October 12 - 14, 2011

Report from the Workshop on Future Directions in Mathematics

Institute for Pure and Applied Mathematics
University of California, Los Angeles

Summary of the Workshop on Future Directions in Mathematics

Los Angeles, CA
February 8, 2012

ABSTRACT

This report summarizes the Workshop on Future Directions in Mathematics, sponsored by the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), Basic Science Office. The workshop was held at the Institute for Pure and Applied Mathematics (IPAM) at UCLA on October 12-14, 2011. It involved 23 invited scientists and 4 government observers.

1. Executive Summary

This report summarizes the Workshop on Future Directions in Mathematics, sponsored by the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), Basic Science Office. The workshop was held at the Institute for Pure and Applied Mathematics (IPAM) at UCLA on October 12-14, 2011. It involved 23 invited scientists and 4 government observers, listed in Appendix I.

The goals of the workshop were to provide input to the ASD(R&E) on the current state of mathematics research, the most promising directions for future research in mathematics, the infrastructure needed to support that future research, and a comparison of mathematics in the US and in the rest of the world. These goals were articulated through a set of six questions, listed in Appendix II, that were sent to the participants prior to the workshop.

The invited mathematical scientists came from universities and industrial labs, and included mathematicians, statisticians, computer scientists, electrical engineers and mechanical engineers. This group consisted of established leaders in various fields of mathematics, and brilliant young researchers representing recent breakthroughs and future directions. Within this report, the terms “mathematics” and “mathematical sciences” are often used interchangeably.

On the first afternoon of the workshop, each of the scientists gave a brief description of their own field. The second day consisted of a general discussion session and a breakout session in the morning, followed by a reporting session and another general discussion session in the afternoon. A general discussion period occurred on the final morning, focused on the outline of the report.

The participants agreed that the main body of the report should consist of 5 sections:

- Drivers for mathematics; i.e., developments outside of mathematics that influenced mathematics over the last decade
- Recent accomplishments; i.e., the major achievements in mathematics over the past decade

- Future directions; i.e., their best prediction for the most important achievements in mathematics over the next decade
- Infrastructure; i.e., the infrastructure requirements for supporting those future achievements
- International developments; i.e., a critical comparison of mathematics in the US and around the world.

The participants identified 6 main drivers for mathematics:

- Computing
- Big data
- Increasing complexity
- Uncertainty and risk
- Rise of interdisciplinary research
- Connectedness.

The participants identified important accomplishments over the last decade in 7 areas of mathematics:

- Information science
- Discrete mathematics
- Partial differential equations and randomness
- Computation
- Bioinformatics
- Optimization and control
- Nanoscale systems.

The participants expect to see great progress over the next decade in 7 areas of mathematics:

- Simulation
- Information science
- High dimensionality and large data sets
- Mathematics of physical systems
- Mathematical Modeling
- Computational and statistical reasoning
- Imaging.

The participants surveyed the infrastructure needs of mathematics and found areas in which the current infrastructure is strong and healthy, and areas in which the infrastructure needs to be strengthened. The participants also found that mathematics in the US is still very strong relative to the rest of the world, but significant international advantages have developed in some key areas.

This report was assembled and edited, based on inputs from the workshop participants, by Russel Caflisch (UCLA), Robert Kosut (SC Solutions) and Stanley Osher (UCLA), who also organized the workshop. Special thanks go to Wen Masters (ONR) who provided significant input and advice for the organization and to Robin Staffin (DoD) and Stu Wolf (DoD) who originally suggested the workshop and provided much of the motivation. The workshop was made possible by support from the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), Basic Science Office.

2. Drivers for Mathematics

Mathematics has changed significantly over the last two decades. Within the discipline, there has been a blurring of the line between pure mathematics and applied mathematics, as well as development of interactions between many different mathematical fields. At the same time, interactions between mathematicians (both pure and applied) and scientists have greatly increased. We expect these trends to continue, with important new developments in many fields.

2.1 Computing

Much of the recent impetus for mathematics has come from the growth in computing power and in computer networking. The increase in both the availability and the need for computing power has led to development of new computer architectures, new computational algorithms and new computational models. Sophisticated mathematics has been required for analysis of these new computational models and algorithms. One example is quantum computing -- the understanding of which has relied on insights from matrix analysis, representation theory, Lie algebras, and approximation theory to a greater extent than classical computing. Meanwhile, though, the state-of-the-art classical algorithms, even for purely combinatorial problems, have developed an increasingly analytic flavor, so that continuous mathematics has become more and more widespread in the theory of classical computing as well. A few places where this has happened include survey propagation for constraint-satisfaction problems, the multiplicative-weights update method, algorithms for sparse matrices (used heavily in "big data" applications), and approximation algorithms based on convex optimization.

Many of the other drivers described below were instigated or enabled by the growth in computing and networking.

2.2 Big data

Large data sets are an increasing feature of science, technology and society, coming from large scale computations, a plethora of imaging modalities (e.g., medical, entertainment, personal, national defense), sensor networks (e.g. for traffic, weather, astronomy), and networks of agents (social, financial, commercial). The explosion in data is creating tremendous opportunities for better modeling and corresponding demand for new mathematical techniques that both exploit

and are able to handle “big data”. For example, a graph may be so large that we are never able to look at all of it. What can we nevertheless say about it? And how can we reason with knowledge that is necessarily uncertain because it was acquired by learning from data?

