Lecture Notes

Foundations of informatics — a bridging course
Mathematical tools

Michael Nüsken

b-it

(Bonn-Aachen International Center
for Information Technology)

Fall 2009

©2009 Michael Nüsken

Foundations of informatics – a bridging course

9⁰⁰ – 16⁰⁰

Michael (Nüsken)

First task:

- Get a bit account.
- Send an email to nuesken@bit.uni-bonn.de from your bit account.

[Possibly: setup a forward!]

Foundations of informatics — a bridging course
Fall 2009
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 exactly all lights are on. (Maybe there's a cord that is hit by focussed light beams from the lamps, but it'll burn only...)

(i) Your particular room has 4 lamps, and the first and second are lit. [2]

(ii) Your room has 6 lamps, and the first and third are lit. [3]

(iii) Develop and describe a general procedure to escape. [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.

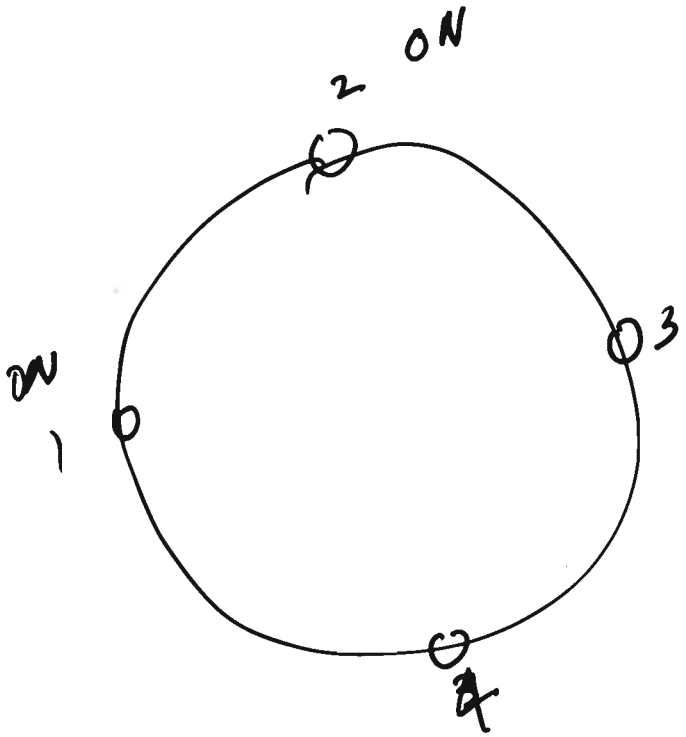
(i) Say $n = 3$, $m = 4$, and $v_1 = 2$, $v_2 = 3$, $v_3 = 7$. [3]

(ii) Say $n = 3$, $m = 5$, and $v_1 = 2$, $v_2 = 3$, $v_3 = 7$. [3]

(iii) Say $n = 4$, $m = 7$, and $v_1 = 2$, $v_2 = 5$, $v_3 = 11$, $v_4 = 3$. [4]

BriCo
13.10.09
(1)

(1)



Switch No 1

then No 4 ON

all other off

Switch No 2

then all are ON

Found by HIT and TRIAL

(2) Try to get 3 neighbouring lights off again and again until we are done...

(3) Jian's proposal

Zürich 13.10.09 (2)

- Replace each switch with a variable s_i, $i \in \{1,2,3,4\}$, which may have values in $\{0,1\}$.

OBSERVATION: Operating a switch twice is like doing nothing

- Replace each lamp's state with a variable which may have values in $\{-1,+1\}$.

Amine's addition:
Why not $\{0,1\}$ here as well?

- Describe final stages by expressions:

$+1 = +1 \cdot (-1)^{s_1+s_2+s_4}$ for lamp 1.

$+1 = +1 \cdot (-1)^{s_1+s_2+s_3}$ for lamp 2.

$+1 = -1 \cdot (-1)^{s_2+s_3+s_4}$ for lamp 3.

$+1 = -1 \cdot (-1)^{s_3+s_4+s_1}$ for lamp 4.

Observe now that
$s_1+s_2+s_4$ must be even.

Tsovinar's idea:

There is a structure where $1+1=0$,

XOR.

Michael's ~~proposal~~ input:

$\mathbb{Z}_2$ ring of integers modulo 2

class (object oriented)

allowed values: $\{0,1\}$,

operations: $+ : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$

$(0,0) \longmapsto 0$

$(0,1) \longmapsto 1$

$(1,0) \longmapsto 1$

$(1,1) \longmapsto 0$

$\cdot : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$

$(0,0) \longmapsto 0$

$(0,1) \longmapsto 0$

$(1,0) \longmapsto 0$

$(1,1) \longmapsto 1$

$\mathbb{Z}_2$ is even a <u>field</u>:

every element but 0 has a multiplicative inverse.

Trivialities accumulated...

Our statement „$s_1 + s_2 + s_4$ even" now becomes:

$$s_1 + s_3 + s_4 = 0 \quad \text{in } \mathbb{Z}_2.$$

This is LINEAR!

Let's put all four equations in this form:

$$\begin{aligned} s_1 + s_2 + \quad\; + s_4 &= 0 \\ s_1 + s_2 + s_3 \quad\; &= 0 \\ \quad\; s_2 + s_3 + s_4 &= 1 \\ s_1 + \quad\; s_3 + s_4 &= 1 \end{aligned}$$

linear system of equations

→ 0 · Gaussian elimination
· Gauss-Jordan algorithm

Write down as ...

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 0 = 1-1 \\ 0 = 1-1 \\ 1 = 1-0 \\ 1 = 1-0 \end{bmatrix}$$

Desired change of lamp states.

Effect of switching switch 1 on the lamps

Switch or not switch?
Push or not push switch i?
Operate switch i?

Thm It does not matter in which order we operate switches

Pf Assume the state lamps is $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{Z}_2^n$.

A certain switch is describe by $s = \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{Z}_2^n$

and another by $t = \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \in \mathbb{Z}_2^n$.

Now: after first operating s and then t we get

$$(a + s) + t,$$

whereas after operating t and then s we get

$$(a + t) + s.$$

Now we have

$$[(a+s)+t]_i$$

$$= (a_i + s_i) + t_i$$

$(\mathbb{Z}_2, +)$ associative

$$= a_i + (s_i + t_i)$$

$(\mathbb{Z}_2, +)$ commutative

$$= a_i + (t_i + s_i)$$

$$= (a_i + t_i) + s_i$$

$$= [(a+t)+s]_i \,.$$

□

Now, let's do Gaussian elimination:

$$\begin{array}{c} r_1 \\ r_2 \\ r_3 \\ r_4 \end{array} \left[\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

$$\begin{array}{c} r_1 \\ r_2 - 1r_1 \\ r_3 - 0r_1 \\ r_4 - 1r_1 \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right] \begin{array}{l} r_1' \\ r_2' \\ r_3' \\ r_4' \end{array}$$

$$\begin{array}{c} r_1' \\ r_3' \\ r_2' \\ r_4' \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right] \begin{array}{l} r_1'' \\ r_2'' \\ r_3'' \\ r_4'' \end{array}$$

$$\begin{array}{c} r_1'' \\ 1 \cdot r_2'' \\ r_3'' - 0 \cdot r_2'' \\ r_4'' - 1 \cdot r_2'' \end{array} \left[\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \begin{array}{l} r_1''' \\ r_2''' \\ r_3''' \\ r_4''' \end{array}$$

Allowed operation:

- exchange rows
- scale a row, i.e. multiply a row with an invertible constant (over a field: non-zero)
- add any multiple of a row to another:

$$\begin{array}{c} r_1 \\ r_2 \end{array} \longmapsto \begin{array}{l} r_1 \\ r_2 + \alpha r_1 \end{array}$$

Aim: make everything below the "diagonal" zero.

i.e.

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

i.e.

$$\left.\begin{array}{rcl} s_1 + s_2 + s_4 &=& 0 \\ s_2 + s_3 + s_4 &=& 1 \\ s_2 + s_4 &=& 0 \\ s_4 &=& 0 \end{array}\right| \begin{array}{l} \rightarrow s_1 = 1 \\ \rightarrow s_2 = 1 \\ \rightarrow s_3 = 0 \\ \rightarrow s_4 = 0 \end{array}$$

Negative of a is the solution of $a + x = 0$

Let's do it again by the Gauß-Jordan algorithm

BriCo
13.10.09
(8)

$$\left[\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{array}\right] \begin{array}{l} r_1 \\ r_2 \\ r_3 \\ r_4 \end{array}$$

$$\left[\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right] \begin{array}{l} r_1' = 1 \cdot r_1 \\ r_2' = r_2 - 1 \cdot r_1' \\ r_3' = r_3 - 0 \cdot r_1' \\ r_4' = r_4 - 1 \cdot r_1' \end{array}$$

$$\left[\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right] \begin{array}{l} r_1'' = r_1' \\ r_2'' = r_3' \\ r_3'' = r_2' \\ r_4'' = r_4' \end{array}$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \begin{array}{l} r_1''' = r_1'' - 1 \cdot r_2''' \\ r_2''' = 1 \cdot r_2'' \\ r_3''' = r_3'' - 0 \cdot r_2''' \\ r_4''' = r_4'' - 1 \cdot r_2''' \end{array}$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \begin{array}{l} r_1'''' = r_1''' - 1 \cdot r_3'''' \\ r_2'''' = r_2''' - 1 \cdot r_3'''' \\ r_3'''' = 1 \cdot r_3''' \\ r_4'''' = r_4''' - 0 \cdot r_3'''' \end{array}$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \begin{array}{l} r_1^5 = r_1'''' - 1 \cdot r_4^5 \\ r_2^5 = r_2'''' - 0 \cdot r_4^5 \\ r_3^5 = r_3'''' - 1 \cdot r_4^5 \\ r_4^5 = 1 \cdot r_4'''' \end{array}$$

$\Updownarrow$

$$\begin{aligned} s_1 &= 1 \\ s_2 &= 1 \\ s_3 &= 0 \\ s_4 &= 0 \end{aligned}$$

Further questions:

✓ • Do solutions exist?

