AGENDA

1. Plotkin + Singleton bounds
2. Reed Solomon Codes!
3. Dual view of RS Codes
   + more algebra!

○ Recall from last time:
  We took some limits, let n get big, and ended up with:

Some questions.

QUESTION

Are there families of codes that beat the GV bound?

ANSWER 1: Yes. For \( q \geq 49 \),

"Algebraic Geometry Codes"
beat the GV bound.

ANSWER 2: ???

For binary codes, we don't know.

OPEN PROBLEM!

QUESTION

Can we find explicit constructions of families of codes that meet the GV bound?

ANSWER 1. For large alphabets, yes.
(We'll see soon)

ANSWER 2. ???

For binary codes, recent work of [Ta-Shma 2017] gives something close in a very particular parameter regime... but in general, OPEN PROBLEM!
Singleton & Plotkin bounds

Let's try to narrow down that region a little bit.

**THM. [Singleton Bound]** If $C$ is an $(n, k, d)_q$ code, then $k \leq n - d + 1$.

**Proof.** For $c \in C$, consider throwing out the last $d - 1$ coordinates:

$$C = \{ (x_1, x_2, \ldots, x_{n-d+1}, x_{n-d+2}, \ldots, x_n) : (x_1, x_2, \ldots, x_{n-d+1}) \in \Sigma^{n-d+1} \}$$

Consider $\tilde{C} = \{ \varphi(c) : c \in C \}$, so $\tilde{C} \subseteq \Sigma^{n-d+1}$

**CLAIM 1:** $|C| = |\tilde{C}|$ \[\Rightarrow\] If not, then $\exists c, c' \text{ s.t. } \varphi(c) = \varphi(c')$. But then $\Delta(c, c') \leq d - 1$.

**CLAIM 2:** $|\tilde{C}| \leq q^{n-d+1}$ \[\Rightarrow\] Since $\tilde{C} \subseteq \Sigma^{n-d+1}$

Thus, $|C| \leq q^{n-d+1} \Rightarrow q^k \leq q^{n-d+1} \Rightarrow k \leq n - d + 1$

**Note** For $q = 2$, the Singleton bound is WORSE than the Hamming bound. However, (a) it's simpler, and (b) as $q \to \infty$ we'll get something better.
The GV bound only works up to \( d/n \leq 1 - \frac{1}{q} \). Is this necessary? Turns out, yes, at least asymptotically.

**THM [Plotkin Bound]**

Let \( C \) be a \((n, k, d)\) code.

(a) If \( d = (1 - \frac{1}{q}) n \), then \( |C| \leq 2q^n \).

(b) If \( d > (1 - \frac{1}{q}) n \), then \( |C| \leq \frac{d}{d - (1 - \frac{1}{q}) n} \).

Notice that either (a) or (b) imply \( R \to 0 \) as \( n \to \infty \). Thus, in order to have a constant-rate code, we should have \( d < (1 - \frac{1}{q}) n \).

We'll omit the proof of the Plotkin bound in class—Check out ESSENTIAL CODING THEORY §4.4 for a proof.

**Cor.** Let \( C \) be a family of codes of rate \( R \) and distance \( \delta < 1 - \frac{1}{q} \). Then:

\[
R \leq 1 - \left( \frac{q}{q-1} \right) \delta + o(1)
\]

**Proof.** (Assuming the Plotkin bound)

Choose \( n' = \left\lfloor \frac{d q^{n'}}{q-1} \right\rfloor - 1 \). For all \( x \in \Sigma^{n-n'} \), define

\[
C_x = \left\{ (c_{n-n'+1}, \ldots, c_n) \mid \exists c \in C \text{ with } (c_1, \ldots, c_{n-n'}) = x \right\}
\]

= the set of ENDS of codewords that BEGIN with \( x \).

Now \( C_x \) has distance \( \geq d \), block length \( n' < (1 - \frac{1}{q})d \).

Applying the Plotkin bound, \( |C_x| \leq \frac{qd}{qd - (q-1)n'} \leq qd \).

Notice that \( n' < \frac{d q^{n'}}{q-1} \), so \( d > (1 - \frac{1}{q}) n' \). This will be useful.

