Application: Error-correcting code (modems, cell phones, CDs, credit card #s, barcodes)

A code is a subset $C \subset S^n$ of codewords of length n over an alphabet S.

Often $S = \{0,1\}$: "binary code"   Assume $S = \mathbb{F}_q$

Distance fn: $d(x,y) = \#$ of positions where x,y differ

(Check: $d(x,y) + d(y,z) \geq d(x,z)$)

Distance d of C = minimum distance between two words.

Idea:
You wish to transmit words over a noisy channel, which may introduce some errors.
If your vocabulary only has words far from each other, then small errors can be corrected.

Note. If I can guarantee $< d/2$ errors, and the code has distance d, I can correct all errors.

The nicest codes are the

Linear codes: k-subspace $U \subset \mathbb{F}_q^n$ "(n,k)-code"

Note: $d(x,y) = d(\underset{\text{in } U}{x-y}, 0) = \#$ of nonzero coords of $x-y$.
$= \operatorname{supp}(x-y)$

So we care about $\operatorname{supp}(x)$ for $x \in U$.

The <u>weight enumerator</u> of the code $U \subset \mathbb{F}_q^n$ is:

$$A_U(z) = \sum_{u \in U} z^{w(u)} \qquad w(u) = \text{weight of } u = |\text{supp } u|$$

$$= \sum_{i=0}^{n} A_i z^i \qquad A_i = \# \text{ of words with } i \text{ non-zero coords}$$

It is extremely useful – it allows you to compute the probabilities that a decoding algorithm will succeed in decoding the errors.

<u>Easy example.</u> $U = \text{rowspace} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \{(x,y,z) \mid x+y+z=0\} \subset \mathbb{F}_2^3$

Want to transmit $\binom{a}{b}$ but an error might be introduced.

So instead transmit $\binom{a}{b}^T \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (a \;\; b \;\; a+b)$.

No error: $a+b+c=0$.
Error: $a+b+c=1$.

$A_U(z) = 1 + 3z^2$ (because $U = \begin{Bmatrix} 000 & 011 \\ 101 & 110 \end{Bmatrix}$)

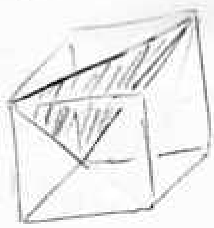
$T_{U_{3,2}}(x,y) = x^2+x+y$

$$\boxed{\begin{array}{l} \underline{\text{Theorem.}} \text{ (Greene 76)} \\ \text{Let } U \subset \mathbb{F}_q^n \text{ be an } (n,k)\text{-code.} \\ \text{Let } M \text{ be the matroid of } U. \\ \quad A_U(z) = (1-z)^k z^{n-k} T_M\left(\dfrac{1+(q-1)z}{1-z}, \dfrac{1}{z}\right) \end{array}}$$

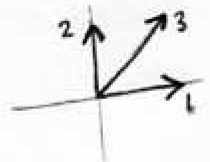
Pf Recall: The matroid M is the matroid of the columns of any matrix whose rowspace is U.

$U = \text{rowspace}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

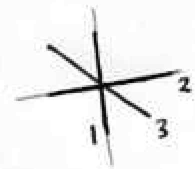
$= \{(x,y,z) \mid x+y+z=0\}$



$V = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$
$\quad v_1 \quad v_2 \quad v_3$



$\mathcal{A} = \begin{cases} x = 0 & H_1 \\ y = 0 & H_2 \\ x+y=0 & H_3 \end{cases}$



A word $u \in U$ is $\quad u = a(101) + b(011)$

$(i\text{-th coord} = 0) \iff (a,b)\cdot v_i = 0 \iff (a,b) \in H_i$

So $\quad w(u) = n - h\left(\begin{pmatrix} a \\ b \end{pmatrix}\right)$

(finite-field method)

$$A_U(z) = \sum_{u \in U} z^{w(u)} = \sum_{a \in \mathbb{F}_q^r} z^{n-h(a)} = z^n \sum_{a \in \mathbb{F}_q^r} (1/z)^{h(a)} = z^n \left(\frac{1}{z}\right)^{n-r} \overline{\chi}_M\left(\frac{1}{z}, t\right) \quad \blacksquare$$

"One of the most powerful theorems of coding theory":

Theorem. (Florence MacWilliams 1963)
Let U be an (n,k) code over $\mathbb{F}_q$, and $U^\perp$ its dual $(n, n-k)$ code.

$$A_{U^\perp}(z) = \frac{(1+(q-1)z)^n}{q^k} A_U\left(\frac{1-z}{1+(q-1)z}\right)$$

Proof:
- $A_U(\text{mess}) = (\text{mess})\, T_M(\text{mess}, \text{mess})$
- $A_{U^\perp}(\text{mess}) = (\text{mess})\, T_{M^*}(\text{mess}, \text{mess})$
- $T_M(\text{mess}_1, \text{mess}_2) = T_{M^*}(\text{mess}_2, \text{mess}_1) \quad \blacksquare$