## 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 $\operatorname{dist}(c, d)$ 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 $\{d \mid \operatorname{dist}(c, d) \leq e\}$ 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

$$
\begin{equation*}
L_{e}(x):=\sum_{l=0}^{e}(-1)^{l}(q-1)^{e-l}\binom{x-1}{l}\binom{n-x}{e-l} \tag{1}
\end{equation*}
$$

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 $|c|=\operatorname{dist}(0, c)$. For any $C \subseteq Q^{n}$, let $w_{C}$ be the weight enumerator of $C$, that is, the function $w_{C}:\{0, \ldots, n\} \rightarrow \mathbb{Z}$ with $w_{C}(i)$ equals to the number of $c \in C$ with $|c|=i$ (for $i=0, \ldots, n\})$. First, we have:
if an e-perfect code exists, then $\left\{w_{C} \mid C e\right.$-perfect code $\}$ spans a subspace of $\mathbb{R}^{\{0, \ldots, n\}}$ 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 $\left\{w_{C_{i}} \mid i=0, \ldots, e\right\}$ is linearly independent, and we have (22).

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

$$
\begin{equation*}
\left(M_{k}\right)_{i, j}:=\text { number of } a \in Q^{n} \text { with }|a|=i \text { and } \operatorname{dist}(a, b)=k, \tag{3}
\end{equation*}
$$

for $i, j=0, \ldots, n$, where $b$ is an arbirary word with $|b|=j$. The value (3) is independent of the choice of $b$, since for any other word $b^{\prime}$ with $\left|b^{\prime}\right|=j$ there is an isometry on $Q^{n}$ that fixes 0 and brings $b$ to $b^{\prime}$. Define

$$
\begin{equation*}
M_{\leq e}:=\sum_{k=0}^{e} M_{k} . \tag{4}
\end{equation*}
$$

Then

$$
\begin{equation*}
\text { for any } e \text {-perfect code } C, M_{\leq e} w_{C}=w_{Q^{n}} . \tag{5}
\end{equation*}
$$

Indeed, for any $k \leq e$ and $i,\left(M_{k} w_{C}\right)_{i}=\sum_{c \in C}\left(M_{k}\right)_{i,|c|}$, which is the number of words of weight $i$ at distance $k$ from $C$. So $\left(M_{\leq e} w_{C}\right)_{i}$ 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 $\left(w_{Q^{n}}\right)_{i}$.

Now (2) and (5) imply: if an $e$-perfect code exists, then $\operatorname{corank}\left(M_{\leq e}\right) \geq e$.

Hence it suffices to prove that

$$
\begin{equation*}
\operatorname{corank}\left(M_{\leq e}\right) \text { is equal to the number } s \in\{1, \ldots, n\} \text { with } L_{e}(s)=0 . \tag{7}
\end{equation*}
$$

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

$$
\begin{equation*}
K_{k, s}:=\sum_{l=0}^{k}(-1)^{l}(q-1)^{k-l}\binom{s}{l}\binom{n-s}{k-l} \tag{8}
\end{equation*}
$$

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

$$
\begin{equation*}
K_{k, s}=\sum_{c,|c|=k} \alpha^{c \cdot d} \tag{9}
\end{equation*}
$$

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 $c$ :

$$
\begin{align*}
& \sum_{c,|c|=k} \alpha^{c \cdot d}=\sum_{\substack{I \subseteq[n] \\
|I|=k}} \prod_{i \in I \cap S} \sum_{c_{i}=1}^{q-1} \alpha^{c_{i} \cdot d_{i}} \cdot \prod_{i \in I \backslash S} \sum_{c_{i}=1}^{q-1} \alpha^{c_{i} \cdot 0} \cdot \prod_{i \in[n] \backslash I} \alpha^{0 \cdot d_{i}}=  \tag{10}\\
& \sum_{\substack{I \subseteq[n] \\
|\bar{I}|=k}} \prod_{i \in I \cap S}(-1) \cdot \prod_{i \in I \backslash S}(q-1) \cdot \prod_{i \in[n \backslash \backslash I} 1=\sum_{l=0}^{k}\left(\begin{array}{l}
s \\
l \\
l
\end{array}\right)(-1)^{l}\binom{n-s}{k-l}(q-1)^{k-l}=K_{k, s} .
\end{align*}
$$

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

$$
\begin{equation*}
\left(K M_{k} K\right)_{s, t}=\delta_{s, t} q^{n} K_{k, t} . \tag{11}
\end{equation*}
$$

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

$$
\begin{align*}
& \left(K M_{k} K\right)_{s, t}=\sum_{i, j} K_{s, i}\left(M_{k}\right)_{i, j} K_{j, t}=\sum_{i, j} \sum_{\substack{,|c|=j}} \sum_{\substack{b,|b|=i \\
\text { dist }(b, c)=k}} \sum_{\substack{a,|a|=s}} \alpha^{a \cdot b} \alpha^{-c \cdot d}=  \tag{12}\\
& \sum_{\substack{a \\
|a|=s}} \sum_{\substack{b, c \\
\text { dist }(t, c, c)=k}} \alpha^{a \cdot b} \alpha^{-d \cdot c}=\sum_{\substack{a, u}} \sum_{c} \alpha^{a \cdot(c+u)} \alpha^{-d \cdot c}= \\
& \sum_{\substack{a, u \\
|a|=s,|u|=k}}^{a \cdot c|=s,|u|=k} c \\
& \alpha^{a \cdot u} \\
& \sum_{c} \alpha^{(a-d) \cdot c}=\sum_{\substack{a, u \\
|a|=s,|u|=k}} \alpha^{a \cdot u} \delta_{a, d} q^{n}=\delta_{s, t} q^{n} \sum_{\substack{u \\
|u|=k}} \alpha^{d \cdot u}=\delta_{s, t} q^{n} K_{k, t} .
\end{align*}
$$

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

$$
\begin{equation*}
\operatorname{corank}\left(M_{\leq e}\right) \text { is equal to the number of } s \text { with } \sum_{k=0}^{e} K_{k, s}=0 \tag{13}
\end{equation*}
$$

Now

$$
\begin{equation*}
\sum_{k=0}^{e} K_{k, s}=L_{e}(s) . \tag{14}
\end{equation*}
$$

This follows by induction on $e$ from

$$
\begin{equation*}
L_{e-1}(s)+K_{e, s}=L_{e}(s) \tag{15}
\end{equation*}
$$

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

$$
\begin{align*}
& K_{e, s}-L_{e}(s)=\sum_{l=0}^{e}(-1)^{l}(q-1)^{e-l}\binom{s}{l}\binom{n-s}{e-l}-\sum_{l=0}^{e}(-1)^{l}(q-1)^{e-l}\binom{s-1}{l}\binom{n-s}{e-l}=  \tag{16}\\
& \sum_{l=1}^{e}(-1)^{l}(q-1)^{e-l}\binom{s-1}{l-1}\binom{n-s}{e-l}=-\sum_{l=0}^{e-1}(-1)^{l}(q-1)^{e-1-l}\binom{s-1}{l}\binom{n-s}{e-1-l}=-L_{e-1}(s)
\end{align*}
$$

This proves the theorem (note that $L_{e}(0)>0$ ).

## References

[1] 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.

