Error Correction Coding: Mathematical Methods and Algorithms

Errata for First Printing

May 25, 2007

In the spirit of "error correction," here are some changes to the text. Most of these are minor. Thanks especially to John Crockett, Partho Choudhury, Wang Peng, Charalampos Tsimendidis, David White, Yi-Ching Liao, Han Wei Kwang, Jan Geldmacher, and the ECE 7670 class of Spring 2007 for their good eyes!

1. Inside front cover: The zlog entries were ordered incorrectly. The tables should correctly appear as:

	zlog :		–	–	3	1	6	2	5	4
	log :		–	0	1	3	2	6	4	5
			0	1	α	α^3	α^2	α^6	α^4	α^5
			0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	**0**	×	0	0	0	0	0	0	0	0
1	**1**	+	1	1	2	3	4	5	6	7
α	**2**		2	3	4	6	3	1	7	5
α^3	**3**		3	2	1	5	7	4	1	2
α^2	**4**		4	5	6	7	6	2	5	1
α^6	**5**		5	4	7	6	1	7	3	6
α^4	**6**		6	7	4	5	2	3	2	4
α^5	**7**		7	6	5	4	3	2	1	3

Addition and multiplication table for $GF(2^3)$ generated by $g(x) = 1 + x + x^3$.

	zlog:		–	–	4	1	8	2	10	5	14	3	7	9	13	6	12	11
	log:		–	0	1	4	2	8	5	10	3	14	9	7	6	13	11	12
			0	1	α	α^4	α^2	α^8	α^5	α^{10}	α^3	α^{14}	α^9	α^7	α^6	α^{13}	α^{11}	α^{12}
			0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	×	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	**1**	+	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
α	**2**		2	3	4	6	8	10	12	14	3	1	7	5	11	9	15	13
α^4	**3**		3	2	1	5	12	15	10	9	11	8	13	14	7	4	1	2
α^2	**4**		4	5	6	7	3	7	11	15	6	2	14	10	5	1	13	9
α^8	**5**		5	4	7	6	1	2	13	8	14	11	4	1	9	12	3	6
α^5	**6**		6	7	4	5	2	3	7	1	5	3	9	15	14	8	2	4
α^{10}	**7**		7	6	5	4	3	2	1	6	13	10	3	4	2	5	12	11
α^3	**8**		8	9	10	11	12	13	14	15	12	4	15	7	10	2	9	1
α^{14}	**9**		9	8	11	10	13	12	15	14	1	13	5	12	6	15	7	14
α^9	**10**		10	11	8	9	14	15	12	13	2	3	8	2	1	11	6	12
α^7	**11**		11	10	9	8	15	14	13	12	3	2	1	9	13	6	8	3
α^6	**12**		12	13	14	15	8	9	10	11	4	5	6	7	15	3	4	8
α^{13}	**13**		13	12	15	14	9	8	11	10	5	4	7	6	1	14	10	7
α^{11}	**14**		14	15	12	13	10	11	8	9	6	7	4	5	2	3	11	5
α^{12}	**15**		15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	10

Addition and multiplication table for $GF(2^4)$ generated by $g(x) = 1 + x + x^4$.

2. p. viii: The correct url is: `ftp://ftp.wiley.com/public/sci_tech_med_error_control`.

3. p. viii, footnote: Trademark.
4. p. 18: First displayed equation in section 1.5.3:

$$p(r|s=\sqrt{E_b}) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2\sigma^2}(r-\sqrt{E_b})^2} \qquad p(r|s=-\sqrt{E_b}) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2\sigma^2}(r+\sqrt{E_b})^2}.$$

