Generalized Hypercube on $n = 2^k$ vertices of degree $d > k$.

Defined by $g_1, \ldots g_d \in \{0,1\}^k$

Has adj eigvals $\mu_b = \sum_{i=1}^{d} (-1)^{g_i^T b \bmod 2} =$

$$(-1)^x = 1 - 2x \quad x \in \{0,1\}$$

Construct $G = \begin{array}{c} \\ d \end{array}\begin{array}{c} k \\ \begin{pmatrix} - g_1 - \\ \vdots \\ - g_d - \end{pmatrix} \end{array}$ entries in $\mathbb{F}_2 = \{0,1\} \bmod 2$

$b \in \mathbb{F}_2^k$

$$\mu_b = d - 2|Gb| \quad \text{where } |x| = \#\{i : x(i) \neq 0\}$$

Hamming weight

$$\mu_0 = d \quad \text{if } \left| |Gb| - \tfrac{d}{2} \right| \leq \varepsilon d \text{ for all } b \neq 0$$

Then graph is an 2ε-expander

Will see $\forall \varepsilon > 0$ is a c s.t. this holds with $d \leq ck$

Coding to send message in $\{0,1\}^m$, transmit $\{0,1\}^n$ $n > m$.

Parity bit $b_1 .. b_m \in \{0,1\}$ append $b_{m+1} = \sum_{i=1}^{m} b_i \bmod 2$

Can now detect one error

But, can't figure out where it is

1-error correction: Hamming Code.

will transmit b_3, b_5, b_6, b_7 e.g. 1 0 1 0

parity bits $b_1 = b_3 + b_5 + b_7$ 1

$b_2 = b_3 + b_6 + b_7$ 0

$b_4 = b_5 + b_6 + b_7$ 1

these satisfy

$$\underbrace{\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}}_{M} \begin{pmatrix} b_1 \\ \vdots \\ b_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

If one bit flipped, to create c, say $c_6 = 0$

then $Mc = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ – the column for bit 6.

and is 6 in binary. So, find location of one error.

Code is a mapping $C: \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^n$ $\quad n > m$

$C(b)$ is a codeword

rate $r = \frac{m}{n}$

Hamming $\mathrm{dist}(c_1, c_2) = |c_1 - c_2|$

minimum distance is $\min_{c_1 \neq c_2} \mathrm{dist}(c_1, c_2) = d$

Can correct up to $d/2$ errors.

If $\mathrm{dist}(c_1, r) < \frac{d}{2}$, then for all $\tilde{c}$

$d \leq \mathrm{dist}(c_1 \tilde{c}) \leq \mathrm{dist}(c_1 r) + \mathrm{dist}(r, \tilde{c}) < \frac{d}{2} + \mathrm{dist}(r, \tilde{c})$

$\Rightarrow \mathrm{dist}(r, \tilde{c}) > \frac{d}{2}$

minimum relative distance $\delta = \frac{d}{n}$

Sequence of codes, $C_1, C_2, \dots,$ is asymptotically good if

$r(C_i) \geq r > 0, \quad \delta(C_i) \geq \delta > 0 \quad \forall i$

$n(C_i)$ should grow.

Linear code: $C(b) = Gb$, for some $G \in \mathbb{F}_2^{n \times m}$

As $G(b_1 + b_2) = Gb_1 + Gb_2 = Gb_1 - Gb_2 \pmod 2$

c_1, c_2 codewords $\Rightarrow$ $c_1 - c_2$ a codeword

min dist $= \min_{b \neq 0} |Gb|$

$C_G \stackrel{\text{def}}{=} \{ C(b) : b \in \mathbb{F}_2^m \}$

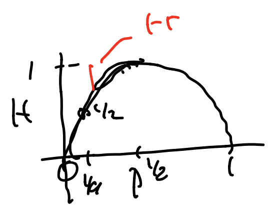
Will see a random G is good.

<u>Lem</u> $\Pr[C_G \text{ has min dist} \geq d] \geq 1 - \frac{2^m}{2^n} \sum_{i=0}^{d} \binom{n}{i}$

<u>proof</u> For G random, Gb is random for every $b \neq 0$

$\Pr[|Gb| = i] = \frac{\binom{n}{i}}{2^n}$ $\Pr[|Gb| \leq d] = \sum_{i=0}^{d} \frac{\binom{n}{i}}{2^n}$

$\Pr[\exists b \neq 0 \text{ s.t. } |Gb| \leq d] \leq 2^m \sum_{i=0}^{d} \frac{\binom{n}{i}}{2^n}$



Analysis. Let $H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$

$\binom{n}{pn} \approx 2^{nH(p)}$

And, for $\beta > H(\delta)$ $\frac{1}{2^{\beta n}} \sum_{i=0}^{\delta n} \binom{n}{i} \underset{n}{\to} 0$

So $\frac{2^{rn}}{2^n} \sum_{i=0}^{\delta n} \binom{n}{i} \to 0$ if $(1-r) > H(\delta)$ $H(\delta)$

That is, if choose $G \in \mathbb{F}_2^{n \times rn}$ at random,
expect min rel dist δ where $H(\delta) \sim 1-r$

$r = \frac{1}{2}, \ \delta \approx \frac{1}{9}$

For $\delta \approx \frac{1}{2}$, r is small but > 0.

For generalized hypercube also need max rel dist,
only a factor 2 on probability $\to$ negligible.

Constructions?

Reed-Solomon is over $\mathbb{F}_p$ - numbers modulo a prime.

message is $f_1 \dots f_m$ encode by
setting $Q(x) = \sum_{i=0}^{p-1} x^i f_{i-1}$ for $x \in \mathbb{F}_p$

transmit $Q(0), Q(1), \dots, Q(p-1)$ so $n = p$

<u>Lem</u> If Q has degree $\leq m-1$ and is 0 at m field elements, then it is 0.

Thm Min dist of RS code is $\geq p-m$

proof let Q^1 and Q^2 be two polys of degree $\leq m$.

So is $Q \stackrel{\text{def}}{=} Q^1 - Q^2$

If $Q^1 \neq Q^2$ then Q is non-zero.

So, Q is zero at most m times,

and $|Q^1 - Q^2| = \text{dist}(Q^1, Q^2) \geq p-m$.

But, This is not over $\mathbb{F}_2$.

Forney: Choose $C^{\text{inner}}: \mathbb{F}_p \to \mathbb{F}_2^{\lceil \log_2 p \rceil} \xrightarrow[\text{code}]{} \mathbb{F}_2^{\ell}$

s.t. $2^{\ell} \geq p$

If min dist of $C^{\text{inner}} > d$,

min dist of whole $> d(p-m)$,

How get C^{inner}?

At random?

By brute search.

Justesen: use all.