Class 17: Sex, Religion, and Politics

CS150: Computer Science
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/evans

Menu

- Debt, Population, Θ, Ω
- Is it useful for a problem to be hard?
- How the Allies broke Fish

PS4

Question 1: For each f and g pair below, argue convincingly whether or not f is (1) $O(g)$, (2) $\Omega(g)$, and (3) $\Theta(g)$ as explained above. For all questions, assume n is a non-negative integer.

…

(f) f: the federal debt n years from today, g: the US population n years from today (this one requires a more informal argument)

Malthusian Catastrophe

Reverend Thomas Robert Malthus, *Essay on the Principle of Population*, 1798

"The great and unlooked for discoveries that have taken place of late years in natural philosophy, the increasing diffusion of general knowledge from the extension of the art of printing, the ardent and unshackled spirit of inquiry that prevails throughout the lettered and even unlettered world, … have all concurred to lead many able men into the opinion that we were touching on a period big with the most important changes, changes that would in some measure be decisive of the future fate of mankind."

Malthus' Postulates

"I think I may fairly make two postulata.

- First, That food is necessary to the existence of man.
- Secondly, That the passion between the sexes is necessary and will remain nearly in its present state.

These two laws, ever since we have had any knowledge of mankind, appear to have been fixed laws of our nature, and, as we have not hitherto seen any alteration in them, we have no right to conclude that they will ever cease to be what they now are…"

Malthus' Conclusion

"Assuming then my postulata as granted, I say, that the power of population is indefinitely greater than the power in the earth to produce subsistence for man.

Population, when unchecked, increases in a geometrical ratio. Subsistence increases only in an arithmetical ratio. A slight acquaintance with numbers will show the immensity of the first power in comparison of the second."

Malthusian Catastrophe

- Population growth is geometric: $\Theta(k^n)$ $(k > 1)$
- Food supply growth is linear: $\Theta(n)$

What does this mean as $n \rightarrow \infty$?

Food per person = food supply / population
= $\Theta(n) / \Theta(k^n)$
As n approaches infinity, food per person approaches zero!

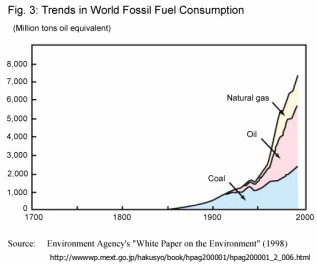
Malthus' Fallacy

Malthus' Fallacy

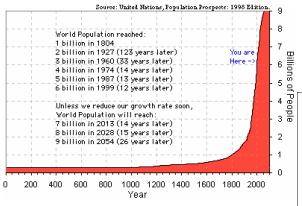
- He forgot how he started: "The great and unlooked for discoveries that have taken place of late years in natural philosophy, the increasing diffusion of general knowledge from the extension of the art of printing, the ardent and unshackled spirit of inquiry that prevails throughout the lettered and even unlettered world…"
- Agriculture **is** an "endless golden age" field:
  - Production from the same land increases as ~ $\Theta(1.02^n)$
  - Increasing knowledge of farming, weather forecasting, plant domestication, genetic engineering, pest repellants, distribution channels, etc.

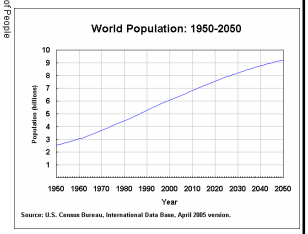
Upcoming Malthusian Catastrophes?

- Human consumption of fossil fuels grows as $\Theta(k^n)$ (fairly large k like 1.08?)
- Available fuel is constant (?)



Malthus was wrong about #2 Also





Advances in science (birth control), medicine (higher life expectancy), education, and societal and political changes (e.g., regulation in China) have reduced k (it is < 1 in many countries now!)

"Cornocopian View"

- Few resources are really finite
- Most things have endless golden ages
- Human ingenuity and economics and politics will solve problems before they become catastrophes
  - No one will sell the last gallon of gas for $2.98

"Kay"-sian View

The best way to predict the future is to invent it.
— Alan Kay

Influence of Malthus

"In October 1838, that is, fifteen months after I had begun my systematic inquiry, I happened to read for amusement Malthus on *Population*, and being well prepared to appreciate the struggle for existence which everywhere goes on from long-continued observation of the habits of animals and plants, it at once struck me that under these circumstances favorable variations would tend to be preserved, and unfavorable ones to be destroyed. The results of this would be the formation of a new species. Here, then I had at last got a theory by which to work."

