

# Topics around Vapnik-Chevronenkis theory

<b>1</b>	<b>The Sauer-Shelah Lemma</b>	<b>2</b>
1	Two equivalent frameworks	2
2	The Sauer-Shelah Lemma	4
3	Pajor variant and the method of shifting	5
4	Notes and references	7
<b>2</b>	<b>Samples and approximations of measures</b>	<b>8</b>
1	Samples and subsamples	8
2	Discrepancy	8
3	Random colorings	9
4	Important inequalities	10
5	A uniform law of large numbers	10
<b>3</b>	<b>A piercing problem</b>	<b>14</b>
1	Appendix: Farkas' lemma	16

# Chapter 1

## The Sauer-Shelah Lemma

### 1 Two equivalent frameworks

Let  $\mathcal{U}$  and  $\mathcal{V}$  be two sets and let  $\varphi \subseteq \mathcal{U} \times \mathcal{V}$ . In other words  $\varphi$  is a **bipartite graph**. We may call  $\varphi$  an (abstract) **incidence relation** and write  $\varphi(x, y)$  for  $\langle x, y \rangle \in \varphi$ . Sets of the form

$$\varphi(\mathcal{U}, b) = \{a \in \mathcal{U} : \varphi(a, b)\}$$

are called **definable sets** or, when other relations are involved,  **$\varphi$ -definable sets**. The collection of all definable sets is denoted by  $\varphi(\mathcal{U}, b)_{b \in \mathcal{V}}$ .

Often we need to consider the **trace** of a definable set on some arbitrary  $A \subseteq \mathcal{U}$

$$\varphi(A, b) = \{a \in A : \varphi(a, b)\}.$$

We call this a **definable subset of  $A$**  and denote by  $\varphi(A, b)_{b \in \mathcal{V}}$  the collection of definable subsets on  $A$ .

Given  $A \subseteq \mathcal{U}$  define the equivalence relation  $\equiv_{\varphi, A}$  defined by

$$\begin{aligned} b \equiv_{\varphi, A} b' &\Leftrightarrow \varphi(a, b) \leftrightarrow \varphi(a, b') \quad \text{for all } a \in A; \\ &\Leftrightarrow \varphi(A, b) = \varphi(A, b'). \end{aligned}$$

The  $\equiv_{\varphi, A}$ -equivalence class are called **types over  $A$** . We denote by  $S_\varphi(A)$  the set types over  $A$ . As there is a one-to-one correspondence between definable subsets and types,  $|S_\varphi(A)| = |\varphi(A, b)_{b \in \mathcal{V}}|$ .

If all subsets of  $A$  are definable, that is  $\mathcal{P}A = \varphi(A, b)_{b \in \mathcal{V}}$ , we say that  $A$  is **shattered** by  $\varphi$ . The following is called the **shatter function**

$$\begin{aligned} \pi_\varphi(n) &= \max \left\{ |\varphi(A, b)_{b \in \mathcal{V}}| : A \in \binom{\mathcal{U}}{n} \right\}. \\ &= \max \left\{ |S_\varphi(A)| : A \in \binom{\mathcal{U}}{n} \right\}. \end{aligned}$$

So,  $\pi_\varphi(n)$  gives the maximal number of definable subsets that a set of cardinality  $n$  may have. Trivially,  $\pi_\varphi(n) \leq 2^n$  for all  $n$ . Moreover, if  $\pi_\varphi(k) = 2^k$  for some  $k$ , then  $\pi_\varphi(n) = 2^n$  for every  $n \leq k$ .

The dual incidence relation  $\varphi^*$  is the relation on  $\mathcal{V} \times \mathcal{U}$  which is sometimes denoted by  $\varphi^{-1}$ . Then dual scattering function is defined as follows (with the obvious meaning of the notation)

$$\begin{aligned} \pi_\varphi^*(n) &= \max \left\{ |\varphi(a, B)_{a \in \mathcal{U}}| : B \in \binom{\mathcal{V}}{n} \right\}. \\ &= \max \left\{ |S_{\varphi^*}(B)| : B \in \binom{\mathcal{V}}{n} \right\}. \end{aligned}$$

**1.1 Definition** The **Vapnik-Chervonenkis dimension** of  $\varphi$ , abbreviated by **VC-dimension**,

is the maximal cardinality of a finite set  $A \subseteq \mathcal{U}$  that is shattered by  $\varphi$ . Equivalently, it is the maximal  $k$  such that  $\pi_\varphi(k) = 2^k$ . If such a maximum does not exist, we say that  $\varphi$  has infinite VC-dimension.

We will say **dual VC-dimension** for the VC-dimension of  $\varphi^*$ .

The **VC-density** of  $\varphi$  is the infimum over all real number  $r$  such that  $\pi_\varphi(n) \in O(n^r)$ . It is infinite if no such  $r$  exist. The **dual VC-density** is defined accordingly.  $\square$

Then if the VC-density is finite so is the VC-dimension. The converse is also true. In fact, in the next section we show that the VC-dimension bounds the VC-density.

**1.2 Proposition** If  $\varphi$  has VC-dimension  $< k$  then its dual VC-dimension is  $< 2^{k+1}$ .

**Proof** Assume that the VC-dimension of  $\varphi^*$  is  $\geq 2^k$ . We prove that the VC-dimension of  $\varphi$  is  $\geq k$ . Let  $B = \{b_I : I \subseteq [k]\}$  be a set of cardinality  $2^k$  shattered by  $\varphi^*$ . That is, for every  $\mathcal{J} \subseteq \mathcal{P}([k])$  there is  $a_{\mathcal{J}}$  such that

$$\varphi(a_{\mathcal{J}}, b_I) \Leftrightarrow I \in \mathcal{J}$$

Let  $a_i = a_{\{I \subseteq [k] : i \in I\}}$ . Then from the equivalence above we obtain

$$\varphi(a_i, b_I) \Leftrightarrow i \in I$$

That is,  $\varphi$  shatters  $\{a_i : i \in [k]\}$ .  $\square$

An alternative formalism uses **set systems** in place of incidence relations. A set system is a collection  $\Phi$  of subsets of some set  $\mathcal{U}$ . We denote a set system by  $(\mathcal{U}, \Phi)$ . Given a set system, we immediately obtain an incidence relation. Fix any  $\mathcal{V}$  containing  $\Phi$  and define  $\varphi(x, y)$  as  $x \in y \in \Phi$ .