Example: $1 \cdot s_1 = 0,1$ has solutions.

$0 \cdot s_1 = 0$ has many solutions.

$0 \cdot s_1 = 1$ has no solutions.

✓ How many solutions do we have?

✓ • How fast can we get existance and solutions? $O(n^3)$

• Structure of the set of solutions,

→ Dimension, → Rank of matrix,

→ Kernel of a matrix, range of matrix, their dimension ...

→ Determinant

Thm

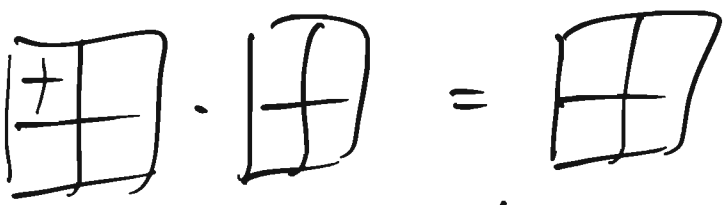
Gaussian elimination
or Gauß-Jordan algorithm
of a $n \times n$-matrix
needs at most

$$\mathcal{O}(n^3)$$

operations in the ground field. □

Strassen (1969):

Gaussian elimination is not optimal.



Strassen does this with 7
instead of 8 operations
(without using commutativity).

$$\rightsquigarrow \mathcal{O}(n^{\log_2 7}) \subset \mathcal{O}(n^{2.83})$$

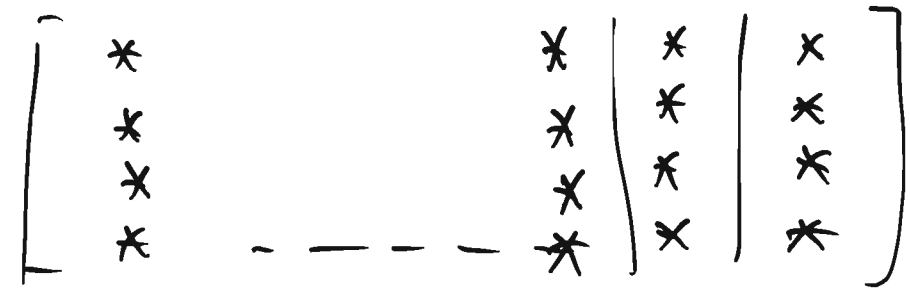
Coppersmith & Vinograd (1990)

$$\rightarrow \mathcal{O}(n^{2.38})$$

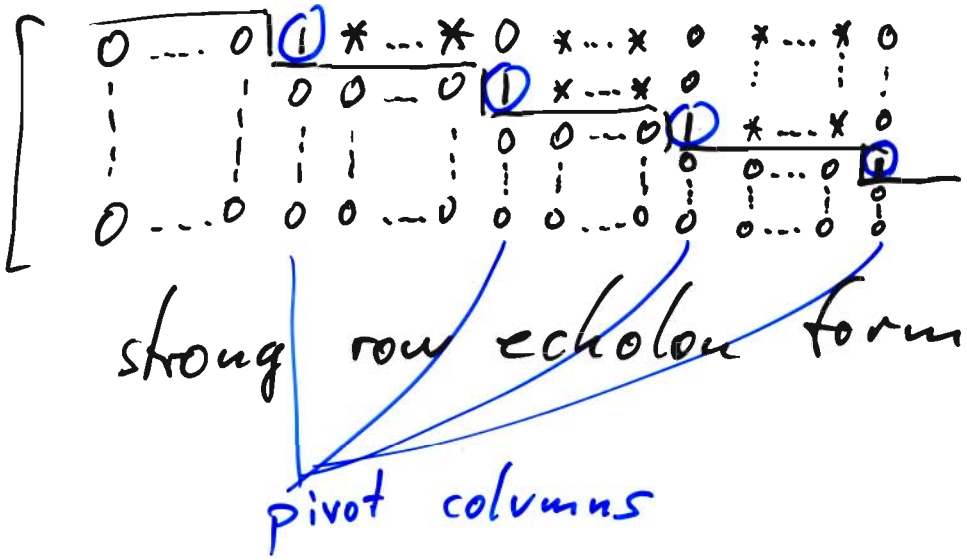
(conjecture: $\tilde{\mathcal{O}}(n^2)$)

BriCo
19.10.09
①

Intended shape?



Want:



Example

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

Task 1: Find a non-zero element for row 1. (now row 1 below!)

Task 2: ~~Finish~~ Move it to row 1, make it 1, and make the rest of the column zero.

Next (after Gauss-Jordan algorithm) perform expansion:

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

BriCo
14.10.09
(2)

Expand: Check for each column whether it is pivot.

If yes: copy the corresponding row.

If no: insert a row with a -1 on the then diagonal position and otherwise zero

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

Now we can describe the set of all solutions:

$$\begin{bmatrix} 0 \\ 0 \\ 3 \\ 0 \\ 3 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_2 \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_4 \begin{bmatrix} 0 \\ 0 \\ 2 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \alpha_6 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$$

Bsp 10
14.10.09
(3)

Let's check the claim:

$$\begin{bmatrix} 0 & 0 & 3 & 0 & 3 & 0 \\ 0 & 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 3 \\ 0 \\ 3 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 3 \\ 0 \end{bmatrix} \checkmark$$

$$\underbrace{\begin{bmatrix} 0 & 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}}_{=: A} \cdot \left(\begin{bmatrix} 0 \\ 0 \\ 3 \\ 0 \\ 3 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right)$$

Use linearity:
$A(x+y) = Ax + Ay$
and
$A(\alpha x) = \alpha \cdot Ax$

$$= A \cdot \begin{bmatrix} 0 \\ 0 \\ 3 \\ 0 \\ 3 \\ 0 \end{bmatrix} + \alpha_1 \cdot A \begin{bmatrix} -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 3 \\ 3 \\ 0 \end{bmatrix} + \alpha_1 \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 3 \\ 3 \\ 0 \end{bmatrix} . \checkmark$$

Also

$$A \cdot \begin{bmatrix} 0 \\ 0 \\ 2 \\ -1 \\ 0 \\ 0 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

↑ vector with α_4

↑ combination of prior pivot columns

↑ 4th column

After the expansion ~~the~~ a -1 column i describe the way of writing the i-th column of A as a linear combination of pivot columns before the i-th column.

$$A \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} = \underbrace{1 \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}_{\text{linear combination of pivot columns before column 6}} - \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

-1 column #6

original column 6

Another example with a complete run:

BriCo
14.10.09
(6)

$$\left[\begin{array}{ccccc|c|c} 0 & 0 & 1 & 1 & 2 & 3 & 3 \\ 0 & 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 2 & 1 & 3 & 4 & 5 & 5 \end{array}\right]$$

(I) Gauss-Jordan

$$\left[\begin{array}{ccccc|cc} 0 & 1 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 2 & 3 & 3 \\ 0 & 2 & 1 & 3 & 4 & 5 & 5 \end{array}\right]$$

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

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

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

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

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

case: second right hand side

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

(II) Done:
No solutions!

The last says:

$$\underbrace{0 \cdot v_1 + 0 \cdot v_2 + \dots + 0 \cdot v_5}_{=0} = 1$$

which is always false.

case: first right hand side

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

(II) ~~Las~~ all zero rows can be deleted

here: no ~~non-zero right~~ contradiction!

(III) expand:

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

(IV) Read off solutions:

$$\begin{bmatrix} 0 \\ 1 \\ 3 \\ 0 \\ 0 \end{bmatrix} + \alpha_1 \begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_4 \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \\ 0 \end{bmatrix} + \alpha_5 \begin{bmatrix} 0 \\ 1 \\ 2 \\ 0 \\ 0 \end{bmatrix}$$

Trying to understand expansion

Brilo
14.10.09
(7)

Assume we have a matrix A in strong row echelon form. We ask for solutions of

$$A x = 0.$$

The set $\ker A := \{x \mid Ax = 0\}$ is the kernel of A.

