# 2. Coding theory

where $\hat{f} = (x_0 + 1)^2 + (f_1 + x_0 f_2)^2$. Of course, all coefficients of $\hat{f}$ are non-negative, as desired.

Finally, we may assume that all monomials in $f$ are square-free, by removing any square in any monomial if necessary. The values assumed by $f$ on binary points will not be altered, for if $u, v$ are monomials, then $u^2 v - v$ takes the constant value 0 on $\{1, -1\}^n$.

## 2. Coding theory

To fix the notation and terminology, we briefly recall a few notions from coding theory. For more information, see [MS].

Consider the vector space $\mathbf{F}_2^N$ with its canonical basis fixed. The *(Hamming) weight* $|z|$ of a vector $z \in \mathbf{F}_2^N$ is the number of non-zero coordinates of $z$. A *binary linear code* (or *code,* for short) is a vector subspace $C$ of $\mathbf{F}_2^N$. The integer $N$ is called the *length* of $C$. The *weight enumerator* of $C$ is the polynomial

$$P_C(T) = \sum_{z \in C} T^{|z|}.$$

A *generator matrix* for $C$ is a $k \times N$ matrix $G$ over $\mathbf{F}_2$ whose rows span $C$. A *parity check matrix* for $C$ is an $(N-k) \times N$ matrix $H$ over $\mathbf{F}_2$ such that

$$C = \{z \in \mathbf{F}_2^N, \quad H \cdot z^{\top} = 0\}.$$

Equivalently, $C$ is the kernel of the map $h : \mathbf{F}_2^N \to \mathbf{F}_2^{N-k}$ whose matrix in the standard bases is $H$. The *dual* of $C$ is the space

$$C^{\perp} = \{y \in \mathbf{F}_2^N \mid y \cdot z = 0 \text{ for all } z \in C\},$$

where $y \cdot z$ denotes the usual dot product of $y$ and $z$ with value in $\mathbf{F}_2$. We have:

$$\dim C^{\perp} = N - \dim C, \text{ and } C^{\perp\perp} = C.$$

A binary matrix $H$ is a generator matrix for $C$ if and only if it is a parity check matrix for $C^{\perp}$. Finally, the weight enumerator of $C$ determines the weight enumerator of its dual $C^{\perp}$ by the *MacWilliams identity* [M]:

$$P_{C^{\perp}}(T) = \frac{1}{|C|} \cdot (1+T)^N \cdot P_C\left(\frac{1-T}{1+T}\right).$$