Mizarによる離散確率の形式化についての考察

岡崎　裕之（信州大学大学院理工学系研究科）
師玉　康成（信州大学工学部）

Mizar

- 本家サイト
  http://mizar.org/
- HTML化ライブラリ
  http://mizar.uwb.edu.pl/version/current/html

Agenda

- Aim:
  Mizarを暗号用途に使えるようにする
  やることが多すぎ

1. 確率
2. 計算量、計算理論
3. 数論など
   素因数分解、楕円曲線、体
4. アルゴリズム
   拡張ユークリド互除法、CRT
5. 分かりやすいやつ
   DES、AES

Agenda

- Aim:
  Mizarを暗号用途に使えるようにする
  離散確率の数え上げに基づく構成法を提案

1. 既存の「確率」 in Mizar 紹介
2. 離散確率の形式定義の提案

   →脱線して、確率変数について

3. 離散確率の形式定義の応用について

   使い方、
   今後の方針等

確率の定義(1)

Definition 1 (Basic definition of probability)
Let Omega be a non empty set (not necessarily finite and discrete) and let Sigma be a σ-field of subsets of Omega. Let A,B be subsets of Omega and let ASeq be a sequences of subsets of Omega. Then, the mode probability P on Sigma yielding a function from Sigma into $\mathbb{R}$ is defined by:

(i) *For every A holds $0 \leq P(A)$,*
(ii) *P(Omega) = 1,*
(iii) *for all A, B such that A misses B holds $P(A \cup B) = P(A) + P(B)$, and*
(iv) *for every ASeq such that ASeq is nonincreasing holds P∗ASeq is convergent and lim(P∗ASeq) = P(Intersection ASeq).*

確率の定義(2)

Definition 2 (Definition of finite probability distribution)
Let p be a finite sequence of elements of $\mathbb{R}$. *Let i be an element of* $\mathbb{N}$. *Then, p is finite probability distribution if and only if:*

(i) *For every i such that* $i \in \mathrm{dom}\, p$ *holds* $p(i) \geq 0$ *and* $\sum p = 1$.

Definition 3 (Definition of prob)
Let E be a finite non empty set and let A be an event of E. Then, the functor prob(A) yields a real number is defined as follows:

(i) $prob(A) = \frac{card\ A}{card\ E}$.

離散確率の形式化

- step1 確率Pr(x)としてFDprobabilityを定義
  (定義３)　「数え上げ」

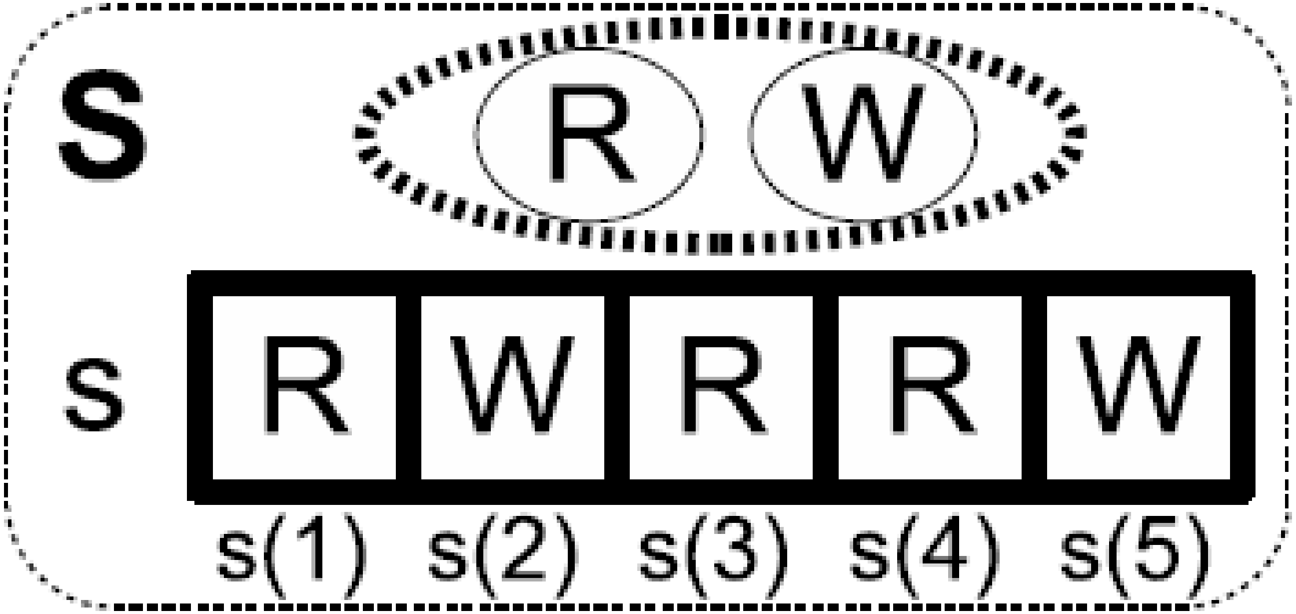
- step2 FDprobabilityの有限列としてFDprobSecを定義
  (定義２)「確率密度関数」

