Coq
定理証明という選択肢

有限会社 ITプランニング
システム開発部　今井宜洋
imai@itpl.co.jp

Coqってなに？

Coqってなに？

- 定理を証明することができるツール

Coqってなに？

- 定理を証明することができるツール
- CoqはフランスのINRIA研究所で開発されている

Coqってなに？

- 定理を証明することができるツール
- CoqはフランスのINRIA研究所で開発されている
- Coqを使ってプログラム開発ができる

Coqってなに？

- 定理を証明することができるツール
- CoqはフランスのINRIA研究所で開発されている
- Coqを使ってプログラム開発ができる

バグがない！

Coqってなに？

- 定理を証明することができるツール
- CoqはフランスのINRIA研究所で開発されている
- Coqを使ってプログラム開発ができる

バグがない！

テストは不要！！

Coqを使った開発の流れ

Coqを使った開発の流れ

- プログラム開発

Coqを使った開発の流れ

- プログラム開発
- 正しいことの証明

Coqを使った開発の流れ

- プログラム開発
- 正しいことの証明
- プログラムを抽出

Coqを使った開発の流れ

- プログラム開発
- 正しいことの証明
- プログラムを抽出

OCaml

Coqを使った開発の流れ

- プログラム開発
- 正しいことの証明
- プログラムを抽出

OCaml　Haskell

Coqを使った開発の流れ

- プログラム開発
- 正しいことの証明
- プログラムを抽出

OCaml Haskell Scheme

Coqを使った開発の流れ

テスト行程は なし！！

- プログラム開発
- 正しいことの証明
- プログラムを抽出

OCaml Haskell Scheme

よくある質問

よくある質問

Q

A

よくある質問

- Coqは習得するのが難しい？

よくある質問

- Coqは習得するのが難しい？

専門理論は不要。練習すれば誰でも使える。

よくある質問

Coqは習得するのが難しい？

専門理論は不要。練習すれば誰でも使える。

よくある質問

Coqは習得するのが難しい？

専門理論は不要。練習すれば誰でも使える。

私のMacでも使える？

よくある質問

Coqは習得するのが難しい？

専門理論は不要。練習すれば誰でも使える。

私のMacでも使える？

MacでもWindowsでもLinuxでもO.K.

よくある質問

Coqは習得するのが難しい？

専門理論は不要。練習すれば誰でも使える。

私のMacでも使える？

MacでもWindowsでもLinuxでもO.K.

よくある質問

Coqは習得するのが難しい？

専門理論は不要。練習すれば誰でも使える。

私のMacでも使える？

MacでもWindowsでもLinuxでもO.K.

システム全体をCoqで作るのは現実的でない？

よくある質問

Coqは習得するのが難しい？

専門理論は不要。練習すれば誰でも使える。

私のMacでも使える？

MacでもWindowsでもLinuxでもO.K.

