ne u previo

Next: Bounds on the size **Up:** Basic concepts of linear **Previous:** Encoding, Decoding, and Shannon's

Sphere Packing Bound

We start to look at bounds on the size of codes.

Definition 1.11.1 *We define* $B_q(n,d)$ *to be the maximum number of code words in a linear code over* $\mathbb{F}_q^n$ *of length* n *and minimum weight* d*.* $A_q(n,d)$ *is the maximum number of code words in any arbitrary code over* $\mathbb{F}_q^n$ *of length* n *and minimum weight* d*.*

Theorem 1.11.2 ***Sphere Packing Bound***

$$B_q(n,d) \leq A_q(n,d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}$$

where $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Proof. Let C be a code over $\mathbb{F}_q$ (possibly nonlinear) of length n and minimum distance d such that C contains M codewords. By Theorem 1.11.2, the spheres of radius t about these distinct codewords are disjoint. Define

$$\alpha := \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

Then, α is the total number of vectors. Then, $M\alpha$ cannot be bigger than the number q^n of vectors in $\mathbb{F}_q^n$. Hence, we must have

$$M\alpha \leq q^n$$

or

$$B_q(n,d) \leq A_q(n,d) \leq \frac{q^n}{\alpha}$$

which is precisely the sphere packing bound.
Λ

Definition 1.11.3 *Let* C *be a* $[n,k,d]_q$ *code and* $t = \left\lfloor \frac{d-1}{2} \right\rfloor$. *If the spheres of radius* t *are pairwise disjoint and their union is the entire space* $\mathbb{F}_q^n$, *then the code* C *is said to be perfect.*

Example: 1.12.2 in the book.
We know that $\mathcal{H}_{q,r}$ over $\mathbb{F}_q$ is an $[n,k,3]$ code where $n = (q^r - 1)/(q-1)$ and $k = n - r$ $(t = 1)$.

Then,

$$\frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-i)^i} = \frac{q^n}{1+n(q-1)} = \frac{q^n}{q^r} = q^k$$

Hence, the Hamming codes are perfect.

Theorem 1.11.4

(i)
: There exist perfect single error-correcting codes over $\mathbb{F}_q$ which are not linear and all codes have parameters corresponding to Hamming codes.

(ii)
: The only non-trivial perfect multiple error-correcting codes have the same length, number of codewords, and minimum distance as either the $[23,12,7]$ Golay code or the $[11,6,5]$ ternary Golay code.

(iii)
: Any binary possibly nonlinear code with 2^{12} (respectively 3^6) vectors containing the $\mathbf{0}$ vector with length 23 (resp. 11) and minimum distance 7 (resp. 5) is equivalent to the [23,12,7] binary (resp. [11,6,5] ternary) Golay code.

Definition 1.11.5 *The **covering radius**, $\rho(C)$ (linear code) is the smallest integer s so that $\mathbb{F}_q^n$ is the union of spheres with radius s centered at codewords. Equivalently,*

$$\rho(C) = \max_{\mathbf{x}\in\mathbf{F}_q^n} \min_{\mathbf{c}\in C} d(\mathbf{x},\mathbf{c})$$

Note that $\rho(C) \geq t$ and $\rho(C) = t$ if and only if C is perfect

Definition 1.11.6 *We say that C is quasi-perfect if $\rho(C) = t+1$.*

Theorem 1.11.7 *Let C be linear and H a parity check matrix.*

(i)
: $\rho(C)$ is the weight of the coset of largest weight.

(ii)
: $\rho(C)$ is the smallest number such that every nonzero syndrome is a combination of s or fewer columns of H, i.e., there exists a syndrome requiring s columns.

Theorem 1.11.8 *Let $C = [n,k]_q$ code, $\hat{C}$ the extension of C, and C^* be the puncturing of C on any coordinate. Then,*

(i)
: $C = C \oplus C_2 \Leftarrow \rho(C) = \rho(C_1)\rho(C_2)$.

(ii)
: $\rho(C^*)$ is either $\rho(C)$ or $\rho(C)-1$.

