Mizarプロジェクト概要と現状

日本における参加状況
(TPP2012年以降)

QED manifesto

- 現代数学のほとんどの核心部分をカバーする
計算機によって形式的に確認された証明の
巨大なライブラリを構築する

- 今後も新しく発表され続けられる成果の正しさを
厳密，迅速に検証するシステムを開発する.

QED manifestoの意義

- 高度化，複雑化し，大量に発表されて行く数学，計算機科学を含む数理科学の研究成果を誰がどのように検証するのか？従来通り人手による査読に頼って行くのか？

- 暗号などの高度な数理アルゴリズム，それらを用いたICTの計算機処理プログラムの動作の正しさを，間違えを犯しやすい人手によって今後も検査していくのか？

数理的知識の深い理解と数学的な思考能力の開発に計算機を援用できる。（人手によるマンツーマン教育の代替）

定理証明支援系

HOL：Cambridge大学のMICHAEL.J.C.GORDONが開発した高階述語論理(higher order logic)用を用いたシステム

HOL Light：John HarrisonによってHOLを改良

Isabelle：HOLの後継システムとして開発された対話型のシステム

Coq：フランスPPS研究所のPI.R2チームによって開発された対話型システム．背理法を認めない直感主義論理に基づいている

Mizar

ポーランドのAndrzej Trybulec教授が1973年頃に開発

古典的な一階述語論理に基づいている

Mizarは: 人手で作成された形式証明の検査を一括処理する

他のシステム: 自動証明に重点,証明記述の　過程でシステムとの逐次対話型で処理しながら形式証明を作成

Mizarの特徴

- 読み易さ

　ASCII文字列で書かれ，ほとんどの数理・情報科学の研究者が読むことができる数学的表現に十分に類似

　数学的な文書に共通した，論理(一階述語論理)と形式で記述されている.

　これを読むのに特別な訓練が必要ないような記述形式を目指している.

Mizarの記述例(TAYLOR展開定理)

- **theorem :: TAYLOR_1:33**

  for n be Nat, f be PartFunc of REAL,REAL, x0,r be Real st

  (0 < r & f is_differentiable_on n+1,].x0-r,x0+r.[ )

  for x be Real st x in].x0-r, x0+r.[holds

  ex s be Real st 0 < s & s < 1

  &f.x=Partial_Sums(Taylor(f,].x0-r,x0+r.[,x0,x)).n + (diff(f,].x0-r,x0+r.[).(n+1)).(x0+s*(x-x0)) * (x-x0) |^ (n+1) / ((n+1)!);

MMLの現状

2013年6月時点で,

Mizar Mathematical Library(MML)は

- 延べ200名を超える著者
- 1181のファイル.
- 約52,000の定理
- 10,000を超える形式上の定義

WEB上に公開

http://mizar.uwb.edu.pl/version/current/html/

(1)学部や修士学生が学習する微積分や関数解析，代数等の基礎的定理のライブラリ整備

ルベーグ積分(岐阜高専，遠藤)

::$N Lebesgue's Bounded Convergence Theorem

theorem :: MESFUN10:19

M.E < +infty & E = dom(F.0) & (for n be Nat holds F.n is_measurable_on E) & F is uniformly_bounded & (for x be Element of X st x in E holds F#x is convergent) implies (for n be Nat holds F.n is_integrable_on M) & lim F is_integrable_on M & ex I be ExtREAL_sequence st (for n be Nat holds I.n = Integral(M,F.n)) & I is convergent & lim I = Integral(M,lim F);

常微分方程式論(茨城大，宮島)

theorem :: ORDEQ_01:57

a<b & Z =]. a,b .[& G is_Lipschitzian_on the carrier of REAL-NS n implies

ex y be continuous PartFunc of REAL,REAL-NS n st

dom y = [' a,b ']

& y is_differentiable_on Z

& y/.a = y0

& for t be Real st t in Z holds diff(y,t) = G.(y/.t);

有限群論(信州大，中正)

theorem :: GROUP_17:35

for G being strict finite commutative Group st card G > 1 holds

ex I be non empty finite set,

F be associative Group-like commutative multMagma-Family of I st

I = support (prime_factorization card G)

& (for p be Element of I holds F.p is strict Subgroup of G &

card (F.p) = (prime_factorization card G).p) &

(for p,q be Element of I st p <> q holds

(the carrier of (F.p)) /¥ (the carrier of (F.q)) = {1_G})

