KTH Computer Science and Communication

Algebraic Gems in TCS: Problem Set 1

Due: Thursday Oct 30, 2014, at 23:59. Submit your solutions as a PDF file by e-mail to `jakobn at kth dot se` with the subject line `Problem set 1: ⟨your full name⟩`. Name the PDF file `PS1_⟨YourFullName⟩.pdf` (with your name coded in ASCII without national characters), and also state your name and e-mail address at the top of the first page. Solutions should be written in LaTeX or some other math-aware typesetting system. Please try to be precise and to the point in your solutions and refrain from vague statements. *Write so that a fellow student of yours can read, understand, and verify your solutions.* In addition to what is stated below, the general rules stated on the course webpage always apply.

Collaboration: Discussions of ideas in groups of two people are allowed—and indeed, encouraged—but you should write down your own solution individually and understand all aspects of it fully. You should also acknowledge any collaboration. State at the beginning of the problem set if you have been collaborating with someone and if so with whom. (Note that collaboration is on a per problem set basis, so you should not discuss different problems on the same problem set with different people.)

Reference material: Some of the problems are "classic" and hence it might be easy to find solutions on the Internet, in textbooks or in research papers. It is not allowed to use such material in any way unless explicitly stated otherwise. Anything said during the lectures or in the lecture notes should be fair game, though, unless you are specifically asked to show something that we claimed without proof in class. It is hard to pin down 100% formal rules on what all this means—when in doubt, ask the lecturer.

About the problems: Some of the problems are meant to be quite challenging and you are not necessarily expected to solve all of them. A total score of around 120 points should be enough for grade E, 155 points for grade D, 190 points for grade C, 225 points for grade B, and 260 points for grade A on this problem set. Any corrections or clarifications will be given at `piazza.com/kth.se/fall2014/dd2442/` and any revised versions will be posted on the course webpage `www.csc.kth.se/DD2442/semteo14/`.

1 (50 p) Let us warm up by doing some exercises in abstract algebra.

1a Recall that a group G is cyclic if it can be written $G = \{g^n \mid n \in \mathbb{Z}\}$ for some generator g. Prove that a cyclic group is abelian, i.e., that for any $a, b \in G$ it holds that $a \cdot b = b \cdot a$.

1b Recall that an integral domain is a commutative ring with unity that does not have zero divisors. Prove that a finite integral domain is in fact a field.

1c We mentioned in class that the multiplicative subgroup $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ is cyclic if $\mathbb{F}$ is a finite field. Is the finiteness condition essential here, or does this in fact hold for all fields?

1d A (univariate) polynomial $p \in \mathbb{F}[x]$ is *irreducible* if there are no two polynomials $q_1, q_2 \in \mathbb{F}[x]$ of degree strictly less than p such that $p = q_1 q_2$. Find an irreducible polynomial p^* of degree 3 over $\mathbb{F}_2[x]$ and prove that p^* is indeed irreducible.

Comment: There are various formal criteria that guarantees that polynomials are irreducible, but this is not what we are looking for here. You should just find a polynomial and prove that it is irreducible from first principles.

1e For any (univariate) polynomials $f, g \in \mathbb{F}[x]$, $g \neq 0$, it holds that f can be written as $f = q \cdot g + r$ where $r = 0$ or $\deg(r) < \deg(g)$. This representation is unique, and we say that r is the polynomial f reduced modulo g. Let $\mathbb{F}[x]/\langle g \rangle$ be the set of polynomials of degree stricly less than $\deg(g)$ with addition and multiplication defined as usual except that the end result is always reduced modulo g as above. It is not hard to see that $\mathbb{F}[x]/\langle g \rangle$ is a commutative ring with unity.

Prove that for the irreducible polynomial p^* you found in problem 1d it holds that $\mathbb{F}[x]/\langle p^* \rangle$ is in fact a field, and then provide the following information:

- The number of elements in $\mathbb{F}[x]/\langle g \rangle$.
- A generator g of the multiplicative subgroup $(\mathbb{F}[x]/\langle g \rangle)^*$. together with a full list $g, g^2, g^3, g^4, \ldots$ of all elements in $(\mathbb{F}[x]/\langle g \rangle)^*$ in the order generated by g.
- A full list of all generators of of the multiplicative subgroup.

