Lecture Notes

Foundations of informatics — a bridging course
Mathematical tools

Michael Nüsken

b-it

(Bonn-Aachen International Center
for Information Technology)

Fall 2013

b-it

Bonn-Aachen International Center
for Information Technology

Foundations of informatics - a bridging course

This course is not listed in Aachen Campus and in Bonn Basis as Foundations of Informatics: a bridging course.

Responsible

Prof. Dr. Joachim von zur Gathen
Prof. Dr. Berthold Vöcking

Lecture

Michael Nüsken
Konstantin Ziegler
Thomas Noll
Walter Unger

Time & Place

- 15 - 18 October 2013, b-it bitmax (Michael Nüsken).
- 21 - 25 October 2013, b-it bitmax (Konstantin Ziegler).
- 24 - 28 February 2014, b-it Rheinsaal (Thomas Noll).
- 04 - 07 March 2014, b-it Rheinsaal (Walter Unger).

Schedule: Mon-Fri 9^{00} - 12^{30} and 14^{00} - 16^{00}, each block includes 30 minutes break. (If a course week advances fast, Friday afternoon may be free.)

Exam

- Exam1: **tba.**
- Post-Exam1: tba.
- Exam2 (repetition): tba.
- Post-Exam2: tba.

The exam is about the entire course. Please note that the second exam is for repetitions.

Credits

For some MI-students this course is obligatory, for the others it's optional. There are no credits for this course.
There will be a written exam after the end of the complete course.

Week 1 - Mathematical tools

This week will deal essentially with three subjects:

- Linear Algebra (Gauß-Jordan-algorithm, expansion, dim ker A + dim im A = n, ...),
- Probabilities (Definitions, conditional probabilities, random variables, expected runtime of a

random exit loop, some applications, ...),
- Integers modulo N (Definition, inversion and extended Euclidean algorithm, square and multiply, exponentiation, Theorem of Lagrange, of Euler and Fermat's little theorem, RSA correctness and efficiency, ...).

Week 2 - Algorithms and Analysis

Agenda

1. foundations (first examples, asymptotic notation, solving recurrence equation)
2. sorting (QUICKSORT, sorting in linear time)
3. data structures (linked lists, hash tables, binary search trees)
4. graph algorithms (elementary (breadth-first, depth-first), single-source shortest path)
5. as time permits: advanced (matrix operations, polynomial and FFT, NP-completeness)

Literature

- Cormen, Leiserson, Rivest, and Stein, Introduction to Algorithms, 3rd edition, MIT Press, 2009.
- Goldreich, Computational Complexity: A conceptual perspective, Cambridge University Press, 2008.
- Knuth, TAOCP, Vol. 1 -- Fundamental Algorithms, 3rd edition, Addison-Wesley.

Week 3 - Regular Languages, Context-Free Languages, Processes and Concurrency

Week 4 - Complexity

Allocation

equivalent V4+Ü4
Note that all Media informatics courses only start in the third week of the lecturing period, so that everybody can participate in this course.

Imprint, webmaster & more

Exercise 0:

(i) Send an email to

nueskem@bit.uni-bonn.de

with subject starting

[13us-brico]

(ii) Make sure you obtain an account in b-it!

Foundations of informatics — a bridging course
Fall 2013
Mathematical tools

MICHAEL NÜSKEN

1. Lights and cards

Exercise 1.1 (Lights on). (10 points)

You are left in a large round hall. In it you discover a circle of lamps. At the wall below each lamp is a switch. Yet, you discover that each switch changes the on/off-status of the lamp and its left and right neighbor. Unattainable for you in the middle of the room is a mechanism that can open the only exit. Yet, it opens only if the room is completely dark, ie. all lights are off.

(i) Your particular room has 4 lamps, and the first and second are lit. $\boxed{2}$

(ii) Your room has 6 lamps, and the first and third are lit. $\boxed{3}$

(iii) Develop and describe a general procedure to escape. $\boxed{5}$

Exercise 1.2 (Cards dealt). (10 points)

Consider a simple game: n players are sitting in a round. Player i has v_i cards. She may give $2k$ cards away, half to the left and half to the right. The team wins when finally all players have a multiple of m cards.

The problem corresponds to distributing the load of a large bunch of given jobs to n computing centers, where each single machines can run m jobs. However, since sending data is expensive data can only be transferred to a neighboring center. To avoid conflicts between the neighbors, both neighbors shall get the same amount of additional jobs. Since starting a machine for less than m jobs is much more expensive than giving that to neighboring centers, the aim is to have a multiple of m jobs.

(i) Say $n = 3$, $m = 4$, and $v_1 = 2$, $v_2 = 3$, $v_3 = 7$. $\boxed{3}$

(ii) Say $n = 3$, $m = 5$, and $v_1 = 2$, $v_2 = 3$, $v_3 = 7$. $\boxed{3}$

(iii) Say $n = 4$, $m = 7$, and $v_1 = 2$, $v_2 = 5$, $v_3 = 11$, $v_4 = 3$. $\boxed{4}$

Exercise 1.3 (A strange treasure). (15 points)

Five beagle boys have finally succeeded in stealing some of Scrooge McDuck gold dollars. They decide that they will split up their treasure the next morning. 15

During the night the first beagle boy wakes up and thinks to himself: Well, better I take my share now. He counts the coins and notices that the number divides by five only after removing one coin which he throws away. Then he takes his share and goes to sleep again.

Well, this repeats for the other four beagle boys as well.

Next morning, the five divide the remaining coins equally among them without any spare coin.

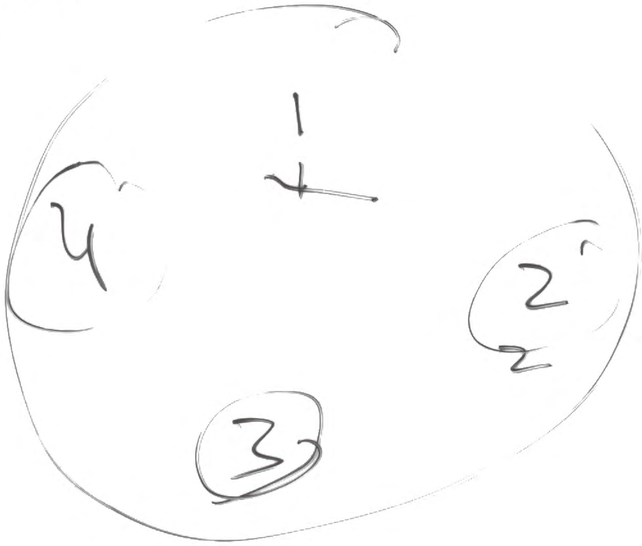
How many coins did the treasure have at the beginning? (And how many coins did each of them get?) Find the smallest answer. Find all answers.

Bus-brico
15.10.13
1

Ex 1

Ideas: Brute force

Uzair:



4 3rd on
2nd off
4th on

4th of
1 off
3rd of

Shekoufeh: use 0, 1 for states
Mustafa : 1, 2, 3, 4 for states
on off

Cifong: combine and add first state at end:

11001

Nikola : write down state with 0, 1
eg. 1100
add eg. 0111 to change state.

Hint 1: Third piece of language? How to write down a solution?

Hint 2: Does the order of moves (:= change of state) matter? Try to state a hypothesis and try to prove it.

ad Hint 1: Recall that Uzair told us to first operate switch 3 and then operate switch 4. How to "code" this?

(1b) How to check whether it is a solution?

Bus-brico
15.10.13
3

A bit of theory

DON'T PANIC twice!

$\mathbb{F}_2 :=$

i.e. $\mathbb{F}_2$ is a field.

- Two elements, two possible values:
  0, 1.
- Two operations:

$$+ : \mathbb{F}_2 \times \mathbb{F}_2 \longrightarrow \mathbb{F}_2$$

{ or: $\mathbb{F}_2$ plus ($\mathbb{F}_2$ x, $\mathbb{F}_2$ y) }

$$\cdot : \mathbb{F}_2 \times \mathbb{F}_2 \longrightarrow \mathbb{F}_2$$

Implementation:

+	0	1
0	0	1
1	1	0

(also called XOR)

·	0	1
0	0	0
1	0	1

(also called AND)

- ~~Twelve~~ 12 rules that holds

+	·
Properly defined	Properly defined
Associativity: $(a+b)+c = a+(b+c)$	Associativity
Neutral element: $0+a=a$, $a+0=a$	Neutral element: $1\cdot a = a$, $a \cdot 1 = a$
Inverses exist: $\forall a\ \exists b:\ a+b=0 \wedge b+a=0$	Inverses exist, unless $a=0$. $\forall a \neq 0\ \exists b:\ a\cdot b = 1 = b \cdot a$
Commutative: $a+b=b+a$	Commutative

Distributive: $a\cdot(b+c) = a\cdot b + a\cdot c$
$(a+b)\cdot c = a\cdot c + b\cdot c$

DON'T: $0 \neq 1$.

Bus-bricks
15.10.13
4

First way to encode a solution:

Use a list of move numbers.

Eg: $(3, 4)$.

<u>Def</u> • A state is an element of $\mathbb{F}_2^n$.

• A move is an element of $\mathbb{F}_2^n$,

but only the following moves are allowed:

$$\mathrm{move}_i = \begin{bmatrix}0\\ \vdots\\ 0\\ 1\\ 1\\ 1\\ 0\\ \vdots\\ 0\end{bmatrix}\begin{matrix}\\ \\ \\ \\ \leftarrow i\\ \\ \\ \\ \\ \end{matrix} \quad \text{for } 0 < i < n-1$$

$$\mathrm{move}_0 = \begin{bmatrix}1\\ 1\\ 0\\ \vdots\\ 0\\ 1\end{bmatrix}\begin{matrix}\leftarrow 0\\ \\ \\ \\ \\ \\ \end{matrix} \qquad \mathrm{move}_{n-1} = \begin{bmatrix}1\\ 0\\ \vdots\\ 0\\ 1\\ 1\end{bmatrix}\begin{matrix}\\ \\ \\ \\ \\ \leftarrow n-1\end{matrix}.$$

• A long solution is a list (of indices) of moves, so an element of $(\mathbb{N}_{<n})^*$

Back to our example:

$(2,3)$ is a solution to ~~enco~~ $\begin{bmatrix}1\\1\\0\\0\end{bmatrix}$.

