Descriptions of Project Topics

MATH 404 Discrete Math, Fall 2005

As part of the required work for this class, you will be turning in a short paper (up to 6 pages) at the end of the semester on one of the topics described below. Notice that topic 3 listed on the syllabus, Scheduling Problems and Bin Packing, has been broken into two, and topic 6, Finite State Automata, is no longer there. A sheet listing, in order of preference, three topics that sound interesting to you, is due in class on *Monday, September 12*. Once I have assigned you a topic, you should start researching it as soon as possible or talk to me if you need help getting started. More details on exactly what I expect you to do will be given later and will depend on the topic.

1. The Apportionment Problem. This problem is concerned with assigning an appropriate number of seats in an organization or a legislative body, such House of Representatives or a Parliament, on the basis of population distribution. Although this problem seems simple on the face of it, it is actually quite hard and interesting because population percentages can be fractional while people, well, can't. The problem has therefore been debated for some 200 years by mathematicians and politicians. Your job in this project would be to describe the problem in more detail and discuss some approaches for a solution.

2. Gödel's Undecidability Theorem. In the early 20^{th} century, many logicians and mathematicians were trying to find a complete set of axioms upon which all of mathematics could comfortably rest. Kurt Gödel put an end to the discussion by proving his celebrated Undecidability Theorem which essentially says that for any set of axioms there will be statements which are neither provable nor disprovable. Your job in this project would be to understand in more detail the exact statement of the theorem, give an outline of the proof, and discuss its historical context in terms of the search for the complete set of axioms. You might also want to learn about Alan Turing's interpretation of Gödel's theorem.

3. Scheduling problems. Scheduling problems require assigning tasks subject to constraints such as deadlines, capacity, task priorities, etc. These pretty much arise in any slightly complicated system which has constraints, such as for example in assigning classrooms to satisfy the needs of students and faculty at a university, but is most commonly discussed in the context of manufacturing or transportation. This type of a problem falls under the heading of "discrete optimization". In your project, you might want to present an example of a scheduling problem and its solution.

4. Bin packing. This is exactly what it says it is – the question is how to fit some number of objects of different volumes into some number of bins in a way that minimizes the number of bins. This has applications in everything from loading trucks with a weight capacity to creating file backups in removable media. As in the above topic, your project here might be to find an example of a bin packing problem and present a solution. There are also algorithms out there that will let you approximate a solution to a bin packing problem numerically with any desired accuracy. An exposition of such a numerical approach is also a good project topic.

5. Traveling Salesmen Problem. This is one of the oldest discrete optimization problems. It has many incarnations but the point is always to find the shortest path connecting some geographic locations while visiting each only once. This clearly has applications in problems such as optimizing airline routes or laying cables but it also appears in some unexpected places such as DNA and genome research. You

project on this topic might be to pose and solve a traveling salesman problem or to write an expository survey of some of the many forms it has taken over the years.

6. Modeling with trees. Any time a decision or an event leads to more options, i.e. there is some kind of a branching, a tree can be used to model the process. Applications can be as simple as creating a small database and as complicated as relationship modeling or file compression. In your project, you would build upon what you learn in class about graphs (trees are special cases), give the basic definitions, list some ways in which trees are useful, and perhaps present a real-life system which can be modeled by trees. I would also like you to discuss spanning trees and why they are important.

8. Pretty Good Privacy (PGP). This is a program, originally written by Philip Zimmermann and available on the web, which lets a user encrypt his or her files and email. It relies on very basic math much like the RSA cryptosystem which we will discuss in class. In addition to researching and writing about the math of PGP, you might also want to learn about the role it has had in the discussion of cryptography regulation and privacy. After Zimmermann wrote PGP, the government did not like that the encryption power was suddenly in users' hands rather than in some central agency's and a lengthy battle ensued. Try looking for Zimmermann's "Why I Wrote PGP" on the web.

9. Secure Socket Layer (SSL). This is a protocol developed by Netscape for secure e-commerce. If you ever used a credit card on the web, then your private information was most likely handled by SSL. Your project on this topic would be to find out how SSL encrypts the information, exchanges a key between two parties, and in general provides authentication, confidentiality, and message integrity. As in the case of PGP, I will teach you enough about public-key cryptography so you can understand how the math behind SSL works.

10. Hash functions. Digital signature algorithms are generally slow and hash functions are designed as a time and space-saving device for this part of the message encryption. Instead of computing the digital signature of the entire message, such a function computes the digital signature of some sort of a digital fingerprint of the message (which is much shorter than the message itself). This is in particular useful in digital timestamping where a document can get stamped without its content being revealed to the stamping service. Your job in this project would be to provide the details of how hashing works.

11. Quantum cryptography. This is a type of cryptography where quantum physics is used for encrypting information which is usually carried by photons. The advantage of this type of cryptography is that in theory one can always detect eavesdroppers. I would like you to explain all this in some detail in your paper. You'll have to learn something about the Heisenberg uncertainty principle, maybe mention quantum computing, give an account of how much of the theory has been experimentally tested, and discuss how far we might be from seeing a widespread use of quantum cryptography.