840377G 中口 悠輝

No. ・ ・ (　　)

第1回

(1) math05_testの問題2B

1. 束が満たすべき4つの性質である、べき等律、結合律、吸収律をのべよ。

2. 束に分配律 $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$ を仮定すると、双対的な分配律 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$ およびモジュラ律 $A\cup B=B\Rightarrow{}^{\forall}C\ (A\cup C)\cap B=A\cup(C\cap B)$ が得られることを示せ。

1 ・べき等律

$A\cap A=A \quad A\cup A=A$

・交換律

$A\cap B=B\cap A \quad A\cup B=B\cup A$

・結合律

$(A\cap B)\cap C=A\cap(B\cap C) \quad (A\cup B)\cup C=A\cup(B\cup C)$

・吸収律

$A\cup(A\cap B)=A \quad A\cap(A\cup B)=A$

2

$(A\cap B)\cup(A\cap C)$

$=((A\cap B)\cup A)\cap((A\cap B)\cup C)$ 分配律

$=(A\cup(A\cap B))\cap(C\cup(A\cap B))$ 交換律

$=A\cap(C\cup(A\cap B))$ 吸収律

$=A\cap((C\cup A)\cap(C\cup B))$ 分配律

$=(A\cap(C\cup A))\cap(C\cup B)$ 結合律

$=(A\cap(A\cup C))\cap(B\cup C)$ 交換律

$=A\cap(B\cup C)$ 吸収律

$(A\cup C)\cap B$

$=B\cap(A\cup C)$ 交換律

$=(B\cap A)\cup(B\cap C)$ 分配律

$=((A\cup B)\cap A)\cup(B\cap C)$ $A\cup B=B$

$=(A\cap(A\cup B))\cup(B\cap C)$ 交換律

$=A\cup(B\cap C)$ 吸収律

(2)

分配則の補元は一意であることを示せ。

まず、この束では補元がとれる(可補束)とする。即ち：

・最大元 M が存在 $A\cap M=A \quad A\cup M=M$

・最小元 m が存在 $A\cap m=m \quad A\cup m=A$

・相補律 $\exists B \quad A\cup B=M$ かつ $A\cap B=m$ (B:補元

ここで、あるAに対して補元がB, Cと2つとれたとすると、

$B=B\cap M$ 最大元

$=B\cap(A\cup C)$ 相補律

$=(B\cap A)\cup(B\cap C)$ 分配律

$=(A\cap B)\cup(B\cap C)$ 交換律

$=m\cup(B\cap C)$ 相補律

$=(A\cap C)\cup(B\cap C)$ 相補律

$=(C\cap A)\cup(C\cap B)$ 交換律

$=C\cap(A\cup B)$ 分配律

$=C\cap M$ 相補律

$=C$ 最大元

よって、$B=C$ で補元は一意的。
即ち、分配可補束は分配相補束(Boole束)に等しい。

第2回

> 半順序集合 $(L, \leq)$ が任意の2元 a, b に対して $\sup\{a,b\}$, $\inf\{a,b\}$ をもつとき，L 上の2項演算 $\wedge, \vee$ を
> $a \vee b = \sup\{a,b\}$ 　 $a \wedge b = \inf\{a,b\}$
> で定義すると，$(L, \wedge, \vee)$ は束になることを示せ．

$$\begin{cases} \sup\{a,b\} = \min\{x \mid a \leq x \text{ かつ } b \leq x\} \\ \inf\{a,b\} = \max\{x \mid x \leq a \text{ かつ } x \leq b\} \\ \forall x \in X\ \ x \leq \max X,\ \ \forall x \in X\ \ \min X \leq x \end{cases}$$

に注意する．

・べき等律

$a \vee a = \sup\{a, a\} = a$

$a \wedge a = \inf\{a, a\} = a$

（半順序の反射性より）

・交換律

$a \vee b = \sup\{a, b\} = \sup\{b, a\} = b \vee a$

$a \wedge b = \inf\{a, b\} = \inf\{b, a\} = b \wedge a$

（集合の性質より）

・結合律

$(a \vee b) \vee c$

$= \sup\{\sup\{a,b\}, c\}$

$= \sup\{\min\{x \mid a \leq x \text{ かつ } b \leq x\}, c\}$

$= \min\{y \mid \min\{x \mid a \leq x \text{ かつ } b \leq x\} \leq y \text{ かつ } c \leq y\}$

ここで，推移律より

$\min\{x \mid a \leq x \text{ かつ } b \leq x\} \leq y \Leftrightarrow a \leq y \text{ かつ } b \leq y$ なので，

