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 $|f^{-1}(v)|$. $\qquad\square$

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

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

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

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

STEP 2. *Reduction to a single equation.*

Let

$$g = \sum_{1 \leqslant k < l \leqslant n} g_{k,l}^2 \, .$$

By construction, we have the following properties:

(1) $g(p) \geqslant 0$ for every binary matrix p;

(2) $g(p) = 0$ if and only if p is Hadamard.

Developing the expression for g, we obtain:

$$
\begin{aligned}
g &= \sum_{k < l} g_{k,l}^2 \\
  &= \sum_{k < l} \left(\sum_r x_{k,r} x_{l,r} \right)^2 \\
  &= \sum_{k < l} \left(n + 2 \sum_{r < s} x_{k,r} x_{l,r} x_{k,s} x_{l,s} \right) \\
  &= n \binom{n}{2} + 2f,
\end{aligned}
$$

where

$$f := \sum_{k < l} \sum_{r < s} x_{k,r} x_{l,r} x_{k,s} x_{l,s} \, .$$

(Of course, the above computation is performed modulo the relations $x_{i,j}^2 = 1$ for all i,j.)

The following properties of $f = \frac{1}{2} \left(g - n \binom{n}{2} \right)$ derive instantly from those of g:

(1) $f(p) \geqslant -\frac{1}{2} n \binom{n}{2}$ for every binary matrix p;

(2) $f(p) = -\frac{1}{2} n \binom{n}{2}$ if and only if p is Hadamard.

STEP 3. *The code associated with* f.

Let $K_n := L_f^\perp$ denote the dual of the binary code L_f associated with f, as defined in Section 3. Explicitly, we consider the map

$$
\begin{aligned}
\phi_n : \qquad \mathbf{F}_2^{\binom{n}{2}^2} &\to \mathbf{F}_2^{n^2} \\
E(k, l; r, s) &\mapsto e_{k,r} + e_{l,r} + e_{k,s} + e_{l,s} \, ,
\end{aligned}
$$

where $\{E(k, l; r, s)\}_{1 \leqslant k < l \leqslant n, 1 \leqslant r < s \leqslant n}$ and $\{e_{i,j}\}_{1 \leqslant i, j \leqslant n}$ denote the standard bases of the left and right spaces, respectively; by construction then, $K_n = \mathrm{Ker}\,(\phi_n)$.

As a direct consequence of Theorem 4 and of the above-mentioned properties of f, we obtain the

THEOREM 6. *Let K_n (n even) be the code of length $\binom{n}{2}^2$ defined as the kernel of the above map $\phi_n : \mathbf{F}_2^{\binom{n}{2}^2} \to \mathbf{F}_2^{n^2}$. Let $P_n(T)$ denote the weight enumerator of K_n . Then the number $h(n)$ of Hadamard matrices of order n is given by*

$$h(n) = \frac{1}{2^{\beta(n)}\,\alpha(n)!} \cdot P_n^{(\alpha(n))}(-1) ,$$

where

1. $\alpha(n) = n^2(n-1)\,(n-2)/8;$

2. $\beta(n) = n^3(n-1)/8 - n^2;$

3. $P_n^{(\alpha(n))}(-1)$ *denotes the $\alpha(n)$-th derivative of $P_n(T)$, evaluated at -1 .*

Proof. In the formula of Theorem 4, replace:

- N, the length of the code, by $\binom{n}{2}^2$;

- v, a lower bound for the values of f , by $-\frac{1}{2}n\binom{n}{2}$; and

- n, the number of variables in f , by n^2 .   □

Thus, the determination of the weight enumerator of K_n is an important problem. We will give below, without proof, the number of codewords of weight 3, 4 and 5 of K_n . (Of course, there are no words of weight 1 or 2 in K_n .) But the problem can be generalized a little bit, as follows. Consider the map

$$\phi_{m,n} : \quad \mathbf{F}_2^{\binom{m}{2}\binom{n}{2}} \quad \to \quad \mathbf{F}_2^{mn}$$

$$E(k,l;r,s) \quad \mapsto \quad e_{k,r} + e_{l,r} + e_{k,s} + e_{l,s} ,$$

where now, the indices $k < l$ range from 1 to m instead of 1 to n . We denote by $K_{m,n}$ the kernel of $\phi_{m,n}$.

Let $\Gamma = \{1, ..., m\} \times \{1, ..., n\}$. We can think of the vector basis $e_{i,j}$ as the point on row i and column j in the grid Γ , and of $E(k,l;r,s)$ as the rectangle determined by rows k, l and columns r, s in Γ . The image of $E(k,l;r,s)$ under $\phi_{m,n}$, then, is the formal sum of its four corners.

Thus, an element of weight w in $K_{m,n}$ can be pictured as a set of w rectangles in the grid Γ , such that every point in the grid coincides with an *even* number of corners of the rectangles in the set.

For example, all elements of weight 3 in $K_{m,n}$ can be represented (up to proper size and location) by the following picture:
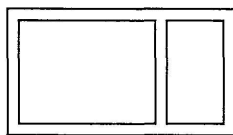
or its vertical analogue. This picture represents a codeword of the form

$$E(k, l; r_1, r_2) + E(k, l; r_1, r_3) + E(k, l; r_2, r_3) .$$

Thus, the number of codewords of weight 3 in $K_{m,n}$ is equal to

$$w_3(K_{m,n}) = \binom{m}{2}\binom{n}{3} + \binom{m}{3}\binom{n}{2} .$$

Similarly, one can show that

$$w_4(K_{m,n}) = 3\binom{m}{2}\binom{n}{4} + 9\binom{m}{3}\binom{n}{3} + 3\binom{m}{4}\binom{n}{2} ;$$

$$w_5(K_{m,n}) = 12\binom{m}{2}\binom{n}{5} + 72\binom{m}{3}\binom{n}{4} + 72\binom{m}{4}\binom{n}{3} + 12\binom{m}{2}\binom{n}{5} + 9\binom{m}{3}\binom{n}{3} .$$

As a last remark, note that an upper bound for the weights in the associated code L_f is given by $\frac{1}{8}n^3(n-1)$, and that this bound is actually attained for some n if and only if there exists a Hadamard matrix of order n. This follows from, say, Corollary 3.

6. THE NUMBER OF PROPER 4-COLORINGS OF A GRAPH

Let $G = (V, E)$ be a simple graph (no loops, no multiple edges) with vertex set V and edge set E. We will identify V with $\{1, ..., n\}$, and denote the cardinality of E by e.

A 4-*coloring* of G is the assignment to every vertex of one among four fixed colors; such a coloring is *proper* if the colors assigned to the end vertices of any edge are distinct. For a survey on the 4-colorings of planar graphs, see [SK].

We will count the number of proper 4-colorings of G, in terms of the weight enumerator of a certain code of length $3e$.

STEP 1. *The defining equations for proper 4-colorings.*

As our palette of colors, we will choose the 4-set $\{1, -1\}^2$. The space of all 4-colorings of G can thus be identified with $\{1, -1\}^{2n}$, for example as follows: