

LABORATORI KRIPTOGRAFI, ANALISIS DAN STRUKTUR

1. Kriptografi Bermatematik *Mathematical Cryptography*

Kriptografi merupakan suatu bidang matematik yang berkembang pesat kerana penggunaannya yang meluas dalam keselamatan maklumat. Penyelidikan berkisar idea dan bidang matematik seperti teori nombor, geometri aljabar bermatematik, teori *chaos*, dan lain-lain cabang aljabar. Antara bidang kajian yang utama adalah pencarian algoritma kriptografi yang efisien, pengujian keperdanaan, pemfaktoran integer besar, kriptografi berasaskan *lattice*, kaedah saringan, kriptografi lengkung dan masalah logaritma diskrit. Tujuan utama adalah membina, memperbaiki dan menggunakan protokol kriptografi yang berasaskan matematik yang menjadi piawai kepada keselamatan komunikasi.

Cryptography is a fast developing mathematical field due to its widespread in information security. Research surrounds mathematical ideas and subjects namely number theory, geometric algebra, chaos theory and other related fields. Amongst the widespread research areas are to find cryptographic efficient algorithms, primarily testing, factoring large integers, lattice-based cryptography, sieve methods, elliptic curve cryptography discrete log problems and other related fields. Eventual aims are the development, improvement and implementation of cryptographic protocols that are that can become standards for communications security.

2. Matematik Analitik dan Struktur *Analytical and Structural Mathematics*

Bidang ini merangkumi tiga sub-bidang iaitu Kaedah Analitik dalam Teori Nombor, Teori Berstruktur Pelbagai Aljabar dan Analisis Fungsian dan Topologi. Di bawah Kaedah Analitik dalam teori Nombor, antara tajuk-tajuk penyelidikan adalah penentuan penganggaran hasil tambah eksponen untuk polinomial pelbagai-pembolehubah, penganggaran hasil tambah eksponen berganda dua-pembolehubah bagi polinomial berdarjah tinggi, mendapatkan saiz p -adic bagi fungsi faktorial dan masalah persamaan diophatus. Tumpuan utama penyelidikan di bawah Teori Berstruktur Pelbagai Aljabar adalah: mencari kelas isomorphisme dan aljabar Leibniz tak berubah, masalah pengelasan aljabar 'Dissociative' dan 'Dendriform', dan untuk mengkaji sifat-sifat Armendariz dan gelang-Gamma dan pengitlakannya. Penyelidikan di bawah Analisis Fungsian dan Topologi mengkaji kelas tak terhingga dimensi ruang dimensi ruang vector topologi yang muncul dalam analisis fungsian. Ruangan tersebut termasuk ruang Fréchet, ruang-LF dan dual mereka, dan ruang fungsi selanjur nilai nyata $C(X)$ di ruang X Hausdorff sekata lengkap, untuk menamakan beberapa.

This field encompasses three subfields which are Analytical Method in Number Theory, Structural Theory of Algebra and Functional Analysis and Topology. Under the analytical Method in Number Theory, among the research topics are the following: determining an estimation of the exponential sums for multi-variable polynomials, estimation of the multiple exponential sums for two-variable polynomials of higher degree, finding the p-adic sizes of factorial functions and the diophantine equation problems. The main focus of research under Structural Theory of Algebra are finding the isomorphism classes and invariants of Leibniz algebras, classification problems of Diassociative and Dendriform algebras and studying the properties of Armendariz and Gamma-rings and their generalizations. Functional analysis and topology study the classes of infinite-dimensional topological vector spaces that appear in functional analysis. Such spaces include Fréchet spaces, LF-spaces and their duals, and the space of continuous real-valued functions $C(X)$ on a completely regular Hausdorff space X , to name a few.

3. Matematik Kewangan *Financial Mathematics*

Matematik Kewangan adalah bidang matematik yang berkenaan dengan aplikasi kaedah-kaedah matematik kepada penyelesaian masalah dalam pasaran kewangan. Secara umumnya, matematik kewangan akan mendapat dan memanjangkan model matematik atau nombor yang dicadangkan oleh pasaran kewangan atau ekonomi kewangan.

