## LLOYD'S THEOREM

## Notes for our seminar — Lex Schrijver

Fix n, e, and  $q \in \mathbb{N}$ , and set  $Q = \{0, \ldots, q-1\}$ . For  $c, d \in Q^n$ , let dist(c, d) be the Hamming distance of c and d, that is, the number of  $i \in [n]$  with  $c_i \neq d_i$ . An *e-perfect code* is a subset  $C \subseteq Q^n$  such that the balls  $\{d \mid \text{dist}(c, d) \leq e\}$  for  $c \in C$  partition  $Q^n$ .

The following was proved by Lloyd [4] for prime powers q, and by Bassalygo [1], Delsarte [2], and Lenstra [3] for general q.

**Theorem** (Lloyd's theorem). If an e-perfect code exists, then the ('Lloyd') polynomial

(1) 
$$L_e(x) := \sum_{l=0}^{e} (-1)^l (q-1)^{e-l} {\binom{x-1}{l}} {\binom{n-x}{e-l}}$$

has e distinct zeroes among  $1, \ldots, n$ .

**Proof.** It will be convenient to assume that Q is equal to the ring  $\mathbb{Z}/q\mathbb{Z}$ .

For any  $c \in Q^n$ , let |c| be the *weight* of c, that is, the number of nonzero entries in c. So |c| = dist(0, c). For any  $C \subseteq Q^n$ , let  $w_C$  be the *weight enumerator* of C, that is, the function  $w_C : \{0, \ldots, n\} \to \mathbb{Z}$  with  $w_C(i)$  equals to the number of  $c \in C$  with |c| = i (for  $i = 0, \ldots, n\}$ ). First, we have:

(2) if an *e*-perfect code exists, then  $\{w_C \mid C \text{ e-perfect code}\}$  spans a subspace of  $\mathbb{R}^{\{0,\dots,n\}}$  of dimension at least e + 1.

Indeed, let C be an e-perfect code. For each  $i = 0, \ldots, e$ , choose a word a with |a| = i, and set  $C_i := \{a + c \mid c \in C\}$ . Then  $C_i$  is an e-perfect code, with  $w_{C_i}(j) = \delta_{i,j}$  for  $j = 0, \ldots, e$ (as a is the unique word in  $C_i$  at distance  $\leq e$  from 0). So  $\{w_{C_i} \mid i = 0, \ldots, e\}$  is linearly independent, and we have (2).

For each k = 0, ..., n, define the  $\{0, ..., n\} \times \{0, ..., n\}$  matrix  $M_k$  by

(3) 
$$(M_k)_{i,j} :=$$
 number of  $a \in Q^n$  with  $|a| = i$  and dist $(a, b) = k$ ,

for i, j = 0, ..., n, where b is an arbitrary word with |b| = j. The value (3) is independent of the choice of b, since for any other word b' with |b'| = j there is an isometry on  $Q^n$  that fixes 0 and brings b to b'. Define

(4) 
$$M_{\leq e} := \sum_{k=0}^{e} M_k.$$

Then

(5) for any *e*-perfect code C,  $M_{\leq e}w_C = w_{Q^n}$ .

Indeed, for any  $k \leq e$  and i,  $(M_k w_C)_i = \sum_{c \in C} (M_k)_{i,|c|}$ , which is the number of words of weight i at distance k from C. So  $(M_{\leq e} w_C)_i$  is equal to the number of words of weight i at distance  $\leq e$  from C. Since C is an e-perfect code, this is equal to the total number of words of weight i, which is  $(w_{Q^n})_i$ .

Now (2) and (5) imply:

(6) if an *e*-perfect code exists, then  $\operatorname{corank}(M_{\leq e}) \geq e$ .

Hence it suffices to prove that

(7) 
$$\operatorname{corank}(M_{\leq e})$$
 is equal to the number  $s \in \{1, \ldots, n\}$  with  $L_e(s) = 0$ 

To this end, let for  $s, i = 0, \ldots, n$ :

(8) 
$$K_{k,s} := \sum_{l=0}^{k} (-1)^{l} (q-1)^{k-l} {s \choose l} {n-s \choose k-l}$$

(the k-th Krawtchouk polynomial).

