JAKOB NORDSTRÖM
THEORY GROUP, KTH CSC
www.csc.kth.se/~jakobn
jakobn@csc.kth.se

But... Don't send e-mail
Sign up at Piazza
piazza.com/kth.se/fall2014/dd2442

Course webpage
www.csc.kth.se/DD2442/semteo14

Course webpage contains all info about course (so no "kurs-PM" handout).
Newsupdates posted to webpage and Piazza

Schedule
Tuesday mornings are problematic for several reasons.
Please fill in poll at
doodle.com/id3wbps4xa4sdh2v
as soon as possible!

Course material
No textbook
Some lectures based on textbook chapters or lecture notes, others on research papers.
Will try to produce my own semi-readable handwritten notes and put scanned PDFs online
(No firm promises, though...)

Examination — Hand in by the deadlines

Problem sets: Graded A–E (Lec 1 2)
Need pass on all to pass

Peer evaluation: pass / fail
Read more on course webpage

For top grade A: Read and present paper

Goals:

- Get you to work in depth with material
- Need to get your "hands dirty" to learn – cannot just learn by reading
- Also learn to read other persons' texts and assess correctness and quality of exposition

Rest of today:

- Brief overview of rest of course
- Recap of some standard concepts and facts in abstract algebra

Next time

- Some more algebra recap
- But mostly action

And then more and more action as the course continues... (Towards the end, probably skip details in proofs to cover more material)

Ramsey graphs: How large can graphs be without containing cliques or independent sets of some given size? Questions like this studied in Ramsey theory, which could easily be the topic of a separate course (or several) – we will barely scratch the surface.
Some applications/connections are to: number theory, Kakeya problem, coding theory, computational geometry, computational complexity lower bounds, extraction of "true randomness" from impure randomness sources.
Will see some constructions using simple linear algebra.

Expander graphs: How can one construct very sparse graphs that are essentially as well-connected as complete graphs? Again, this could easily be the topic of a separate course (and perhaps will be in a few years, if someone in the TCS group gets the necessary energy). And again, we will just scratch the surface.
Applications: Robust networks, derandomization, error-correcting codes, data structures, computational complexity lower bounds.
Will use linear algebra to analyze a graph by looking at its adjacency matrix and look at connections between expansion and eigenvalues of this matrix.
Also, algebra can be used to construct good expanders. Hope to see some of this.

Error-correcting codes: How can one transmit messages reliably over a noisy channel?
Spoiler alert: One way is to use evalutations of polynomials. Used e.g. in CDs. We will look at how to construct such codes and how to decode messages efficiently even if they have been corrupted.
This is a fascinating (and very active) research area with many beautiful results. Has been the topic of a separate course in the TCS group, although this was a while back.

Circuit complexity: How can one prove lower bounds on circuits computing Boolean functions?
Approach towards separating *P* and *NP*.
General model: AND-, OR-, NOT-gates of bounded fan-in. Most functions are hard to compute (counting argument) but very hard to prove lower bounds.
Restricted models: E.g. bounded depth. State of the art: strong lower bounds for circuits using AND-, OR-, NOT-, MOD-gates (ACC_0).
Proof technique uses polynomials in ingenious ways.

Interactive and probabilistically checkable proofs: How can interaction between computational agents be used to exactly characterize classical complexity classes?
NP: Problems with solutions verifiable in polynomial time.
PSPACE: Problems solvable in with memory usage scaling polynomially in problem instance size.
Interactive proofs:
(1) Verifier: polynomial-time bounded.
(2) Prover: All-powerful, but might not be trustworthy.
Verifier wants to interact with prover to solve problems but without being fooled.
Such games can be used to exactly characterize, e.g., *NP* and *PSPACE*.
How? Among other things by using polynomials.

Kakeya conjecture for finite fields:
Kakeya problem: How large volume must a body have if a 1 cm needle can be turned from any direction to any direction inside this body?
Finite field version: How large must a set of vectors be to contain a line in every direction in a vector space? Attracted some of the very

brightest minds in math – Spectacular(ly simple) solution by TCS PhD student in 2008.