$\alpha \cdot \begin{bmatrix} \alpha \\ 0 \\ \vdots \end{bmatrix} + \beta \cdot \begin{bmatrix} \beta \\ 0 \\ \vdots \end{bmatrix} + \gamma \cdot \begin{bmatrix} \gamma \\ 0 \\ \vdots \end{bmatrix} - 1 \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \vdots \end{bmatrix} = 0$

We have

$$A = \begin{bmatrix} 0 \cdots 0 & 1 & * \cdots * & 0 & * \cdots * & \alpha \\ \vdots & \vdots & 0 \cdots 0 & 1 & * \cdots * & \beta \\ \vdots & \vdots & \vdots & 0 & \cdots & \gamma \\ 0 \cdots 0 & 0 & 0 \cdots 0 & 0 & 0 \cdots 0 & \vdots \end{bmatrix}$$

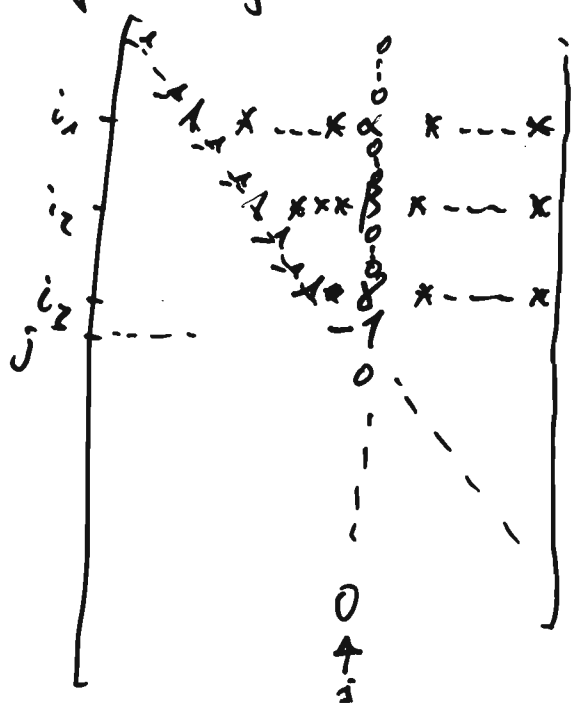
(columns: $0 \cdots 0\ \alpha\ 0 \cdots 0\ \beta\ 0 \cdots 0\ \gamma\ -1\ 0 \cdots 0$; pivot columns i_1, i_2, i_3, j)

Thus

$$A \cdot \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \alpha \\ 0 \\ \vdots \\ 0 \\ \beta \\ 0 \\ \vdots \\ 0 \\ \gamma \\ -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

(α at i_1, β at i_2, γ at i_3, -1 at j)

On the other hand side expanding A gives j-th column:



Conclusion: The -1-columns in the expanded matrix are vectors/elements in the kernel.

Of course, if

$$A x_1 = 0 \quad \text{and} \quad A x_2 = 0$$

then also $A(x_1 + x_2) = 0$

and

$$A(\alpha_1 x_1 + \alpha_2 x_2) = 0.$$

Short:

$x_1 \in \ker A, \quad x_2 \in \ker A$

$\Rightarrow \quad \alpha_2 x_1 + \alpha_1 x_2 \in \ker A.$

Let A^* be the expanded matrix of A.

Then $\ker A = \{ \sum \alpha_i A^*_{\cdot i} \mid \alpha_i \in F^6 \}$ (base field)

(i non-pivot)

any combination of -1-columns of the expanded matrix.

Clearly: $\sum \alpha_i A^*_{\cdot i} = \begin{bmatrix} * \\ \vdots \\ * \\ -\alpha_j \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ ← last $\alpha_i \neq 0$.

Claim $\ker A \subseteq \{ \underbrace{\sum \alpha_i A^*_{\bullet i}}_{\text{combinations of -1-columns.}} \mid \alpha_i \in F \}$

Proof

Assume $x \in \ker A$, ie. $A \cdot x = 0$.
And all $x + \sum \alpha_i A^*_{\bullet i}$ have more zeros at the end.
Then ~~Without loss of generality~~ $x = 0$.
↑ Without loss of generality the last $(n-j)$ coordinates of x are zero.
In other words $(x_j \neq 0,)\ x_{j+1} = \dots = x_n = 0$.

Now: Assume we have this for $i < j$.

Claim: $x_j \neq 0 \Rightarrow j$ non-Pivot.

Pf: Otherwise $0 = (Ax)_j = x_j \cdot 1 \neq 0$ ↯ □

$x \in \ker A$ $\quad$ j Pivot $\quad$ $x_j \neq 0$

Thus $x + x_j \cdot A^*_{\bullet j} \in \ker A$.

Claim $\ker A \subseteq \{ \underbrace{\sum \alpha_i A^*_{\cdot i}}_{\text{combination of } -1\text{-columns}} \mid \alpha_i \in F \} =: K$

Pf Assume $x \in \ker A$, i.e. $Ax = 0$,
and the number of 0 at the end cannot be increased by subtracting an element of K.

Then $x = 0$.

[Once we have proved this, we are done:
Given any $x \in \ker A$.
Reduce it: $x' = x - \sum_{\substack{i \text{ non-} \\ \text{pivot}}} \alpha_i A^*_{\cdot i}$
so that x' has as many 0 at the end as possible.
By the claim then $x' = 0$.
Thus $x = \sum_{\substack{i \\ \text{non-pivot}}} \alpha_i A^*_{\cdot i} \in K$.]

Assume $x \neq 0$ and j is the last position with $x_j \neq 0$.
Then j is non-Pivot.

[Otherwise: $0 = (Ax)_j = x_j \cdot 1 \neq 0$
($x \in \ker$; j Pivot; $x_j \neq 0$) ↯.]

But now

$$x + x_j \cdot A^*_{\bullet j}$$

has more zero coordinates at the end! $\lightning \rightarrow x = 0$. $\square$

How to solve $Ax = b$?

This ~~essen~~ ~~almost~~ the same than solving

$$Ax = -b\, x_{n+1} \quad \wedge \quad x_{n+1} \neq 0.$$

This is the same as

$$\begin{bmatrix} A & b \end{bmatrix} \begin{bmatrix} x \\ x_{n+1} \end{bmatrix} = 0 \quad \wedge \quad x_{n+1} \neq 0$$

This is solvable iff b is a non-Pivot column!

Case: b is Pivot

ends in

$$GJ([A\ b])^* = \begin{bmatrix} \ddots & & \\ & \ddots & \\ 0 & 0 & 1 \end{bmatrix} \rightarrow \text{solution } \begin{bmatrix} x \\ x_{n+1} \end{bmatrix} = \begin{bmatrix} * \\ \vdots \\ * \\ 0 \end{bmatrix}$$

Case: b non-Pivot:

$$GJ([A\ b])^* = \begin{bmatrix} \ddots & & * \\ & \ddots & \vdots \\ & & * \\ & & -1 \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x_{n+1} \end{bmatrix} = \begin{bmatrix} * \\ \vdots \\ * \\ -1 \end{bmatrix} \text{ is a solution}$$

Exercises

Solve $Ax = b$ over $\mathbb{Z}_7$

$\{0, \pm 1, \pm 2, \pm 3\}$

addition, multiplication are done modulo 7.

Eg: $3+3 = -1$.

or: $-2 \cdot 3 = +1$

$$A = \begin{bmatrix} 1 & 2 & -1 \\ 0 & 3 & 1 \\ 2 & 0 & 1 \end{bmatrix}, \quad b_1 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}$$

$$b_2 = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & 2 & -1 & 1 \\ 0 & 3 & -1 & 2 \\ 2 & 0 & -3 & -3 \end{bmatrix}, \quad b_1 = \begin{bmatrix} -2 \\ -1 \\ 2 \end{bmatrix}$$

$$b_2 = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix}$$

$4 \cdot 5 = 6$ in $\mathbb{Z}_7$

In particular:

$$\frac{1}{1} = 1, \quad \frac{1}{2} = -3, \quad \frac{1}{3} = -2,$$

$$\frac{1}{-1} = -1, \quad \frac{1}{-2} = 3, \quad \frac{1}{-3} = 2.$$

BwCo
14.10.09
(12)

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

$$\left[\begin{array}{ccc|cc} 1 & 2 & -1 & 2 & 3 \\ 0 & 3 & 1 & 1 & 0 \\ 0 & 3 & 3 & 3 & 2 \end{array}\right] \cdot (-2)$$

$$\left[\begin{array}{ccc|cc} 1 & 0 & 3 & -1 & 3 \\ 0 & 1 & -2 & -2 & 0 \\ 0 & 0 & 2 & 2 & 2 \end{array}\right] \cdot (-3)$$

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

↓ expand!

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

Thus $x_1 = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}$, $x_2 = \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix}$

Xcheck:

$$Ax_1 = \begin{bmatrix} 3 \\ 0 \\ -1 \end{bmatrix} + \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \checkmark$$

$$Ax_2 = \begin{bmatrix} -3 \\ -1 \\ 0 \end{bmatrix} + \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}$$

BriCo
14.10.09
13

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

$$\left[\begin{array}{cccccc} 1 & 2 & -1 & 1 & -2 & 2 \\ 0 & 3 & -1 & 2 & -1 & 1 \\ 0 & 3 & -1 & 2 & -1 & +3 \end{array}\right] \cdot (-2)$$

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

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

$\rightarrow$ b_1: Expand:

$$\left[\begin{array}{cccc|c} 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 2 & 3 & 2 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \end{array}\right] \rightarrow x_1 = \begin{bmatrix} 1 \\ 2 \\ 0 \\ 0 \end{bmatrix} + \alpha_3 \begin{bmatrix} 2 \\ 2 \\ -1 \\ 0 \end{bmatrix} + \alpha_4 \begin{bmatrix} 2 \\ 3 \\ 0 \\ -1 \end{bmatrix}$$

$\alpha_3, \alpha_4 \in \mathbb{Z}_7$

$\rightarrow$ b_2 : Pivot

$\Rightarrow$ No solution!

