2005

A Survey In Network Economics: Spam Email, Internet Routing, Graphical Economics, and International Trade

Mark E. Haase
University of Pennsylvania

A Survey In Network Economics: Spam Email, Internet Routing, Graphical Economics, and International Trade

Abstract
A survey of current topics in network economics, a relatively new and growing field of research at the intersection of economics and network theory. Case studies in spam email, Internet routing, and graphical economics are presented as practical applications. A network economic analysis of international trade is also offered. Most of the current literature addresses a highly technical audience. This paper intends to bridge the gap by presenting network economics in language that will be familiar to students of economics.

Keywords
graph theory, social networks, economics, network economics, trade, spam, routing

Subject Categories
Other Economics

A Survey In Network Economics:
Spam Email, Internet Routing, Graphical Economics, and International Trade

Abstract: A survey of current topics in network economics, a relatively new and growing field of research at the intersection of economics and network theory. Case studies in spam email, Internet routing, and graphical economics are presented as practical applications. A network economic analysis of international trade is also offered. Most of the current literature addresses a highly technical audience. This paper intends to bridge the gap by presenting network economics in language that will be familiar to students of economics.

Mark E. Haase
PPE Honors Thesis
May 2005

Advisor: Michael Kearns

I. Introduction

Network Economics is a relatively new field of study that is emerging at the intersection of network theory and economics. Network theory is a growing field that attracts researchers from a variety of other fields including physics, sociology, and computer science. The cross-fertilization of ideas between network theory and economics is creating powerful, new analytic tools. Network theory is providing new ideas and new models to the mature field of economics as well as new results, and economics offers solutions to new problems that are arising in certain, real-world networks.

The term network economics has several possible meanings. At times it has been applied to economic problems that include a significant network externality, which is a component of demand that changes in response to others' consumption of a particular good. Network economics can also mean the study of economic problems in the context of network models. In this paper, the definition of network economics will be liberally expanded to refer to what might properly be called network theory economics–the interdisciplinary study of how principles of network theory and economics interact. Although this is not yet a unified field, this paper will demonstrate how network theory and economics relate to each other and it will present practical examples that display the power of network economic theory.

The reader only needs basic familiarity with microeconomics, game theory, and simple math. Section 2 will present a brief discussion of network theory that is a suitable introduction to the uninitiated, with some comments on issues of complexity theory and its relevance to the current topic. Readers who are already familiar with these topics can easily skip this section. Sections 3-6 will present several case studies that highlight various applications of network economics. Section 7 will conclude with a discussion of the important themes and future direction of network economics.

II. A Primer In Network Theory

Network theory is a relatively new science, but it is built on the foundation of graph theory, a branch of mathematics that originates from the work of Leonard Euler in the 18th century. A graph is a mathematical description of a system of interconnected objects; graph theory has nothing to do with histograms, bar charts, or scatter plots. Graph theory has been studied intensively and is understood very well, with various practical applications in computer science, physics, and even cartography. The two fields are closely related, and in this paper the terms *network* and *graph* will be used interchangeably.

In order to be well defined, a network must have two specifications. First, a set of *vertices* must be specified. These vertices can represent any kind of objects, such as people, network routers, economic markets, etc. Second, a set of *edges* must be specified. Edges associate one vertex with another vertex and indicate some kind of relationship between the two. This definition of a network is exceedingly generic so that network theory can be applied to as wide a range of systems as possible.

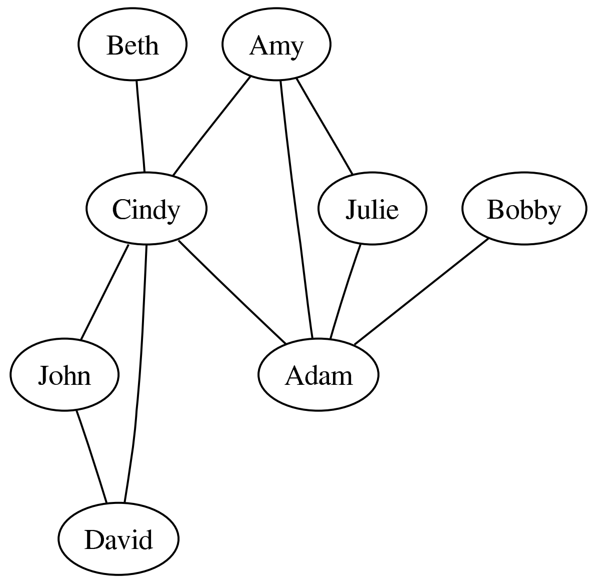

Figure 1: A friendship network.

Networks can be defined in any number of ways. In a social context, each vertex could represent a person and an edge would exist between two people if and only if they are good friends. In a different social network definition, an edge might indicate mere acquaintanceship. Or the vertices of a network could represent the boards of Fortune 500 corporations, and an edge exists between two boards if and only if one or more board members sit on both boards. Clearly, the properties of any particular network depend intimately on how the network is defined. Therefore, precise definitions are always mandatory.

To clarify this point, an example network is presented in Figure 1. This is a friendship network. Each vertex in this network is a person, and an edge exists between two people if and only if those two people are friends. Therefore, the network stores information about relationships among these people. Just by looking at the diagram it is easily inferred that John is friends with David but not Beth. John is, however, indirectly connected to Beth by sharing a mutual friend named Cindy.

Notice that this diagram is only a visual representation of the network. Strictly speaking, a network is only an abstract entity defined by its set of vertices and set of edges, but visualizing the network often aids analysis. In this paper, network diagrams will be referred to simply as networks, but the distinction between the two terms is important because any particular network could be drawn in an infinite number of different ways. Figure 2 shows two layouts of the same network. In this case, the network represents a metro transit system. Each vertex is a station in the transit network, and two stations have an edge between them only if a metro rail directly connects those two stations. The two different diagrams represent the same network, yet seeing either layout in isolation might lead to different conclusions about the network. The diagram on the left suggests a hierarchy, whereas the diagram on the right resembles an actual metro rail map. Therefore, it is important to be aware of the difference between the abstract network and its visual representations.

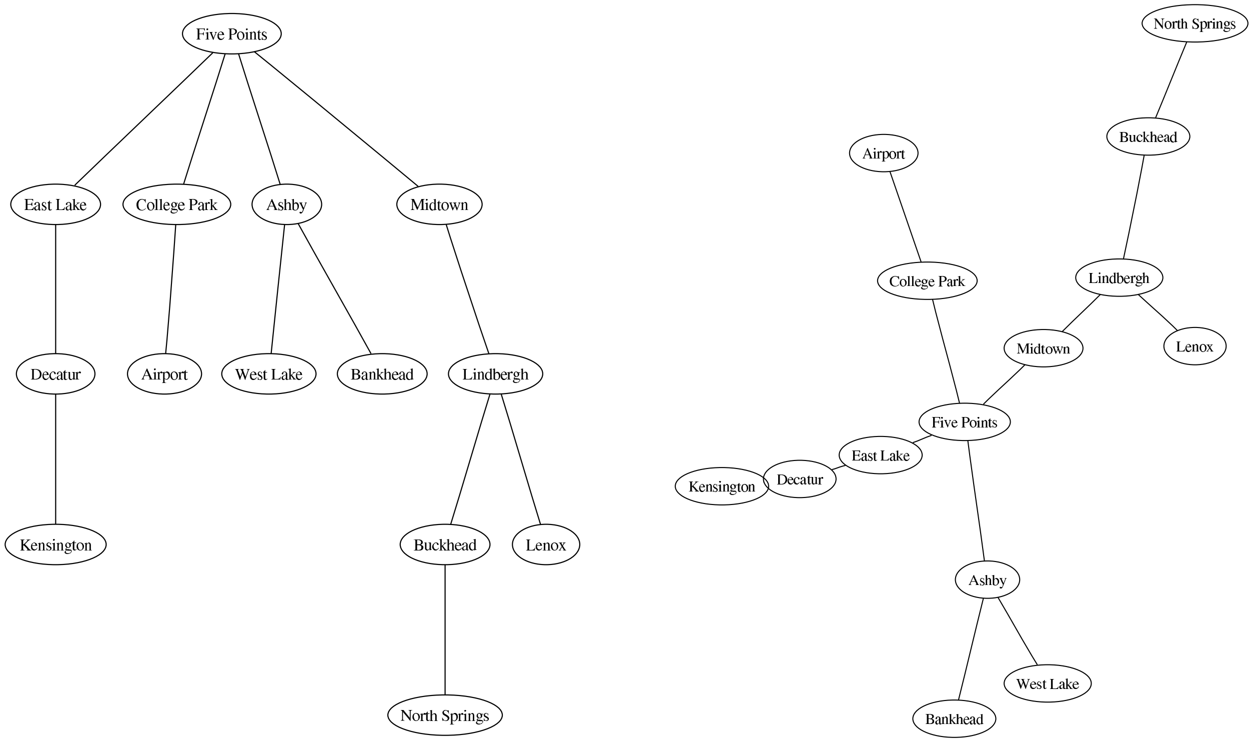

Figure 2: Two different visualizations of the same network.

Networks possess a number of interesting, measurable properties that are important for comparing and classifying various types of networks. The *degree* of a vertex is equal to the number of edges that are attached to that vertex. In the metro rail network presented above Five Points has a degree equal to four, and Lenox has a degree equal to one. The *degree distribution* of a network is a histogram of the degrees of all vertices. The *distance* between two vertices is equal to the number of edges on the shortest path that connects those two vertices. The distance between College Park and Buckhead is four. The *diameter* of a network can be measured in several ways. In some applications, the diameter is defined as the worst-case path length, i.e. the maximum shortest path between any pair of vertices in the graph. For this paper, though, the diameter is defined as the average path-length, i.e. the average over all pairs of nodes of the shortest path between each pair.

