Errata

January 18, 2006

Chapter. 6

- p.163 In the Lemma 6.2's proof, see the first line. If $d \equiv 0 \pmod N$, then $\sum_{k=0}^{N-1} \alpha^{i\cdot 0} = N$. $\longrightarrow$ $\sum_{i=0}^{N-1} \alpha^{i\cdot 0} = N$
- p.164 ' Suppose that F_q has characteristic p. Because N is a factor of $q^n - 1$, we have $N \equiv -1 \pmod p$. So, $N^{-1} \equiv -1 \pmod p$...'
  $\longrightarrow$ It's not true because of the following counterexample. If $p = 3$ and $n = 3$, then $13|(3^3 - 1)$ but 13 is not equivalent to $-1 \pmod 3$. Therefore, this paragraph and 2-nd line in Table 6.1 should be modified together. $N \equiv -1 \pmod p$ is right only if $N = q^n - 1$. To cover all the cases of N which is a divisor of $q^n - 1$, the equation (6.6) in page 170 and Table 6.2 in page 172 also need to be modified.
- p.165 In the expansion of a_1, $\sum_{k=0} 6A_k\alpha^{-k} \longrightarrow \sum_{k=0}^{6} A_k\alpha^{-k}$
- p.167 In the equaton (6.5) $Z_N \longrightarrow \mathbb{Z}_N$
- p.178 In the equaton (6.11) $f(x) = \sum_{k=0}^{2^n-1} A_k x^k \longrightarrow f(x) = \sum_{k=1}^{2^n-1} A_k x^k, f(0) = A_0$
- p.179 In the middle paragraph beginning with ' Because there are...', $(2^m)^{\triangle_2(m)} = 2^{m\triangle_2(m)} \longrightarrow (2^m)^{|\triangle_2(m)|} = 2^{m|\triangle_2(m)|}$
- p.186 First line in the Propositon 6.3 $\mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{p^n}$
- p.186 last line; $Tr(\lambda x) \longrightarrow Tr(x)$
- p.187 Example 6.10; $\mathbf{a} = (1110010) \longrightarrow (1110100)$
- p.189 Example 6.11;

$$A_{f,g}(w) = \sum_{i=0}^{7} (-1)^{f(t_i+t_\tau)+g(t_i)}, ...$$

where $t_i + t_\tau$ is reduced modulo 2^3

$$\longrightarrow \quad A_{f,g}(w) = \sum_{i=0}^{7} (-1)^{f(t_{i+\tau})+g(t_i)}, ...$$

where $i + \tau$ is reduced modulo 2^3

- p.190 equation (6.42) $C_f(0) = \sum_{x\in\mathbb{F}_{p^n}} w^{f(x)} \longrightarrow C_f(0) = \sum_{x\in\mathbb{F}_{p^n}} w^{-f(x)}$
- p.193 First line in Proposition 6.5, ' Let $f(x)$ be a function...' $\longrightarrow$ ' Let $f(x)$ and $g(x)$ be functions ...'
- p.197 equation (6.55)

$$(a_0, a_1, a_2, \ldots, a_{N-1}) = (A_0, A_1, A_2, \ldots, A_{N-1})M^{-1} \longrightarrow (a_0, a_1, a_2, \ldots, a_{N-1}) = \frac{1}{N}(A_0, A_1, A_2, \ldots, A_{N-1})M^{-1}$$

- p.199 3-rd line; $\mathbf{a} = (1110010) \longrightarrow (1110100)$
  4-th line; $\mathbf{c} = (1,-1,1,-1,1,1,-1,-1) \longrightarrow (-1,1,1,-1,1,-1,-1)$
  7-th line; $(\hat{f}(0),\hat{f}(1),\hat{f}(\alpha),\ldots,\hat{f}(\alpha^6)) = (1,-1,-1,-1,1,1,-1,1)H \longrightarrow (\hat{f}(0),\hat{f}(1),\hat{f}(\alpha),\ldots,\hat{f}(\alpha^6)) = (1,-1,-1,-1,1,-1,1,1)H$
  10-th line; 2nd element to 8-th element in the second row should be changed to $[-1,1,1,-1,1,-1,-1]$ and other rows(except 1st row) should be changed to its cyclic shifts.

Chapter. 10

- p.325 Second line below the equation (10.4); $\chi(\mathbf{x}) = (w^{x_0},\ldots,w^{x^{v-1}}) \longrightarrow \chi(\mathbf{x}) = (w^{x_0},\ldots,w^{x_{v-1}})$
- p.325 Second to the last line; $F_p \longrightarrow \mathbb{F}_p$
- p.326 (d) in Table 10.1; $w^{d-c} < \mathbf{a},\mathbf{b} > \longrightarrow w^{c-d} < \mathbf{a},\mathbf{b} >$
- p.327 Fourth line; $C_{\mathbf{a},\mathbf{a}^{(d-1)}}(\tau) \longrightarrow C_{\mathbf{a},\mathbf{a}^{(d^{-1})}}(\tau)$
- p.330 Second line from Example 10.3; ' weight of the sequence in S in Example 10.1 ...' $\longrightarrow$ ' weight of the sequence in S in Example 10.2 ...'
- p.357 Fifth line; $f(x_0,x_1,x_2,x_3) = x_0x_1+x_0x_2+x_0x_3+x_1x_2++x_1x_3+x_2x_3+x_2 \longrightarrow f(x_0,x_1,x_2,x_3) = x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_1x_3+x_2x_3+x_2$. Therefore, 7-th line also needs to change.

  Second line in Example 10.13; ' where $y=\eta x, \lambda=\eta^d \in \mathbb{F}_{2^m}^*$...' $\longrightarrow$ ' where $y=\eta x, \lambda=\eta^{-d} \in \mathbb{F}_{2^m}^*$...'

Chapter. 11

- p.385 Second line from **Case 1.**; ' The necessary condition is clear. We only need to show that it is sufficient.' $\longrightarrow$ ' The sufficient condition is clear. We only need to show that it is necessary.'
- p.385 Third line

$$\left.\begin{array}{l} w+z=x+y \\ w+x=y+z \\ w+y=x+y \end{array}\right\} \longrightarrow \left.\begin{array}{l} w+z=x+y \\ w+x=y+z \\ w+y=x+z \end{array}\right\}$$

- p.385 First line in **Case 2.**; ' Assume that the sufficient condition...' $\longrightarrow$ ' Assume that the necessary condition...'