&

(for y be Element of G

ex x be (the carrier of G)-valued total I -defined Function

st (for p be Element of I holds x.p in F.p) & y = Product x)

&

for x1,x2 be (the carrier of G)-valued total I -defined Function st

(for p be Element of I holds x1.p in F.p) &

(for p be Element of I holds x2.p in F.p) &

Product x1 = Product x2 holds x1=x2;

関数解析(信州大，師玉)

::$N Open Mapping Theorem

theorem :: LOPBAN_6:16

for X, Y be RealBanachSpace, T be Lipschitzian LinearOperator of X,Y, T1 be

Function of LinearTopSpaceNorm X,LinearTopSpaceNorm Y st T1=T & T1 is onto

holds T1 is open;

線形代数(信州大，中村)

theorem :: MATRIX_7:36

for n being Nat, K being Field, p being Element of

Permutations(n), A being Matrix of n,K st n>=1 holds (Path_product(A@)).(p") =

(Path_product(A)).p;

theorem :: MATRIX_7:37

for n being Nat, K being Field, A being Matrix of n,K st n

>=1 holds Det (A) = Det (A@);

(2)暗号理論や情報工学分野での形式検証に必要なライブラリの整備を当面の目標にライブラリ作成に取り組んでいる.

暗号系(東京理科大，荒井、信州大，岡崎)

definition

let SBT,MixColumns;

let cipher be Element of 128-tuples_on BOOLEAN;

let Key be Element of 256-tuples_on BOOLEAN;

func AES256-DEC(SBT,MixColumns,cipher,Key) ->

Element of 128-tuples_on BOOLEAN equals

:: AESCIP_1:def 24

(AES-Statearray)".(AES-DEC(SBT,MixColumns,AES-Statearray.cipher,

AES-KeyInitState256(Key)));

end;

theorem :: AESCIP_1:39

for SBT be Permutation of (8-tuples_on BOOLEAN),

MixColumns be Permutation of 4-tuples_on(4-tuples_on (8-tuples_on BOOLEAN)),

message be Element of 128-tuples_on BOOLEAN,

Key be Element of 256-tuples_on BOOLEAN holds

AES256-DEC(SBT,MixColumns,AES256-ENC(SBT,MixColumns,message,Key),Key) =

message;

暗号系(その2)　　NICT(辻井教授)　プロジェクトへの参加　(信州大、岡崎)

確率論からのアプローチ

従来の測度論的確率論を踏襲しつつも、暗号系に向いた具体的な確率論を指向

論理暗号からのアプローチ

(今後の展開に、新たな)定理証明の系の応用を模索中)

数論アリゴリズム(信州大，岡崎)

```
theorem :: NTALGO_1:15
 for nlist be non empty FinSequence of [:INT,INT:],
 a,b be non empty FinSequence of INT,
 x,y be Element of INT
 st len a = len b & len a = len nlist     &
 (for i be Nat st i in Seg (len nlist)     holds b.i <> 0 )     &
 (for i be Nat st i in Seg (len nlist)
 holds
 (nlist.i)`1 = a.i & (nlist.i)`2 =b.i )     &     (for i,j be Nat st i in Seg (len nlist)     & j in Seg (len nlist)
 & i <> j     holds b.i,b.j are_coprime )     &     (for i be Nat st i in Seg (len nlist)

 holds x mod b.i = a.i mod b.i )     & y = Product b     holds ALGO_CRT(nlist) mod y = x mod y;
```

楕円曲線論(北陸先端大，布田)

```
theorem :: EC_PF_2:63
 for p be 5_or_greater Prime, z be Element of EC_WParam p,
 g2, g3, g4, g8, gf1, gf2, gf3, gf4 be Element of GF(p),
 P be Element of EC_SetProjCo(z`1,z`2,p),
 R be Element of
 [:the carrier of GF(p), the carrier of GF(p), the carrier of GF(p):]
 st g2 = 2 mod p & g3 = 3 mod p & g4 = 4 mod p & g8 = 8 mod p &
 gf1 = z`1*(P`3_3 |^2) + g3*(P`1_3 |^2) & gf2 = P`2_3*(P`3_3) &
 gf3 = P`1_3*(P`2_3)*gf2 & gf4 = (gf1 |^2) - g8*gf3 &
 R = [g2*gf4*gf2, gf1*(g4*gf3-gf4) - g8*(P`2_3 |^2)*(gf2 |^2), g8*(gf2 |^3)]
 holds g4*(gf2 |^2)*(P`3_3 |^2)*
 ((R`2_3 |^2)*(R`3_3) - ((R`1_3 |^3) +
  z`1*(R`1_3)*(R`3_3 |^2) + z`2*(R`3_3 |^3))) = 0.GF(p);
```