7^2 solutions

i.e. dimension 2.

structure?

$$\ker A := \{ x \mid Ax = 0 \}$$

kernel of A.

Thm $\ker A$ is a vector space,

ie. $x, y \in \ker A \Rightarrow \alpha x + \beta y \in \ker A$.

Pf $x, y \in \ker A \rightarrow Ax = 0, \; Ay = 0$

$$\rightarrow A(\alpha x + \beta y) = \alpha \cdot Ax + \beta \cdot Ay$$
$$= \alpha \cdot 0 + \beta \cdot 0$$
$$= 0.$$

$\rightarrow \alpha x + \beta y \in \ker A$. □

$$\text{range } A := \text{im } A := \{ Ax \mid x \}$$

Thm range A is a vector space.

□

Pf Homework.

Def A basis $b_1, \dots, b_k$ of a vector space V is a set $\{b_1, \dots, b_k\} \subset V$ such that

- generating: $V = \{ \sum \alpha_i b_i \mid \alpha_i \in \mathbb{F} \}$
- linearly independent: $\sum \alpha_i b_i = 0 \Rightarrow \forall \alpha_i = 0$.

BriCo
14.10.09
15

Thm

If $\{b_1 \dots b_k\}$ and $\{c_1, \dots, c_\ell\}$ are two bases of the same vector space V then

$$k = \ell .$$

$$\overset{\shortparallel}{\dim V} \quad \dots$$

intuitive: # of free parameters

Consider $V = \ker A$, $A \in F^{m \times n}$ ← columns

Say the strong row echelon form of A is

$$\begin{bmatrix} 1 & 0 & 3 & 0 & 3 & 3 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

From the example we guess:

$\dim \ker A = n - \#\text{Pivot}$

Expansion gives:

$$\begin{array}{c} \begin{bmatrix} 1 & 0 & 3 & 0 & 3 & 3 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix} \end{array} \begin{array}{c} 0 \\ 0 \\ \vdots \\ 0 \end{array}$$

$$\to \ker A = \left\{ \alpha_2 \cdot \begin{bmatrix} 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_3 \cdot \begin{bmatrix} 3 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_5 \begin{bmatrix} 3 \\ 0 \\ 0 \\ 1 \\ -1 \\ 0 \end{bmatrix} + \alpha_6 \begin{bmatrix} 3 \\ 0 \\ 0 \\ 0 \\ 0 \\ -1 \end{bmatrix} \right\}.$$

Now consider $A \in F^{m \times n}$

$$V = \text{range } A = \text{im } A$$
$$= \{ Ax \mid x \in F^n \}.$$

In our example

$$A = \begin{bmatrix} 2 & 0 & 6 & 0 & 6 & 6 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 3 & 1 & 4 & 3 \end{bmatrix}$$

we have

$$V = \{ x_1 \begin{bmatrix} 2 \\ 0 \\ 1 \end{bmatrix} + x_2 \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} + x_3 \cdot \begin{bmatrix} 6 \\ 0 \\ 3 \end{bmatrix}$$
$$+ x_4 \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + x_5 \cdot \begin{bmatrix} 6 \\ 1 \\ 4 \end{bmatrix} + x_6 \begin{bmatrix} 6 \\ 0 \\ 3 \end{bmatrix};$$
$$x_1, \dots, x_6 \in F \}$$

However: the columns of A are <u>not</u> linearly independent.

Of course they do generate range A.

The columns of A corresponding to the Pivot positions form a basis of the range $\text{im } A$ of A.

Its dimension is the number of Pivots.

It is called the <u>rank of A</u>.

Brilo
14.10.09
(17)

Theorem For any matrix $A \in F^{m \times n}$ we have

$$\boxed{\dim \ker A + \dim \operatorname{im} A = n}$$

where F is any field.

Corollary

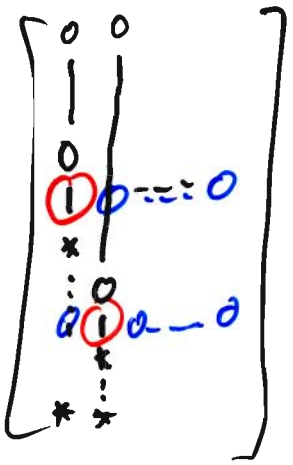
$$\text{column-rank}(A) = \text{row-rank}(A)$$

Pf

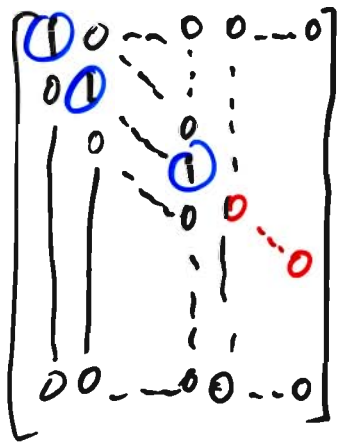
$$\text{column-rank}(A) = \#\text{Pivots in } GJ(A)$$

$$GJ(A) = \begin{bmatrix} 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & * & * & 0 \\ \vdots & & \vdots & 0 & 0 & \cdots & 0 & 1 & * & * & * & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & 0 & \cdots & 0 & 1 & \cdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \end{bmatrix}$$

transpose it:



Gauß Jordan →



$$\text{row-rank}(A) = \text{column-rank}(A^T)$$

and $GJ\left(GJ(A)^T\right)^T = GJ\left(GJ(A^T)^T\right)$

thus the two ranks are equal. ☐

Summary

Zilo
14.10.08
(18)

We have

- Gaussian elimination and Gauss-Jordan algorithm.
- Both need at most $O(n^3)$ operations on a $n \times n$-matrix ~~ab~~ in the ground field.
- Dimension & basis
- $\ker A$: obtain a basis by applying Gauss-Jordan + expansion and selecting the -1-columns.
  $\dim \ker A = n -$ # Pivots.
- $\operatorname{im} A$: obtain a basis by selecting those columns of A that correspond to the Pivot positions of $GJ(A)$.
  $\dim \operatorname{im} A =$ # Pivots.
- $Ax = b \iff [A \; b] \begin{bmatrix} x \\ x_{n+1} \end{bmatrix} = 0 \wedge x_{n+1} \neq 0.$

Missing: Determinant

BriCo 15.10.09 (1)

Goal: Given a square matrix A. Describe a polynomial expression $\det A$ such that

$$\det A = 0 \iff Ax = 0 \text{ has multiple solutions}$$

Possible first Definition:

Consider applying Gaussian elimination or the Gauß-Jordan algorithm without scaling rows.

Problem: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{matrix} r_1 \\ r_2 \end{matrix}$

Case $a \neq 0$

$$\begin{bmatrix} a & b \\ & d - \frac{c}{a} b \end{bmatrix} \begin{matrix} r_1 \\ r_2 - \frac{c}{a} r_1 \end{matrix}$$

Now, take the product of the diagonal:

$$ad - cb.$$

$$\begin{bmatrix} 0 & \\ & 0 \end{bmatrix} - \begin{bmatrix} & 0 \\ 0 & \end{bmatrix}$$

Case $a = 0$

$$\begin{bmatrix} c & d \\ 0 & -b \end{bmatrix}$$

Now...:

$$-bc.$$

Not so clear that it works.
But it's well motivated:

$Ax=0$ has mult. solutions $\Leftrightarrow$ $\ker A \neq \{0\}$

$\Leftrightarrow$ row echelon form of A has a zero row

$\Leftrightarrow$ row echelon form of A has a non-Pivot column

$\Leftrightarrow$ there is a zero on the diagonal of $GJ(A)$.

↳ Multiply the diagonal of $GJ(A)$...

Forbid scalings and exchanging rows to keep the expression without divisions and case distinctions.

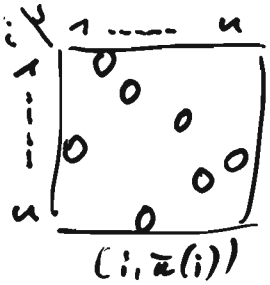
It turns out that this works.

Theorem

$$\det A = \sum_{\pi \text{ a permutation of } \{1,\dots,n\}} (-1)^{\operatorname{sgn}(\pi)} \prod_{1 \le i \le n} A_{i\,\pi(i)}$$

$\operatorname{sgn}(\pi)$: 0 if π is even, 1 if π is odd

$\{\text{bijection } \{1,\dots,n\} \to \{1,\dots,n\}\}$



We can turn this expression into a program.

But:

summands

= # permutations of $\{1,\dots,n\}$

$= n! \sim 2^{nH(n)}$

exponential in n!

thus runtime $\geq \Omega(n\,2^{n/2})$ ..

operations

How to compute it then?

