} |A|/|A'| < 32 \cdot v(A) < v(A)^2,$$

(for large enough $v(A)$).

Thus A' satisfies the requirements of Claim 3.2. □

4 Proof of the Technical Lemma

In this section we give the proof of Lemma 3.1. Define

$$I_0 = \{i \in [n] \mid |A(i)| \geq (1/2) \cdot v(A)\}.$$

Obviously,

$$\sum_{I_0} |A(i)| = \sum_{[n]} |A(i)| - \sum_{[n] \setminus I_0} |A(i)| = n \cdot v(A) - \sum_{[n] \setminus I_0} |A(i)|$$
$$\geq n \cdot v(A) - n \cdot (1/2) \cdot v(A) = (1/2) \cdot n \cdot v(A).$$

The set I will be defined to be a subset of I_0.

For every $i \in I_0$, let $s_i \leq t_i$ be two indices such that

1. $|A(i) \cap [1, s_i]| \geq (1/4) \cdot |A(i)|$,

2. $|A(i) \cap [t_i, n]| \geq (1/4) \cdot |A(i)|$,

3. $|A(i) \cap [s_i, t_i]| \geq (1/2) \cdot |A(i)|$,

and define

$$\widetilde{A(i)} = A(i) \cap [s_i, t_i].$$

Then

$$\sum_{I_0} |\widetilde{A(i)}| \geq (1/2) \cdot \sum_{I_0} |A(i)| \geq (1/4) \cdot n \cdot v(A).$$

We will define the indices s, t to be such that

$$|[s, t]| = \lceil (1/16) \cdot v(A) \rceil.$$

Since $[n]$ can be covered by $\lceil 16n/v(A) \rceil$ such intervals, we will be able to find such s, t that also satisfy

$$\sum_{I_0} |\widetilde{A(i)} \cap [s, t]| \geq (1/4) \cdot n \cdot v(A) / \lceil 16n/v(A) \rceil$$

$$\geq (1/4) \cdot n \cdot v(A)/(17n/v(A)) = (1/68) \cdot v(A)^2.$$

We can now define $I_1 \subset I_0$ by

$$I_1 = \{i \in I_0 \mid |\widetilde{A(i)} \cap [s, t]| > 0\},$$

and get

$$\sum_{I_1} |A(i) \cap [s, t]| \geq \sum_{I_1} |\widetilde{A(i)} \cap [s, t]| = \sum_{I_0} |\widetilde{A(i)} \cap [s, t]| \geq (1/68) \cdot v(A)^2.$$

The set I will be defined to be a subset of I_1.

Every $i \in I_1$ already satisfies the first 3 requirements of the lemma:

1. By the definition of I_0,

$$|A(i)| \geq (1/2) \cdot v(A).$$

2. By the definition of I_1 we have $|\widetilde{A(i)} \cap [s, t]| > 0$, and therefore by the definition of $\widetilde{A(i)}$ we can conclude that $s_i \leq t$. Hence,

$$|A(i) \cap [1, s]| \geq |A(i) \cap [1, s_i]| - |[s+1, t]| \geq (1/4) \cdot |A(i)| - \lceil (1/16) \cdot v(A) \rceil + 1$$

$$\geq (1/4) \cdot |A(i)| - (1/16) \cdot v(A) \geq (1/4) \cdot |A(i)| - (1/8) \cdot |A(i)| = (1/8) \cdot |A(i)|.$$

3. In the same way,

$$|A(i) \cap [t, n]| \geq (1/8) \cdot |A(i)|.$$

Since I will be a subset of I_1, every $i \in I$ will satisfy requirements 1,2,3. Thus we only have to make sure that I is large enough and that every $i \in I$ satisfies requirement 4. We will now split the proof into two cases:

Case A:

$$|I_1| \geq (1/68) \cdot v(A)^{3/2}.$$

In this case we define $I = I_1$, and since we assumed that $v(A) > 20$ we have

$$m = |I_1| \geq (1/68) \cdot v(A)^{3/2} \geq (1/16) \cdot v(A).$$

For every $i \in I_1$ requirement 4 is satisfied by

$$|A(i) \cap [s,t]| \geq |\widetilde{A(i)} \cap [s,t]| \geq 1 \geq (1/68) \cdot v(A)^{3/2} \cdot m^{-1}.$$

Case B:

$$|I_1| < (1/68) \cdot v(A)^{3/2}.$$

In this case we define I by

$$I = \{i \in I_1 \mid |A(i) \cap [s,t]| \geq (1/2) \cdot v(A)^{1/2}\}.$$

Then

$$\begin{aligned}
\sum_I |A(i) \cap [s,t]| &= \sum_{I_1} |A(i) \cap [s,t]| - \sum_{I_1 \setminus I} |A(i) \cap [s,t]| \\
&\geq \sum_{I_1} |A(i) \cap [s,t]| - |I_1| \cdot (1/2) \cdot v(A)^{1/2} \\
&\geq \sum_{I_1} |A(i) \cap [s,t]| - (1/68) \cdot v(A)^{3/2} \cdot (1/2) \cdot v(A)^{1/2} \\
&\geq (1/68) \cdot v(A)^2 - (1/136) \cdot v(A)^2 = (1/136) \cdot v(A)^2.
\end{aligned}$$

But for every i

$$|A(i) \cap [s,t]| \leq |[s,t]| = \lceil (1/16) \cdot v(A) \rceil \leq (2/17) \cdot v(A),$$

(where we used again the assumption $v(A) > 20$). Hence,

$$|I| \cdot (2/17) \cdot v(A) \geq \sum_I |A(i) \cap [s,t]| \geq (1/136) \cdot v(A)^2,$$

that is

$$m = |I| \geq (1/16) \cdot v(A).$$

Requirement 4 is satisfied for every $i \in I$, since by the definition of I,

$$|A(i) \cap [s,t]| \geq (1/2) \cdot v(A)^{1/2} \geq (1/68) \cdot v(A)^{3/2} \cdot m^{-1}.$$

□

Acknowledgments

I would like to thank Mario Szegedy for introducing me to the acyclic linear orders problem and for many important discussions that led to this result. I would like to thank Peter Fishburn for the encouragement in writing up this manuscript.

References

[Abe] J.M. Abello, "The weak Bruhat order of S_Σ, consistent sets, and Catalan numbers", *SIAM Journal of Discrete Math.*, 4, (1991), 1–16.

[Bla] D.J. Black, "The theory of committees and elections", Cambridge Press, London, 1958.

[Con] Marquis de Condorcet, "Essai sur l'application de l'analyse à la probabilité des decisions rendues à la pluralité de voix", Paris, 1785.

[Fis] P. Fishburn, "Acyclic sets of linear orders", *Social Choice and Welfare*, 14, (1997), 113–124.

[Rik] W.H. Riker, "Arrow's theorem and some examples of the paradox of voting", Foundation monograph, Southern Methodist University Press, Dallas, 1961.

[Sau] N. Sauer, "On the density of families of sets", *Journal of Combinatorial Theory*, Series A 13, (1972), 145–147.

[VC] V.N. Vapnik and A.Ya Chervonenkis, "On the uniform convergence of relative frequencies of events to their probabilities", *Theory of Probability Applications*, 16, (1971), 264–280.