   (2π in denominators should have square root).
5. p. 38: 6th line after heading "A Trellis Representation": should read "develop a decoding algorithm"
6. p. 62: G3: Write as "... such that $a * b = b * a = e$ ...
7. p. 66: Permutation table in middle of page: bottom left entry of table should be p_7, not d^2.
8. p. 67: Def. 2.8: Change "smallest n such that ..." to "smallest positive n such that ...".
9. p. 70: The definitions 2.13 and 2.14 are are mistaken: one-to-one functions are injective; onto functions are surjective.
10. p. 71: Sentence after Def. 2.17: Should be $\mathbb{Z}_6/H$ instead of $\mathbb{Z}_6/H_0$. (Since $H = H_0$, these are the same, but it is slightly more clear this way.)
11. p. 75: line before def. 2.21: "which is briefly introduced in Section 2.3 and thoroughly developed in Chapter 5.
12. p. 89: Second sentence after Example 3.6: The number of vectors ..." (not codewords)
13. p. 90: Box 3.1, last sentence: "while the inner product is a function $\mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$" ...
14. p. 95: Line before Lemma 3.7: Last symbol should be $\mathbb{F}_2$ instead of $\mathbb{F}_2^n$.
15. p. 121: First item in itemized list in middle of page: "... has a unique minimal-degree, monic polynomial ..." (add the word "-degree,").
16. p. 129: Figure 4.2: The input and output signals should be $a(x)$ and $b(x)$, not $a(D)$ and $b(D)$, to be consistent with the other figures.
17. p. 118: Def. 4.5: Should be "a bijective function $\phi : R \to \mathcal{R}$"
18. p. 162: 8th line from end: should read "the correlation at all other lags is".
19. p. 166: Exercise 4.15, Boxed equation should read:

$$\boxed{1 - x^n = (1-x)(1 + x + x^2 + \cdots + x^{n-1})}$$

20. p. 169, Exercise 4.42(b): should be

$$p(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{p-1} x^{p-1}$$

    (change last term in polynomial).
21. p. 172: Last line of H in (5.1): The element $f_4(3)$ should have been $f_5(3)$.
22. p. 186: Example 5.18, line 1 should read: $a^{p-1} - 1 = 2^6 - 1 = 63$
23. p. 198: Last line of first paragraph: "define α to be a root of g. (Add "a").
24. p. 201: In the proof, should read: "For a prime p and any integer $i \neq 0$ ...
25. p. 204: 2 lines before Thm. 5.23: $GF(q)$ is the splitting field for the polynomial $x^q - x$.
26. p. 206: Sentence before Ex. 5.33: "By induction, it follows that an element $\beta \in GF(q^n)$ lies in the subfield $GF(q)$ if $\beta^{q^n} = \beta$ for any $n \geq 0$."
27. p. 206: Last line: "As an element of the field $GF(q^j)$, ..."
28. p. 207: Sentence after Example 5.34: replace $x^{p^m} - 1$ with $x^{p^m-1} - 1$ (two places).
29. p. 215: 2nd sentence of 5.10: When $n = q^m - 1$, from Theorem 5.22, every nonzero element of $GF(q^m)$ is a root of $x^{q^m-1} - 1$, so

$$x^{q^m-1} - 1 = \prod_{i=0}^{q^m-2} (x - \alpha^i)$$

    ...
30. p. 217: In list of powers of β in example 5.42, should be a comma after β^6.
31. p. 223: In algorithm 5.4, the first program should be `testgcdpoly.cc`.
32. p. 224: 3rd line after "Programming Part": should read class `ModAr`.
33. Last displayed equation on page:

$$\mathbf{0} = \mathbf{m}\begin{bmatrix} h_{i_1} & h_{i_2} & \cdots & h_{i_{n-k}} \end{bmatrix} \stackrel{\triangle}{=} \mathbf{m}\tilde{H}.$$

34. p. 248: First line: "(if there is a non-zero error, it must be 1)." (remove "to").
35. p. 249: 3rd line from bottom: "operations take place in" (add the word "place")
36. p. 250: 4th line of (6.7): Last term should be $X_{\nu-2}X_{\nu-1}X_\nu$.