Comment: This is one particular example of a general method for constructing finite fields of any given (prime power) size q.

2 (50 p) Recall that the rules for forming clubs in *Even town* are as follows:

- Every club must have an even (and non-zero) number of members.
- No two clubs can have exactly the same set of members.
- Every two clubs must share an even number of members.

2a Prove that if Even town has n citizens, then $2^{\Omega(n)}$ clubs can be formed.

2b What is the best *upper bound* you can obtain on the number of clubs for n citizens? You may assume that n is even.

Hint: You might want to use that for the null space $L^\perp$ of a linear space $L \subseteq \mathbb{F}^n$ (as defined in class) it holds that $\dim(L^\perp) = n - \dim(L)$.

3 (30 p) Suppose that P is a set of n points in the plan, not all on one line. Prove that the pairs of points $(p_1, p_2) \in P^2$ define at least n distinct lines.
Hint: Use Fisher's inequality.

4 (30 p) Prove that there cannot exist any families of (n, d, ρ)-edge expanders for $\rho > d/2$.
Hint: Show that there must exist a subset S of $n/2$ vertices such that $|E(S, \overline{S})| \approx dn/4$.

5 (60 p) The purpose of this problem is to deal with some technicalities that we swept under the rug when presenting the explicit expander construction based on graph products.

5a Prove that if G is an (n, d, λ)-spectral expander with normalized adjacency matrix A, then the (multi-)graph G^2 with normalized adjacency matrix A^2 is an (n, d^2, λ^2)-spectral expander.

5b In class we actually defined the graph matrix product $G_1 \cdot G_2$ in general for arbitrary undirected regular graphs G_1 and G_2 as long as $|V(G_1)| = |V(G_2)|$, although we only used the properties of this product for graphs G^2 as in problem 5a to claim that if G is an n-vertex d-regular graph with $\lambda(G) = \lambda$, then it holds that $G^2 = G \cdot G$ is an n-vertex d^2-regular graph with $\lambda(G^2) = \lambda^2$.

For the other graph products we considered more general statements, the analogue of which would be the claim that if G_1 is an (n, d_1, λ_1)-spectral expander and G_2 is an (n, d_2, λ_2)-spectral expander, then $G_1 \cdot G_2$ is an $(n, d_1 d_2, \lambda_1 \lambda_2)$-spectral expander. Can we prove such a statement for matrix product as well, only that we do not really need it? Please decide whether the statement is true or false and back it up with a proof.

5c When analysing the spectral properties of graph tensor products $G_1 \otimes G_2$ (which as we recall are defined in terms of tensor products of the corresponding normalized adjacency matrices), we claimed that if A is an $n \times n$ matrix with eigenvectors $\mathbf{u}^1, \ldots, \mathbf{u}^n$ and corresponding eigenvalues $\alpha_1, \ldots, \alpha_n$ and B is an $m \times m$ matrix with eigenvectors $\mathbf{v}^1, \ldots, \mathbf{v}^n$ and corresponding eigenvalues $\beta_1, \ldots, \beta_n$, then $A \otimes B$ has eigenvectors $\mathbf{u}^i \otimes \mathbf{v}^j$ and corresponding eigenvalues $\alpha_i \beta_j$ for $i \in [n]$, $j \in [m]$. Prove this claim.

5d In our analysis of the expansion properties of the replacement product, towards the end we went so fast as to completely ignore that we needed to bound the matrix norm of tensor products. In particular, we implicitly used that for any symmetric matrix B it holds for the matrix norm of the tensor product $I_n \otimes B$ that $\|I_n \otimes B\| \leq \|B\|$. Prove this claim.

5e Although we did not pay much attention to this during the lecture, it is not hard to see that our expander construction is in fact strongly explicit, which by what was said in class means that we can plug in this expander in the randomness reduction argument that we covered right before starting the expander construction. Could we have been a bit more relaxed and used a merely explicit expander construction to get the same kind of randomness reduction? Explain why this works or why it does not.