Vice versa, to an incidence relation  $\varphi$  we associate  $\Phi = \{\varphi(\mathcal{U}, b) : b \in \mathcal{V}\}$ , the set system of the definable subsets of  $\mathcal{U}$ . The **VC-dimension of  $\Phi$**  is defined to be that of the associated incidence relation. The shatter function  $\pi_\Phi(n)$  is defined in a similar way.

An incidence relation is **extensional** if  $\varphi(\mathcal{U}, b) = \varphi(\mathcal{U}, b')$  implies  $b, b' \in \mathcal{V}$ . The correspondence between extensional incidence relations and set systems is one-to-one. In general, the correspondence is many-to-one. However, as we are mainly interested the set system associated, we may switch from one formalism to the other according to which one is more convenient.

- 1.3 Example**
- a. Set systems of cardinality 1 are those with an incidence relation of the form  $A \times \mathcal{V}$  for some  $A \subseteq \mathcal{U}$ . They shatter only the empty set, therefore they have VC-dimension 0. Their shatter function is identically 1.
  - b. Let  $\Phi$  be a non trivial partition of  $\mathcal{U}$ . Then only singletons are shattered, so the VC-dimension is 1. The shatter function is  $\pi_\Phi(n) = \min\{n, |\Phi|\}$ .
  - c. If  $\Phi$  is a non trivial chain of subsets of  $\mathcal{U}$  the situation is identical to that described in b.
  - d. Let  $\mathcal{U} = \mathbb{R}$  and let  $\Phi$  be the collection of open intervals. Any set of 2 points is shattered but no set with 3 points can. So the VC-dimension is 2.
  - e. Let  $\mathcal{U} = \mathbb{R}^2$  and let  $\Phi$  be the collection of half planes. Any set of 3 non collinear points is shattered but no set with 4 points can (by Radon's Theorem). So the VC-dimension is 3.

- f. Let  $\Phi = \mathcal{U}^{[\leq k]}$  be the collection of all subsets of  $\mathcal{U}$  of cardinality  $\leq k$ . Then  $\Phi$  has VC-dimension  $k$  and

$$\pi_{\Phi}(n) = \sum_{i=0}^k \binom{n}{i}.$$

- g. Let  $\mathcal{U} = \mathbb{R}^2$  and let  $\Phi$  be the collection of polygons. Then  $\Phi$  has VC-dimension  $\infty$ . □

## 2 The Sauer-Shelah Lemma

According to Gil Kalai in [3], Sauer-Shelah's Lemma can be described as an *eigen-theorem* because it is important in many different areas of mathematic (model theory, learning theory, probability theory, ergodic theory, Banach spaces, to name a few). No wonder it has been discovered and rediscovered many times.

It has been proved independently by Shelah [6], Sauer [5], and Vapnik-Chervonenkis [7] around 1970 (Shelah gives credit to Micha Perles). Saharon Shelah was working in model theory while Norbert Sauer, Vladimir Vapnik and Alexey Chervonenkis were in statistical learning theory.

We shall present three proofs of this lemma, one in this section and two in the next section. I am aware of a forth proof which uses linear algebra, see e.g. [2].

**1.4 Proposition (Sauer-Shelah's Lemma)** *If  $\varphi$  has VC-dimension  $k$  then for every  $n \geq k$*

$$\pi_{\varphi}(n) \leq \sum_{i=0}^k \binom{n}{i}.$$

The set system presented in f of Example 1.3 shows that the bound is optimal.

**Proof** If  $k = 0$ , both sides of the inequality are 1. Now, assume the lemma is true for  $k - 1$ . We prove by induction on  $n$  that for every  $A$  of cardinality  $n$

$$|\varphi(A, b)_{b \in \mathcal{V}}| \leq \sum_{i=0}^k \binom{n}{i}.$$

If  $n = k$  the r.h.s. of the inequality above is  $2^n$  and the claim is trivial. So, assume the claim is true for  $n - 1$  and let  $A$  have cardinality  $n$ . Fix some  $a \in A$  and let  $A' = A \setminus \{a\}$ . We can assume that  $\varphi(A, b) \triangle \varphi(A, b') = \{a\}$  for some  $b, b'$ , otherwise  $|\varphi(A, b)_{b \in \mathcal{V}}| = |\varphi(A', b)_{b \in \mathcal{V}}|$  and the claim follows immediately from the induction hypothesis.

Define a new incidence relation

$$\psi(x, y) = x \in A' \wedge \varphi(x, y) \wedge \exists y' [\varphi(A, y) \triangle \varphi(A, y') = \{a\}].$$

Note that if  $A''$  is shattered by  $\psi$  then  $A'' \cup \{a\}$  it is shattered by  $\varphi$ . Then the VC-dimension of  $\psi$  is at most  $k - 1$ . We also have that

$$|\varphi(A, b)_{b \in \mathcal{V}}| = |\varphi(A', b)_{b \in \mathcal{V}}| + |\psi(A', b)_{b \in \mathcal{V}}|.$$

Hence by induction hypothesis

$$|\varphi(A, b)_{b \in \mathcal{V}}| \leq \sum_{i=0}^k \binom{n-1}{i} + \sum_{i=0}^{k-1} \binom{n-1}{i}$$

$$\begin{aligned}
&= \binom{n-1}{0} + \sum_{i=1}^k \left[ \binom{n-1}{i} + \binom{n-1}{i-1} \right] \\
&= \binom{n-1}{0} + \sum_{i=1}^k \binom{n}{i} \\
&\leq \sum_{i=0}^k \binom{n}{i}
\end{aligned}$$

which completes the proof of the proposition.  $\square$

Next corollary states an important dichotomy. It says that the shatter function grows exponentially unless the VC-dimension is finite. In this case the growth is only polynomial. Therefore the VC-dimension is an upper bound to the VC-density.

**1.5 Corollary** *For every incidence relation  $\varphi$  one of the following obtains*

1. *the VC-dimension is infinite and  $\pi_\varphi(n) = 2^n$  for every positive integer  $n$ ;*
2. *the VC-dimension is  $k$  and  $\pi_\varphi(n) \in O(n^k)$ .*

**Proof** If VC-dimension is infinite claim 1 is obvious. So assume  $\varphi$  has VC-dimension is  $k$ . Then

$$\pi_\varphi(n) \leq \sum_{i=0}^k \binom{n}{i} \leq \sum_{i=0}^k \frac{n^i}{i!} \leq e n^k \quad \square$$

### 3 Pajor variant and the method of shifting

An alternative proof of the Sauer-Shelah's Lemma derives it as corollary of a lemma by Alain Pajor [4].