37. p. 275: Second paragraph of sect. 6.8.2: Let $\Lambda(x) = \prod_{i=1}^{v}(1 - X_i x)$.
38. p. 275: Last equation of page

$$E_j = -\sum_{k=1}^{v} \Lambda_k E_{j-k}.$$

39. p. 285: 3rd line of 5): "`rsencode` is a program." (add "a").
40. p. 286: In second line of equation array after (6.55), place $(-1)^j$ in the summation.
41. p. 297: 3 lines above (7.10). $E_{\alpha^c} = \{\alpha^{i_{v_1+1}}, \cdots, \alpha^{v}\}$ should be $E_{\alpha^c} = \{\alpha^{i_{v_1+1}}, \cdots, \alpha^{i_v}\}$.
42. p. 297: 1st line below equation (7.11): $W_c(x) = \prod_{i \in L_c}(x - \alpha^i)$ should be $W_c(x) = \prod_{i \in E_c}(x - \alpha^i)$.
43. p. 298: 1st line below Example 7.1: "Hereafter we will refer to the $N(x)$ and $W(x)$ as $N_1(x)$ and $W_2(x)$" should be "Hereafter we will refer to the $N(x)$ and $W(x)$ as $N_1(x)$ and $W_1(x)$".
44. p. 300: The line below equation (7.19), $y_{i+1} = r_k g'(\alpha^{(b+k)})\alpha^{b(2-d+k)}$ should be $y_{i+1} = r_k g'(\alpha^{(b+i)})\alpha^{b(2-d+i)}$.
45. p. 333: Sentence after (7.74): "Since $C(v, l)$ is increasing in its second argument ...".
46. p. 334: After (7.82), the text should read:

    It can be shown [230, p. 10-2] that $C(v, mK_\infty - 1) > m^2 K_\infty^2/(2v)$. Then

$$C(v, mK_\infty - 1) > \frac{m^2 K_m^2}{2v} = n\frac{m(m+1)}{2}\left(\frac{m}{m+1}\frac{K_\infty^2}{vn}\right).$$

47. p. 345, last equation of page:

$$\begin{aligned} g_{i,j} &= \Delta\, xf - (D_i xf) f = (D_{r,s} f(x_i, y_i)) xf(x, y) - D_{r,s} xf(x, y)\Big|_{x=x_i, y=y_i} f(x, y) \\ &= x D_{r,s} f(x_i, y_i) - \left[x_i D_{r,s} f(x_i, y_i) + D_{r-1,s} f(x_i, y_i)\right] f(x, y) \qquad \text{(using (7.97))} \\ &= D_{r,s} f(x_i, y_i)(x - x_i) f(x, y) \qquad \text{(since } D_{r-1,s} f(x_i, y_i) = 0\text{)} \\ &= (\text{const})(x - x_i) f(x, y). \end{aligned}$$

48. p. 346: Algorithm 7.6: Line 21 comment should be (for j), and line 22 comment should be (if J).
49. p. 347: In $i = 3$ iteration: Add $\Delta = \alpha^{14}$. In g_0 polynomial, eliminate parenthesis on coefficient α^3 of y.

    In $i = 4$ iteration: Change: $\Delta_1 = \alpha^7$ Add $\Delta = \alpha^{11}$.
50. p. 368: 4th line of reference: "distanceto" should be "distance to."
51. p. 373: In item 1 (about halfway down page), add phrase "Note that each row and column of J_p sums to 0 since each row contains $(p-1)/2$ elements of 1 and $(p-1)/2$ elements of -1, and that $J_p + J_p^T = \mathbf{0}$.
52. p. 374: Matrix equation after proof: (2,2) element of final matrix should contain $U + (J_p - 1)(J_p^T - 1)$. (Add ^{T}.)
53. p. 374: 2nd line up from "Hadamard Codes": should read "$U + (J_p - I)(J_p^T - I) = U + pI - U - J_p - J_P^T + I = (p+1)I$"
54. p. 378: 9th line of proof of Thm. 8.8: change $d((\mathbf{f}, \mathbf{f}'), (\mathbf{f}, \mathbf{f}'))$ to $d((\mathbf{f}, \mathbf{f}), (\mathbf{f}', \mathbf{f}'))$.
55. p. 396: last line of page: change 5 to β^5.
56. p. 398: 2nd to last line of proof: add): "(being both odd powers of ρ).
57. p. 400: 5 lines from bottom: remove) after errors.
58. p. 444: 8th line of proof (after "Now let"): $\boldsymbol{\alpha} = \sum_{b=0}^{J} \lambda_b \alpha_b$.
59. p. 454: 3rd line from bottom: Change [{ to {{.
60. p. 455: last line: should read $\mathbf{c} = \mathbf{m} * gbf^{(j)}$.
61. p. 456: In the first two matrices, all Ls in subscripts of g should be rs.
62. p. 458: In Figure 12.5(b): Arrow leading from state 00 to state 01 (labeled with 0/11) should point from state 01 to state 00.
63. p. 458: Fig 12.5(d): Change label below trellis from $t+3$ and $t+4$ to $t+2$ and $t+3$.
64. p. 459: arrowhead from 6 to 2 is too big.
65. p. 461: 2nd line above 12.2.1: Change "What it the" to "What is the".
66. p. 462: 4th line up from Def. 12.3: Change "code but," to "code, but".
67. P. 481: Final decoding trellis: the output bits on the third and fourth branch should be 10 and 11, respectively, instead of 00 and 10.

