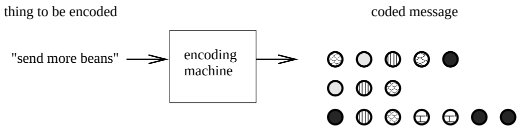


FIGURE 1. Sending a message

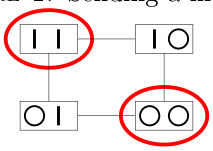


FIGURE 2. A code in $\mathbb{F}_2^2$

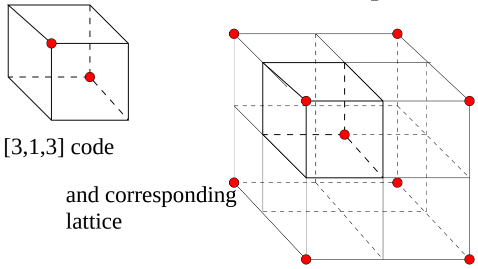
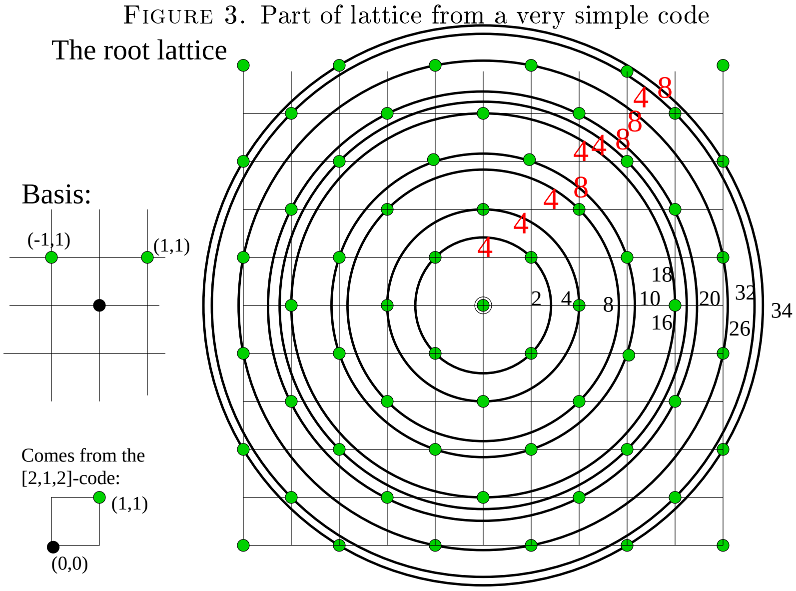


FIGURE 3. Part of lattice from a very simple code



$$\vartheta_\Gamma(q) = 1 + 4q^2 + 4q^4 + 4q^8 + 8q^{10} + 4q^{16} + 4q^{18} + 8q^{20} + 8q^{26} + 4q^{32} + 8q^{34} + \ldots..$$