Answer: use Gaussian elimination or the Gauß-Jordan algorithm.

Fact $\det(AB) = \det A \cdot \det B$ by keeping track of our actions!

Observe: • exchange rows i, j

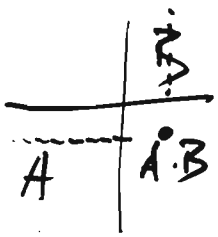
$B \longmapsto$ B

$\det \% = -1$

- scale row i by $\alpha \neq 0$

$$B \longmapsto \underbrace{\begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & \alpha & \\ & & & \ddots \\ & & & & 1 \end{bmatrix}}_{\det \% = \alpha} B$$

- add row i multiplied by β to row j



$$B \longmapsto \underbrace{\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & \beta & \ddots & \\ & & & & 1 \end{bmatrix}}_{\det \% = 1} B$$

Keeping track of row exchanges and row scaling in the Gauß-Jordan algorithm gives the determinant almost for free:

runtime $O(n^3)$ operations!

BuCo
14.10.09
(12)

15.10.09
(5)

Over $\mathbb{Z}_7$.

$$\left[\begin{array}{ccc|cc} 1 & 2 & -1 & 2 & 3 \\ 0 & 3 & 1 & 1 & 0 \\ 2 & 0 & 1 & 0 & 1 \end{array}\right] \quad \det A$$

$$\left[\begin{array}{ccc|cc} 1 & 2 & -1 & 2 & 3 \\ 0 & 3 & 1 & 1 & 0 \\ 0 & 3 & 3 & 3 & 2 \end{array}\right] \cdot(-2) \quad \det A$$

$$\left[\begin{array}{ccc|cc} 1 & 0 & 3 & -1 & 3 \\ 0 & 1 & -2 & -2 & 0 \\ 0 & 0 & 2 & 2 & 2 \end{array}\right] \cdot(-3) \quad (-2)\cdot\det A$$

$$\left[\begin{array}{ccc|cc} 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right] \quad 1 = \det\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} = (-3)(-2)\det A$$

$$\det A = 2\cdot 3 = -1$$

↓ expand!

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

Thus $x_1 = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}$, $x_2 = \begin{bmatrix} 0 \\ 2 \\ 1 \end{bmatrix}$

Xcheck:

$$Ax_1 = \begin{bmatrix} 3 \\ 0 \\ -1 \end{bmatrix} + \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \checkmark$$

$$Ax_2 = \begin{bmatrix} -3 \\ -1 \\ 0 \end{bmatrix} + \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 1 \end{bmatrix}$$

Foundations of informatics — a bridging course
Fall 2009
Mathematical tools
MICHAEL NÜSKEN

3. Probabilities

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

Give examples where randomness

(i) decides about win or loose. 2

(ii) helps simulating difficult reality. 2

(iii) helps solving difficult finite problems. 2

(iv) models errors. 2

(v) makes decisions. 2

(vi) hides secrets. 2

(vii) Does something else which is interesting. +4

Network control

Game theory

Crypto.

Speech recognition.
Machine learning.

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? 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. 2

(ii) Calculate the unconditional probability that your door is the winning one, and its complement. [1]

[5] What do you do? Reason!

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.

[8] (i) Find a strategy that allows some of them to go.

[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

[0] (a) exactly one hour?

[1] (b) exactly two hours?

[1] (c) exactly three hours?

[1] (d) exactly four hours?

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

[3] (a) ... by definition? [Give a formula.]

[2] (b) ... by value? [Calculate!]

Probabilities

BriCo
15.10.09
6

Classical definition

$$\text{prob}(\text{event } X) = \lim_{n\to\infty} \left(\begin{array}{l} \text{relative frequency} \\ \text{of event } X \\ \text{in } n \text{ trials} \end{array} \right)$$

Tchebycheff:

$$\text{prob}(\text{event } X) = \underline{\text{chosen.}}$$

Formally:

$$\text{prob} : \{ \text{subset of } \Omega \} \to [0,1]$$

such that

$$\text{prob}(\Omega) = 1$$

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

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

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

$$\Rightarrow (A \subset B \Rightarrow \text{prob}\, A \leq \text{prob}\, B)$$

This works out fine as long as Ω finite.

This is fine for us!

Thm of large numbers
Laxely spoken says:

$$\text{prob}(A) = \lim_{n\to\infty} \text{rel. frequency of } A \text{ in } n \text{ trials.}$$

Examples

rolling a die

$\Omega = \{1, 2, 3, 4, 5, 6\}$

A = die shows up with even number

$= \{2, 4, 6\}$.

prob: {subsets of Ω} $\longrightarrow [0, 1]$.

$\text{prob}(\{i\}) := \frac{1}{6}$.

Since $\text{prob}(\{1,2,3,4,5,6\}) = \frac{1}{6} + \ldots + \frac{1}{6} = 1$

$\text{prob}\,\Omega$

✓

Good: it works.

But it is cumbersome

for die also $\Omega = \{ (1, \text{rain}), (1, \neg\text{rain}), (2, \text{rain}), (2, \neg\text{rain}), 3, 4, 5, 6 \}$

Random variables

BriCo
15.10.05
(8)

$$X : \Omega \longrightarrow S$$

S: some set,
e.g. $\{1,2,3,4,5,6\}$
or $\mathbb{R}$
or ~~$\mathbb{Z}_7$~~ S'.

Then
$$\text{prob}(X = a)$$
$$= \text{prob}(\{\omega \in \Omega \mid X(\omega) = a\})$$

The term
$$\text{prob}(X = a)$$
does not show any dependence on the universe Ω.

This allows to combine various random variables without needing to care about changing universes...

The only thing I need is:
$\{\text{outcomes of } X\} \longrightarrow [0,1]$ distribution of X.
$a \longmapsto \text{prob}(X = a)$

Theorem

If X, Y are random variables (on different universes) there is a universe such that

$$\text{prob}(X=a,\ Y=b) = \text{prob}(X=a) \cdot \text{prob}(Y=b)$$

i.e. X and Y are r.v. over some new universe and they are (stochastically) independent.

You can now combine random variables independently, operate with functions on them

...

Example

A computer can use 3 random bits and shall produce the outcome of a die roll.

1. Repeat
2. set $X_2, X_1, X_0 \in_R \{0,1\}$
3. let $X := X_2 \cdot 4 + X_1 \cdot 2 + X_0$
4. until $X \neq 0$ and $X \neq 7$.
5. Return X.

Expected # of repetitions?

$\rightarrow \frac{1}{\text{exit prob}} = \frac{1}{75\%} = \frac{4}{3}$.

Thus the average number of random bits used here is 4.

Bri Co
15.10.09
10

$$\text{prob}(A \mid B) = \frac{\text{prob}(A \cap B)}{\text{prob}(B)}$$

Ex 3.4

(i) Strategy p:
The Prisoner chooses "Yes, I want" with probability p
and "No, I do not want" with probability $1-p$.

where $0 < p < 1$.

(ii) prob(Players loose, ie. no one goes)

$$= \begin{cases} 1, & p = 0 \text{ or } p = 1. \\ \underbrace{\text{prob(all say no)}}_{(1-p)^{100}} + \underbrace{\text{prob(all say yes)}}_{p^{100}} \end{cases}$$

$$= (1-p)^{100} + p^{100}$$

Modelling this?:

Let $X_i = \begin{cases} 0 & \text{if prisoner } i \text{ says No.} \\ 1 & \text{if prisoner } i \text{ says Yes.} \end{cases}$

for $i \in \{1, \dots, 100\}$ be a random variable. We assume that they are mutually independent and

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

What, now, is the number N of prisoners going to the theatre?

$$N = \begin{cases} 0 & \text{if all } X_i = 1, \\ \sum_{i=1}^{100} X_i & \text{otherwise.} \end{cases}$$

We want that the "expected value" of N is large.