(iii)

C) $\rho($ is either $\rho(\mathcal{C})$ or $\rho(\mathcal{C})+1$.

(iv)

If $q=2$, then C) $=\rho(\mathcal{C})+1$.

(v)

Assume $\mathbf{x}$ is a coset leader of $\mathcal{C}$. If $\mathbf{x}' \in \mathbb{F}_q^n$, all of whose nonzero entries agree with $\mathbf{x}$, then $\mathbf{x}'$ is also a coset leader of $\mathcal{C}$. In particular, if there exists a coset with weight s, there exists a coset of any weight less than s.

Proof. Part (iv). Let $\mathbf{x}=(x_1,\ldots,x_n)$ be a coset leader; then define $\mathbf{x}'=(x_1,\ldots,x_n,1)$. It is enough to show that $\mathbf{x}'$ is a coset leader. Let $\mathbf{c}=(c_1,\ldots,c_n)\in\mathcal{C}$ and $\hat{\mathbf{c}}$ be its extension.

If the weight of $\mathbf{c}$ is even, then

$$\mathrm{wt}(\hat{\mathbf{c}}+\mathbf{x}')=\mathrm{wt}(\mathbf{c}+\mathbf{x})+1\geq \mathrm{wt}(\mathbf{x})+1$$

where the last inequality is because $\mathbf{x}$ is a coset leader ($\mathrm{wt}(\mathbf{x})\leq\mathrm{wt}(\mathbf{x}+\mathbf{c})$ for all codewords).

If the weight of $\mathbf{c}$ is odd, then

$$\mathrm{wt}(\hat{\mathbf{c}}+\mathbf{x}')=\mathrm{wt}(\mathbf{c}+\mathbf{x})$$

By Theorem 1.4.3, we get that the $\mathrm{wt}(\mathbf{c}+\mathbf{x})$ is odd if and only if $\mathrm{wt}(\mathbf{x})$ is even. In particular, the $\mathrm{wt}(\mathbf{c}+\mathbf{x})\neq\mathrm{wt}(\mathbf{x})$. Therefore,

$$\mathrm{wt}(\mathbf{c}+\mathbf{x})>\mathrm{wt}(\mathbf{x})$$

and

$$\mathrm{wt}(\hat{\mathbf{c}}+\mathbf{x}')=\mathrm{wt}(\mathbf{c}+\mathbf{x})\geq \mathrm{wt}(\mathbf{x})+1$$

Thus, the

$$\mathrm{wt}(\mathbf{x}')=\mathrm{wt}(\mathbf{x})+1\leq\mathrm{wt}(\hat{\mathbf{c}}+\mathbf{x}')$$

for all C $\hat{\mathbf{c}}\in\hat{}$. Hence, $\mathbf{x}'$ is a coset leader. Λ

Example 1.12.7: Let $\mathcal{C}$ be generated by $G=[1,1,2]$. Then,

$$\mathcal{C}=\{000,112,221\}$$

$d=3,\ t=1$.

$$|B_1(\mathbf{c})|=\sum_0^1\binom{3}{i}2^i=1+6=7$$

However, let $(x_1, x_2, x_3) \in \mathbb{F}_3^3$. Note that each vector is less than two away from an element of $\mathcal{C}$, so $\rho(\mathcal{C}) = 2$.

Now, let's consider the extension of $\mathcal{C}$, CL. This is generated by $\hat{G} = [1122]$:

$$\mathcal{C} = \{0000, 1122, 2211\}$$

Here, $d = 4$ and $t = 1$. We can tell that C) ¿ 1 $\rho($ because $\rho(\mathcal{C}) = 2$. Suppose that (x_1, x_2, x_3, x_4) is not within 2 of 0000 and 1122. By exhaustion, we can see that this cannot happen.

Wednesday, 6-15-2005:

---

ne: u previo

Next: Bounds on the size **Up:** Basic concepts of linear **Previous:** Encoding, Decoding, and Shannon's
Brian Bockelman 2005-06-29