**1.6 Proposition (Pajor's Lemma)** *Let  $A \subseteq \mathcal{U}$  be finite. Then  $\varphi$  shatters at least  $|S_\varphi(A)|$  subsets of  $A$ .*

We show how Sauer-Shelah's Lemma follows from Pajor's Lemma. Fix a set  $A \subseteq \mathcal{U}$  of cardinality  $n$  such that  $\pi_\varphi(n) = |S_\varphi(A)|$ . By Pajor's Lemma there are  $|S_\varphi(A)|$  subsets of  $A$  shattered by  $\varphi$ . These subsets cannot have cardinality larger than the VC-dimension of  $\varphi$ , then

$$\pi_\varphi(n) = |\varphi(A, b)_{b \in \mathcal{V}}| \leq \left| \bigcup_{i=0}^k \binom{A}{i} \right| = \sum_{i=0}^k \binom{n}{i}.$$

**Proof** If  $A$  is empty then  $|S_\varphi(A)| = 1$  and  $\emptyset$  is the only subset of  $A$  that  $\varphi$  shatters. Fix  $a \in A$  and assume the lemma holds for  $A' = A \setminus \{a\}$ . Let  $\psi$  be the relation defined in the proof of Proposition 1.4. Recall that

$$|\varphi(A, b)_{b \in \mathcal{V}}| = |\varphi(A', b)_{b \in \mathcal{V}}| + |\psi(A', b)_{b \in \mathcal{V}}|.$$

and that if  $A'' \subseteq A'$  is shattered by  $\psi$  then  $A'' \cup \{a\}$  is shattered by  $\varphi$ . By induction hypothesis  $\varphi$  shatters least  $|\varphi(A', b)_{b \in \mathcal{V}}|$  subsets of  $A'$  and at least  $|\psi(A', b)_{b \in \mathcal{V}}|$  containing  $a$ . The lemma follows.

We present a different wording of essentially the same proof. Consider the set system  $\Phi = \varphi(A, b)_{b \in \mathcal{V}}$  and reason by induction of  $|\Phi|$ . The proposition holds

trivially if  $|\Phi| = 1$ . Now, suppose it holds for set systems of cardinality  $< |\Phi|$ . Fix  $a \in A$  and let  $\Phi_0 = \{B \in \Phi : a \notin B\}$  and  $\Phi_1 = \Phi \setminus \Phi_0$ . As  $|\Phi| > 1$ , we can choose  $a$  such that  $\Phi_i \neq \Phi$ . By the inductive hypothesis, both  $\Phi_i$  shatter at least  $|\Phi_i|$  subsets of  $A$ . If no set is shattered by both  $\Phi_i$ , the claim follows immediately. Otherwise, note that for each set shattered by both  $\Phi_i$  there are two sets shattered by  $\Phi$ , one containing  $a$  and one not containing  $a$ . The claim follows.  $\square$

We give different proof of Pajor's Lemma by a method which is interesting in itself because of its many applications. The method has been introduced by Erdős, Ko and Rado to prove their eponymous theorem. They named it *compression*, but is also known as *shifting*.

When  $A' \subseteq A$  and  $A \setminus A' = \{a\}$ , we write  $A' \subseteq_a A$ . We write

$$B_{\varphi,a} = \{b : \varphi(a,b) \text{ and } \neg \exists b' \varphi(\mathcal{U}, b') \subseteq_a \varphi(\mathcal{U}, b)\}$$

We say that  $\varphi$  is **compressed** if  $B_{\varphi,a} = \emptyset$  for every  $a \in \mathcal{U}$ .

**1.7 Proposition** *If  $\varphi$  is compressed then any co-finite subset of a definable set is definable. In particular  $\varphi$  shatters every finite subset of a definable set.*

**Proof** If for contradiction  $\psi(\mathcal{U}, b) \setminus \{a\}$  is not definable, then  $b \in B_{\varphi,a}$ .  $\square$

**1.8 Proposition** *Let  $\psi = \varphi \setminus \{a\} \times B_{\varphi,a}$ . Then*

$$\varphi(\mathcal{U}, b) = \varphi(\mathcal{U}, b') \Leftrightarrow \varphi(\mathcal{U}, b) = \varphi(\mathcal{U}, b') \quad \text{for all } b, b' \in \mathcal{V}.$$

**Proof**  $\Rightarrow$  Assume  $\varphi(\mathcal{U}, b) \neq \varphi(\mathcal{U}, b')$ . We may also assume that  $\varphi(\mathcal{U} \setminus \{a\}, b) = \varphi(\mathcal{U} \setminus \{a\}, b')$ , otherwise  $\psi(\mathcal{U}, b) \neq \psi(\mathcal{U}, b')$  is immediate. Then  $\varphi(a, b) \nleftrightarrow \varphi(a, b')$ , say  $\varphi(a, b)$  and  $\neg \varphi(a, b')$ . Then  $\varphi(\mathcal{U}, b') \subseteq_a \varphi(\mathcal{U}, b)$  and  $b \notin B_{\varphi,a}$ . So  $\psi(a, b)$  and  $\neg \psi(a, b')$ .

$\Leftarrow$  Assume  $\psi(\mathcal{U}, b) \neq \psi(\mathcal{U}, b')$ . Again, we may also assume that  $\psi(\mathcal{U} \setminus \{a\}, b) = \psi(\mathcal{U} \setminus \{a\}, b')$ . Then  $\psi(a, b) \nleftrightarrow \psi(a, b')$ , say  $\psi(a, b)$  and  $\neg \psi(a, b')$ . As  $\varphi(a, b)$  is clear, we only have to prove that  $\neg \varphi(a, b')$ . Suppose for a contradiction that  $\varphi(a, b')$ . Then  $b' \in B_{\varphi,a}$ . This is a contradiction as  $\psi(\mathcal{U}, b) \subseteq_a \psi(\mathcal{U}, b')$ .  $\square$

**1.9 Proposition** *Let  $\psi = \varphi \setminus \{a\} \times B_{\varphi,a}$ . Then every set shattered by  $\psi$  is shattered by  $\varphi$ .*

**Proof** Assume  $A$  is shattered by  $\psi$ . We prove that for every  $b$  here is a  $b'$  such that  $\psi(A, b) = \varphi(A, b')$ . We may assume that  $a \in A$ . If  $\psi(a, b)$  then we may chose  $b = b'$ . So, assume  $\neg \psi(a, b)$ . As  $\psi$  shatters  $A$  then there is  $c$  such that  $\psi(A, c) = \psi(A, b) \cup \{a\}$ . Then  $\exists b' \varphi(\mathcal{U}, b') \subseteq_a \varphi(\mathcal{U}, c)$ . Therefore  $\psi(A, b) = \varphi(A, b')$ .  $\square$