The network is *connected* if a path exists between every pair of vertices. The metro rail network is connected, because any station can be reached from any other station. The *edge density* is equal to the number of edges in the network divided by the maximum possible number of edges that could exist in the network. In the metro rail network, there are thirteen edges, but the network could have as many as ninety-one edges in it, so the edge density is *13/91*, which is roughly *.14*. A network is *complete* if every pair of vertices is directly connected by an edge; a complete network has an edge density of *1.0* by definition. The metro rail network is not complete, because there are obviously many pairs of vertices which are not directly connected. Finally, a network can be characterized by its *clustering coefficient*, a measure of the extent to which vertices are organized into distinct neighborhoods. The clustering coefficient will be formalized in Section 6. There are of course a number of other important properties, but those defined above are the most pertinent to this paper.

Networks can be configured in any variety of ways: small diameter, large diameter, low clustering, high clustering, etc. Network theorists have discovered, however, that many classes of networks share similar characteristics. In this paper, the primary interest is in so-called *small world networks*. This class of networks is typically defined by three properties: small diameter, high clustering, and heavy-tailed degree distribution. In many cases, small world networks also share the common characteristic that they formed spontaneously and without centralized control.

Researchers have discovered and documented countless examples of networks that fit this description, including most social networks, many economic networks, the World Wide Web, the national power grid, and even the neural network in the brain of the worm *C. Elegans* (Watts, 95-98). These networks take their name from the universal anecdote in which two strangers discover that they have a mutual friend and remark on a what a "small world" it is. Stanley Milgram, a noted sociologist, made the term famous in a 1967 paper in which he estimated the diameter of the global acquaintanceship network to be roughly six, which in turn spawned the phrase "six degrees of separation" and acquaintanceship games such as "Six Degrees Of Kevin Bacon".

Milgram's experiment has been criticized for lack of rigor and small sample size. Consequently, his estimate of the diameter of the global acquaintanceship network is certainly questionable. Whatever the exact number is, though, the lesson remains the same: in a network with as many nodes as there are people on the earth – 3.6 billion in 1967 (United Nations) – the average shortest path between any two people is amazingly small, perhaps less than or equal to ten.

Bipartite networks will also be important in this paper. A bipartite network is characterized by having two different types of nodes, and edges that only exist between vertices of different types. As an example, some research has been performed on romantic relationship networks. Assuming only heterosexual relationships, these networks must be bipartite because the vertices can be divided into two types (male and female), and edges only exist between males and females. No edge connects one male to another male or one female to another female.

Before proceeding, it will be helpful to comment briefly on the role that complexity plays in network theory. Complexity theory is a field between math and computer science that studies the computational resources needed to solve problems algorithmically. Nearly all algorithms, independent of the hardware resources available, will vary in running time as the size of their input varies. Table 1 demonstrates how various types of algorithms scale with the input size. Linear algorithms scale in direct proportion to the size of the input. If the size of the input doubles, the running time doubles as well. A quadratic algorithm scales in proportion to the square of the input size, so doubling the input size quadruples the running time, because 2^2 is 4. The exponential function grows the fastest, however. Increasing the input size by a factor of ten increases the running time by a factor of 1024, because 2^{10} is 1024.

Type of algorithm:	1 input bits	2 input bits	3 input bits	10 input bits
Linear	1 second	2 seconds	3 seconds	10 seconds
Quadratic	1 second	4 seconds	9 seconds	100 seconds
Exponential	1 second	4 seconds	8 seconds	1024 seconds

Table 1: Various types of algorithms and hypothetical running times.

The difference between polynomial and exponential running time is quite striking. An exponential algorithm might be faster than a polynomial algorithm for small inputs, but the running time explodes as the input gets larger. Consider simply that 500^2 is only 250,000, but 2^500 is about 3.3 x 10^150, a number so large that it makes the number of nanoseconds since the big bang (4.7 x 10^26) seem miniscule and dwarfs even the largest estimates of the number of subatomic particles in the universe (10^128) (Yolkowski). If a calculation's best-known algorithmic solution is exponential, it becomes an intractable problem for all but the smallest inputs. Even with computers billions of times more powerful than those that exist today, these calculations will still be impossibly time consuming.

The difference between these two kinds of algorithms is important in network theory because it makes some calculations difficult to do on large networks. There are reasonably fast algorithms for many basic calculations such as diameter and clustering.

The running time of Floyd's algorithm, which is used in this paper to calculate the diameter of a global trade network, is proportional to the cube of the number of vertices. This means that if the algorithm requires one second to compute the diameter of a network with a hundred vertices, it will require eight seconds to run on a network with two hundred vertices, because two raised to the third power is eight. Thus, doubling the size of the network increases the running time by a factor of eight. (Note that on modern computers, Floyd's algorithm actually runs much faster – well under one millisecond for moderately sized networks.) If the above is confusing, the most important point to remember is that many network theoretic algorithms run in exponential time, and so only approximated solutions are feasible. An example of an exponential algorithms in network economics will be touched on in Section 5.

III. Spam Email

Every person on the planet who has an Internet email account knows what spam is: high-volume, unsolicited email that clogs inboxes with various scams, pornography, and product pitches. While spam is obviously irritating, it is also becoming a waste of resources. In 2003, Andrew Leung estimated that spam comprised 40% of all email (3). He also noted that the problem was growing rapidly: Earthlink reported a 500% increase in the volume of spam email over an 18-month period. In 2002, U.S. corporations are estimated to have spent $8.9 billion combatting spam. The huge volume of spam on the Internet pushes up bandwidth, server storage and support staff costs, costing U.S. corporations $3.7 billion. The lost productivity of workers, who spend several seconds handling each spam message, adds up to another $4 billion. In addition to the economic costs, Leung notes that home users also waste time and money fighting spam and they experience a "psychological effect comparable to having [their] home broken into" (9).

Although spam might appear to be an ineffective means of marketing, it is actually (and unfortunately) very economically sound. A spam advertiser has very low fixed costs. The essential tools include a personal computer, a broadband internet service provider (ISP), and a database of emails. The marginal costs, however, are virtually non-existent. The cost of sending a single email is virtually the same as the cost of sending a million. In traditional industries, firms operate whenever marginal revenues exceed marginal costs.

> Email based spam, however, is not yet at economic equilibrium, primarily because the first factor – the cost of sending spam – is more or less non-existent in the email world. (Osterman)

Marginal revenues, on the other hand, are significant. A very small positive response rate to a spam campaign will cover costs and turn a profit.

> Response rates to bulk commercial email are thought to be as low as .005%. That means the typical message appeals to 50 people and annoys 999,950…Marketers now pay $150 for a compact disk with 70 million email addresses – or 3,500 new customers…And here's the really troubling development: the economics of spam are only getting worse from a public standpoint. Thanks to aggressive new techniques for harvesting email accounts, the cost of hooking new customers is constantly plummeting. (France)

In principal, the problem with spam email is that spam advertisers pay ultra-low marginal cost but their actions produce a negative externality. This is similar to a free-rider problem, and the only answer is to make spam advertisers internalize the social and economic costs of their actions. There are a variety of legal and technological approaches to achieving this end; most of the strategies employed so far have found limited success. As anti-spam measures improve, spam advertisers improve their tactics as well.

Most ISPs have used several tactics to curtail spam. They have secured mail servers by requiring user authentication and closed down open relays (servers which forward mail blindly). They have also terminated accounts that were used to send spam. In addition, ISPs have set up databases known as DNS-based black hole lists (DNSBLs)[i] to track the IP addresses of third party open relay servers and known spam advertisers. If an ISP is suspected of allowing or supporting spam advertising, their entire subnet (the range of IP addresses which they manage) might be blackholed (Leung) – a death knell for an ISP and a good local incentive to promote the globally desired outcome.

Despite the efficacy of these cost internalization regimes, spam advertisers have continued and spam email is still growing. Spam advertisers exploit competition between ISPs by opening new accounts frequently and thus evade being permanently blackholed. They have also brought freedom of speech lawsuits against organizations that maintain DNSBLs and used other means of legal intimidation to shut down or cripple the ISPs' anti-spam measures.

Governmental response has been slow and ineffective. Part of the problem can be attributed to bureaucratic confusion and delay. But there is also a fundamental dilemma in enacting anti-spam legislation: there is no precedent for protecting consumers from advertising (Leung). Legislation enacted thus far deals only with spam email that contains inappropriate material or misleading sales information. The fact that some readers do respond positively to spam email legitimates the claim that spam is speech protected in the U.S. by the Bill of Rights. Even in the cases where spam is legally prohibited, spam advertisers can dodge the law by operating in foreign countries (France).

The mediocre performance of black hole lists and legal intervention has left a vacuum in the effort to reduce spam. To date, the most successful means of increasing spam advertisers' costs seems to be the use of spam filtering software. These software programs use sophisticated statistical measures to determine if incoming email messages are legitimate or if they are spam. They are imperfect, but by blocking a significant fraction of all spam email from ever reaching the readers' eyes, the filters should reduce the positive response rate that spam advertisers see. Filters are designed to make false positives extremely unlikely, because a filter throwing away a valid message is several orders of magnitude worse than the filter letting spam email messages slip by. For this reason, filters are necessarily less effective than they could be.

Filtering software also has two intrinsic problems that are quite formidable. First, filtering software only works if users install it and use it. The adoption rate of filtering software has been disappointing, however. The average user apparently does not trust spam filters nor wish to spend time installing and configuring a filter. Second, spam filters encourage a virtual arms race between anti-spam developers and spam advertisers (Leung). Although some spam filters were extremely successful when they were first introduced, spam advertisers have found a number of ways to sneak emails past the filters. One tactic is to send an innocent, personal email with an advertising image attached. The text of the email sneaks it past the filter, then the user opens the message and sees the advertisement. Determining if attached images are spam-related is a difficult problem to solve in software. Some advertisers use random generators to transform normal English text into pseudo-English, by spuriously committing misspellings, inserting spaces in the middle of words, replacing letters with numbers that look similar, e.g. a 1 for a lower-case l (Goodman). Although spam filters can eventually respond to specific permutations of a word, there are so many permutations of common words that even sophisticated filters will continue to be outwitted by these simple tricks.