$(1,2,1,3)$ also is a solution.

$(3,1,0,2,0,1)$ is a solution.

$(3,1,0,1,2,0)$

$(3,1,1,1,2,1)$

$(2,1,2,0,2,3,0,1)$

To define ~~what~~ how a solution works

define: $+ : \mathbb{F}_2^4 \times \mathbb{F}_2^4 \longrightarrow \mathbb{F}_2^4$. coordinatewise.

Note that we have PANIC for this combination $(\mathbb{Z}_2^{*}, +)$.

Derived rule: General associativity:

Given $a_0, \dots a_{k-1}$

Then

$$z = (\dots((a_{\sigma 0} + a_{\sigma 1}) + \dots + a_{\sigma(k-1)})$$

does not depend on the permutation σ of the index set $\{0, 1, 2, \dots k-1\}$.

Lemma

In $\mathbb{Z}_2$ and also $\mathbb{Z}_2^{*}$ for every element a we have $a + a = 0$.

Theorem

If $(i_0, \dots, i_{k-1})$ is a ~~sep~~ long solution then also $(i_{\sigma(0)}, \dots, i_{\sigma(k-1)})$ is a long solution and we may even drop any pair of equal indices.

Shortest long description: sort and drop pairs.

Eg: $(3, 1, 1, 1, 2, 1)$ reduces to $(\underbrace{1, 1}, \underbrace{1, 1}, 2, 3)$ and to $(2, 3)$

Bus-brico
15.10.13
6

Def A short solution is an element of $\mathbb{Z}_2^4$.

Eg. $(2,3)$ translates into $\begin{array}{c} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \end{array} \begin{array}{l} \\ \\ \leftarrow \text{move } 2 \\ \leftarrow \text{move } 3 \end{array}$

~~By~~ By our theorem any long solution is equivalent to a unique short solution.

Def Given a starting state $s \in \mathbb{Z}_2^4$ and a possible solution $x \in \mathbb{Z}_2^4$ the result of the game, ie. executing the solution on the starting state is

$$s + M x$$

where $M = [\text{move}_0, \ldots \text{move}_{n-1}]$.

$$= \begin{bmatrix} 1 & 1 & 0 & & 0 & 1 \\ 1 & 1 & 1 & \ddots & \vdots & 0 \\ 0 & 1 & 1 & \ddots & \vdots & \vdots \\ \vdots & 0 & 1 & \ddots & 0 & \vdots \\ \vdots & \vdots & 0 & \ddots & 1 & 0 \\ 0 & \vdots & \vdots & \ddots & 1 & 1 \\ 1 & 0 & 0 & & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} =: s$$

Want given starting s and move m and "selector" α, to ~~obtain~~

$$s' = \begin{cases} s & \text{if } \alpha = 0 \\ s + m & \text{if } \alpha = 1. \end{cases}$$

$$= s + \alpha \cdot m$$

Bus-brico
15.10.13
7

Def A possible solution x is a (true) solution iff

$$s + \Pi x = 0.$$

Note that this is the same as $\boxed{\Pi x = s}$ since we have the Lemma, saying $a + a = 0$.

How to solve linear systems?

- Gaußian elimination
- Gauß-Jordan-algorithm.

Let's example of the second:

We work over the field

$$\mathbb{F}_7 : \{-3, -2, -1, 0, 1, 2, 3\}.$$

$$+, \cdot : \mathbb{F}_7 \times \mathbb{F}_7 \to \mathbb{F}_7$$

$$(x, y) \longmapsto (x \underset{\cdot_{\mathbb{Z}}}{+_{\mathbb{Z}}} y) \bmod 7$$

In particular:

$\cdot$	0	(±)1	(±)2	(±)3
0	0	0	0	0
(±)1	0	1	2	3
(±)2	0	2	-3	-1
(±)3	0	3	-1	2

and

x	±1	±2	±3
x^{-1}	±1	∓3	∓2

We consider the system:

$$\begin{bmatrix} 2 & 1 & -2 \\ 0 & 3 & 1 \\ 1 & 0 & 2 \end{bmatrix} x = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \quad \text{over } \mathbb{F}_7 .$$

To solve we just write a condensed form.

$$\left[\begin{array}{ccc|c} 2 & 1 & -2 & 2 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 2 & 0 \end{array}\right]$$

← divide row 0 by 2, i.e. multiply with -3
subtract new row 0 from row 2 once.

$$\left[\begin{array}{ccc|c} 1 & -3 & -1 & 1 \\ 0 & 3 & 1 & 1 \\ 0 & 3 & 3 & -1 \end{array}\right]$$

← divide row 1 by 3, i.e. mult. with -2
subtract new row 1 from row 0 -3 times
from row 2 3 times.

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & -2 & -2 \\ 0 & 0 & 2 & -2 \end{array}\right]$$

← divide row 2 by 2, i.e. mult. with -3
subtract new row 2 from row 1 -2 times

$$\left[\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & -1 \end{array}\right]$$

→ $x_0 = 2$
$x_1 = 3$
$x_2 = -1$.

Xcheck:

$$\begin{array}{c|c} & \begin{bmatrix} 2 \\ 3 \\ -1 \end{bmatrix} \\ \hline \begin{bmatrix} 2 & 1 & -2 \\ 0 & 3 & 1 \\ 1 & 0 & 2 \end{bmatrix} & \begin{matrix} 2 \\ 1 \\ 0 \end{matrix} \end{array} \quad \checkmark$$

Find Pivot element by scanning unused rectangle column-wise for a non-zero element.

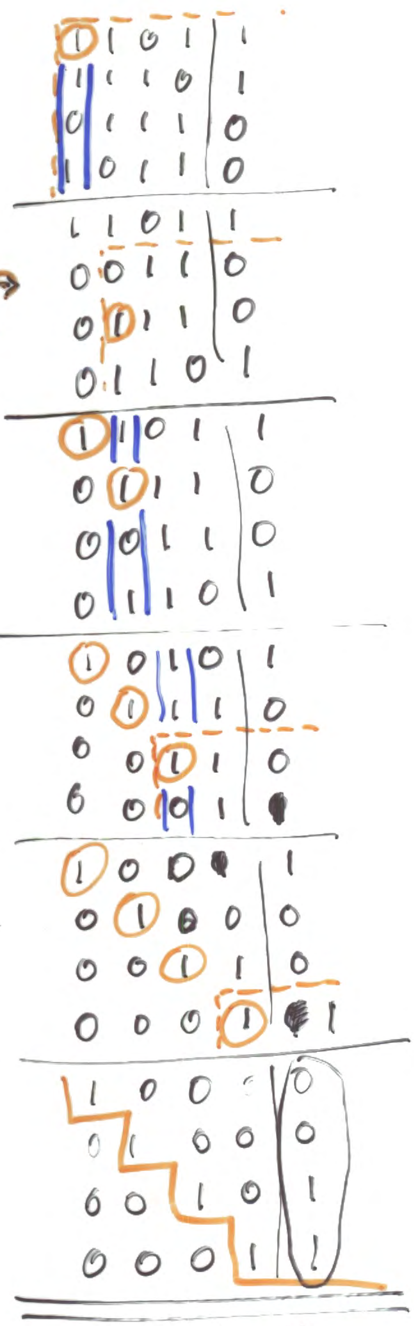
Swap rows to have the Pivot element as high as possible.

Scale row to have Pivot element equal 1.

Add multiples of the Pivot row to the other rows to make Pivot column a unit vector.

Bos-brico 15.11.13 (9)

1.1 (i)



We read off:

$x_0 = 0$

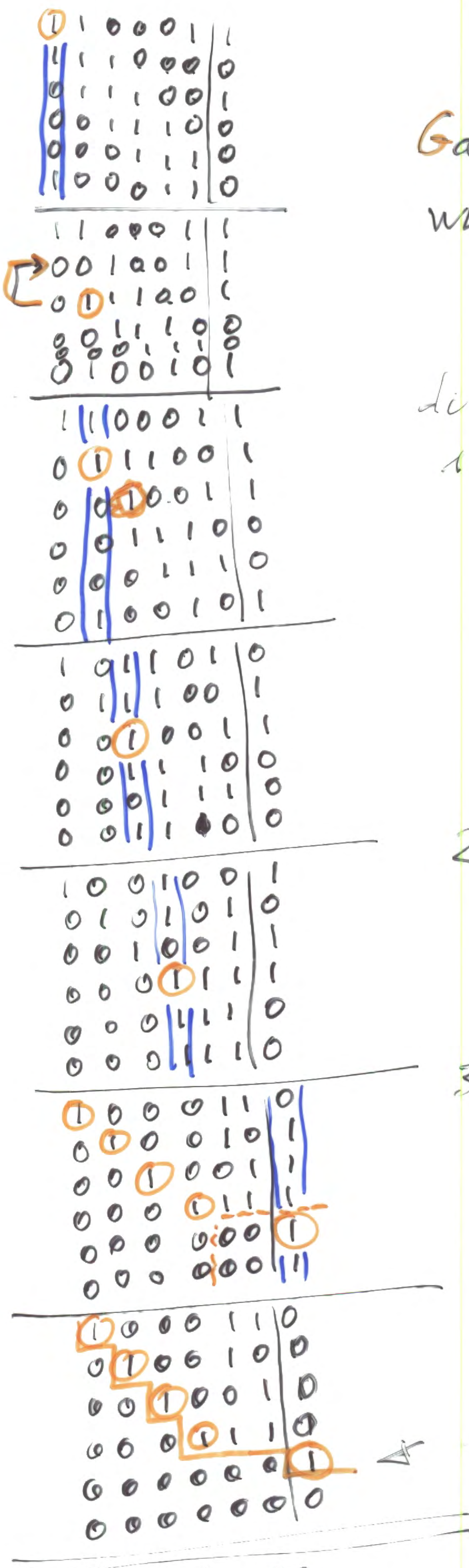
$x_1 = 0$

$x_2 = 1$

$x_3 = 1$

i.e. switch lamps 3 and 4.

1.1 (ii)



We read off:
system has no solution because of that row.