**1.10 Second proof of Pajor's Lemma** Let  $\varphi$  be a finite extensional incidence relation associated to  $\Phi$ . Let  $\varphi_0 = \varphi$  and  $\varphi_{i+1} = \varphi_i \setminus \{a\} \times B_{\varphi_i,a}$  for some  $a$ . As  $\varphi$  is finite, we can assume that at some stage  $n$  we obtain a compressed relation  $\psi = \varphi_n$ . Let  $\Psi$  be the set of  $\psi$ -definable sets. By Proposition 1.7,  $\Psi$  shatters at least  $|\Psi|$  sets. By Proposition 1.9, every set shattered by  $\Psi$  is shattered by  $\Phi$ . By Proposition 1.8,  $|\Psi| = |\Phi|$ .  $\square$

Define  $E_{\varphi,a} \subseteq \mathcal{V}^2$  as the set of e pairs  $\langle b', b \rangle$  such that  $\varphi(\mathcal{U}, b') \subseteq_a \varphi(\mathcal{U}, b)$ . Note incidentally that  $E_{\varphi,a}$  is the graph of a partial injections of  $\mathcal{V}$  into itself.

**1.11 Proposition** Let  $\psi = \varphi \setminus \{a\} \times B_{\varphi,a}$ . Then  $E_\varphi \subseteq E_\psi$

**Proof** Both the range and the domain of  $E_{\varphi,a}$  are disjoint from  $B_{\varphi,a}$ . □

We call  $E_\varphi = \bigcup_{a \in U} E_{\varphi,a}$  the unit distance diagram of  $\varphi$ .

**1.12 Proposition** Let  $\varphi$  be a finite extensional incidence relation with VC-dimension  $k$ . Then  $|E_\varphi| \leq k |\mathcal{V}|$ .

**Proof** Let  $\psi$  be as defined in Proof 1.10. By Propositions 1.7 and 1.9, every  $b \in \mathcal{V}$  has at most  $k$  ancestors. Therefore

$$\frac{|E_\varphi|}{|\mathcal{V}|} \leq \frac{|E_\psi|}{|\mathcal{V}|} \leq k \quad \square$$

## 4 Notes and references

- [1] R. P. Anstee, Lajos Rónyai, and Attila Sali, *Shattering news*, Graphs Combin. **18** (2002), no. 1, 59–73.
- [2] Timothy Gowers, *Dimension arguments in combinatorics*, Gowers’s Weblog (2008).
- [3] Gil Kalai, *Extremal Combinatorics III: Some Basic Theorems*, Combinatorics and more (2008).
- [4] Alain Pajor, *Sous-espaces  $l_1^n$  des espaces de Banach*, Travaux en Cours [Works in Progress], vol. 16, 1985.
- [5] N. Sauer, *On the density of families of sets*, J. Combinatorial Theory Ser. A **13** (1972), 145–147.
- [6] Saharon Shelah, *A combinatorial problem; stability and order for models and theories in infinitary languages*, Pacific J. Math. **41** (1972), 247–261.
- [7] V. N. Vapnik and A. Ya. Chervonenkis, *On the uniform convergence of relative frequencies of events to their probabilities*, Measures of complexity, Springer, Cham, 2015, pp. 11–30. Reprint of Theor. Probability Appl. **16** (1971), 264–280.

## Chapter 2

### Samples and approximations of measures

#### 1 Samples and subsamples

A sample is a just sequence of elements of  $\mathcal{U}$  where we disregard the order and only consider the number of times they appear. Formally, a **sample** is a **multiset**, that is is a function  $A : \mathcal{U} \rightarrow \mathbb{N}$ . We interpret  $A(x)$  as the **multiplicity** of the element  $x \in \mathcal{U}$ . The **support** of  $A$  is the set  $\text{supp}(A) = \{x : A(x) \neq 0\}$ . The **size of  $A$**  is defined as

$$|A| = \sum_{x \in \mathcal{U}} A(x).$$

If we identify sets with  $\{0, 1\}$ -valued samples, the size generalizes cardinality.

We say that  $C$  is a **subsample** of  $A$ , and write  $C \subseteq A$ , if  $C(x) \leq A(x)$  for all  $x \in \mathcal{U}$ . We also define the **intersection** and the **difference** of two samples. The element  $x \in \mathcal{U}$  has multiplicity  $A(x) \wedge C(x)$  in  $A \cap C$  and multiplicity  $A(x) \dot{-} C(x)$  in  $A \setminus C$ . Note that  $|A| = |A \cap C| + |A \setminus C|$ .

If  $\mathcal{B} \subseteq \mathcal{U}$  we define the **frequency** of  $\mathcal{B}$  over  $A$

$$\text{Fr}(\mathcal{B}/A) = \frac{|\mathcal{B} \cap A|}{|A|}$$

Note that  $\text{Fr}(\cdot/A)$  is a probability measure on  $\mathcal{U}$ .

An  **$\varepsilon$ -approximation** of a sample  $A$  is a subsample  $C \subseteq A$  such that for every definable set  $\mathcal{B}$

$$\left| \text{Fr}(\mathcal{B}/A) - \text{Fr}(\mathcal{B}/C) \right| \leq \varepsilon$$

With exception of enumerations, the definitions above easily generalize to **fractional samples** i.e., function with values on the non negative real. These will be used in the next chapter.

#### 2 Discrepancy

Given  $\varepsilon$  we are interested in the least  $n$  such that some  $\varepsilon$ -approximations of size  $n$  exist. The idea is to start with an approximation of large size and reduce size at the cost of slightly enlarging  $\varepsilon$ . We now introduce a powerful technique to achieve this.

In general  $\mathcal{U}$  may not be among the definable sets. As it is often convenient to include it, we write  $\Phi'$  for  $\Phi \cup \{\mathcal{U}\}$ .

Let  $C \subseteq A$  and  $\mathcal{B} \in \Phi'$ . We call the quantity

$$\Delta_{A,C,\mathcal{B}} = \frac{|C \cap \mathcal{B}| - |(A \setminus C) \cap \mathcal{B}|}{|A|}$$

the **discrepancy** of  $C$  in  $\mathcal{B}$ . The **relative discrepancy** of  $C$  in  $\mathcal{B}$  is



$$\delta_{A,C,\mathcal{B}} = \frac{\Delta_{A,C,\mathcal{B}}}{|A|}.$$

The **relative discrepancy** of  $C$  is

$$\delta_{A,C} = \sup_{\mathcal{B} \in \Phi'} |\delta_{A,C,\mathcal{B}}|.$$

The **relative discrepancy** of  $A$  is

$$\delta_A = \inf_{C \subseteq A} \delta_{A,C}$$

The next lemma is intuitive, if an  $\varepsilon$ -approximation has small discrepancy then we can halve its size at a small cost.