Mathematical Finance is a field of mathematics which is concern with application of mathematical methods to the solution of problems in financial markets. Generally mathematical finance will derive and extend the mathematical and numerical models suggested by mathematical markets or financial economics.

LABORATORI STATISTIK KOMPUTASI DAN PENYELIDIKAN OPERASI

1. Statistik Gunaan dan Komputasi *Applied and Computational Statistics*

Bidang Statistik Gunaan merangkumi pembangunan teknik atau model dan ia melibatkan penggunaan kaedah statistik untuk menyelesaikan masalah yang digunakan dalam kedua-dua bidang Statistik dan pelbagai bidang lain seperti Ekonomi, Alam Sekitar, Pertanian, Biologi, Kejuruteraan, Perubatan dan lain-lain.

Statistik Komputasi adalah penggunaan komputer yang intensif yang menyelesaikan pelbagai masalah statistik secara berkomputer.

Bidang Statistik Gunaan dan Komputasi merangkumi sub-bidang seperti berikut:

- 1) Pemodelan Statistik dan Ramalan
- 2) Statistik Berkompulasi dan Inferens
- 3) Analisis Kebolehpercayaan

Deskripsi yang lebih terperinci bagi sub-bidang adalah seperti berikut:

1) Sub-bidang Pemodelan Statistik dan Ramalan merangkumi bidang Analisis Siri Masa, Ramalan, Pemodelan Ruang, Teori Nilai Ekstrim, Envirometrik, Analisis Regresi dan Rekabentuk Uji kaji. Siri masa adalah suatu jujukan pembolehubah rawak yang dicerapkan dengan satu set indeks. Penyelidikan siri masa berkisar tentang model 'Generalised ARMA (GARMA). Dalam bidang pemodelan ruang penyelidikan ditumpukan kepada model FISSARMA dan model ruang yang bernilai integer. Dalam teori nilai ekstrim penyelidikan ditumpukan kepada pemodelan data ruang ekstrim dan alam sekitar. Penyelidikan dalam analisis regresi di tumpukan kepada diagnostik, teknik teguh dan tak berparameter serta regresi logistik. Diagnostik, Model Linear Am untuk rekabentuk ujikaji dengan respon tak normal dan teknik teguh merupakan penyelidikan terkini.

2) Sub-bidang Statistik Berkompulasi meliputi Statistik Teguh, Diagnostik Berpengaruh, Bootstrapping, Statistik Bayesian, Monte Carlo Rantai Markov (MCMC) dan Perlombongan Data Berstatistik. Dalam statistik teguh, tumpuan penyelidikan kepada regresi teguh, pengecaman titik terpencil, penganggaran parameter bagi model linear dan taklinear dan teknik kawalan kualiti. Teknik bootstrapping teguh merupakan satu lagi tumpuan utama penyelidikan. Statistik Bayesian tertumpu pada maklumat terdahulu, formulasi dan menyelesaikan masalah teori keputusan mudah dan sukar. Penyelidikan MCMC tertumpu pada algoritma MCMC bagi membuat pentakbiran Bayesian ke atas model stokastik yang kompleks. Dalam perlombongan data berstatistik, penyelidikan tertumpu pada pembentukan teknik pentakbiran baharu dalam perlombongan data dengan menggunakan teknik pengoptimuman, banging dan boosting.

3) Sub-bidang Analisis Kebolehppercayaan merangkumi empat bidang penyelidikan iaitu Analisis Mandirian, Statistik Perubatan, Biostatistik dan Kawalan Kualiti. Bidang analisis mandirian adalah cabang statistik yang berkaitan dengan kematian organisma biologi dan kegagalan dalam sistem mekanik. Secara lebih amnya, analisis mandirian melibatkan pemodelan masa hingga sesuatu peristiwa berlaku. Statistik perubatan adalah bidang berkaitan dengan aplikasi statistik dalam bidang kesihatan dan perubatan seperti kesihatan umum, perubatan forensik termasuk sains klinikal. Biostatistik ialah aplikasi statistik dalam bidang biologi yang membawa kepada permohonan tertentu untuk perubatan dan pertanian. Tumpuan penyelidikan ialah mandirian relatif, 'cure fraction', 'survival tree' dan analisis.