Low-degree testing: Given a (huge) function table for a multivariate function, is it possible to probe the table in just a few positions and decide with high confidence whether the function is a low-degree polynomial or not?
Fundamental question about polynomials.
Of fundamental importance for, e.g., hardness of approximation: proving that some problems are not only *NP*-hard to solve exactly, but that even getting approximate solutions is also *NP*-hard.

Polynomial identity testing: Very efficient probabilistic methods are known to test whether two polynomials are the same, but is there a way to do this deterministically?
Another fundamental question about polynomials.
Deep connections to central problems in computational complexity.
Will have guest lectures by a leading expert on this.

We probably will not be able to cover all of the above. Topics left out could be suitable for reading projects, though.

SOME ALGEBRA BACKGROUND

GROUP For a set G and an operator $\circ : G \times G \to G$, the pair $(G, \circ)$ is a GROUP if

1) $\exists e \in G$ s.t. $\forall a \in G \quad a \circ e = a$ (identity)
2) $\forall a, b, c \in G \quad a \circ (b \circ c) = (a \circ b) \circ c$ (associativity)
3) $\forall a \in G \; \exists b \in G$ s.t. $a \circ b = e$ (inverse)

$(G, \circ)$ is ABELIAN if $\forall a, b \in G \quad a \circ b = b \circ a$

Some conventions

- In general case: The identity often written 1 and inverse a^{-1}
- For Abelian groups, group operation written $+$
- For Abelian groups, identity written 0 and inverse $-a$

A group is CYCLIC if there is a $g \in G$ that generates the whole group, i.e. $G = \{ g^n \mid n \in \mathbb{Z} \}$
(where $g^n = \underbrace{g \circ g \circ \cdots \circ g}_{n \text{ times}}$)

Examples

a) Integers $\mathbb{Z}$ under addition
b) Positive rational numbers $\mathbb{Q}^+$ under multiplication
c) Invertible $n \times n$ matrices over $\mathbb{R}$ under multiplication (not Abelian)

Often abuse terminology a bit by saying that "G is a group" assuming that the group operation is understood from context

RING For a set R and binary operators $\circ : R \times R \to R$, $+ : R \times R \to R$ over R, the triple $(R, +, \circ)$ is a RING (WITH UNITY) if

1) $(R, +)$ is an Abelian group with identity element $0 \in R$
2) $\exists\, 1 \in R$ s.t. $\forall a \in R \quad a \circ 1 = a$
3) $\forall a, b, c \in R \quad a \circ (b \circ c) = (a \circ b) \circ c$

(2) and (3) together: $(R, \circ)$ is a MONOID

4) $\forall a, b, c \in R \quad a \circ (b + c) = a \circ b + a \circ c$

Convention: multiplication binds higher than addition →

A ring is COMMUTATIVE if $\forall a, b \in R \quad ab = ba$

An element $a \in R$, $a \neq 0$ is a ZERO DIVISOR if $\exists\, b \in R$, $b \neq 0$, s.t. $a \circ b = 0$

A ring that does not have zero divisors is an INTEGRAL DOMAIN

Examples

a) The integers $\mathbb{Z}$ with addition and multiplication is an integral domain
b) The ring of polynomials $\mathbb{Z}[x]$ with polynomial addition and multiplication of polynomials with integer coefficients is a ring (actually an integral domain).

FIELD For a set F with binary operators $+, \cdot$ over F, the triple $(F, +, \cdot)$ is a FIELD (sv. KROPP) if

1) $(F, +, \cdot)$ is an integral domain.
2) $(F \setminus \{0\}, \cdot)$ is an Abelian group

Can also write out explicit list of field axioms if we like

	Addition	Multiplication
Associativity	$(a+b)+c = a+(b+c)$	$(ab)c = a(bc)$
Commutativity	$a+b = b+a$	$ab = ba$
Distributivity	$a(b+c) = ab+ac$	$(a+b)c = ac+bc$
Identity	$a+0 = a = 0+a$	$a \cdot 1 = a = 1 \cdot a$
Inverses	$a+(-a) = 0 = (-a)+a$	$a \cdot a^{-1} = 1 = a^{-1} \cdot a$ if $a \neq 0$

