

1. ISOPERIMETRIC INEQUALITIES

Proposition 1. *Suppose $G \cong \mathbb{F}_2^n$ and that G acts transitively on itself by translation, i.e. $x \mapsto g+x$. Let $A \subset G$ and $k \in \mathbb{N}$ fixed such that*

$$\binom{n}{k} \leq |A| < \binom{n}{k+1}$$

and $[n] = \{1, \dots, n\}$. Then we have

$$\begin{aligned} \forall \epsilon > 0, \exists n_0 \in \mathbb{N}; \forall n \geq n_0, \exists B'_\epsilon \subset [n]; |B'_\epsilon| \geq (1 - \epsilon)n; \\ \forall i \in B'_\epsilon \quad |e_i A \setminus A| \geq \frac{1}{2(k+2)}|A| \end{aligned}$$

Proof. Let $M = \{g \in G \mid |gA \setminus A| < |A|/2\}$ and $m = |M|$. Then we have the implication

$$\frac{1}{|G|} \sum_g |gA \setminus A| + |A|^2/|G| = |A| \implies m \leq 2|A|.$$

Here the key property is that $0 \leq |gA \setminus A| \leq |A|$ holds. Indeed,

$$\frac{1}{|G|} m |A|/2 + \frac{1}{|G|} (|G| - m) |A| + |A|^2/|G| = |A| - (m/2)/|G| + |A|^2/|G| \geq |A|$$

Hence there are at most $2|A|$ elements in G that satisfy $|gA \setminus A| < |A|/2$. We proceed by proving the implication

$$(1.1) \quad \forall 0 < \epsilon < 1, \exists n \in \mathbb{N}, \forall B_\epsilon \subset [n]; \forall i \in B_\epsilon, |e_i A \setminus A| < \frac{1}{2(k+2)}|A| \implies |B_\epsilon| < \epsilon n.$$

We prove this by contradiction, i.e. we assume that there exist $0 < \epsilon < 1$ such that for all $n \in \mathbb{N}$, $|B_\epsilon| \geq \epsilon n$ holds. We consider the set $\Omega = \{\sum_{j=1}^{k+2} e_i \mid i \in B_\epsilon\}$, since $G \cong \mathbb{F}_2^n$ we have

$$\exists n \in \mathbb{N}; \quad |\Omega| \geq \binom{\epsilon n}{k+2} > 2|A|$$

and consequently there exists some $g \in \Omega$ such that $|gA \setminus A| \geq |A|/2$. By assumption for any $i \in B_\epsilon$ $|e_i A \setminus A| < \frac{1}{2(k+2)}|A|$ holds and we obtain the contradiction

$$\frac{1}{2}|A| \leq |gA \setminus A| \leq \sum_{j=1}^{k+2} |e_{i_j} A \setminus A| < \frac{1}{2}|A|.$$

Therefore there exists some $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ less than ϵn elements of $[n]$ satisfy $|e_i A \setminus A| \geq \frac{1}{2(k+2)}|A|$. As a result, for $n \geq n_0$ there exists some $B'_\epsilon \subset [n]$, where $|B'_\epsilon| \geq (1 - \epsilon)n$ with the property

$$\forall i \in B'_\epsilon; \quad |e_i A \setminus A| \geq \frac{1}{2(k+2)}|A|$$

and the proposition follows. \square

Let $a = (a_1, \dots, a_n) \in Q_2^n$. We set

$$(1.2) \quad |(a_1, \dots, a_n)| = \sum_{a_i} a_i$$

where the sum is taken in \mathbb{Q} . We define a linear ordering \leq over Q_2^n as follows

$$\alpha \leq \beta \iff (|\alpha| < |\beta|) \vee (|\alpha| = |\beta| \wedge \alpha <_{\text{lex}} \beta).$$

Via \leq we assign an ordinal to each Q_2^n -vertex, denoted by

$$\omega_\leq : Q_2^n \longrightarrow \mathbb{N}, \quad a \mapsto \omega_\leq(a)$$

i.e. ω_\leq labels each $a \in Q_2^n$ counting up from $\omega_\leq(0, \dots, 0) = 1$ to $\omega_\leq(1, \dots, 1) = 2^n$. For any $A \subset Q_2^n$ let $x_{|A|} \in Q_2^n$ such that $\omega_\leq(x_{|A|}) = |A|$ and set

$$(1.3) \quad \mathbf{B}_n(A) = \{x \mid x \leq x_{|A|}\}.$$

$\mathbf{B}_n(A)$ is the initial segment of the order \leq , i.e. the set obtained by successively filling spheres centered at $(0, \dots, 0)$ according to the lexicographical order. We call $\mathbf{B}_n(A)$ the near Hamming ball of size $|A|$ and set

$$(1.4) \quad \mathbf{d}(A) = \{a \notin A \mid \exists 1 \leq i \leq n, e_i a \in A\}, \quad \text{and} \quad \partial A = |\mathbf{d}(A)|.$$

