Definition. *We set* $\mathcal{Z}_m$ *the zonotope generated by all* $v \in \{0,1\}^m$*.*

We aim to prove the following theorem.

Theorem. *The number of facets* $F(m)$ *of* $\mathcal{Z}_m$ *is at least* $2^{\frac{1}{2}mlog(m)+\mathcal{O}(mloglog(m))}$*.*

Lemma. *The following equivalences hold.*

$$c \text{ is a facet defining vector}$$
$$\Longleftrightarrow$$
$$c \in \mathbb{R}^m, dim(c^\perp \cap \{0,1\}^m) = m-1$$
$$\Longleftrightarrow$$
$$\exists\{v_1,\ldots,v_{m-1}\} \text{ linearly independent vectors of } \{0,1\}^m \text{ perpendicular to } c.$$

There further is a bijection between each facet and all positive multiples of some facet-defining vector c*.*

We may suppose $c \in \mathbb{Z}^m$ since there exist an integer solution to $Ac = 0$ as soon as A is rational. To get a unique c, we may suppose the coordinates of c are coprime.

Notation. $c^\perp := \{x \in \mathbb{R}^m | c^T x = 0\} \cap \{0,1\}^m$,
$Im(c) := \{c^T v | v \in \{0,1\}^m\}$
We use "facet" colloquially for a facet-defining vector c*.*
We note $\begin{pmatrix} 0 \\ c^\perp \end{pmatrix} := \{\begin{pmatrix} 0 \\ v \end{pmatrix} | v \in c^\perp\}$.

Proposition. *Each facet* $c \in \mathbb{Z}^m$ *of* $\mathcal{Z}_m$ *generates* $|Im(c)|$ *unique facets of* $\mathcal{Z}_{m+1}$ *in* $\mathbb{Z}^{m+1}$*.*

Proof. Let $Im(c) = \{\alpha_1, \ldots, \alpha_i\}$, with $\alpha_1 = 0$. And define $d_k := \begin{pmatrix} -\alpha_k \\ c \end{pmatrix}$.

Then each d_k is a facet of $\mathcal{Z}_{m+1}$. Indeed, $d_k \neq 0$ and $d_k^\perp$ includes both $\begin{pmatrix} 0 \\ c^\perp \end{pmatrix}$ and some vector of the form $\begin{pmatrix} 1 \\ v \end{pmatrix} \in \{0,1\}^{m+1}$. It hence includes m linearly independant vectors and generates a facet.

We must show the facets are unique and that there is no overlap from two different facets of $\mathcal{Z}_m$. We cannot have $d_k^\perp = d_l^\perp$ for some $l \neq k$, since the added vector $\begin{pmatrix} 1 \\ v \end{pmatrix} \in \{0,1\}^{m+1}$ is not perpendicular to d_l.

For two different starting facets $c, c' \in \mathbb{Z}^m$, the generated facets of $\mathcal{Z}_{m+1}$ are also different since the vectors perpendicular to them with first coordinate 0 are exactly $\begin{pmatrix} 0 \\ c^\perp \end{pmatrix}$ and $\begin{pmatrix} 0 \\ (c')^\perp \end{pmatrix}$ respectively. $\square$

Definition. *$F(m) := f_{m-1}(\mathcal{Z}_m) =$ number of facets of $\mathcal{Z}_m$.*
$\alpha_l := \{c$ facets of $\mathcal{Z}_m : |Im(c)| = l\}$.

Note that the size of the image is invariant under positive multiplication. Also, $\sum_{l\geq 2} \alpha_l = F(m)$, and the sum is finite. It starts at 2 since $dim(c^\perp) = m-1$.

Corollary.

$$F(m+1) \geq \sum_{l\geq 2} l\alpha_l.$$

And hence $F(m+1) \geq 2F(m)$.

Example. *Let's compute the first coefficient α_2.*
Take a $c \in \mathbb{Z}^m$ such that $Im(c) = \{0, \alpha\}$, $\alpha \in \mathbb{Z}$, and decompose it as

$$c = (0, 0, \dots, 0, \tilde{c}),$$

with $\tilde{c}_k \neq 0 \forall k$ and up to a choice of placement of the nonzero coefficients.