From now on: boldface $\mathbb{F}$ denotes generic field

Examples

a) Rational numbers $\mathbb{Q}$
b) Real number $\mathbb{R}$
c) $\mathbb{Z}/p\mathbb{Z}$ Integers counting mod p for a prime p

Math notation $GF(p)$ - for Galois field
CS notation $\mathbb{F}_p$ - what we will usually write

Field elements are $\{0, 1, 2, \ldots, p-1\}$
Standard addition and multiplication, but reduce mod p

subscript = # elements in (finite) field

For any $a \in \mathbb{Z}$, can write it uniquely as

$$a = q \cdot p + r \qquad 0 \le r < p$$

$$(a \bmod p) = r$$

In $\mathbb{F}_{17}$

$$11 + 9 = 3$$
$$6 \cdot 3 = 1$$

How do we know $\mathbb{F}_p$ is a field?

- Straightforward to check that addition and multiplication work as they should (reducing mod p doesn't change anything)
- Additive inverse easy $(-a) = p - a$
- Multiplicative inverse?

Recall; for any $a, b \in \mathbb{Z}$ (let's say $a, b > 0$) their greatest common divisor $d = GCD(a, b)$ (let's insist $d > 0$) can be written as

$$k \cdot a + \ell b = d$$

for some $k, \ell \in \mathbb{Z}$

For prime p, $a < b$, $GCD(a, p) = 1$.

Setting $b = p$, we get $a^{-1} = k$.

What is the inverse of 7 in $\mathbb{F}_{17}$? Use Euclidean algorithm

$$17 = 2 \cdot 7 + 3$$
$$7 = 2 \cdot 3 + (1) \quad \text{GCD}$$

so $7^{-1} = 5$

$$1 = 7 - 2 \cdot 3 = 7 - 2(17 - 2 \cdot 7) = 5 \cdot 7 - 2 \cdot 17$$

And one final algebraic structure...

VECTOR SPACE A set V (whose elements are called VECTORS) along with a vector addition operation $+ : V \times V \to V$ and a scalar multiplication operation $F \times V \to V$ is a VECTOR SPACE over the field F if

1) $(V, +)$ is an Abelian group
2) $\forall \alpha \in F \; \forall x, y \in V \quad \alpha(x+y) = \alpha x + \alpha y$
3) $\forall \alpha, \beta \in F \; \forall x \in V \quad (\alpha+\beta)x = \alpha x + \beta x$
4) $\forall \alpha, \beta \in F \; \forall x \in V \quad \alpha(\beta x) = (\alpha\beta)x$
5) $\forall x \in V \quad 1 \cdot x = x$ where 1 multiplicative identity unit of F

(2)-(3) distributivity
(4) associativity
(5) identity field element

A map ψ between two groups/rings/fields/vector spaces is an ISOMORPHISM if it

1) is one-to-one / injective
2) is onto / surjective
3) preserves results of all algebraic operations
i.e., for any operation $\circ$ it holds that
$\psi(a) \circ \psi(b) = \psi(a \circ b)$

Two isomorphic objects are "the same" for all practical purposes.

PROPOSITION All finite vector spaces V over a field $\mathbb{F}$ are isomorphic to $\mathbb{F}^n$ for some n.

$$V = \{ (x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{F} \}$$

Coordinate-wise addition and multiplication.

SOME MORE FACTS ABOUT FINITE FIELDS

DEF A field is PRIME if $|\mathbb{F}| = p$ for some prime p.

THM For every prime p there exists a finite field $\mathbb{F}_p$ of size p, and it is unique up to isomorphism

Proof sketch Suppose K, L fields, $|K| = |L| = p$. Let ψ map 0_K to 0_L, 1_K to 1_L. Verify that this is an isomorphism. $\mathbb{Z}/p\mathbb{Z}$ shows there exists such a field.

Notation Write $\mathbb{F}^* = F \setminus \{0\}$ to denote the MULTIPLICATIVE GROUP of $\mathbb{F}$.

LEMMA For a finite field $\mathbb{F}$ it holds that $\mathbb{F}^*$ is cyclic.