Now

$$E(N) = \sum_{\substack{n \in \text{possible} \\ \text{outcomes of } N \\ n \in \{0, \dots, 100\}}} n \cdot \text{prob}(N = n)$$

Enrico
15.10.09
(12)

We might write

$$prob(N=n) = prob(N \le n) - prob(N \le n-1)$$

Fix $n \in \{0, \dots, 100\}$. Consider

Case $n = 100$

$$prob(N=n) = 0$$

Case $n = 0$

$$prob(N=0) = prob(\text{all } X_i = 1 \text{ i } \sum X_i = 0)$$

$$= prob(\text{all } X_i = 1) + prob(\text{all } X_i = 0)$$

Independence

$$= \prod_{i=1}^{100} \underbrace{prob(X_i = 1)}_{p} + \prod_{i=1}^{100} \underbrace{prob(X_i = 0)}_{1-p}$$

$$= p^{100} + (1-p)^{100}.$$

Cases $0 < n < 100$

$$prob(N=n) = prob\left(\sum_{i=1}^{100} X_i = n\right)$$

$$\binom{100}{n} p^n (1-p)^{100-n}$$

$$= prob(\exists I \subset \{1, \dots, 100\}: (\forall i \in I: X_i = 1 \text{ i } \#I = n \text{ i } \forall i \in \{1, \dots, 100\} \setminus I: X_i = 0))$$

$$= \sum_{I} prob(\dots)$$

$$= \sum_{I} \prod_{i \in I} prob(X_i = 1) \cdot \prod_{i \notin I} prob(X_i = 0)$$

$$= \sum_{I \in \binom{\{1,\dots,100\}}{n}} \underbrace{p^n (1-p)^{100-n}}_{\text{independent of } I}$$

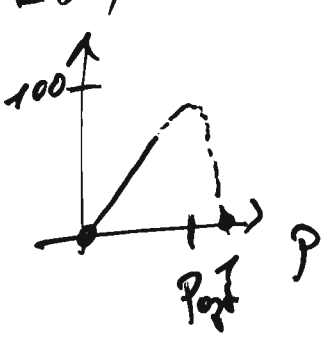
$$= \binom{100}{n} \cdot p^n (1-p)^{100-n}.$$

Together

$$\mathbb{E}(N) = \sum_{n=1}^{99} n \cdot \binom{100}{n} p^n (1-p)^{100-n} + 0 \cdot \left(p^{100} + (1-p)^{100} \right)$$

$$n \cdot \binom{100}{n} = 100 \cdot \binom{99}{n-1}$$

$$(x+y)^{99} = \sum_{n=1}^{100} \binom{99}{n-1} x^{n-1} y^{99-n+1}$$



Take $x = p$, $y = 1-p$.

Then: $100p = \sum_{n=1}^{100} 100 \binom{99}{n-1} p^n (1-p)^{100-n}$.

Now:

$$E(N) = 100p - 100 \cdot \binom{99}{100-1} p^{100} (1-p)^0.$$

$$= 100 \left(p - p^{100} \right) = 100 \cdot p \cdot (1 - p^{99})$$

$$\frac{d\,E(N)}{dp} = 100\,(\underbrace{1 - 100\cdot p^{99}}) \qquad \text{This is zero at } p_{opt} = \left(\frac{1}{100}\right)^{1/99}.$$

This results in

$$E(N) = 100 \cdot \left(\frac{1}{100}\right)^{1/99}\left(1 - \frac{1}{100}\right)$$

$$= 99 \cdot \left(\frac{1}{100}\right)^{1/99}.$$

3.2 $N = \begin{cases} 1 & \text{if person British} \\ 0 & \text{otherwise} \end{cases}$

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

$$\text{prob}(N=1) = 60\% = 0.6$$
$$\text{prob}(H=1 \mid N=1) = 0.75$$
$$\text{prob}(H=1 \mid N=0) = 0.25$$

Q: $\text{prob}(N=1 \mid H=1) = ?$

observe: $\text{prob}(N=0) = 0.4$

$$\text{prob}(H=1 \mid N=1) \overset{\text{Def}}{=} \frac{\text{prob}(H=1 \wedge N=1)}{\text{prob}(N=1)}$$

↳ $\text{prob}(H=1 \wedge N=1) = 0.6 \cdot 0.75$

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

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

$$\frac{0.6 \cdot 0.75}{0.6 \cdot 0.75 + 0.4 \cdot 0.25} = \frac{9}{11}.$$

Random exit

BriCo
15.10.09
(15)

Given a program:

1. Repeat
2. Do whatever
3. Until condition holds

where prob(condition) = p

Then the expected number of repetitions is

$$1/p.$$

To do this introduce independent random variables

$$X_i = \begin{cases} 1 & \text{if you do not exit} \\ 0 & \text{if you do exit.} \end{cases}$$

The number of repetitions is

$$N = \min\{ i : X_i = 0 \}.$$

Calculate $E(N)$ when $\text{prob}(X_i = 0) = p$.

Zürich
15.10.09
(16)

How to?

$$\text{prob}(N=n)$$

$$= \text{prob}(X_1 = 0, \dots, X_{n-1} = 1, X_n = 0)$$

$$= (1-p)^{n-1} \cdot p$$

Next:

$$E(N) = \sum_{n=0}^{\infty} n \cdot (1-p)^{n-1} \cdot p$$

$$\left(\frac{1}{1-q}\right)' \qquad q = 1-p$$

$$= \frac{1}{p}.$$

Elementary Number Theory

BriCo
16.10.09
(1)

Ex Compute in $\mathbb{Z}_{15}$ all powers of $2, 3, 7, \ldots$?

i	0	1	2	3	4	5	6
2^i	1	2	4	−7	1		
3^i	1	3	−6	−3	6	3	
7^i	1	7	4	−2	1		

cycle not from beginning

1 : cycle of length 1
−1 : 2
4 : 2
5 : 2 but from beginning
$6 = 2 \cdot 3$: 4 but from beginning
$-7, \ldots, -1$ → all cycles latest after 4 positions
0 : cycle of length 1 but from beginning.

BriCo
16.10.09
②

Observations:

- The sequence a^i in $\mathbb{Z}_m$ always cycles.
- There is something special about numbers a that have a factor in common with m.
- All other cycles start at the beginning.

RSA (Rivest, Shamir & Adleman 1978)

Setup

Choose two different prime numbers p, q, both large.
Then choose two numbers e, d such that $ed-1$ is a multiple of $L := (p-1)\cdot(q-1)$.
Finally, let $N := p \cdot q$.

Now:
(N, e) is the public key,
(N, d) is the private key.

And we discard everything else.

Encrypt

Given a message $x \in \mathbb{Z}_N$.
Compute
$y := x^e$.

Decrypt

Given a encryption $y \in \mathbb{Z}_N$
Compute
$z := y^d$.

Question: Is $z = x$?

What is $\mathbb{Z}_N$ and how do we work with or in it?

Object oriented approach:

$\mathbb{Z}_N$ is a class,

allowed values are

$$\left[\frac{N}{2}\right]+1-N, \ldots, -2, -1, 0, 1, 2, \ldots, \left[\frac{N}{2}\right]$$

(Alternative: values are $0, 1, 2, \ldots, N-1$.)

addition $+ : \mathbb{Z}_N \times \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$

$$(a, b) \longmapsto c$$

where $c = (a +_{\mathbb{Z}} b) \bmod N$

Divide the integer $a +_{\mathbb{Z}} b$ by N, take the remainder $(a +_{\mathbb{Z}} b) \operatorname{rem} N \in \mathbb{Z}$, and interpret it in the class.

multiplication $\cdot : \mathbb{Z}_N \times \mathbb{Z}_N \longrightarrow \mathbb{Z}_N$,

$$(a, b) \longmapsto (a \cdot_{\mathbb{Z}} b) \bmod N.$$

Claim $\mathbb{Z}_N$ is a ring with 1 commutative.

ie. the following axioms hold

- group
  - $P+$: proper definition of addition, ie. $+ : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$
  - $A+$: for any $a,b,c \in \mathbb{Z}_N$: $(a+b)+c = a+(b+c)$
  - $N+$: there is a neutral element $0 \in \mathbb{Z}_N$ such that for any $a \in \mathbb{Z}_N$ $a+0=a$, $0+a=a$.
  - $I+$: for any $a \in \mathbb{Z}_N$ there is an element $b \in \mathbb{Z}_N$ such that $a+b=0$, $b+a=0$.
  - $C+$: for any $a,b \in \mathbb{Z}_N$ we have $a+b=b+a$.
- commut. ring with 1
  - $P\cdot$: proper definition of multiplication, ie. $\cdot : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{Z}_N$.
  - $A\cdot$: $\forall a,b,c \in \mathbb{Z}_N$: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
  - $N\cdot$: there is a neutral element $1 \in \mathbb{Z}_N$ such that: $a\cdot 1 = a$, $1\cdot a = a$
  - $C\cdot$: $\forall a,b \in \mathbb{Z}_N$: $a\cdot b = b\cdot a$.
  - D : $\forall a,b,c \in \mathbb{Z}_N$: $a(b+c) = ab+ac$, $(a+b)\cdot c = ac+bc$
  - ONT : $0 \neq 1$.

What about inverses?
Do we have

? I.: $\forall a \in \mathbb{Z}_N \ \exists b \in \mathbb{Z}_N$:
$a \cdot b = 1$, $b \cdot a = 1$

Example $N=2$: $\mathbb{Z}_2 = \{0,1\}$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

We do not I. because $0 \cdot b = 1$ has no solution!
Instead try

I'.: $\forall a \in \mathbb{Z}_N \setminus \{0\} \ \exists b \in \mathbb{Z}_N$:
$a \cdot b = 1$, $b \cdot a = 1$

This I'. holds in $\mathbb{Z}_2$.

Example $N=7$ $\mathbb{Z}_7 = \{-2,-1,0,1,2,-3,3\}$

I'. holds! $\frac{1}{2} = -3$, $\frac{1}{3} = -2$, $\frac{1}{1} = 1$,

$\frac{1}{-2} = 3$, $\frac{1}{-3} = 2$, $\frac{1}{-1} = -1$.

Example $N=15$

I'.? Claim: $3 \in \mathbb{Z}_{15}$ has no inverse.

Pf Assume $3 \cdot b = 1$ in $\mathbb{Z}_{15}$.

Then $3b - 15q = 1$ in $\mathbb{Z}$ for some q.

But $3 \mid 15$. (3 divides 15).