Z-加群(北陸先端大，布田，信州大　岡崎)

```
definition
  struct (addLoopStr) Z_ModuleStruct
    (# carrier -> set,
         ZeroF -> Element of the carrier,
          addF -> BinOp of the carrier,
          Mult -> Function of [:INT, the carrier :], the carrier #);
end;
theorem :: ZMODUL03:37
  for p be Prime, V be finite-rank free Z_Module holds
  rank V = dim Z_MQ_VectSp(V,p);
```

Petrinet (信州大，カワモト)

definition

struct (PT_net_Str) Colored_PT_net_Str (# carrier, carrier' ->

set, S-T_Arcs -> Relation of the carrier,the carrier', T-S_Arcs ->

Relation of the carrier', the carrier, ColoredSet -> non empty

finite set, firing-rule -> Function #);

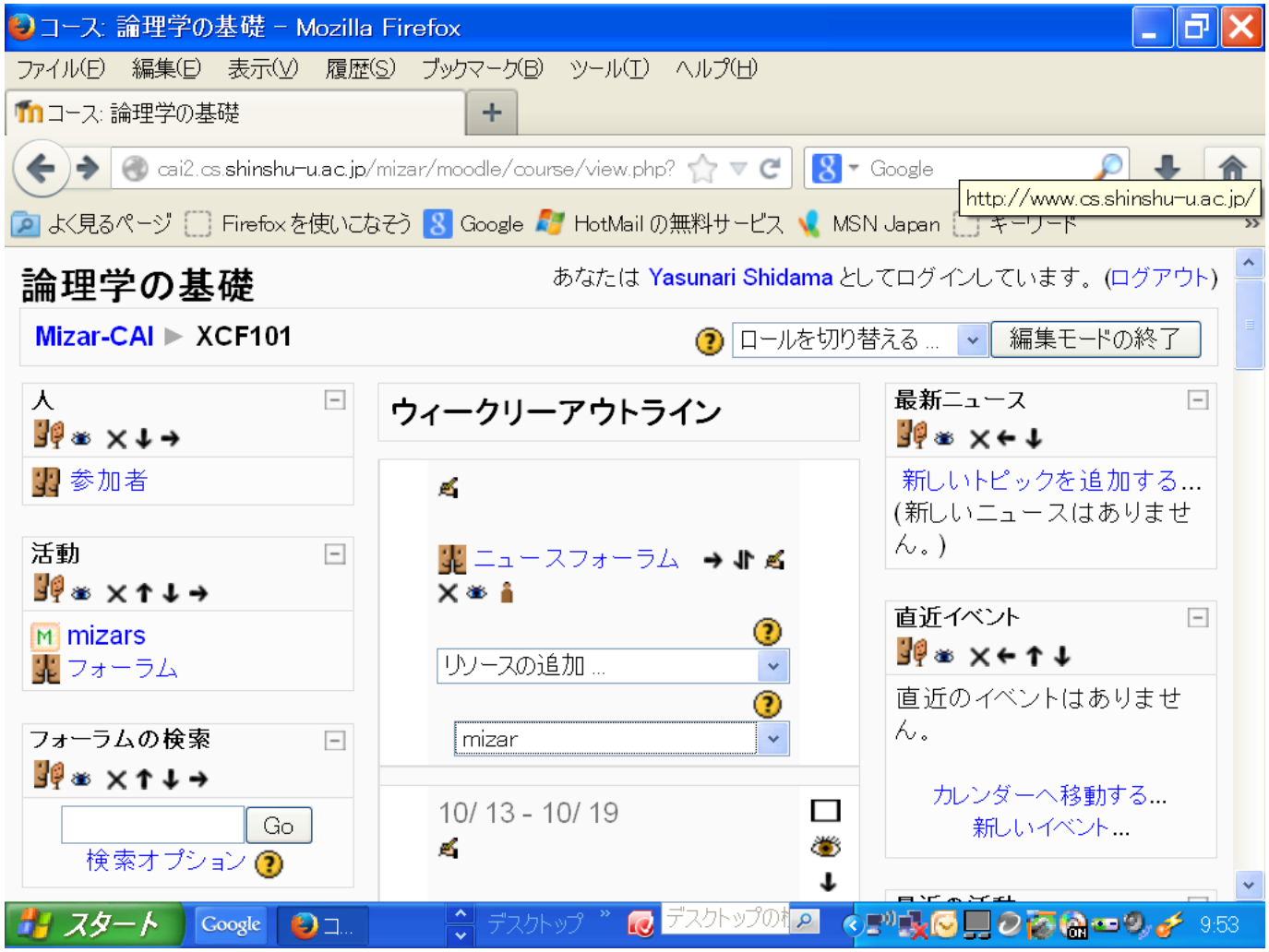
end;