Charles Darwin, in his autobiography (1876)

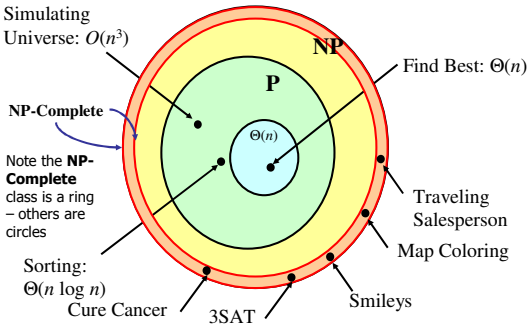
PS4

Question 1:
(f) f: the federal debt n years from today, g: the US population n years from today (this one requires a more informal argument)

Debt increases:
Spending – Revenues: this varies, but usually positives
+ Interest on the existing Debt (exponential)
= $\Theta(k^n)$
Population increase is not exponential: rate continues to decrease

=> as n increases, debt per person approaches infinity!
This will *eventually* be a problem, but orders of growth analysis doesn't say when.

Problem Classes if P ≠ NP:



Graph (Map) Coloring Problem

- Input: a graph of nodes with edges connecting them and a minimum number of colors
- Output: either a coloring of the nodes such that no connected nodes have the same color, or "no".

If given a coloring, easy to check if it no connected nodes have the same color, and the number of colors used.

Best Map Coloring Problem

- Input: a graph of nodes with edges connecting them
- Output: the minimum number of colors that can be used to color the map without any adjacent nodes having the same color

```
(define (best-map-coloring graph)
  (define (bmc-helper graph guess)
    (if (has-map-coloring? graph guess)
        guess
        (bmc-helper graph (+ 1 guess)))
  (bmc-helper graph 0)))
```

Since has-map-coloring? is in NP and we can solve best-map-coloring using a polynomial number of calls to has-map-coloring? we know best-map-coloring is also in NP

Is it ever *useful* to be confident that a problem is *hard*?

Factoring Problem

- Input: an n-**digit** number
- Output: two prime factors whose product is the input number
- Easy to multiply to check factors are correct
- **Not** proven to be NP-Complete
  - Most people think it is (except *Sneakers*)
- Most used public key cryptosystem (RSA) depends on this being hard (click on the key symbol at the bottom of your web browser)

Breaking Fish

- GCHQ learned about first Fish link (Tunny) in May 1941
  - Intercepted unencrypted Baudot-encoded test messages
- August 30, 1941: Big Break!
  - Operator retransmits failed message with same starting configuration
  - Gets lazy and uses some abbreviations, makes some mistakes
    - SPRUCHNUMMER/SPRUCHNR (Serial Number)

"Two Time" Pad

- Allies have intercepted:

  C1 = M1 XOR **K1**

  C2 = M2 XOR **K1**

  Same key used for both (same starting configuration)
- Breaking message:

  C1 XOR C2 = (M1 XOR **K1**) XOR (M2 XOR **K1**)

  = (M1 XOR M2) XOR (**K1** XOR **K1**)

  = M1 XOR M2

"Cribs"

- Know: C1, C2 (intercepted ciphertext)

  C1 XOR C2 = M1 XOR M2
- Don't know M1 or M2
  - But, can make some guesses (cribs)
    - SPRUCHNUMMER
    - Sometimes allies moved ships, sent out bombers to help the cryptographers get good cribs
- Given guess for M1, calculate M2

  M2 = C1 XOR C2 XOR M1
- Once guesses that work for M1 and M2

  K1 = M1 XOR C1 = M2 XOR C2

Finding K1

- From the 2 intercepted messages, Col. John Tiltman worked on guessing cribs to find M1 and M2
  - 4000 letter message, found 4000 letter key
- Bill Tutte (recent Chemistry graduate) given task of determining machine structure from key
  - Already knew it was 2 sets of 5 wheels and 2 wheels of unknown function

Reverse Engineering Lorenz

- Looked at patterns of bits in key
- Found repeating sequence:
  - Repetition period of 41, learned first wheel had 41 pins
  - Similar for other wheels, determining S/M/K wheel structure
- After 6 months of hard work: determined likely machine structure that would generate K1

Intercepting Traffic

- Set up listening post to intercept traffic from 12 Lorenz (Fish) links
  - See map on back of book
  - Different links between conquered capitals
  - Slightly different coding procedures, and different configurations
- 600 people worked on intercepting traffic
- Sent intercepts to Bletchley (usually by motorcycle courier)

Breaking Traffic

- Knew machine structure, but a different initial configuration was used for each message
- Need to determine wheel setting:
  - Initial position of each of the 12 wheels
  - 1271 possible starting positions
  - Needed to try them fast enough to decrypt message while it was still strategically valuable

Continues in Lecture 18...

Charge

- Exam 1 out now, due Wednesday
  - Beginning of class
  - No exceptions without prior arrangement
- Enjoy your reading break