Gauß-Jordan:

While something non-zero remains below and right of last Pivot
do

1. Find the "first" non-zero (invertible) element ~~and~~ swap rows to bring it into the row below the previous Pivot
2. Scale Pivot row to make the Pivot element equal to 1.
3. Subtract(add) the Pivot row to the other rows in order to make the Pivot column a unit vector

So solving in general just does this:

$$\left\{ M = \begin{bmatrix} \ddots & & \\ & \ddots & \\ & & \ddots \end{bmatrix}, \quad s \text{ is the starting state.} \right\}$$

Bus brico 15.10.13 (10)

- Set up M and s
- Solve $Mx = s$ using the Gauß-Jordan-alg. on $(M|s)$. $O(n^3)$
- Read off the solution(s).

Observation

If the number n of lamps is a multiple of 3

then

$$x = 0 \quad \text{or} \quad x = \begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ \vdots \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ \vdots \end{bmatrix} \quad \text{or} \quad x = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ \vdots \end{bmatrix} \quad \text{or} \quad x = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ \vdots \end{bmatrix}$$

does nothing, i.e.

$$Mx = 0.$$

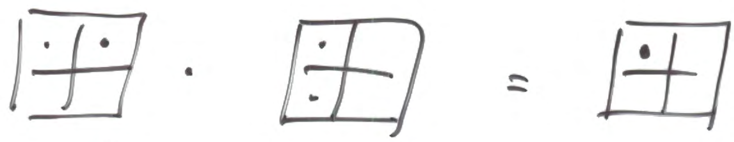
Thus: if $Mx = s$ has a solution it has (at least) four solutions.

Innsbruck
16.10.13
1

Matrix multiplication

Gaussian elimination, Gauß-Jordan take $O(n^3)$ operations in the ground field for an $n \times n$ system.

Volker Strassen (1969) Gaussian elimination is not optimal:



School method: need 8 operations of the blocks.
V. Strassen: can do with 7 ~~operations~~ multiplications without changing order of multiplication.

Use that recursively!

for $2^k \times 2^k$ matrices instead of 8^k we can do with 7^k multiplications

ie. in total, based on $n = 2^k$, we need

$$O(n^{\log_2 7})$$

$$7^k = 2^{k \log_2 7} = n^{\log_2 7}$$

$$\log_2 7 = 2.81\ldots < 2.83.$$

Can do matrix multiplication with $O(n^{2.83})$ op's.

Current (almost) record:

Coppersmith & Winograd (1990): $O(n^{2.38})$

<u>Conjecture</u> Can do it in $O(n^{2+\varepsilon})$ for any $\varepsilon > 0$.

Bus-brico
16.10.13
②

How to read off solutions after Gauß-Jordan?

Say Gauß-Jordan has produced the following strong echelon form:

$$\underbrace{\begin{bmatrix} 0 & 1 & 2 & -3 & 0 & 2 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}}_{=:A} x = \begin{bmatrix} 3 \\ 2 \\ 1 \\ 0 \end{bmatrix} \quad \text{over } \mathbb{F}_7 .$$

⚠ **WARNING:** Expansion only works correctly after Gauß-Jordan.

How to "read off" the set of solutions?

We perform "<u>expansion</u>":

$$\begin{array}{l} \left[\begin{array}{ccccccccc|c} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & -3 & 0 & 2 & 0 & 0 & -1 & 3 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \end{array}\right] \end{array} \begin{array}{l} \leftarrow \text{no Pivot in col 0, so add this row.} \\ \leftarrow \text{copy of row with Pivot in col 1.} \\ \leftarrow \text{add} \\ \leftarrow \text{add} \\ \leftarrow \text{copy} \\ \leftarrow \text{add} \\ \leftarrow \text{add} \\ \leftarrow \text{copy} \\ \leftarrow \text{add} \end{array}$$

(all) homogeneous solutions — a special solution

Claim:
(i) The rhs of the expanded matrix is a solution x_0 to the original system.

(ii) Each -1 column x_i of the expanded matrix is a solution of the homogeneous system.

(iii) Any solution of $Ax = s$ is of the form

$$x = x_0 + \sum_{i \text{ non-Pivot}} \alpha_i x_i \quad \text{with } \alpha_i \in \text{groundfield.}$$

Linear algebra happens where?

$\rightarrow$ Vector spaces.

A vector space is ...

V, set,

$+ : V \times V \to V$, addition,

$\cdot : F \times V \to V$ scalar multiplication

where F is a field and the following rules hold:

PANIC^{+}. (i.e. ~~addition~~ $(V,+)$ is a commutative group)

$\text{PAN}^{\cdot}$

$1 \cdot v = v$

$\alpha \cdot (\beta \cdot v) = (\alpha \cdot \beta) \cdot v$ for all $\alpha, \beta \in F$, $v \in V$

D

$(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$

$\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$

Simplest examples of vector spaces: $V = F^n$

with componentwise addition and scalar mult.

Another example: $V = F[x]$

or $V = F[x] / (x^2 + x + 1) \cong F^2$

in particular:

$$\mathbb{F}_2[x] / (x^2 + x + 1) =: \mathbb{F}_4 .$$

or $V = \mathbb{C}$ over $F = \mathbb{R}$.

$$\mathbb{C} = \mathbb{R}[x] / (x^2 + 1)$$

Fundamental theorem on vector spaces:

Bus-brico
16.10.13
4

Every vector space has a basis, and any two bases are of the same size (cardinality).

Def A basis B is a subset $B \subset V$ of V such that

(1) B is linearly independent, ie. if $\sum_{b \in B} \alpha_b b = 0$ then $(\alpha_b)_b = 0$.

(2) B is generating; ie. for every $v \in V$ there exist $(\alpha_b)_b \in F^n$ such that $v = \sum_{b \in B} \alpha_b b$.

Fact $B \subset V$ is a basis

iff B is maximally linearly independent

iff B is minimally generating.

Def The dimension of a vector space V is the size of some basis B:

$$\dim V := \# B .$$

Bustrico
16.10.13
5

Given a matrix $A \in \mathbb{F}^{m \times n}$.

It defines a map

$$f_A : \begin{array}{ccc} \mathbb{F}^n & \longrightarrow & \mathbb{F}^m \\ x & \longmapsto & A \cdot x \end{array}$$

and we define

$$\ker A = \ker f_A$$
$$:= \{ x \in \mathbb{F}^n \mid Ax = 0 \} \subset \mathbb{F}^n$$

$$\operatorname{im} A = \operatorname{im} f_A$$
$$:= \{ A x \mid x \in \mathbb{F}^n \} \subset \mathbb{F}^m$$

Notice:

- $\ker A$ is a vector space.
- $\operatorname{im} A$ is a vector space.

E.g. with the matrix $A \in \mathbb{F}_7^{4 \times 9}$ from the above example:

$$\ker A = \operatorname{span} \left\{ \begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -3 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 3 \\ 0 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 2 \\ -1 \end{bmatrix} \right\}$$

where $\operatorname{span} S := \{ \sum_{s \in S} \alpha_s s \mid \forall \alpha_s \in \mathbb{F} \}$.

$$\operatorname{im} A = \operatorname{span} \{ A_{\cdot 1}, A_{\cdot 4}, A_{\cdot 7} \} = \operatorname{span} \left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\}$$

In general, you take exactly those columns that became a Pivot-column in the Gauß-Jordan algorithm.

Bus-brico
16. 10. 13
⑥

Notice: by definition of "span S" the set S is a generating set for it.

Here, both generating sets are even linearly independent.

I.e.: $\dim \ker A = 6 = \#$ non-Pivot columns

$\dim \operatorname{im} A = 3 = \#$ Pivot columns

$\dim \ker A + \dim \operatorname{im} A = \#$ columns

<u>Theorem</u> $A \in F^{n \times m}$. Then

$$\dim \ker A + \dim \operatorname{im} A = m$$

<u>Exercise</u>

Let $A = \begin{bmatrix} 1 & 2 & 3 & 0 \\ 0 & 0 & 1 & 2 \\ 3 & -1 & 3 & 2 \end{bmatrix} \in \mathbb{F}_7^{3 \times 4}$.

① Solve $Ax = b_1$ and $Ax = b_2$ for $b_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}$, $b_2 = \begin{bmatrix} -1 \\ 3 \\ 1 \end{bmatrix}$.

② Determine $\ker A$ and $\operatorname{im} A$ and their dimensions.

$$\left[\begin{array}{cccc|cc} 1 & 2 & 3 & 0 & 2 & -1 \\ 0 & 0 & 1 & 2 & 1 & 3 \\ 3 & -1 & 3 & 2 & 0 & 1 \end{array}\right]$$

$$\left[\begin{array}{cccc|cc} 1 & 2 & 3 & 0 & 2 & -1 \\ 0 & 0 & 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & 2 & 1 & -3 \end{array}\right]$$

$$\left[\begin{array}{ccccc|c} 1 & 2 & 0 & 1 & -1 & -3 \\ 0 & 0 & 1 & 2 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$\begin{array}{cccccc} 1 & 2 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}$$

Expand with first rhs:

$$\begin{array}{ccccc} 1 & 2 & 0 & 1 & -1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{array}$$

Thus $\{Ax = b_1\}$

$$= \left\{ \begin{bmatrix} -1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \alpha \begin{bmatrix} 2 \\ -1 \\ 0 \\ 0 \end{bmatrix} - \beta \begin{bmatrix} 1 \\ 0 \\ 2 \\ -1 \end{bmatrix} \;\middle|\; \alpha, \beta \in \mathbb{F}_7 \right\}$$

~~Ker A =~~

and $\{Ax = b_2\} = \emptyset$.

$$\ker A = \operatorname{span}\left\{ \begin{bmatrix} 2 \\ -1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 2 \\ -1 \end{bmatrix} \right\}, \dim = 2$$

$$\operatorname{im} A = \operatorname{span}\left\{ \begin{bmatrix} 1 \\ 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix} \right\}, \dim = 2.$$

Bus-brico
16.10.13
8

Monty Hall Problem

- Candidate chooses one door.
- Then Monty Hall (the quizz master) opens one of the remaining doors and reveals a goat

- The candidate may now switch her choice or not.

What shall she do?

