Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 40 (1994)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ENUMERATIVE COMBINATORICS AND CODING THEORY
Autor: Eliahou, Shalom
Kapitel: 4. ON THE LEAST VALUE OF f
DOI: https://doi.org/10.5169/seals-61109

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 18.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

4. On the least value of f

Let us consider again an integral polynomial $f = u_1 + \cdots + u_N$, with $u_i \in M_n$ for all i. By Theorem 2 and the MacWilliams identity, the cardinality of $f^{-1}(v)$ can be expressed in terms of the weight enumerator of the dual code $K_f = L_f^{\perp}$, for every v in $\mathbf{Z}$.

In this section, we will obtain another such formula for $|f^{-1}(v)|$, provided v is a lower bound for the range of f. These results could be applied to "count" the number of binary zeros of f, since $v = 0$ is a lower bound for the range of f^2, and f^2 has as many binary zeros as f does.

THEOREM 4. *Let $f = u_1 + \cdots + u_N$ with $u_i \in M_n$ for all i, and let $K := L_f^{\perp}$ be the dual of the code L_f associated with f, with weight enumerator $P_K(T)$. Assume that $v \in \mathbf{Z}$, $v \equiv N \bmod 2$, is a lower bound for f, i.e.*

$$v \leqslant f(p)$$

for all $p \in \{1, -1\}^n$. Then we have

$$|f^{-1}(v)| = \frac{1}{2^{\beta} \cdot \alpha!} \cdot P_K^{(\alpha)}(-1)$$

where

1. $\alpha = \alpha(v) = (N + v)/2$,
2. $\beta = \beta(v) = (N - v)/2 - n$, *and*
3. $P_K^{(\alpha)}(-1)$ *denotes the value at* -1 *of the* α*-th derivative of* $P_K(T)$.

Proof. Let $P_L(T) = \sum_{i=0}^{N} a_i T^i$ denote the weight enumerator of $L = L_f$, and let $\gamma = \gamma(v) = (N - v)/2$. By Corollary 3, we have $\deg P_L \leqslant \gamma$ since $f(p) \geqslant v$ for all p, and

$$|f^{-1}(v)| = 2^{n - \dim L} \cdot \alpha_\gamma . \tag{1}$$

Now, by the MacWilliams identity, the weight enumerator of K is given by

$$\begin{aligned} P_K(T) &= \tfrac{1}{|L|} \cdot \textstyle\sum_{i=0}^{\gamma} a_i (1+T)^{N-i}(1-T)^i \\ &= \tfrac{1}{|L|} \cdot (1+T)^{N-\gamma} \cdot \left(a_\gamma (1-T)^\gamma + (1+T)Q(T)\right) , \end{aligned}$$

where $Q(T)$ is some polynomial in T. Note that $N - \gamma = \alpha = (N + v)/2$.

To extract α_γ from the above expression, we derive α times, and evaluate at $T = -1$:

$$\begin{aligned} P_K^{(\alpha)}(-1) &= \tfrac{1}{|L|} \alpha!\, \alpha_\gamma 2^\gamma \\ &= \tfrac{1}{2^{\dim L}} \alpha!\, \alpha_\gamma 2^{N-\alpha} , \end{aligned}$$

and therefore

$$\alpha_\gamma = \frac{1}{2^{N-\alpha-\dim L}\,\alpha!} P_K^{(\alpha)}(-1) .$$

Multiplying both sides by $2^{n-\dim L}$, and plugging in equation (1), we obtain the claimed formula for $|f^{-1}(v)|$. □

COROLLARY 5. *Let* v_{min} *be the least value assumed by* f *on binary points. Then*

$$\frac{1}{2}(N + v_{min}) = \textit{the order of } -1 \textit{ as a root of } P_K(T) . \qquad \square$$

5. THE NUMBER OF HADAMARD MATRICES OF ORDER n

A *Hadamard matrix* is a square matrix H of order n with entries in $\{+1, -1\}$, satisfying the relation

$$H \cdot H^\top = nI_n .$$

($H^\top$ denotes the transpose of H, and I_n the identity matrix of order n.)

It is well known that the order of a Hadamard matrix can only be 1, 2 or a multiple of 4. Conversely, the existence of a Hadamard matrix of order n for every $n \equiv 0 \bmod 4$ is a longstanding conjecture, due to Jacques Hadamard [H]. The smallest open case currently occurs at $n = 428$. For a survey on Hadamard matrices, see [SY].

The theory exposed above yields a counting formula for Hadamard matrices of order n, in terms of the weight enumerator of a certain binary linear code of length $\binom{n}{2}^2$.

STEP 1. *Defining equations for Hadamard matrices.*

We represent binary matrices of order n as points $p = (p_{i,j}) \in \{1, -1\}^{n^2}$. Considering n^2 variables $\{x_{i,j}\}_{1 \leqslant i,j \leqslant n}$, let

$$g_{k,l} = \sum_{r=1}^{n} x_{k,r} x_{l,r} .$$

If $p = (p_{i,j})$ is a binary matrix, then $g_{k,l}(p)$ is the dot product of the k-th and l-th rows of p. Thus, a binary matrix p is Hadamard if and only if

$$g_{k,l}(p) = 0 \quad \text{for all } 1 \leqslant k < l \leqslant n .$$