**2.1 Lemma** *Let  $A$  be a sample of size  $n$ . Let  $C \subseteq A$  have discrepancy  $\delta_{A,C}$ . Then either  $C$  or  $A \setminus C$  is an  $\varepsilon$ -approximation of size  $\leq n/2$  for  $\varepsilon = 2\delta_{A,C}$ .*

**Proof** Define  $n^+ = |C|$  and  $n^- = |A \setminus C|$ . We may assume that  $n^+ \leq n/2$ , otherwise swap  $C$  and  $A \setminus C$ . Then  $\delta_{A,C,\mathcal{U}} = (n^+ - n^-)/n < 0$ . Now, let  $\mathcal{B} \in \Phi'$  be arbitrary

$$\begin{aligned} 1. \quad \frac{|A \cap \mathcal{B}|}{n} &= \frac{|C \cap \mathcal{B}| + |(A \setminus C) \cap \mathcal{B}|}{n} \\ (*) &= \frac{2|C \cap \mathcal{B}|}{n} - \delta_{A,C,\mathcal{B}} \\ &\leq \frac{|C \cap \mathcal{B}|}{n^+} + \delta_{A,C} \end{aligned}$$

We also have

$$\begin{aligned} 2. \quad (*) &= \frac{|C \cap \mathcal{B}|}{n^+} (1 + \delta_{A,C,\mathcal{U}}) - \delta_{A,C,\mathcal{B}} \\ &\geq \frac{|C \cap \mathcal{B}|}{n^+} - 2\delta_{A,C} \end{aligned}$$

Combining 1 and 2 we obtain

$$\begin{aligned} |\text{Fr}(\mathcal{B}/A) - \text{Fr}(\mathcal{B}/C)| &\leq \left| \frac{|\mathcal{B} \cap A|}{n} - \frac{|\mathcal{B} \cap C|}{n^+} \right| \\ &\leq 2\delta_{A,C} \end{aligned}$$

as claimed by the lemma. □

### 3 Random colorings

An **enumeration** of a sample  $A$  is a tuple  $a = \langle a_1, \dots, a_n \rangle \in \mathcal{U}^n$  such that

$$A(x) = |\{i : a_i = x\}|.$$

Clearly, all enumerations of  $A$  have length  $n = |A|$ . We write **rng**( $a$ ) for the sample enumerated by  $a$ .

Fix an enumeration  $a = \langle a_1, \dots, a_n \rangle$  of  $A$ . A tuple  $c = \langle c_1, \dots, c_n \rangle \in \{-1, +1\}^n$  is called a **coloring**. To each coloring  $c$  we associate a subsample of  $A$

$$C_c(x) = |\{i : a_i = x, c_i = +1\}|$$

Note that the quantity

$$\Delta_{a,c,\mathcal{B}} = \sum_{a_i \in \mathcal{B}} c_i.$$

coincide with the discrepancy of  $C_c$  over  $\mathcal{B}$ . As in particular it does not depend the enumeration of  $A$ , below we will write  $\Delta_{A,c,\mathcal{B}}$

When

## 4 Important inequalities

**2.2 Proposition (Weak Law of Large Numbers)** *Let  $\mu$  be a probability measure on  $\mathcal{U}$ . Then, for every event  $\mathcal{B} \subseteq \mathcal{U}$  and every  $n, \varepsilon > 0$*

$$1 - \frac{1}{4n\varepsilon^2} < \mu^n \left( c \in \mathcal{U}^n : \left| \mu\mathcal{B} - \frac{1}{n} |c^\circ \cap \mathcal{B}| \right| \leq \varepsilon \right)$$

**Proof** Note that  $X = X(c) = |c^\circ \cap \mathcal{B}|$  is a binomial random variable with success probability  $p = \mu\mathcal{B}$ . Hence  $E(X) = p$  and  $\text{Var}(X) = p(1-p)/n$ . Apply Chebyshev's inequality.  $\square$

## 5 A uniform law of large numbers

An  **$\varepsilon$ -approximation** of a sample  $A$  is a subsample  $C \subseteq A$  such that for every definable set  $\mathcal{B}$

$$\left| \text{Fr}(A, \mathcal{B}) - \text{Fr}(C, \mathcal{B}) \right| \leq \varepsilon$$

We want to estimate the minimal size of an  $\varepsilon$ -approximation of  $A$ . We want a bound that depends solely on  $\varepsilon$ , not on the size of  $A$ . It is also important to note requirement of uniformity: the same approximation works for all definable sets.

If we allow  $C$  to depend on  $\mathcal{B}$ , its existence follows easily from the weak law of large numbers.

**2.3 Proposition (Weak law of large numbers)** *For every sample  $A$ , every  $\mathcal{B} \subseteq \mathcal{U}$  and every  $\varepsilon > 0$  there is a  $C \subseteq A$  of size  $n = 1/4\varepsilon^2$  such that  $|\text{Fr}(A, \mathcal{B}) - \text{Fr}(C, \mathcal{B})| \leq \varepsilon$ .*

**Proof** Define  $\text{Pr}(\cdot) = \text{Fr}(A, \cdot)$ . Fix  $\mathcal{B}$  and set  $p = \text{Pr}(\mathcal{B})$ . Consider the Bernoulli random variables  $X_i$  that on input  $c \in \mathcal{U}^n$  output

$$X_i(c) = \begin{cases} 1 & \text{if } c_i \in \mathcal{B} \\ 0 & \text{if } c_i \notin \mathcal{B} \end{cases}$$

Define also  $\bar{X} = \frac{1}{n} \sum_i X_i$ . Then  $E(\bar{X}) = p$  and  $\text{Var}(\bar{X}) = \frac{p(1-p)}{n} \leq \frac{1}{4n}$ .