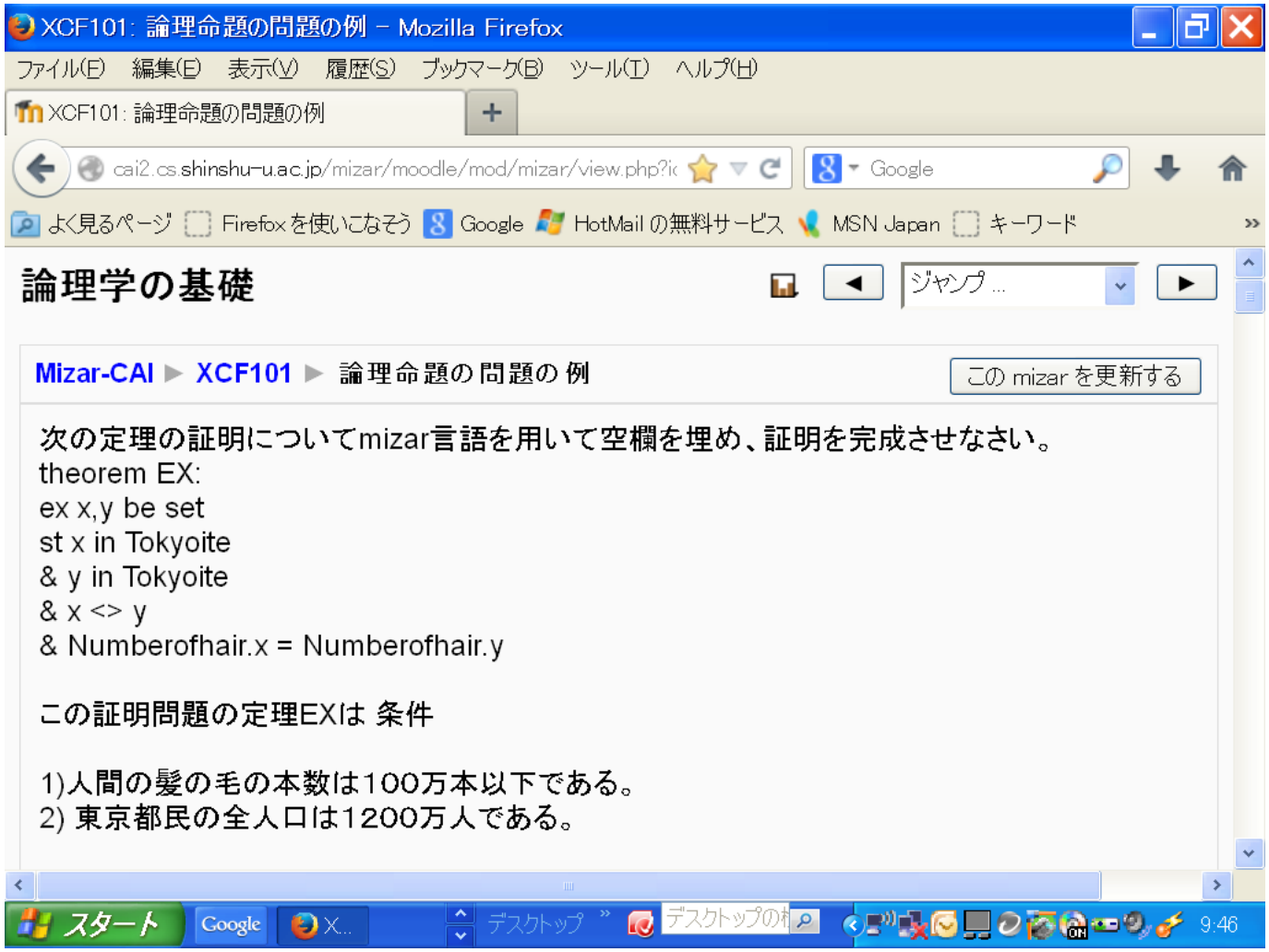
Mathenmatical Morphology (信州大，山崎)

