Verification of my Galois Facts PhL 1.26.13

I wrote this so long ago, I have no idea where I got these Facts from. The folder of 1991 shows a WP scan and a Rhee scan, but they are pretty small. Some Facts I don't worry about, but some I do. I will try to accumulate here web support for some of my more dubious Facts.

****

Fact 4: The minimum distance d of a code is equal to the minimum number of columns of the matrix H which are linearly dependent. (7.35)

www.cs.toronto.edu/~radford/csc310.S04/week11a.pdf

Finding Minimum Distance From a Parity-Check Matrix

We can find the minimum distance of a linear code from a parity-check matrix for it, H.

The minimum distance is equal to the smallest number of linearly-dependent columns of H.

Why? A vector $\mathbf{u}$ is a codeword iff $\mathbf{u}H^T = \mathbf{0}$. If d columns of H are linearly dependent, let $\mathbf{u}$ have 1s in those positions, and 0s elsewhere. This $\mathbf{u}$ is a codeword of weight d. And if there were any codeword of weight less than d, the 1s in that codeword would identify a set of less than d linearly-dependent columns of H.

Special cases:

- If H has a column of all zeros, then $d = 1$.
- If H has two identical columns, then $d \leq 2$.
- For binary codes, if all columns are distinct and non-zero, then $d \geq 3$.

If a column is all zeros, then you can write $\alpha \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0$ and in this one column would be called linearly dependent by my definition. I say : For example, three columns C_1, C_3 and C_6 are linearly dependent if $\alpha C_1 + \beta C_3 + \gamma C_6 = 0$ for some non-zero α,β,γ. So if only one term, then you have your d = 1.

So I agree: if H has a column of all zeros, then d = 1.

****