Thus $3b - 15q$ is a multiple of 3,

or $3 \mid (3b - 15q)$.

Thus $3 \mid 1$, which is wrong. ↯

So our assumption cannot hold:

$3b = 1$ has no solution in $\mathbb{Z}_{15}$. □

Concluding: I'. does not hold for $\mathbb{Z}_{15}$.

Generalizing the claim and its proof we obtain:

> if $N = p \cdot M$ for some prime p and $M \neq 1$
>
> then p has no inverse in $\mathbb{Z}_N$,
>
> ie. I'. does not hold for $\mathbb{Z}_{p \cdot M}$.

So it may be that I'. holds if N is prime, but never does so if N is composite (= non-prime).

More general question: task:

Find an algorithm that
given N and $a \in \mathbb{Z}_N$
decides whether a has an inverse
and if so computes it.

The algorithm has to consider

find $b \in \mathbb{Z}_N$: $a \cdot_{\mathbb{Z}_N} b = 1$ in $\mathbb{Z}_N$.

This is equivalent to

find $b, q \in \mathbb{Z}$: $a \cdot_{\mathbb{Z}} b + N \cdot_{\mathbb{Z}} q = 1$ in $\mathbb{Z}$

Example

$N = 71$, $a = 17$

Find b, q such that

$$17b + 71q = 1.$$

Trial: Brute force
Run through $q = 0, \dots, -16$.
until you find also a fitting b...

But: Brute force is no solution!

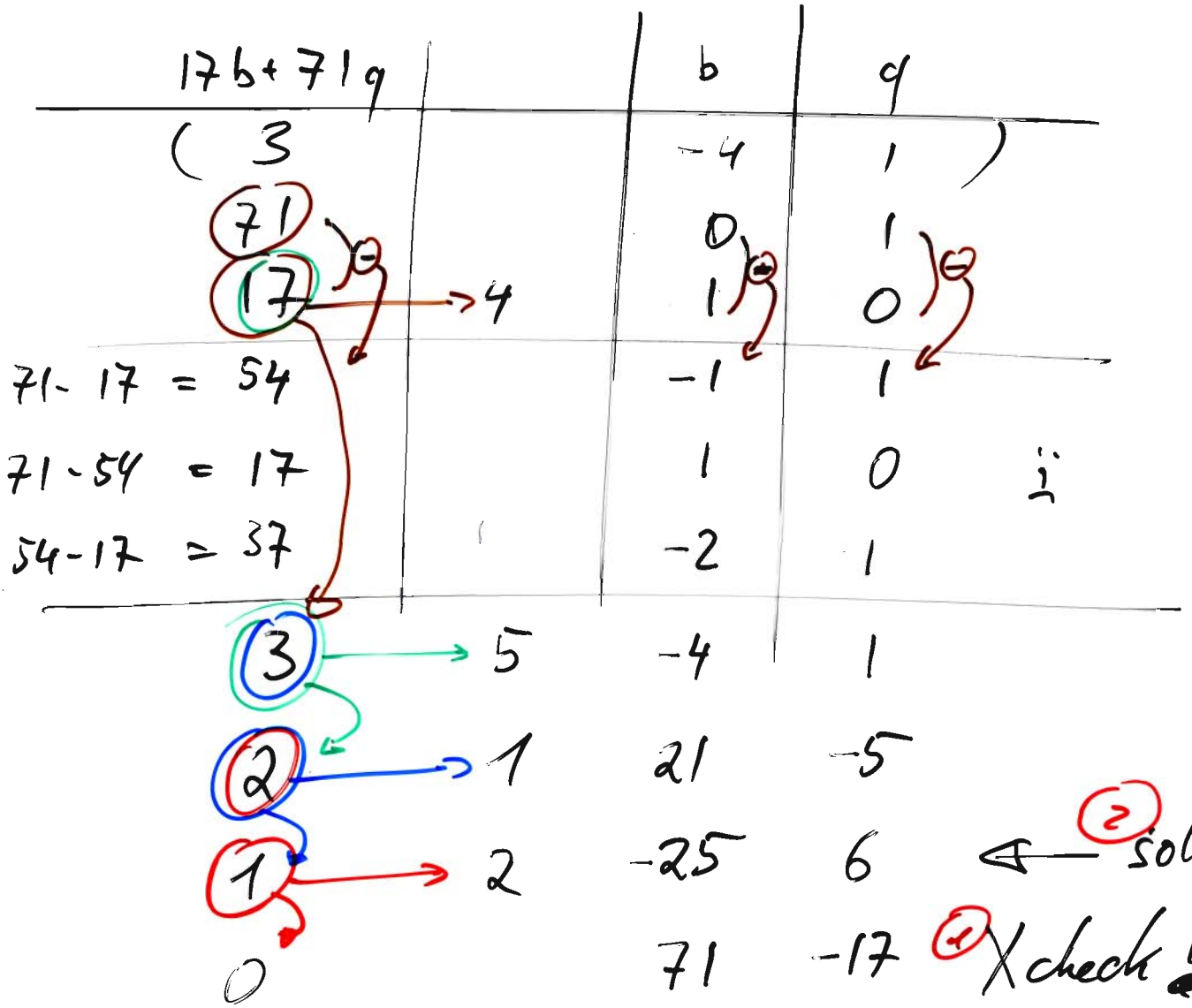
Better?

Observe: 1 is the smallest positive integer.

Try instead to find
$b, q \in \mathbb{Z}$ such that

$$17 \cdot b + 71 \cdot q$$

is small (in absolute value).



$17b+71q$		b	q	
(3		-4	1)	
71		0	1	
17	→ 4	1	0	
$71-17=54$		-1	1	
$71-54=17$		1	0	i
$54-17=37$		-2	1	
3	→ 5	-4	1	
2	→ 1	21	-5	
1	→ 2	-25	6	← (2) solution
0		71	-17	(4) X check!

This is an example run of the Extended Euclidean Algorithm (EEA)

We read off the solution (after having done the X check!):

$1 = 17 \cdot (-25) + 71 \cdot 6$ in $\mathbb{Z}$.

Thus $1 = 17 \cdot (-25)$ in $\mathbb{Z}_{71}$

or $\frac{1}{17} = -25$ in $\mathbb{Z}_{71}$.

Another example

$N = 15, \quad a = 3.$

$r = 3b + 15q$		b	q
15		0	1
3	5	1	0
0		−5	1

remainder column

Claim $r_0, r_1 \in \mathbb{Z}$

$q, r_2 \in \mathbb{Z}$ such that

$r_0 = q \cdot r_1 + r_2$ in $\mathbb{Z}$.

Then $\gcd(r_0, r_1) = \gcd(r_1, r_2)$.

Pf .... □

Consequence: The EEA computes as the last non-zero remainder the greatest common divisor of the input elements.

A final example

say $N = 78$, $a = 18$

BriCo
16.10.09
(10)

(1)

$r = 18s + 78t$	q	s	t
78		0	1
18	4	1	0
6	3	-4	1
0		13	-3

(2) Xcheck: $0 = 18 \cdot 13 + 78 \cdot (-3)$?

$\frac{78}{6}$ $\quad$ $-\frac{18}{6}$

(3) Read off:

6 divides both 78 and 18.

Thus $18s + 78t$ always is a multiple of 6.

and thus can never equal 1.

Say: find the inverse of $18 \in \mathbb{Z}_{77}$.

3rd Co
16.10.09
(11)

Ie. solve $18b = 1$ in $\mathbb{Z}_{77}$.

Or: solve $18b + 77q = 1$ in $\mathbb{Z}$.

Rem EEA on 77 and 18:

77		0	1
18	4	1	0
5	3	-4	1
3	1	13	-3
2	1	-17	4
1	2	30	-7
0		-77	18

Xcheck: $0 \stackrel{?}{=} 18 \cdot (-77) + 77 \cdot 18$ ✓

Solution: $1 = 18 \cdot 30 + 77 \cdot (-7)$

Thus $1 = 18 \cdot 30$ in $\mathbb{Z}_{77}$.

or $\frac{1}{18} = 30$ in $\mathbb{Z}_{77}$.

BriCo
16.10.05
(12)

Theorem

The Extended Euclidean Algorithm

computes given two numbers r_0, r_1

either:

a solution s, t of the equation

$$s \cdot r_0 + t \cdot r_1 = 1$$

or:

a proof that no such solution exists, by means of the last non-zero remainder $r_e > 1$ which shows that

$$s\, r_0 + t\, r_1$$

always is a multiple of $r_e > 1$ and thus never 1.

In general: the EEA outputs

$$s, t, g$$

such

$$s \cdot r_0 + t \cdot r_1 = g$$

and

$$g = \underline{gcd}(r_0, r_1)$$

greatest common divisor.

△

Thm The EEA always terminates and actually in at most $O(n)$ steps

where n = # of bits in the larger of the ~~two~~ input numbers

ie. in time $O(n^3)$ bit operations.

Actually, it is even in runtime $O(n^2)$ bit operations.

Side remark:

We have just used that multiplying two n-bit integers can be done with $O(n^2)$ bit op's.

