Details for Hamming(68,60) Code

(In support of comments #611 and #612 against D1.0)

Kechao Huang
Huawei

Supporters

Xiang He, Huawei

Sridhar Ramesh, Maxlinear

Matt Brown, Alphawave Semi

Arnon Loewenthal, Alphawave Semi

Vasudevan Parthasarathy, Broadcom

Jamal Riani, Marvell

Zvi Rechtman, Nvidia

Introduction

- Comment #611 submitted by author to include details on the construction process and parity-check matrix of the adopted Hamming(68,60) code in sub-clause “177.4.4 Inner FEC encode”.

- Comment #612 to correct the terminology of Generator Matrix.

Cl **177** *SC* **177.4.4** *P* **253** *L* **48** # 611

Huang, Kechao Huawei Technologies Co., Ltd.

Comment Type **T** *Comment Status* **X**

The systematic Hamming code is most naturally defined in terms of its parity-check matrix, as pointed out in many textbooks and standard documents. One famous example is the systematic double-extended Hamming(128,119) code in OIF-400ZR and ITU-T G.709.3.

SuggestedRemedy

Suggest to include the construction process and parity-check matrix of the adopted Hamming(68,60) code to enhance the completeness of the document. A Supporting Presentation will be provided.

Cl **177** *SC* **177.4.4** *P* **253** *L* **48** # 612

Huang, Kechao Huawei Technologies Co., Ltd.

Comment Type **T** *Comment Status* **X**

"The generation matrix G(60,8) for the Hamming(68,60) encoder is given in
Table 177–1" is not accurate. The generation matrix for the Hamming(68,60) should be with 60 rows and 68 columns, where the most-left 60 columns is the indentity matrix.

SuggestedRemedy

Suggest to change the sentence to "The generator matrix of the Hamming(68,60) code is G=[I_60 ; G_(60×8)],where I_60 is the 60×60 identity matrix, and G_(60×8) is a 60×8 matrix used to generate the 8 parity bits given in
Table 177–1."

Introduction (Cont'd)

- For a linear (n,k) code, each k-bit message $\boldsymbol{u}$ is encoded into a n-bit codeword $\boldsymbol{c}$ by a $k \times n$ generator matrix $\boldsymbol{G}$

$$\boldsymbol{c} = \boldsymbol{u} \cdot \boldsymbol{G}$$

- There exists an $(n-k) \times n$ parity-check matrix $\boldsymbol{H}$ such that an n-bit $\boldsymbol{c}$ is a codeword if and only if

$$\boldsymbol{c} \cdot \boldsymbol{H}^{\boldsymbol{T}} = \boldsymbol{0}$$

- There is a fact that

$$\boldsymbol{G} \cdot \boldsymbol{H}^{\boldsymbol{T}} = \boldsymbol{0}$$

- The systematic Hamming code is most naturally defined in terms of its parity-check matrix
  - Hamming(128,119) in [OIF-400ZR]() and ITU-T G.709.3
  - See *Error Control Coding by S. Lin and D. J. Costello*

The systematic double-extended Hamming code is most naturally defined in terms of its parity-check matrix. Consider the function g which maps an integer $i, 0 \le i \le 127$, to the column vector

$$g(i) = \begin{bmatrix} s_{0,i} \\ s_{1,i} \\ \vdots \\ s_{6,i} \\ s_{7,i} \\ 1 \end{bmatrix},$$

where, $i = 64s_{6,i} + 32s_{5,i} + \cdots + 2s_{1,i} + s_{0,i}$, and

$$s_{7,i} = (s_{0,i} \wedge s_{2,i}) \vee (\overline{S_{0,i}} \wedge \overline{S_{1,i}} \wedge \overline{S_{2,i}}) \vee (s_{0,i} \wedge s_{1,i} \wedge \overline{S_{2,i}}).$$

The parity-check matrix is then a 9×128 binary matrix:

$$H = [g(0){:}\,g(62), g(64){:}\,g(94), g(96){:}\,g(110), g(112){:}\,g(118), g(120), g(122), g(124), g(63), g(95), g(111), g(119), g(121), g(123), g(125){:}\,g(127)]$$

almost consecutive values

where g(a):g(b) represents [g(a),g(a+1),g(a+2),…,g(b)].

