

## Math 5251 Kraft & McMillan inequalities (§3.2)

Can we **arbitrarily** specify the word lengths

$l_1, \dots, l_m$  for a code  $\mathcal{C} = \{w_1, \dots, w_m\}$

on alphabet  $\Sigma$  of size  $n$ ?

called an  **$n$ -ary** alphabet/code

e.g.  $\Sigma = \{0,1\}$  binary = 2-ary

$\Sigma = \{0,1,2\}$  ternary = 3-ary

---

**EXAMPLE**  $\mathcal{C} = \{0, 1, 20, 21, 22\}$  on  $\Sigma = \{0,1,2\}$

has  $(l_1, l_2, l_3, l_4, l_5)$

$= (1, 1, 2, 2, 2)$

$m=5$

$n=3$

---

Certainly **not arbitrarily**, e.g. if  $\Sigma = \{0,1\}$

then  $(l_1, l_2, l_3, l_4, l_5) = (2, 2, 2, 2, 2)$

is **impossible** since  $\Sigma^*$  has only

4 words of length 2:

00  
01  
10  
11

If we further insist on the code being **uniquely decipherable**, it imposes even more of a constraint on  $(l_1, \dots, l_m)$ ; interestingly it's the same constraint for codes that are prefix.

---

**THEOREM** Let  $\Sigma$  be an alphabet with  $n$  letters, and  $(l_1, l_2, \dots, l_m)$  positive integers.

(a) **(Kraft)** If  $\sum_{i=1}^m \frac{1}{n^{l_i}} = \frac{1}{n^{l_1}} + \frac{1}{n^{l_2}} + \dots + \frac{1}{n^{l_m}} \leq 1$

then  $\exists$  a **prefix code**  $\mathcal{C}$  on  $\Sigma$  with those lengths.  
(instantaneous)

(b) **(McMillan)** If  $\exists$  a **uniquely decipherable** code  $\mathcal{C}$  on  $\Sigma$  with those lengths,

$$\text{then } \sum_{i=1}^m \frac{1}{n^{l_i}} \leq 1$$


---

**SAME inequality for both!** So one concludes

$$\begin{aligned} \{ \text{lengths of u.d. } n\text{-ary codes} \} & \quad \equiv \quad \{ \text{lengths of prefix } n\text{-ary codes} \} \\ & \quad \equiv \quad \{ (l_1, \dots, l_m) \text{ with } \sum_i \frac{1}{n^{l_i}} \leq 1 \} \end{aligned}$$

Kraft-McMillan inequality  $\Rightarrow$

EXAMPLES If  $n=3 = |\Sigma|$ , say  $\Sigma = \{0,1,2\}$   
 then  $\nexists$  any u.d. code  $\mathcal{C}$  with  
 word lengths  $(1,1,2,2,2,3)$  because

$$\frac{1}{3^1} + \frac{1}{3^1} + \frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{3^3} = \frac{9+9+3+3+3+1}{27} = \frac{28}{27} > 1$$

On the other hand, there  $\exists$  a  
 prefix code  $\mathcal{C}$  with lengths  $(1,2,2,2,3,3)$  because

$$\frac{1}{3^1} + \frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{3^3} + \frac{1}{3^3} = \frac{9+3+3+3+3+1+1}{27} = \frac{23}{27} \leq 1$$

In fact, let's prove Kraft first, via an algorithm  
 to find  $\mathcal{C}$ . Assuming  $(l_1, \dots, l_m)$  has  $t_i$   
 occurrences of length  $i$ , then the inequality assumes

$$\sum_{i=1}^m \frac{1}{n^{l_i}} = \frac{t_1}{n^1} + \frac{t_2}{n^2} + \frac{t_3}{n^3} + \dots \leq 1$$

and we try to pick the shorter words first.

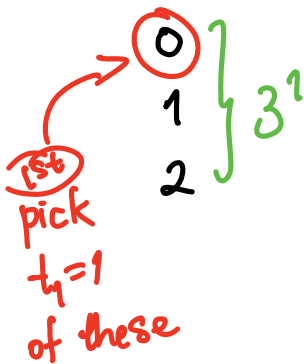
EXAMPLE  $(l_1, \dots, l_m) = (1, \underbrace{2, 2, 2, 2}_{t_2=4}, \underbrace{3, 3}_{t_3=2})$

has  $\frac{t_1}{3^1} + \frac{t_2}{3^2} + \frac{t_3}{3^3} = \frac{1}{3^1} + \frac{4}{3^2} + \frac{2}{3^3} \leq 1$

$\Rightarrow \frac{t_1}{3^1} \leq 1$

so  $t_1 \leq 3^1$

allowing us to pick  $t_1$  words of length 1:



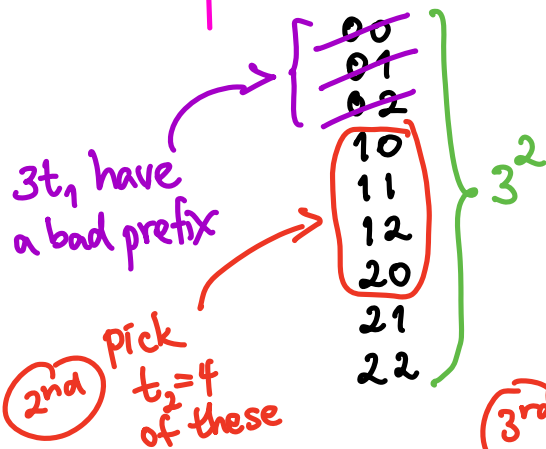
$\Rightarrow \frac{t_1}{3^1} + \frac{t_2}{3^2} \leq 1$

so  $3t_1 + t_2 \leq 3^2$

$t_2 \leq 3^2 - 3t_1$

this many length 2 words have a prefix from our length 1 choices

allowing us to pick  $t_2$  words of length 2:



$\Rightarrow \frac{t_1}{3^1} + \frac{t_2}{3^2} + \frac{t_3}{3^3} \leq 1$

so  $3^2 t_1 + 3 t_2 + t_3 \leq 3^3$

$t_3 \leq 3^3 - (3^2 t_1 + 3 t_2)$

this many length 3 words have a bad prefix

allowing us to pick  $t_3$  words of length 3



proof of Kraft's inequality:

If  $(l_1, \dots, l_m)$  has  $t_i$  occurrences of  $i$  and

$$\frac{t_1}{n^1} + \frac{t_2}{n^2} + \frac{t_3}{n^3} + \dots = \sum_{i=1}^m \frac{1}{n^{l_i}} \leq 1$$

we show how to pick a prefix code  $\mathcal{C}$  with those lengths. Assuming one has already picked the words of length  $\leq i-1$ , and show they leave  $\geq t_i$  words of length  $i$  that avoid them as prefixes.

Previously one has picked

$t_{i-1}$  of length  $i-1 \rightsquigarrow$  create  $n t_{i-1}$  with bad prefix

$t_{i-2}$  of length  $i-2 \rightsquigarrow$  create  $n^2 t_{i-2}$  with bad prefix

$\vdots$

$t_2$  of length 2  $\rightsquigarrow$  create  $n^{i-2} t_2$  with bad prefix

$t_1$  of length 1  $\rightsquigarrow$  create  $n^{i-1} t_1$  with bad prefix

Since there are  $n^i$  words of length  $i$

in total using alphabet  $\Sigma$ , ...

this leaves

$$n^i - (n^{i-1}t_1 + n^{i-2}t_2 + \dots + n^2t_{i-2} + nt_{i-1})$$

words of length  $i$  from which to choose  $t_i$  for  $\mathcal{C}$ .

We claim the above quantity is **at least**  $t_i$ ,

$$\text{since } \frac{t_1}{n^1} + \frac{t_2}{n^2} + \dots + \frac{t_{i-2}}{n^{i-2}} + \frac{t_{i-1}}{n^{i-1}} + \frac{t_i}{n^i} \leq 1$$

$\} \text{ multiply by } n^i$

$$n^{i-1}t_1 + n^{i-2}t_2 + \dots + n^2t_{i-2} + nt_{i-1} + t_i \leq n^i$$

$$\text{i.e. } t_i \leq n^i - (n^{i-1}t_1 + n^{i-2}t_2 + \dots + n^2t_{i-2} + nt_{i-1})$$



proof of McMillan inequality:

Assume  $\mathcal{C}$  is a uniquely decipherable  $n$ -ary code having  $t_i$  codewords of length  $i$  for  $i=1,2,\dots,l$ .

We want to show  $\frac{t_1}{n^1} + \frac{t_2}{n^2} + \dots + \frac{t_l}{n^l} \leq 1$

call this sum  $A$ ; want  $A \leq 1$ .

IDEA: Instead, for each  $p=1,2,3,\dots$  we will show

$$A^p = \sum_{s=1}^{pl} \frac{c_s}{n^s} \text{ for some coefficients } c_s \leq n^s$$

$$\Rightarrow A^p \leq \sum_{s=1}^{pl} 1 = pl$$

$$\Rightarrow A \leq (pl)^{\frac{1}{p}}$$

$$\Rightarrow A \leq \lim_{p \rightarrow \infty} (pl)^{\frac{1}{p}} = 1, \text{ as desired}$$

take  $p^{\text{th}}$  root of both sides

$$\lim_{p \rightarrow \infty} (pl)^{\frac{1}{p}} = \lim_{p \rightarrow \infty} e^{\frac{\ln(pl)}{p}} = e^{\lim_{p \rightarrow \infty} \frac{\ln(p) + \ln(l)}{p}}$$

$$\stackrel{\text{L'H\^opital}}{=} e^{\lim_{p \rightarrow \infty} \frac{\frac{1}{p} + 0}{1}} = e^0 = 1$$

Calculus  
interlude!