Computational Statistics are computer intensive methods to solve existing statistical problems computationally.

The field of Applied and Computational Statistics comprises of the following sub-fields:

- 1) *Statistical Modelling and Forecasting*
- 2) *Computational Statistics and Inference*
- 3) *Reliability Analysis*

A detailed description of these sub-fields are as follows:

1) *The sub-field of Statistical Modelling and Forecasting encompasses Time Series Analysis, Forecasting, Spatial Modelling, Extreme Value Theory, Envirometrics, Regression Analysis and Design of Experiments. Time Series is a sequence of random variables observed over an indexed set. Time series research is centered about Generalised ARMA (GARMA) models. In spatial modeling, research is focused on FISSARMA and integer-valued spatial models. In extreme value theory research is focused on spatial extreme and environmental models. Research interest in regression analysis is focused on diagnostics, robust and nonparametric techniques and logistic regression. Diagnostics, Generalized Linear Model for designed experiments with non-normal response and robust techniques in Design and Analysis of Experiments are also the current research area.*

2) *This sub-field of Computational Statistics and Inference comprises of Robust Statistics, Influence Diagnostics, Bootstrapping, Bayesian Statistics, Monte Carlo Markov Chain (MCMC) and Statistical Data Mining. In robust statistics, research is focused in robust regression, outlier detection, estimation of parameters in linear and non linear models and quality control techniques. A robust bootstrapping technique is another focus area of research. Research interest in Bayesian statistics focuses on prior information, formulation and solution of simple and complicated decision theory problems. The MCMC research interest focuses on the MCMC algorithm for performing Bayesian inferences on complex stochastic models. In statistical data mining, research is focused on developing new inferential techniques in data mining by optimization technique, bagging and boosting.*

3) *The sub-field of Reliability Analysis consists of four areas of research which are Survival Analysis, Medical Statistics, Biostatistics and Quality Control. Survival analysis is a branch of statistics dealing with death in biological organisms and failure in mechanical systems. More generally, survival analysis involves the modeling of time to event data. Medical statistics is the field of medicine dealing with applications of statistics to the field of health and medicine such as a public health, forensic medicine, as well as clinical sciences. Biostatistics is the application of statistics to a wide range of areas in Biology that leads to a particular application to medicine and to agriculture. Research is focused on Relative Survival, Cure Fraction, Survival Tree and Bayesian Survival Analysis.*

2. Penyelidikan Operasi Berkomputasi ***Computational Operations Research***

Bidang ini merangkumi empat bidang penyelidikan iaitu Pengaturcaraan Bermatematik, Penghampiran, Pengoptimuman dan Penyelidikan Operasi. Penyelidikan ditumpukan kepada Algoritma Genetik, Meta-heuristik, Analisis Pengumpulan Data dan sebagainya.

This programme consists of four research area namely mathematical programming, approximation, optimization and operations research. Research is focused on genetics algorithm, meta-heuristics, data envelopment analysis etc.

3. Biologi Bermatematik dan Berkomputasi ***Computational and Mathematical Biology***

Biologi Bermatematik dan Berkomputasi adalah suatu bidang yang menuju kepada perwakilan, analisis dan pemodelan proses biologi menggunakan pelbagai teknik matematik seperti kalkulus, teori kebarangkalian, statistik, teori graf, topologi, sistem dinamik, persamaan pembezaan, teori pengkodan dsb. Ia mempunyai aplikasi praktikal dalam penyelidikan biologi, bioteknologi, biomedik dan juga epidemiologi dan dinamik populasi. Tumpuan penyelidikan kini termasuklah pemodelan penyakit, pemodelan insilico protin dan bioinformatik.

Computational and mathematical biology is an area that aims at the mathematical representation, analysis, and modeling of biological processes using a variety of applied mathematical techniques such as calculus, probability theory, statistics, graph theory, topology, dynamical systems, differential equations, coding theory, and etc. It has practical applications in biology, biotechnology, biomedical research and also epidemiology and population dynamics. Current research interest includes disease modeling, in silico modeling of proteins and bioinformatics.

