University of Virginia 28 October 2011
cs1120: Introduction of Computing
Explorations in Language, Logic, and Machines

Class 28: Reverse in Python, Entropy

Upcoming Schedule

- **Friday, 4 November:** Read Tyson's *Golden Age of Science*
- **Monday, 7 November:** Problem Set 6

Tuples and Lists

Tuples in Python are comparable to regular (immutable) lists in Scheme.

Python	Scheme
"Tuple"	"List"
()	**null**
p = (1, 2, 3)	**(define p (list 1 2 3))**
p[0]	**(car p)**
p[1:]	**(cdr p)**
p[2]	**(car (cdr (cdr p)))**
p[*i*]	**(car ((n-times cdr i) p))**
len(p)	**(length p)**

Lists in Python are comparable to **mutable** lists in Scheme.

Python	Scheme
"List"	"Mutable List"
[]	**null**
p = [1, 2, 3]	**(define p (mlist 1 2 3))**
p[0]	**(mcar p)**
p[0] = 4	**(set-mcar! p 4)**
p[1:]	**(mcdr p)**
[2, 3]	
p[1:] = [3, 4]	**(set-mcdr! p (mlist 3 4))**
p is now **[4, 3, 4]**	
p.append(5)	**(mlist-append! p (mlist 5))**
p is now **[4, 3, 4, 5]**	

University of Virginia 28 October 2011
cs1120: Introduction of Computing
Explorations in Language, Logic, and Machines

For loops in Python

Statement ::= **for** *Varible* **in** *Expression*: *Block*

```
def gaussSum (n):
   sum = 0
   for i in range(1, n+1):
         sum = sum + i
   return sum
```

range(a, b) ~ ((n-times cdr a) (intsto (- b 1)))
(e.g., range(0,3) = [0, 1, 2])

```
(define (loop index result test update proc)
 (if (test index)
     (loop (update index)
           (proc index result)
           test update proc)
     result))

(define (gauss-sum n)
   (loop 1 0 (lambda (i) (<= i n))
             (lambda (i) (+ i 1))
             (lambda (i sum) (+ i sum))))
```

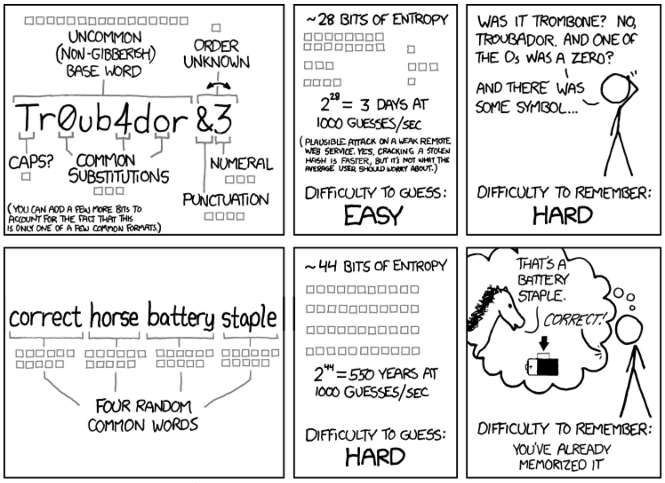
Shannon's Entropy Formula

$H = -\Sigma p_i \log_2 p_i$

p_i : probability of f event *i*
Sum over all events
Result is number of **bits of entropy**

Calculate the entropy in an *ideal* coin toss?

Calculate the entropy in a *real* coin toss (51% likelihood of landing in initial state)?



UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

How good is Randall Munroe's entropy estimate?