This can be done with

$$O(n^{\log_2 3}) < O(n^{1.57})$$ bit op.

by the Karatsuba method

$$(ax+b)(cx+d) = ac\cdot x^2 + (ad+bc)x + bd.$$

$$(a+b)(c+d) - ac - bd$$

Schönhage & ~~Volker~~ Strassen (1971)

$O(n \log n \log\log n)$

Which elements are invertible in $\mathbb{Z}_N$?

BriCo
16.10.09
(14)

$$\mathbb{Z}_N^\times := \{ a \in \mathbb{Z}_N \mid a \text{ is invertible} \}$$

$$= \{ a \in \mathbb{Z}_N \mid \gcd(a, N) = 1 \}.$$

Claim $\mathbb{Z}_N^\times$ is a group.

Pf

P.: $a, b \in \mathbb{Z}_N^\times$. $(ab)^{-1} = b^{-1}a^{-1}$. ✓

A.: ✓

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

C.: ✓

I.: $a \in \mathbb{Z}_N^\times$.

Then $a^{-1} \in \mathbb{Z}_N$

and $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.

Obviously: $(a^{-1})^{-1} = a$.

Thus: $a^{-1} \in \mathbb{Z}_N^\times$! □

Since

$$\frac{\#(\mathbb{Z}_N \setminus \mathbb{Z}_N^{\times})}{\#\mathbb{Z}_N}$$

is very small

we focus on $x \in \mathbb{Z}_N^{\times}$ when trying to prove

$$x^{ed} = x .$$

(That's what we need for the correctness of RSA!)

Actually: if $N = p \cdot q$ then

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

Thus

$$\#\mathbb{Z}_N^{\times} = p \cdot q - p - q + 1$$

$$= (p-1) \cdot (q-1)$$

Back to the experiment...

$$\# \mathbb{Z}_{15}^{\times} = (3-1)(5-1) = 8.$$

$$\mathrm{lcm}(3-1, 5-1) = 4.$$

Now: we are working in a group $G = \mathbb{Z}_N^{\times}$ (the unit group of $\mathbb{Z}_N^{\times}$) and consider exponentiation

$$x \longmapsto x^e.$$

Question: when is $x^e = 1$?

(or: when is $x^i = x^j$?

... but here: $x^{i-j} = 1$!

(assume $i > j$))

Theorem (Lagrange)

Given a group G and $x \in G$

finite

Then $x^{\#G} = 1$.

<u>Pf</u> (Lagrange, in case G commutative)

Consider a list

$$a_1, a_2, \ldots, a_{\#G}$$

of all group elements.
Multiply each element with x:

$$xa_1, xa_2, \ldots, xa_{\#G}.$$

Claim: This is another list of all group elements.

(0) Clearly: $xa_i \in G$.

(i) Assume $xa_i = xa_j$.

Then also $x^{-1}xa_i = x^{-1}xa_j$

$$\underset{a_i}{\shortparallel} \qquad \underset{a_j}{\shortparallel}$$

Thus $i = j$.

(ii) Each a_i occurs on the new list!

Problem: find j such that $a_i = xa_j$.

i.e. $\underbrace{x^{-1}a_i}_{\in G} = a_j$

Thus we find j because the first list is complete.

(iii) Both list have same (finite) length.

Since G is commutative the product over the first list equals the product over the second:

$$a_1 \cdot a_2 \cdot \ldots \cdot a_{\#G} = x a_1 \cdot x a_2 \cdot \ldots \cdot x a_{\#G} .$$

Multiply this with the inverses of $a_1, a_2, \ldots a_{\#G}$:

$$1 \cdot 1 \cdot \ldots \cdot 1 = \underbrace{x \cdot x \cdot \ldots \cdot x}_{\#G} .$$

ie.

$$1 = x^{\#G} .$$

□

Corollary (Euler)

Given N a integer, ≥ 2 and a with $\gcd(a, N) = 1$.

Then

$$a^{\varphi(N)} = 1$$

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

φ ← Euler totient function

Pf: Apply Thm (Lagrange) with $G = \mathbb{Z}_N^\times$. □

Corollary (Fermat)

Given a prime p and $0 < a < p$

Then

$$a^{p-1} \bmod p = 1 .$$

Pf Apply Thm (Euler) with $N = p$ prime. Compute $\varphi(p) = p-1$. □

Thm RSA is correct in most cases!

Pf We have to show

$$x^{ed} = x$$

where $x \in \mathbb{Z}_N^\times$ ($\rightsquigarrow$ most cases!)

and $ed-1$ is a multiple of $L = \#\mathbb{Z}_N^\times$.

Now:

$$x^{ed} = x \cdot x^{ed-1} \quad \text{for some } k.$$

$$= x \cdot x^{kL}$$

$$= x \cdot (x^L)^k = x \cdot 1^k = x. \quad \square$$

Exercise

Compute $2^{3141592502}$ in $\mathbb{Z}_{101}$.

Answer: $= (\underbrace{2^{100}}_{=1})^{31415925} \cdot 2^2 = 4.$

because 101 is prime
& Thm (Fermat)

Exercise

2^{129} in $\mathbb{Z}_{1001}$.

BriCo
16.10.09
(20)

Dumb solution:

$2, 2^2, 2^3, 2^4, 2^5, 2^6, \dots, 2^{129}$

takes 128 multiplications.

Better:

$2, 2^2, 2^4, 2^8, 2^{16}, 2^{32}, 2^{64}, 2^{128}, 2^{129}$

takes 7 squarings + 1 multiplication
= 8 operations.

And in general?

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

Start: $x, x^2, x^{2\cdot 2}, x^{2^3}, x^{2^4}, x^{2^5}, \dots, x^{2^k}$

Square ~~as long as~~ til $2^k \le e < 2^{k+1}$

$x^{2^k} \cdot x^{2^j} = x^{2^k + 2^j} = x^{10\dots010\dots0_2}$

$\le e = 10\dots01101001\dots0_2$

Example: x^{37}: $x, x^2, x^4, x^8, x^{16}, x^{32}, x^{36}, x^{37}$

That needs at most $2(n-1)$ multiplications of n-bit numbers

(where N is an n-bit number, $2^{n-1} \le N < 2^n$).

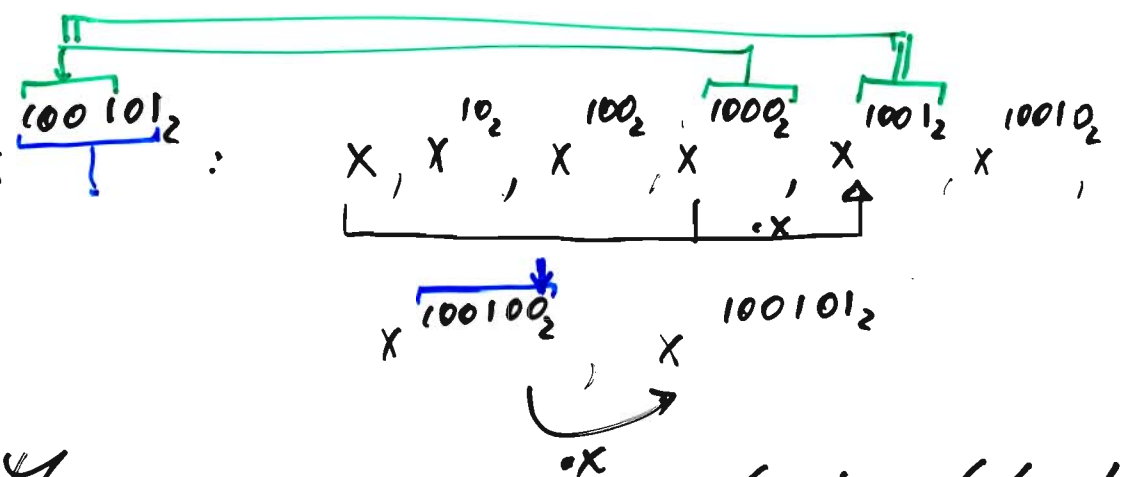
~~Another~~ Example again:

$x^{37} = x^{100101_2}$: $x, x^{10_2}, x^{100_2}, x^{1000_2}, x^{10000_2}, x^{100000_2}, x^{100100_2}, x^{100101_2}$

Bad feature: need to store all intermediate results.

Better:

$x^{37} = x^{100101_2}$: $x, x^{10_2}, x^{100_2}, x^{1000_2}, x^{1001_2}, x^{10010_2}$



This: Square and Multiply.

Runtime of this in $\mathbb{Z}_N$:

$x \in \mathbb{Z}_N^\times$, $e \in \mathbb{Z}_{\varphi(N)}$. Now computing x^e takes at most $O(n^3)$ bit operations.

Running RSA

Setup
- → generate primes $\tilde{\mathcal{O}}(n^4)$
- → compute N, L $\mathcal{O}(n^2)$
- → find e, d

(need: $ed = 1$ in $\mathbb{Z}_L$!)

choose $e \in_R \mathbb{Z}_L$ and
use EEA to compute $d = e^{-1}$

repeat until $e \in \mathbb{Z}_L^\times$.

more e, d to $\mathbb{Z}$. (Forget about L!)

Price: $\mathcal{O}(n^2)$

- → Publish.

Encrypt / Decrypt:
one exponentiation $\mathcal{O}(n^3)$

Thm RSA is efficient.
(i.e. polynomial time).