Proof is not hard but requires a bit too much algebra for us at this point

Example Look at $\mathbb{F}_7 = \{0,1,2,3,4,5,6\}$. We have

3
$3^2 = 9 = 2$
$3^3 = 6$
$3^4 = 18 = 4$
$3^5 = 12 = 5$
$3^6 = 15 = 1$

so 3 generates $\mathbb{F}_7^*$

DEF The CHARACTERISTIC of a field $\mathbb{F}$, $\mathrm{char}(\mathbb{F})$, is the smallest positive integer n such that $n \cdot 1 = \underbrace{1+1+\dots+1}_{n} = 0$, or 0 if no such n exists.

Examples $\mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{Q}) = 0$

$\mathrm{char}(\mathbb{F}_p) = p$ for a prime p

LEMMA Any finite field has prime characteristic.

THM Let p be a prime ~~$\mathbb{P}$~~ and let $r \in \mathbb{N}^+$. Then there exists a field $\mathbb{F}_{p^r}$ of order p^r (i.e., with p^r elements) and it is unique up to isomorphism.

The way to prove this is to actually construct such fields, starting from "base fields" $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, but it would take us too far right now.

SOME MORE FACTS ABOUT POLYNOMIAL RINGS

(Univariate) polynomial in $\mathbb{F}[x]$

$$f = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0$$

DEGREE of polynomial = largest degree of monomial with non-zero coefficient

Just as for integers, can do Euclid's algorithm to find a greatest common divisor

Division Lemma

Let $f, g \in \mathbb{F}[x]$. Then there exists a unique pair (q, r), $q, r \in \mathbb{F}[x]$, such that

$$f = q \cdot g + r$$

and

$$\deg(r) < \deg g.$$

Proof Existence follows from standard polynomial division. To argue uniqueness, suppose

$$f = q \cdot g + r = q' \cdot g + r'$$

Then

$$(q - q')g - (r - r') = 0$$

If $q \neq q'$, then $(q-q')g$ has higher degree than $r - r'$ and so can't cancel.
If $q = q'$ then this forces $r = r'$ since otherwise LHS nonzero. ∎

Can use this to compute GCD by Euclidean algo:

$$f = q_1 g + r_1 \qquad GCD(f, g) = GCD(g, r_1)$$
$$g = q_2 r_1 + r_2 \qquad GCD(g, r_1) = GCD(r_1, r_2)$$
$$r_1 = q_3 r_2 + r_3 \qquad GCD(r_1, r_2) = GCD(r_2, r_3)$$
$$\vdots$$

Until get $r_j = 0$

Aside: Can explicitly construct fields $\mathbb{F}_{p^r}$ by starting with $\mathbb{F}_p$ and count in polynomials over $\mathbb{F}_p[x]$ modulo some irreducible polynomial p of degree r — won't need this.

A polynomial $f \in F[x]$ is IRREDUCIBLE if there are no polynomials $g, h \in F[x]$, $0 < \deg(g), \deg(h) < \deg(f)$, such that

$$f = g \cdot h$$

analogue of primes among integers

This depends heavily on the field.

$x^2 + 1$ is irreducible over $\mathbb{Q}[x]$.

Over $\mathbb{F}_2$ $(x+1)(x+1) = x^2 + 2x + 1 = x^2 + 1$
so here $x^2 + 1$ is reducible.

Corollary 1 of Division Lemma

Let $f \in F[x]$ and evaluate f over any $a \in F$
Then $f(x) \equiv f(a) \mod (x-a)$

Proof

$$f = q \cdot (x-a) + r \quad \text{for } \deg(r) = 0 < 1$$

I.e. r is a constant in F. Evaluating f yields

$$f(a) = q(a)(a-a) + r = r$$

Hence f divided by $(x-a)$ gives remainder $f(a)$.

Corollary 2

If $f \in F[x]$ has degree r, then f has at most r roots in F.

Proof If a is a root, then $f = q \cdot (x-a)$ where $\deg(q) = \deg(f) - 1$. This can happen at most r times.

This corollary is a (simple but) extremely useful fact that we will use over and over