Fortunately, two promising methods should force spam advertisers to internalize the social and economic costs that they inflict on others. One approach uses direct economic disincentives to increase spam advertisers' marginal costs. The other approach uses information about network context and some basic network theoretic analysis. The synthesis of these two methods reveals the combined power of network theory and economics; their deployment would result in the most effective deterrent to spam advertisers yet. Better yet, these techniques are more resistant to retaliation than previous techniques have been.

The economic disincentive technique is straightforward in concept but the implementation could be tricky. The basic idea is to tax every email some very small amount – some proposals suggest the term "micropayment." The theory is that a very small percentage of email users generate a very large percentage of total emails. For the average user sending several hundred or thousand emails per year, the total cost would be at most only a few dollars. For spam advertisers sending millions of emails per year, however, the cost would be in the thousands or ten thousands. This slight increase in marginal costs would make most spam advertising ventures unprofitable.

At least two implementations are possible. In one possible implementation, ISPs would update their mail server software so that it demands a micropayment for putting mail into a user's inbox on that server. Payments would be handled through pre-paid accounts that were debited by the micropayments in real-time. Large providers, such as Earthlink, AOL and MSN, would negotiate directly with each other to buy large blocks of credit. Smaller providers could use third party email brokers to buy standardized units of credit that were accepted by all major providers. The micropayment price would need to be set at such a level so as to deter spam but not to curtail legitimate usage of email. Each ISP would pass the costs of email transmission on to each user as a surcharge on that user's monthly bill and in proportion to the amount of email that user sends.

This implementation requires trust in the software to appropriately account for billions of micropayments, but open source software and a healthy market for information should prevent cheating. ISPs are expected to spontaneously adopt this implementation (if it is available and robust) because the small profit subsidizes increased overhead costs, and users will demand ISPs that can offer better spam prevention. Some implementation details are more problematic, such as how to tax an email that is routed through several email servers before reaching its destination. If each server taxed the same email equally, the micropayment system would have the unintended and undesirable consequence of excessively taxing email between far-flung nodes on the Internet. Dividing the micropayment equally among each server would be difficult because each server in the chain would need to know about all of the other servers, which is not how mail forwarding currently works.

The alternative implementation would be to allow end users to specify rates at which they accept mail from various sources. Each user would declare a set of prices and these prices would be stored on their local mail server. When another user wanted to send email to the first, his client software would query the remote server and determine the cost of sending the email. To make usage simple, senders would set a maximum on the prices they were willing to pay. If the cost exceeded that maximum, their email software would display the price and ask whether to continue. The micropayment scheme is more complex in this implementation – technology standards and universal adoption are imperative. The benefit is that users could set their price schedule differently for various users and groups on the Internet. Everybody on their list of family, close friends and colleagues could be made exempt from payment. Unknown addresses from trusted domains could be charged a small amount in proportion to the probability of receiving spam from a user in that domain. Larger amounts would be charged to users from unknown or suspicious domains. The use of a tiered price schedule is too complicated for the average user, but the process could be simplified by using a standard format and user-friendly software. It could be further simplified if consumer advocacy organizations made price schedule templates available online. In this way, novice users could base their price schedules on expert advice.

The user-centric implementation has a one major flaw. The micropayment management software would exhibit a positive network externality.[ii] Users would not buy in until most of their email contacts also had the software. The only solution would seem to be a major public relations campaign financed by major ISPs and the software providers. The network externality will have a tipping point, i.e. a threshold where consumption of the software is high enough that the externality suddenly becomes negligible. If ISPs deployed the software on their own servers, then a few major ISPs could tip the entire population towards the desired equilibrium.

The micropayment model is immensely valuable for deterring spam, however, because spam advertisers will not be able to avoid paying for the true costs incurred by their spam email. The social and economic costs that they have been imposing on society will be internalized and for most spam advertisers the business model will be destroyed.

A network-centric model proposed by Boykin & Roychowdhury is now presented. Combined with the micropayment model, this model will increase spam advertisers' marginal costs even further. As a side benefit, the model demonstrates a synergistic relationship with current spam filtering software. The model is built on the idea that the structure of email networks conveys important information about the type of email transmitted on that network. In the global email network, each vertex represents an email address and an edge exists between any two addresses if they are both in the email header of the same message. (The email header is the part of the message that stores, among other things, the subject, the list of recipients, the carbon copies, blind carbons, etc.) Consider the following example: User A sends an email to user B, with Cc: to Users C and D. When B receives the message, he infers that A is connected to both C and D, but he also infers that C and D are connected to each other.

Given a large volume of email, an extensive email network can be constructed. The information is localized to a specific user, so that the user only has an idea of the network context in which they are situated; the user knows very little of the overall email exchange graph structure. Given a user's network context, however, Boykin & Roychowdhury demonstrate that most spam comes from certain subcomponents and most legitimate email comes from other subcomponents. Legitimate email never comes from a spam subcomponent, and spam email never comes from a legitimate subcomponent. Better yet, the types of these subcomponents can be distinguished using a handful of simple network theoretic tools.

Email networks, like most social networks, have small diameter and high clustering. As was previously discussed, these types of properties seem to be rooted in the decentralized, spontaneous creation of the network. Subcomponents of the graph with high clustering coefficients can be assumed to have formed in such a manner. These subcomponents are therefore considered legitimate; users in these subcomponents can be safely whitelisted. Spam emails form a very different kind of subcomponent. Spam emails often have multiple recipients, and since spam advertisers share common lists of email addresses, spam emails are often sent to the same sets of email addresses, thus the graph of a spam subcomponent is bipartite. The clustering coefficient in these subcomponents is very near zero. Users in these subcomponents can safely be blacklisted. See Figure 3 for examples of a spam component and a legitimate subcomponent. The spam subcomponent is clearly bipartite, and the legitimate subcomponent shows significant clustering.

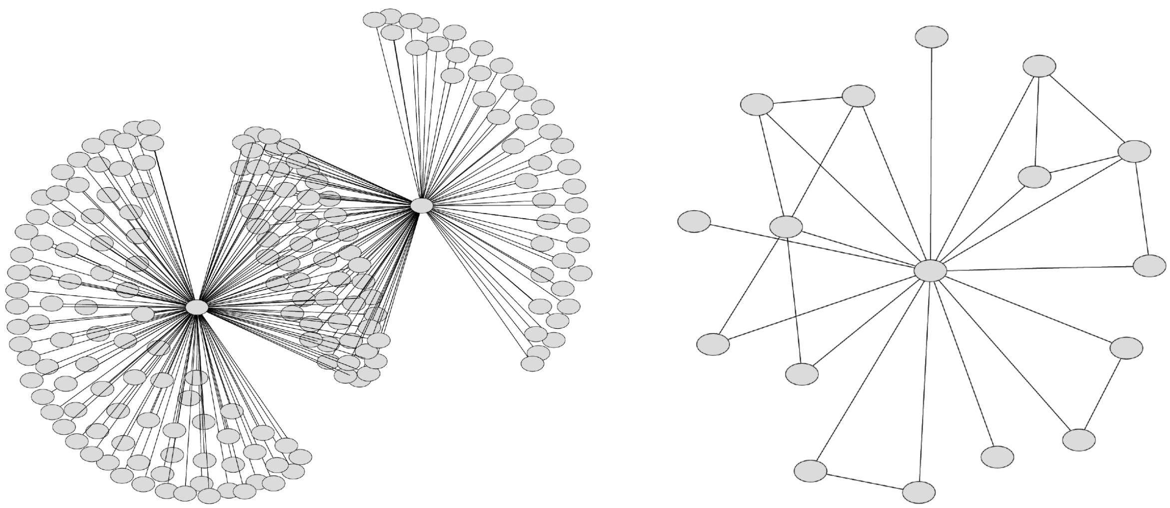

Figure 3: Spam Component (left) and Legitimate Subcomponent (right), reprinted with permission (Boykin & Roychowdhury, 3).

A test of this model proved it remarkably stable. Based on a data set of nearly 5,500 archived email messages, Boykin & Roychowdhury were able to construct a network context and its corresponding whitelist and blacklist. Applied to an email archive compiled from one of the author's actual inboxes, the algorithm correctly identified 53% of the messages as either spam or non-spam with 100% accuracy. The algorithm did not classify the remaining 47% into either category. The accuracy of this filter is amazing. To reiterate, false positives are several orders of magnitude worse than false negatives. This algorithm, however, does not sacrifice false negatives in order to reduce false positives.[iii]

Two anomalies arise in this model. First, some subcomponents are so small that the clustering coefficient is unstable. Removing or adding a single edge would change the coefficient greatly. These subcomponents are not classified, and messages originating in these subcomponents comprise the 47% of emails that were not classified in the above experiment. The second anomaly occurs when a spam email happens by chance to include two recipients who belong to the same legitimate subcomponent. The algorithm then connects the spam subcomponent to the legitimate subcomponent, and the clustering coefficient becomes an intermediate value that is ambiguous. To resolve this situation, Boykin & Roychowdhury use a graph theoretic statistic called *edge betweenness*. This statistic, designed to measure the extent to which a particular edge bridges two communities in a graph, is computed by counting how many shortest paths between all pairs of vertices include that edge. By removing the edges with highest betweeness one at a time, the subcomponent will eventually break into two, smaller subcomponents. The process is repeated until subcomponents can be identified unambiguously as either spam or legitimate, or else they get so small as to be unclassifiable.

Boykin and Roychowdhury also point out that their filter integrates well with statistically based, textual filters. Those kinds of filters need to be "trained" by being provided with example emails that are already classified as being either spam or legitimate. Many of these filters are trained first by the software developers, and then the end user tweaks the training by running the filter on some of his own personal email. Because the network-centric filter can positively identify over 50% of e-mail as either spam or legitimate, it can also provide a training set for a statistical filter as well, which takes the burden of training off of the end user.

The combination of these two techniques represents a very new way of dealing with technological networks. In reality, technological networks are economic networks as well, because economics applies wherever there exists demand for scarce resources. At the same time, technological networks encode meaning into their own topologies. In the case of the global e-mail network, that meaning can be discerned by analyzing the network topology with a few simple statistics. Surprisingly, however, agents within a network rarely consider the topology of the network. In some cases, it is impossible to construct the entire network; even then, local topology is usually available. It is this *network context* that makes network theory very useful. An agent who can discern the structure of the network around him can use that information in powerful ways.