LABORATORI SAINS BERKOMPUTASI DAN FIZIK BERMATEMATIK

1. Matematik Berkomputasi *Computational Mathematics*

Matematik adalah bidang matematik yang bertujuan secara umumnya dengan cara bagaimana untuk mengira penyelesaian untuk pelbagai masalah dengan menggunakan teori analisis berangka. Melalui pembangunan dan pelaksanaan aturcara komputer, penyelesaian hampiran berangka dapat dicapai berbanding dengan penyelesaian analitik. Oleh kerana komputer kelajuan tinggi semakin membenarkan keupayaan simulasi, kepentingan bidang menjadi lebih ketara. Tumpuan penyelidikan kini termasuk penyelesaian berangka persamaan pembeza jenis biasa, lewat, kabur, beraljabar dan tegar. Kaedah tertumpu kepada kaedah Runge-Kutta, kaedah langkah berganda, kaedah hibrid, kaedah blok dan kaedah berangka selari.

Computational mathematics is the branch of mathematics which is concerned primarily with ways in which to compute results to various problems by applying the theory of numerical analysis. Through the development and execution of sophisticated computer programs, approximate numerical solutions are achieved as opposed to the analytic solutions. As high speed computers provide ever increasing simulation capabilities, the importance of this field has never been greater. Current research interests include the numerical solution of differential equations of types ordinary, delay, fuzzy, algebraic and stiff. The area of focus is the Runge-Kutta method, multistep method, hybrid method, block method and parallel numerical method.

2. Fizik & Kejuruteraan Bermatematik *Mathematical Physics and Engineering*

Fizik & Kejuruteraan Bermatematik adalah umumnya kajian struktur dan teknik matematik dalam sains fizikal dan kejuruteraan. Skop kajian meliputi bidang tradisi matematik gunaan seperti persamaan dinamik bendalir, mekanik kontinum dan sistem dinamik; dan juga bidang-bidang dari sains kuantum dan teori kerelatifan. Termasuk bidang terkemudian adalah peninjauan struktur matematik novel yang mendasari teori kuantum dan ruang-masa, dan topik lazim teori operator, persamaan fizik matematik, dan kaedah bergeometri & bertopologi. Topik yang kini diselidiki adalah masalah retakan, persamaan pembeza-kamiran, asas teori kuantum, maklumat kuantum dan penyelesaian kosmologi.

Mathematical Physics & Engineering is broadly the study of mathematical structures and techniques in physical sciences and engineering. The scope of study covers traditional areas of applied mathematics like equations of fluid dynamics, continuum mechanics, and dynamical systems; as well as those from quantum sciences and relativity. The latter includes exploring novel mathematical structures that underlie quantum theory and space-time, and established topics of operator theory, equations of mathematical physics, and geometric & topological methods. Topical areas of interest are problems of cracks, integro-differential equations, foundations of quantum theory, quantum information and cosmological solutions.

3. Dinamik Bendalir *Fluid Dynamics*

Dinamik bendalir adalah kajian aliran bendalir yang mempunyai banyak aplikasi seperti dalam aerodinamik kenderaan, aliran bahanapi dan hidrologi. Persamaan pembezaan tak linear yang memerihal alir bendalir lazimnya tidak mempunyai penyelesaian bentuk tertutup dan selalunya memerlukan manipulasi analitik yang bijak atau komputasi berangka. Tumpuan penyelidikan kini termasuklah kestabilanalir bendalir, fenomena kecerunan ketegangan permukaan dan alir berbutir.

Fluid dynamics is the study of fluid flow and has many applications such as in aerodynamics of vehicles, fuel flow and hydrology. The nonlinear differential equations that describe fluid flow do not usually have closed-form solutions and often requires either clever analytic manipulations or numerical computations. Recent research interests include stability of fluid flow, surface tension gradient phenomena and granular flow.