$= \min\{y \mid a \leq y \text{ かつ } b \leq y \text{ かつ } c \leq y\}$

$= \min\{y \mid a \leq y \text{ かつ } \min\{x \mid b \leq x \text{ かつ } c \leq x\} \leq y\}$

$= \min\{y \mid a \leq y \text{ かつ } \sup\{b, c\} \leq y\}$

$= \sup\{a, \sup\{b, c\}\}$

$= a \vee (b \vee c)$

$\wedge$ については，sup を inf に，min を max に，$X \leq Y$ を $Y \leq X$ に書きかえればよい．

・吸収律

$a \vee (a \wedge b)$

$= \sup\{a, a \wedge b\}$

$= \sup\{a, \inf\{a, b\}\}$

$= \min\{y \mid a \leq y \text{ かつ } \max\{x \mid x \leq a \text{ かつ } x \leq b\} \leq y\}$

ここで，$\max\{x \mid x \leq a \text{ かつ } x \leq b\} \leq a$ なので，

$a \leq y$ なら $\max\{x \mid x \leq a \text{ かつ } x \leq b\} \leq y$ であり，

（推移律）

$= \min\{y \mid a \leq y\}$

$= a$

$a \wedge (a \vee b)$ については，sup と inf を，min と max を交換し，$X \leq Y$ を $Y \leq X$ に書きかえればよい．

No.

第3回

以下を示せ。

1, $H(AB) = H(A) + H(B|A)$
2, $I(A;B) = I(B;A)$
3, $H(B|A) \le H(B) \le H(AB)$
4, $0 \le I(A;B) \le H(A)$

①

$H(B|A) = -\sum_{i,j} p(a_i, b_j) \log p(b_j|a_i)$

ここで, $p(b_j|a_i) = \dfrac{p(a_i, b_j)}{p(a_i)}$ より

$= -\sum_{i,j} p(a_i, b_j)(\log p(a_i, b_j) - \log p(a_i))$

今, $H(AB) = -\sum_{i,j} p(a_i, b_j) \log p(a_i, b_j)$
であり また, $-\sum_{i,j} p(a_i, b_j) \log p(a_i)$
$= -\sum_i p(a_i) \log p(a_i) = H(A)$ より

$= H(AB) - H(A)$
$\therefore H(AB) = H(A) + H(B|A)$

②

$I(A;B)$
$= H(A) - H(A|B)$
$= H(A) - (H(AB) - H(B))$
$= H(B) - (H(AB) - H(A))$
$= H(B) - H(B|A)$
$= I(B;A)$

③

$H(A) + H(B|A) = H(AB)$ (∵①)
$\le H(A) + H(B)$
$\therefore H(B|A) \le H(B)$

$H(AB) = H(B) - H(A|B)$ (∵①)
$H(A|B) \ge 0$ より
$H(B) \le H(AB)$

あわせれば,
$H(B|A) \le H(B) \le H(AB)$

④

$I(A;B) = H(A) - H(A|B) \ge 0$
(∵③の $H(A) \ge H(A|B)$ より)

また, $H(A|B) \ge 0$ より
$I(A;B) = H(A) - H(A|B) \le H(A)$

あわせれば, $0 \le I(A;B) \le H(A)$

第4回

正整数列 l_i が Kraftの不等式
$$\sum_i 2^{-l_i} \leq 1$$
を満たすなら，i番目の符号語の符号長が l_i となるような（2元）語頭符号が存在することを示せ．

まず，$l_i = m$ となるような i の個数を α_m とする。
$$(\alpha_m := \#\{ l_i ; l_i = m \})$$
これは，符号長が m であるような符号の数に相当する。

次に，正数列 l_i のうちで最大のものを L とすれば
$$(L = \max_i \{ l_i \})$$
Kraftの不等式は
$$\sum_i 2^{-l_i} = \sum_{m=1}^{L} \alpha_m 2^{-m} \leq 1 \quad \cdots ☆$$
と書きかえられる。

さて，語頭符号の存在を言うには，葉の深さの数を集めると集合 $\{l_i\}$ に一致するような2分木の存在を言えばよい。

証明は符号長に関する帰納法による。

(i) まず，符号長が1である符号は全て深さ1の葉に割当てることができることを示す。

☆の不等式は，Σの和の範囲を m=1 に限っても成立つので，
$$\alpha_1 2^{-1} \leq 1$$
$$\Leftrightarrow \quad \alpha_1 \leq 2$$
これは，符号長が1である符号の数が2以下であるということだが，深さ1の葉は0と1の2つが可能なので，じゅうぶん割当てることができる．