IV. Internet Routing and Peering

Similar to many social and economic networks, the Internet has formed in a decentralized fashion. Currently the Internet comprises a number of autonomously managed networks, each known as an Autonomous System (AS). In order to provide connectivity for the Internet, autonomous systems must establish links to one another. Each link connects one autonomous system to another autonomous system, and there are two types of links possible: transit and peering. In a transit link regime, one autonomous system pays the other in proportion to the network traffic going over the link that originates from its own side and vice-versa. Transit link regimes are rare at high levels – between the largest providers – because measuring Internet traffic is a tedious task that requires a significant amount of overhead. Peering regimes are links between autonomous systems with no monetary exchange or traffic constraints.

This simple depiction of peering in the Internet ought to provide an intuition about Internet routing: there exists a perverse incentive to direct as much traffic to your neighbors as possible, since the marginal costs are nil. If there exists a fixed cost for maintaining a peering link, but no marginal cost for traffic over that link, then each autonomous system will exploit that link as much as possible.

The autonomous system network is complete, i.e. there is at least one link between every autonomous system. If this were not the case, then that autonomous system would not be able to connect their users to every part of the Internet. When there are multiple links between a pair of autonomous systems, however, each autonomous system can exploit the placement of this link to their own advantage. The net result is that the overall performance of the Internet is lower than it could be if peering links were planned by a third party whose only interest was to maximize the Internet's performance. Therefore, Internet routing can be conceived of as a planning problem. A variable of interest when analyzing planning problems is known as the *price of anarchy*, which is the ratio of total benefit under a centrally-planned regime to total benefit under a decentralized regime. The price of anarchy is a concept that tries to capture the magnitude of dead-weight loss that results from selfishness. Numerous papers have analyzed the price of anarchy in Internet peering, and estimates of inefficiencies range from 33% to 80% (e.g. Roughgarden, 9).

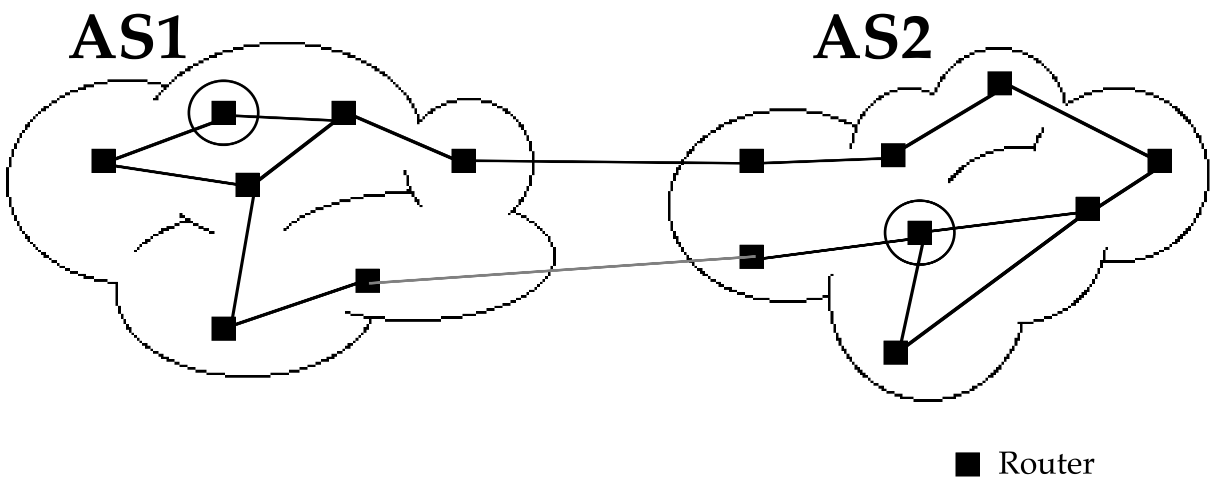

Figure 4: An example peering configuration.

A quick graphical example will demonstrate how peering links are exploited. In Figure 4, each cloud represents a single autonomous system. Each black box represents a router, and lines between routers indicate network connections. There are two peering links between AS1 and AS2. Suppose that the router in AS1 which is circled wants to send a packet of data to the router in AS2 which is circled. The distance to the top link is only two hops: the data packet only goes through two routers before jumping into AS2. The distance to the bottom link is 4 hops, however. All other things being equal, it takes longer to get a packet to the bottom link than to the top link. Since each hop requires bandwidth and processing resources, AS1 will enforce a routing policy that always forwards packets from the circled router to the top link.

This policy is inefficient from a global perspective, because when the packet enters AS2 it takes six hops to reach its destination. In total, the packet traveled eight hops, but if AS1 had sent the packet on the bottom link, it would have taken six hops to reach its destination. Therefore, AS1's selfish routing policy leads to a 33% dead-weight loss versus the globally optimal solution. This loss is the price of anarchy; by forgoing centralized planning and instead allowing self-interested, rational actors to determine an equilibrium outcome, the global outcome is inefficient. It is also important to note that not only is this outcome inefficient in the global sense, but one autonomous system shoulders most of the cost.

The above example is contrived to an extent because it imposes an unlikely network topography onto each autonomous system. This was only done for simplification, however. In reality, routers and connections between routers are not made equal. In fact, since the infrastructure of an autonomous system is developed over time in an iterative process, it is guaranteed that some routers are capable of handling more traffic than others and some connections have more bandwidth than others. Each autonomous system will have an incentive to route traffic away from these weak spots; otherwise, they would need to spend money upgrading the equipment to handle the increased load. Therefore, autonomous systems all use a routing policy called "nearest exit." The idea is to forward the packet to the neighboring autonomous system using as little of their own resources as possible. This routing policy is also called "hot potato" – referring to the fact that autonomous systems want to hold on to data traffic for as short a time as possible.

Unfortunately, the solution to selfish peering in the Internet is not easy. Centralized planning is neither feasible nor appealing. If the problem is construed as a tragedy of the commons, then the Coase Theorem applies: declare property rights and an efficient outcome necessarily results. But the Coase Theorem does not guarantee an equalitarian outcome, and assigning property rights to shared links would be arbitrary and unfair. Ideally, autonomous systems would be forced to internalize costs by switching to transit regimes and paying fees for bandwidth induced on interdomain links. As mentioned above, this solution is generally infeasible for large providers because of the sheer volume of data flowing along these links. The overhead required to track the amount of data coming and going currently outweighs the cost savings.

Technology tends to get more powerful and less expensive at the same time, so that transit regimes may become feasible in the future. The question that remains is whether the feasibility of transit regimes will encourage autonomous system behavior that results in the globally desired outcome. There are two types of loss incurred in the current peering regime: the global loss in efficiency and the potential costs incurred by unequal usage of the peering link. To this end, Corbo and Petermann model interdomain linking in game theoretic terms. The two autonomous systems are players in a repeated game. Each autonomous system has a network that it would like to connect to the other autonomous system's network. There is a very high penalty for being disconnected. Each autonomous system pays costs for the amount of traffic on their network, as well for the maintenance of the interdomain link. On each turn, one autonomous system randomly decides to propose either adding a link or removing a link. If the link is acceptable to both autonomous systems then it is added. Either autonomous system can unilaterally remove a link.

Corbo and Petermann applied this game theoretic model to networks that are similar to small world networks. They used a generative model called preferential attachment, which results in networks that have small diameter and heavy-tailed degree distribution but almost no clustering. They found that the number of peering links is very sensitive to the price of peering links; the number of links established vanishes rapidly as the price rises. Although the equilibria are robust to differences in size between the two autonomous systems, they are very sensitive to asymmetries in traffic flow between the two.

> We note a paucity of stochastically stable peering configurations under asymmetric conditions, particularly to unequal interdomain flow, with adverse effects on system-wide efficiency. The volatility of peering relationships in the face of perceived asymmetries suggests that peering will become increasingly rare as traffic and cost monitoring become more accurate and available. (Corbo & Petermann, 6)

Although research in this area is ongoing, these early results indicate that as technology provides the tools to make transit regimes feasible, autonomous systems should spontaneously adopt them. As a side effect, transit regimes will bring about the globally desired effect of improving overall latency and resource utilization. This result follows from the Coase theorem: transit regimes declare property rights and the efficient outcome necessarily results. Like the spam email problem, selfish peering in the internet demonstrates the need for an economic point of view on technological problems.

V. Graphical Economics

Graphical economics is the study of economic interactions in the context of graph theory. Generally, this means that economic interactions are constrained by the topology of the graph. For example, two economic agents can exchange only if they have an edge between them, or trade between two markets is allowed only if they have an edge between them. These constraints are not necessarily arbitrary either. Most classical economic models can be construed as taking place on a graph that is complete, i.e. a graph where every vertex is directly connected to every other vertex. Therefore, those classical economic models are actually just a special case of graphical economics. Since graph theory and network theory are so closely related, it makes sense to co-opt graphical economics into network economics. In fact, the main difference between graphical economics and network economics is that graphical economics is unconcerned with topology. Network economics projects an expected topology onto a graph, such as the small world topology. With this slight distinction in mind, the terms network and graph will be used interchangeably in this section.

Modeling economic problems on incomplete networks makes intuitive sense. Consider an economy consisting of multiple, disparate marketplaces. In order to buy or sell in one of these marketplaces, an agent must physically go to that marketplace. Those agents clearly pay a cost for each market they visit, yet as they visit more markets they have a wider range of other agents to buy or sell from. Intuitively, there ought to be an equilibrium that balances the benefit of participating in multiple marketplaces with the costs of monitoring those marketplaces. The same principle applies in a more familiar setting: an individual interested in buying a particular good is only willing to go to a handful of stores to find the lowest price. Therefore, there is a limited amount of connectivity between producers and consumers, and local variations in price should result.