4. Elektromagnetik Berkomputasi *Computational Electromagnetics*

Terdapat banyak fenomena fizik yang melibatkan gelombang mekanik dan gelombang elektromagnet melalui pelbagai medium dan dalam pelbagai keadaan. Menyelesaikan persamaan pembezaan separa yang memerihal rambatan gelombang adalah penting dalam banyak aplikasi. Tumpuan penyelidikan kini termasuklah rambatan gelombang elektromagnet dalam telekomunikasi dan dalam sensor.

Many physical phenomena involve mechanical and electromagnetic waves propagating through various mediums and in various conditions. Solving the partial differential equations describing their propagation is of importance to many applications. Recent research interests include propagation of electromagnetic waves in telecommunications and in sensors.

5. Struktur Bolehkomputasi dan Komputasi Sainifik *Computable Structures and Scientific Computing*

Kemajuan dalam Sains Komputer telah menunjukkan komputasi tidak lagi terhad kepada jenis berangka. Struktur yang lebih umum kini telah banyak digunakan untuk manipulasi maklumat dan komputasi. Sebagai tambahan, sistem logik berlainan dan idea umum kebolehan komputasi kini ada dikaji. Kemajuan ini melibatkan pertindihan bidang-bidang matematik tulen, teori sains komputer dan fizik teori. Aplikasi bidang adalah dalam pengaturcaraan simbolik dan grafik, kepintaran buatan, bahasa pengaturcaraan baru ds. Tumpuan penyelidikan kini termasuk teori automata, komputasi kuantum, pangaturcaraan aljabar komputer dan aplikasi.

Advances in computer science have shown that computing is no longer limited to numerical type. More general structures are now very much being used for information manipulation and computing. In addition different logical systems and general ideas of computability are currently being explored. These developments overlap areas of pure mathematics, theoretical computer science and theoretical physics. Application included symbolic and graphic programming, artificial intelligence, new programming language etc. Current research interests include automata theory, quantum computing, computer algebra programming and applications.

LABORATORI ETNOMATEMATIK DAN DIDAKTIK

1. Etnomatematik

Ethnomathematics

Etnomatematik adalah kajian tentang hubungan antara matematik dan budaya yang bertujuan untuk menyumbang kepada pemahaman tentang perkembangan dan perkaitan antara matematik dan budaya.

Ethnomathematics is a study of the relationship between mathematics and culture which is aimed to contribute both to the understanding of culture and mathematics and their interrelationships.

2. Pendidikan Matematik

Mathematics Education

Bidang ini merangkumi pengajian tentang teori dan amalan dalam pendidikan matematik untuk peningkatan pemahaman matematik. Antara pendekatan yang dikaji adalah pendekatan konstruktivisme, masteri, koperatif, kolaboratif, kontekstual, dan pendekatan berasaskan penyelesaian masalah. Perspektif yang juga dikaji adalah berdasarkan cognitive-guided instruction; zone of proximal development; nilai, kepercayaan, dan epistemologi berkaitan pendidikan matematik; perkembangan pemikiran matematik; impak pengintegrasian teknologi dalam pengajaran matematik; rekabentuk teknologi dalam pengajaran matematik; serta isu atau polisi semasa yang berkaitan dengan pendidikan matematik.

The main focus for this branch of research is to study the history of mathematics with respect to the philosophical ideas embedded within selected topics in logic, number theory, algebra, trigonometry, geometry and astronomy.

3. Sejarah dan Falsafah Matematik

Philosophy and History of Mathematics

Fokus utama dalam kajian ini ialah kearah penyelidikan aspek sejarah matematik yang berkaitan dengan falsafah yang tersirat dalam tajuk pilihan tertentu dalam mantik, nombor teori, aljabar, trigonometri, geometri dan falak.

This field covers studies related to theories and practices in mathematics education for the enhancement of mathematical understanding. Amongst the approaches to be investigated are: constructivism; mastery; cooperative; collaborative; contextual learning and problem-based learning. Other pedagogical perspectives include cognitive-guided instruction; zone of proximal development; values, beliefs and epistemology related to mathematics education; development of mathematical thinking; impact of integration of technology in mathematics teaching; technology design in mathematics teaching; and current issues or policies related to mathematics education.