3. Bounds on Code Parameters

The Singleton Bound

- The *Singleton bound*.

Theorem

For any (n, M, d) code over an alphabet of size q,

$$d \leq n - (\log_q M) + 1 .$$

Proof. Let $\ell = \lceil \log_q M \rceil - 1$. Since $q^\ell < M$, there must be at least two codewords that agree in their first ℓ coordinates. Hence, $d \leq n - \ell$. □

- For linear codes, we have $d \leq n - k + 1$.
- $\mathcal{C} : (n, M, d)$ is called *maximum distance separable (MDS)* if it meets the Singleton bound, namely $d = n - (\log_q M) + 1$.

MDS Code Examples

- Trivial and semi-trivial codes
  - $[n, n, 1]$ whole space $\mathbb{F}_q^n$, $[n, n-1, 2]$ parity code, $[n, 1, n]$ repetition code

- *Normalized generalized Reed-Solomon (RS) codes*
  Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be *distinct* elements of $\mathbb{F}_q$, $n \leq q$. The RS code has PCM

$$H_{\mathrm{RS}} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \ldots & \alpha_n^{n-k-1} \end{pmatrix}.$$

Theorem

Every Reed-Solomon code is MDS.

Proof. Every $(n-k) \times (n-k)$ sub-matrix of H_{RS} has a nonsingular *Vandermonde* form. Hence, every $(n-k)$ columns of H_{RS} are l.i.
$\Longrightarrow d \geq n-k+1$. $\square$

Vandermonde matrix

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_r \\ x_1^2 & x_2^2 & \dots & x_r^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{r-1} & x_2^{r-1} & \dots & x_r^{r-1} \end{pmatrix} .$$

Square matrix, with determinant

$$\det(V) = \prod_{1 \le i < j \le r} (x_j - x_i)$$

Nonzero if and only if all x_i are distinct.

The Sphere-Packing Bound

The *sphere* of center $\mathbf{c}$ and radius t in $\mathbb{F}_q^n$ is the set of vectors at Hamming distance t or less from $\mathbf{c}$. Its *volume* (cardinality) is

$$V_q(n,t) = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i \; .$$

Theorem (The sphere-packing (SP) bound)

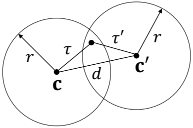
For any (n,M,d) code over $\mathbb{F}_q$,

$$M \cdot V_q(n, \lfloor (d-1)/2 \rfloor) \le q^n \; .$$

Proof. Spheres of radius $t = \lfloor (d-1)/2 \rfloor$ centered at codewords must be disjoint. $\square$

For a linear $[n,k,d]$ code, the bound becomes $V_q(n, \lfloor (d-1)/2 \rfloor) \le q^{n-k}$. For $q=2$,

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} \le 2^{n-k}$$



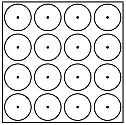
$$2r \ge \tau + \tau' \ge d$$
$$\Longrightarrow r > \lfloor (d-1)/2 \rfloor$$

Perfect Codes

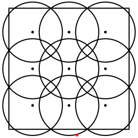
- A code meeting the SP bound is said to be *perfect*.
- Known perfect codes:
  - $[n, n, 1]$ whole space $\mathbb{F}_q^n$,
  - $[n, 1, n]$ repetition code for n odd
  - $\mathcal{H}_{q,m}$, q any GF size, $m \geq 1$
  - the $[23, 12, 7]$ binary and $[11, 6, 5]$ ternary *Golay* codes

In a well-defined sense, this is it!!!
Any perfect code must have parameters identical to one of the above

- Perfect *packing* codes are also perfect *covering codes*



packing



covering

application

The Gilbert-Varshamov bound

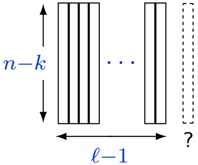
The Singleton and SP bounds set *necessary* conditions on the parameters of a code. The following is a *sufficient* condition:

Theorem (The Gilbert-Varshamov (GV) bound)