The first graphical economic problem to be considered is the "brain-dead" model of exchange (Kearns, 17). Each vertex represents an economic agent and an edge between two agents represents the ability for them to exchange. All agents begin with an initial endowment. At each time step, every agent divides his wealth equally among all of his neighbors and distributes it to them. At the same time, therefore, each agent also collects a small payment from each his neighbors. Regardless of the topology of the network and the distribution of initial endowments, this model always converges to a predicable, static equilibrium. The percentage of the overall wealth possessed at each vertex is equal to the ratio of that vertex's degree over the total number of edges in the network.

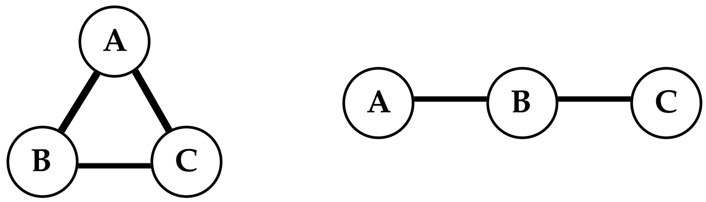

Figure 5: Two examples of network topology.

As a simple example, consider the first of the two network topologies presented in Figure 5. Imagine that agents A, B and C have initial endowments of 3, 2 and 1 respectively. In the first time period, agent A will distribute 1.5 to B and 1.5 to C. B will distribute 1 to A and 1 to C, etc. At the end of the first time period, A, B and C will have 1.5, 2 and 2.5 respectively. Aggregate wealth obviously remains the same, but disparity decreases: initially the wealthiest node A controlled half of the wealth, but after one time period the wealthiest node controls only 42% of the aggregate wealth. After another time period, A, B and C will have 2.25, 2 and 1.75, and the wealthiest node only controls 38% of the aggregate wealth. After a few more iterations, the wealth distribution becomes nearly uniform. In the second network topology, the wealth distribution converges, but it converges to a non-uniform distribution. Specifically, A, B and C will have 1.5, 3 and 1.5 at equilibrium.

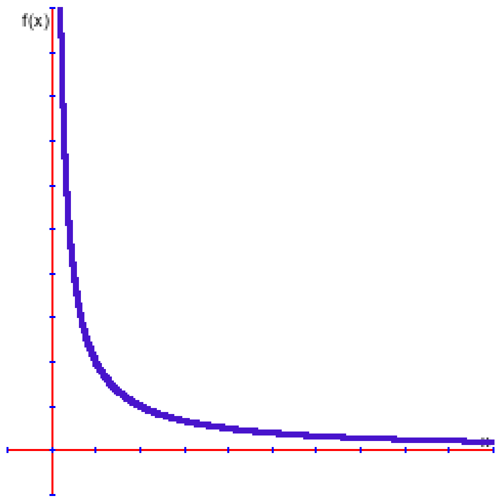

Figure 6: A power law function.

In this model, it pays to have a large number of neighbors relative to everybody else. The first network topology is complete: every vertex is connected to every other vertex. The result is a uniform distribution of wealth. In real life, economic networks are typically not complete; thus, local variations arise at equilibrium. If economic networks are constrained to be small world networks, then the wealth distribution at equilibrium takes on a more significant meaning. One of the key characteristics stipulated for small world networks is their heavy-tailed degree distribution. Network theorists use a function called a power law to model these degree distributions. A power law is a hyperbolic function of the form: $f(x) = k / x^{\alpha}$. Figure 6 visualizes this function for $k = 1/2$ and $\alpha = 1$. This function is related to a number of naturally occurring distributions, as noted by George Zipf in Zipf's law: income distribution, sizes of cities, and occurrence of words in large texts. Figure 7 confirms a Zipf distribution for GDP in the fifty wealthiest nations in the world. An informal comparison of the two figures reveals congruity. Connecting the top of each bar in Figure 7 to its adjacent bars traces a line just like the one in Figure 6.

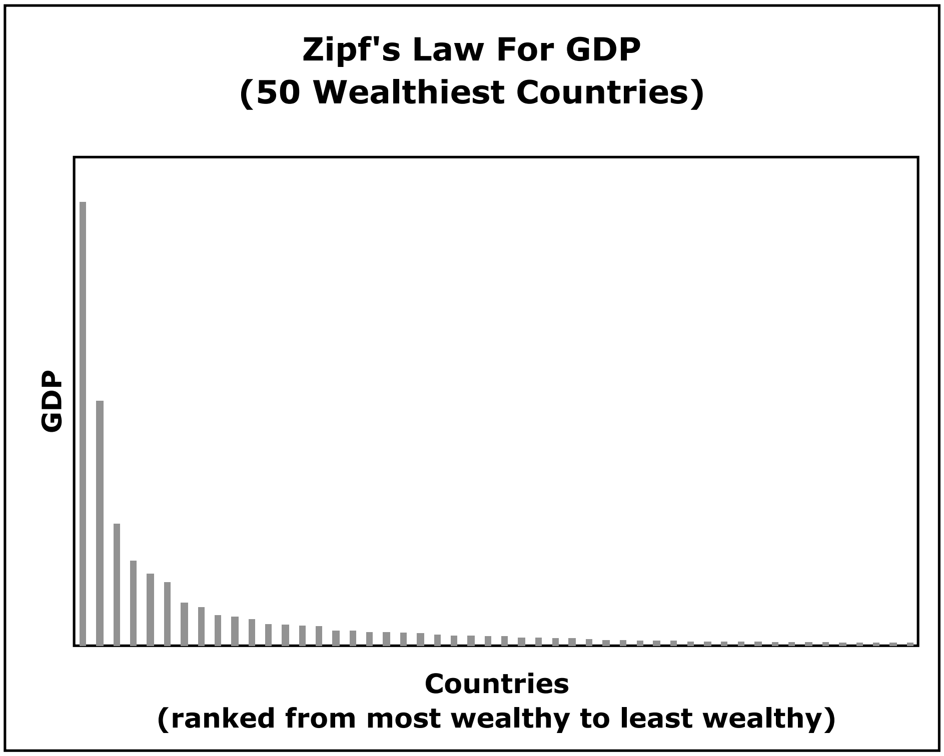

Figure 7: Zipf Distribution for GDP.

Although this brain-dead exchange model is a drastic simplification of the complex dynamics of economic exchange, it has merit. The model describes a sort of socialism, where each individual produces as much as possible with the inputs he is given and then shares equally with all neighbors. In such a society, those who share more will get more back.

A better model is desirable, of course, and it is possible to adapt any general economics equilibrium model to a graphical model. Kakade, Kearns, and Ortiz demonstrate Arrow-Debreu equilibria on incomplete economic networks, i.e. networks where trade is constrained so that not all pairs of agents can trade directly with each other. Under roughly the same assumptions that Arrow-Debreu requires, they prove the existence of a general equilibrium for the graphical Arrow-Debreu. Another interesting result is that, like the brain-dead model presented above, the graphical Arrow-Debreu model allows for local variations in price.

In a general Arrow-Debreu model, there are a number of agents each with a specific initial endowment; there are also a number of goods that these agents have utility for. The price for each good is constant for all players. Each player sells his initial endowment and then uses that revenue to buy goods so as to maximize his utility. Assuming that agents' utility functions are monotonically increasing, i.e. they generally prefer more of a good to less of it, then Arrow and Debreu show that there is a set of prices for which the market clears. That is, there exists a set of prices so that demand exactly equals supply.

The graphical Arrow-Debreu model proceeds in the same fashion, except that each agent is constrained to only buy from or sell to his neighbors in the network. In this case, the market clears at each vertex. That is, each vertex has each good supplied to it in exactly the quantity it demands, given the prices for each good. This local clearance condition guarantees, of course, a global market clearance as well. The only difference between the graphical Arrow-Debreu equilibrium and the classic is that the graphical model allows a different set of prices at each vertex.

Consider again the network topologies in Figure 5.[iv] In these markets, there are two goods. Agent A has linear utility for good 1 only, B has equal, linear utility for both goods, and C has linear utility for good 2 only. Agent A has an endowment of (1,2), B has (1,1) and C has (2,1). In the first network, a price set that establishes equilibrium is (1,1). At these prices, Agent A sells his endowment for 3, B sells his for 2, and C sells his for 3. Agent A ends up with a consumption bundle of (3,0), B has (1,1), and C has (0,3). The network is reproduced in Figure 8 with annotations indicating the equilibrium outcome. Notice that a single set of prices clears the market because the graph is complete. In other words, the graphical equilibrium in the first network is a general Arrow-Debreu equilibrium as well. This result is expected because the classical Arrow-Debreu is just a special case of the graphical Arrow-Debreu, and the first network represents that special case of a complete trading network.

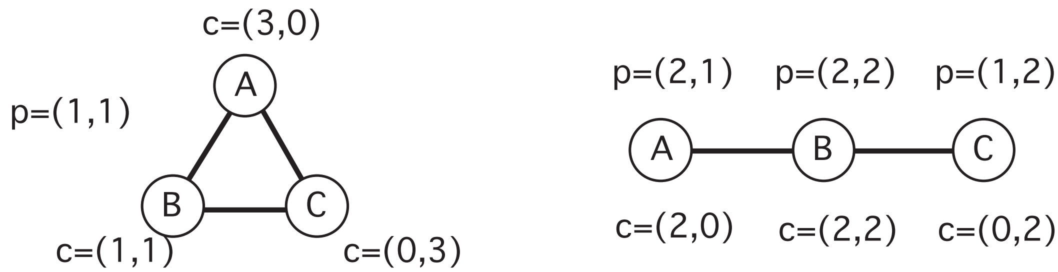

Figure 8: Equilbrium outcomes in two different networks.

The second network is not complete, however, and given the same utility functions and endowments the equilibrium is quite different. In fact, the only way to clear the market globally is for each agent to charge a different set of prices for the goods. In equilibrium, Agent A charges (2,1) for goods 1 and 2, respectively, B charges (2,2), and C charges (1,2). Now B sells his initial endowment for 4, while A and C sell their endowments for 3 each. Agent A ends up with a consumption bundle of (2,0), B has (2,2), and C has (0,2). Compared to the first network, agent B has doubled his consumption of each good, which comes at the expense of agents A and C who each lose a unit of consumption. Therefore, agent B has profited by acting like a broker to agents A and C, who had mutually desirable endowments but were unable to trade directly with each other. This scenario comports with the real-world reality of imperfect information. If a buyer and seller cannot find each other, a third party can profit by buying from one and selling to the other. Therefore, incomplete information, which creates incomplete trading graphs, can lead to local price variations. This is an intuitive result that is powerfully confirmed by this example.