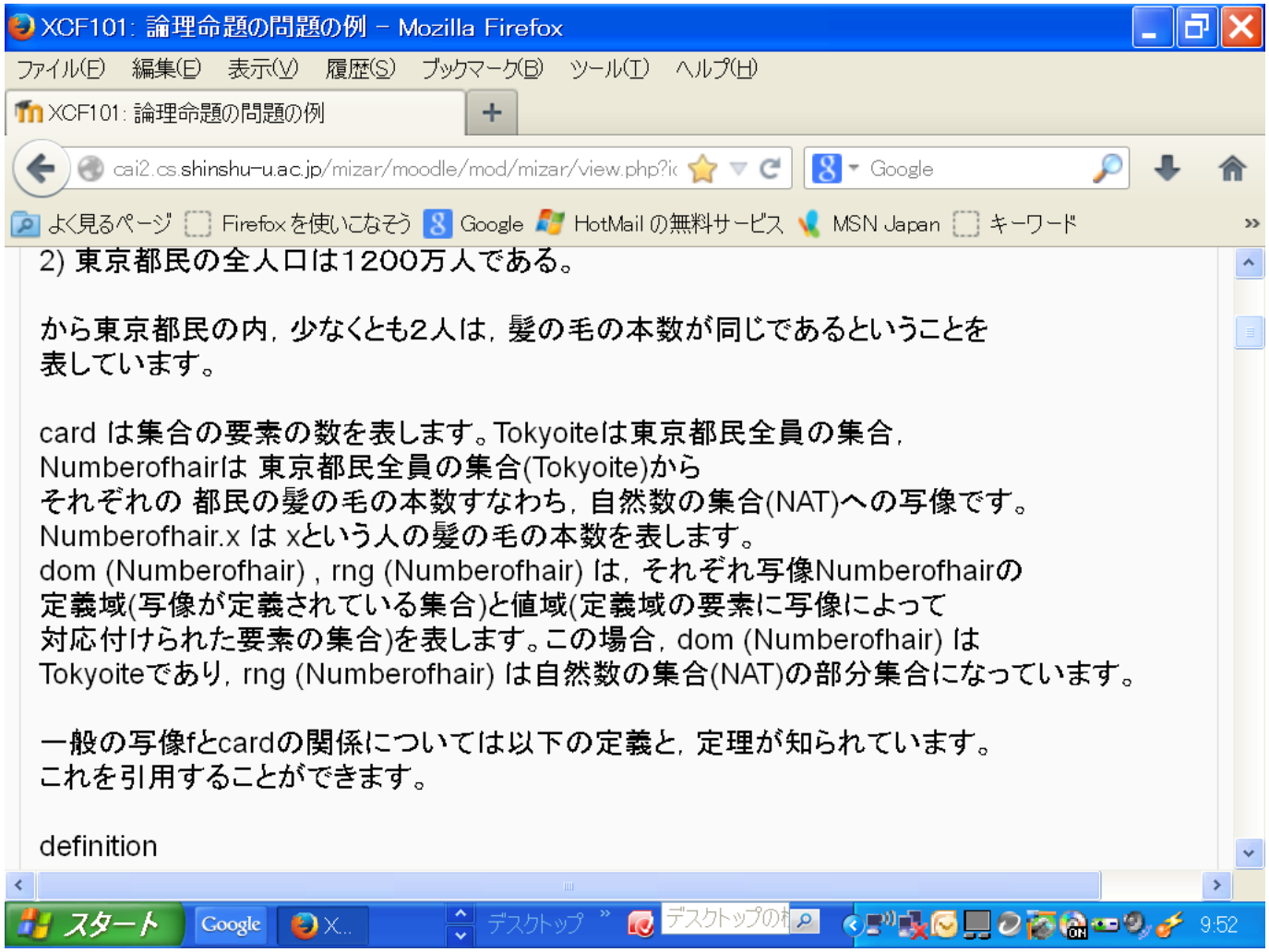
```
definition
  let E be RealLinearSpace;
  let B be binary-image of E;
  func erosion (B)
  -> Function of bool the carrier of E, bool the carrier of E means   :: MORPH_01:def 3
  for A be binary-image of E holds it.A = A(-)B;
end;
theorem :: MORPH_01:26
  (dilation(B)).(union F)     = union {(dilation(B)).X where X is binary-image of E: X in F};
theorem :: MORPH_01:27
  A c= B implies (dilation(C)).A c= (dilation(C)).B;
```