Determinants and matrix inverse

BUS-brico
16.10.13
9

Consider a square matrix $A \in \mathcal{F}^{n \times n}$.

Def

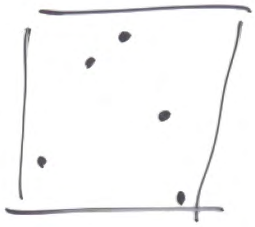
$$\det A := \sum_{\pi \in \mathcal{S}_n} (-1)^{\mathrm{sign}(\pi)} \prod_i A_{i,\pi(i)}$$

$\pi \in \mathcal{S}_n$ = permutations of $\{0, \dots, n-1\}$

$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$

runtime:

$\mathcal{O}(n \cdot n!)$

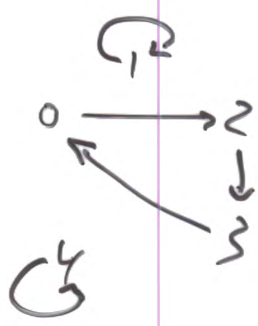


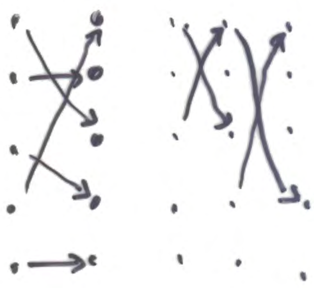
where $\mathrm{sign}(\pi) = \mathrm{parity}(\pi) :=$

$=$ (# swap's in any representation of π by swaps) mod 2.

e.g. π:
$0 \mapsto 2$
$1 \mapsto 1$
$2 \mapsto 3$
$3 \mapsto 0$
$4 \mapsto 4$.

$\pi = (0\ 2\ 3)\ (1)\ (4) = (0\ 2\ 3)$





~~take~~ ~~4~~ ~~3~~ $(0\ 3) \circ (0\ 2)$

$= (0\ 2\ 3) = \pi$

so the $\mathrm{parity}(\pi) = (\#\text{ swaps})$ ~~mem~~ mod 2 $= 2 \bmod 2 = 0$.

How to compute $\det A$
and what does it mean?

Properties

(1) $\det A$ invertible (non-zero) $\Leftrightarrow$ A invertible.

(i.e. does there exist B such that $A \cdot B = \mathbb{1}$ and $B \cdot A = \mathbb{1}$?).

(2) $\det \mathbb{1} = 1$

(3) $\det (AB) = \det A \cdot \det B$.

(4) if B is the matrix A with two rows swapped then $\det B = -\det A$.

(5) if B is the matrix A with one row scaled by a scalar α then

$$\det B = \alpha \cdot \det A.$$

(6) if B is the matrix A with some row replaced by itself plus a multiple of another then

$$\det B = \det A$$

Combining (4) – (6) and $\det \mathbb{1} = 1$, $\det$(any other strong row echelon square matrix) $= 0$, we may use the Gauß-Jordan-algorithm (or Gaussian elimination) to compute the determinant in $O(n^3)$ field operations.

Bus-brico
11.10.13
11

Let's do an example:

$$A = \begin{bmatrix} 3 & 2 & 1 & -1 \\ -2 & 0 & 0 & -3 \\ 2 & 3 & 1 & 0 \\ 0 & -2 & 1 & 3 \end{bmatrix} \in \mathbb{F}_7 = \{-3,-2,-1,0,1,2,3\}$$

Aim: compute $\det A$ and A^{-1}. ...

$A \cdot B = \mathbb{1}$

i.e. $A \cdot B_{\cdot i} = \mathbb{1}_{\cdot i}$ simultaneously for all i.

So just use $A|B$ as input to the Gauß-Jordan-algo.

So let's do it:

$$\left[\begin{array}{cccc|cccc} 3 & 2 & 1 & -1 & 1 & 0 & 0 & 0 \\ -2 & 0 & 0 & -3 & 0 & 1 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & -2 & 1 & 3 & 0 & 0 & 0 & 1 \end{array}\right]$$

divide row_1 by $\underline{3}$

$$\left[\begin{array}{cccc|cccc} 1 & 3 & -2 & 2 & -2 & 0 & 0 & 0 \\ 0 & -1 & 3 & 1 & 3 & 1 & 0 & 0 \\ 0 & -3 & -2 & 3 & -3 & 0 & 1 & 0 \\ 0 & -2 & 1 & 3 & 0 & 0 & 0 & 1 \end{array}\right]$$

divide row_1 by -1

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & -2 & 0 & 3 & 0 & 0 \\ 0 & 1 & -3 & -1 & -3 & -1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 2 & -3 & 1 & 0 \\ 0 & 0 & 2 & 1 & 1 & -2 & 0 & 1 \end{array}\right]$$

divide row_2 by 3

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & -2 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 0 & 3 & -1 & -2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 3 & -3 & 1 \end{array}\right]$$

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & -3 & 3 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 3 & -2 & 1 \\ 0 & 0 & 1 & 0 & 3 & -1 & -2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 3 & -3 & 1 \end{array}\right]$$

Thus

$$\det A = 3 \cdot (-1) \cdot 3 = -2.$$

and

$$A^{-1} = \begin{bmatrix} -3 & 3 & 1 & 2 \\ 1 & 3 & -2 & 1 \\ 3 & -1 & -2 & 0 \\ 2 & 3 & -3 & 1 \end{bmatrix}.$$

$$\text{prob}(\text{random } A \text{ invertible}) = \prod_{i=1}^{4} (1 - 7^{-i}) = \frac{6}{7} \cdot \frac{48}{49} \cdot \frac{342}{343} \cdot \frac{2400}{2401} = 0.8368\ldots < \frac{6}{7} = 0.857\ldots$$

```
[d,B]:=gaussjordan(A,MZ7(op(linalg::matdim(A)),(i,j)->if i=j then 1
else 0 end_if)):
Starting.
```

$$\begin{pmatrix} 3 & 2 & 1 & -1 & 1 & 0 & 0 & 0 \\ -2 & 0 & 0 & -3 & 0 & 1 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & -2 & 1 & 3 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Scaling row 1 by -2.

$$\begin{pmatrix} 1 & 3 & -2 & 2 & -2 & 0 & 0 & 0 \\ -2 & 0 & 0 & -3 & 0 & 1 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & -2 & 1 & 3 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Pivoting column 1.

$$\begin{pmatrix} 1 & 3 & -2 & 2 & -2 & 0 & 0 & 0 \\ 0 & -1 & 3 & 1 & 3 & 1 & 0 & 0 \\ 0 & -3 & -2 & 3 & -3 & 0 & 1 & 0 \\ 0 & -2 & 1 & 3 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Scaling row 2 by -1.

$$\begin{pmatrix} 1 & 3 & -2 & 2 & -2 & 0 & 0 & 0 \\ 0 & 1 & -3 & -1 & -3 & -1 & 0 & 0 \\ 0 & -3 & -2 & 3 & -3 & 0 & 1 & 0 \\ 0 & -2 & 1 & 3 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Pivoting column 2.

$$\begin{pmatrix} 1 & 0 & 0 & -2 & 0 & 3 & 0 & 0 \\ 0 & 1 & -3 & -1 & -3 & -1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 2 & -3 & 1 & 0 \\ 0 & 0 & 2 & 1 & 1 & -2 & 0 & 1 \end{pmatrix}$$

Scaling row 3 by -2.

$$\begin{pmatrix} 1 & 0 & 0 & -2 & 0 & 3 & 0 & 0 \\ 0 & 1 & -3 & -1 & -3 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 & -1 & -2 & 0 \\ 0 & 0 & 2 & 1 & 1 & -2 & 0 & 1 \end{pmatrix}$$

Pivoting column 3.

$$\begin{pmatrix} 1 & 0 & 0 & -2 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 0 & 3 & -1 & -2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & -3 & 1 \end{pmatrix}$$

Pivoting column 4.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -3 & 3 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 3 & -2 & 1 \\ 0 & 0 & 1 & 0 & 3 & -1 & -2 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & -3 & 1 \end{pmatrix}$$

Completed. det(A)= -2.

Bus-brico
17.10.13
1

A steep introduction to probabilities

„What is a random bit? 0? 1?"

1. Events

to make it easier!

A **universe** Ω is a finite set of possible outcomes of an experiment.

An **event** A is just a subset of Ω, $A \subset \Omega$.

Rules: $\text{prob}(\emptyset) = 0$, $\text{prob}(\Omega) = 1$,

$$\text{prob}(A \,\dot\cup\, B) = \text{prob}\,A + \text{prob}\,B.$$

where $A \,\dot\cup\, B$ means ~~that~~ $A \cup B$ and that $A \cap B = \emptyset$.

Consequence:

$$\text{prob}(\Omega \setminus A) = 1 - \text{prob}\,A$$

⌜ $A \,\dot\cup\, (\Omega \setminus A) = \Omega$ and thus

$$\text{prob}\,A + \text{prob}(\Omega \setminus A) = \text{prob}(\Omega) = 1. \lrcorner$$

$$\text{prob}(A \cup B) = \text{prob}\,A + \text{prob}\,B - \text{prob}(A \cap B).$$

Conditional probabilities

with non-zero probability

Given that an event C occurred what is the probability for landing in A:

$$\text{prob}(A \mid C) = \frac{\text{prob}(A \cap C)}{\text{prob}\,C}.$$

Def A and B are **independent**

iff $\text{prob}(A \cap B) = \text{prob}\,A \cdot \text{prob}\,B$

iff $\text{prob}(A \mid B) = \text{prob}\,A$

uniform

Example Rolling a die: $\Omega := \{1,2,3,4,5,6\}$, $\text{prob}\,A := \frac{\#A}{\#\Omega}$.

$C = \{2,4,6\}$, $B = \{4,5,6\}$: $\text{prob}(B \mid C) = \frac{2}{3}$, $\text{prob}\,B = \frac{1}{2}$. Not independent.