2.3 Increasing complexity

Complexity and its significance have been growing in systems of all types. This includes engineered systems such as the internet and the power grid; social systems such as the financial system and social networks; natural systems such as the global climate system and the global ecological system; and mathematical systems such as large scale graphs and multiscale models. This increased complexity requires new approaches to mathematical modeling, new computational algorithms, and new methods of analysis.

2.4 Uncertainty and risk

Uncertainty is an essential feature of many systems. While it has always been present, uncertainty has become more important in many systems because of their increased size and complexity. Examples include: climate for which uncertainties in modeling (e.g., for clouds and for ocean/atmospheric interactions) can make a significant difference in the severity of global warming predictions; the power grid in which small random disruptions can cascade into large systemic power outages; and financial systems, in which risk has long been a central feature but recent examples of financial contagion and collapse demonstrate that current models of risk and techniques for managing risk are not sufficient.

2.5 Rise of interdisciplinary research

Many of the most interesting developments in science and technology over the last two decades have been interdisciplinary, including nanoscience, bioinformatics and sustainability (e.g., climate, environment, energy). The role of mathematics in interdisciplinary research is three-fold: it can provide a common language for people to communicate across fields, it can provide a framework for rigorous analysis, and it can provide new techniques to address problems involving complex physical interactions. Moreover in the last decade, mathematics has been crucial to the development of new methods for extracting information from heterogeneous, high-dimensional data. There are, however, some barriers to success. Linguistic differences challenge the communication among mathematicians, scientists, and engineers, not to mention across fields of mathematics. Different fields have different time scales on which progress is measured as well as different goals, meaning that there are even disagreements as to what constitutes progress, or what is meant by a “result”. Coming to terms with these issues is critical in drawing multidisciplinary teams together.

2.6 Connectedness

Highly connected systems are proliferating, such as networked sensors and actuators, mobile devices and distributed surveillance. They share a communications resource (and sometimes a computing resource) and occupy a dynamically evolving environment including varying priorities of needs. Dynamical systems theory, game theory, decisions with imperfect information, and control with unreliable communication all provide mathematical approaches with which to address this topic. Examples include energy smart grids, air traffic control, surveillance, computer network control, and real-time resource management.

3. Recent Accomplishments

There has been tremendous recent progress in mathematics, which we describe in 7 areas.

3.1 Information science

3.1.1 Compressed Sensing

Many large datasets have a sparse representation, in the sense that the number of significant features in the data is much smaller than the size of the dataset. Compressed sensing provides a method to take advantage of this sparsity; for example, a method for reconstruction of the full large dataset from a number of measurements that is only logarithmically larger than the small number of features. By its combination of harmonic analysis, probability and numerical analysis, compressed sensing epitomizes the new applications of pure mathematics and the interdisciplinary interactions between areas of mathematics. More generally, compressed sensing has inspired the use of sparsity and order reduction in many other areas of mathematics, science, and engineering.

3.1.2 Partial differential equations and stochastic methods for imaging and animation

Automated analysis of images and extraction of features have become important because of the proliferation of imaging. Great progress in image analysis and manipulation of images has been achieved through the use of variational principles and PDEs. For example, PDEs that sharpen interfaces have been used for denoising, and numerical methods based on PDEs have proven to be robust and stable. More recently, non-PDE methods, such as the method of nonlocal means, have been surprisingly successful at image restoration and other imaging tasks such as dictionary based processing. For problems such as oil exploration, the resulting images are dominated by noise; e.g., due to fluctuations in the material properties such as the sound speed. Methods based on stochastic analysis have been successful at extracting features in these problems.

3.1.3 Efficient search algorithms, using graph theory

The emergence of the Web and online social systems give graph theory an important new application domain. We live in a highly interconnected world. Small world phenomena have fascinated the public imagination for many years. With the increased ease of communication, this is true today more than ever. Recent study has found that the average distance between

members of the social network Facebook, that contains roughly half of the world's population above the age of 13, is 4.74. This connectedness and network structure is not limited to our social network, but affects almost all aspects of our lives, including financial networks and the web. Our technological and economic systems are increasingly tightly connected by large networks. Such networks provide great opportunities, but also provide great challenges. The sheer size of these networks makes it hard to study them. The interconnectedness of the financial network makes financial interactions easy, but the recent financial crisis provides a good example of its dangers. Understanding to what extent networks are susceptible to such cascading failures is an important area of study. From a very different domain, the network structure of the web is what makes it most useful. Links provide the web with a network structure. Such links help us navigate on the web, but linking is also a type of endorsement. This network of endorsement is what allows search companies such as Google to effectively find useful pages. Understanding how to harness such a large network of recommendations continues to be a challenge, and our dependence on large networks also presents new challenges.

3.2 Discrete mathematics

3.2.1 Prime progressions

The field referred to as additive/arithmetic combinatorics came to international attention with the celebrated Green-Tao theorem on long arithmetic progressions of primes in 2004. A prime progression is a sequence of prime numbers $p_1, p_2, \ldots, p_L$ such that the difference between any two successive primes p_i and p_{i+1} is equal to the same number K; i.e., $p_{i+1} - p_i = K$ for any i. The Green-Tao Theorem says that for any L and M (no matter how large), there is a prime progression with parameters K and L, for some K>M. The proof of this result used number theory, combinatorics, probability and analysis.