(ii) 次に，符号長が n−1 以下の符号は全て符号長と同じだけの深さの葉に割合てることができているときに，符号長が n の符号を深さ n の葉に割当てることができることを示す。

まず，深さ n で葉になりえる節点がいくつあるのかを考えたい。
本来，深さが n−1 以下のところに葉が全く無ければその数は単純に 2^n であるが，深さが j ($1 \leq j < n$) の葉はその数を1つあたり 2^{n-j} 個減らす。深さが j の葉は α_j 個なので，
$$2^n - \sum_{j=1}^{n-1} \alpha_j 2^{n-j}$$
個だけ深さ n の節点がある。

ここで，☆の不等式は和の範囲を m=1 から m=n までに限っても成立つので，
$$\sum_{m=1}^{n} \alpha_m 2^{-m} \leq 1$$
$$\Leftrightarrow \alpha_m \leq 2^n - \sum_{m=1}^{n-1} \alpha_m 2^{n-m}$$
これは，符号長が n である符号の数が $2^n - \sum_{m=1}^{n-1} \alpha_m 2^{n-m}$ 個以下であるということだが，深さ n の葉は先程 $2^n - \sum_{j=1}^{n-1} \alpha_j 2^{n-j}$ 個可能と分かったので，じゅうぶん割当てることができる．

以上，(i)，(ii) を n が L になるまで続ければ，語頭符号を帰納的に構成できる．

No.

第5回

> (1) ISBNの誤り検出の工夫
> (2) 数字に1つ誤りがあっても検出できることを示せ.
> (3) 2つ以上誤りがあると失敗する例を示せ.
> (4) 1つの誤りを訂正できるか否か.

• 旧ISBN (ISBN-10) について

(1) ISBNは10桁のコードからなり, 最後の1桁が「チェックディジット」と呼ばれる, 誤り検出のために付与された冗長性である。

具体的には「モジュラス11 ウェイト10−2」という計算法により算出される: チェックディジットを除いた9つの数字に左から10, 9, …, 2をかけて和をとり, その11で割った余りを11から引いたものをチェックディジットとする。

(2) ISBNの10桁のコードを左から順に $a_1, a_2, \cdots, a_{10}$ とする。(a_{10}がチェックディジットである。)
以下全て mod 11 で考えると, (1)より

$$a_{10} \equiv 11 - \sum_{i=1}^{9} (11-i) a_i$$

$$\Leftrightarrow \sum_{i=1}^{9} i a_i - a_{10} \equiv 0$$

両辺 $11 a_{10} \equiv 0$ を加えれば,

$$\Leftrightarrow \sum_{i=1}^{10} i a_i \equiv 0 \quad \cdots (*)$$

ここでもし, i番目の文字 a_i を入力しまちがえて $a_i + e$ $(-9 \le e \le 9$ かつ $e \ne 0)$ としてしまうと, 左辺は ie だけ増える。もし $ie \equiv 0$ であれば式(*)は依然として成立ち誤りが検出できないが, mod 11 の 11 は素数なので

$ie \equiv 0 \Leftrightarrow i \equiv 0$ or $e \equiv 0$

これはありえない。
よって, 1文字の誤りであれば必ず検出できる。

(3) i番目の文字 a_i と j番目の文字 a_j を入力しまちがえて各々 $a_i + e_i$, $a_j + e_j$ としてしまうと, $(i \ne j, -9 \le e_i, e_j \le 9$ かつ $e_i^2 + e_j^2 \ne 0)$
式(*)の左辺は $i e_i + j e_j$ だけ増える。しかしこれは 0 と mod 11 で等しくなることがありえる, たとえば

$i = 3$, $e_i = 2$ $j = 5$ $e_j = 1$

つまり3番目の文字を2だけ多く入力しまちがい, 2番目の文字を1だけ多く入力しまちがうと, 依然として(*)式が成立ってしまう, つまり誤った後も同じチェックディジット a_{10} を返してしまう。

(4) 誤りは, 誤った桁数 i と, 誤って数字をいくつ増やしてしまったか e に対し, (*)の左辺を計算すると $ie\ (\ne 0)$ となることで発覚する。

しかし mod 11 で ie が分かっても, そこから i, e を割出すことはできない。例えば

$i = 2, e = 3$ と $i = 5, e = -1$

は mod 11 で同じ ie を与える。つまり, チェックディジットからは「2文字目を3多く入力してしまった」と「5文字目を1少なく入力してしまった」を区別できない。

即ち, 誤りを訂正することはできない。