68. Page 486: Tables and discussion at top of page:

The $-\log$ probabilities are

$-\log(P(q_t\|a))$ | $q_t =$	00	01	10	11
$a = 1$	3.9120	1.9661	1.0788	0.6931
$a = -1$	0.6931	1.0788	1.966	3.9120

The logarithms of these probabilities can be approximated as integer values by computing a transformation $a(\log P(q_t|a) - b)$. We use

$$-1.619(\log P(q_t|a) - \log P(00|1)),$$

where the factor $a = 1.619$ was found by a simple computer search and b was chosen to make the smallest value 0, resulting in the following metrics:

$a(-\log(P(q_t\|a) - b)$ | $q_t =$	00	01	10	11
$a = 1$	5.211	2.061	0.624	0
$a = -1$	0	0.624	2.061	5.211

which can be rounded to

round $a(-\log(P(q_t\|a) - b)$ | $q_t =$	00	01	10	11
$a = 1$	5	2	1	0
$a = -1$	0	1	2	5

69. p. 494: Figure 12.22(a): line from state 00 to state 01 should have arrow on other end.
70. p. 498: Last line before section 12.5.2:

$$T(D) = \frac{2D^2 - D^{10}}{1 - 5D^2 + 2D^2}.$$

71. p. 503: last line of text: (see Exercise 1.12). (Move parenthesis.)
72. p. 505: Figure 12.27 caption: should be (2,1), not (3,1).
73. p 507: In the $R = 2/3$ table, the $g^{(2,3)}$ element of the $L = 2$, $\nu = 2$ entry should be 4.
74. p. 510: 2nd line from bottom: "are random variables".
75. p. 513: Two displayed equations after (12.45) should be

$$\log_2 P(\tilde{\mathbf{a}}^{(i)}|\tilde{\mathbf{r}}) = \sum_{j=0}^{n_i-1} \left[\log_2 p(\mathbf{r}_j|\mathbf{a}_j^{(i)}) - \log_2 p(\mathbf{r}_j)\right] - \log_2 Rnn_i.$$

Add the logarithms inside the brackets. Similarly add logarithms on the next displayed equation.

76. p. 526: First line of background: "Since both polynomial and systematic rational encoders are "convolutional encoders," they share many attributes."
77. p. 527: Arrow leading to state 4 should have smaller head.
78. p. 532: Ex. 12.24: Remove period after first displayed equation.
79. p. 540: 6th line of first complete paragraph: "Diverge then come back together".
80. p. 541: First line and first equation: replace D_1 with D_7 throughout.

1st line of penultimate paragraph: "schemes that can".

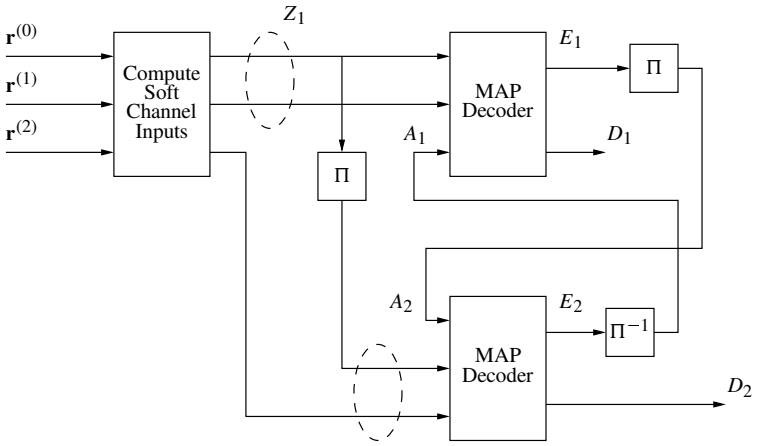
Last line of page, then beginning of 542