Here, we use the fact that \( qd - (q-1)n' \) is an integer \( > 0 \), so in particular it is \( \geq 1 \).
proof ctd.

But then

\[ |C| = \sum_{x \in \Sigma^{n-n'}} |C_x| \leq q^{n-n'} \cdot \varphi d \]

\[ = q^0 \left( n - \frac{qd}{q-1} + 1 \right) \varphi d \]

\[ = \exp_q \left( n - \frac{qd}{q-1} + o(n) \right) \]

\[ = \exp_q \left( n \left( 1 - \delta \left( \frac{d}{q-1} \right) + o(1) \right) \right) \]

So \( R \leq 1 - \left( \frac{d}{q-1} \right) s + o(1) \), as desired.

Did we make progress? Yes! We narrowed down the yellow region a bit.

For \( q = 2 \):

Note: There are bounds better than Hamming-A-Plotkin, but we won't cover them in this course.

**Fun exercise:** What happens to this picture as \( q \to \infty \)?
2 REED-SOLOMON CODES.

Notice that for any fixed $q$, the Plotkin bound is strictly better than the Singleton bound.

AND YET, today we are going to see Reed-Solomon Codes, which EXACTLY ACHIEVE the SINGLETON BOUND.

(The trick: the alphabet size will be growing with $n$)

We can define polynomials over finite fields, just like we can over IR.

$$f(X) = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \cdots + a_d \cdot X^d$$

$a_i \in \mathbb{F}_q$ $X$ is a variable that we think of as taking values in $\mathbb{F}_q$ $d$ is the DEGREE of the polynomial.

The set of all univariate polynomials w/ coeffs in $\mathbb{F}_q$ is denoted $\mathbb{F}_q[X]$.

FACT. A polynomial $f$ of degree $d$ over $\mathbb{F}_q$ has at most $d$ roots.

"pf". (Sketch). If $f(p) = 0$, then $(X-p) \mid f$. So if $\beta_1, \ldots, \beta_d$ are roots of $f$, then $(X-\beta_1)(X-\beta_2) \cdots (X-\beta_d) \mid f$, a contradiction.

[This proof implicitly uses:

"Thm." Arithmetic over $\mathbb{F}[X]$ behaves like you think it should.

That Theorem is true.]

Note: depending on your background, it's totally normal to use capital $X$ as a variable or it's totally weird. If it's the latter, get over it.
EXAMPLES  Over $F_3$,

\[ f(X) = X^2 - 1 \] has two roots.  \[ f(2) = f(1) = 0 \]

\[ f(X) = X^2 + 2X + 1 \] has one root.  \[ f(2) = 2^2 + 2 \cdot 2 + 1 = 9 = 0 \]

\[ f(X) = X^2 + 1 \] has zero roots.  \[ f(0) = 1, f(1) = 2, f(2) = 5 = 2 \]

Notice that $X^2 + 1$ DOES have a root over $F_2$, so the field matters.

DEF.  A VANDERMONDE MATRIX has the form

\[
V = \begin{bmatrix}
1 & a_1 & a_1^2 & \cdots & a_1^m \\
1 & a_2 & a_2^2 & \cdots & a_2^m \\
1 & a_3 & a_3^2 & \cdots & a_3^m \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & a_n & a_n^2 & \cdots & a_n^m 
\end{bmatrix}
\]

for some $a_1, \ldots, a_n \in F_q$.  Aka, $V_{ij} = a_i^{j-1}$.

[Note: I also use "Vandermonde" to refer to the transpose of a matrix of this form.]

FACT.  A square Vandermonde matrix is invertible.

proof 1.  \[ V \cdot \hat{a} = \begin{pmatrix}
\Sigma_i a_i a_1^i \\
\Sigma_i a_i a_2^i \\
\Sigma_i a_i a_3^i \\
\Sigma_i a_i a_n^i 
\end{pmatrix} = \begin{pmatrix}
f(a_1) \\
f(a_2) \\
f(a_3) \\
f(a_n)
\end{pmatrix} \]

if \[ f(X) = a_0 + a_1 X + \cdots + a_n X^n \].

