Applied Mathematics MSc - Topics of the Final Exam

1. **Introduction to algorithm theory:**

Turing machines, Graph coloring, Greedy node coloring, The Hungarian method (Alternating path method) Linearization (standard) Perfect Matching via SAT, Balas's algorithm (Lazy version) Satisfiability problem

2. **Integer programing:**

The standardized form of the back-pack problem. Back-pack problems. Branch and bound method.

3. **Fundamentals of Abstract Algebra:**

Basic algebraic structures (semigroups, groups, rings, fields). Subgroups. Group morphisms. Lagrange's theorem. Normal subgroups and quotient groups. Ring morphisms. Subrings and ideals. Quotient rings. Finite fields.

4. **Fundamentals of Number Theory:**

Divisibility, the division algorith, greatest common divisor, the euclidean algorithm, the fundamental theorem of arithmetic, congruences, algebra of residues mod m, Euler's function, RSA algorithm.

5. **Codes and Symmetrical Structures:**

Finite geometry, projective planes, homogenous coordinates, combinatorial properties of finite projective planes, Desargues's plane, affine planes, combinatorial properties of affine planes, latin squares, orthogonality of latin squares, Bruck-Ryser theorem, block design, divisibility conditions, theorem of Wilson, Steiner triple system, Möbius planes, Dobble, SET game, Cayley graphs.

6. **Fundamentals of Analysis:**

Metric spaces, Topological spaces, Continuous functions in metric spaces, complete metric spaces, Eucledian, Hilbert and Banach spaces and their properties, Fixpoint theorem, Orthogonal systems, Sequence and Function spaces, Differentiation and Integration (Riemann, Lebesgue).

7. **Applied Analysis:**

The Fourier series of periodic signals. Convergence propeties of Fourier series: pointwise convergence, uniform convergence, Fejér means, norm convergence. Continuous time Fourier transform. Properties of continuous Fourier transform. Laplace transform. The relation between the Laplace transform and Fourier transform. Propetries of the Laplace transform. Region of

convergence. Discrete Fourier transform, relation between the continuous and discrete transforms. Applications in signal processing.

.

8. **Complex Analysis:**

Analytic functions. Cauchy integral formula. Hardy spaces. Harmonic functions. Their limits to the boundary. Poisson integrals. Approximation of identies and their relation to the Fourier series. Abel-Poisson means of Fourier series.

9. **Information Theory:**

Entropy, relative entropy, mutual information, Kolmogorov complexity.

10. **Numerical Mathematics:**

Machine Numbers, Errors in mathematical modelling, Direct solution of linear systems, Iterative solution of linear systems, solution of nonlinear equations, polynomial interpolations, Hermite and inverse interpolation, piecewise polynomial approximation, least square method, generalized inverse of a matrix, and generalized solution of a linear system, numerical integration, classical quadratures, newton-cotes formulae, Chebyshev and Gaussian quadrature, Approximation in Hilbert spaces, polynomial approximation in the 2-norm.

11. **Probability and statistics:**

Probability models and axioms, Counting, Combinatorics, Discrete Random variables, Continuous Random Variables, Multiple Continuous Random Variables, Conditioning (conditional probabilities) and Bayes' role, independence, Classical statistical inference, Bayesian statistical inference, Discrete and continuous Bayes' Role, Derived distributions, covariance, Iterated expectations, Bernuolli processes, law of large numbers, central limit theorem, Markov processes.

12. **Cryptograpy:**

Symmetric key cryptography, Design principles of encryption methods (Kerchkoffs's principles), the attacker's toolkit, Classical cryptographic protocols (shift cipher, mono-alphabetic replacement, Vigenére cipher, poly-alphabetic shift), Definition of secure encryption, perfect security and secrecy, Computational secrecy, perfectly secret scheme, OTP (one-time pad), random sequences, Security proofs by reduction, pseudorandomness, stream cipher, CPA-secure cipher, Block ciphers, Modes of operation: ECB (Electronic Code Book mode), CBC (Cipher Block Chaining mode), OFB (Output Feedback mode), CTR ((Randomized) Counter mode), Feistel network, Substitution-permutation networks, AES key generation and expansion, Rijndael-test, Hash functions: in data structures, cryptography, Merkle-Damgård construction, Message Authentication Code (MAC), Symmetric vs. public-key crypto.

13. **Ordinary differential equations:**

Classification of ODEs, Initial value problems, First order linear ODE (Bernoulli and Lagrange method), Exact DE, Bernoulli's equation, Ricatti's equation, Clairaut's equation, Integrating factor, High-order DE, Boundary-value problem, differential operator, n-th order (differential) polynomial operator, n-th order linear ODE (homogenuous and non-homogenuous case), variation of parameters method, annihilator operator, Laplace-transform (solving differential equations), inverse Laplace-transform, series solution of ODEs, Differential equation systems.

14. **Partial differential equations PDEs:**

Classification of PDEs, Linear transport equation, elementary PDEs, Boundary conditions, The method of characteristics, quasilinear PDE, Classification of second order PDEs (parabolic, hyperbolic, elliptic): canonical forms, solutions, D'Alambert's method, The Fourier's method of separation of variables, formal solution of the Dirichlet problem, Steady-state solution of PDEs, Weak derivatives, properties of weak derivatives, Sobolev spaces, completeness of Sobolev spaces, approximation by smooth functions, First order Sobolev space, Sobolev inequality, Sobolev-Gagliardo–Nirenberg inequality, Sobolev-Poincaré inequality.

15. **Statistics and applications:**

Sample size calculations, Basics of statistical inference: hypothesis testing, Confidence level, effect size, test power, one- and two sided tests, non-parametrical and parametrical statistical tests, multiple testing correction: post hoc tests, sample size calculation for the variance.

16. **Numerical modelling, numerical solutions of ODEs:**

Numerical methods for the eigen-problem: Localization of eigenvalues, Gershgorin-theorem and its applications, Fadeyev's Trace method, Construction of the characteristic polynomial in tridiagon case, Power iteration, Inverse power iteration and modifications, Jacobi method, LU- and QR-algorithms.

Numerical methods for solving ODEs: Iterative approximation method, Taylor-series method, (Onestep) Euler method, Multistep (implicite) Euler method, Explicite Runge-Kutta methods, Linear Multistep Methods (construction of Adams- and Adams-Bashfort methods)

17. **Integral Geometry:**

Basic concepts of differential geometry, parametrization of curves, curvature, torsion, Frenet formulas, fundamental theorem of curves. Parametrization of surfaces, geodesics, fundamental forms, Gaussian curvature. Radon transform, applications.