

『格子暗号解読のための数学的基礎』 正誤表

著者名 青野 良範・安田 雅哉

初版 1 刷

No	頁	行	誤	正
1	23	3	成分 $\mu_{[i,j]}$	成分を $\mu_{[i,j]}$
2	25	21	$(b_{\forall \ell}^*, \dots, b_n^*)_R$	これは $m = n$ の場合のみで成立
3	41	6	現在正確の	現在正確な
4	76	アルゴリズム 7、ステップ 15	$b_i \leftarrow v$	$b_i \leftarrow v$ は for 文の外で計算 (つまり、ステップ 16 の直後で計算)
5	105	アルゴリズム 11、ステップ 1	$B_i = \ b_i\ ^2$	$B_i = \ b_i^*\ ^2$ (* が必要)
6	118	16	$S_{[q\beta+1]}$	$S_{[q+1]}$
7	130	1	$x^* \in \mathbb{R}$	$x^* \in \mathbb{R}^n$
8	133	アルゴリズム 14、ステップ 5	$\mu_{[i,n]}$	$\mu_{[n,i]}$
9	138	8	等号	不等号 $\geq$
10	156	図 4.3	$B(j_1, \dots, j_n)$	$B(j_1, \dots, j_k)$
11	158	最終行	$j=0, \dots, T-1$	$j=1, \dots, T$
12	159	図 4.4	図中の 15 か所の $L_{[a,b]}$	$L_{[a,b+1]}$
13	161	6,11	$\Lambda_{[t,0]}$	$\Lambda_{[t,1]}$
14	166	10	区間 $[-2^{-m_i}, 2^{-m_i}]$	区間 $[-2^{-(m_i-1)}, 2^{-(m_i-1)}]$
15	169	13	$2^{(-k+i)/2}$	$2^{(k-i)/2}$
16	180	9, 10	不等号	等号付きの不等号
17	180	14	等号付きの不等号	等号
18	189	6	$\sigma \ v\ \leq \sigma \beta$	$\sigma \sqrt{m} \ v\ \leq \sigma \sqrt{m} \beta$
19	189	7	$\sigma \beta \ll q$	$\sigma \sqrt{m} \beta \ll q$
20	189	注釈 53	$\ e\ \approx \sigma$	$\ e\ \approx \sigma \sqrt{m}$

21	190	注釈 59	5.2 節	5.2.5 項
----	-----	-------	-------	---------