To obtain the encoder matrix G, we calculate

$$P = B[g(0){:}\,g(62), g(64){:}\,g(94), g(96){:}\,g(110), g(112){:}\,g(118), g(120), g(122), g(124)],$$

where:

$$\mathrm{B} = [\, g(63), g(95), g(111), g(119), g(121), g(123), g(125){:}\,g(127)]^{-1}.$$

Finally, the generator matrix of the Hamming code is

$$G = [I; P^T],$$

and a 119-bit message

$$b = [b_0, b_1, \dots, b_{118}]$$

is encoded to the 128-bit code word

$$c = [c_0, c_1, \dots, c_{127}] = bG$$

Hamming(128,119)

- The construction process and parity-check matrix can provide guidance for implementation, especially for decoder design.

Construction process of Hamming(68,60) code

- Consider a single-error-correcting primitive (or narrow-sense) BCH(127,120) code, usually known as Hamming(127,120), with following parity-check matrix

$$\boldsymbol{H}_{7\times 127} = [\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{67}, \alpha^{68}, \ldots, \alpha^{125}, \alpha^{126}]$$

See *Error Control Coding (S. Lin and D. J. Costello)*

- Here, α is a primitive element in Galois field GF(2^7) with primitive polynomial $x^7 + x^3 + 1$. The element α^i in GF(2^7) can be represented as a binary vector of length 7 bits

$$\alpha^i = \begin{bmatrix} s_{0,i} \\ s_{1,i} \\ s_{2,i} \\ s_{3,i} \\ s_{4,i} \\ s_{5,i} \\ s_{6,i} \end{bmatrix}$$

- The corresponding parity-check matrix of the extended Hamming(128,120) code is as follows:

$$\boldsymbol{H}_{8\times 128} = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \ldots & \alpha^{67} & \alpha^{68} & \ldots & \alpha^{125} & \alpha^{126} & 0_{7\times 1} \\ 1 & 1 & 1 & & 1 & 1 & & 1 & 1 & 1 \end{bmatrix}$$

- The Hamming(68,60) code can be obtained by deleting the right-most 60 columns of $\boldsymbol{H}_{8\times 128}$:

$$\boldsymbol{H}_{8\times 68} = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \ldots & \alpha^{67} & \alpha^{68} & \ldots & \alpha^{125} & \alpha^{126} & 0_{7\times 1} \\ 1 & 1 & 1 & & 1 & 1 & & 1 & 1 & 1 \end{bmatrix}$$

Construction process of Hamming(68,60) code (Cont'd)

- The parity-check matrix of the Hamming(68,60) code is

$$\boldsymbol{H}_{8\times 68}=\begin{bmatrix}\alpha^{0} & \alpha^{1} & \alpha^{2} & \dots & \alpha^{67}\\ 1 & 1 & 1 & & 1\end{bmatrix}$$

$$=\left[\begin{array}{cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc:cccccccc}
1&0&0&0&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0&1&1&0&1&1&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1&1&0&0&1&1&1&1&0&1&1&0&1&0&0&0&0&1\\
0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0&1&1&0&1&1&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1&1&0&0&1&1&1&1&0&1&1&0&1&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0&1&1&0&1&1&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1&1&0&0&1&1&1&1&0&1&1&0&1&0&0&0\\
0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0&1&1&0&1&1&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1&1&0&0&1&1&1&1&0&1&1&0&1&0&0&0&0&1&0&1&0&1\\
0&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0&1&1&0&1&1&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1&1&0&0&1&1&1&1&0&1&1&0&1&0&0&0&0&1&0&1&0\\
0&0&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0&1&1&0&1&1&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1&1&0&0&1&1&1&1&0&1&1&0&1&0&0&0&0&1&0&1\\
0&0&0&0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&1&0&1&1&1&0&1&0&1&1&0&1&1&0&0&0&0&0&1&1&0&0&1&1&0&1&0&1&0&0&1&1&1&0&0&1&1&1&1&0&1&1&0&1&0&0&0&0&1&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{array}\right]$$