Kakade et. al. compute a graphical equilibrium for a larger network (7) and find that price variations arise, with highly connected vertices tending to have a higher utility than others. Unlike the brain-dead model, however, utility is not directly correlated to degree. Instead, other subtle factors affect utility. A vertex that has only a few neighbors can have a high utility if those neighbors do not have any other neighbors of their own. In that case, the vertex profits by having a captive market for its goods – essentially a monopoly. Intuitively, we might also expect that clusters will demonstrate local minima of prices because of the high degree of competition and vertices with high betweenness stand to profit from arbitrage; these results have not been proven yet.

Calculating graphical equilibria is quite complex, especially for very large graphs. These calculations suffer from combinatorial explosion, a mathematical term which refers to the fact that the possible combinations of buyer and seller becomes huge when there are only a few hundred vertices in the graph. Kakade et al. in their 2004 paper propose an algorithm called ADProp that scales exponentially with the number of edges in the graph. A small increase in the number of edges results in a huge increase in the running time of the algorithm. ADProp scales polynomially with the number of vertices, however, which is a big improvement over previous, non-graphical algorithms (Kakade, et al., 13). Algorithms that solve these problems tend to use iterative methods that achieve rough solutions very quickly and then slowly converge to the true minima by minimizing an error term. Iterative algorithms sometimes fail to find the true minimum, converging to a local minimum instead. Although imperfect, iterative algorithms are still desirable because they make computer experiments feasible.

Augmenting traditional economic equilibrium models with network theoretic constraints and computer experiments permits new insights. Specifically, the local variation in prices reflects the reality of incomplete information better than classical models do. Also, graphical economics may provide insight into inequities in wealth distribution. The next section demonstrates the application of network economics to a practical case study, with the intention of understanding how network structure affects wealth.

VI. International Trade

The principles of network economics are applicable to a broad range of real-world problems. One interesting network that has attracted previous research is the network of international trade partners (e.g. Kakade, et al., 7-8). In this paper, the international trade network is defined as follows: every nation or semi-autonomous region (Hong Kong, for example) that reported any trade in the year 2004 is a vertex in the network. An edge exists between any two vertices for which the aggregate trade between the two exceeds some threshold k. Adjusting k up or down affects the edge density of the network, so in order to yield an informative but manageable data set I have selected $k=\$1bn$.

The data for this network was extracted from the United Nations Statistics Divisions' Comtrade Database. This database provides (self-reported) data on the amount of trade between nations measured in thousands of U.S. dollars. The dataset has some ambiguities that impede rigorous statistical analysis. Some countries' reports conflict; for instance, Albania reports imports from Algeria totaling 179,761,000 but Algeria does not report any exports to Albania. Therefore, aggregating trade data is error-prone, but the resulting network should still be meaningful.

The network was extracted using a custom java application that tracks all import and export records and sums their values for each pair of countries. The application then outputs the network in the *dot* format, a file format for network graphs that is useful for rendering graph visualizations. At a threshold of *k=$1bn*, the resulting network has 237 nodes and 993 edges. This graph is complex enough to defy the method of visual inspection used in Section V. Figure 9 is a high-level visualization of the network. If this visualization was enlarged enough to be readable, the visualization would be twenty feet square. Even at this small size, it is possible to discern the existence of perhaps thirty to forty highly connected nodes where a number of edges cross and form a dark black star. Also, the layout algorithm used to render this network visualization tries to place central nodes towards the middle of the diagram.[v] Otherwise, the visualization is far too small to be useful. Statistical analysis and analysis of specific subcomponents will be necessary to infer meaningful information from this graph.

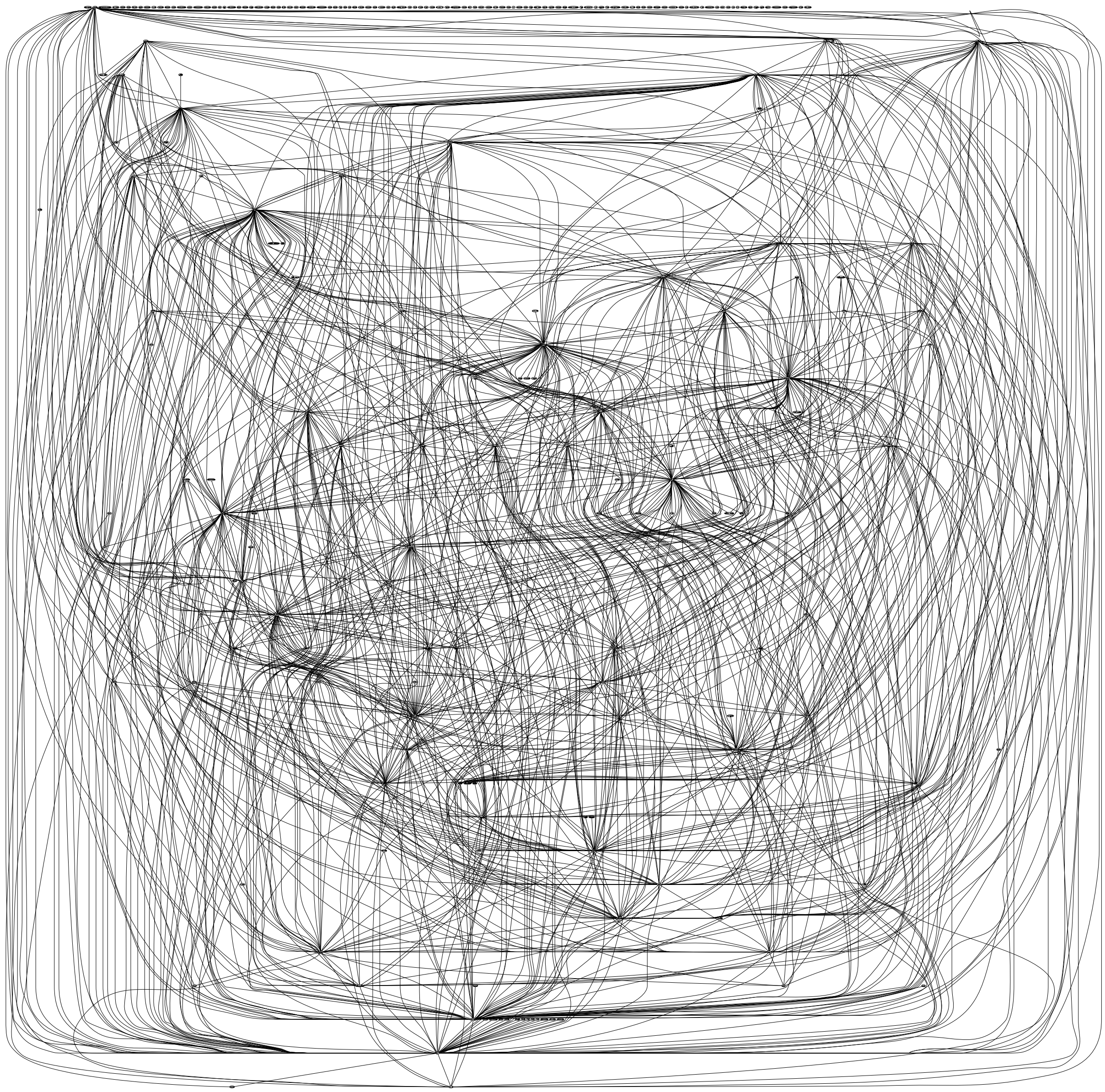

Figure 9: High-level Visualization of the Global Trade Network, k=$1bn.

First, it will be useful to determine whether this international trade network conforms to the properties of a small world network. Recall that "small world" implies that a network has small diameter, high clustering, and heavy-tailed degree distribution. The term has nothing to do with the fact that the network at hand is based on international trade. These three characteristics are only very meaningful for a connected graph; therefore, the first step in this analysis is to remove all vertices with degree zero from the graph. This leaves a connected graph with 131 vertices and 993 edges. The diameter is computed with Floyd's algorithm and the clustering coefficient is computed by using Eq. 1.

$$C(g) = \frac{1}{N} \sum_{n \in g} \frac{2y_n}{z_n(z_n - 1)} \qquad \textbf{(Eq. 1)}$$

In this equation, *g* is the graph for which we are computing the clustering coefficient *C(g)*. For each node *n* in the graph *g*, the ratio of the actual number of edges y_n connecting *n*'s neighbors to each other is divided by the total possible number of edges that could exist between *n*'s neighbors. Then the clustering coefficients are averaged across all nodes to find the clustering coefficient for the graph. The data for the connected component of the international trade graph are given in Table 1. The diameter is very small and the clustering coefficient is very high – the characteristic small world qualities. The maximum possible clustering coefficient is 1.0, which occurs only when the graph is complete. As a comparison, Duncan Watts reports that the clustering coefficient of the neural network of C. Elegans is 0.28 and the coefficient for the national power grid is 0.080 (Watts, 96).

Nodes	131
Edges	993
Diameter	2.13
Clustering Coefficient	.59
Mean Degree	15.2
Median Degree	6

Table 2: Global Trade Network Statistics.