システム全体をCoqで作るのは現実的でない？

一番大切なところだけをCoqで開発すればいい

作ってみた例

Webアプリケーション

日報管理システム

SQLインジェクション

データベースを不正に

アクセスされる危険性

作ってみた例

Webアプリケーション

日報管理システム

SQLインジェクション

データベースを不正に

アクセスされる危険性

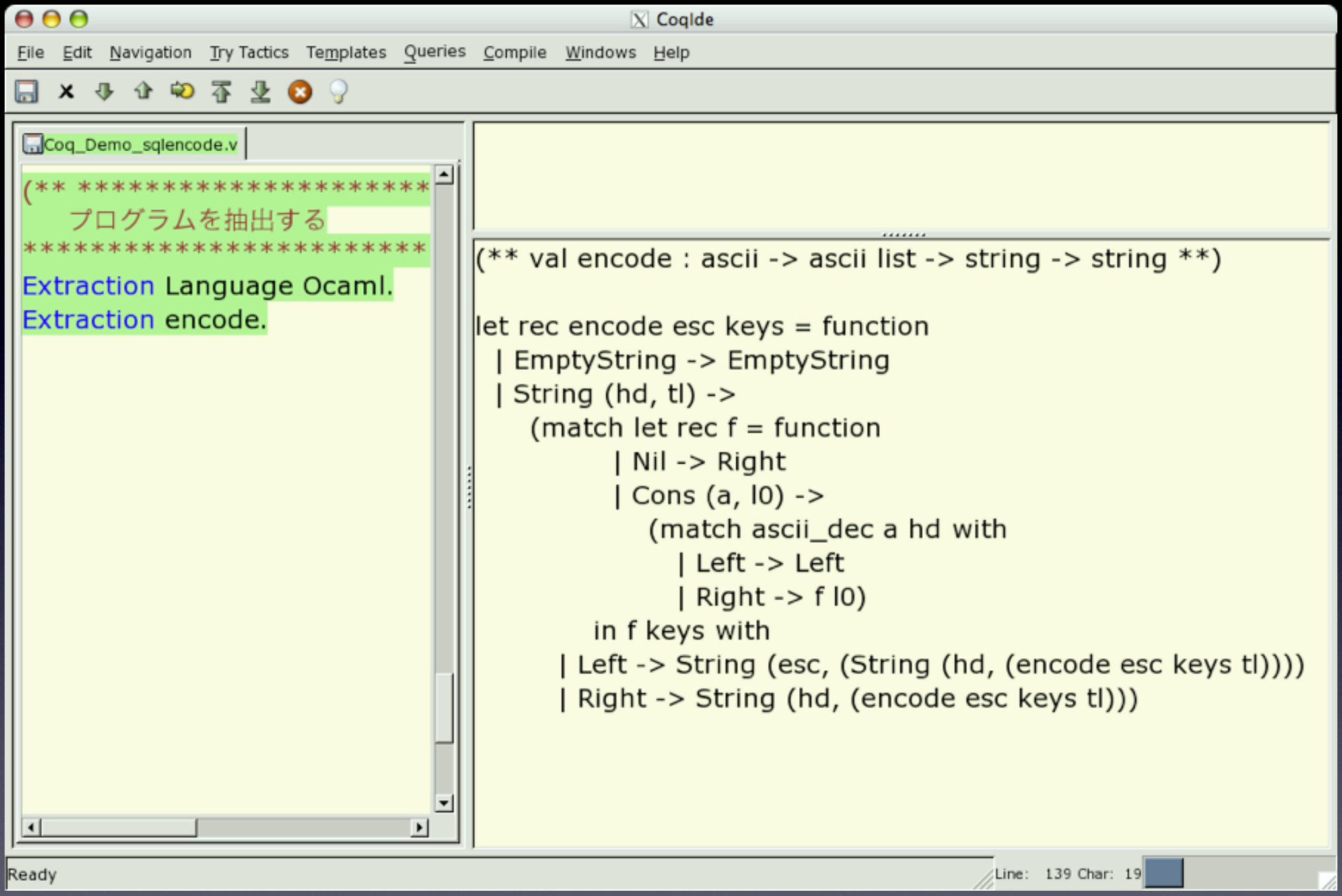
起こりえない！！

証明したこと

```
Theorem sql_encoding_safety :
forall s : string,
sql_safe (sql_encode s).
```

すべての文字列sに対して、

エンコードしたものは安全である。


CoqIde
File Edit Navigation Try Tactics Templates Queries Compile Windows Help
Coq_Demo_sqlencode.v
(** **********
プログラムを抽出する
****
Extraction Language Ocaml.
Extraction encode.
(** val encode : ascii -> ascii list -> string -> string **)
let rec encode esc keys = function
| EmptyString -> EmptyString
| String (hd, tl) ->
(match let rec f = function
| Nil -> Right
| Cons (a, l0) ->
(match ascii_dec a hd with
| Left -> Left
| Right -> f l0)
in f keys with
| Left -> String (esc, (String (hd, (encode esc keys tl))))
| Right -> String (hd, (encode esc keys tl)))
Ready
Line: 139 Char: 19

Coqをはじめよう！！

Coqをはじめよう！！

Coqをインストールする
http://coq.inria.fr/distrib-eng.html

チュートリアル, FAQ, リファレンスマニュアル
http://coq.inria.fr/doc-eng.html

ブログ「にわとり小屋でのプログラミング日記」
http://d.hatena.ne.jp/yoshihiro503/

OCaml-Nagoya: 名古屋で関数型言語やCoqを勉強しています
http://tsukimi.agusa.i.is.nagoya-u.ac.jp/~sydney/ocaml/