Since 2004 the ideas and techniques have spread in many different directions, touching not only on number theory, combinatorics, harmonic analysis and ergodic theory, but also on geometric group theory, theoretical computer science, model theory, point set topology and other fields. A better name for the field might now be "approximate structures". In any case, it is clear that the algebraic, combinatorial and probabilistic aspects of very large structures (e.g., graphs, networks and matrices) have become a topic of great interest and wide applicability.

3.2.2 Deterministic primality testing

In 2002 the first provably polynomial-time test for primality was invented by Agrawal, Kayal and Saxena. This was a great surprise to the mathematics community and one of the celebrated results of the last decade. It represents important progress both for number theory and for computational complexity.

3.2.3 Langlands program

For the past 40 years, the Langlands Program has provided the thrust for some of the deepest and widest-reaching advances in all of pure mathematics. It ties together number theory,

representation theory, automorphic forms, harmonic analysis, algebraic geometry and even quantum physics - and has been referred to as a "grand unified theory" of mathematics.

To date three Fields Medals have been awarded for work in this area, the most recent being just last year to Ngo Bao Chau for his work on the so-called "Fundamental Lemma".

3.2.4 Lattice-based cryptography

Over the past decade, a new type of public-key cryptography has emerged, whose security is based on the presumed intractability of finding a "good" basis for a high-dimensional lattice (where "good" means that the basis vectors are short). Compared to currently-popular public-key cryptosystems, such as RSA and Diffie-Hellman, lattice-based cryptography promises at least three advantages. First, as far as anyone knows today, lattice-based cryptography would remain secure even against attacks by quantum computers. Second, the encryption and decryption functions in lattice-based cryptography are remarkably simple mathematically -- basically amounting to a matrix-vector multiply, plus addition or subtraction of a small error term. Third, lattice-based cryptography opens up new possibilities for cryptographic protocols: most notably "fully homomorphic encryption," for which arbitrary computations may be directly performed on the data in its encrypted state (discussed further in Section 4.2.1). The study of lattice-based cryptography has led to many beautiful mathematical ideas -- and strangely, understanding the security even of "classical" lattice-based systems has often required arguments and assumptions involving quantum computation. Following an initial proposal by Ajtai and Dwork in 1996, significant breakthroughs in lattice-based cryptography were achieved by Regev, Peikert, and Gentry among others.

3.3 Partial differential equations and randomness

3.3.1 Poincaré conjecture

In 2002-03, Grigoriy Perelman presented a proof of the Poincaré Conjecture that every simply connected, closed 3-manifold is homeomorphic to the 3-sphere. His proof was based on the Ricci-flow method developed by Hamilton. In spite of some initial controversy about the proof, its correctness and full credit to Perelman are now well settled. This was the first solution to one of the seven Millennium Prize Problems from the Clay Mathematics Institute.

3.3.2 Schramm-Loewner evolution (a.k.a. Stochastic Loewner evolution or SLE)

Schramm–Loewner evolution is a conformally invariant stochastic process. It is a family of random planar curves that are generated by solving Loewner's differential equation with Brownian motion as input. Schramm–Loewner evolution is conjectured or proved to describe the scaling limit of various stochastic processes in the plane, such as critical percolation, the critical Ising model, the dimer model, and other statistical mechanics models that exhibit conformal invariance.

3.3.3 Compactness and regularization in PDEs and statistical physics

Compactness of a set of functions in a function space is the property that any bounded sequence of functions in the set has a limiting function. Regularization is a modification of the original PDE in a way that ensures some smoothness properties for the solutions. Analysis of solutions for PDEs often depends on constructing a sequence of approximate solutions depending on some regularization, showing that the approximate solutions lie in a compact set so that a limiting function can be extracted, and finally showing that the limiting function is a solution. For a range of equations from statistical physics (e.g., the Boltzmann equation for rarefied gas dynamics), compactness results have been derived, based on regularization through dispersion, velocity averaging, entropy cutoff or other methods. These techniques have been used to prove existence results and limiting results (e.g., the fluid dynamic limit for the Boltzmann equation).

3.4 Computation

3.4.1 Fast Multipole Methods and analysis-based fast algorithms

The last decade has seen the emergence of analysis-based fast algorithms as a broad generalization of the Fast Multipole Method (FMM) (developed in the 1980s for electrostatic and acoustic applications). FMM-based schemes are now in wide use in stealth modeling, in the chip industry, and in quantum chemistry. Previously intractable problems with millions or billions of unknowns can now be solved routinely using FMM-accelerated iterative schemes. More recently, both "physics-based" and linear algebraic extensions of the method are permitting the fast, direct solution of large-scale linear systems with the potential for a dramatic change in "design by simulation". For example, butterfly schemes allow for fast computation of the Fourier transform or other integral operators, without use of a regular grid (as required by FFT).

3.4.2 Shor's algorithm and quantum information science

In 1994, Shor discovered a remarkable algorithm for factoring integers efficiently using a quantum computer. The factoring problem is important not only because it resisted an efficient classical solution for millennia, but because since the 1980s, its conjectured hardness has been the basis for almost all cryptography used on the Internet. Shor's algorithm provided the first convincing evidence that quantum computers could actually help in solving a practical problem—other than the simulation of quantum mechanics itself.

Since then, the field of quantum computing has exploded in interest. Notable achievements include: Grover's algorithm for searching unordered lists; limitations of quantum algorithms for search, collision-finding, and many other problems; the theory of topological and anyonic quantum computation; the quantum adiabatic algorithm; the theory of quantum proofs (QMA-completeness) and quantum advice; quantum interactive proof systems and the QIP=PSPACE theorem; and quantum communication protocols that provably exponentially outperform classical protocols.

