Weights of Binary Linear Code

I was looking at this problem related to coding theory: How do we know a linear code have even weight?

Can anyone explain how we know either all codewords have even weight or half the codewords have even weight and half have odd weight? This fact seems to just be stated without being proven...

(coding-theory)

edited Apr 13 at 12:19 Community ♦ 1

asked Mar 17 '15 at 23:09 VMars 1 2

Lemma: Let $q \in \mathbb{P}$ and let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. All words in $\mathcal{C}$ start with 0 or exactly $\frac{1}{q}$ words of $\mathcal{C}$ start with zero. Prove this lemma and try to use it. – Git Gud Mar 17 '15 at 23:17

I'm not sure where to go with proving the lemma... And if $q = 2$ then that would show either all have even weight or half have odd weight assuming the weight is determined by the starting value. But why would starting with 0 mean the code word is even? – VMars Mar 17 '15 at 23:31

Extend $\mathcal{C}$ to $\overline{\mathcal{C}} := \{1\mathbf{c}\colon \mathbf{c} \in \mathcal{C} \wedge \mathbf{w}_H(\mathbf{c}) \text{ is odd}\} \cup \{0\mathbf{c}\colon \mathbf{c} \in \mathcal{C} \wedge \mathbf{w}_H(\mathbf{c}) \text{ is even}\}$ and use the lemma on $\overline{\mathcal{C}}$. – Git Gud Mar 17 '15 at 23:37

That theorem you mention doesn't seem to say much. Suppose not all words have even weight, then there is at least one with odd weight. Therefore not all words of $\overline{\mathcal{C}}$ start with 0. Use the lemma and proceed. – Git Gud Mar 17 '15 at 23:57

I'm not sure I'm understanding but I think I may have read something that helps. I found a theorem which says for an [n, k] code C, either C is only a set of even-like codewords or the set of even-like codewords is an [n, k-1] subcode of C. So it would make sense that exactly half the words are of odd weight if $n = 2 * (k - 1)$, correct? – VMars Mar 18 '15 at 0:00

|

1 Answer

Since the discussion in the comments between @GitGud and the OP seems to converging far too slowly to a solution, and since I wrote the answer wherein the statement in question occurred, here goes with a few hints for a different approach which will, along the way force you to learn some useful facts about binary vectors.

Suppose $\mathcal{C}$ denotes a linear binary code. Partition $\mathcal{C}$ into two subsets $\mathcal{C}_0$ and $\mathcal{C}_1$ consisting respectively of all the codewords of even Hamming weight and all the codewords of odd Hamming weight.

- Show that for *every* linear binary code, $\mathcal{C}_0$ is a non-empty set. Hint: find a codeword of even weight in $\mathcal{C}$. (Subhint: 0 is an *even* integer).
- Explain why if $\mathcal{C}_1$ is an empty set, then we have proved part of the statement in question.

Digression:

- Show that the sum of two binary vectors of even Hamming weight is a vector of even Hamming weight.
- Show that the sum of two binary vectors of *odd* Hamming weight is *also* a vector of *even* Hamming weight.
- Show that the sum of a binary vector of odd Hamming weight and a binary vector of even Hamming weight is a vector of odd Hamming weight.

End of digression

Suppose that $\mathcal{C}_1$ is *non-empty* and let x denote a fixed element of $\mathcal{C}_1$.

- Show that $x + \mathcal{C}_0 = \{z\colon z = x + y, y \in \mathcal{C}_0\}$ is a collection of $|\mathcal{C}_0|$ distinct vectors, all of which have odd Hamming weight. Argue that $x + \mathcal{C}_0 \subset \mathcal{C}_1$ and so it must be that $|\mathcal{C}_1| \geq |\mathcal{C}_0|$.
- Show that $x + \mathcal{C}_1 = \{u\colon u = x + v, v \in \mathcal{C}_1\}$ is a collection of $|\mathcal{C}_1|$ distinct vectors all of which have even Hamming weight. Argue that $x + \mathcal{C}_1 \subset \mathcal{C}_0$ and hence $|\mathcal{C}_1| \leq |\mathcal{C}_0|$.

Conclude, if you dare, that either $\mathcal{C}_1 = \emptyset$ and so all the codewords in $\mathcal{C}$ have even Hamming weight, **or** that $\mathcal{C}$ contains codewords of even Hamming weight as well as odd Hamming weight and that

$$|\mathcal{C}_1| = |\mathcal{C}_0| = \frac{1}{2}|\mathcal{C}|.$$

edited Mar 20 '15 at 17:05

answered Mar 19 '15 at 16:36 Dilip Sarwate 16.8k 1 20 51