FIGURE 4. Example of a theta function

1. pictures

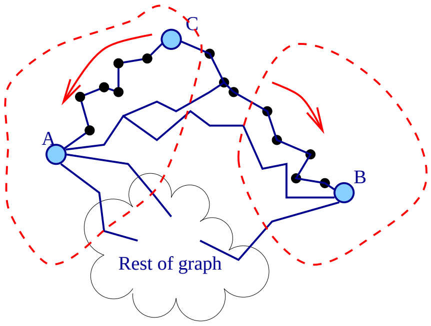


FIGURE 5. Correction of errors

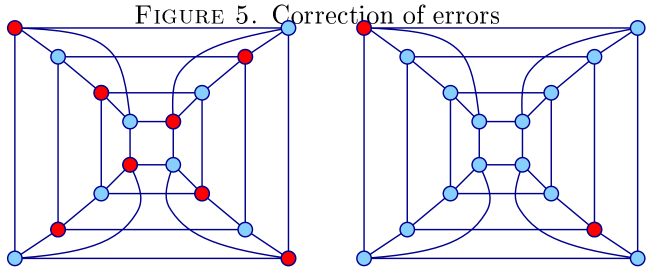


FIGURE 6. Codes in $\mathbb{F}_2^4$

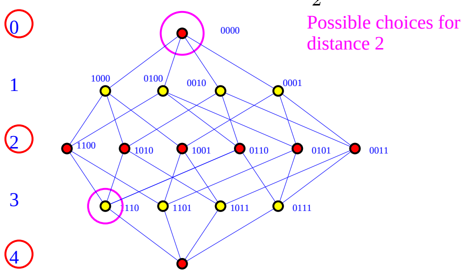


FIGURE 7. Graph for $\mathbb{F}_2^4$

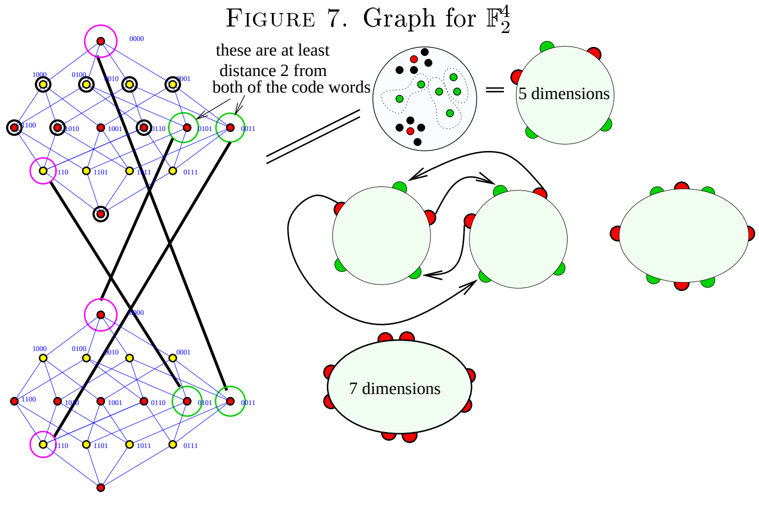


FIGURE 8. Towards the Hamming code

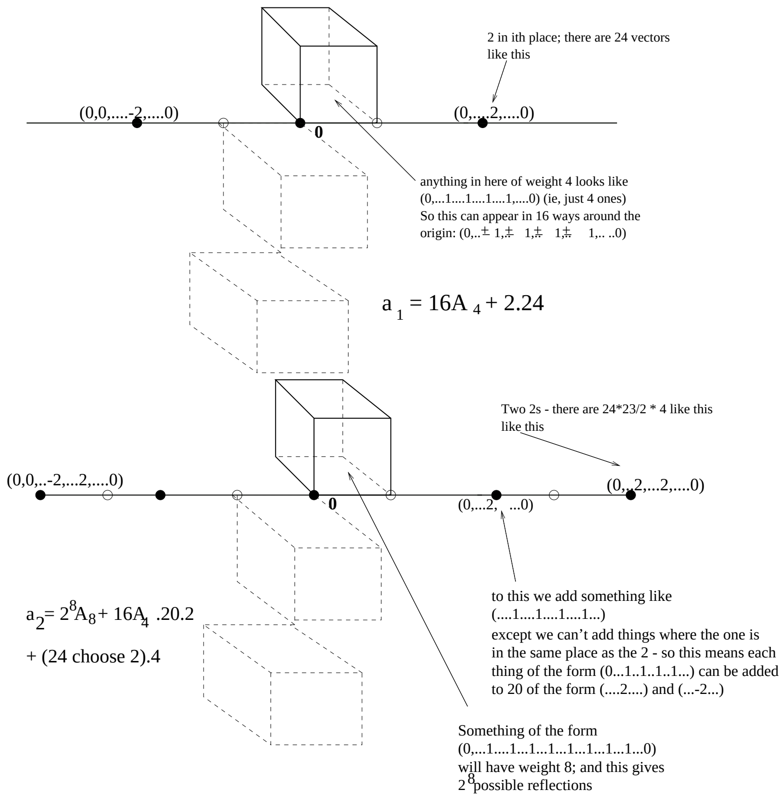


FIGURE 9. Where relations between a_i and A_i come from

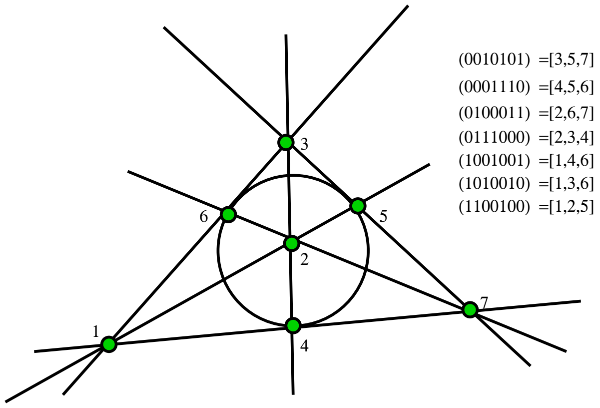


FIGURE 10. Steiner $S(2, 3, 7)$ system

2. Definitions

Finite simple group: a group G with no normal subgroup

Normal subgroup: $H \leq G$, s.t $\forall g \in G$, $g^{-1}Hg \leq H$.

Lattice, Γ: $\Gamma = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n \subset \mathbb{R}^n$, $\{e_i\}$ a basis of $\mathbb{R}^n$.

Integral lattice, Γ: $\forall x, y \in \Gamma$, $x.y \in \mathbb{Z}$.

Dual lattice, Γ: $\Gamma^* = \{x \in \mathbb{R}^n | x.y \in \mathbb{Z} \forall y \in \Gamma\}$

Unimodular lattice Γ: $\Gamma = \Gamma^*$.

even lattice Γ: $\forall x \in \Gamma, 2|x.x$.

Root vector $x \in \Gamma$: $x.x = 2$.

Root Lattice Γ: Γ is generated by it's roots.

Code of lenght n: $C \subset \mathbb{F}_q^n$.

Binary code of length n: $C \subset \mathbb{F}_2^n$. (We just cover this case today.)

distance between code words: number of places they differ.

Weight of a code word: Number of non zero entries.

Linear code: Linear subspace of ${\mathbb{F}_q}^n$

(n,M,d)-code: $C \subset \mathbb{F}_2^n$, $|C| = M$, min distance between code words is d.

[n,k,d]-code: $C \cong \mathbb{F}_2^k \subset \mathbb{F}_2^n$, minimum distance between code words is d.

Information rate: $R := \frac{log_2(M)}{n}$

modular form of weight k: A function $f(\tau)$, $\tau \in \mathbb{H}$, the upper half plane, with $f(\gamma\tau) = (c(\gamma, \tau))^k f(\tau)$, and $f(\tau)$ has an expansion in terms of $q = exp(2\pi i\tau)$. Here $c(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau) = (c\tau + d)$.

Theta function of a lattice Γ, $\vartheta_\Gamma(\tau)$: $\vartheta_\Gamma(\tau) = \sum_{x \in \Gamma} q^{\frac{1}{2}x.x}, q = e^{2\pi i\tau}$

Steiner system, S(n,m,l): $(X, \mathcal{B})$, X a set, $|X| = n$, $\mathcal{B} \subset \mathcal{P}(X)$, $\forall U \in \mathcal{B}$, $|U| = m$; $\forall O \subset X, |O| = l \Rightarrow \exists! U \in \mathcal{B} \ni O \subset U$.