Note that c is a facet of $\mathcal{Z}_m$ if and only if $\tilde{c} \in \mathbb{Z}^d$ is a facet of $\mathcal{Z}_d$. Furthermore, note that $Im(c) = Im(\tilde{c}) = \{0, \alpha\}$. However, since $\tilde{c}_k$ is in the image for each k, and it is nonzero, we must have $\tilde{c} = (\alpha, \dots, \alpha)$. In this case, $Im(\tilde{c}) = \{0, \alpha, 2\alpha, \dots d\alpha\}$, which implies directly that $d = 1$. Up to normalization, the only two possible $\tilde{c}$ are in fact 1 and -1.

This implies in turn that only $2m$ vectors c exist with the supposed properties, and $\alpha_2 = 2m$.

Lemma.

$$\alpha_l \leq l m^{l^2} F(l^2).$$

Proof. We split $c \in \mathbb{Z}^m$ as

$$c = (0, 0, \dots, 0, \tilde{c}),$$

with $\tilde{c}_k \neq 0 \forall k$ and up to a choice of placement of the nonzero coefficients. We aim now to bound the dimension d that $\tilde{c} \in \mathbb{Z}^d$ defines a facet in.

Since $|Im(c)| = l$, each $\alpha \in Im(c)$ may appear in $\tilde{c}$ at most l times. This gives directly that $d \leq l^2$.

Hence

$$\alpha_l \leq \sum_{i=1}^{l^2} \binom{m}{i} F(i) \leq l^2 m^{l^2} F(l^2).$$

□

Proposition.

$$F(m+1) \geq \frac{1}{4}\sqrt{\frac{m}{log(m)}} F(m),$$

for all m sufficiently large.

Proof. Set the threshold $T := \frac{1}{2}\sqrt{\frac{m}{log(m)}}$. The corollary above gives

$$\begin{aligned} F(m+1) \geq \sum_{l \geq 2} l\alpha_l &\geq \sum_{l=2}^{T-1} l\alpha_l + T \sum_{l \geq T} \alpha_l, \\ &\geq \sum_{l=2}^{T-1} l\alpha_l + T \left[F(m) - \sum_{l=2}^{T-1} \alpha_l \right], \\ &= TF(m) + \sum_{l=2}^{T-1} (l-T)\alpha_l. \end{aligned}$$

By the proposition, $\alpha_l \leq l m^{l^2} F(l^2)$, and therefore

$$(l-T)\alpha_l \geq -Tl^2 m^{l^2} F(l^2).$$

Furthermore, since $F(m+1) \geq 2F(m)$, we get

$$(l-T)\alpha_l \geq -Tl^2 m^{l^2} 2^{l^2-m} F(m).$$

Since $l \leq T = \frac{1}{2}\sqrt{\frac{m}{log(m)}}$, we evaluate the expression to

$$(l-T)\alpha_l \geq -m^{\frac{3}{2}} 2^{\frac{1}{4}m} 2^{\frac{1}{4}m-m} F(m) \geq -2^{-\frac{1}{4}m} F(m),$$

for m sufficiently large.

In conclusion,

$$
\begin{aligned}
F(m+1) \geq \sum_{l\geq 2} l\alpha_l \geq TF(m) + \sum_{l=2}^{T-1}(l-T)\alpha_l, \\
&\geq TF(m) - 2^{-\frac{1}{4}m}F(m), \\
&\geq \frac{1}{2}TF(m) = \frac{1}{4}\sqrt{\frac{m}{log(m)}}F(m),
\end{aligned}
$$

for m again sufficiently large. $\square$

Corollary. *The number of facets of $\mathcal{Z}_m$ is at least $2^{\frac{1}{2}mlog(m)+\mathcal{O}(mloglog(m))}$.*

Proof. Since $F(m+1) \geq \frac{1}{4}\sqrt{\frac{m}{log(m)}}F(m)$ for all $m > N$ for some constant N,

$$
\begin{aligned}
F(m) &\geq 4^{-m}\sqrt{\frac{m!}{\prod_{k=2}^{m} log(k)}}\sqrt{\frac{\prod_{k=2}^{N} log(k)}{N!}}F(N), \\
&= 2^{\frac{1}{2}mlog(m)+\mathcal{O}(mloglog(m))},
\end{aligned}
$$

because $\prod_{k=2}^{m} log(k) \leq 2^{mloglog(m)}$ (tight). $\square$