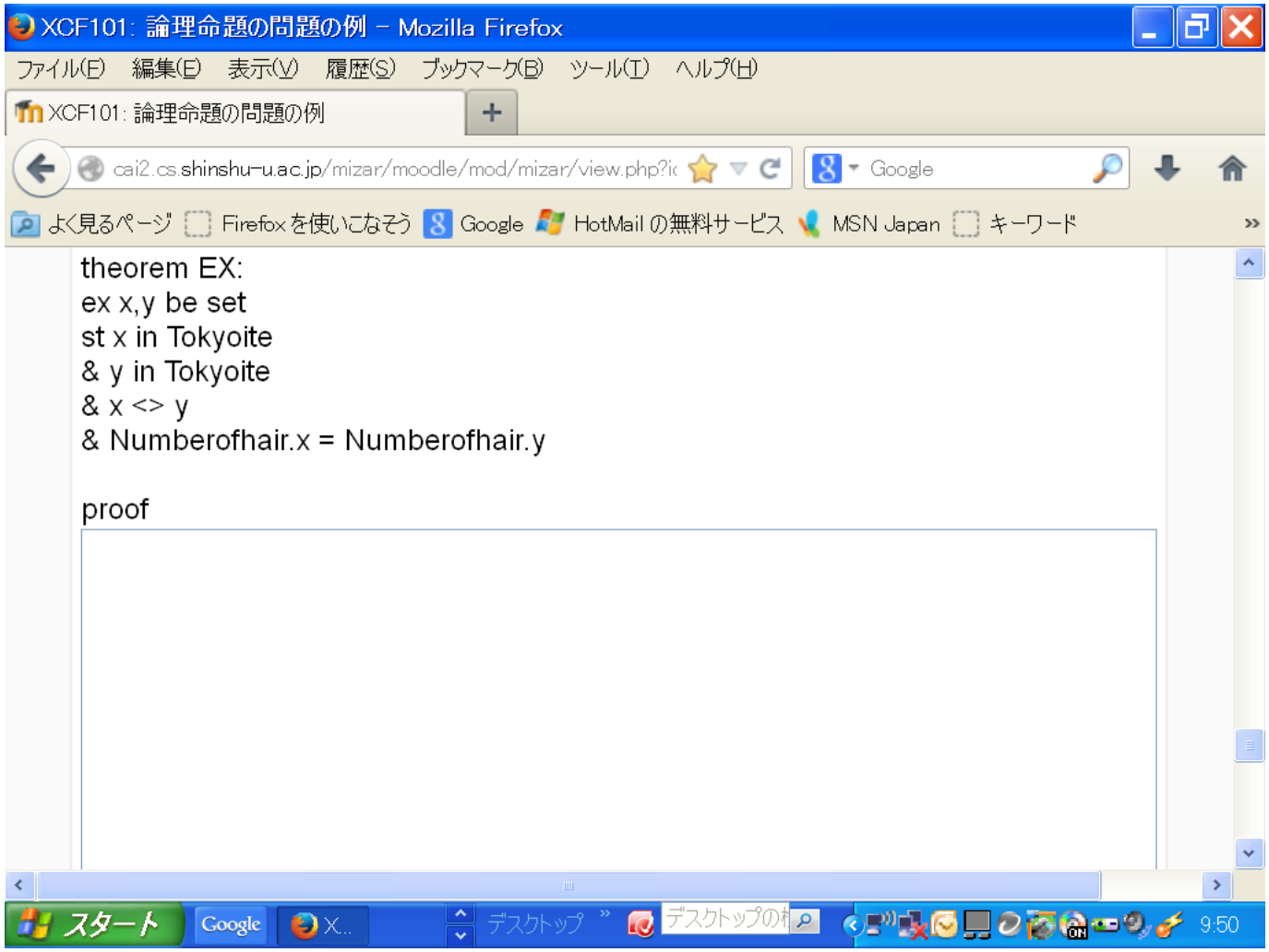
(3)数理的思考訓練用の教材を汎用CMSに組み込む研究 (信州大，和﨑)