- step3 FDprobabilityを用いて確率測度を定義
  (定義1)　「コルモゴロフによる公理的な定義」

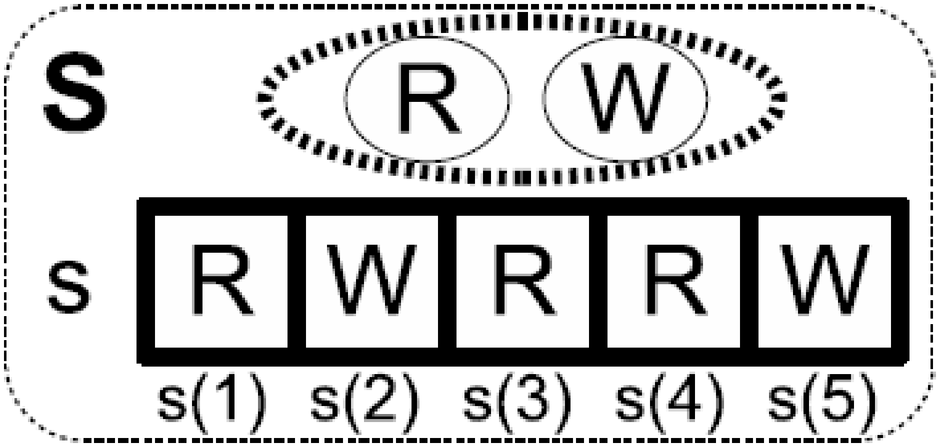
例

赤玉２個,白玉３個が入った袋から
赤玉を取り出す確率

空でない有限集合Sの要素の有限列sとして定義



確率変数



有限列sと確率変数とみなして話を進める

確率変数って何？

確率変数

実数値関数X がσ-可測関数

確率空間(Ω, σ, P)

$\forall r \in \boldsymbol{R}$

$$\{\omega \in \Omega; X(\omega) > r\} \in \sigma$$

⇓

X は （実）確率変数

（一般化） E-値確率変数

$$
\begin{array}{ccc}
\Omega & \xrightarrow{\quad X \quad} & E \\
\sigma & \xleftarrow{\quad X^{-1} \quad} & \mathcal{E} \\
\Big\downarrow P & & \\
\boldsymbol{R} & &
\end{array}
$$