3.4.3 Randomized methods

Compressed sensing and similar computations depend on randomized numerical linear algebra methods. This is not Monte Carlo; randomness is required so that the numerical basis elements have nontrivial intersection with the basis elements in the sparse representation. This has opened up a new field of numerical linear algebra and many open problems remain, such as construction of high order randomized methods.

3.5 Bioinformatics

3.5.1 Sequencing algorithms for genomics

Dramatic advances in massively parallel sequencing technology during the past few years have resulted in a growth rate of genomic sequence data that is faster than Moore's law. Our ability to extract useful information from this massive accumulation of fundamental genetic data hinges on the availability of efficient algorithms for sequence alignment/assembly, and statistical methods for the modeling of sequence variations and the correlation with phenotypic data. Recent accomplishments in this direction include the De Bruijn graph approach to sequence assembly, Bayesian models for SNP and indel calling, variants of hidden Markov models for haplotype reconstruction and population admixture analysis, and advanced statistical methods for controlling false discovery rates in large scale functional genomics analysis.

3.6 Optimization and control

3.6.1 Coordination of autonomous systems

Mathematics has been essential for addressing problem with coordinated autonomous systems. For example, in the coordination of motion for autonomous vehicles, algebraic graph theory, (distributed) dynamical systems and non-smooth analysis were combined to advance the understanding of how local interactions give rise to global emergent behavior. Moreover, for distributed sensing among ad hoc networks of autonomous vehicles, stochastic analysis and game theory have been critical components in the development and performance analysis of consensus algorithms and other approaches to distributed estimation.

3.6.2 Convex optimization

Convex optimization problems are easily solved, but most interesting problems are non-convex. A surprisingly large number of important problems can be convexified, usually by relaxation of the non-convex constraints, resulting often in small or no effect on the optimal solution. Penalization using an L^1 norm, and variants, is a frequent tool in making optimization problems convex. L^1 penalization is also used in statistics (lasso), image processing (TV), shock-capturing methods (TVD), and compressed sensing.

Currently there is an emergence of very efficient software tools, freely available on the internet, which can handle very large problem sizes. Moreover, these tools come with an interface language that is almost one-to-one compatible with how the problem would be stated

mathematically. For even relatively large problem sizes, the tools are now almost as easy to use as standard least-squares or eigenvalue solvers.

3.6.3 Control

For the past several decades the theory of control design has benefited enormously from the infusion of mathematics, e.g., from the pioneering work of Wiener, Bode, and Kalman, to today's common use of user-friendly software tools for design and analysis. There is now a beneficial blur between control, communication, signal processing, and optimization, resulting in the ability to control very complex systems using these sophisticated tools. Increasingly, this blur between control, communication and computation reflects both the common mathematical roots of these disciplines and also the presence of fundamental limitations in each, which are the subject of considerable current research. The conformity of many problems in quantum computing and information with control problems is a case in point. Further, in the more applied areas, control is regarded as a bottleneck technology linking modeling, data analysis, and feedback dynamics. The mathematical underpinnings of control are a significant area of research, especially in the formal handling of modeling and of uncertainty/robustness.

3.6.4 Game theoretic management of networks

In settings ranging from the Internet architecture to global financial markets, interactions happen in the context of a complex network. The most striking feature of these networks is their size and global reach: they are built and operated by people and agents of diverse goals and interests, i.e., diverse socioeconomic groups and companies that each try to use a network to their advantage. Much of today's technology depends on our ability to successfully build and maintain systems used by such a diverse set of autonomous users, and to ensure that participants cooperate despite their diverse goals and interests. Such large and decentralized networks provide amazing new opportunities for cooperation, but they also present large challenges.

Game theory provides a mathematical framework that helps us understand the expected effects of interactions, and develop good design principles for building and operating such networks. In this framework we think of each participant as a player in a non-cooperative game. In the game each player selects a strategy, selfishly trying to optimize his or her own objective function. The outcome of the game for each participant depends, not only on his own strategy, but also on the strategies chosen by all other players. Mechanism theory deals with the setting of objective or payoff functions for the players of a game. These rules inherently reward efficient behavior and punish errant actions by individual players. Game theory more widely deals with the concepts of cooperative or competitive dynamics and of equilibria and strategy. This emerging area is combining tools from many mathematical areas, including game theory, optimization, and theoretical computer science.

3.7 Nanoscale systems

Nanoscale systems present a number of important challenges to mathematics and science. They are maximally complex in that they involve both quantum and classical physics, as well as

continuum, atomistic and n-body phenomena. An important consideration for nanoscale systems is that surface forces often dominate over bulk forces, since the surface to bulk ratio is so large.

3.7.1 Thermal effects

Transitions between local minima are often the most interesting microscopic phenomena in a nanoscale system, and the transitions are often driven by thermal noise. For simple systems with isolated minima and large barrier energies, the nudged elastic band method finds reaction pathways between local minima. These transitions are rare and thus difficult to simulate, but accelerated molecular dynamics methods (including hyperdynamics, parallel replication and temperature accelerated dynamics) developed by Voter and co-workers have proved to be very effective. For more complex systems, such as those with entropic barriers or systems with many small barriers (e.g., bio-molecules in explicit solvent), the transition path sampling technique and the finite temperature string method are so-far the most effective at finding reaction pathways. Many issues still remain, the most important of which is the lack of effective techniques for discrete systems (such as the Ising model). Large deviation theory can serve as a mathematical basis for these methods.