$A = \{1,2\}$: $\text{prob}(A \mid C) = \frac{1}{3}$, $\text{prob}\,A = \frac{1}{3}$. A and C

Bus-brico
17.10.13
2

2. Random variables

Def A <u>random variable</u> X is a function on the universe Ω with possible outcomes in some set S and we assume that we know its distribution:

$$\begin{aligned} S &\longrightarrow \mathbb{R} \cap [0,1] \\ x &\longmapsto \operatorname{prob}(X = x) \\ &\qquad\quad \shortparallel \\ &\quad \operatorname{prob}(\{\omega \in \Omega \mid X(\omega) = x\}) \end{aligned}$$

Property of a distribution: $\displaystyle\sum_{x \in S} \underbrace{\operatorname{prob}(X = x)}_{} = 1.$

Def Two random variables X and Y are <u>independent</u>

iff $\forall x \in \operatorname{im} X,\ y \in \operatorname{im} Y:$

$$\operatorname{prob}(X = x \wedge Y = y) = \operatorname{prob}(X = x) \cdot \operatorname{prob}(Y = y)$$

Example

X = rolling a fair die,

thus we set: $\operatorname{prob}(X=1) = \frac{1}{6}$, $\operatorname{prob}(X=2) = \frac{1}{6}, \ldots, \operatorname{prob}(X=6) = \frac{1}{6}$.

Y = rolling a forged die,

thus we set: $\operatorname{prob}(Y=1) = \frac{1}{10}, \ldots, \operatorname{prob}(Y=5) = \frac{1}{10}$,

$$\operatorname{prob}(Y=6) = \frac{1}{2}.$$

And we may require that X, Y are independent!

Now we can ask $\operatorname{prob}(X + Y > 10) = ?$ $\frac{11}{60}$ 4

Here: $\operatorname{prob}(X+Y>10) = \operatorname{prob}(X=5, Y=6) + \operatorname{prob}(X=6, Y=5) + \operatorname{prob}(X=6, Y=6) =$ [illegible]

Ex 3.5

Bus-Enrico
17.10.13
3

Introduce random variables

$$X_i = \begin{cases} 1 & \text{if the door opens at ~~the~~ hour } i \\ 0 & \text{else.} \end{cases}$$

We assume

$$\text{prob}(X_i = 1) = p, \quad \text{prob}(X_i = 0) = 1-p.$$

and

they are all independent.

Define

$N :=$ # ~~rounds~~ hours until we exit.

Now, that is defined by:

$$N = i \;:\Longleftrightarrow\; X_1 = 0 \wedge X_2 = 0 \wedge \dots \wedge X_{i-1} = 0 \wedge X_i = 1.$$

So we obtain

$$\begin{aligned} \text{prob}(N=i) &= \text{prob}(X_1 = 0 \wedge X_2 = 0 \wedge \dots \wedge X_{i-1} = 0 \wedge X_i = 1) \\ &= \text{prob}(X_1 = 0) \cdot \text{prob}(X_2 = 0) \cdot \ldots \cdot \text{prob}(X_{i-1} = 0) \cdot \text{prob}(X_i = 1) \\ &= (1-p) \cdot (1-p) \cdot \ldots \cdot (1-p) \cdot p \\ &= (1-p)^{i-1} \cdot p \end{aligned}$$

What is the expected number of hours until exit?

<u>Def</u> Given a (finite) random variable Z with real values. Then its expected value is defined to be

$$E(Z) := \sum_{z \in \text{im } Z} z \cdot \text{prob}(Z = z)$$

Bus-brico
17.10.13
④

So we can use for $E(N)$:

$$E(N) = \sum_{i \in \mathbb{N}'} i \cdot prob(N = i)$$

$$= \sum_{i \geq 1} i \cdot (1-p)^{i-1} \cdot p \quad ;$$

we neglect the technicality that we should only consider finitely many r.v. !

Analysis tells us:

$$\sum_{i \geq 0} x^i = \frac{1}{1-x} \quad \text{for } |x| < 1.$$

$\boxed{\text{geometric series}}$

⌜Recall: $(1-x) \sum_{0 \leq i < n} x^i = 1 - x^n$. ⌟

Further, we may take derivates "under" the sum as long as convergence is nice (absolute):

Thus:

$$\sum_{i \geq 1} i x^{i-1} = \frac{1}{(1-x)^2}.$$

Plug in $x = 1-p$:

$$E(N) = \frac{1}{(1-(1-p))^2} \cdot p = \frac{1}{p}.$$

Since $prob(N \geq i) \longrightarrow 0$ with $i \to \infty$ the technicality is no problem.

Ex 3.2

Bus-brico
17.10.13
5

introduce random variables:

$$B = \begin{cases} 1 & \text{if the person is british} \\ 0 & \text{otherwise} \end{cases}$$

$$H = \begin{cases} 1 & \text{if .... eats ham for breakfast} \\ 0 & \text{otherwise} \end{cases}$$

with

$$\text{prob}(B=1) = 0.6 \rightsquigarrow \text{prob}(B=0) = 0.4$$

$$\text{prob}(H=1 \mid B=1) = 0.75$$
$$\text{prob}(H=1 \mid B=0) = 0.25$$

We are looking for:

$$\text{prob}(B=1 \mid H=1) = ?$$

We compute:

$$\text{prob}(H=1 \wedge B=1) = \text{prob}(H=1 \mid B=1) \cdot \text{prob}(B=1) = 0.75 \cdot 0.6$$

$$\text{prob}(H=1 \wedge B=0) = 0.25 \cdot 0.4$$

$$\text{prob}(H=1) = \text{prob}(H=1 \wedge B=1) + \text{prob}(H=1 \wedge B=0) = 0.75 \cdot 0.6 + 0.25 \cdot 0.4$$

Want:

$$\text{prob}(B=1 \mid H=1) = \frac{\text{prob}(B=1 \wedge H=1)}{\text{prob}(H=1)}$$

$$= \frac{0.75 \cdot 0.6 \; \cancel{+ 0.25 \cdot 0.4}}{0.75 \cdot 0.6 + 0.25 + 0.4}$$

$$= 0.81\ldots$$

Foundations of informatics — a bridging course
Fall 2013
Mathematical tools
MICHAEL NÜSKEN

2. A network problem

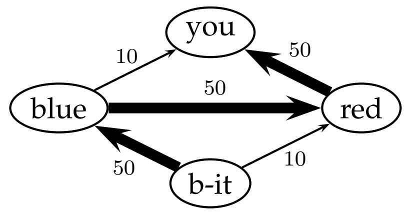


Figure 2.1: Network

Consider a streaming application over the bufferless network in Figure 2.1. We want to transmit a movie through the network from b-it to you. The numbers at the edges indicate how many MBit/sec may be transported over that connection. In order to do that the film is split into small packets. Note that a larger bandwidth can also be used to lower the average time for transmitting a packet over it. There are two important aspects:

(V) The data sent out from a node must always be equal (and not less) to the data received. Otherwise, data would pile up at a node. For example, $f_{\text{b-it,blue}} = f_{\text{blue,red}} + f_{\text{blue,you}}$, where $f_{x,y}$ denotes the flow from node x to node y, that is, the number of packets transmitted. (Note that there is a flow f 'into' the node b-it and a corresponding flow f out of the node you.)

(E) The time a specific packet needs must be almost constant regardless of its path through the network. Otherwise, the recipient machine would have too much work in reassembling the packets in the original order. (We assume that a little buffer space is available to smooth over variations in the network.) For example, $t_{\text{b-it,blue}} + t_{\text{blue,you}} = \text{totaltime}$, where $t_{x,y}$ is the time needed to transmit one packet from x to y. The total time must be the same for all connections.

This is very similar to an electronic current.

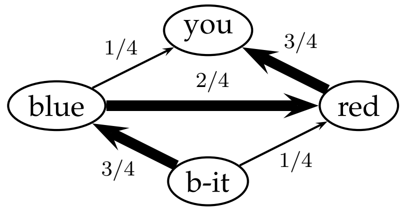


Figure 2.2: Relative flows

Exercise 2.1. (10 points)

(i) Set up a system of linear equations describing the entire system. $\boxed{4}$

(ii) Solve it and read off the flows. $\boxed{4}$

(iii) Determine the complete flow f. $\boxed{2}$

As a control of your results the resulting relative flows are given by Figure 2.2.

Foundations of informatics — a bridging course
Fall 2013
Mathematical tools
MICHAEL NÜSKEN

3. Probabilities

Exercise 3.1 (Randomness helps). (12+4 points)

Give examples where randomness

(i) decides about win or loose. $\boxed{2}$

(ii) helps simulating difficult reality. $\boxed{2}$

(iii) helps solving difficult finite problems. $\boxed{2}$

(iv) models errors. $\boxed{2}$

(v) makes decisions. $\boxed{2}$

(vi) hides secrets. $\boxed{2}$

(vii) Does something else which is interesting. $\boxed{+4}$

Exercise 3.2 (Conference breakfast). (5 points)

You are at a probability theory conference. 60% of the participants are British. 75% of the British eat ham at breakfast, yet only 25% of the others. This morning your table neighbour eats ham. What is the probability that she is British? $\boxed{5}$

Exercise 3.3 (Monty Hall Problem). (8 points)

We are guests in a game show and close to win a great fortune. The quiz master asks us to choose one of three (closed) doors. She explains that behind one of them awaits you a million Euros. Once you fixed your choice the quiz mastress opens one of the other doors and shows you that this was only a goat. She gives you a final chance: you may either retain your door or switch to the remaining closed one.

(i) Say door 3 is opened. Calculate the conditional probability that your door is the winning one given that the door 3 is a fail, and its complement. $\boxed{2}$

(ii) Calculate the unconditional probability that your door is the winning one, and its complement. $\boxed{1}$

What do you do? Reason! $\boxed{5}$

Exercise 3.4 (Prisoner's dilemma). (10 points)

A hundred prisoners are given a great opportunity. Some of them may make a day trip to the nearby theatre. Each of them can make one of two choices: either choose to join the trip or not to join the trip. All who want can see the piece, yet only unless all of them choose to go.

The prisoners cannot communicate with each other, all are equally selfish, and follow the same strategy. Strategy 0 is to choose not to go. Then nobody goes. Strategy 1 is to choose to go. Then nobody goes.

$\boxed{8}$ (i) Find a strategy that allows some of them to go.

$\boxed{2}$ (ii) Optimize the strategy so that the expected number of prisoners to see the show is larger than 94.5.