Since $f$ is a nonzero polynomial of degree $\leq n-1$, it doesn’t have $n$ roots, so $V \cdot \hat{a} \neq 0$ for all nonzero $\hat{a} \in F_q^n$.  Hence, $\text{Ker}(V) = \emptyset$, so $V$ is invertible.

proof 2.  \[ \det(V) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \Pi_{i=1}^n a_i^{\sigma(i)-1} = \Pi_{1 \leq i < j \leq n} (a_j - a_i) \]

Since $a_i \neq a_j \forall i \neq j$, the RHS has no zero factors and so is nonzero.  [This uses the fact from your HW that $\alpha \beta = 0$ if $\alpha, \beta \neq 0$.]
Any square submatrix of a Vandermonde matrix is invertible.

**Proof.** A square submatrix looks like
\[
\begin{bmatrix}
\alpha_i^j & \alpha_i^{j+1} & \alpha_i^{j+2} & \ldots & \alpha_i^{j+r} \\
\alpha_{i+1}^j & \alpha_{i+1}^{j+1} & \alpha_{i+1}^{j+2} & \ldots & \alpha_{i+1}^{j+r} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{i+r}^j & \alpha_{i+r}^{j+1} & \alpha_{i+r}^{j+2} & \ldots & \alpha_{i+r}^{j+r}
\end{bmatrix} = D \cdot V
\]

These facts about Vandermonde matrices will be useful. First, they imply:

**Theorem.** “Polynomial interpolation works over \( \mathbb{F}_q \).”

Formally, given \((\alpha_i, y_i) \in \mathbb{F}_q \times \mathbb{F}_q\) for \( i = 1, \ldots, d+1\), there is a unique degree polynomial \( f \) so that \( f(\alpha_i) = y_i \) for all \( i \).

**Proof.** If \( f(x) = a_0 + a_1 x + \ldots + a_d x^d \), then the requirements that \( f(\alpha_i) = y_i \) for all \( i \)
are precisely
\[
\begin{bmatrix}
\alpha_i^j & \alpha_i^{j+1} & \alpha_i^{j+2} & \ldots & \alpha_i^{j+r} \\
\alpha_{i+1}^j & \alpha_{i+1}^{j+1} & \alpha_{i+1}^{j+2} & \ldots & \alpha_{i+1}^{j+r} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\alpha_{i+r}^j & \alpha_{i+r}^{j+1} & \alpha_{i+r}^{j+2} & \ldots & \alpha_{i+r}^{j+r}
\end{bmatrix} V = \begin{bmatrix} y_i \end{bmatrix}
\]

Hence, \( a = V^{-1} y \) is the unique solution. (Because linear algebra “works over \( \mathbb{F}_q \).”)

Moreover, the proof implies that we can find \( f \) efficiently.

**FACT.** All functions \( f: \mathbb{F}_q \to \mathbb{F}_q \) are polynomials of degree \( \leq q-1 \).

**Proof.** There are only \( q^2 \) pts in \( \mathbb{F}_q \), so we can interpolate a (unique) degree \( \leq q-1 \) polynomial through any function.

[Second proof: there are \( q^2 \) such functions and also \( q^2 \) such polynomials]
EXAMPLE. \( f(X) = X^8 \) must have some representation as a degree \( \leq 3 \) poly over \( \mathbb{F}_q \). What is it?

**ANSWER:** \( X^8 = X \). This is because \[ \text{FACT: } X^8 = x \forall x \in \mathbb{F}_q. \]

**DEF. (REED-SOLOMON CODES)**

Let \( n \geq k \), \( q \geq n \). The REED-SOLOMON CODE of dimension \( k \) over \( \mathbb{F}_q \), with evaluation points \( \alpha = (\alpha_1, \ldots, \alpha_n) \), is

\[ \text{RS}_q(\alpha, n, k) = \{ (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathbb{F}_q[X], \deg(f) \leq k - 1 \} \]

**Note:** This definition implies a natural encoding map for RS codes:

\[ x = (x_0, \ldots, x_{k-1}) \mapsto (f_x(\alpha_1), \ldots, f_x(\alpha_n)), \text{ where } f_x(X) = x_0 + x_1X + \ldots + x_{k-1}X^{k-1} \]

[We've been 1-indexing but here it is convenient to zero-index.]