1. e-learning教材を開発する際には，他を参照する必要のない自己完結的な教材が提供できる.
2. Mizarの既存のライブラリと一体で数学の公理体系から出発して必要な定理に至る全ての結果・ 証明を収録した教材の作成ができる.
3. QED manifestoの目的の一つである数学的な思考能力の開発に合致する
4. http://cai2.cs.shinshu-u.ac.jp/mizar/moodle/


コース: 論理学の基礎 - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
コース: 論理学の基礎
cai2.cs.shinshu-u.ac.jp/mizar/moodle/course/view.php?
Google
http://www.cs.shinshu-u.ac.jp/
よく見るページ
Firefox を使いこなそう
Google
HotMail の無料サービス
MSN Japan
論理学の基礎
あなたは Yasunari Shidama としてログインしています。(ログアウト)
Mizar-CAI ▶ XCF101
ロールを切り替える ...
編集モードの終了
人
参加者
活動
mizars
フォーラム
フォーラムの検索
Go
検索オプション
ウィークリーアウトライン
ニュースフォーラム
リソースの追加 ...
mizar
10/ 13 - 10/ 19
最新ニュース
新しいトピックを追加する...
(新しいニュースはありません。)
直近イベント
直近のイベントはありません。
カレンダーへ移動する...
新しいイベント...
スタート
Google
デスクトップ
9:53


XCF101: 論理命題の問題の例 – Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
XCF101: 論理命題の問題の例
cai2.cs.shinshu-u.ac.jp/mizar/moodle/mod/mizar/view.php?i
Google
よく見るページ Firefoxを使いこなそう Google HotMailの無料サービス MSN Japan キーワード
論理学の基礎
ジャンプ ...
Mizar-CAI ▶ XCF101 ▶ 論理命題の問題の例
この mizar を更新する
次の定理の証明についてmizar言語を用いて空欄を埋め、証明を完成させなさい。
theorem EX:
ex x,y be set
st x in Tokyoite
& y in Tokyoite
& x <> y
& Numberofhair.x = Numberofhair.y
この証明問題の定理EXは 条件
1)人間の髪の毛の本数は100万本以下である。
2) 東京都民の全人口は1200万人である。
スタート
Google
デスクトップ
9:46


XCF101: 論理命題の問題の例 – Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
XCF101: 論理命題の問題の例
cai2.cs.shinshu-u.ac.jp/mizar/moodle/mod/mizar/view.php?i
Google
よく見るページ Firefoxを使いこなそう Google HotMailの無料サービス MSN Japan キーワード
2) 東京都民の全人口は1200万人である。
から東京都民の内，少なくとも2人は，髪の毛の本数が同じであるということを
表しています。
card は集合の要素の数を表します。Tokyoiteは東京都民全員の集合，
Numberofhairは 東京都民全員の集合(Tokyoite)から
それぞれの 都民の髪の毛の本数すなわち，自然数の集合(NAT)への写像です。
Numberofhair.x は xという人の髪の毛の本数を表します。
dom (Numberofhair) , rng (Numberofhair) は，それぞれ写像Numberofhairの
定義域(写像が定義されている集合)と値域(定義域の要素に写像によって
対応付けられた要素の集合)を表します。この場合，dom (Numberofhair) は
Tokyoiteであり，rng (Numberofhair) は自然数の集合(NAT)の部分集合になっています。
一般の写像fとcardの関係については以下の定義と，定理が知られています。
これを引用することができます。
definition
スタート
Google
デスクトップ
9:52


XCF101: 論理命題の問題の例 – Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
XCF101: 論理命題の問題の例
cai2.cs.shinshu-u.ac.jp/mizar/moodle/mod/mizar/view.php?i
Google
よく見るページ
Firefox を使いこなそう
Google
HotMail の無料サービス
MSN Japan
キーワード
theorem EX:
ex x,y be set
st x in Tokyoite
& y in Tokyoite
& x <> y
& Numberofhair.x = Numberofhair.y
proof
スタート
Google
デスクトップ
9:50