Exercise 3.5 (Random exit). (8 points)

You are trapped again in a locked room. Once every hour you have the chance to open the door. This succeeds with a certain probability p.

(i) What is the chance that you can leave the room after

$\boxed{0}$ (a) exactly one hour?

$\boxed{1}$ (b) exactly two hours?

$\boxed{1}$ (c) exactly three hours?

$\boxed{1}$ (d) exactly four hours?

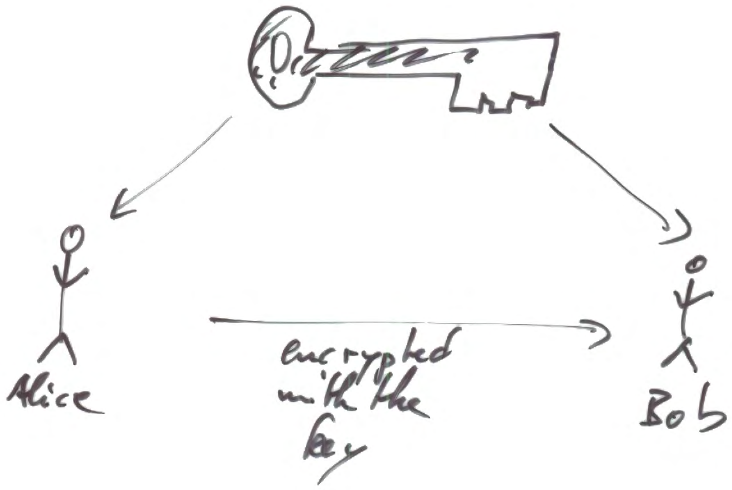
(ii) What is the expected number of hours that you have to stay

$\boxed{3}$ (a) ...by definition? [Give a formula.]

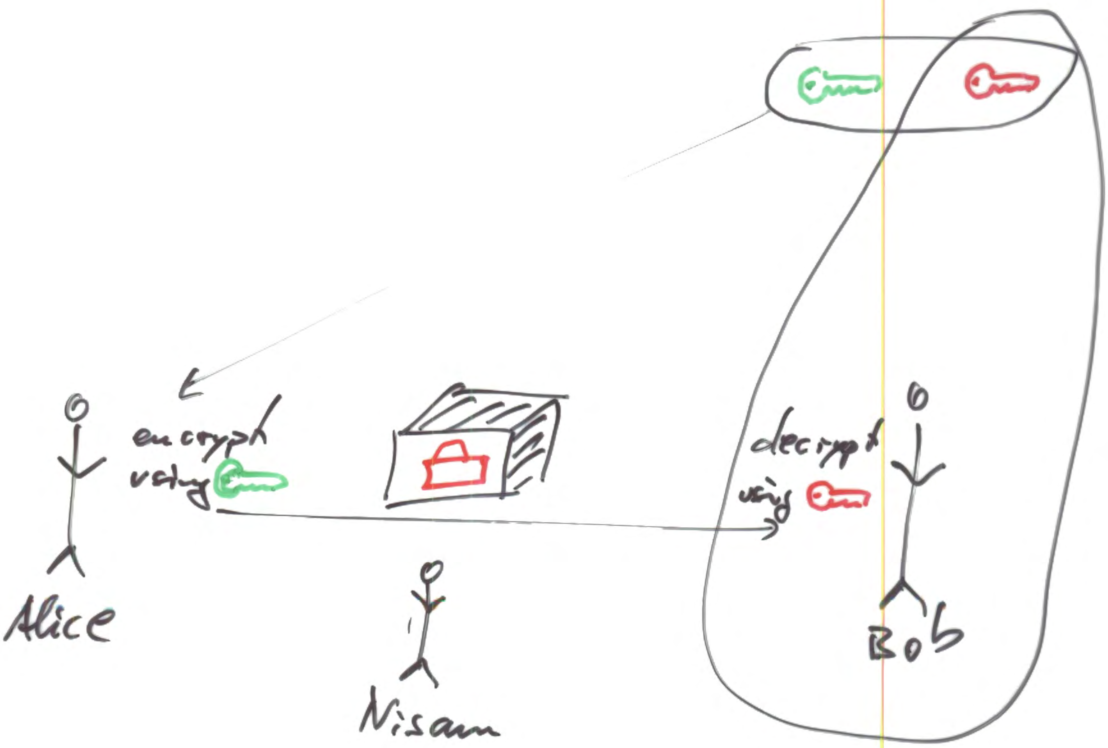
$\boxed{2}$ (b) ...by value? [Calculate!]

Set up a model (some random variables!) and use only the rules...

Classically:



New solutions: [1970-72 CESG @ British Secret Service]
1976 Diffie & Hellman
1978 Rivest, Shamir & Adleman: RSA



RSA

generate_keys

Input: security parameter $k \in \mathbb{N}$
Output: key pair

1. Generate a random prime p of about $\frac{k}{2}$ bits length. $O(k^4)$
2. Generate a random prime q of about $\frac{k}{2}$ bits length. $O(k^4)$
3. Compute $N := p \cdot q$. $O(k^2)$
4. Compute $L := (p-1)\cdot(q-1) = N - (p+q) + 1$. $O(k^2)$
5. Find two numbers $e, d \in \mathbb{Z}^{+}$ randomly, but subject to the condition that
$$0 < e, d < L$$
and
$$e \cdot d = 1 - t \cdot L \quad \text{for some } t \in \mathbb{Z}.$$
$O(k^2) \subset O(k^3)$
6. Return public key (N, e) and private key (N, d). and clear memory.

encrypt

Input: public key (N, e), message $x \in \mathbb{Z}_N = \{0, 1, \ldots, N-1\}$.
Output: ciphertext $y \in \mathbb{Z}_N$

1. Return $y := x^e$ in $\mathbb{Z}_N$. $O(k^3)$

decrypt

Input: private key (N, d) ciphertext $y \in \mathbb{Z}_N$
Output: message $z \in \mathbb{Z}_N$

1. Return $z := y^d$ in $\mathbb{Z}_N$. $O(k^3)$

Bus-brico
17.10.13
8

Todo

(0) Understand the algorithms.

(1) Correctness? Is $z = x$?

(provided (N,e), (N,d) is a key pair).

(2) Efficiency?

Is everything reasonably fast?

(3) Security?

Integers modulo N

Let $N \in \mathbb{N}_{\geq 2}$.

$\mathbb{Z}_N$: $\{0, 1, 2, \dots, N-1\}$,

$+ : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$, $(x,y) \longmapsto (x +_{\mathbb{Z}} y) \bmod N$

$\cdot :$ $(x,y) \longmapsto (x \cdot_{\mathbb{Z}} y) \bmod N$

Rules: $\left.\begin{array}{l} \text{PANIC}^+ \\ \text{PANIC}^{\cdot} \\ \text{DØNT} \end{array}\right\}$ commutative ring with 1.

Implementation runtimes?

runtime $+$: $O(k)$

runtime $\cdot$: $O(k^2)$ using school method

We can do better:

Karatsuba : use $(x_1 \cdot 2^\beta + x_0)(y_1 2^\beta + y_0)$

$= (x_1 y_1) \cdot 2^{2\beta} + (\underset{\overset{\shortparallel}{(x_1+x_0)(y_1+y_0) - x_1y_1 - x_0y_0}}{\underline{x_1 y_0 + x_0 y_1}}) 2^\beta + x_0 y_0$.

runtime $O(k^{\log_2 3})$

Even better:

Schönhage & Strassen (1971): $O(k \cdot \log k \cdot \log\log k)$ op's. FFT

Bus-brico
17.10.13
9

<u>Theorem</u> (Division with remainder in $\mathbb{Z}$)

Given two integers $x, y \in \mathbb{Z}$, $y \neq 0$ then there exist (unique) integers $q, r \in \mathbb{Z}$ such that

$$x = q \cdot y + r$$

and

$$0 \leq r < |y|.$$

we define

$$x \text{ rem } y := r \in \mathbb{Z}$$

$$x \text{ quo } y := q \in \mathbb{Z}$$

$$x \bmod y := [\mathbb{Z}_y]\, r \in \mathbb{Z}_y .$$

Note that the theorem implies that addition and multiplication in $\mathbb{Z}_N$ are properly def'd.

For the proving the rules, let's consider a example:

A$\cdot$: Give $x, y, z \in \{0, 1, 2, \ldots N-1\}$.

$$(x \cdot y) \cdot z \qquad x\,y \text{ quo } N$$

$$= (x \mathbin{\dot{\mathbb{Z}}} y - q \cdot N) \mathbin{\dot{\mathbb{Z}}} z - \hat{q} \cdot N \qquad \in \underline{\underline{\{0, \ldots N-1\}}}.$$

$$= (x \mathbin{\dot{\mathbb{Z}}} y) \mathbin{\dot{\mathbb{Z}}} z - (q \mathbin{\dot{\mathbb{Z}}} z + \hat{q}) \cdot N$$

$$\overset{A\dot{\mathbb{Z}}}{=} x \mathbin{\dot{\mathbb{Z}}} (y \mathbin{\dot{\mathbb{Z}}} z) - \tilde{q} \cdot N$$

$$\vdots$$

$$= x \cdot (y \cdot z)$$

$\square$

Bus-brico
17.10.13
10

How to compute x^e in $\mathbb{Z}_N$?

The definition says

$$x^e = x^{e-1} \cdot x$$
$$= \underbrace{(\dots(((x \cdot x) \cdot x) \cdot x) \cdot \dots) \cdot x}_{e-1 \text{ multiplication.}}$$

But $e-1$ is much too large.

Let's try a very simple case: $e = 2^s$.

$x^{a \cdot b} = (x^a)^b$

$$x^e = x^{2^s} = (x^2)^{2^{s-1}} = \underbrace{(\dots((x^2)^2)^2 \dots)^2}_{s \text{ squarings.}}$$

That's only $O(\log e)$ op's, ie. $O(k)$ multiplication.

Write
$$e = \sum_{0 \le i < k} e_i 2^i .$$

Now

$x^{a+b} = x^a \cdot x^b$

$$x^e = \prod_{0 \le i < k} (x^{2^i})^{e_i} = \underbrace{\prod_{i : e_i = 1} x^{2^i}}$$

SQUARE & MULTIPLY

at most k factors, each factor needs at most k squarings. Even in total.