6 (80 p) In this problem we want to study properties of the spectrum of normalized adjacency matrices of undirected, regular graphs, some of which were claimed without proof in class. In all of the problems below, we let G be an undirected n-vertex d-regular graph (for $d > 0$) with normalized adjacency matrix A (also known as the random-walk matrix of G), and we write $\mu_1 \geq \mu_2 \geq \ldots \geq \mu_n$ to denote the eigenvalues of A sorted in decreasing order.

6a Suppose that B is any $n \times n$ real, symmetric matrix that can be decomposed as $B = UVU^T$, with $V = \mathrm{diag}(\nu_1, \ldots, \nu_n)$ being a diagonal matrix and U being an orthonormal matrix (this is known as a *symmetric eigenvalue decomposition* and is guaranteed to exist by the Spectral theorem). Verify that the columns $\mathbf{u}_i$ of U are indeed eigenvectors of B with corresponding eigenvalues ν_i.

6b We say that two $n \times n$ matrices B and C are *similar* if there exists a matrix P such that $C = P^{-1}BP$. Prove that similar matrices have the same eigenvalues with the same multiplicity. (You can assume that B and C are real and symmetric if you like.)

Hint: This might be useful for the problems below, since it allows you to massage A as convenient without loss of generality.

6c Prove that $\mu_1 = 1$ and that the multiplicity of this eigenvalue is equal to the number of connected components of G (so, in particular, $\mu_2 < 1$ if and only if G is connected).

6d Prove that $\mu_n < 0$.

6e Prove that if G is bipartite, then $\mu_n = -1$, and more generally that if μ is an eigenvalue, then so is $-\mu$ (and with the same multiplicity).

Hint: Here you can use problem 6b again.

7 (60 p) ***For this problem, and for this problem only, please feel free to use textbooks, search in the research literature, or roam the internet to find helpful information.***

Let us say that a *Ramsey graph* $G(s,t)$ is a graph that has no independent set of size s and no clique of size t. The *Ramsey number* $R(s,t)$ is the smallest n such that no Ramsey graph $G(s,t)$ exists. Let $x_{i,j}$, $1 \leq i < j \leq n$, be propositional variables and consider the CNF formula

$$F_n^{s,t} = \bigwedge_{\substack{S \subseteq [n] \\ |S|=s}} \bigvee_{\substack{i,j \in S \\ i \neq j}} x_{i,j} \;\wedge\; \bigwedge_{\substack{T \subseteq [n] \\ |T|=t}} \bigvee_{\substack{i,j \in T \\ i \neq j}} \overline{x}_{i,j} \;.$$

If we think of $x_{i,j}$ as encoding the existence or non-existence of an edge (i,j) in an n-vertex graph, we can see that $F_n^{s,t}$ is satisfiable if and only if there is a Ramsey graph $G(s,t)$ on n vertices.

7a Can you compute any interesting Ramsey graphs (and exact Ramsey numbers) by feeding formulas $F_n^{s,t}$ to a state-of-the-art SAT solver? Please give examples of both constructions and Ramsey numbers obtained in this way, and identify the limits for this approach (where we consider a formula to be beyond the limits of what we can handle if that SAT solvers does not solve it in half an hour on a workstation, say).

7b Looking at the literature, does there seem to have been any serious use of SAT solvers to compute Ramsey numbers? If so, how large Ramsey numbers can one compute by using SAT solving, and are there any other encodings than $F_n^{s,t}$ and/or any additional tweaks used in order to get these results?

7c Looking at the literature, can you find any theoretical results that shed light on the potential and limitations of current SAT solving techniques when it comes to attacking propositional encodings of Ramsey graphs/Ramsey numbers such as $F_n^{s,t}$?

Comment: Before starting to do serious computations, please ask for an account on one of our workstations in the TCS group and for some information about which SAT solvers are available and how to use them. Please contact the lecturer via Piazza regarding these questions.