Theorem 1. *Suppose Q_2^n is the binary n -cube and $\mathbf{B}_n(A)$ the near Hamming ball of size $|A|$. Suppose $\binom{n}{k} \leq |A| < \binom{n}{k+1}$, then we have*

$$(1.5) \quad \partial A \geq \partial \mathbf{B}_n(A).$$

Proof. The idea is to prove via induction on n . To facilitate this we introduce the notion of i -compressed sets. Let us begin by setting $A_0(i) = \{(a)_j \mid a_i = 0\}$, $A_1(i) = \{(a)_j \mid a_i = 1\}$ and

$$(1.6) \quad C_i(A) = \left\{ x \in Q_2^n \mid x \in \begin{cases} \mathbf{B}_{n-1}(A_0(i)) & \text{for } x_i = 0 \\ \mathbf{B}_{n-1}(A_1(i)) & \text{for } x_i = 1 \end{cases} \right\}.$$

Claim 1. For any $1 \leq i \leq n$ we have $\partial C_i(A) \leq \partial A$.

We will prove Claim 1 by induction on n . First, we can w.l.o.g. assume that $|A_0(i)| \geq |A_1(i)|$. For any $\alpha \in \mathbf{d}(A)$ we have either $d(\alpha, A_0(i)) = 1$ or $d(\alpha, A_1(i)) = 1$. As a result we derive

$$(1.7) \quad \{\alpha \mid \alpha_i = 1, d(\alpha, A_1(i)) = 1\} \dot{\cup} \{\alpha \mid \alpha_i = 0, d(\alpha, A_0(i)) = 1\} \subset \mathbf{d}(A)$$

$$(1.8) \quad \{\alpha \mid \alpha_i = 1, d(\alpha, A_0(i) \setminus e_i A_1(i)) = 1\} \dot{\cup} \{\alpha \mid \alpha_i = 0, d(\alpha, A_0(i)) = 1\} \subset \mathbf{d}(A)$$

Eq. (1.7) and (1.8) imply

$$(1.9) \quad \partial A \geq \partial_{n-1} A_0(i) + \partial_{n-1} A_1(i)$$

$$(1.10) \quad \partial A \geq |A_0(i) \setminus e_i(A_1(i))| + \partial_{n-1} A_0(i)$$

where ∂_{n-1} denotes the vertex boundary taken in the $n - 1$ -cubes obtained by setting the i th-coordinate to 0 and 1, respectively. Indeed eq. (1.10) holds since an element in $\mathbf{d}(A) \cap \mathbf{d}(A_0(i))$ with i th coordinate being 1 is obtained by translation with the unit vector e_i . Then only elements can contribute which are not in $e_i(A_1(i))$ since only elements of $\mathbf{d}(A)$ count. Accordingly, eq. (1.9) and eq. (1.10) are equivalent to

$$(1.11) \quad \partial A \geq \max\{\partial_{n-1} A_0(i) + \partial_{n-1} A_1(i), |A_0(i) \setminus e_i(A_1(i))| + \partial_{n-1} A_0(i)\} .$$

We now proceed by induction on n . The case $n = 1$ being trivial we have by induction hypothesis

$$\begin{aligned} \partial_{n-1} C_i(A_0(i)) &\leq \partial_{n-1} A_0(i) \\ \partial_{n-1} C_i(A_1(i)) &\leq \partial_{n-1} A_1(i) , \end{aligned}$$

whence

$$\begin{aligned} \partial A \geq \max\{\partial_{n-1} C_i(A_0(i)) + \partial_{n-1} C_i(A_1(i)), \\ |A_0(i)| - |A_1(i)| + \partial_{n-1} C_i(A_0(i))\} . \end{aligned}$$

Our goal consists now in establishing the equality

$$\begin{aligned} \partial C_i(A) = \max\{\partial_{n-1} C_i(A_0(i)) + \partial_{n-1} C_i(A_1(i)), \\ |A_0(i)| - |A_1(i)| + \partial_{n-1} C_i(A_0(i))\} \end{aligned}$$

In order to prove this we show

$$\begin{aligned} \{\alpha \in \mathbf{d}(C_i(A)) \mid \alpha_i = 0\} &= \mathbf{d}(C_i(A_0(i))) \\ \{\alpha \in \mathbf{d}(C_i(A)) \mid \alpha_i = 1\} &= \begin{cases} e_i(C_i(A_0(i)) \setminus e_i C_i(A_1(i))) \\ \mathbf{d}(C_i(A_1(i))) \end{cases} \end{aligned}$$