Each op in $\mathbb{Z}_N$!

$\rightarrow$ $O(k)$ multiplications are enough.

Example $x^{530} = x^{512+16+2} = x^{2^9} \cdot x^{2^4} \cdot x^2$ $512 = \underline{100001010}_2$

So compute: $x, x^2, x^{2^2}, x^{2^3}, x^{2^4}, x^{2^5}, x^{2^6}, x^{2^7}, x^{2^8}, x^{2^9}, x^{2^9+2^4}, x^{2^9+2^4+2}$.

Other option: $x, x^{10}, x^{100}, x^{1000}, x^{10000}, x^{100000}, x^{100001}, x^{1000010}, x^{10000100}, x^{10000101}, \dots$

square

How to perform step 5? ie.
How to find e, d such that

$$e \cdot d = 1 - t \cdot L$$

for some $t \in \mathbb{Z}$, $e, d \in \mathbb{N}_{<L}$.

We try:

1. Repeat
2. Pick $e \in_R \mathbb{N}_{<L}$ uniformly at random.
3. Try to find $d \in \mathbb{N}_{<L}$, $t \in \mathbb{Z}$ such $d \cdot e + t \cdot L = 1$.
4. Until successful.

Observe that

- we look for a linear combination of e and L.
- and we want that it is 1.

Note: 1 is very small, actually it's smallest positive integer.

Let's try to start more modestly:

Can we name linear combinations of e and L which are somehow "small" for a start?

Bus-brico
18.10.13
2

What s, t make $s \cdot e + tL$ modestly small:

s	t	$s \cdot e + t \cdot L$
1	0	e
0	1	L

To improve we could ...?

Let's consider an example:

$L = 60$ $\quad [= (7-1) \cdot (11-1)]$

$e = 17$

$r = s \cdot e + t \cdot L$	q	s	t	comment
$L = 60$		0	1	
$e = 17$	3	1	0	
9	1	-3	1	new $r = 60 - 3 \cdot 17 = 9$
8	1	4	-1	$4 \cdot e - 1 \cdot L = 8$
1	8	-7	2	$-7 \cdot e + 2 \cdot L = 1$
0		60	-17	

$$\begin{aligned} \text{new } r &= 60 - 3 \cdot 17 = 9 \\ &= (0 \cdot e + 1 \cdot L) - 3 \cdot (1 \cdot e + 0 \cdot L) \\ &= (0 - 3 \cdot 1) \cdot e + (1 - 3 \cdot 0) \cdot L \\ &= -3e + 1 \cdot L \end{aligned}$$

Xcheck 9

Xcheck! These are the numbers we started apart from one sign!

Ad: $60 \cdot e - 17 \cdot L = 0$

$$\begin{aligned} -7e + 2L &= 1 \\ 60e - 17L &= 0 \\ \hline 53e - 15L &= 1 \end{aligned}$$

Read off!

$-7 \cdot e + 2 \cdot L = 1$, i.e. $d = -7 + L$
$= 53$

→ (77, 17), (77, 53) is a RSA key pair

Bus-brico
18.10.13
3

Let's do another example:

$L = 60$

$e = 21$

r	q	s	t	
60		0	1	$60 = 0 \cdot e + 1 \cdot L$
21	2	1	0	$21 = 1 \cdot e + 0 \cdot L$
18	1	-2	1	
3	6	3	-1	
0		-20	7	

Xcheck: $-20 = -\frac{60}{3}$, $7 = \frac{21}{3}$

and $-20 \cdot e + 7 \cdot L = \frac{-60 \cdot e + 21 \cdot L}{3} = 0$

Notice that 3 divides both 60 and 21, and thus any linear combination $s \cdot 60 + t \cdot 21$. If we could find s, t so that we obtain 1, then we would that 3 divides 1. But that's wrong. Thus a solution cannot exist.

The above is called the

Extended Euclidean Algorithm.

(EEA)

Bvs-brico
18.10.13
4

EEA

Input: two values $a, b \in \mathbb{Z}$.

Output: $r, s, t \in \mathbb{Z}$

1. $r_0 = a$, $s_0 = 1$, $t_0 = 0$ // $r_0 = s_0 a + t_0 b$.
2. $r_1 = b$, $s_1 = 0$, $t_1 = 1$ // $r_1 = s_1 a + t_1 b$.
3. $i = 1$.
4. While $r_i \neq 0$ do
5. $\quad q_i = r_{i-1}$ quo r_i. Division with remainder
6. $\quad r_{i+1} = r_{i-1} - q_i r_i$.
7. $\quad s_{i+1} = s_{i-1} - q_i s_i$.
8. $\quad t_{i+1} = t_{i-1} - q_i t_i$.
9. $\quad$ increment i.
10. $e := i - 1$.
11. Return (r_e, s_e, t_e).

Addon: to save memory take indices modulo 3.

Exercise

Run the EEA for inputs:

(i) 30, 83.

(ii) 33, 21.

Bus-brico
18.10.13
5

30		0	1
83	0	1	0
30	2	0	1
23	1	1	-2
7	3	-1	3
2	3	4	-11
1	2	-13	36
0		30	-83

Xcheck: ok ✓

$-13 \cdot 83 + 36 \cdot 30 = 1$

33		0	1
21	1	1	0
12	1	-1	1
9	1	2	-1
3	3	-3	2
0		11	-7

Xcheck: $11 = \frac{33}{3}$, $7 = \frac{21}{3}$: ok.

$-3 \cdot 21 + 2 \cdot 33 = 3$.

No solution for "$= 1$".

Bus-brico
8.10.13
6

Fact For all i we have

- $r_i = s_i a + t_i b$
- $r_{i-1} = q_i r_i + r_{i+1}$
- and $0 \le r_{i+1} < |r_i|$ } division with remainder

□

Remark The EEA only requires that the domain is a comm. ring with 1 that allows a division with remainder.

Lemma For $i \ge 3$ we have $|r_{i+1}| \le \frac{1}{2} |r_{i-1}|$.

Proof: Exercise. □

Corollary EEA is fast!

Ie: $\ell \le 2 \max\{\lceil \log_2 |a| \rceil, \lceil \log_2 |b| \rceil\} + 2$,

runtime (EEA | $\mathbb{Z}$) $\in \mathcal{O}(k^3)$.

Pf

$$1 \le |r_\ell| = \frac{1}{2^{\lfloor \ell/2 \rfloor - 1}} \underbrace{|r_{\ell - 2(\lfloor \ell/2 \rfloor - 1)}|}_{\le \max\{|a|, |b|\}}$$

$$2^{\lfloor \ell/2 \rfloor - 1} \le \max\{|a|, |b|\}$$

$$\ell \le 2 \log_2 \max\{|a|, |b|\} + 2.$$

□

Actually, runtime $\in \mathcal{O}(k^2)$.

Def Given two numbers a, b, a greatest common divisor d is a number that fulfills

(i) $d \mid a \wedge d \mid b$ (d is a common divisor)

(ii) if $c \mid a \wedge c \mid b$ then $c \mid d$. (in particular $|c| \le |d|$).

Fact

(i) $\gcd(r_{i+1}, r_i) = \gcd(r_i, r_{i-1})$

(ii) $\gcd(a, b) = \ldots = \gcd(r_e, 0) = r_e$

In other words: the EEA computes the greatest common divisor r and a representation of it: $r = sa + tb$. (Bézout equation).

Theorem

The EEA computes in time $O(k^3)$ for two input k-bit numbers a, b "their" greatest common divisor r and two numbers s, t such that

$$r = sa + tb. \quad \text{(Bézout)}$$

Corollary

If the EEA finds $r \neq \pm 1$ then the equation $sa + tb = 1$

has no solution.

Otherwise the Bézout equation is one solution.

Pf $g := \gcd(a,b) = r_e \neq \pm 1$.

Assume $sa + tb = 1$ for some s, t.

Then $g \mid a$, $g \mid b$ so $g \mid sa + tb$, ie. $g \mid 1$.

But then $g = \pm 1$ ↯.

∎

Bus-brico
18.10.13
8

Let's consider

$$\mathbb{Z}_N^\times := \{ x \in \mathbb{Z}_N \mid \underbrace{\exists y \in \mathbb{Z}_N : xy = 1}_{x \text{ is invertible}} \text{ in } \mathbb{Z}_N \}$$

Is $(\mathbb{Z}_N^\times, \cdot)$ nice?

Theorem $(\mathbb{Z}_N^\times, \cdot)$ is commutative group.

Pf P: Let $x_1, x_2 \in \mathbb{Z}_N^\times$, say $x_1 y_1 = 1$, $x_2 y_2 = 1$.

Then $(x_1 x_2)(y_2 y_1) = x_1 \cdot 1 \cdot y_1 = 1$.

So multiplication is properly defd.

A: ✓

N: Is $1 \in \mathbb{Z}_N^\times$? Yes: $1 \cdot 1 = 1$.

I: Let $x \in \mathbb{Z}_N^\times$, say $xy = 1$ with $y \in \mathbb{Z}_N$.

Then $yx = 1$ and so $y \in \mathbb{Z}_N^\times$.

C: ✓ □

Another description:

$$\mathbb{Z}_N^\times = \{ x \bmod N \in \mathbb{Z}_N \mid x \in \mathbb{Z} \text{ and } \exists y \in \mathbb{Z}, t \in \mathbb{Z} : xy + tN = 1 \}$$

EEA

$$= \{ x \bmod N \in \mathbb{Z}_N \mid x \in \mathbb{Z},\ 0 \le x < N,\ \gcd(x, N) = 1 \}$$

Bus-brico
18.16.13
9

First examination:

- Assume $N = p$ prime. Determine $\# \mathbb{Z}_p^\times$:

$$\# \mathbb{Z}_p^\times = p - 1.$$

In other words: all elements of $\mathbb{Z}_p$ but 0 have a multiplicative inverse in this case.

Or: $\mathbb{Z}_p$ is a <u>field</u>!

(And we may use the EEA to ~~find~~ compute inverses!)