So for  $\mathcal{C}$  u.d., we need to show

$$A := \frac{t_1}{n^1} + \frac{t_2}{n^2} + \dots + \frac{t_l}{n^l} \text{ has } A^p = \sum_{s=1}^{pl} \frac{c_s}{n^s} \text{ with } c_s \leq n^s$$

In fact, we can interpret  $c_s$  as counting the number of messages  $(w_1, w_2, \dots, w_p)$  of  $p$  words from  $\mathcal{C}$  with a total length of  $s$  letters from  $\Sigma$ .

Since there are  $n^s$  strings in  $\Sigma^*$  with  $s$  letters, and  $\mathcal{C}$  is uniquely decipherable, this shows  $c_s \leq n^s$ ; each string comes from at most one message.  $\blacksquare$

(proof by)  
**EXAMPLE**  $\mathcal{C} = \{0, 1, 20, 21, 22\}$ ,  $\Sigma = \{0, 1, 2\}$   
 $n=3$   
 $t_1=2$   $t_2=3$

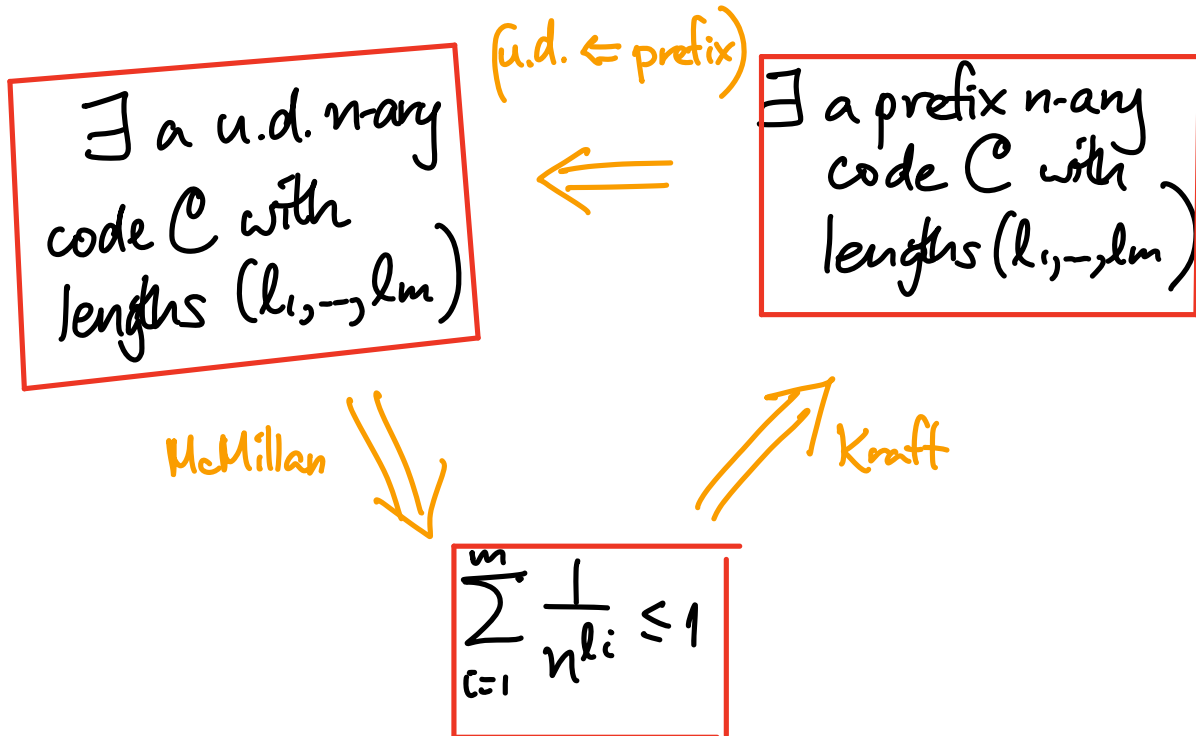
$$\left(\frac{t_1}{3^1} + \frac{t_2}{3^2}\right)^2 = \frac{t_1 \cdot t_1}{3^2} + \frac{(t_1 t_2 + t_2 t_1)}{3^3} + \frac{t_2 \cdot t_2}{3^4}$$

$$= \frac{2 \cdot 2}{3^2} + \frac{2 \cdot 3 + 3 \cdot 2}{3^3} + \frac{3 \cdot 3}{3^4}$$

00	020	200	2020
01	021	201	2021
10	022	210	2022
11	120	211	2120
	121	220	2121
	122	221	2122
			2220
			2221
			2222



RECAP: We showed



so all 3 statements are equivalent.