81. p. 544: Fig. 13.8: Second output line of convolutional encoder should be c_1 instead of c_0.
82. p. 547 Last equation; p. 548, first equation: d_{free} should have free in roman (not italic) text).
83. p. 553: 6th line from bottom: remove word "values".
84. p. 567: 1st line of "Sources of coding gain": remove extra "to".
85. p. 568: 4th line from bottom: should read "a constellation with a spherical boundary"
86. p. 575: 2nd line from bottom: remove comma after 13.9.
87. p. 577: Two lines above (3.12): Should be $S2_1$, $S3_1$, $S2_2S3_2$, $S2_3S3_3$.
88. p. 577: Last line before Example 13.12: Should be $Y0_nI1_nS2_1S3_1$, $Y0_nI1_nS2_2S3_2$, and $Y0_nI1_nS2_3S3_3$.
89. p. 580: Last sentence of first paragraph should be: "Rotational invariance also appears in ...".
90. p. 587: In figure 14.4(a), place D in each box.
91. p. 589: Third equation: move . outside right square bracket.
92. p. 598. Displayed equation before section 14.4.9: P_t should be G_t.
93. p. 591: Remove semicolon from second boxed equation.

94. p. 598. Displayed equation in section 14.3.9 should be

$$\min \leftrightarrow \text{sum} \qquad \text{sum} \leftrightarrow \text{product}$$

95. p. 600: 5th line of 14.3.11: replace "encoders" with "decoders".
96. p. 602: 6th line: "for a bit x_t is only ...".
97. p. 602: 9th line: "Thus the dependence of the extrinsic ...".
98. p. 610: 2nd line from bottom: $\mathbf{x}_0^{t-1}$ denotes the sequence of inputs from time 0 to time $t-1$.
99. p. 620: Figure 14.13: missing a line from permuter to second MAP decoder:



100. p. 631: Exercise 14.2(h): Lower left corner of box should contain $+1.0$.
101. p. 635: Line 8 of 15.2: "such that $AG = \mathbf{0}$.
102. p. 635: Equation displayed in middle of page

$$H = A_p^{-1}A = \begin{bmatrix} I & -A_2 \end{bmatrix}.$$

(add the minus sign; this makes no difference over $GF(2)$, but was suggested by a reader for clarification for those may not be as familiar with $GF(2)$.)

103. p. 635: 3rd line from bottom: "LDPC generator is regular" should be "LDPC parity check matrix is regular".
104. p.642: First line of proof: should start off with

$$q_n(x) = P(c_n = x|\mathbf{r}, \{z_m = 0, m \in \mathcal{M}_n\}) = \frac{P(c_n = x, \{z_m = 0, m \in \mathcal{M}_n\}|\mathbf{r})}{P(\{z_m = 0, m \in \mathcal{M}_n\}|\mathbf{r})}$$
$$= \ldots$$

105. p. 642: Last equation on page:

$$q_n(x) = \frac{1}{P(\{z_m = 0, m \in \mathcal{M}_n\}|\mathbf{r})} P(c_n = x|r_n) \prod_{m \in \mathcal{M}_n} P(z_m = 0|c_n = x, \mathbf{r}).$$