- Assume $N = p \cdot q$ an RSA number with p, q prime.

Then

$$\# \mathbb{Z}_N^\times = (p-1)(q-1) = L.$$

Well:

$$\mathbb{Z}_N \setminus \mathbb{Z}_N^\times = \{ a \cdot p \mid 0 \leq a < q \} \cup \{ b \cdot q \mid 0 \leq b < p \}$$

so

$$\#(\mathbb{Z}_N \setminus \mathbb{Z}_N^\times) = q + p - 1.$$

or

$$\# \mathbb{Z}_N^\times = pq - (q+p) + 1 = (p-1)(q-1).$$

Bus-brico
18.10.13
10

When considering repeated multiplication in a finite group, like $\mathbb{Z}_N^\times$, we immediately observe that the sequence

$$1,\ x,\ x^2,\ x^3,\ x^4,\ \ldots$$

must have collisions ~~at least~~ when reaching $x^{\#\mathbb{Z}_N^\times}$.

Thus $$x^\alpha = x^\beta \quad \text{for some } 0 \le \alpha < \beta \le \#\mathbb{Z}_N^\times$$

and so $$x^{\beta-\alpha} = 1.$$

Thus necessarily $$x^{(\#\mathbb{Z}_N^\times)!} = 1$$

even $$x^{\operatorname{lcm}(1,2,3,\ldots\#\mathbb{Z}_N^\times)} = 1.$$

But much more is true:

Theorem (Lagrange)

Given a finite group G.
Then for any element $x \in G$ we have
$$x^{\#G} = 1.$$

Pf in case G is commutative:

13us-brico
18.10.13
(14)

Consider a list of all elements of G:

L: $x_0, x_1, x_2, \dots, x_{k-1}$

where $k = \# G$. Now, multiply each element by x:

xL: $xx_0, xx_1, xx_2, \dots, xx_{k-1}$.

Claim: The lists L and xL are equal up to order.

Any two of the following three observations prove this:

1. There are k elements in the second list.
2. The elements of xL are pairwise different.
3. Any element of G occurs in xL.

Eg. 2: if $xx_i = xx_j$ then $x_i = x_j$ (because G is a group) and so $i = j$ because L has only different elements.

Now:

$$\prod_{y \in L} y \overset{\text{due to general associativity and commutativity}}{=} \prod_{y \in xL} y$$

$$\prod_{y \in L} y = x_0 \cdot \ldots \cdot x_{k-1}$$

$$\prod_{y \in xL} y = xx_0 \cdot xx_1 \cdot \ldots \cdot xx_{k-1} = x^k \cdot (x_0 \cdot \ldots \cdot x_{k-1}).$$

Thus

$$1 = x^k$$

with $k = \# G$.

$\square$

Corollary (Theorem of Euler)

Given $N \in \mathbb{N}_{\geq 2}$. Then for any $x \in \mathbb{Z}_N^\times$ we have

$$x^{\varphi(N)} = 1 \quad \text{in } \mathbb{Z}_N$$

where $\varphi(N) = \# \mathbb{Z}_N^\times$

Pf Just take $G = \mathbb{Z}_N^\times$ in the previous theorem. □

Fermat's little theorem

Given a prime p and $0 < x < p$. Then

$$x^{p-1} \equiv_p 1 .$$

$\equiv_p$: modulo p.

Pf Use the theorem of Euler for $N = p$ and note that $\# \mathbb{Z}_p^\times = p-1$. □

Now we can prove correctness of RSA, at least for most messages:

Take x invertible, ie. $x \in \mathbb{Z}_N^\times$.

(Notice that $\frac{\# \mathbb{Z}_N^\times}{\# \mathbb{Z}_N} = 1 - \frac{p+q-1}{pq} = (1-\frac{1}{p})(1-\frac{1}{q}) \sim 1.$)

Now:

$$z = y^d = (x^e)^d = x^{ed}$$

$$= x^{1-t\cdot L} = x \cdot (x^L)^{-t} \overset{\square}{=} x \cdot 1^{-t} = x.$$

and by the theorem of ~~Lagrange~~ Euler we know:

$$x^{\# \mathbb{Z}_N^\times} = 1 \quad \text{and also} \quad \# \mathbb{Z}_N^\times = L.$$

RSA is correct!!

13us-brico
18.10.13
13

Open: • how to find primes?
→ how to test a number for primality/compositeness?
→ how many prime numbers are there?
• Security?

Properties of primes:

• $\mathbb{Z}_N$ is a field iff N is prime.

• little Fermat: if $N=p$ is prime then $x^{p-1} \equiv_p 1$.

otherwise: $x^{N-1} \equiv_N 1$ may fail.

Now over a field the polynomial x^2-1 can have at most two roots, namely ± 1.

Now over $\mathbb{Z}_{pq}$ that polynomial has four roots!

Strong Fermat test.

To find a prime: pick a random number of the desired length and test it for primality. Repeat until found.

Exit probability? Prime Number Theorem

$$\frac{\pi(x)}{x} \sim \frac{1}{\ln x}$$

$$\frac{\log_2 e}{\log_2 2^k} = \frac{\log_2 e}{k} < \frac{2}{k}, \quad > \frac{1}{k}$$

$\mathcal{O}(k)$ iterations of $\mathcal{O}(k^3)$ work.

Bus-brico
18.10.13
(14)

Strong Fermat test (Miller; Rabin)

Input: a number $\ell \in \mathbb{Z}$ to be tested.

Output: a verdict: "ℓ is not prime."
or "ℓ may be prime"

0. Test ℓ for small factors $\longrightarrow$
1. Pick $x \in_R \mathbb{Z}_\ell \setminus \{0\}$ at random.
2. If $x \notin \mathbb{Z}_\ell^\times$, ie. $\gcd(a,\ell) \neq 1$
   then return "ℓ is not prime".
   (factor: $\gcd(a,\ell)$)
3. Write $\ell - 1 = \lambda \cdot 2^s$ with λ odd, $s \geq 1$.
4. Compute $b_0 = x^\lambda$ in $\mathbb{Z}_\ell$, $O(k^3)$
   $b_1 = b_0^2 = x^{\lambda 2}$, $b_2 = b_1^2 = x^{\lambda 2^2}$, ..., $b_s = x^{\lambda \cdot 2^s} = x^{\ell-1}$ in $\mathbb{Z}_\ell$.
5. If $b_s \neq 1$ then return "ℓ is not prime".
6. If $b_0 = 1$ then return "ℓ may be prime".
7. Say $b_t \neq 1$, $b_{t+1} = 1$.
   If $b_t \neq -1$ then return "ℓ is not prime".
   (proof: $b_t^2 \equiv_\ell 1$.)
   and also a factor can be given...
8. Return "ℓ may be prime".

Error probability = prob("ℓ may be prime" | ℓ composite)

$$\leq \frac{1}{4}.$$

Thus repeating ten times: error $\leq \frac{1}{4^{10}} \sim \frac{1}{10^6}$.

Bus-brico 18.10. B (15)

One last thing:

Chinese Remainder Theorem (CRT)

Assume $N = m_1 \cdot m_2$, $\gcd(m_1, m_2) = 1$.
Then

$$\varphi: \mathbb{Z}_N \xrightarrow{\simeq} \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$$

$$x \bmod N \longmapsto (x \bmod m_1,\ x \bmod m_2)$$

and this respects both addition and multiplication.

Example

$\mathbb{Z}_5^\times$

$\mathbb{Z}_3 \backslash \mathbb{Z}_5$	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

$\mathbb{Z}_3^\times$ $\mathbb{Z}_{15}^\times$

$$\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$$

Counterexample

$\mathbb{Z}_3 \backslash \mathbb{Z}_6$	0	1	2	3	4	5
0	0,6,12			3,9,15		
1		1,7,13			4,10,16	
2			2,8,14			5,11,17

$$\mathbb{Z}_{18} \not\simeq \mathbb{Z}_3 \times \mathbb{Z}_6$$

Corollary

$$\mathbb{Z}_N^\times \simeq \mathbb{Z}_{m_1}^\times \times \mathbb{Z}_{m_2}^\times$$

In particular, for $N = p \cdot q$ we get

$$L = \# \mathbb{Z}_N^\times = \# \mathbb{Z}_p^\times \cdot \# \mathbb{Z}_q^\times = (p-1) \cdot (q-1).$$

13us-bvi ro
18.10.13
16

How to find x such that

$$x \equiv_{m_1} a_1 \,, \qquad x \equiv_{m_2} a_2 \qquad ?$$

Observe that this is equivalent to finding

$$x \in \mathbb{Z}\,, \quad t_1 \in \mathbb{Z}\,, \quad t_2 \in \mathbb{Z}$$

such that

$$x = a_1 + t_1 \cdot m_1 \,, \qquad x = a_2 + t_2 \cdot m_2 .$$

In particular, we need

$$t_1 \cdot m_1 - t_2 \cdot m_2 = a_2 - a_1 .$$

Since m_1, m_2 are coprime the EEA gives s, t such that

$$s \cdot m_1 + t\, m_2 = 1.$$

and so

$$(a_2 - a_1)s \cdot m_1 - (a_1 - a_2)t \cdot m_2 = a_2 - a_1.$$

and

$$x = a_1 + (a_2 - a_1)s \cdot m_1$$
$$= a_2 + (a_1 - a_2)t \cdot m_2 .$$

That's easy and cheap. $O(\ell^2)$.

This proves that φ from the CRT is surjective and thus a bijection.

Bus-briro
18.10.13
17

One of things that we actually performed was this:

Say $x = 13 \in \mathbb{Z}_{29}$.

Compute x^{-1}.

To do that we have to solve

$$x \cdot y \equiv_{29} 1$$

ie.

$$x \cdot y + t \cdot 29 = 1$$

ie. we run $EEA(\overset{x}{\overset{\shortparallel}{13}}, 29)$.

29		0	1
13	2	1	0
3	4	-2	1
1	3	9	-4
0		-29 ✓	13 ✓

→ Xcheck passed :)

$$1 = 9 \cdot 13 + -4 \cdot 29.$$

modulo 29

$$1 \equiv_{29} 9 \cdot 13$$

So $13^{-1} = 9$ in $\mathbb{Z}_{29}$.