4. Future Directions

Looking toward the next decade, we foresee significant progress in 7 areas.

4.1 Simulation

4.1.1 Simulation-based science and engineering

Modern simulation is now sufficiently fast and accurate that it can be used for many science and engineering purposes. In many systems, some important degrees of freedom that cannot be measured experimentally are accessible through computation. An example is the wave function for a quantum system, for which the act of measurement can change the state. In addition, simulation may be the optimal way to explore parameter space, when experiments are time consuming and expensive. This has been true for decades in the aerospace industry, and we expect that it will become true in other fields such as electromagnetic design.

4.1.2 Adaptive algorithms

The design of efficient and reliable algorithms, in which mathematics plays a crucial role, would greatly benefit scientific and engineering computing in the coming years. As an example, for solutions lacking regularity (e.g. discontinuous solutions such as shocks), high order accuracy is possible in terms of a suitably weak measurement (i.e., a “negative norm”) for error in the full solution. On the other hand, high order accuracy in strong measures (e.g., a uniform norm) of errors for engineering quantities should be achievable by mathematics-based postprocessing. Algorithms that are tailored towards new computer platforms such as exascale massively parallel computers should also be designed based on rigorous guidance from mathematics.

4.1.3 Uncertainty quantification

There is an emerging need to quantify the uncertainty of results and conclusions obtained with complex, large scale scientific calculations. This involves more than just issues around accuracy and stability of numerical methods for large and complex problems, which have been the domain of numerical analysis since the dawn of modern computing more than fifty years ago. What is needed is a way to assess uncertainties in the computations that arise from uncertainties in the mathematical modeling, in the parameters that enter the formulation, and in the initial and boundary conditions. For this task, there is a need for effective probabilistic methods that are also well adapted to the underlying computational techniques. This is a challenge and an opportunity for two established areas in mathematics, numerical analysis and probability theory. They need to join forces and develop a new, forward looking methodology for uncertainty quantification.

4.2 Information science

4.2.1 Homomorphic cryptography

In 2009, Gentry proposed the first scheme for "fully homomorphic encryption" -- in other words, for encryption that allows arbitrary computations on encrypted data without decrypting the data first (mentioned already in Section 3.2.4). The result of such a computation can be understood and verified by a "client" who possesses the decryption key, even if it's completely meaningless to the "server" that performed the actual computation. Besides its theoretical importance, Gentry's breakthrough could have major ramifications for cloud computing, where users with limited resources wish to offload difficult computational tasks to the "the cloud," without thereby compromising the security of their data. However, before homomorphic encryption becomes widely adopted, there will need to be significant improvements to its efficiency, as well as more detailed mathematical analysis of its security. This is an area where one can confidently expect progress within the next few years.

4.2.2 Quantum information processing and its mathematical basis

Even as experimentalists race to make quantum computing practical, there is still an enormous amount to be learned about the theoretical capabilities and limitations of quantum computers. In this regard, one exciting direction (though far from the only one) is to explore the space "between" classical computing and full universal quantum computing. What sorts of physical resources are really needed to solve classically-intractable problems? What can one do using an extremely "noisy" quantum computer (too noisy for the existing fault-tolerant constructions to apply), or a small-depth quantum circuit, or limited resources such as nonadaptive linear optics, commuting Hamiltonians, or "stoquastic" Hamiltonians? Not only do these topics naturally invite closer engagement between quantum computing theory and experiment (and between computer science and physics), they have also been found to lead to many novel questions in mathematics and complexity theory. For this reason, we hope and expect to see much more work over the next decade applying the methods of quantum computing theory to "realistic" (in the relatively near term) physical systems.

4.2.3 Design for Quantum Technology

The unique properties of quantum mechanical systems have opened the door to the design of many new electronic devices. Because of the underlying "mysterious" properties of quantum mechanics, the physical layout of such devices is not always intuitively conceivable. However, the functionality of the device is often quite clear. For example, a quantum computation can in principle achieve massive parallelism by acting on the entire probabilistic range of the state of the system. The elementary component of a quantum system is a qubit, which may be implemented as the spin of a single electron in a quantum dot. Taking advantage of this unique property of quantum mechanical systems requires designing the appropriate electronic device. For example, a target density of states is specified and an adaptive optimization algorithm is employed to search the physical parameter space of atomic clusters in an attempt to achieve the target. The resulting design, although it may be "obvious" after it was found by optimization, was not obvious from the start. In these examples there are two key elements: a physical model and optimization over the set of design parameters to achieve a specified goal. In order for this procedure to be practical, that is, to ensure that the device can *actually* be built, we add the third key element: manufacturability. In an optimization problem this translates to achieving the target despite uncertainties in the system, that is, *robust optimization*. In the near future it is conceivable that efficient and reliable optimization methods and algorithms will be an intrinsic part of the architecture for this new quantum technology.

4.3 High dimensionality and large data sets

4.3.1 Metric geometry for high dimensional data sets

Large discrete systems, for which there are no underlying continuum approximations, are a fact of modern life; e.g., large data sets, social networks, the electric grid. These systems are often high dimensional as well, since each node has many attributes. The distance between nodes can be measured by the distance between the attributes vectors, so that the system is a metric space. Despite some importance progress on the geometry of metric spaces, much more is needed, including: fast randomized algorithms and other new numerical methods; a way of finding canonical coordinates (or a replacement for them); methods for discovering and displaying the geometry of a metric space; and an understanding of the natural operators on the metric space, especially multiscale operators, with corresponding fast numerical methods. We expect rapid development of numerical and analytical methods for metric geometry in response to these applications.