- To obtain the encoder matrix $\boldsymbol{G}$, we calculate

$$\boldsymbol{P}=\boldsymbol{B}\cdot[g(0),g(1),g(2),\dots,g(58),g(59)]$$

where,

$$\boldsymbol{B}=[g(60),g(61),g(62),g(63),g(64),g(65),g(66),g(67)]^{-1}$$

- Finally, the generator matrix of the Hamming(68,60) code is,

$$\boldsymbol{G}=\left[\boldsymbol{I}_{60}\ ;\ \boldsymbol{G}_{60,8}\right],$$

where $\boldsymbol{I}_{60}$ is the 60×60 identity matrix, and $\boldsymbol{G}_{60,8}=\boldsymbol{P}^{T}$ is a 60×8 matrix to generate the 8 parity bits.

Summary

- Details on the construction and parity-check matrix of the Hamming(68,60) code are provided as an informative part in the specification draft
  - One can have verification by checking $\boldsymbol{G} \cdot \boldsymbol{H}^{\boldsymbol{T}} = \boldsymbol{0}$
  - Generator matrix remains the same
  - The implementer may choose any parity-check matrix satisfying the constraint $\boldsymbol{G}\cdot\boldsymbol{H}^{\boldsymbol{T}} = 0$ for Inner FEC decoder implementation
- Suggest to include the details on Hamming(68,60) code to enhance the completeness of the sub-clause “177.4.4 Inner FEC encode”

Proposed Changes to D1.0

- Change the sentences in sub-clause “177.4.4 Inner FEC encode”, page 253 lines 48-50 to the following text:

*Following the description style of Hamming(128,119) code in OIF-400ZR and ITU-T G.709.3

The systematic Hamming code is most naturally defined in terms of its parity-check matrix. Consider the function g which maps an integer i, $0 \le i \le 67$, to a column of binary vector:

$$g(i) = \begin{bmatrix} \alpha^i \\ 1 \end{bmatrix} = \begin{bmatrix} s_{0,i} \\ s_{1,i} \\ s_{2,i} \\ s_{3,i} \\ s_{4,i} \\ s_{5,i} \\ s_{6,i} \\ 1 \end{bmatrix}$$

where $(s_{0,i}, s_{1,i}, s_{2,i}, s_{3,i}, s_{4,i}, s_{5,i}, s_{6,i})$ is the binary vector corresponding to the element α^i in the Galois field GF(2^7) with primitive polynomial $x^7 + x^3 + 1$. The element α^i can be expressed as a linear combination of $\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ as follows:

$$\alpha^i = s_{0,i} \times \alpha^0 + s_{1,i} \times \alpha^1 + s_{2,i} \times \alpha^2 + s_{3,i} \times \alpha^3 + s_{4,i} \times \alpha^4 + s_{5,i} \times \alpha^5 + s_{6,i} \times \alpha^6$$

Proposed Changes to D1.0 (Cont'd)

The parity-check matrix is then an 8×68 binary matrix

$$\boldsymbol{H}=[\, g(0), g(1), g(2), \ldots, g(66), g(67)]$$

To obtain the encoder matrix $\boldsymbol{G}$, we calculate

$$\boldsymbol{P}=\boldsymbol{B}\cdot[g(0), g(1), g(2), \ldots, g(58), g(59)]$$

where,

$$\boldsymbol{B}=[g(60), g(61), g(62), g(63), g(64), g(65), g(66), g(67)]^{-1}$$

Finally, the generator matrix of the Hamming(68,60) code is

$$\boldsymbol{G} = \left[\boldsymbol{I}_{60} \; ; \; \boldsymbol{G}_{60,8}\right],$$

where $\boldsymbol{I}_{60}$ is the 60×60 identity matrix, and $\boldsymbol{G}_{60,8} = \boldsymbol{P}^{T}$ is a 60×8 matrix given in Table 177–1 used to generate the 8 parity bits. In Table 177–1, the first row is $\boldsymbol{G}_{60,8}(0)$ and the last row is $\boldsymbol{G}_{60,8}(59)$, and within each row the MSB is on the left.

Thank you