If we set  $C = \text{rng}(c) \cap A$ , we obtain

$$\begin{aligned} |E(\bar{X}) - \bar{X}(c)| &= |\text{Fr}(A, \mathcal{B}) - \text{Fr}(\text{rng}(c), \mathcal{B})| \\ &\geq |\text{Fr}(A, \mathcal{B}) - \text{Fr}(C, \mathcal{B})| \end{aligned}$$

So it suffices that  $|E(\bar{X}) - \bar{X}| \leq \varepsilon$  has positive probability for some large enough  $n$ . By Chebyshev's inequality

$$1 - \frac{1}{4n\varepsilon^2} < \text{Pr} \left( |E(\bar{X}) - \bar{X}| \leq \varepsilon \right)$$

Hence the probability above is positive for  $\frac{1}{4\varepsilon^2} \leq n$ .  $\square$

**2.4 Theorem (Uniform law of large numbers)** Assume  $(\mathcal{U}, \Phi)$  has VC-density  $d$ . Then every sample  $A$  has an  $\varepsilon$ -approximation of size

$$n \leq c \frac{d}{\varepsilon^2} \ln \frac{1}{\varepsilon},$$

where  $c$  is an absolute constant.

The lemma above tells that  $\varepsilon$ -approximations with small discrepancy are useful, but as yet we have no clue as to finding one. We are going to prove that when the number of definable subsets of  $A$  is relatively small, then the discrepancy of  $A$  is not too large. We use a probabilistic argument to prove this bound (when you don't have a clue how to do something, you might as well do it randomly).

First, we make a brief digression into probability theory. The following inequality is a classical tool in this context.

**2.5 Lemma (Chernoff's bound, special case)** For  $i = 1, \dots, n$  let  $X_i$  be independent identically distributed random variables such that  $\Pr(X_i = \pm 1) = 1/2$ . Then for every  $\varepsilon > 0$

$$\Pr(\bar{X} \geq \varepsilon) \leq \exp(-\frac{n}{2}\varepsilon^2) \quad \text{where } \bar{X} = \frac{1}{n} \sum_{i=1}^n X_i$$

**Proof** Let  $t > 0$  be arbitrary. Then

$$\begin{aligned} \# \quad \Pr(\bar{X} \geq \varepsilon) &= \Pr(e^{t\bar{X}} \geq e^{t\varepsilon}) \\ &\leq e^{-t\varepsilon} \mathbb{E}(e^{t\bar{X}}) \end{aligned}$$

In fact, the equality follows because the exponential is an increasing function and the inequality is Markov's inequality, which says that  $\Pr(X \geq a) \leq a^{-1}\mathbb{E}(X)$  for every  $a$  and is immediate to verify. Now observe that

$$\begin{aligned} \mathbb{E}(e^{tX_i}) &= \frac{1}{2}e^t + \frac{1}{2}e^{-t} \\ &= \frac{1}{2} \sum_{i=0}^{\infty} \frac{t^i}{i!} + \frac{1}{2} \sum_{i=0}^{\infty} \frac{(-t)^i}{i!} \\ &= \sum_{i=0}^{\infty} \frac{t^{2i}}{(2i)!} \\ &\leq \sum_{i=0}^{\infty} \frac{(t^2/2)^i}{i!} \\ &= e^{t^2/2} \end{aligned}$$

From this, by independence we have

$$\mathbb{E}(e^{t\bar{X}}) = \prod_{i=1}^n e^{(t/n)X_i} = e^{t^2/2}$$

Substituting in  $\#$  gives  $\Pr(\bar{X} \geq \varepsilon) \leq e^{t^2/2 - t\varepsilon}$ . Finally Chernoff's inequality is obtained substituting  $\varepsilon$  for  $t$ .  $\square$

**2.6 Lemma** Let  $A$  be a sample of size  $\leq n$ . Assume the support of  $A$  has  $\leq m$  definable subsets. Then  $\delta_A \leq \sqrt{(2/n) \ln(m+1)}$ .

**Proof** To prove that  $\delta_A \leq \varepsilon$  it suffices to show that there is a  $C \subseteq A$  such that  $\delta_{A,C,B} \leq \varepsilon$  for all  $B$ . It suffices to define a probability on the subsamples of  $A$  and

show that

$$\Pr(\forall \mathcal{B} \in \Phi' \quad \delta_{A,C,\mathcal{B}} \leq \varepsilon) > 0$$

or, as  $\Phi'$  has at most  $m + 1$  elements, that for every  $\mathcal{B} \in \Phi'$

$$4. \quad \Pr(\delta_{A,C,\mathcal{B}} \geq \varepsilon) \leq \frac{1}{m+2}.$$

Suppose  $c = \langle c_1, \dots, c_n \rangle \in \{\pm 1\}^n$  is obtained tossing  $n$  times a fair coin. Fix  $\mathcal{B}$  and let  $n' = |\mathcal{B}|$ . Consider the Bernoulli random variables  $X_i$  that on input  $c$  output  $c_i$ . Define also  $\bar{X} = (1/n') \sum_{a_i \in \mathcal{B}} X_i$ . Then  $\delta_{A,C,\mathcal{B}} = \bar{X}(c)$  and 4 is equivalent to

$$\Pr(\bar{X} \geq \varepsilon) \leq \frac{1}{m+2}.$$

By the Chernoff's bound this is satisfied if

$$\exp(-\frac{n'\varepsilon^2}{2}) \leq \frac{1}{m+2}.$$

As  $n' \leq n$ , this yields the required bound.  $\square$

**2.7 Proof of Proposition 2.4** Set  $A_0 = A$  and  $\varepsilon_0 = 0$ . We construct a decreasing chain  $A_i$  of  $\varepsilon_i$ -approximations. We denote by  $n_i$  and  $\delta_i$  the cardinality, respectively the discrepancy, of  $A_i$ . By lemma 2.1, we can require that  $\varepsilon_{i+1} = \varepsilon_i + 2\delta_i$  and  $n_{i+1} \leq n_i/2$ . Then

$$\varepsilon_h = 2 \sum_{i=1}^h \delta_i$$

Let  $h$  be the largest such that  $\varepsilon_h \leq \varepsilon$ . The theorem claims that  $2^{-h}n_0 \leq c(d/\varepsilon^2) \log(1/\varepsilon)$ , independently of  $n_0$ .

$$2 \sum_{i=1}^h \delta_i \leq 2 \sum_{i=1}^h \sqrt{(2/n_i) \ln(n_i^d + 2)}$$

and, as  $n_i = 2^{-i}n_0$ , the sum above is proportional to its largest term,

$$\leq c \sqrt{(d/n_h) \ln(n_h)}$$

Hence a sufficient condition for  $\varepsilon_h < \varepsilon$  is

$$c \sqrt{(d/n_h) \ln(n_h)} \leq \varepsilon$$

which is equivalent to

$$\frac{c^2 d}{\varepsilon^2} \leq \frac{n_h}{\ln n_h}$$

this in turn is ensured if

$$n_h \leq 2 \frac{c^2 d}{\varepsilon^2} \ln \frac{c^2 d}{\varepsilon^2}$$

**2.8 Corollary** Let  $\Phi$  be a finite set-system of VC-dimension  $1 < k < \omega$ . Then for every positive  $\varepsilon < 1$ , every probability measure  $\Pr$  admits a multi-set  $\varepsilon$ -approximation of cardinality bounded by  $\mathfrak{h}$  of Theorem 2.4.

