In LDPC decoders, the Lemma:

$$P_{even}^{m} = \frac{1}{2} + \frac{1}{2}\prod_{i=1}^{m}(1-2p_i) \tag{1}$$

is used to determine the probability that in a sequence of $m$ bits, an even number of bits are equal to 1, given the probability of bit $i$ being 1 is $p_i$. A proof is provided in [1], however the introductory paper [2] suggests using induction which is the approach taken here.

For single bit $m = 1$ case, $bit_1 = 0$ is the only outcome with an even number (zero) of bits set to 1, therefore $P_{even}^{1} = prob(bit_1 = 0) = 1 - p_1$. Expanding (1) for $m = 1$ gives the same result, proving the Lemma for $m = 1$.

Now consider the case of a sequence of $m$ bits followed by one additional bit $m + 1$. $P_{even}^{m+1}$ will occur if there is a string of $m$ bits with an even number of ones followed by $bit_{m+1} = 0$, or a string of $m$ bits with an odd number of ones followed by $bit_{m+1} = 1$:

$$\begin{aligned} P_{even}^{m+1} &= P_{even}^{m}(1-p_{m+1}) + (1-P_{even}^{m})p_{m+1} \\ &= P_{even}^{m}(1-2p_{m+1}) + p_{m+1} \end{aligned} \tag{2}$$

Expanding (1) for $m + 1$, and noting that $\frac{1}{2}\prod_{i=1}^{m}(1-2p_i) = P_{even}^{m} - \frac{1}{2}$:

$$\begin{aligned} P_{even}^{m+1} &= \frac{1}{2} + \frac{1}{2}((1-2p_1)...(1-2p_m)(1-2p_{m+1})) \\ &= \frac{1}{2} + \frac{1}{2}\prod_{i=1}^{m}(1-2p_i)(1-2p_{m+1}) \\ &= \frac{1}{2} + (P_{even}^{m} - \frac{1}{2})(1-2p_{m+1}) \\ &= P_{even}^{m}(1-2p_{m+1}) + p_{m+1} \end{aligned} \tag{3}$$

which agrees with (2), proving that (1) is correct for $m + 1$ bits, given it is correct for $m$ bits. Combined with the $m = 1$ case this proves the Lemma for all $m$.

# References


[1] Robert G Gallager. Low-density parity-check, 1963.

[2] William E Ryan et al. An introduction to ldpc codes. *CRC Handbook for Coding and Signal Processing for Recording Systems*, 5(2):1–23, 2004.