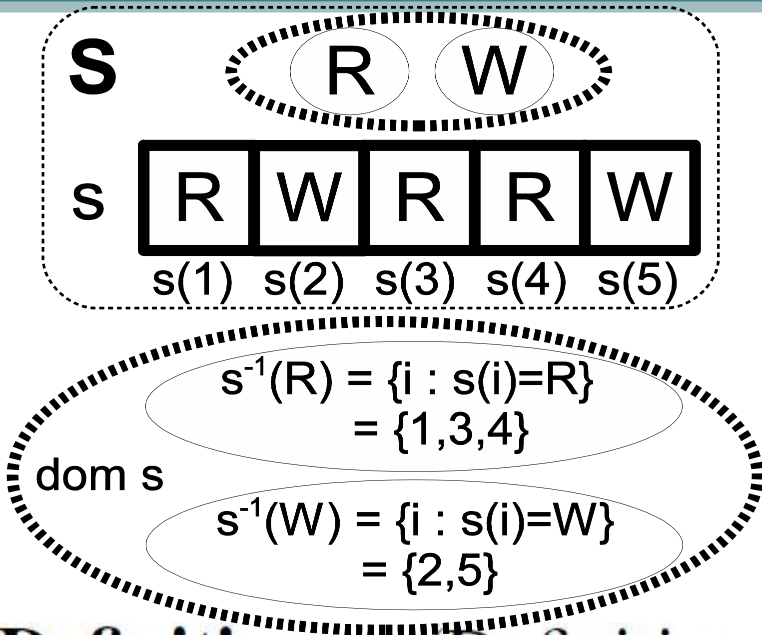
$\forall A \in \mathcal{E}$

$P(X^{-1}(A))$

$P(A)$と書いてある

Finite sequence は確率変数

theorem :
  for S be finite non empty set,
  F be non empty FinSequence of S
  holds
  F is random_variable of
  Trivial-SigmaField (Seg (len F)),
  Trivial-SigmaField (S);



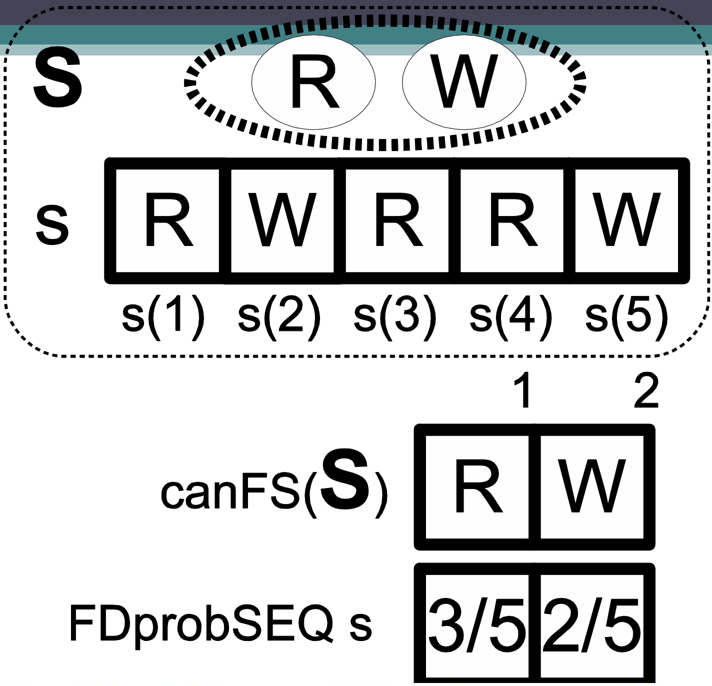
$$s^{-1}(x) = \{i \in dom\ \ s : s(i) = x\}$$

Definition (Definition of FDprobability)

Let S be a non empty finite set, let s be a finite sequence of elements of S, and let x be a set. Then, the functor FDprobability(x,s) yielding a real number is defined as follows:

$$FDprobability(x, s) = \frac{card\ \ s^{-1}(x)}{len\ \ s}.$$

FDProbabilityを並べて有限列を作る



Definition 5 (Definition of FDprobSEQ)
Let S be a non empty finite set and let s be a finite sequence of elements of S. Then, the functor FDprobSEQ s yielding a finite sequence of elements of $\mathbb{R}$ *is defined by:*

(i) *dom (FDprobSEQ s) = Seg(card S) and for every natural number n such that n* $\in$ *dom (FDprobSEQ s) holds (FDprobSEQ s)(n) = FDprobability((canFS(S))(n),s).*

確率の定義(1)

Definition 1 (Basic definition of probability)
Let Omega be a non empty set (not necessarily finite and discrete) and let Sigma be a σ-field of subsets of Omega. Let A,B be subsets of Omega and let ASeq be a sequences of subsets of Omega. Then, the mode probability P on Sigma yielding a function from Sigma into $\mathbb{R}$ is defined by:

(i) *For every A holds $0 \leq P(A)$,*
(ii) *P(Omega) = 1,*
(iii) *for all A, B such that A misses B holds $P(A \cup B) = P(A) + P(B)$, and*
(iv) *for every ASeq such that ASeq is nonincreasing holds P∗ASeq is convergent and lim(P∗ASeq) = P(Intersection ASeq).*