4.3.2 The curse of dimensionality in control theory.

Many problems in control are intractable because they reduce to Hamilton-Jacobi partial differential equations in many dimensions. Recently it has been observed that the notion of tropical geometry is applicable here. This follows because viscosity solutions of these first order nonlinear equations behave linearly with respect to the max operation. This may lead to a computational breakthrough in this long standing difficulty.

4.4 Mathematics of physical systems

4.4.1 Metamaterials

Metamaterials are basically composite materials with properties or a combination of properties not found in nature. Typically they are made by combining materials with highly contrasting phases. There has been an explosion of interest in metamaterials due to a wealth of potential applications, and the unprecedented ability we now have to tailor-make desired microstructures. In practice the operation of many metamaterials is not in the homogenization limit, so mathematics needs to be developed to satisfactorily account for their properties. Numerical algorithms, especially optimization codes, need to be developed as tools for designing new microstructures. In addition there is a wealth of relatively unexplored areas, such as non-linear metamaterials, metamaterials with dynamic microstructures, and more generally, active metamaterials with controllable properties. Progress in developing an understanding of these topics would be greatly accelerated by mathematicians. There is a lot of excitement in the field, and as a result, a lot of speculative claims, some of which are dubious, have been made. Mathematics is needed to separate truth from fiction.

4.4.2 Density functional theory

There are several different but equivalent formulations of density functional theory (DFT): as a nonlinear eigenvalue problem, as a subspace (the eigen-subspace) problem, or as a fixed point problem for the Kohn-Sham map. Most existing numerical algorithms are based on the first two viewpoints. However, the last viewpoint has the advantage that it does not explicitly involve wave functions, and it seems to work equally well for metallic and insulating systems.

Several obstacles have to be overcome in order to construct efficient algorithms based on the last viewpoint: Discretization of the Fermi-Dirac operator in the definition of the Kohn-Sham map, extracting the diagonal part of various inverse matrices, convergence of the self-consistent iterations, etc. These issues are both mathematically interesting and profound. One expects mathematics to be of great value for constructing efficient algorithms based on this approach. Preliminary results are already quite promising. Indeed the most efficient existing general-purpose algorithm was constructed this way. It has a complexity of $O(N^2)$ for 3D problems, $O(N^{1.5})$ for 2D problems and O(N) for 1D problems, where N is the number of atoms in the problem.

4.5 Mathematical Modeling

4.5.1 Multiscale and hierarchical models

Much progress has been made on multiscale modeling for applications involving multiphysics, such as materials defects (cracks, dislocations, etc.) and kinetics for fluids and plasmas. More effort is needed, for example, on numerical analysis of multiscale computational methods.

Hierarchical models involve a series of different interacting models, for which the relationship between the different models is not necessarily based on time or length scales. Examples include

financial portfolios in which there are multiple models for the fluctuations in the individual components of the portfolio, and climate models in which the various models differ by choice of which physical effects to include. Numerical and analytic methods are needed for this wider class of models.

4.5.2 Experimental design and fitting of models to data

In many science and engineering areas, investigators have the ability to perform controlled experiments to dissect causal relations or to build models with mechanistic interpretations. The effective design of such experiments involves taking into account the subject matter knowledge and noise characteristics, as well as statistical modeling and estimation procedures. At one extreme, one has classical experimental design methods that trace back to classic works by Fisher, Yates and Box on agricultural and industrial experiments. These classical methods consider linear statistical models and are mostly of a non-sequential nature, but they are very effective in guarding against systematic bias and can resolve confounding among many factors. On the other extreme, there are settings in robotics with much better specified (possibly nonlinear) systems equations where the objective might be to design real time feedback-control algorithms rather than resolving factor effects. In between these extremes is a vast spectrum of problems that may involve sequential experimentation with iterative designed experimentation, model specification, model selection and parameter estimation. Such an approach will be needed, for example, in building mechanistic models in systems biology from sequential or incremental batches of gene knock-up/down experiments.

4.5.3 Data assimilation

As technology enables both increasing amounts of observational data and output from computational models, gaining maximal information from them has become imperative. The area of Data Assimilation (DA) offers a way to balance model and observational information. Its aim is to use them in concert to optimize state estimations and predictions in a given physical system. Bayes Theorem provides a framework for DA, but its application to models of the kind of complexity seen in environmental and biological applications has raised challenges that go far beyond current mathematical and statistical theories. The core issue can be summarized as a tension between handling nonlinearity in the system and working in the full dimensions demanded by the applications. The development of effective methods that resolve this tension promises to frame the emerging nexus of applied mathematics and statistics in the next decade.

4.6 Computational and statistical reasoning

4.6.1 Autonomous systems

Collections of autonomous systems equipped with limited communication and local computation need to cooperate to yield solutions to mutual objectives that are unachievable individually. Examples include the energy grid, surveillance, air traffic control, vehicles and networks. A particular example is that of cognitive radio where individual software-defined (and therefore reprogrammable) radios are required to share a radio resource equitably. Techniques from

dynamic game theory will play a central role in determining the local incentives to ensure coordination and foiling malicious attempts to garner an unfair proportion of the network resource. Methods from feedback control and estimation will underpin the development of stable interconnections capable of accommodating large and unpredictable external perturbations without excursions which could damage individual elements. Mathematical techniques will center on graph theory, dynamical systems, probability and distributed optimization.