There exists an $[n, k, d]$ *code over the field* $\mathbb{F}_q$ *whenever*

$$V_q(n-1, d-2) < q^{n-k}.$$

Proof. Construct, iteratively, an $(n-k) \times n$ PCM where every $d-1$ columns are l.i., starting with an identity matrix, and adding a new column in each iteration. Assume we've gotten $\ell-1$ columns. There are at most $V_q(\ell-1, d-2)$ linear combinations of $d-2$ or fewer of these columns. As long as $V_q(\ell-1, d-2) < q^{n-k}$, we can find a column we can add without creating a dependence of $d-1$ or fewer columns. $\square$



linear comb. of 0 columns: $\binom{\ell-1}{0}(q-1)^0$

linear comb. of 1 columns: $\binom{\ell-1}{1}(q-1)^1$

linear comb. of 2 columns: $\binom{\ell-1}{2}(q-1)^2$

$\vdots$

linear comb. of $d-2$ columns: $\binom{\ell-1}{d-2}(q-1)^{d-2}$

adds up to $V_q(\ell-1, d-2)$

Examples

Consider a binary $[10, 5]$ code. What's the best possible d?

- Sphere packing: $\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} \leq 2^{n-k}$

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{10}{i} \leq 32$$

$\binom{10}{0} = 1,\ \binom{10}{1} = 10,\ \binom{10}{2} = 45 \implies \lfloor (d-1)/2 \rfloor \leq 1 \implies d \leq 4.$

- Gilbert-Varshamov: $\sum_{i=0}^{d-2} \binom{n-1}{i} < 2^{n-k}$; $\exists\, [10, 5, d]$ whenever

$$\sum_{i=0}^{d-2} \binom{9}{i} < 32$$

$\binom{9}{0} = 1,\ \binom{9}{1} = 9,\ \binom{9}{2} = 36 \implies d-2 \leq 1 \implies \exists$ code with $d = 3$.

In fact, there exists a $[10, 5, 4]$ code:

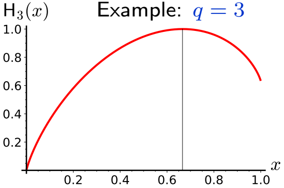
- Start with $[15, 11, 3]$ Hamming code of order 4.
- Extend with overall parity check $\implies$ $[16, 11, 4]$.
- Shorten by 6 $\implies$ $[10, 5, 4]$.

Asymptotic Bounds

- **Definition:** *relative distance* $\delta = d/n$
- We are interested in the behavior of δ and $R = (\log_q M)/n$ as $n \to \infty$.
- Singleton bound: $d \leq n - \lceil \log_q M \rceil + 1 \quad \Longrightarrow \quad \boxed{R \leq 1 - \delta + o(1)}$
- For the SP and GV bounds, we need estimates for $V_q(n, t)$
- **Definition:** *symmetric q-ary entropy function* $\mathsf{H}_q : [0,1] \to [0,1]$

$$\mathsf{H}_q(x) = -x \log_q x - (1-x) \log_q (1-x) + x \log_q (q-1) \ ,$$

  - $\mathsf{H}_q(0) = 0, \ \mathsf{H}_q(1) = \log_q(q-1)$, strictly $\cap$-convex, $\max = 1$ at $x = 1 - 1/q$
  - coincides with $\mathsf{H}(x)$ when $q = 2$



Asymptotic Bounds (II)

Lemma. *For* $0 \le t/n \le 1 - (1/q)$, *we have*

$$\frac{1}{n+1} q^{n\mathsf{H}_q(t/n)} \le V_q(n,t) \le q^{n\mathsf{H}_q(t/n)} .$$

(lower bound holds more generally for $0 \le t \le n$*).*

Theorem (Asymptotic SP bound)

For every $(n, q^{nR}, \delta n)$ *code over* $\mathbb{F}_q$,

$$R \le 1 - \mathsf{H}_q(\delta/2) + o(1) .$$

Theorem (Asymptotic GV bound)

Let n, nR, δn *be positive integers such that* $\delta \in (0, 1-(1/q)]$ *and*

$$R \le 1 - \mathsf{H}_q(\delta) .$$

Then, there exists a linear $[n, nR, \ge\delta n]$ *code over* Fq.

Plot of Asymptotic Bounds