Suppose $\alpha \in \mathbf{d}(C_i(A))$, then we have the implication

$$(1.12) \quad \alpha_i = 0 \implies \alpha \in \mathbf{d}_{n-1}(C_i(A_0(i))) .$$

Indeed, suppose $\alpha_i = 0$ then either $\mathbf{d}(\alpha, C_i(A_0(i))) = 1$ or $\mathbf{d}(\alpha, C_i(A_1(i))) = 1$. In the case of $\mathbf{d}(\alpha, C_i(A_1(i))) = 1$, there exists some $a \in C_i(A_1(i))$ with the property $e_i a = \alpha$ but by construction we have $e_i C_i(A_1(i)) \subset C_i(A_0(i))$, which contradicts $\alpha \in \mathbf{d}(C_i(A))$. Therefore eq. (1.12) follows. By definition of $C_i(A)$ we have the alternative

$$\begin{aligned} \mathbf{d}_{n-1}(C_i(A_1(i))) &\subset e_i [C_i(A_0(i)) \setminus e_i C_i(A_1(i))] \quad \text{or} \\ e_i [C_i(A_0(i)) \setminus e_i C_i(A_1(i))] &\subset \mathbf{d}_{n-1}(C_i(A_1(i))) . \end{aligned}$$

and consequently

$$(1.13) \quad \{\alpha \in \mathbf{d}(C_i(A)) \mid \alpha_i = 1\} = \begin{cases} e_i [C_i(A_0(i)) \setminus e_i C_i(A_1(i))] \\ \mathbf{d}_{n-1}(C_i(A_1(i))) \end{cases} .$$

By combining eq. (1.12) and eq. (1.13) we obtain

$$\begin{aligned} \partial C_i(A) &= \max\{\partial_{n-1} C_i(A_0(i)) + \partial_{n-1} C_i(A_1(i)), \\ &\quad |A_0(i)| - |A_1(i)| + \partial_{n-1} C_i(A_0(i))\} . \end{aligned}$$

Hence we have for any $1 \leq i \leq n$, $\partial C_i(A) \leq \partial A$, and Claim 1 is proved.

We consider $C_i : \{A' \subset Q_2^n\} \rightarrow \{A' \subset Q_2^n\}$ and proceed by showing

$$(1.14) \quad \omega(C_i(A)) \leq \omega(A) \quad \text{where} \quad \omega(A) = \sum_{a \in A} \omega(a) .$$

and $\omega(C_i(A)) = \omega(A)$ if and only if $C_i(A) = A$. Suppose $\eta \in A \neq C_i(A)$, w.l.o.g. we can assume $\eta_i = 0$. Then consider the mapping

$$c_i : A \longrightarrow C_i(A)$$

defined as follows. Totally order A via ω . Let ω_i be the induced order obtained by removing the i th coordinate. Then $A_0(i)$ and $A_1(i)$ have the property suppose $v, v' \in A_j(i)$ then $\omega_i(v) < \omega_i(v')$ iff $\omega(v) < \omega(v')$. Then $c_i(a) = x_{\omega_i(a)}$ and c_i has the property that $\omega(c_i(a)) \leq \omega(a)$ and $\eta \neq c_i(\eta)$ implies $\omega(c_i \eta) < \omega(\eta)$. Therefore $A \neq C_i(A)$ implies $\omega(C_i(A)) < \omega(A)$. As a result we can successively apply C_1, \dots, C_n and have a sequence of sets A, A_1, A_2, \dots with the properties $\omega(A_{i+1}) \leq \omega(A_i)$. This is a monotone sequence which is also bounded from below and therefore converges to say ξ . Consequently we arrive at some set $C(A)$ with the property $\omega(C(A)) = \xi$ and

$$\forall 1 \leq i \leq n, \quad C_i(C(A)) = C(A) .$$

Claim 2. For A such that $\binom{n}{k} \leq |A| < \binom{n}{k+1}$ we have $C(A) = B_n(A)$.

Indeed, let β be minimal w.r.t. \leq in the complement of $C(A)$ and α be maximal in $C(A)$. By

assumption $C_i(C(A)) = C(A)$, for any $i = 1, \dots, n$ from which we conclude that each element in $C(A)$ has the property $|\alpha| \leq k + 1$. Hence for β and α there exists at least one coordinate $j = 1, \dots, n$ such that $\beta_j = \alpha_j = 0$. But then $\omega_{\leq}(\alpha) < \omega_{\leq}(\beta)$ since $C_j(C(A)) = C(A)$ and $C_j(C((A)))_0(j) = B_{n-1}(C(A)_0(j)) = B_{n-1}(A_0(j))$. Therefore we have shown

$$C(A) = B_n(A)$$

and

$$\partial A \geq \partial \mathbf{B}_n(A)$$

and the proof of the theorem is complete. □