

2019 年度 情報数理特論 B 練習問題 3

学籍番号：_____

氏名：_____

問題の質問や不明な点は、授業終了後またはオフィスアワーを利用して、質問してください。

出題者：幸山 直人
出題日：2019 年 6 月 4 日 (火)

問 1 集合 $\{a, b, c, d\}$ から成る符号について、符号語 $\mathbf{x} = (a, b, c, a, d, a, a, c, c, a, b, b, a, d, d)$ と $\mathbf{y} = (a, c, c, a, a, a, a, c, c, a, b, b, a, b, b)$ のハミング距離を求めなさい。

問 2 α をガロア拡大体 $\text{GF}(2^4)$ の原始多項式 $x^4 + x + 1$ の 1 つの根 (原始元) とするとき、次の (1)~(2) の問いに答えなさい。ヒント: $\alpha^4 = \alpha + 1$, $\alpha^{15} = 1$ 。

(1) テキストの表 2.5 (p.43) に習って、以下のガロア拡大体 $\text{GF}(2^4)$ のべき表現とベクトル表現の表を完成しなさい。

べき表現	展開	ベクトル表現
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3		
α^4		
α^5		
α^6		
α^7		
α^8		
α^9		
α^{10}		
α^{11}		
α^{12}		
α^{13}		
α^{14}	$\alpha^3 + 1$	1001

(2) 次の①～④を計算し、その値を (1) の表のべき表現で答えなさい。

① $\alpha^5 + \alpha^{10} =$

② $\alpha^4 - \alpha^5 =$

③ $\alpha^9 \cdot \alpha^{10} =$

④ $\alpha^7 / \alpha^{14} =$

問 3 α をガロア拡大体 $\text{GF}(2^8)$ の原始多項式 $x^8 + x^4 + x^3 + x^2 + 1$ の 1 つの根 (原始元) とするとき、 $\text{GF}(2^8)$ 上の多項式 $h(x) = \alpha^{122}x^3 + \alpha^2x^2 + \alpha^{15}x + \alpha^{201}$ を多項式 $g(x) = x^2 + \alpha^{167}x + \alpha^{98}$ で割り、剰余 $r(x)$ を求めなさい。ヒント：付録 A のガロア拡大体 $\text{GF}(2^8)$ の表を利用。