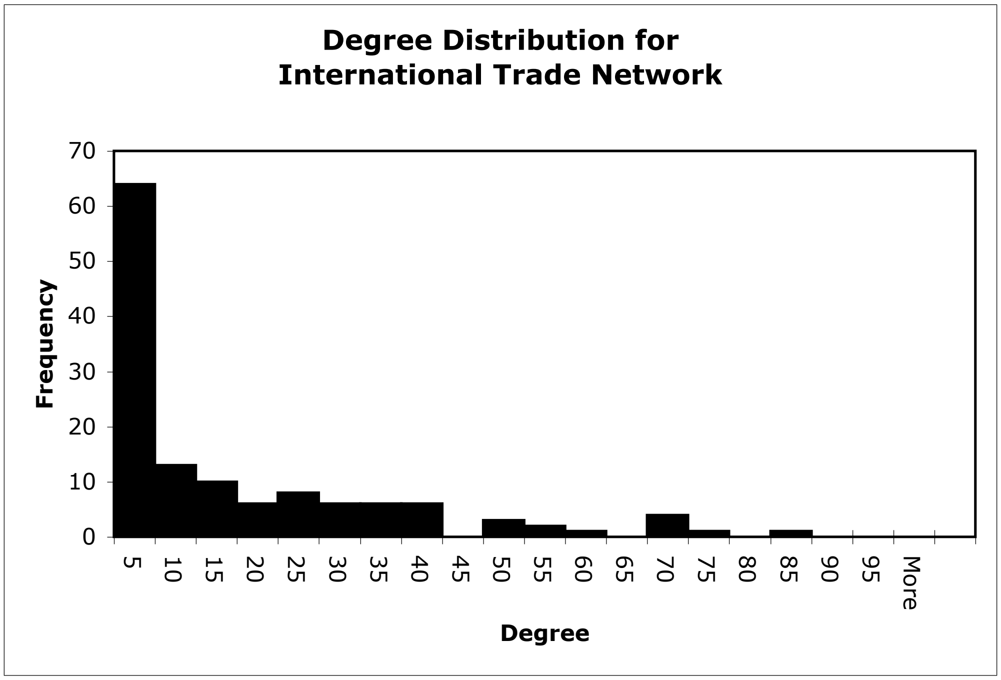

Figure 10: Degree Distribution.

The degree distribution of the connected component of the international trade graph is presented in Figure 10. For each bin, the graph shows the number of countries in that bin. For instance, in the *1-5 bin*, there are over 60 countries, but in the *6-10 bin* there are just over 10 countries. This degree distribution clearly shows a significantly heavy-tailed degree distribution. The U.S.A. and Germany are the top two, with degrees of 84 and 74, respectively. Intuitively, it makes sense that two nations known for heavy industry should have numerous significant trade links. This data supports the conclusion that the international trade network displays distinct small world characteristics.

The next mode of inquiry is to look at interesting subcomponents of the graph, such as areas of the graph that have free trade agreements. Two prime examples are the European Union (EU) and the Association for Southeast Asian Nations (ASEAN). The network visualizations for these two countries are presented in Figure 11 and Figure 12. The European Union trade network has twenty-three vertices and one hundred thirty-six edges. The ASEAN trade network has eight nodes and nine edges. Two nations in the ASEAN are disconnected.

	EU	ASEAN
Nodes	23	8
Edges	136	9
Diameter	1.41	1.17
Clustering Coefficient	.799	.678
Mean Degree	11.8	3.00
Median Degree	13	3

Table 3 summarizes the key statistics for the EU trade network and for the connected component of the ASEAN trade networks.

	EU	ASEAN
Nodes	23	8
Edges	136	9
Diameter	1.41	1.17
Clustering Coefficient	.799	.678
Mean Degree	11.8	3.00
Median Degree	13	3

Table 3: Network Statistics for EU & ASEAN Trade Networks

The clustering coefficient for both of these free trade areas is very high, which could be a result of the economic incentive to trade provided by free trade agreements. The diameters are roughly equal, but because the ASEAN is a much smaller network the small diameter is not surprising. The EU's diameter is significantly small, however, considering that there are twenty-three vertices. The degree distributions for these two networks are presented in Figure 13. The distributions are nearly flat, *not* heavy-tailed like small world networks. Degree seems to decrease linearly with decreasing rank, implying perhaps that those nations who entered into these free trade regions already belonged to the same economic class, where each nation's trade was constrained to be in the same order of magnitude as the other member nations.

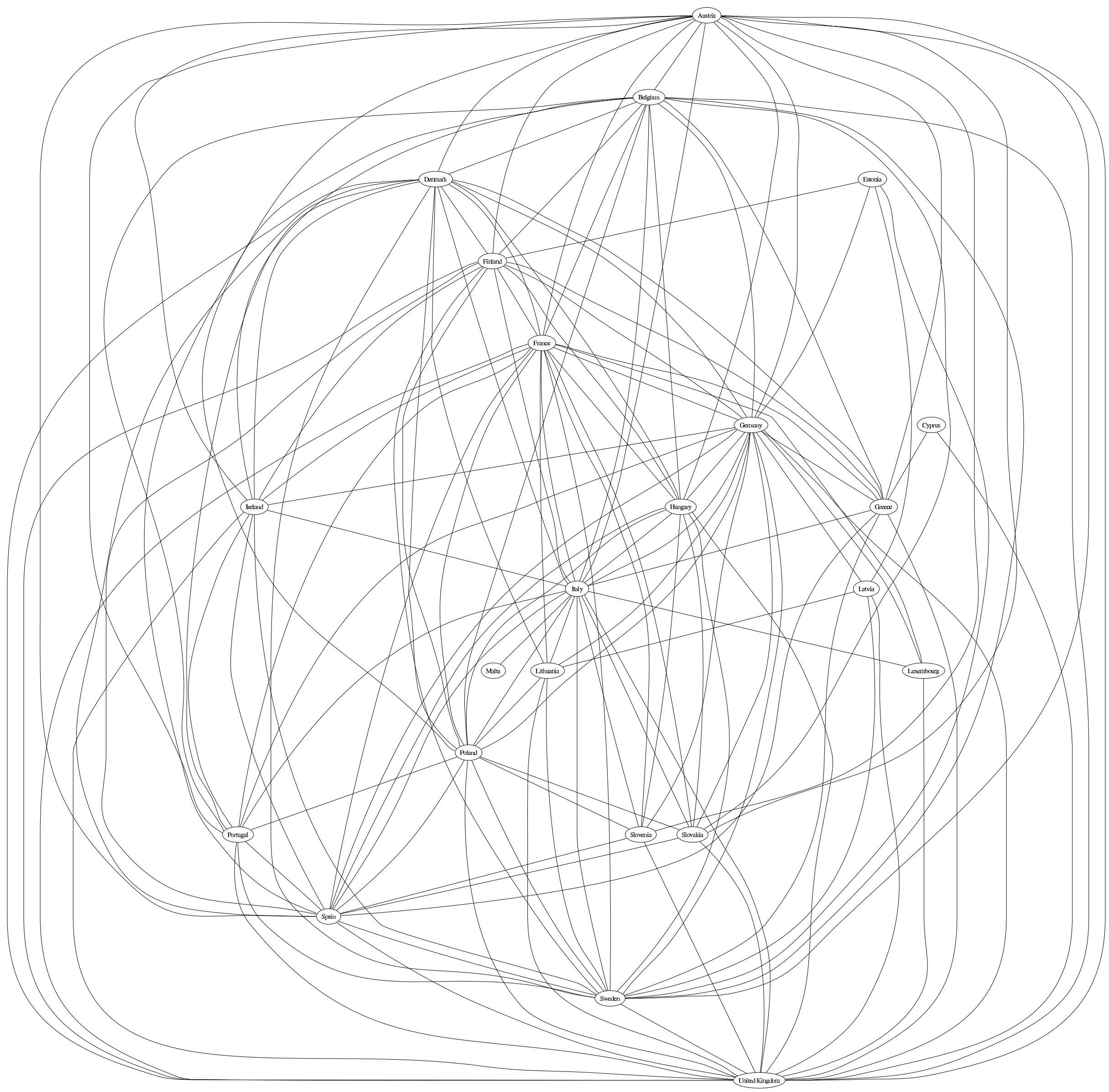

Figure 11: Visualization of the EU Trade Network.

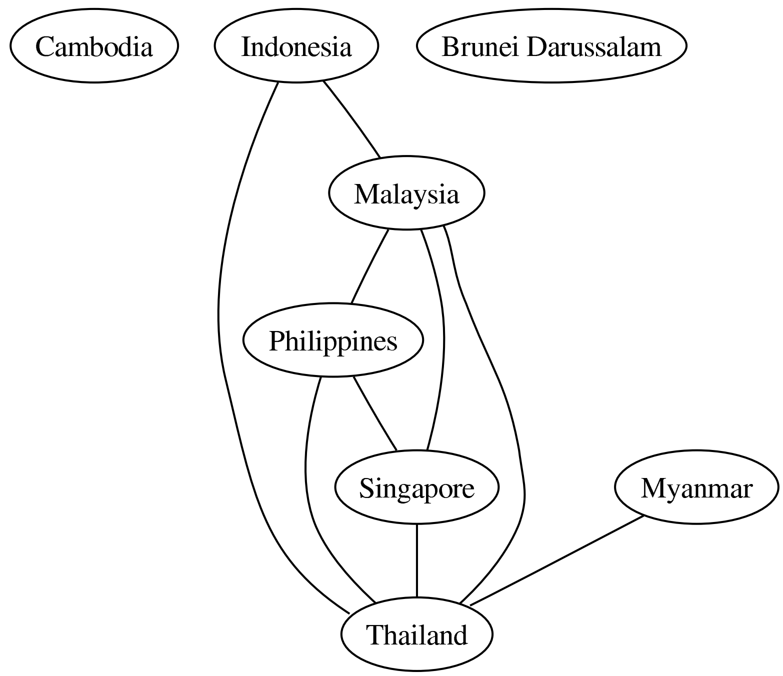

Figure 12: Visualization of the ASEAN Trade Network.