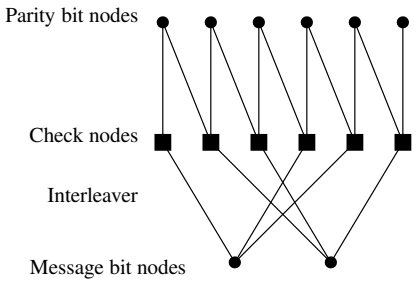
106. p. 653: Second to last paragraph: should read "rate 1/3 code with $(N, K) = (15000, 5000)$"
107. p. 654: Figure 15.8. Caption should read rate 1/2 and rate 1/3.
108. p. 663: Example 15.10: Replace η with ν (3 places).
109. p. 664: Table 15.2: Replace η with ν (12 places).
110. p. 667: Last line of page: remove "is".
111. p. 668: Third sentence of sec. 15.11: "First, if the rows of A are not linearly independent, some rows can be eliminated, which serves to *increase* the rate of the code by decreasing the redundancy."
112. p. 669: Last paragraph: Modify as:

By row and column permutations, we bring the parity check matrix into the form indicated in Figure 15.16, where the upper right corner can be identified as a lower triangular matrix. Because it is obtained only by permutations, the parity check matrix is still sparse. We denote the permutation/decomposition of the parity check matrix as H, where

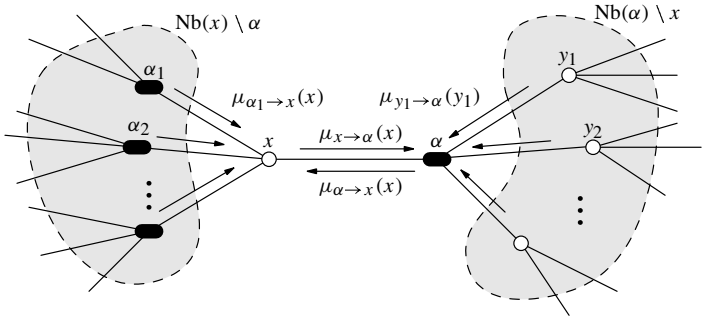
113. p. 671: Second table on page:

$\mathbf{x}_6 = B\mathbf{p}_1$ Multiplication by sparse matrix $O(N)$
$\mathbf{x}_7 = \mathbf{x}_1 + \mathbf{x}_6$ Addition $O(N)$
$\mathbf{p}_2 = T^{-1}\mathbf{x}_7$ Solve $T\mathbf{p}_2 = \mathbf{x}_7$ by backsubstitution

114. p. 673: Fig. 15.19: Figure not correct. Swap the edges from the message bits to the last two nodes.



115. p. 674: 9th line from bottom right: "oriented and column-oriented" (remove "a").
116. p. 675: Programming assignment: Use `A1-3.txt` for a rate 1/3 code. (Something weird in the `A1-4.txt` file!).
117. p. 679: Last sentence 2nd paragraph: should be "squares" not "squared."
118. p. 684: Example 16.4: last sentence, replace (y_1, y_2, y_3) with (y_0, y_1, y_2) (two places).
119. p. 691: 5th line of 16.4.2: "it is more efficient to take...".
120. p. 692. Add α to right filled node:



121. p. 706: Ex. 16.3(a): add period.
122. p. 722: Equation above "Assuming the elements..." should be

$$P(\mathbf{c} \to \mathbf{e} | h_{j,i},\, j = 1, 2, \ldots, m, i = 1, 2, \ldots, n) \le \prod_{j=1}^{m} \exp\bigl(-\boldsymbol{\beta}_j^H D \boldsymbol{\beta}_j E_s / 4N_0\bigr)$$
$$= \prod_{j=1}^{m} \exp\bigl(-\sum_{i=1}^{n} \lambda_i |\beta_{i,j}|^2 E_s / 4N_0\bigr).$$

(remove the extra 4 in the numerator of the last exponent).

123. p. 729: last sentence of Example 17.9: replace "show" with "shows".
124. p. 732: 1st line of 17.6: remove double "cannot".
125. p. 739: Ref. 14: "optimial" should be "optimal".

Errata After Second Printing

1. p. 464: penultimate paragraph: ... where $A(x)$ and $B(x)$ are again polynomial unimodular matrices and $\Gamma(x)$ is diagonal with rational entries $\gamma_i(x) = \alpha_i(x)/\beta_i(x)$, such that $\alpha_i(x)|\alpha_{i+1}(x)$ and $\beta_{i+1}(x)|\beta_i(x)$.

2. p. 59: Ex. 1.22: ... for a cyclic code of length $n = 7$.