This isn't the ONLY encoding map, but it's the one we will think about for most of the class.

**Prop.** \( \text{RS}_q(\alpha, n, k) \) is a linear code, and the generator matrix is the \( n \times k \) Vandermonde matrix with rows corresponding to \( \alpha_1, \alpha_2, \ldots, \alpha_n \).

**Proof.** Staring \( (\text{if } x \text{ has the coefficients of } f \text{, then } Vf = \left( \begin{array}{c} f(\alpha_1) \\ \vdots \\ f(\alpha_n) \end{array} \right) ) \)

Notice: Since \( V \) has rank \( k \), this implies that \( \dim(\text{RS}(n,k)) = k \).
Prop. The distance of $RS_q(n, k)$ is $d = n - k + 1$.

Proof. Since $RS_q(n, k)$ is linear, $\text{dist}(RS_q(n, k)) = \min_{c \in RS} w(c)$. The minimum weight of any codeword is at least $n-k+1$, since any degree $k-1$ polynomial has at most $k-1$ roots.

Equivalent proof: the follows from the fact that every $k \times k$ minor of the generator matrix is full rank.

Cor. RS codes exactly meet the Singleton Bound.

YAY! OPTIMALITY!! For any $n$ and $k$ we like!

DEF. A linear $(n, k, d)_q$ code with $d = n - k + 1$ (aka, meeting the Singleton bd) is called MAXIMUM DISTANCE SEPARABLE, (MDS)

So, RS codes are MDS. Notice that MDS-ness is equivalent to the property: “every $k \times k$ minor of the generator matrix is full rank,” which we just saw was true for RS codes.

In particular, if $C$ is MDS, then any $k$ positions of $c \in C$ determine all of $c$.

Notice that $q$ must be growing in order to get an MDS code (by the Plotkin bound). How big does $q$ have to be? OPEN QUESTION!

CONJECTURE (“MDS conjecture”). If $k=q$, then $n \leq q+1$, unless $q = 2^k$ and $k=3$ or $k=q-1$, in which case $n \leq q+2$.

aka, RS codes basically have the smallest alphabet size w/ $n=q$. \[\]
③ Dual View of RS Codes

What is the parity-check matrix of an RS code?
We'll need a bit more algebra.

\[ \text{DEF } \mathbb{F}_q^* \text{ is the multiplicative group of nonzero elements in } \mathbb{F}_q. \]

Aka, \( \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\} \) as a set, and I can define multiplication and division everywhere in \( \mathbb{F}_q^* \).

**Example.**
\[ \mathbb{F}_5 = \{0,1,2,3,4\} \mod 5 \text{ equipped w/ } + \text{ and } * \]
\[ \mathbb{F}_5^* = \{1,2,3,4\} \mod 5 \text{ equipped w/ just } * \]

**Fact.** \( \mathbb{F}_q^* \) is CYCLIC, which means there's some \( \gamma \in \mathbb{F}_q^* \) so that
\[ \mathbb{F}_q^* = \{ \gamma, \gamma^2, \gamma^3, \ldots, \gamma^{q-2} \} \]
\( \gamma \) is called a PRIMITIVE ELEMENT of \( \mathbb{F}_q \).

**Example.** 2 is a primitive element of \( \mathbb{F}_5^* \) and
\[ \mathbb{F}_5^* = \{ 2, 2^2=4, 2^3=3, 2^4=1 \} \]
4 is NOT a primitive element, since \( 4^2=1, 4^3=-1, 4^4=1, 4^5=-1, \ldots \)
and we'll never generate 2 or 3 as a power of 4.

**Fun Exercise:**
If you haven't seen this before, play around w/ this and other examples:
What elements of \( \mathbb{F}_p \) are primitive? If an element isn't primitive, what can you say about its ORBIT \( \{ \gamma^i : i=1,2,3, \ldots \} \)?
**FACT/LEMMA.** For any $0 < d < q-1$, \( \sum_{\alpha \in \mathbb{F}_q} \alpha^d = 0 \).