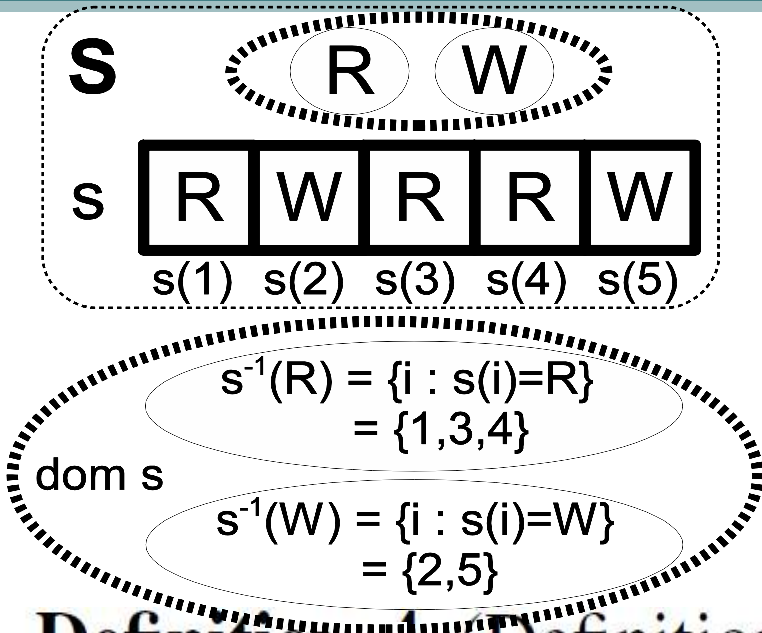
確率の形式化

FDprobability(x,s)=Pr(x)以外の確率が形式化されていない

任意の確率事象に対する形式化をしたい

1、Ωから要素xを選ぶ
2、条件判定オラクルCOを呼び出す
3、COはxが条件を満たすかどうか判定

上記モデルを確率の形式化に利用



$$s^{-1}(x) = \{ i \in dom\ \ s : s(i) = x \}$$

Definition 1 (Definition of FDprobability)

Let S be a non empty finite set, let s be a finite sequence of elements of S, and let x be a set. Then, the functor FDprobability(x,s) yielding a real number is defined as follows:

i) $FDprobability(A, s) = \dfrac{card\ \ s^{-1}(A)}{len\ \ s}.$ ただし$A \subset S$

（一般化） E-値確率変数

$$\Omega \xrightarrow{\quad X \quad} E$$

$$\sigma \xleftarrow{\quad X^{-1} \quad} \mathcal{E}$$

$$\sigma \xrightarrow{\quad P \quad} \boldsymbol{R}$$

$$\forall A \in \mathcal{E}$$

$$P(X^{-1}(A))$$

$P(A)$と書いてある

確率の形式化

FDprobability(x,s)=Pr(x)以外の確率が形式化されていない

任意の確率事象に対する形式化をしたい

1、Ωから要素iを選ぶ
2、条件判定オラクルCOを呼び出す
3、COはs.iが条件を満たすかどうか判定

上記モデルを確率の形式化に利用

（一般化） E-値確率変数

$$\Omega \xrightarrow{\quad X \quad} E$$

$$\sigma \xleftarrow{\quad X^{-1} \quad} \varepsilon$$

$$\sigma \xrightarrow{\quad P \quad} \boldsymbol{R}$$

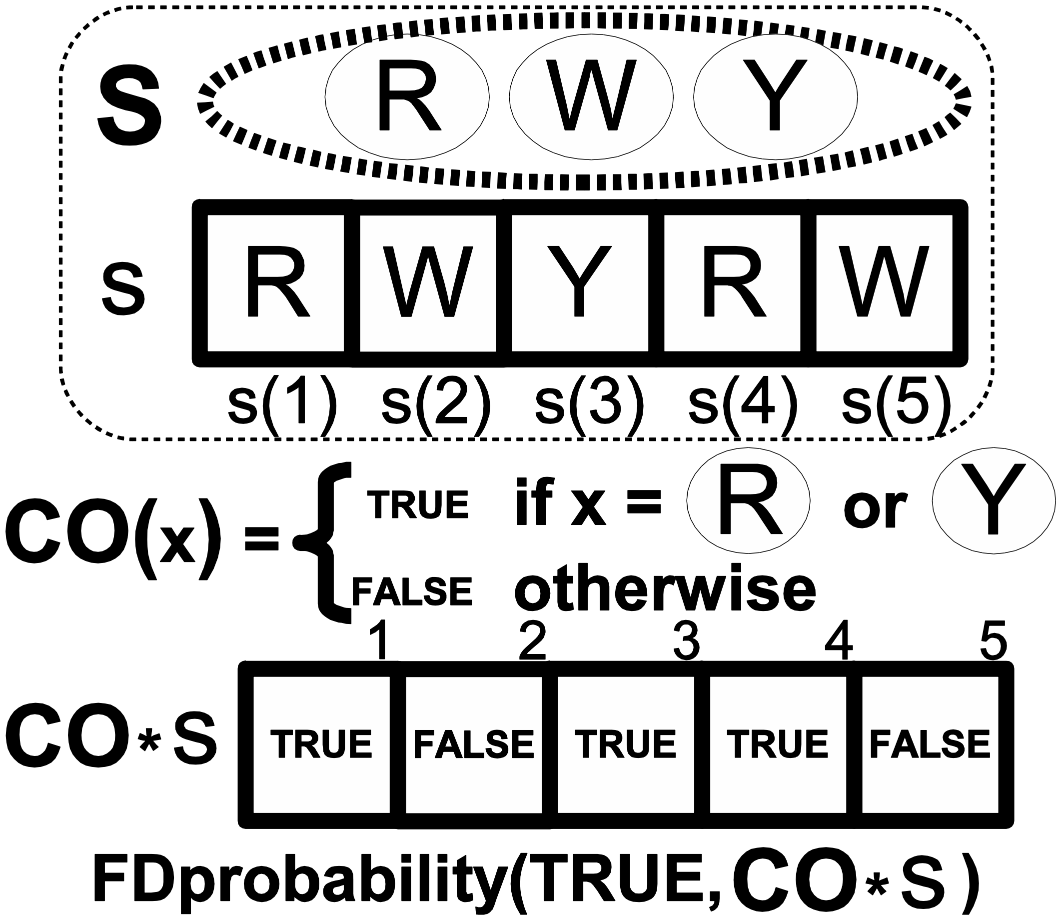
coは

Function of E,BOOLEAN

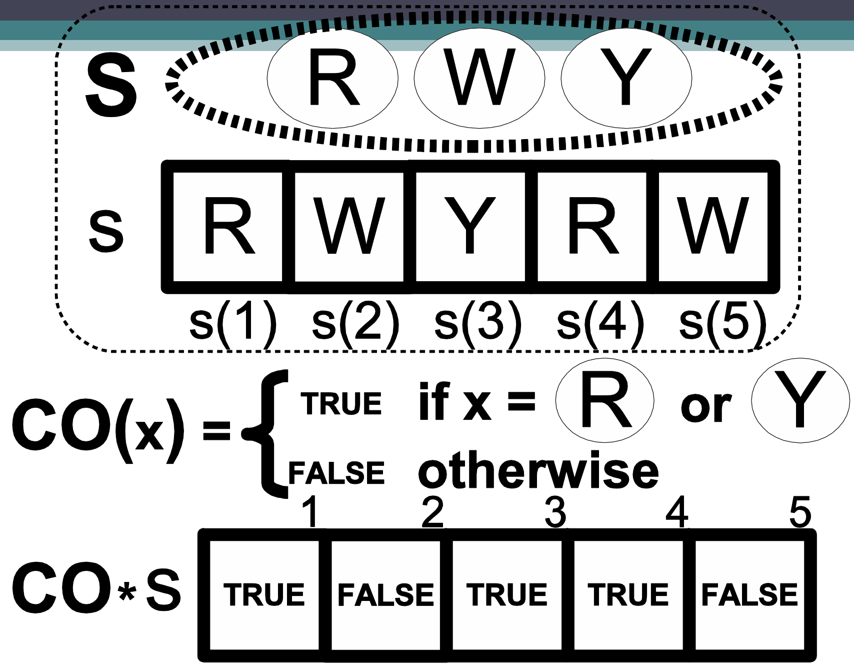
ならなんでもよい

Formalization of Probability

FDprobability(x,s)=Pr(x) → Formalize probability



Probの定義



CO*s
||
Composition of CO and s

Definition 10 (Definition of Prob)

Let S be a non empty finite set, let D be a well distributed element of the distribution family of S, let s be an element of D, and let CO be a function from S into BOOLEAN. Then, the functor Prob(CO,s) yielding a real number is defined as follows:

(i) $Prob(CO, s) = FDprobability(TRUE, CO * s)$.