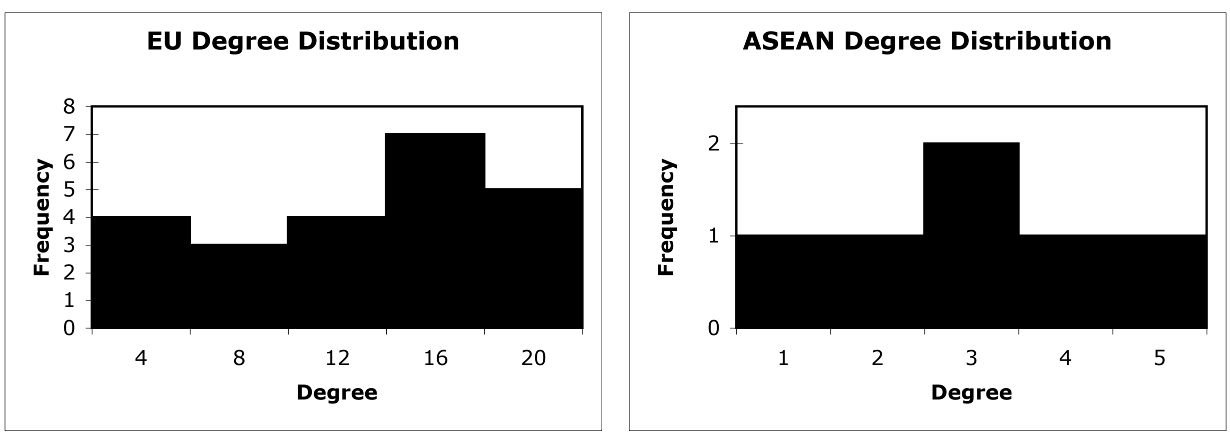

Figure 13: Degree Distributions of the EU and ASEAN Trade Networks.

The final analysis compares how degree affects GDP. For the twenty-three EU nations, the GDP per capita for each member state has been plotted against both that state's degree in the international trade network and that state's degree in the EU trade network. In Figure 14, the vertical axis on the left measures the degree of a state in the international trade network; the vertical axis on the right measures the degree of the state in the EU trade network. The black dots represent degree in the international trade network and gray dots represent degree in the EU trade network. GDP per capita is reported in thousands of U.S. dollars. Interestingly enough, there is almost no correlation between GDP per capita and degree. The scatter plot shows a least-squares regression linear fit; the coefficient of the GDP per capita term is almost zero, implying a very weak or nonexistent correlation. The r-squared term indicates that GDP has very little explanatory power for degree.

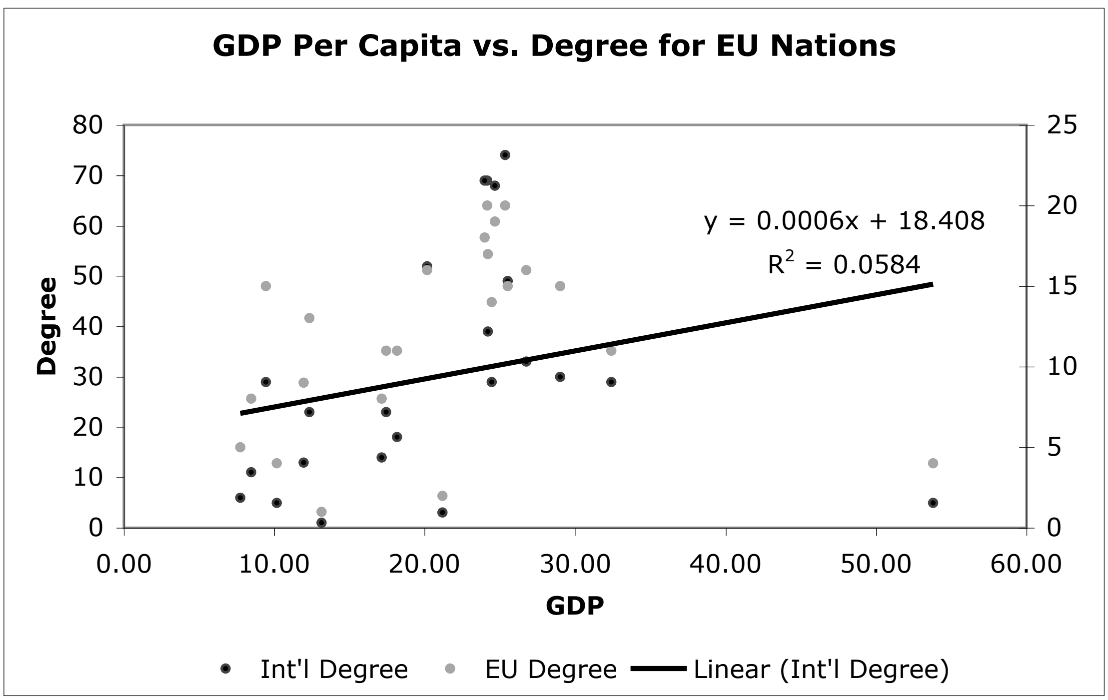

Figure 14: Correlating GDP to Degree.

Removing Luxembourg, the obvious outlier in the bottom right corner of the scatter plot, increases the r-squared term to .35. This result comports with the conclusions from the graphical Arrow-Debreu model in Section V: in an economic exchange network, degree is a significant but not comprehensive predictor of wealth. The law of comparative advantage states that each country should concentrate on producing only those goods in which they are comparatively efficient and acquire the rest of the goods they need through trade. Intuitively, the law of comparative advantage and free trade should result in higher wealth for countries that trade more, because they use their labor more efficiently that way. In other words, wealth should be partially correlated to high degree. This simple analysis is insufficient to determine the direction of causality, but degree and wealth are correlated.

VIII. Closing Remarks

There are several important themes brought out by the case studies in this paper. For one, it has become clear that many technological systems would benefit by the application of economic principles. Spam email and Internet routing are just two examples. In general, whenever many users are competing for scarce resources, economic principles will apply. When local incentives are perverse, the global equilibrium will be inefficient. When designing systems such as the next Internet protocol or the next email protocol, designers need to consider how the local payoffs to each user will be crafted in order to promote the ideal global equilibrium. This is a familiar problem for economists, the social planner problem, and it is well understood and thoroughly researched.

At the same time, network theory is providing new tools for economists. As stated above, network economics is really just a generalization of classical equilibrium models. It is an intuitive generalization, however, and it yields more realistic results than previous models without adding unnecessary complication. One important conclusion is that network topology affects the nature of economic outcomes. By imposing various network topologies that resemble real world economic networks, we can understand how information and connectedness affect market activity and wealth.

Additionally, network economics can help explain what happens as the edge density of an economic network increases. Links are established in economic networks by information: the more markets one can surveil, the greater bargaining power he has. The modern era is characterized by an ever-growing stream of information. Shopping on the Internet, for instance, allows consumers to make track prices across many more suppliers than was previously feasible. By creating more links between consumers and producers, information increases the edge density of the network. As a result, price variation should drop. This conclusion is supported directly in the Arrow-Debreu model.

Computational experiments should be a major focus for network economics in the near future. Because of complexity issues, progress will be made most quickly by running simulations of economic models on various network topologies and measuring how various outcomes correlate to various network statistics such as diameter, clustering, and degree distribution. Hopefully, a deeper understanding of network economic interactions can be developed. This knowledge would be useful both in business – to study profit making opportunities – but also in public policy. With an understanding of network structure and its relationship to information and economic outcomes, public policy can focus on how best to inform consumers.

Bibliography

Boykin, P. Oscar and Vwani Roychowdhury. "Personal Email Networks: An Effective Anti-Spam Tool." University of California, Los Angeles. Feb 3, 2004.

Corbo, Jacomo and Thomas Petermann. "Selfish Peering and Routing in the Internet." Harvard and Cambridge Universities. 2004.

France, Mike. "Needed Now: Laws to Can Spam". Business Week. Sept 26, 2002. <http://www.businessweek.com/smallbiz/content/sep2002/sb20020926_5958.htm>

Goodman, Joshua, David Heckerman, and Robert Rounthwaite. "Stopping Spam." Scientific American. April, 2005.

Kakade, Sham M., Michael Kearns, Luis E. Ortiz, Robin Pemantle, and Siddharth Suri. "Economic Properties of Social Networks." University of Pennsylvania. 2004.

Kakade, Sham M., Michael Kearns, and Luis E. Ortiz. "Graphical Economics." University of Pennsylvania. 2004.

Kearns, Michael. "The Network Nature of Society." CSE-112 class notes. University of Pennsylvania. 2005.

Leung, Andrew. *SPAM: The Current State*. TELUS Corporation. 2003.

Milgram, Stanley. "The Small World Problem." *Psychology Today*. May 1967: 60-67.

Osterman, Michael. "Spam not at economic equilbrium." *Network World Fusion*. Feb 11, 2003. <http://honolulu.hawaii.edu/legacylib/mlahcc.html>.

Roughgarden, Tim. "Selfish Routing." Cornell University. May 2002.

Watts, Duncan J. *Six Degrees: The Science Of A Connected Age*. New York: W. W. Norton & Company, Inc. 2003.

World Population Prospects: The 2004 Revision Population Database. United Nations. <http://esa.un.org/unpp/>.

Yolkowski, James. *The Mathematics Lair*. "The Mathematics Lair – Really Large Numbers." 2002. <http://www.stormloader.com/ajy/reallife.html>.

Endnotes

[i] E.g. http://www.mail-abuse.com/lookup.html or http://www.spews.org/

[ii] Once again, network externalities imply a different meaning for *network* than I am generally intending in this paper. A positive network externality simply means that a good becomes more desirable as others' consumption of it increases. E.g., I am more likely to purchase Microsoft Word because everybody else uses it; I might value the program itself below its competitors but the desire to be as compatible as possible overrides that valuation.

[iii] The whitelist and blacklist in this model are much more versatile than those currently in use. In order to contact Boykin & Roychowdhury to request permission to reprint their diagrams, I sent Boykin an e-mail with a Cc: to Roychowdhury, and the network-centric model infers that my email is legitimate simply because I emailed them both simultaneously. Boykin's filter sees that I am connected to Roychowdhury because his email address and my email address are in the same header. Therefore, Boykin can be confident that the message is not spam, even though I am a perfect stranger to him and we likely do not have any common acquaintances. If Boykin had a static whitelist (like most in use today), I would have difficulty reaching him by email without communicating by some other medium first.

[iv] This example is based on an example presented in Kakade, et al., 6-7.

[v] See http://www.graphviz.org/ for more information about the visualization software.