**Proof.** 
\[
\sum_{\alpha \in \mathbb{F}_q} \alpha^d = \sum_{\alpha \in \mathbb{F}_q} \alpha^d
\]

For any $x \neq 1$, 

\[
(l-x) \cdot (\sum_{i=0}^{n-1} x^i) = 1 - x^n,
\]

and so 
\[
\sum_{i=0}^{n-1} x^i = \frac{1 - x^n}{l - x}
\]

for any $n$. Apply this with $x = \gamma^d$.

Now we can answer our question about the parity-check matrix of RS codes.

**Prop.** Let $n = q-1$, and let \( \gamma \) be a primitive element of \( \mathbb{F}_q \).

\[
\text{RS}_q((\gamma^0, \gamma^1, \gamma^2, ..., \gamma^{n-1}), n, k)
\]

\[
= \left\{ (c_0, c_1, ..., c_{n-1}) \in \mathbb{F}_q^n : c(\gamma^j) = 0 \text{ for } j = 1, 2, ..., n-k \right\}
\]

where \( c(x) = \sum_{i=0}^{n-1} c_i \cdot x^i \).

**Cor.** The parity check matrix of \( \text{RS}_q((\gamma^0, ..., \gamma^{n-1}), n, k) \) is

\[
H = \begin{bmatrix}
1 & \gamma & \gamma^2 & \cdots & \gamma^{n-1} \\
1 & \gamma^2 & \gamma^4 & \cdots & \gamma^{2(n-1)} \\
\vdots & & \ddots & \ddots & \vdots \\
1 & \gamma^{n-k} & \gamma^{2(n-k)} & \cdots & \gamma^{(n-k)(n-1)}
\end{bmatrix} \in \mathbb{F}_q^{(n-k) \times n}
\]
Proof of PROP. It suffices to show that

\[ \begin{pmatrix}
1 & \gamma & \gamma^2 & \cdots & \gamma^{n-k} \\
1 & \gamma^2 & \gamma^4 & \cdots & \gamma^{2(n-k)} \\
\vdots & & & & \ddots \\
1 & \gamma^{n-k} & \gamma^{2(n-k)} & \cdots & \gamma^{(n-k)(n-k)}
\end{pmatrix} = 0 \]

So let's just consider the \((i,j)\) entry of the product. This is

\[ \begin{pmatrix}
\gamma^i & \gamma^{2i} & \gamma^{3i} & \cdots & \gamma^{(n-1)i}
\end{pmatrix} \cdot \begin{pmatrix}
\gamma^j \\
\gamma^{2j} \\
\gamma^{3j} \\
\vdots \\
\gamma^{(n-1)j}
\end{pmatrix} = \sum_{l=0}^{n-1} \gamma^{li} \cdot \gamma^{lj} \\
= \sum_{l=0}^{n-1} \gamma^{l(i+j)} \\
= \sum_{l=0}^{n-1} (\gamma^q)^{(i+j)} \\
= \sum_{\alpha \in \mathbb{F}_q^*} \alpha^{(i+j)} \\
= 0 \\
\end{pmatrix} 
\]

Since \(i+j \leq (n-k)+k = n = q-1 < q \)

\[ \text{and } i,j > 0 \text{ since } i > 0 \]

Notice: \(RS(n,k)^\perp\) has generator matrix \(H^T\), which again looks a lot like a Vandermonde matrix! So \(RS(n,k)^\perp\) is again (kind of) an RS code!

This particular derivation used the choice of eval. pts heavily. However, a statement like this is true in general.
DEF. A generalized RS code $\text{GRS}_q(\tilde{\alpha}, n, k; \tilde{\beta})$ is

$$\text{GRS}_q(\tilde{\alpha}, n, k; \tilde{\beta}) = \left\{ (x_0 f(x_0), x_1 f(x_1), \ldots, x_n f(x_n)) \mid f \in \mathbb{F}_q[x], \deg(f) \leq k-1 \right\}.$$ 

THM. $\text{GRS}_q(\tilde{\alpha}, n, k; \tilde{\beta})^\perp = \text{GRS}_q(\tilde{\alpha}, n, n-k; \tilde{\delta})$ 
for some $\tilde{\delta} \in (\mathbb{F}_q^*)^n$.

Proof: Fun exercise!

QUESTIONS TO PONDER

1. How would you modify RS codes to make them binary?
2. How would you decode RS codes from errors efficiently? Do you think it's possible?