**Proof** Without loss of generality we can assume that  $\Pr$  is rational valued. Then there is a uniform probability measure  $\Pr'$  on some finite set  $\mathcal{U}'$  and a surjection  $f : \mathcal{U}' \rightarrow \mathcal{U}$  such that  $\Pr(f^{-1}\varphi) = \Pr(\varphi)$ . By Theorem 2.4  $\Pr'$  admits an  $\varepsilon$ -approximation

$B'$  with cardinality by  $\mathfrak{h}$ , for every positive  $\varepsilon < 1$ . We now define a multi-set  $B$  such that  $B(a) = |B' \cap f^{-1}a|$  for every  $a \in \mathcal{U}$ . As  $|B'| = |B|$  and  $|B' \cap f^{-1}\varphi| = |B \cap \varphi|$ , this is the required multi-set  $\varepsilon$ -approximation.  $\square$

The following corollary is used in Theorem 3.1 below. Though it is sufficient for our application, stronger bounds are known (essentially, we can replace  $\varepsilon$  for  $\varepsilon^2$ ).

**2.9 Corollary** *Let  $\Phi$  be a finite set-system of VC-dimension  $1 < k < \omega$ . Then for every positive  $\varepsilon < 1$ , every probability measure  $\Pr$  admits a multi-set  $\varepsilon$ -net of cardinality bounded by  $\mathfrak{h}$  of Theorem 2.4.*

**2.10 Exercise** Suppose that  $\{a\}, \{b\} \in \Phi$  for some  $a, b \in \mathcal{U}$ . Show that, if  $\Pr$  and  $\varepsilon$  are such that  $0 < \varepsilon < \Pr(a)$  and  $2\varepsilon < \Pr(b) - \Pr(a)$ , then  $\Pr$  admits no  $\varepsilon$ -approximation.  $\square$

## Chapter 3

### A piercing problem

After Pierre Simon, after Jiri Matousek, after Noga Alon and Daniel Kleitman.

Let  $q \leq p < \omega$  we say that  $\Phi$  has the  $(p, q)$ -property if out of every  $p$  sets in  $\Phi$  some  $q$  have non empty intersection. It has the dual  $(p, q)$ -property if for every  $p$  point in  $\mathcal{U}$  some  $q$  are belong to the same set in  $\Phi$ .

The following is a particular case of a theorem of Matousek (based on a proof of Noga Alon and Daniel Kleitman). The proof by Pierre Simon is simpler. [I will add details, references, and much more.]

**3.1 Theorem** *Let  $\mathcal{U}$  be finite and let  $\Phi$  have VC-dimension  $k < \omega$ . There are some integers  $q$  and  $h$  that depends only on  $k$  such that, if every  $B \subseteq \mathcal{U}$  of cardinality  $q$  is a subset of some  $\varphi \in \Phi$ , then  $\mathcal{U}$  is covered by some  $X \subseteq \Phi$  of cardinality  $h$ .*

This theorem is often stated in the dual form which explains why it is sometimes called a piercing (or Helly-type) theorem: there are some integers  $q$  and  $h$  that depends only on  $k$  such that, if every  $q$  sets in  $\Phi$  have non-empty intersection, then there is a  $B \subseteq \mathcal{U}$  of cardinality  $h$  that intersects every  $\varphi \in \Phi$ . See Exercise 3.3.

Recall that the dual system is  $\mathcal{U}^* = \Phi$  and  $\Phi^* = \{\Phi_i : i < m\}$ , where  $\Phi_i = \{\varphi \in \Phi : a_i \in \varphi\}$ . By Proposition ?? the dual system has VC-dimension  $2^k$ . Choose some  $\varepsilon = 1/2$ . From Theorem 2.4 we obtain an  $h$  such that every probability measure  $\mu^*$  on  $\Phi$  has an  $\varepsilon$ -approximation of cardinality  $h$ . As  $\varepsilon$  is fixed, this  $h$  only depends on  $k$ . Then there is a multi-set  $X : \Phi \rightarrow \omega$  of cardinality  $h$  such that Moreover  $|Y| \leq h$  as required. Suppose we can find some  $x_j \in \mathbb{R}$  such that for every  $i < m$  In fact, We can also rescale solutions so, setting  $\mu^*(\varphi_j) \stackrel{\text{def}}{=} x_j$ , we obtain a well-defined probability measure It suffices to show that clause 2 of Farkas' Lemma cannot obtain, that is, for every  $\lambda_i \in \mathbb{R}_+$  there are some  $x_j \in \mathbb{R}_+$  such that Note that for every  $j$  we have By assumption, there is a  $j$  such that  $\{a : B(a) \neq 0\} \subseteq \varphi_j$  hence  $|B \cap \varphi_j| = q$ . Therefore  $\mu(\varphi_j) > 1 - \varepsilon$ . Let  $\check{x}_j$  be 1 for  $j = \check{j}$  and 0 otherwise. We claim that the tuple  $\langle x_j : j < n \rangle$  is a solution of  $\mathbb{b}\mathbb{b}$ . In fact

**Proof** Let  $\langle a_i : i < m \rangle$  and  $\langle \varphi_j : j < n \rangle$  enumerate  $\mathcal{U}$  and  $\Phi$  without repetitions. Recall that the dual system is  $\mathcal{U}^* = \Phi$  and  $\Phi^* = \{\Phi_i : i < m\}$ , where  $\Phi_i = \{\varphi \in \Phi : a_i \in \varphi\}$ . By Proposition ?? the dual system has VC-dimension  $2^k$ . Choose some  $\varepsilon = 1/2$ . From Corollary 2.9 we obtain an  $h$  such that every probability measure  $\mu^*$  on  $\Phi$  admits an  $\varepsilon$ -net of cardinality  $h$ . As  $\varepsilon$  is fixed, this  $h$  only depends on  $k$ . Restating this explicitly there is a set  $X \subseteq \mathcal{U}^*$  of cardinality  $h$  such that

$$\# \quad |\mu^*(\Phi_i)| > \varepsilon \Rightarrow X \cap \Phi_i \neq \emptyset$$

So, if the probability measure on  $\Phi$  is such that  $\mu^*(\Phi_i) > \varepsilon$  for all  $i < m$ , then  $X \subseteq \Phi$  cover  $\mathcal{U}$  as required by the theorem. So we only need to find such a probability measure.