Let  $\alpha$  be a primitive q-th root of unity. Then for any word d with |d| = s:

(9) 
$$K_{k,s} = \sum_{c,|c|=k} \alpha^{c \cdot d},$$

where  $c \cdot d := \sum_{i} c_{i} d_{i}$ . Indeed, let S be the support of d. We can split the summands in (9) by the support I of c:

(10) 
$$\sum_{\substack{c,|c|=k}} \alpha^{c \cdot d} = \sum_{\substack{I \subseteq [n] \\ |I|=k}} \prod_{i \in I \cap S} \sum_{c_i=1}^{q-1} \alpha^{c_i \cdot d_i} \cdot \prod_{i \in I \setminus S} \sum_{c_i=1}^{q-1} \alpha^{c_i \cdot 0} \cdot \prod_{i \in [n] \setminus I} \alpha^{0 \cdot d_i} = \sum_{\substack{I \subseteq [n] \\ |I|=k}} \prod_{i \in I \cap S} (-1) \cdot \prod_{i \in I \setminus S} (q-1) \cdot \prod_{i \in [n] \setminus I} 1 = \sum_{l=0}^{k} {s \choose l} (-1)^l {n-s \choose k-l} (q-1)^{k-l} = K_{k,s}.$$

This gives, for all  $s, t = 0, \ldots, n$ :

(11) 
$$(KM_kK)_{s,t} = \delta_{s,t}q^n K_{k,t}.$$

Indeed, choose d with |d| = t arbitrarily. Then

(12) 
$$(KM_{k}K)_{s,t} = \sum_{i,j} K_{s,i}(M_{k})_{i,j}K_{j,t} = \sum_{i,j} \sum_{c,|c|=j} \sum_{\substack{b,|b|=i\\ \operatorname{dist}(b,c)=k}} \sum_{a,|a|=s} \alpha^{a\cdot b} \alpha^{-c\cdot d} = \sum_{\substack{a,u\\|a|=s,|u|=k}} \sum_{c} \alpha^{a\cdot (c+u)} \alpha^{-d\cdot c} = \sum_{\substack{a,|a|=s\\|a|=s,|u|=k}} \sum_{c} \alpha^{a\cdot (c+u)} \alpha^{-d\cdot c} = \sum_{\substack{a,|a|=s\\|a|=s,|u|=k}} \alpha^{a\cdot u} \sum_{c} \alpha^{(a-d)\cdot c} = \sum_{\substack{a,u\\|a|=s,|u|=k}} \alpha^{a\cdot u} \delta_{a,d} q^{n} = \delta_{s,t} q^{n} \sum_{\substack{u\\|u|=k}} \alpha^{d\cdot u} = \delta_{s,t} q^{n} K_{k,t}.$$

So  $X \mapsto KXK$  simultaneously diagonalizes all  $M_k$ , with  $q^n$  times the k-th row of K as diagonal of  $KM_kK$ . Hence it diagonalizes  $M_{\leq e}$  and implies

(13)  $\operatorname{corank}(M_{\leq e})$  is equal to the number of s with  $\sum_{k=0}^{e} K_{k,s} = 0$ .

Now

(14) 
$$\sum_{k=0}^{e} K_{k,s} = L_e(s).$$

This follows by induction on e from

(15) 
$$L_{e-1}(s) + K_{e,s} = L_e(s).$$

The latter follows from  $\binom{s}{l} - \binom{s-1}{l} = \binom{s-1}{l-1}$ :

(16) 
$$K_{e,s} - L_{e}(s) = \sum_{l=0}^{e} (-1)^{l} (q-1)^{e-l} {s \choose l} {n-s \choose e-l} - \sum_{l=0}^{e} (-1)^{l} (q-1)^{e-l} {s-1 \choose l} {n-s \choose e-l} = \sum_{l=1}^{e} (-1)^{l} (q-1)^{e-l} {s-1 \choose l-1} {n-s \choose e-l} = -\sum_{l=0}^{e-1} (-1)^{l} (q-1)^{e-l-l} {s-1 \choose l} {n-s \choose e-l-l} = -L_{e-1}(s).$$

This proves the theorem (note that  $L_e(0) > 0$ ).

## References

- L.A. Bassalygo, Generalization of Lloyd's theorem to arbitrary alphabet [in Russian], Problemy Upravlenija i Teorii Informacii 2:2 (1973) 133–137 [English translation: Problems of Control and Information Theory 2:2 (1973) 25–28].
- [2] P. Delsarte, An Algebraic Approach to the Association Schemes of Coding Theory, Philips Research Reports Supplements 1973 No. 10, Philips Research Laboratories, Eindhoven, 1973.
- [3] H.W. Lenstra, Jr, Two theorems on perfect codes, *Discrete Mathematics* 3 (1972) 125–132.
- [4] S.P. Lloyd, Block coding, The Bell System Technical Journal 36 (1957) 517-535.