4.6.2 Machine learning and data mining

Machine learning and data mining are notable for the quantity and variety of mathematical techniques they use. To date this has mostly consisted of applying existing techniques, but in the future we can expect to see new mathematical concepts inspired by the problems in these areas. The development of methodologies for "deep learning" from "big data" offers exciting opportunities and will stimulate progress in both computer science and statistics.

One area that promises to see major advances is Bayesian nonparametric approaches to unsupervised learning. Latent and hierarchical Dirichlet-process models have already revolutionized some current research areas such as document modeling, but many other important problems may also be amenable to similar approaches. Furthermore, the difficult but fundamental area of high-dimensional density estimation is also poised for a breakthrough. If successful, this will enable significant advances in downstream learning tasks such as anomaly detection. The mathematical analysis of the properties of these nonparametric learning methods will require new ideas in function representation and approximation theory.

Another significant area is structured prediction. Margin-based methods like kernel/support vector machines have already had major impact in areas like text classification, pattern recognition and computational biology, but their extension to problems where an entire structure has to be predicted, rather than a single scalar variable, has the potential for revolutionary progress.

4.6.3 Large scale statistical modeling and inference

Modern high throughput technologies are capable of generating simultaneous measurements that can support a large number (many thousands or more) of comparisons. This gives rise to a class of statistical problems where the objective is to test the significance of a large number of hypotheses. In a landmark paper Benjamini and Hochberg (B&H) argued that the False Discovery Rate (FDR) is the appropriate performance index for such large scale testing problems, and they introduce a provably correct method to control the FDR. Subsequent work by Efron and others have connected this theory to the theory of Empirical Bayes. This development has had an enormous impact in many application areas, as evident from the astounding number of citations of B&H's paper. This is a very exciting development that will continue for some time; for instance much progress can be expected to make the method work under more general dependency structure among the test statistics, and there will be associated development of

alternative inferential frameworks, such as the Empirical Bayes approach to large scale inference that is being pursued by Efron and others.

4.7 Imaging

Imaging (including video) has been a fertile area for applications of mathematics and for development of new mathematical ideas and methods. Over the next decade, we hope to see the emergence of a new field of mathematical imaging science. This new field would greatly assist those disciplines that depend on imaging but currently develop their own techniques for

imaging without any interdisciplinary fertilization. Some of the expected aspects of this new mathematical discipline would be the following:

4.7.1 New modalities for imaging

New methods, such as transient elastography, real-time imaging with motion estimation and the virtual source method, are being invented in the context of engineering applications. Development of mathematical foundations for these applications will be an important endeavor.

4.7.2 Connections with information science

The line between imaging and general information science is becoming blurry, and techniques are crossing over it. For example social network analysis and other social science projects, such as the mathematics of crime are beginning to use successfully some of the techniques mentioned in 3.1.2 and 3.6.2.

A basic problem is the development of automatic systems to provide multiple hypotheses that are consistent with a desired outcome or mission, to involve data that is uncertain, imprecise, incomplete and/or contradictory, to provide a capability to suggest experiments or activities that distinguish between hypotheses, to identify data with appropriate quality, and to support efficient computation. Again the techniques of 3.1.2 and 3.6.2, as well as some statistical ideas, are relevant here. The goal is to discover new automated methods for mission-relevant identification, as well as representation of relationships, intentions and objectives from unstructured data.

4.7.3 Connections with combinatorics, probability and physics

New links between combinatorics, stochastic, and continuous methods for optimization will be developed. Combinatorial approaches for denoising image processing and scientific computing algorithms on embedded systems, such as DSP's and FPGA's, will be developed to allow for real-time processing, with limited resources (e.g., energy). Random sampling is often impractical but is a basic assumption of compressive sensing and elsewhere. We expect the development of useful deterministic sensing algorithms again based on techniques from 3.1.2 and 3.6.2. Blind restoration algorithms, e.g., deblurring with unknown kernels as in imaging through turbulence, will be developed. These may use the physics of the image formation.

4.7.4 Measures of accuracy

We expect the development of new metrics for sampling error in graph based algorithms and imaging in general. SNR and L2 error measurements do not necessarily correlate well with the human visual system or even with automated sensors. We think the use of new modalities such as fMRI will help here. We also note that the beta process approach often gives quantifiable probabilistic metrics.

5. Infrastructure

Infrastructure for mathematics is needed to support interdisciplinary interactions and computing, and to maintain the pipeline of quality students going into mathematics. We see both significant improvements and also some losses in the quality and availability of infrastructure for mathematics.

5.1 Support for intra-disciplinary and cross-disciplinary collaboration

As of fall 2011, the NSF Division of Mathematical Sciences (DMS) has established eight national mathematics institutes (IPAM is one of them) that promote collaborations between mathematicians, as well as interdisciplinary interactions between mathematicians and scientists. Together they have supported an extraordinary range of applications of mathematics. The result has been that mathematics has become a much more common and reliable partner in the scientific enterprise. Current plans call for formation of virtual math institutes involving international partners, which has the potential of greatly leveraging the existing institutes.

Preservation of presentation files (e.g., powerpoint or pdf) and video recording or streaming of lectures greatly extends the reach of the math institutes, as well as that of seminars throughout the US and the world. There is still a need to organize these resources in a way that allows for convenient access and search capabilities. The Access Grid provides resources that may help with this.