For  $i < m$  and  $j < n$  let  $P_{i,j} = 1$  if  $a_i \in \varphi_j$  and 0 otherwise. Suppose we can find some  $x_j \in \mathbb{R}$  such that for every  $i < m$

$$\flat \quad \sum_{j < n} (P_{i,j} - \varepsilon) x_j > 0$$

Then we can assume that all  $x_j$  are positive. In fact,

$$\sum_{j < n} P_{i,j} \geq 1$$

(because every  $a_i$  belongs to some  $\varphi_j$ ) so we can translate solutions of any positive quantity. We can also rescale solutions so, setting  $\mu^*(\varphi_j) \stackrel{\text{def}}{=} x_j$ , we obtain a well-defined probability measure

$$\mu^*(\Phi_i) = \sum_{j < n} P_{i,j} x_j > \varepsilon$$

We only have to prove that equation  $\flat$  has a solution. It suffices to show that clause 2 of Farkas' Lemma cannot obtain, that is, for every  $\lambda_i \in \mathbb{R}_+$  there are some  $x_j \in \mathbb{R}_+$  such that

$$\flat\flat \quad \sum_{i < m} \lambda_i \sum_{j < n} (P_{i,j} - \varepsilon) x_j > 0.$$

As we can assume the  $\lambda_i$  add to 1, setting  $\mu(a_i) \stackrel{\text{def}}{=} \lambda_i$ , we obtain a probability measure on  $\mathcal{U}$ . Note that for every  $j$  we have

$$\mu(\varphi_j) = \sum_{i < m} \lambda_i P_{i,j}.$$

Apply Corollary 2.9 once again to the set-system  $\langle \mathcal{U}, \neg\Phi \rangle$ . There is a  $q$  such that for every probability measure  $\mu$  on  $\mathcal{U}$  there is a set  $B \subseteq \mathcal{U}$  of cardinality  $q$  such that

$$\sharp\sharp \quad \mu(\neg\varphi_j) > \varepsilon \Rightarrow B \not\subseteq \varphi_j$$

As  $\varepsilon$  is fixed,  $q$  only depends on  $k$ . By assumption, there is a  $\check{j}$  such that  $B \subseteq \varphi_{\check{j}}$  and therefore  $\mu(\varphi_{\check{j}}) \geq 1 - \varepsilon$ . Let  $\check{x}_j$  be 1 for  $j = \check{j}$  and 0 otherwise. We claim that the tuple  $\langle x_j : j < n \rangle$  is a solution of  $\flat\flat$ . In fact

$$\sum_{i < m} \lambda_i \sum_{j < n} (P_{i,j} - \varepsilon) \check{x}_j = \sum_{i < m} \lambda_i (P_{i,\check{j}} - \varepsilon) = \mu(\varphi_{\check{j}}) - \varepsilon \geq 1 - \varepsilon > 0.$$

This concludes the proof.  $\square$

The following is a classical result. The proof may be found in any introductory text of convex analysis or linear programming. There are many (sometimes non equivalent) ways to state it, we recommend Terence Tao's exposition which may be found in his mathematical blog (we have reversed strict and weak inequalities, but the proof is identical).

**3.2 Proposition (Farkas' Lemma)** For  $i < m$  let  $P_i : \mathbb{R}^n \rightarrow \mathbb{R}$  be affine linear functions. Then the following are equivalent

1.  $\bigwedge_{i < m} P_i(x) > 0$  for some  $x \in \mathbb{R}^n$ ;
2. there are no  $\lambda_i \in \mathbb{R}_+$  such that  $\sum_{i < m} \lambda_i P_i(x) \leq 0$  for every  $x \in \mathbb{R}^n$ .  $\square$

It will help induction Up to rescaling we can assume that  $P_{i,j}(x, y)$  have the form

**3.3 Exercise** Let  $k, q$  and  $h$  be some integers as in Theorem 3.1 and let  $\Phi$  be a set-system with dual VC-dimension  $k$ . Suppose that any  $q$  sets in  $\Phi$  have non-empty intersection and prove that there is some set  $B \subseteq \mathcal{U}$  of cardinality  $h$  that intersects every  $\varphi \in \Phi$ .  $\square$

# 1 Appendix: Farkas' lemma

Below, an affine version of Farkas' Lemma tailored to our purposes.

**3.4 Proposition** Fix some  $v_1, \dots, v_n, u \in \mathbb{Q}^k$  and let  $r_1, \dots, r_n, s \in \mathbb{Q}$ . Let

$$X(r_1, \dots, r_n) = \{x \in \mathbb{Q}^k : r_i \leq v_i \cdot x, \text{ for every } i = 1, \dots, n\}.$$

Then the following are equivalent

1.  $s \leq u \cdot x$  for all  $x \in X(r_1, \dots, r_n)$ ;
2. there exist  $q_1, \dots, q_n \in \mathbb{Q}^+$  such that  $\sum_{i=1}^n q_i v_i = u$ .

**Proof** Implication  $2 \Rightarrow 1$  is immediate. To prove  $1 \Rightarrow 2$  assume 1. We claim that

3.  $0 \leq u \cdot x$  for all  $x \in X(0, \dots, 0)$ .

Suppose not and let  $x \in X(0, \dots, 0)$  be such that  $u \cdot x < 0$ . Let  $y \in X(r_1, \dots, r_n)$ . Then  $y + ax \in X(r_1, \dots, r_n)$  for every  $a \in \mathbb{Q}^+$ . From 1 we obtain  $s \leq u \cdot (y + ax)$  which, for  $a$  is sufficiently large, is a contradiction.

From 3 it follows that if  $x \cdot v_i = 0$  for  $i = 1, \dots, n$  then  $0 = u \cdot x$ . We can assume without loss of generality that  $v_1, \dots, v_n$  are linearly independent. Then by linear algebra  $\sum q_i v_i = u$  for some  $q_i \in \mathbb{Q}$ . Now fix  $i$  and verify that  $q_i$  is non-negative. Let  $x_i$  such that  $x_i \cdot v_j = 1$ , if  $i = j$ , and 0 otherwise. Then  $0 \leq x_i \cdot u = q_i$ .  $\square$