Websites devoted to collaboration among mathematicians are starting to form, through the efforts of individual researchers and educators. An example is the Polymath Project, which was started by Timothy Gowers with the goal of enabling "massively collaborative mathematics". MathOverflow was started by a group of graduate students and postdocs, and serves both as a collaborative blog and an online community.

5.2 Support for simulation and computation

Software development is an important part of applied mathematics that can be valuable to both mathematicians and scientists. Yet, there is little institutionalized support for academic software development, and often academic mathematicians do not earn credit towards tenure and promotions from their software development. While the latter is a mathematics cultural problem

that is difficult to address, infrastructure to support software development would be helpful, including funding for programmers to write and test software and repositories for software.

Infrastructure is also needed for simulation and computation, including data repositories and tools for data collection. Black-hat/white-hat style challenge competitions would promote collaborations among simulation researchers.

5.3 Graduate student and postdoctoral fellowship support

Currently there is a significant need for more funding for graduate students in mathematics departments to ensure that there is an adequate supply of quality replacements for the impending retirement of many senior mathematicians. US departments have become dependent on foreign graduate students, especially from China, which has worked extremely well over the last three decades, but may not be sustainable in the future. The availability of research fellowships will ensure a more rapid doctorate completion time than is currently the case if teaching assistantships are relied on for financial support.

Similarly, the provision of postdoctoral fellowships will permit the focused training of the next generation of mathematical researchers to replace the aging population currently active. Because of the reliance of mathematical research on individual efforts, this is a critical infrastructure for mathematics.

6. International Developments

Mathematics is an international endeavor. In fact, although all of the invited scientists at this workshop live and work in the US, roughly half of them are foreign-born, originating from 5 continents.

A survey of the strengths of mathematics in the US, relative to the rest of the world was part of the charge to this workshop. Mathematics in the US is still very strong, but some significant international advantages have developed. For example

- Software development and applications, e.g., development of software and its applications for the fast multipole method (FMM) and for density functional theory (DFT), are now centered in Europe
- Many centers for quantum information processing are in Europe, Asia or Australia, rather than in the US
- Imaging science is developing rapidly in Asia and Europe.

A key role in these developments is the strength of public, non-academic institutions that can support large scale software development and other tasks that are not entirely academic. Examples include the Max-Planck Institutes in Germany and the National Key Laboratories in China. By contrast in the US, there has been significant diminution of non-academic research centers, both governmental and industrial. Notable exceptions to this trend are found in

information technology, including Microsoft Research (with locations around the world) and Google.

7. Conclusions

This is a golden age for mathematics. As described in this report, mathematics is meeting the challenges of massive data sets, increasing complexity and large scale computing through new developments, such as compressed sensing, network analysis and image processing that draw on both pure and applied mathematics, as well as statistics, computer science and theoretical engineering. The scientists at this workshop are strongly optimistic about the future of mathematics, as well as the future of science, in part because of the wonderful success over the past decade and the strong prospects for future research breakthroughs.

While we have made an effort to adopt a broad and fair view of mathematics, the specific topics described here are influenced by the individuals who attended this workshop and are an incomplete sample of both the achievements of mathematics over the last decade and the areas that are ripe for future development.

Appendix I: Attendees at the Workshop on Future Directions in Mathematics

Invited Scientists

Scott Aaronson, MIT, aaronson@csail.mit.edu
Robert Bitmead, UCSD, rbitmead@ucsd.edu
Russel Caflisch, UCLA, IPAM, rcaflisch@ipam.ucla.edu
Pedro Domingos, U Washington, pedrod@cs.washington.edu
Weinan E, Princeton, weinan@math.princeton.edu
Charles Epstein, U Penn, cle@math.upenn.edu
Mark Green, UCLA, mlg@ipam.ucla.edu
Leslie Greengard, NYU, greengard@courant.nyu.edu
Alfred Hales, CCR, hales@ccrwest.org
Peter Jones, Yale, jones@math.yale.edu
Christopher Jones, UNC &Warwick, ckrtj@email.unc.edu
Robert Kosut, SC Solutions, kosut@scsolutions.com
C. David Levermore, Maryland, lvrmr@math.umd.edu
William McEneaney, UCSD, wmceneaney@ucsd.edu
Eric Michielssen, Michigan, emichiel@umich.edu
Graeme Milton, Utah, milton@math.utah.edu
Stanley Osher, UCLA, IPAM, sosher@ipam.ucla.edu
George Papanicolaou, Stanford, papanico@math.stanford.edu
Pablo Parrilo, MIT, parrilo@mit.edu
Chi-Wang Shu, Brown, shu@dam.brown.edu
Terence Tao, UCLA, tao@math.ucla.edu
Eva Tardos, Cornell, eva@cs.cornell.edu
Wing Wong, Stanford, whwong@stanford.edu

Government Observers

Neil Gupta, DoD
Tristan Nguyen, ARO
Robin Staffin, DoD
Stuart Wolf, DoD

Appendix II: Questions Posed to the Workshop Participants

1. What have been the major breakthroughs in mathematics over the last decade?
2. What new areas do you see emerging in the next decade?
3. What accomplishments or capabilities will be attainable in 5 years? 10 years? 15 years?
4. Are there particular infrastructure needs that the DoD should be investing in? Why?
5. Where are existing and emerging global centers of excellence in mathematics?
6. What are the most important efforts for DoD to support in the next decade?